Topics in Commutative Algebra

Lecturer: Tamás Szamuely
Typed by: Szabolcs Mészáros

January 3, 2016

Remark. This is the live-texed notes of Topics in Commutative Algebra course held by Tamás Szamuely in the winter of 2015. Any mistakes and typos are my own.

First Lecture, 13th of January

Literature:

- Matsumura: Commutative Ring Theory (useful encyclopedia-type reference book)
- Atiyah - MacDonald: Introduction to Commutative Algebra
- Eisenbud: Commutative algebra with a view toward Algebraic Geometry
- J. de Jong et al.: The Stacks Project (www.math.columbia.edu)

Outline:

1. Krull's Hauptidealsatz (principal ideal theorem)
2. Cohen's structure theorem for complete local rings)
3. Serre's characterization of regular local rings by homological dimension
4. Notion of depths in local rings
5. Cohen-Macaulay rings
6. Koszul complex

1 Hauptidealsatz

Assumptions: In the following $\Bbbk$ is an algebraically closed field and $\mathbb{A}^n_{\Bbbk}$ stands for the n-dimensional affine space. Every ring in this course will be commutative with a unity and all homomorphisms will respect this unity.

An affine closed set X is the common locus of an ideal in $I \lhd \Bbbk[x_1, \dots, x_n]$, i.e. $X = V(I)$. Similarly, we can define the corresponding ideal $I(X)$ to a closed set X by the property "f vanishes on every point of X". Hilbert Nullstellensatz states that $I(V(I)) = \sqrt{I}$ for every ideal $I \lhd \Bbbk[x_1, \dots, x_n]$. Therefore, $I \leftrightarrow V(I)$ induces an (inclusion-reversing) bijection between radical ideals (i.e. $I = \sqrt{I}$) and closed sets of $\mathbb{A}^n_{\Bbbk}$. In particular, maximal ideals correspond to points of $\mathbb{A}^n_{\Bbbk}$ and prime ideal correspond to irreducible closed subsets of $\mathbb{A}^n_{\Bbbk}$ (the ones that cannot be written as the union of two proper closed subsets), sometimes also called (affine) varieties.

Understanding all closed subsets of $\mathbb{A}^n_{\Bbbk}$ is, in principle, equivalent to understanding irreducible closed subsets of $\mathbb{A}^n_{\Bbbk}$ because every closed subset is the union of finitely many irreducible closed subsets. Algebraically, it means that every ideal is the intersection of finitely many prime ideals. This is also a consequence of the existence of a primary decomposition in general Noetherian rings.

Definition 1.1. The *dimension* of a variety is the maximal length of a chain $X \supsetneq Z_n \supsetneq Z_{n-1} \supsetneq \cdots \supsetneq Z_1$ of subvarieties contained in X.

Definition 1.2. Let A be a ring and $P \subseteq A$ be a prime ideal. Then

$$\mathrm{ht}(P) := \sup\{r \in \mathbb{N} \mid \exists P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r \subsetneq P \text{ chain of prime ideals in } P\}$$

Analogously, the *Krull dimension* of the ring A is

$$\dim(A) := \sup\{\mathrm{ht}(P) \mid P \subseteq A \text{ prime}\}$$

Remark 1.3. If $X = V(I)$ is an affine variety where $I = \sqrt{I}$ then the coordinate ring of X is $\mathcal{A}_X := \Bbbk[x_1, \dots, x_n]/I$. By this terminology, $\dim(X)$ is basically defined as Krull $\dim(\mathcal{A}_X)$.

Theorem 1.4. (Krull's Hauptidealsatz) *Let A be a Noetherian ring and $x \in A$. If P is a minimal prime ideal such that $x \in P$ then* $\mathrm{ht}(P) \leq 1$.

Theorem 1.5. ("Zusatz") *Moreover, if x is not a zero-divisor then* $\mathrm{ht}(P) = 1$.

Theorem 1.6. (Generalization of Krull's Hauptidealsatz) *Let A be a Noetherian ring and $x_1, \dots, x_r \in A$. If P is a prime ideal which is minimal among the ideals with $x_i \in P$ for all i then* $\mathrm{ht}(P) \leq r$.

Corollary 1.7. (Of Theorem 1.6) *The prime ideals in a Noetherian ring satisfy the descending chain condition. (Or in other words, every prime ideal has finite height.)*

Reminder: If A is a ring, $S \subseteq A$ is a multiplicatively closed subset (i.e. $1 \in S$, $x, y \in S$ then $xy \in S$) then there exists a localization of A by S. It is a ring $A[S^{-1}]$ together with a ring homomorphism $\lambda : A \to A[S^{-1}]$ such that for all ring homomorphisms $\varphi : A \to R$ such that $\varphi(s)$ is a unit in R for all $s \in S$ there exists a unique factorization: $\varphi = \hat{\varphi} \circ \lambda$.
Important special cases are when $S = \{1, x, x^2, x^3, \dots\}$ or when $S = A \backslash P$ where P is a prime ideal. In this latter case, we write $A_P = A[S^{-1}]$ where A_P is a local ring with a unique maximal ideal PA_P. (There is a slight abuse of notation: PA_P refers to $\lambda(P)A_P$.) More generally, $I \mapsto \lambda(I)A_P$ induces a bijection between ideals contained in P and the ideals of A_P.

Lemma 1.8. *If A is a Noetherian ring that has exactly one prime ideal P then A is Artinian.*

Proof. Generally, in any Noetherian ring, the intersection of the prime ideals is the set of nilpotent elements. Therefore, if $x \in P$ then x must be nilpotent. Since A is Noetherian, P is finitely generated so for a generating system $y_1, \dots, y_k$ there is a big enough exponent N such that $y_i^N = 0$ for all i hence all products of $k \cdot N$ elements in P are zero. Now, we have a finite filtration of A with the ideals $A \supseteq P \supseteq P^2 \supseteq P^3 \supseteq \cdots \supseteq P^N = 0$ where every quotient is a finite dimensional (since finitely generated) vector space over the field A/P. So we are done because the finite extension of Artinian submodules (such as the above finite dimensional vector spaces) is also Artinian. ☐

Proof of Theorem 1.4. : We show that if $Q \subsetneq P$ then $\mathrm{ht}(Q) = 0$. Replace A by A_P so we may assume that A is local with maximal ideal P. Let $Q^{(n)} := \big(Q^n : (A \backslash Q)\big) = \{q \in A \mid \exists s \notin Q \text{ such that } sq \in Q^n\}$. This looks a not really well motivated definition but in fact it is the preimage of $(QA_Q)^n$ by the localizing map $\lambda : A \to A_Q$. Its name is the symbolic n-th power of Q.

Now, we can apply the previous Lemma 1.8 on $A/(x)$ since P is minimal over (x) and a maximal ideal at the same time. The lemma tells that $A/(x)$ is Artinian. Therefore, the chain $(x, Q) \supseteq (x, Q^{(2)}) \supseteq \cdots \supseteq (x, Q^{(m)}) \supseteq \dots$ stabilizes at some level n. So if $f \in Q^{(n)} \subseteq (x, Q^{(n)}) = (x, Q^{(n+1)})$ then $f = ax + q$ for some $a \in A$ and $q \in Q^{(n+1)}$. Then $ax = f - q \in Q^{(n)}$ but $x \notin Q$ because $Q \subsetneq P$ and P is minimal over x. By definition, there exists $s \notin Q$ such that $sax \in Q^n$ but then $a \in Q^{(n)}$ since $sx \notin Q$ by the prime property of Q.

In summary, we got that $Q^{(n)} \subseteq (x)Q^{(n)} + Q^{(n+1)}$ and the reverse containment is automatic. Therefore, $Q^{(n)}/Q^{(n+1)} = P\big(Q^{(n)}/Q^{(n+1)}\big)$ because $x \in P$ and we just proved that every element of $Q^{(n)}/Q^{(n+1)}$ can be expressed as an element of $(x)Q^{(n)}/Q^{(n+1)}$. So – by Nakayama's lemma – we get $Q^{(n)}/Q^{(n+1)} = 0$. In other words, $(QA_Q)^n = (QA_Q)^{n+1}$ as ideals in A_Q. So now we can apply Nakayama in A_Q where the radical is QA_Q what implies that $(QA_Q)^n = 0$. Now, we are left with a local ring with a nilpotent maximal ideal. It means that QA_Q is the only prime ideal in A_Q since the intersection of the prime ideals is exactly the set of nilpotent elements. Therefore, $\mathrm{ht}(Q) = 0$ and that was the statement. □

Lemma 1.9. *In a Noetherian ring all minimal prime ideals consist of zero-divisors.*

Proof of Theorem 1.5. : The above lemma clearly implies the statement. □

Proof of the Lemma 1.9. : Note that there exists only finitely many minimal prime ideals in A. Indeed, we can look at an irredundant primary decomposition of $\sqrt{(0)}$ which consists of finitely many minimal prime ideals, let these be $P_1, \ldots, P_r$. If P would be a minimal prime ideal not listed here then by $\prod P_i \subseteq \cap P_i = \sqrt{(0)} \subseteq P$ we get that there exists an $i \leq r$ such that $P_i \subseteq P$. Hence $P_i = P$ by minimality. Now, we proceed by induction on r.

If $r = 1$ then we are done since the $\sqrt{(0)}$ is a prime ideal that is contained in any other prime ideal. If $r > 1$ then pick an $a \in P_1$. We show that a is a zero-divisor and then the statement follows. First, there exists $b \in P_2 \cap \cdots \cap P_r$ such that $b \notin P_1$ because the decomposition is irredundant. Clearly, $ab \in P_1 \cap \cdots \cap P_r$ so $(ab)^n = 0$ for big enough n since $P_1 \cap \cdots \cap P_r = \sqrt{(0)}$. But $b^n \neq 0$ since $b \notin P_1$ so there exists an i such that $a^i b^n \neq 0$ but $a^{i+1} b^n = 0$ and then a is a zero-divisor. □

Proof of the generalized Hauptidealsatz. : We prove by induction on r. The case $r = 1$ is exactly the Hauptidealsatz. For $r > 1$ pick any prime ideal $P_1 \subsetneq P$ such that there does not exist P': $P_1 \subsetneq P' \subsetneq P$ (i.e. it is maximal in P which exists by the Noetherian property). We show that there exists $y_1, \ldots, y_{r-1} \in A$ such that P_1 is minimal over $(y_1, \ldots, y_{r-1})$ so then we can use induction.

We may assume that P is maximal by replacing A by A_P. Since $P_1 \subsetneq P$ and P is minimal above $(x_1, \ldots, x_r)$ there exists an i such that $x_i \notin P_1$. Let's say that is x_r. Then P is a minimal prime ideal such that $(x_r, P_1) \subseteq P$. then $A/(x_r, P_1)$ has dimension zero because its only one maximal ideal is a minimal prime (Same argument as before). Therefore, the image of P in $A/(x_r, P_1)$ is a nilpotent ideal because it is the intersection of every prime ideal, so for all $i \leq r-1$ we have $x_i^m = a_i x_r + y_i$ for some $y_i \in P_1$, $a_i \in A$ and big enough m. It means that the image of P in $A/(y_1, \ldots, y_{r-1}, x_r)$ is nilpotent hence the image of P in $A/(y_1, \ldots, y_{r-1})$ is minimal over (x_r).

Now, by the Hauptidealsatz $\mathrm{ht}(P) \leq 1$ in $A/(y_1, \ldots, y_{r-1})$ so $\mathrm{ht}(P_1) = 0$ in $A/(y_1, \ldots, y_{r-1})$ and that was our statement.

Second Lecture, 20th of January □

Proposition 1.10. (Converse of Hauptidealsatz) *If A is Noetherian and $P \lhd A$ is a prime ideal and* $\mathrm{ht}(P) \leq r$ *then there exists $x_1, \ldots, x_r \in A$ such that P is minimal above $(x_1, \ldots, x_r)$.*

Lemma 1.11. (Prime avoidance) *Let A be any (commutative, unital) ring, $I_1, \ldots, I_n, J \lhd A$ ideals such that all I_j are prime ideal except perhaps I_{n-1} and I_n. If $J \not\subseteq I_j$ for all j then there exists $x \in J$ such that $x \notin I_j$ for all $j \leq n$. (Equivalently, $J \subseteq \cup I_j$ implies $J \subseteq I_i$ for some $i \leq n$.)*

Proof. Induction on n: the case $n = 1$ is clear. For $n > 1$, assume that $J \subseteq \cup I_j$. By induction, for $i = 1, \ldots, n$ there exists an $x_i \in J$ such that $x_i \notin I_j$ for all $j \neq i$. For $n = 2$: By the assumption, $x_i \in I_i$ must hold so $x_1 + x_2 \notin I_1$ and also $x_1 + x_2 \notin I_2$ and we are done. If $n > 2$ then I_1 is necessarily a prime ideal so $x_1 + \prod x_i \notin \cup_{j=1}^n I_j$ and that is a contradiction. □

Proof of Proposition 1.10. : We proceed by induction on r: the case $r = 0$ is an empty statement. Assume that $\mathrm{ht}(P) = r$. To prove the statement, we construct the sequence $x_1, \ldots, x_r$ recursively with the stronger property requiring for all $1 \leq i \leq r$ and for all minimal primes above $(x_1, \ldots, x_i)$ to have height at least i (hence exactly i by the Hauptidealsatz 1.4).

First, let $x_1 \in P$ be an element such that it is not contained in the minimal primes of A which exists by Lemma 1.11 since P is not minimal by $\mathrm{ht}(P) = r > 0$. Then all minimal primes above (x_1) have height 1 by the Zusatz 1.5 and by noting that the union of minimal primes is the set of zero-divisors. For $1 < i \leq r$, if we have already constructed $x_1, \ldots, x_{i-1}$ then choose an $x_i \in P$ such that it is not contained in the minimal primes above $(x_1, \ldots, x_{i-1})$. By Lemma 1.11 such an x_i exists else the Lemma claims that one of the minimal primes above $(x_1, \ldots, x_{i-1})$ would contain P giving the contradiction $\mathrm{ht}(P) \leq i-1 < r$ using the Hauptidealsatz 1.4. The resulting ideal $(x_1, \ldots, x_i)$ indeed has the required property because any minimal prime above $(x_1, \ldots, x_i)$ is not minimal above $(x_1, \ldots, x_{i-1})$ by the choice of x_i. Hence, it contains a minimal prime above $(x_1, \ldots, x_{i-1})$ which has height at least $i-1$. Therefore, any minimal prime above $(x_1, \ldots, x_i)$ has height at least (hence equally) i proving the claim. □

Proposition 1.12. *Let $\varphi : A \to B$ a homomorphism of Noetherian rings, $Q \subseteq B$ be a prime ideal, and denote $P = \varphi^{-1}(Q)$. Then $\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim B_Q/PB_Q$.*

Proof. We may replace A by A_P, P by PA_P, B by B_Q and Q by QB_Q since it does not change the relation of the mentioned numbers. So we may assume that A and B are local and then we have to prove that $\dim B \leq \dim A + \dim B/PB$. Set $r := \mathrm{ht}(P)$ and $s := \mathrm{ht}(Q \bmod PB)$. By Proposition 1.10 we get $x_1, \ldots, x_r \in A$ such that P is minimal above them and similarly, let $y_1, \ldots, y_s \in B$ such that Q modulo PB is minimal above $y_1 \ldots, y_s$ modulo PB. Then by a similar argument as before (i.e. a maximal ideal being minimal prime is nilpotent, see the proof of Theorem 1.4) we get that $Q^N \subseteq PB + (y_1, \ldots, y_s)$ and similarly $P^M \subseteq (x_1, \ldots, x_r)$ therefore $Q^{NM} \subseteq (\varphi(x_1), \ldots \varphi(x_r), y_1, \ldots, y_s)$. This means that Q is a minimal ideal above $(\varphi(x_1), \ldots \varphi(x_r), y_1, \ldots, y_s)$.

So we got that $\dim(B) = \dim(Q) \leq r + s = \mathrm{ht}(P) + \dim(B/PB)$ where the inequality is a consequence of the Generalized Hauptidealsatz (Theorem 1.6). □

Corollary 1.13. *If A is a Noetherian ring then $\dim A[x] = \dim A + 1$. (In particular, $\dim \Bbbk[x_1, \ldots, x_n] = n$.)*

Proof. The inequality $\geq$ is easy: a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ in A can be considered as a chain of primes in $A[x]$ using the natural embedding $\varphi : A \to A[x]$ since the factors of the images $A[x]/A[x]\varphi(P_i) \cong (A/P_i)[x]$ are still domains. However, the image of a maximal ideal P_n will not be maximal in $A[x]$ because the factor is not a field (x is not invertible). Therefore, $\dim(A[x]) \geq \dim A + 1$.

Conversely, it is enough to show that for a maximal ideal $Q \lhd A[x]$ we have $\mathrm{ht}(Q) \leq \mathrm{ht}\big(A \cap Q\big) + 1$. For this, set $P := A \cap Q$ which is a prime ideal in A hence has height at most n. By the previous proposition we know that

$$\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim\big(A[x]_Q/P \cdot A[x]_Q\big)$$

So we need to prove that the appearing dimension on the right is at most 1 (in fact it is always exactly one). This can be computed as follows

$$A[x]_Q/P \cdot A[x]_Q \cong \big(A[x]/P \cdot A[x]\big)_Q \cong \big((A/P)[x]\big)_Q \cong$$

where we can first localize at the smaller multiplicative subset $A \backslash P \subseteq A[x] \backslash Q$ giving

$$\cong \big((A/P)_P[x]\big)_Q \cong \big(\kappa(P)[x]\big)_Q$$

using the notation $\kappa(P) := (A/P)_{(0)} = (A/P)_P \cong A_P/PA_P$ for the residue field at P. Since $\kappa(P)[x]$ is a one-variable polynomial ring over a field, it has dimension 1 and localizing at Q can only lower it. This proves the statement. □

Remark 1.14. Without the Noetherian property the statement is not true: For a ring A, the polynomial ring $A[x]$ can have arbitrary dimension between $\dim A + 1$ and $2 \dim A + 1$. The point where we rely on Noetherian property is at Proposition 1.12 and its proof.

By an analogous argument, we also get

Corollary 1.15. *If A is a Noetherian ring and* $\dim A[[x]] = \dim A + 1$. *(In particular,* $\dim \Bbbk[[x_1, \dots, x_n]] = n$.*)*

Proof. Clearly, an increasing chain of prime ideals in A gives an increasing chain of prime ideals in $A[[x]]$ too by $A[[x]]/PA[[x]] \cong (A/P)[[x]]$. Moreover, $(A/P)[[x]]$ is never a field (x is not invertible) so $\dim A[[x]] \geq \dim A + 1$ as in the previous proof. Conversely, for a maximal ideal $Q \lhd A$ and $P = A \cap Q$ we have

$$\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim \big(A[[x]]_Q / P \cdot A[[x]]_Q\big)$$

by Proposition 1.12. Here, we can still compute the ring on the right:

$$A[[x]]_Q / P \cdot A[[x]]_Q \cong \big((A/P)[[x]]\big)_Q \cong \big((A/P)_P[[x]]\big)_Q \cong \big(\kappa(P)[[x]]\big)_Q$$

So we only have to observe that $\dim \big(\kappa(P)[[x]]\big) = 1$ which is true since it is a primary example of a discrete valuation ring. In details, every element can be written as $x^n \cdot (c + x \cdot p)$ where $c \in \kappa(P)$ and $p \in \kappa(P)[[x]]$, but $c + x \cdot p$ is invertible with inverse $\frac{1}{c} \sum_{k=0}^{\infty} \Big(- \frac{xp}{c} \Big)^k$, so the only nontrivial ideals are (x^n) for $n \geq 1$. ☐

Remark 1.16. If A is an integral domain which is finitely generated algebra over a field $\Bbbk$ then $\mathrm{tr.deg}_{\Bbbk}(A)$ denotes the maximal number of elements in A that are algebraically independent over $\Bbbk$.

Proposition 1.17. *If A is an integral domain then* $\mathrm{tr.deg}_{\Bbbk}(A) = \dim A$. *(Without proof, we would need the going up theorem, not only the Hauptidealsatz.)*

Remark 1.18. Geometric interpretation of the Hauptidealsatz: Let $X \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk = \bar{\Bbbk}$ and $X = V(I)$ for some radical ideal in $\Bbbk[x_1, \dots, x_n]$. Then $f_1, \dots, f_r \in \mathcal{A}_X = \Bbbk[x_1, \dots, x_n]/I$ define a closed subset $Z \subseteq X$. The terms Z_i in the irreducible decomposition of $Z = \cup Z_i$ correspond to minimal prime ideals above $f_1, \dots, f_r$. In this context, Generalized Hauptidealsatz means that $\dim Z_i \geq \dim - r$ for all i (the existence of such i would be much easier).

Corollary 1.19. (Dimension Theorem) *Let $X, Y \subseteq \mathbb{A}^n$ be subvarieties such that $X \cap Y \neq \emptyset$. Write $X \cap Y = \cup Z_i$ where Z_i's are the irreducible components. Then $\dim Z_i \geq \dim X + \dim Y - n$ for all i.*

Remark 1.20. By the notation $\mathrm{codim} X := n - \dim X$ the claim says that $\mathrm{codim} Z_i \leq \mathrm{codim} X + \mathrm{codim} Y$.

Proof. (Sketch!) The intersection $X \cap Y \cong (X \times Y) \cap \Delta^n$ where Δ^n stands for the diagonal in $\mathbb{A}^n \times \mathbb{A}^n$. (Isomorphic in the sense of varieties.) Fortunately, $\dim X \times Y = \dim X + \dim Y$ because of Proposition 1.17. So, by Proposition 1.12 and by the description of $\Delta^n = V(x_i - y_i \mid i \leq n)$ the statement follows. ☐

2 Regular rings

Definition 2.1. A Noetherian local ring A with a maximal ideal P is a *regular* local ring if $\dim_{A/P} P/P^2 = \dim A$ where A/P is used as a field in $\dim_{A/P}$.

Remark 2.2. The algebraic meaning of regularity is the following: if $x_1, \dots, x_r \in P$ are such that their images modulo P^2 generate P/P^2 then they generated P as an ideal as well (by Nakayama: the elements of $P \cdot P$ are superfluous in a generator system of the module P). If the images form a basis in P/P^2 then we call $x_1, \dots, x_r$ a *regular system of parameters*. On the other hand, if $x_1, \dots, x_r$ generates P then $r \geq \dim A$. (By the generalization of the Hauptidealsatz since P is the maximal ideal so $\mathrm{ht}(P) = \dim A$.) In short, a Noetherian local ring is regular if and only if P is generated by the smallest possible number of elements.

Remark 2.3. The geometric meaning of regularity is the following: Let X be an affine variety and A be the local ring of it at P. Therefore, $P/P^2 \cong T_P^* X$ the cotangent space at P. So A is regular if and only if $\dim T_P^* X = \dim X$, i.e. if P is a smooth point.

Proposition 2.4. *If A is a regular local ring and $x_1, \dots, x_r$ a regular system of parameters in A then $A/(x_1, \dots, x_i)$ is a regular local ring of dimension $r - i$ for all $1 \leq i \leq r$.*

In fact, we prove more:

Proposition 2.5. *If A is a Noetherian ring, P is a minimal prime above $x_1, \dots, x_r$ and $\mathrm{ht}(P) = r$ then $\mathrm{ht}(P/(x_1, \dots, x_i)) = r - i$ in $A/(x_1, \dots, x_i)$ for all $1 \leq i \leq r$.*

The previous Proposition follows from it as locality is trivially inherited by the factor, the dimension of P/P^2 decreases by one at each step (i.e. when we factor out one more x_i) so we only need that height of P decreases by one at a step and not more. And this is the actual statement.

Proof. By the Hauptidealsatz 1.4 we have $\mathrm{ht}(P/(x_1, \dots, x_i)) \leq r - i$ since $P/(x_1, \dots, x_i)$ is minimal above the images of $x_{i+1}, \dots, x_r$ in $A/(x_1, \dots, x_i)$. Assume that $\mathrm{ht}(P/(x_1, \dots, x_r)) = s$. By the converse of Hauptidealsatz 1.10, we get elements $\bar{y_1}, \dots, \bar{y_s}$ such that $P/(x_1, \dots, x_i)$ is minimal above $\bar{y_1}, \dots, \bar{y_s}$. Now, lift them into A as $y_1, \dots, y_s \in P$ so it is minimal above $x_1, \dots, x_i, y_1, \dots, y_s$, i.e. $s \geq r - i$. □

Theorem 2.6. *A regular local ring is an integral domain.*

Proof. We prove by induction on $\dim A$. (Note that regularity implicitly contains the finiteness of $\dim A$.) Let us denote $\dim(A) = d$. If $d = 0$ then $P/P^2 = 0$ but P is nilpotent so $A = A/P$ which is a field. Now, assume the proposition for $d - 1$. Let $P_1, \dots, P_m$ be the minimal prime ideals of A. We can apply prime avoidance to $P_1, \dots, P_m, P^2$ and P (here, P^2 is not necessarily prime but it is not needed in the prime avoidance). We know that $P \not\subseteq P_i$ and $P \not\subseteq P^2$ so there exists an $x \in P \backslash P^2$ such that $x \notin P_i$ for all i. (Geometrically, it vaguely corresponds to taking a function that is not vanishing and has nonzero derivative where it is not necessary.) Then we can take a regular system of parameters containing x.

Now, we can apply the previous Proposition 2.4 on $A/(x)$ so it is regular and local with $\dim A/(x) = d - 1$. By the induction, we know that $A/(x)$ is an integral domain so (x) is a prime ideal. It is of height 1 by the Hauptidealsatz 1.4 and the Zusatz 1.5. Then there exists i such that $P_i \subseteq (x)$ by minimality. On the level of elements, it means that for all $y \in P_i$ we have $y = ax$ for some $a \in A$. But $x \notin P_i$ so $a \in P_i$. Hence, we conclude that $P_i = (x)P_i$, so even $P_i = PP_i$ is true. Therefore, by Nakayama, $P_i = 0$ what means that zero is a prime ideal, as we stated. □

2.1 Regular sequences

Definition 2.7. Let A be a ring, $x_1, \dots, x_n \in A$ is a *regular sequence* if

1. x_i is not a zero-divisor modulo $(x_1, \dots, x_{i-1})$ for all $1 \leq i \leq n$.

2. $(x_1, \dots, x_n) \neq A$.

Remark 2.8. We will later prove that the property does not depend on the order of the elements in a Noetherian ring. It is not that surprising in the light of Proposition 2.4.

Remark 2.9. Geometrically, it corresponds to the existence of a flag of local subvarieties in a local finitely generated $\mathbb{k}$-algebra.

Definition 2.10. Let A be a ring and $I = (x_1, \dots, x_n)$ a finitely generated ideal such that $\cap_{n=1}^{\infty} I^n = 0$. Look at the filtration $I \supseteq I^2 \supseteq I^3 \supseteq \dots$ the associated graded ring is $\mathrm{gr}_I(A) = \oplus_{i=0}^{\infty} I^i / I^{i+1}$. There exists an induced multiplication on $\mathrm{gr}_I(A)$.

There also exists a natural surjective morphism of graded rings $(A/I)[t_1, \ldots, t_n] \to \mathrm{gr}_I(A)$ where we took the usual grading on $(A/I)[t_1, \ldots, t_n] = \oplus_{n=0}^{\infty}\{\text{homogeneous polynomials with coefficient in } A/I \text{of degree } n\}$ sending t_i to x_i modulo I.

Theorem 2.11. *Let A be a Noetherian local ring with maximal ideal P and $x_1, \ldots, x_n$ a minimal (hence regular) system of generators for P. Then the following conditions are equivalent:*

1. *A is a regular local ring*
2. *$x_1, \ldots, x_n$ is a regular sequence*
3. *The above map $\Bbbk[t_1, \ldots, t_n] \to \mathrm{gr}_P(A)$ is an isomorphism, where $\Bbbk = A/P$.*

Third Lecture, 27th of January

Proof. 1) ⇒ 2) was proved last time in Proposition 2.4 and Theorem 2.6. 3) ⇒ 2): By the assumption for all i we have isomorphisms $\Bbbk[t_i, \ldots, t_n] \overset{\cong}{\to} \mathrm{gr}_{P/(x_1,\ldots,x_{i-1})}(A/(x_1, \ldots, x_{i-1}))$ by factoring out the given isomorphism on both sides. So it is enough to prove the following lemma:

Lemma 2.12. *Let A be a ring, $I \subseteq A$ an ideal such that $\cap_j I^j = 0$. Assume that $\mathrm{gr}_I(A)$ is an integral domain, then A is also an integral domain.*

To check the assumptions of the lemma observe that $\Bbbk[t_i, \ldots, t_n]$ is an integral domain. Moreover, in Corollary 3.18 we will prove that $\cap_m(x_1, \ldots, x_{i-1})^m = 0$ using that $(x_1, \ldots, x_{i-1})$ is the maximal ideal of the local ring $A/(x_i, \ldots, x_n)$. Therefore, the above lemma can be applied proving that $x_1, \ldots, x_n$ is a regular sequence by definition, this proves the discussed direction of the theorem.

Remark 2.13. Note that the originally proposed argument for $\cap_m(x_1, \ldots, x_{i-1})^m = 0$ using Nakayama's lemma does not work. The reason of it is that $P \cdot \cap_m P^m$ is not necessarily $\cap_m P^m$ but may be smaller, this is exactly the content of Corollary 3.18 where this distinction is bridged by the non-trivial Artin-Rees lemma, 3.17.

Proof of Lemma 2.12. : Let $0 \neq a, b \in A$. Then by $\cap_j I^j = 0$ there exists r and s such that $a \in I^r \backslash I^{r+1}$ and $b \in I^s \backslash I^{s+1}$. Set $\bar{a} = a \mod I^{r+1}$ and $\bar{b} = b \mod I^{s+1}$ as "they live in that degree". Similarly, let $\overline{ab} = ab \mod I^{r+s+1}$. Then by the definition of product in $\mathrm{gr}_I(A)$ we get $\overline{ab} = \bar{a} \cdot \bar{b} \in \mathrm{gr}_I(A)$ where $\bar{a} \cdot \bar{b} \neq 0$ because $\mathrm{gr}_I(A)$ is an integral domain so it implies $ab \neq 0$. □

Now, we prove 2) ⇒ 1): For this we need the following lemma:

Lemma 2.14. *If A Noetherian local ring and $x_1, \ldots, x_r$ is a regular sequence in A then* $\dim A/(x_1, \ldots, x_r) = \dim A - r$.

Remark 2.15. Note that here $x_1, \ldots, x_r$ is a regular *sequence* (i.e. a sequence of non-zerodivisors in the appropriate factors) while in the similarly shaped Proposition 2.4 it was merely a regular *system* (i.e. a representing system for an A/P-basis of P/P^2) but there we assumed regularity of the ring while here we are trying to prove that.

Now, to get direction 2) ⇒ 1) of the theorem, apply the lemma with $n = r$ so we get that $0 = \dim A/P = \dim A - n$ meaning that A is regular.

Proof of Lemma 2.14. : To prove $\dim A/(x_1, \ldots, x_r) \geq \dim A - r$ we use the same method as in the proof of 2.5 (which statement is not directly applicable now, compare the assumptions!). First, note that by the Converse of Hauptidealsatz 1.10 there exists $y_1, \ldots, y_s \in A/(x_1, \ldots, x_r)$ such that $P/(x_1, \ldots, x_r)$ is minimal containing $y_1, \ldots, y_s$ where $s = \mathrm{ht}\big(P/(x_1, \ldots, x_r)\big) = \dim A/(x_1, \ldots, x_r)$. Therefore, $P \lhd A$ is minimal among prime ideals containing $x_1, \ldots, x_r, y_1, \ldots, y_s$ hence $\dim A = \mathrm{ht}P \leq r + s$ by the generalized Hauptidealsatz 1.6. For the converse, we use that x_1 is not a zerodivisor in A so for all minimal prime ideals $P' \supseteq (x_1)$ we have

$\mathrm{ht}(P') = 1$ by the Zusatz, Theorem 1.5. Therefore $\dim A/(x_1) \le \dim A - 1$. Now, we can use induction on r since the definition of a regular sequence is also inductive and we get that $\dim A/(x_1, \dots, x_r) \le \dim A - r$. □

Now, we prove the hard part of Theorem 2.11: 2) ⇒ 3). More generally, we prove the following theorem due to Rees:

Theorem 2.16. (Rees) *Let A be a ring and $x_1, \dots, x_n$ be a regular sequence. The (surjective) graded map $A[t_1, \dots, t_n] \to \mathrm{gr}_I(A)$ where $I = (x_1, \dots, x_n)$ given by $t_i \mapsto x_i \bmod I^2$ induces an isomorphism*

$$(A/I)[t_1, \dots, t_n] \overset{\cong}{\to} \mathrm{gr}_I(A)$$

In other words, $A[t_1, \dots, t_n] \ni F \mapsto 0 \in \mathrm{gr}_I(A)$ is possible only if it is trivially true, namely if $F \in I[t_1, \dots, t_n]$.

Proof. Note that if F is homogeneous element of $A[t_1, \dots, t_n]$ of degree d then $F(x_1, \dots, x_n) \in I^d$ so the map is indeed graded. The proof will go by a double induction on n and d where d still stands for the degree F which is assumed to be homogeneous. In more details, if we denote by $\Psi(n, d)$ the statement of the theorem for a fixed $n, d \in \mathbb{N}$ then to prove $\Psi(n, d)$ we will use $\Psi(n-1, c)$ for arbitrary c (in fact $c \le d-1$ is enough) together with $\Psi(n, d-1)$.

The case $n = 0$ is the empty statement and the case $n = 1$ is easy: if $F(x_1) \in (x_1^{d+1})$ then F has coefficients divisible by x_1 since x_1 is regular i.e. a non-zerodivisor. Now, assume that the theorem is true for $n-1$ (and for all $d \in \mathbb{N}$).

Lemma 2.17. *x_n is not a zerodivisor on $A/(x_1, \dots, x_{n-1})^j$ for all $j > 0$.*

Proof. We prove by induction on j (which induction is an inner induction relative to the induction of the theorem on n). The case $j = 1$ is just our assumption: $x_1, \dots, x_n$ is a regular sequence. If $j > 1$ then assume that $x_n \cdot y \in (x_1, \dots, x_{n-1})^j$. Since $(x_1, \dots, x_{n-1})^{j-1} \supseteq (x_1, \dots, x_{n-1})^j \ni x_n \cdot y$ we can apply the induction on j: x_n is not a zero-divisor modulo $(x_1, \dots, x_{n-1})^{j-1}$ hence y must be in $(x_1, \dots, x_{n-1})^{j-1}$. This means that (by definition) there exists $G \in A[t_1, \dots, t_{n-1}]$ homogeneous of degree $j-1$ such that $y = G(x_1, \dots, x_{n-1})$, in particular $x_n G(x_1, \dots, x_{n-1}) \in (x_1, \dots, x_{n-1})^j$. The latter fact can be expressed as

$$A[t_1, \dots, t_{n-1}] \ni x_n G(t_1, \dots, t_{n-1}) \mapsto 0 \in \mathrm{gr}_{(x_1, \dots, x_{n-1})}(A)$$

where $x_n \in A$ but the t_i's are purposely variables. Now, we can apply the induction hypothesis of the theorem on n (in fact $\Psi(n-1, j-1)$). It claims that the polynomial $x_n G(t_1, \dots, t_{n-1})$ has coefficients in $(x_1, \dots, x_{n-1})$. However, x_n is not a zerodivisor modulo $(x_1, \dots, x_{n-1})$ so G has coefficients in $(x_1, \dots, x_{n-1})$ too. As G is homogeneous of degree $j-1$ we got that $y = G(x_1, \dots, x_{n-1}) \in (x_1, \dots, x_{n-1}) \cdot (x_1, \dots, x_{n-1})^{j-1} = (x_1, \dots, x_{n-1})^j$ and that was the statement. □

Continuation of the proof of Theorem 2.16: Let $F \in A[t_1, \dots, t_n]$ homogeneous of degree d for some $d > 0$, and assume that $F(x_1, \dots, x_n) \in I^{d+1}$. We have to show that $F \in I[t_1, \dots, t_n]$. First, we reduce to the case of $F(x_1, \dots, x_n) = 0$ by finding and subtracting an appropriate element of $I[t_1, \dots, t_n]$ having the same evaluation as F. The assumption $F(x_1, \dots, x_n) \in I^{d+1}$ means that there exists $\tilde{F} \in A[t_1, \dots, t_n]$ homogeneous of degree $d+1$ such that $F(x_1, \dots, x_n) = \tilde{F}(x_1, \dots, x_n)$. Now, write $\tilde{F} = \sum_i t_i \tilde{F}_i$ where $\tilde{F}_i$ is homogeneous of degree d for all i. Then $F - \sum_i x_i \tilde{F}_i \in A[t_1, \dots, t_n]$ is homogeneous of degree d (note that here x_i's are parts of the coefficients, that does the trick) and it is zero on $x_1, \dots, x_n$. Since $x_i \tilde{F}_i \in I[t_1, \dots, t_n]$ by the definition of $I = (x_1, \dots, x_n)$, it is enough to prove $F - \sum_i x_i \tilde{F}_i \in I[t_1, \dots, t_n]$ to get $F \in I[t_1, \dots, t_n]$ i.e. the reduction to the case $F(x_1, \dots, x_n) = 0$ is indeed possible by replacing F by $F - \sum_i x_i \tilde{F}_i$.

Now, decompose $F = G + t_n H$ into a t_n-free component $G \in A[t_1, \dots, t_{n-1}]$ and the remaining $t_n H$ where $\deg H = d-1$ since F is homogeneous. We will prove that separately, G and H are in $I[t_1, \dots, t_n]$ hence the claim. Turning to the image (i.e. evaluating the equality $F = G + t_n H$ on $x_1, \dots, x_n$) gives

$$x_n H(x_1, \dots, x_n) = -G(x_1, \dots, x_{n-1}) \in (x_1, \dots, x_{n-1})^d$$

since G is homogeneous of degree d and $F(x_1,\dots,x_n)=0$ by the previous paragraph. The above Lemma 2.17 applied on $j=d$ claims that $H(x_1,\dots,x_n)\in(x_1,\dots,x_{n-1})^d$. This means that we are in a weird situation because $H(x_1,\dots,x_n)$ by nature is only in I^{d-1} i.e. not that deep by $\deg H=d-1$, but in a bigger ideal. We use both of its deviations: First, by $H(x_1,\dots,x_n)\in I^d$ and $\deg H=d-1$ we get $H\in I[t_1,\dots,t_n]$ using the induction hypothesis on d (precisely, this is $\Psi(n,d-1)$). So the problem of H is solved.

Secondly, to prove $G\in I[t_1,\dots,t_n]$ it seems reasonable to find a way to apply the induction hypothesis (precisely $\Psi(n-1,d)$) on G and proving the stronger $G\in(x_1,\dots,x_{n-1})\cdot A[t_1,\dots,t_{n-1}]$ but we cannot easily check the assumptions on G. Instead, we take a substitute $\tilde{H}\in A[t_1,\dots,t_{n-1}]$ of degree d such that $H(x_1,\dots,x_n)=\tilde{H}(x_1,\dots,x_{n-1})$ which exists since $H(x_1,\dots,x_n)\in(x_1,\dots,x_{n-1})^d$ (as in the first paragraph). Then we can interchange H with $\tilde{H}$ in the equation

$$(G+x_n\tilde{H})(x_1,\dots,x_{n-1})=F(x_1,\dots,x_n)=0$$

Therefore, by $G+x_n\tilde{H}\in A[t_1,\dots,t_{n-1}]$ and $\deg(G+x_n\tilde{H})=d$ we can apply the induction hypothesis on n (precisely, this is $\Psi(n-1,d)$) so we get that $G+x_n\tilde{H}\in I[t_1,\dots,t_{n-1}]$. But $x_n\tilde{H}$ already had coefficients in I by $x_n\in I$ hence G is also in $I[t_1,\dots,t_n]$. Therefore, after the two observations we get $F=G+t_nH\in I[t_1,\dots,t_n]$. □

End of the proof of Theorem 2.11: The implication 2) ⇒ 3) follows from 2.16 by setting $I=P$. □

3 Completions

Motivation: When studying algebraic varieties, regular functions are fractions of polynomials and one comfortable way to study them is to introduce generalized regular functions in the form of power series. So we should study rings of power series with an algebraic treatment.

Definition 3.1. Let A be a ring and $I\subseteq A$ is an ideal. The *completion* of A with respect to I is $\hat{A}:=\{(a_n)\in\prod_{n=1}^{\infty}(A/I^n)\mid a_n=a_{n+1}\mod I^n\ \forall n\}$. There exists a natural map $a\mapsto a \mod I^n$. If it is an isomorphism then A is said to be *complete*.

Example 3.2.

1. Let $A=\Bbbk[x]$ and $I=(x)$. Then A/I^n is the truncated polynomial ring of degree $\leq n-1$. Then $\hat{A}=\Bbbk[[x]]$.
2. More generally, if A is a polynomial ring $\Bbbk[x_1,\dots,x_n]$ and $I=(x_1,\dots,x_n)$ then $\hat{A}:=\Bbbk[[x_1,\dots,x_n]]$. The answer for $A=\Bbbk[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$ is the same. This is an example of a regular local ring such that completion is the power series ring. However, generally it does not hold for all regular, local ring.
3. For $A=\mathbb{Z}$ and $I=(p)$ we get the p-adic integers $\mathbb{Z}_p$.

As before, we have $\mathrm{gr}_I(A)=\oplus_{n=0}^{\infty}I^n/I^{n+1}$. In example 1) and 2) we get back the polynomial ring this way.

Remark 3.3. Recall that an inverse system of modules (over a fixed ring) indexed by $n\in\mathbb{N}$ is given by

- modules M_n for all $n\in\mathbb{N}$
- morphisms $\varphi_n:M_n\to M_{n-1}$ for all $n\in\mathbb{N}$.

Then the *inverse limit* of this sequence is

$$\varprojlim M_n=\left\{(m_n)\in\prod_{n=0}^{\infty}M_n\mid m_n=\varphi_{n+1}(m_{n+1})\ \forall n\in\mathbb{N}\right\}$$

Exercise 3.4.

1. Given a chain of submodules $M^0 \supseteq M^1 \supseteq M^2 \supseteq \dots$ one can construct an inverse system where $M_n := M/M^n$ where the maps $M_n \to M_{n-1}$ are the natural ones. Let us denote the inverse limit by $\hat{M}$. There exists a projection $p_n : \hat{M} \to M_n$ by forgetting all components except the n-th one. These maps are obviously surjective but they can have kernel $\hat{M}^n := \ker(p_n)$. Nevertheless, $\hat{M}/\hat{M}^n \overset{\cong}{\to} M/M^n$ is an isomorphism.

2. There is an important special case: when $I \subseteq A$ is an ideal and $M^n := I^n M$. In this case, $\hat{M}$ is called the *I-adic completion of M*. An even more special case is when $A = M$. This way we get back the previous definition of a completion of a ring.

Remark 3.5. M can be endowed with a topology in which M^i form a basis of neighborhoods of (0). In the case where $M^n = I^n M$ it is called the *I-adic topology.*

Definition 3.6. $(m_n) \subseteq M$ is a *Cauchy-sequence* if for all n there exists an N_0 such that $m_i - m_j \in M^n$ for all $i, j \geq N_0$. It converges to $m \in M$ if for all n there exists an i_0 such that $i \geq i_0$ we have $m - m_i \in M^n$.

Remark 3.7. If A is Noetherian then in $\hat{M}$, every Cauchy-sequence is convergent, i.e. it is a completion in the metric sense using the pseudo-metric

$$d(x, y) = \exp\big(-\max\{n \in \mathbb{N} \mid x - y \in M^n\}\big)$$

which is a metric if $\cap_n M^n = 0$. If A is not necessarily Noetherian this completion is not necessarily complete (!). Counterexample: Take $A = \Bbbk[x_1, x_2 \dots]$ the polynomial ring in infinitely many variables over a field as a module over itself and set $I = (x_1, x_2, \dots)$. Then it is easy to check that $\hat{A} = \Bbbk[[x_1, x_2, \dots]]$ and similarly for $\hat{M}$. However, the sequence $a_n = \sum_{i=1}^n x_i^i$ is Cauchy but has no limit. Indeed, if it would have then that could be only $\sum_{i=1}^\infty x_i^i$ by looking at the finite degree parts but the tails $\sum_{i=n+1}^\infty x_i^i$ are not elements of $I^k M$ for any k. (see Amnon Yekutieli: On Flatness and Completion for Infinitely Generated Modules over Noetherian rings, Communications in Algebra, 2011)

Proposition 3.8. *Slogan: If M^n and N^n generate the same topology then the completions are isomorphic. Precisely: Let M be an A-module with two chains of submodules $M^0 \supseteq M^1 \supseteq M^2 \supseteq \dots$ and $N^0 \supseteq N^1 \supseteq N^2 \supseteq \dots$ such that for all n there exists an m such that $N^m \subseteq M^n$ and similarly with the reversed order of N and M (This property is sometimes called "nested sequences"). Then there exists a canonical isomorphism such that*

$$\lim_{\leftarrow} M/M^n \overset{\cong}{\to} \lim_{\leftarrow} M/N^m$$

Proof. In the special case, when (N^m) is a subsequence of M^n, the statement is obvious since the natural map $\lim_{\leftarrow} M/M^n \to \lim_{\leftarrow} M/N^m$ forgetting the unnecessary elements gives an isomorphism. (We can define the inverse explicitly). Generally, there exist strictly increasing maps $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ such that $N^{\alpha(n)} \subseteq M^n$ and $M^{\beta(n)} \subseteq N^n$. Hence, we get natural projections $M/N^{\alpha(n)} \to M/M^n$ and $M/M^{\beta(n)} \to M/N^n$ yielding maps

$$\lim_{\leftarrow} M/M^n \to \lim_{\leftarrow} M/N^{\alpha(n)} \qquad \text{and} \qquad \lim_{\leftarrow} M/N^n \to \lim_{\leftarrow} M/M^{\beta(n)}$$

which can be composed from the right with the previously constructed maps in the case of subsequences. So we get two maps between $\lim_{\leftarrow} M/M^n$ and $\lim_{\leftarrow} M/N^n$ and by the canonicity of the construction it is easy to verify that they are inverses of each other. □

Proposition 3.9. *Let A be a local ring with maximal ideal P. Then $\hat{A}$ is a local ring with maximal ideal $\hat{P} := \mathrm{Ker}(\hat{A} \to A/P)$.*

Proof. First, if $m \in \hat{P}$ then $1 - m$ is a unit in $\hat{A}$ because $\sum_{i=0}^{\infty} m^i \in \hat{M}$ is its inverse. Moreover, since $\hat{A}/\hat{P} \overset{\cong}{\to} A/P$ is a field, $\hat{P}$ is a maximal ideal. What is not so trivial is that it does not have any other maximal ideals. If $P' \subseteq \hat{A}$ is a maximal ideal, $m \in \hat{P} \backslash P'$ then $(m, P') = \hat{A}$ by maximality of P'. This means that there exists an $a \in \hat{A}$ and $b \in P'$ such that $1 = am + b$. However, then $1 - am = b \in P'$ what contradicts $1 - am$ being a unit. □

Fourth Lecture, 3rd of February

Assumptions: In the following A will be a fixed Noetherian ring, $I \subseteq A$ is a fixed ideal and M is a fixed A-module. We consider the completion $\hat{M} := \lim_{\leftarrow} M/I^n M$.

Proposition 3.10. *Completion is an exact functor. In details: let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of finitely generated A-modules. Then their completions $0 \to \hat{M}_1 \to \hat{M}_2 \to \hat{M}_3 \to 0$ also form an exact sequence.*

Before proving it, we first list some of its consequences.

Corollary 3.11. *There exist canonical isomorphisms $\hat{A}/\hat{I} \cong A/I$ and more generally $\hat{I}^n/\hat{I}^{n+1} \overset{\cong}{\to} I^n/I^{n+1}$ for all $n \in \mathbb{N}$. Therefore, $\mathrm{gr}_{\hat{I}}(\hat{A}) \overset{\cong}{\to} \mathrm{gr}_I(A)$ by "bringing the generators into the generators" i.e.*

$$\begin{array}{ccc} \Bbbk[x_1, \ldots, x_n] & \longrightarrow & \mathrm{gr}_I(A) \\ \Big\| & & \Big\downarrow \\ \Bbbk[x_1, \ldots, x_n] & \longrightarrow & \mathrm{gr}_{\hat{I}}(\hat{A}) \end{array}$$

Proof. (of the corollary) Apply the previous proposition with $M_1 = I^{n+1}$, $M_2 = I^n$ and $M_3 = I^n/I^{n+1}$ and observe that $I^n/I^{n+1} \cong \widehat{I^n/I^{n+1}}$. Therefore the stated isomorphisms exist (by $I^0 = A$ the first one as well) and $\mathrm{gr}(.)$ is just the direct sum of the appropriate terms. □

Corollary 3.12. (Corollary of Corollary 3.11) *Assume that A is a Noetherian, local ring. Then A is a regular if and only if $\hat{A}$ is regular ring.*

Proof. By Proposition 3.9 we know that $\hat{A}$ is local, if A is local. The regularity follows directly from the previous corollary $\mathrm{gr}_P(A) \cong \mathrm{gr}_{\hat{P}}(\hat{A})$ and Theorem 2.11 telling that regular local rings are characterized by the property that the natural map $(A/P)[x_1, \ldots, x_n] \to \mathrm{gr}_P(A)$ is an isomorphism. . □

Corollary 3.13. (of Proposition 3.10) *If $J \subseteq A$ is any ideal then its I-adic completion (as an A-module) satisfies $\hat{J} \cong J \cdot \hat{A}$ where $J\cdot$ stands for multiplication with the image of J in $\hat{A}$. (Note that A is not necessarily a subring of $\hat{A}$.)*

Proof. Let's apply the Proposition 3.10 on the short exact sequence $0 \to J \to A \to A/J \to 0$ yielding

$$0 \longrightarrow \hat{J} \longrightarrow \hat{A} \longrightarrow \widehat{A/J} \longrightarrow 0$$

so we get that $\widehat{A/J} \cong \hat{A}/\hat{J}$. Now, assume that $J = (a_1, \ldots, a_n)$ by Noetherian property. Let's define a map

$$\varphi : A^n \to A$$

$$(t_1, \ldots, t_n) \mapsto \sum_{i=1}^{n} a_i t_i$$

This induces a map on the completions $\hat{\varphi} : \hat{A}^n \to \hat{A}$ given by the same formula. The image of φ is exactly $AJ = J$ (we defined it so) hence the sequence

$$A^n \xrightarrow{\varphi} A \longrightarrow A/J \longrightarrow 0$$

is exact. Therefore, its completion

$$\hat{A}^n \xrightarrow{\hat{\varphi}} \hat{A} \longrightarrow \hat{A}/\hat{J} \longrightarrow 0$$

is also exact. But $\hat{J} \overset{\text{exactness}}{=} \operatorname{Im} \hat{\varphi} \overset{\text{def of } \varphi}{=} J\hat{A}$ so we got the statement. □

Corollary 3.14. *If $I = (a_1, \ldots, a_n)$ and we complete A at I then $\hat{A} \cong A[[x_1, \ldots, x_n]]/(x_1 - a_1, \ldots, x_n - a_n)$.*

The statement seems a bit counter intuitive when compared to the isomorphism $A[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong A$. However, it is at least a characterization but not a really nice one.

Proof. Let $B := A[x_1, \ldots, x_n]$ and $J = (x_1 - a_1, \ldots, x_n - a_n)$. Then we get a short exact sequence:

$$0 \longrightarrow J \longrightarrow B \longrightarrow A \longrightarrow 0$$

where we mapped $B \ni x_i \mapsto a_i$ for all i. Half-exactness is clear and exactness can be proved by the following elementary argument: if $p \in \ker(B \to A)$ then

$$\sum_i c_i x^i =: p(x) = p(x) - p(a) = \sum_i c_i(x^i - a^i) = (x - a) \sum_i c_i(x^{i-1} + x^{i-2}a + \cdots + a^{i-1})$$

proving $p \in J$. For $n > 1$ we can use induction on the number of variables.

Now, we complete everything with respect to $(x_1, \ldots, x_n)$ as a B-module, where $J \subset B$ is a B-module in a natural way and A is a B-module by the $B \to A$ map we just described. Hence, completing these modules gives – by the Proposition 3.10 – that $\hat{A} = \hat{B}/\hat{J}$. But $\hat{J} = J\hat{B}$ by the Corollary 3.13 and $\hat{B} = A[[x_1, \ldots, x_n]]$ by unpacking the definition. The statement follows. □

Example 3.15. Let $A = \mathbb{Z}$ and $I = (p)$ where p is an arbitrary prime. We observed that the completion with respect to (p) gives $\mathbb{Z}_p$, the p-adic integers. By the proposition we get that

$$\mathbb{Z}_p \cong \mathbb{Z}[[x]]/(x - p)$$

Remark 3.16. The idea of the proof of Proposition 3.10 is that completion is automatically a left exact functor (as it is an inverse limit) and we have a condition, called Mittag-Leffler condition that can decide whether a left exact functor is exact. In principle, we check this condition on the completion functor but in a more direct language.

Proof. The first step is showing that the following short sequence is exact:

$$0 \longrightarrow \lim_{\leftarrow} M_1/(I^n M_2 \cap M_1) \longrightarrow \lim_{\leftarrow} M_2/I^n M_2 \longrightarrow \lim_{\leftarrow} M_3/I^n M_3 \longrightarrow 0$$

where the reason we took $M_1/(I^n M_2 \cap M_1)$ is that the natural filtration induced on the "image" of M_1 in $M_2/I^n M_2$ is $(I^n M_2 \cap M_1)$.

The second step is to show that for all $m > 0$ there exists an $n > 0$ such that $I^n M_2 \cap M_1 \subseteq I^m M_1$. Besides, note that $I^m M_1 \subseteq I^m M_2 \cap M_1$ obviously holds so by the second step we will see that the two filtrations give the same topology on M_1. Therefore, by Proposition 3.8, $\lim_{\leftarrow} M_1/I^n M_1 \cong \lim_{\leftarrow} M_1/(I^n M_2 \cap M_1)$. In short, we can replace the first term in the short exact sequence.

To prove the first step, we will use the following general statement about inverse limits: let (N_n^1), (N_n^2), (N_n^3) be inverse systems of modules such that for all n there exists a commutative diagram of exact sequence as

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_n^1 & \xrightarrow{f_n} & N_n^2 & \xrightarrow{g_n} & N_n^3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\varphi_n^1} & & \downarrow{\scriptstyle\varphi_n^2} & & \downarrow{\scriptstyle\varphi_n^3} & & \\ 0 & \longrightarrow & N_{n-1}^1 & \xrightarrow{f_{n-1}} & N_{n-1}^2 & \xrightarrow{g_{n-1}} & N_{n-1}^3 & \longrightarrow & 0 \end{array}$$

If φ_n^2 and φ_n^3 are surjective for all n (hence φ_n^1 too) then

$$0 \longrightarrow \lim_{\leftarrow} N_n^1 \longrightarrow \lim_{\leftarrow} N_n^2 \longrightarrow \lim_{\leftarrow} N_n^3 \longrightarrow 0$$

is exact. Indeed, the left-exactness is true for every (inverse) limit by general nonsense while exactness at $\lim_{\leftarrow} N_n^3$ follows from diagram chasing: if we have a sequence $(c_n)_{n\in\mathbb{N}} \in \prod_n N_n^3$ representing an element of the limit, i.e. $\varphi_n^3(c_n) = c_{n-1}$ then by induction we can choose a compatible system of preimages $(b_n)_{n\in\mathbb{N}} \in \prod_n N_n^2$ so that $\varphi_n^2(b_n) = b_{n-1}$ and $g_n(b_n) = c_n$ as follows. The induction can start by an arbitrary preimage b_1. Now, assume that b_{n-1} is already given. Take a preimage $\tilde{b}_n \in N_n^2$ of $c_n \in N_n^3$ along g_n arbitrarily (which exists by row-exactness). It can happen that $\varphi_n^2(\tilde{b}_n)$ is not b_{n-1} so take the difference $b_{n-1} - \varphi_n^2(\tilde{b}_n)$. This maps to $0 \in N_{n-1}^3$ because

$$g_{n-1}\varphi_n^2(\tilde{b}_n) = \varphi_n^3 f_n(\tilde{b}_n) = \varphi_n^3(c_n) = c_{n-1} = g_{n-1}(b_{n-1})$$

Therefore, we can take a preimage of the difference $a_{n-1} \in N_{n-1}^1$ along f_{n-1} and also its (arbitrarily chosen) preimage $a_n \in N_n^1$ along φ_n^1. Then $b_n := \tilde{b}_n + f_n(a_n)$ has the required properties: $\varphi_n^2(b_n) = b_{n-1}$ and $g_n(b_n) = c_n$. This proves the first step since the surjectivity assumption on the three sequences $M_1/(I^n M_2 \cap M_1)$, $M_2/I^n M_2$ and $M_3/I^n M_3$ are trivially satisfied so the exactness of the first sequence of the proof follows.

Moreover, step two follows from the following statement:

Lemma 3.17. (Artin-Rees Lemma) *Let A be a Noetherian ring, I and ideal and M be a finitely generated A-module. Let $M_1 \subseteq M$ be a (necessarily finitely generated) submodule. Then there exists a $k > 0$ such that $I^n M \cap M_1 = I^{n-k}(I^k M \cap M_1)$ for all $n > k$.*

One can see the second step by choosing $M_1 = M_1$ and $M = M_2$, moreover, choosing n so large that $n - k > m$.

Proof. The key of the lemma is a clever application of the Hilbert Basissatz to the following special ring. Consider $B_I(A) := \oplus_{n=0}^{\infty} I^n$ and $B_I(M) = \oplus_{n=0}^{\infty} I^n M$. The former is a graded ring and the latter is a graded module over this ring. Clearly, $I^n(I^k M) \subseteq I^{n+k} M$ for all $n, k > 0$. Moreover, M is a finitely generated A-module so $B_I(M)$ is a finitely generated $B_I(A)$-module using the same generators. Besides, a finite set of generators of I together with $1 \in I^0$ generates $B_I(A)$ as an A-algebra. Therefore, it is Noetherian by the Hilbert Basissatz.

Let $B_1 := \oplus_{n=0}^{\infty}(I^n M \cap M_1)$. It is a $B_I(A)$-submodule of the finitely generated module $B_I(M)$ hence it is also finitely generated by the Noetherian property proved in the previous paragraph. It means that there exists a $k > 0$ such that all generators are contained in $\oplus_{n=0}^{k}(I^n M \cap M_1)$. Let $m_1, \ldots, m_r$ be these generators, where we may assume that each m_i is homogeneous (if one is not then we replace it with its homogeneous components). So for all $1 \le j \le r$ there exists an $\alpha(j) \le k$ such that

$$m_j \in I^{\alpha(j)} M \cap M_1$$

Now, assume that $m \in I^n M \cap M_1$ for some $n > k$. Then, by the above notation it has a decomposition

$$m = \sum_{j=1}^{r} i_j^{n-\alpha(j)} m_j$$

where $i_1, \ldots, i_r \in I$ (so the exponents are just representing the degrees of the coefficients). Now, let us express this m as

$$m = \sum_{j=1}^{r} i_j^{n-k}(i_j^{k-\alpha(j)} m_j) \in I^{n-k}(I^k M \cap M_1)$$

by the choice of m_j and $\alpha(j)$. This is exactly the required form. □

The statement follows. □

Corollary 3.18. (Krull's Intersection theorem) *If A is a Noetherian local ring with maximal ideal P then the intersection $\cap_n P^n = (0)$.*

Proof. Set $N := \cap_n P^n$. It is enough to prove $PN = N$ since then $N = 0$ by Nakayama. Clearly, $PN \subseteq N$ and for the converse we use the Artin-Rees lemma. The Artin-Rees Lemma gives a k such that

$$N = P^{k+1} \cap N = P(P^k \cap N)$$

by the choice of $N = M_1$ and $P = M$. However, the right hand side is already contained in PN so we got the claim. □

Remark 3.19. Note that this corollary is already used in proving Theorem 2.11 about regular sequences but this does not yield a circular argument since in the proof of Corollary 3.18 we only used the Nakayama lemma and the Artin-Rees lemma 3.17 (hence the Hilbert Basissatz), nothing more.

Corollary 3.20. *Under the assumption of Krull's Intersection theorem, $A \to \hat{A}$ is injective.*

Proof. The claim depends only on the fact that the kernel of this map is exactly $\cap_n P^n$ which is now zero by the referred statement. □

4 Cohen Structure Theorem

Theorem 4.1. *Let A be a complete Noetherian local ring that contains a subfield $\Bbbk \subseteq A$ that maps isomorphically onto A/P via $A \to A/P$. Then A is a quotient of some power series ring $\Bbbk[[x_1, \ldots, x_n]]$. If, moreover, A is regular then $A \cong \Bbbk[[x_1, \ldots, x_n]]$.*

Remark 4.2.

1. The power series ring is regular since it is complete and its associated graded ring is the polynomial ring (see Theorem 2.11).

2. For the most natural local regular rings, i.e. the local rings at a point of a variety over $\Bbbk = \overline{\Bbbk}$ satisfy the above assumption.

Lemma 4.3. *Let $\varphi : A \to B$ a homomorphism of complete local rings (with maximal ideals P_A and P_B) such that $\varphi(P_A^n) \subseteq P_B^n$ for all $n \in \mathbb{N}$. If the induced homomorphism $\mathrm{gr}\varphi : \mathrm{gr}_{P_A}(A) \to \mathrm{gr}_{P_B}(B)$ is injective (resp. surjective) then φ too.*

Proof. Consider the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_A^n/P_A^{n+1} & \longrightarrow & A/P_A^{n+1} & \longrightarrow & A/P_A^n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{gr}_n(\varphi)} & & \downarrow{\scriptstyle \varphi_{n+1}} & & \downarrow{\scriptstyle \varphi_n} & & \\
0 & \longrightarrow & P_B^n/P_B^{n+1} & \longrightarrow & A/P_B^{n+1} & \longrightarrow & A/P_B^n & \longrightarrow & 0
\end{array}$$

where φ_n is induced by φ on the factor by $\varphi(P_A^n) \subseteq P_B^n$. By induction we can prove that all the φ_n are injective. For $n = 0$ we can apply the hypothesis since $\varphi_0 = \mathrm{gr}_0(\varphi) : A/P_A \to B/P_B$. For the induction step, assume that φ_n is injective. Then in the above diagram $\mathrm{gr}_n(\varphi)$ and φ_n are injective so φ_{n+1} is injective too by the Snake-lemma. The injectivity of φ follows by the left-exactness of the inverse limit.

In the case of surjectivity, one has to be more careful since we want to lift the elements in a compatible way. The proof is diagram chasing, see reference. □

Proof of Theorem 4.1. : Let $t_1, \ldots, t_d$ be a system of generators of the maximal ideal $P \subsetneq A$. Then there exists a unique $\Bbbk$-algebra homomorphism $\lambda : \Bbbk[[x_1, \ldots, x_d]] \to A$ by $x_i \mapsto t_i$, because for all n there exists

$$\Bbbk[[x_1, \ldots, x_d]]/(x_1, \ldots, x_d)^n \cong \Bbbk[x_1, \ldots, x_d]/(x_1, \ldots, x_d)^n \to A/P^n$$

because the polynomial ring is a free $\Bbbk$-algebra, these together build λ. To prove surjectivity of λ we would like to use the previous Lemma so we turn to the induced map $\mathrm{gr}(\lambda) : \mathrm{gr}_{(x_1,\ldots,x_d)}(\Bbbk[[x_1, \ldots, x_n]]) \to \mathrm{gr}_P(A)$. Since $A/P \cong \Bbbk$ where $P = (t_1, \ldots, t_d)$ and the λ_n's for $n > 0$ are surjective too by $t_1, \ldots, t_d$ being a system of generators for P, we get that $\mathrm{gr}(\lambda)$ is surjective too. Therefore, by Lemma 4.3 we get that the above defined λ is surjective.

The second part of the statement states that if A is regular then λ is also injective. Again, we would like to use the previous lemma. By the assumption, we can choose $d = \dim A$ in $t_1, \ldots, t_d$ by the definition of regularity. Therefore,

$$\lambda : \Bbbk[[x_1, \ldots, x_d]] \to A$$

is surjective with kernel the prime ideal Q. (It is indeed a prime since by Theorem 2.6 a regular local ring is an integral domain). However, $\dim A = \dim \Bbbk[[x_1, \ldots, x_d]] = d$ hence $\mathrm{ht}Q = 0$ so it is zero as $\Bbbk[[x_1, \ldots, x_d]]$ is an integral domain. □

Corollary 4.4. *Assume now that A is a regular local ring and there exists a $\Bbbk \subseteq A$ subfield mapping onto A/P. Then there exists an injection $A \to \Bbbk[[t_1, \ldots, t_d]]$.*

Proof. We know by Corollary 3.20 that $A \to \hat{A}$ is injective and $\hat{A}$ is regular by Corollary 3.12 if the original A was. However, then by the previous Theroem 4.1 we know that $\hat{A}$ is isomorphic to a power series ring, proving the statement. □

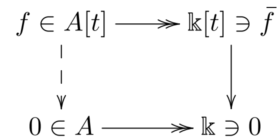
Remark 4.5. In the $d = 1$ case, there is also an elementary proof. Assume that $b \in A$ and $P = (t)$ (by $d = 1$). Then write $b = a_0 + b_1 t$ where $a_0 \in \Bbbk$ and $b_1 \in A$. Now, we can iterate this on $b_1 = a_1 + b_2 t$, then on b_2 and so on. So we get a power series expansion for b. One can check that it gives an injective homomorphism.

Fifth Lecture, 10th of February

4.1 Equi-characteristic case

Goal: The condition $\Bbbk \subseteq A$ in Theorem 4.1 is superfluous if the characteristic of A is the same as of the residue field $\Bbbk$.

Lemma 4.6. (Hensel's lemma) *Let A be a complete local ring with maximal ideal P and residue field $A/P =: \Bbbk$. Let $f \in A[t]$ and $\overline{f}$ be the image of f in $\Bbbk[t]$. Assume that $\overline{a} \in \Bbbk$ is such that $\overline{f}(\overline{a}) = 0$ but $\overline{f}'(a) \neq 0$. Then there exists a unique $a \in A$ such that $\overline{a} = a$ mod P and $f(a) = 0$. In other words, the following diagram can be completed if $\overline{f}'(a) \neq 0$:*



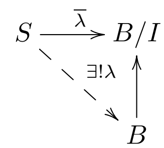
Proof. Since A is complete with respect to P, it is enough to construct elements $a_n \in A/P^n$ for all n such that $a_1 = \overline{a}$, $a_{n-1} = a_n \mod P^n$ and $f(a_n) = 0$ in A/P^n. (This is called successive approximation.) Therefore, it is enough to prove the following:

Claim 4.7. Let B be an arbitrary ring with ideal I such that $I^2 = 0$ and $f \in B[t]$ with a $b \in B$ such that $f(b) \in I$ but $f'(b)$ is a unit in B. Then there exists a unique $c \in B$ such that $f(c) = 0$ and $c = b \mod I$.

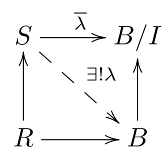
The claim implies Lemma 4.6: by the choice $B = A/P^n$, $I = P^{n-1}/P^n$ and $a_n := b$ being any lift of a_{n-1} to A/P^n. Then to continue the induction all the conditions of the claim are clear except maybe that $f'(b)$ is a unit in A/P^n. But this is also true because a_n maps to $\overline{a} \mod P/P^n$ hence $f'(a_n)$ maps to $f'(\overline{a})$ in P/P^n which is nonzero hence it is invertible by locality.

In fact, instead of the claim, we will prove an even more general fact:

Proposition 4.8. *Let B be an R-algebra (i.e. a ring and an R-module with a compatible way) with an ideal I such that $I^2 = 0$. Let $S = R[T]/(f)$ which is naturally an R-algebra as $R \subseteq S$. If for a map $\overline{\lambda} : S \to B/I$ there exists a preimage $b \in B$ of $\overline{\lambda}(T)$ such that $f'(b)$ is a unit in B then there is a unique map of R-algebras λ completing the following diagram commutatively:*



Remark 4.9. If one wants to remove the word R-algebras and unpack the definition "morphism of R-algebras" then the statement is equivalent to the following diagram



since for a unital ring A an R-algebra structure is the same as having a fixed ring-morphism $R \to A$. Similarly, the morphism of R-algebras is just the compatibility of a ring morphism with these fixed ones.

The previous claim is a special case of this proposition by the choice $R = B$, $\mu = \mathrm{id}_B$ and $\overline{\lambda} : B[T]/(f) \to B/I$ mapping T to $b + I$. Then $c := \lambda(b)$ satisfies the stated conditions in the previous claim.

Proof of Proposition 4.8. : Choose b as in the Proposition. To define λ it is sufficient to find $h \in I$ such that $f(b+h) = 0$ since then $\lambda(T) := b + h$ gives a well-defined map with $(/I) \circ \lambda = \overline{\lambda}$. (In fact, there is no other way to define the image of T in the form of $b+h$ to make the diagram commutative.) If, moreover, we prove the uniqueness of h then that proves uniqueness of λ as well.

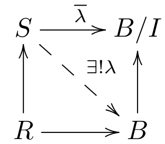
By the "Taylor-formula" for polynomials, write

$$f(b+h) = f(b) + f'(b)h$$

which has no more terms since $h^2 \in I^2 = 0$. Therefore, $h = (f'(b))^{-1}(-f(b))$ which makes sense since $f'(b)$ is a unit. This choice of h satisfies the statement. Moreover, since we expressed h by known terms, h is unique hence λ too. □

This proves Hensel's lemma 4.6. □

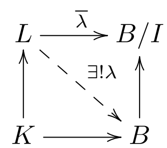
Remark 4.10. Grothendieck defines an R-algebra S to be *formally étale* if for all R-algebra B and $I \subseteq B$ such that $I^2 = 0$ and for every R-algebra map $\overline{\lambda} : S \to B/I$, there exists a unique map $\lambda : S \to B$ that makes the following diagram commutative:



i.e. as an R-algebra morphism $\overline{\lambda}$ can be lifted to B. If it only exists but not uniquely then it is called *formally smooth*. So, in these terms, we have proven that $S = R[T]/(f)$ is formally étale if $(f, f') = (1)$ in $R[T]$. (In fact, we proved a little more since our assumption was somewhat weaker.)

Proposition 4.11. (Generalization of Proposition 4.8, not proven) *Let* $S = R[T_1, \dots, T_n]/(f_1, \dots, f_n)$ *and define* $\mathrm{Jac}(f_1, \dots, f_n) := \det[\partial_i f_j]$. *If this latter maps to a unit in* S *then* S *is formally étalé over* R. *Similarly, if* $S = R[T_1, \dots, T_n]/(f_1, \dots, f_m)$ *such that the maximal minors of* $[\partial_i f_j]$ *map to units in* S *then* S *is formally smooth.*

Corollary 4.12. *Let* $L \mid K$ *be a (not necessarily finite) separable algebraic field extension,* B *a* K*-algebra with an ideal* I *such that* $I^2 = 0$. *Then there exists a unique* $\lambda : L \to B$ *such that the following diagram commutes:*



The same holds if instead of $I^2 = 0$ *we assume that* B *is complete with respect to* I.

Proof. If $L \mid K$ is a finite separable extension then $L = K[T]/(f)$ where f' is a unit modulo (f). So the statement in this case is the direct consequence of Proposition 4.8. In the general case $L = \cup_{i \in I} L_i$ where $L_i \mid K$ is a finite separable extension for all i and $\overline{\lambda}|_{L_i}$ lifts to λ on L_i uniquely (!). Hence they "glue together" since on the intersection they have to coincide. □

Remark 4.13. If $L \mid K$ is not finite then this is an example of a formally smooth algebra that is not of finite type.

Definition 4.14. A complete local integral domain is called *equi-characteristic* if $\operatorname{char} A = \operatorname{char} \Bbbk$ where $\Bbbk = A/P$, the residue field.

Remark 4.15. Note that A is equi-characteristic if and only if A contains a field. Indeed, if $\operatorname{char} A = \operatorname{char} \Bbbk = p \neq 0$ then we have the prime field $\mathbb{F}_p$ (the generated subfield of 1). Similarly, if $\operatorname{char} A = \operatorname{char} \Bbbk = 0$ then $\mathbb{Z} \subseteq A$ and for this we have $\mathbb{Z} \cap P = (0)$ by the assumption. Therefore, every nonzero $m \in \mathbb{Z}$ is a unit hence $\mathbb{Q} \subseteq A$. The converse is even more straightforward. This field in A could be always smaller than $\Bbbk$. The following theorem states that it is not.

Theorem 4.16. (Cohen) *If* A *is an equi-characteristic complete local domain with residue field* $\Bbbk$ *then there exists a subfield in* A *mapping isomorphically onto* $\Bbbk$ *via* $A \to A/P \cong \Bbbk$. *(I.e.* $A \to A/P$ *is a retraction.)*

Combining this theorem with Theorem 4.1 gives

Corollary 4.17. (Cohen Structure Theorem) *If* A *is equi-characteristic complete local domain with residue field* $\Bbbk$ *then* A *is a quotient of some power series ring* $\Bbbk[[t_1, \dots, t_n]]$. *If, moreover,* A *is regular of dimension* d *then* $A \cong \Bbbk[[t_1, \dots, t_n]]$.

Proof of Theorem 4.16. : First, assume that $\operatorname{char} A = \operatorname{char} \Bbbk = 0$. Then we want to factor through on A the identity map of $\Bbbk$. We can choose a maximal subfield $\Bbbk' \subseteq \Bbbk$ for which such a factorization exists. Indeed, there exists $\mathbb{Q} \subseteq \Bbbk$ and we can use Zorn's lemma since the supremum of a chain is its union.

Assume, indirectly, that $\Bbbk' \subsetneq \Bbbk$. If there exists $\overline{x} \in \Bbbk$ transcendental over $\Bbbk'$ then lift it to $x \in A$. Then $\Bbbk'[x] \cap P = (0)$ else it would be generated by an element $f(x)$ hence $\overline{x}$ is algebraic which is a contradiction. It means that all nonzero elements of $\Bbbk'[x]$ are units so $\Bbbk'(x) \subseteq A$ but that is a contradiction since $\Bbbk'(\overline{x}) \to \Bbbk(x)$ is a larger subfield. So there are no transcendental elements over $\Bbbk'$. In other words, $\Bbbk \mid \Bbbk'$ is algebraic of characteristic zero hence it is also separable. Therefore we can apply Corollary 4.12 what gives a contradiction (because there is a lifting).

Now, assume that $\operatorname{char} A = \operatorname{char} \Bbbk = p > 0$. The proof follows from the following lemma the same way as the characteristic zero case:

Lemma 4.18. *Let B be a ring with an ideal I such that $I^2 = 0$ and let L be a field of characteristic $p > 0$. Then every nonzero map $\overline{\lambda} : L \to B/I$ lifts to $\lambda : L \to B$. In particular, L is a formally smooth $\mathbb{Z}$-algebra.*

Proof. In characteristic $p > 0$, $L^p \subseteq L$ is a subfield by the binomial theorem. Define $\lambda_p : L^p \to B$ as follows: Given an element $a \in L$, lift $\overline{\lambda}(a)$ to $b \in B$ and set $\lambda_p(a^p) := b^p$. First, observe that this is well-defined: If b' is another lift of $\overline{\lambda}(a)$ then $b - b' \in I$ so $b^p - (b')^p$ is the same as $(b - b')^p \in I^p \subseteq I^2 = 0$. If L is perfect then – by definition – $L^p = L$ so we are done.

If L is not perfect then analogously to the proof in zero characteristic, we can find a maximal subfield $L' \subseteq L$ such that $L' \supseteq L^p$ and $\overline{\lambda}|_{L'}$ lifts to $L' \to B$. We show that $L' = L$. Assume that it is not, and pick an $\alpha \in L \backslash L'$. Then $\alpha^p \in L^p \subseteq L'$ and hence $x^p - \alpha^p$ is the minimal polynomial over L' (by straightforward general nonsense about non-separable field extensions). Moreover, if we lift $\overline{\lambda}(\alpha)$ to β, then $\beta^p = \lambda_p(\alpha^p)$ by the definition of λ_p so $\alpha \mapsto \beta$ induces a map $L'(\alpha) = L'[x]/(x^p - \alpha^p) \to B$. That contradicts the maximality of L'. □

The theorem follows. □

4.2 Mixed characteristic case

Question. *What about complete local rings of mixed character, i.e. when* $\operatorname{char} A = 0$ *and* $\operatorname{char} \Bbbk = p > 0$.

Step1: Given a field $\Bbbk$ of characteristic $p > 0$ there exists a complete discrete valuation ring A_0 of characteristic 0 (called the *Cohen ring*) with residue field $\Bbbk$ and maximal ideal (p). (We will only prove this for the case of perfect residue field.)

Step2: Let A be a complete local domain of characteristic zero with maximal ideal P and residue field $A/P =: \Bbbk$ of characteristic $p > 0$. If A_0 is a Cohen ring with residue field $\Bbbk$ then $\mathrm{id}_\Bbbk$ lift to a homomorphism $A_0 \to A$. (This was a project for grade.)

Remark 4.19. The map $A_0 \to A$ must be injective since it has only one nontrivial prime ideal (p) but A has characteristic zero so it is impossible to have (p) as the kernel.

Step3: For $A_0 \subseteq A$ as in the previous step, there exists a surjective homomorphism $A_0[[x_1, \dots, x_n]] \twoheadrightarrow A$. If, moreover A is regular and $p \notin P^2$ then there exists a map for $n = d = \dim A_0 - 1$ and $A \cong A_0[[x_1, \dots, x_n]]$. By the presence of Step 2, the proof is the same as in Theorem 4.17: we find a minimal system $p, t_1, \dots, t_d$ of generators of P (here, $p \notin P^2$ is crucial) and we define maps $A_0[[x_1, \dots, x_n]]/(p, x_1, \dots, x_n)^n \to A/P^n$...

Sixth Lecture, 17 of February

Motivation: There are some situations when we want to deduce similar theorems in characteristic zero that are true in characteristic p and vice versa. For such purposes the construction below can be useful, where the residue field of the local ring has characterstic p and the field of fractions is characteristic zero.

Definition 4.20. (Serre, Lazard) An integral domain of characteristic $p > 0$ is *perfect* if and only if $x \mapsto x^p$ is an isomorphism. A *strict p-ring* is a ring A complete with respect to the ideal $pA \subseteq A$ such that p is not a zero-divisor and $\cap_n p^n A = (0)$.

Remark 4.21. In the definition we do not assume that pA is maximal.

Theorem 4.22.

1. *Given a perfect ring B of characteristic p, there exists a strict p-ring A with $A/pA \cong B$.*
2. *The described A is unique up to unique isomorphism, i.e. given strict p-rings A_1 and A_2 such that $B_i = A_i/pA_i$ is perfect for $i = 1, 2$ then every isomorphism $B_1 \stackrel{\overline{\varphi}}{\to} B_2$ lifts to a unique isomorphism $\varphi : A_1 \to A_2$ such that $/ \circ \varphi = \overline{\varphi} \circ /$.*

Remark 4.23. In case B is a field, the construction will give a complete discrete valuation ring A with $A/pA \cong B$. For our purposes, this is the interesting case, but we discuss the theorem for rings.

Example 4.24.

1. $\mathbb{Z}_p$ is a strict p-ring with $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$
2. Given a ring R, p a prime. Let $R[x^{p^{-\infty}}]$ be the R-algebra generated by the indeterminates x^{-p^i} with relations $(x^{p^{-(i+1)}})^p = x^{p^{-i}}$. In other words, this is the union of the polynomial rings $R[x, x^{p^{-1}}, \dots, x^{p^{-n}}]$. If $R = \mathbb{F}_p$ then this is a perfect ring. Indeed, there are no nilpotents so $x \mapsto x^p$ has kernel zero and any element has a p-th root by substituting $x^{p^{-1}}$. Moreover, if we complete $\mathbb{Z}[x^{p^{-\infty}}]$ with respect to $p\mathbb{Z}[x^{p^{-\infty}}]$ then we get a strict p-ring with "residue field" (i.e. factor at the ideal generated by p) $\mathbb{F}_p[x^{p^{-\infty}}]$.
3. We can generalize the second example to arbitrary number of indeterminates, even for infinite I. Perform a similar construction with $R[x_\alpha, \dots, x_\alpha^{p^{-n}} \mid \alpha \in \Lambda]$ where $\{x_\alpha \mid \alpha \in \Lambda\}$ is a family of variables. After completing and applying the above Theorem we get a strict p-ring $\mathbb{Z}[\{x_\alpha\}, p^{-\infty}]$ with residue ring $\mathbb{F}_p[\{x_\alpha\}, p^{-\infty}]$.

Remark 4.25. If B is a perfect ring, $\{b_\alpha \mid \alpha \in \Lambda\}$ are elements of B then it makes sense to substitute $x_\alpha \mapsto b_\alpha$ in $F \in \mathbb{F}_p[\{x_\alpha\}, p^{-\infty}]$ since in a perfect ring we can take (unique) p-th root, so this way we get an element of B.

Lemma 4.26. (Key Lemma) *Given a strict p-ring A, the natural map $A \to A/pA$ has a unique multiplicative section, i.e. a map $A/pA \stackrel{\rho}{\to} A$ such that $\pi \circ \rho = \mathrm{id}_{A/pA}$ and $\rho(\overline{a} \cdot \overline{b}) = \rho(\overline{a}) \cdot \rho(\overline{b})$. Moreover, $\rho(\overline{a})$ is the unique element of A such that $\overline{a} = \rho(\overline{a})$ modulo pA and $\rho(\overline{a}) \in \cap_{n=0}^\infty A^{p^n}$.*

Definition 4.27. This $\rho(\overline{a})$ is called the Teichmüller representative of $\overline{a}$.

Proof. It is enough to show that for given $\overline{a}$ there exists a unique $\rho(\overline{a})$ satisfying $\overline{a} = \rho(\overline{a})$ modulo pA and $\rho(\overline{a}) \in \cap_{n=0}^\infty A^{p^n}$. Indeed, the existence of the map $A/pA \stackrel{\rho}{\to} B$ follows from the existence of $\rho(\overline{a})$ for each $\overline{a}$, the multiplicativity follows from the uniqueness and the retractive property is exactly $\overline{a} = \rho(\overline{a})$ modulo pA.

So first, given $\overline{a} \in A/pA$ we prove that there exists an $a_i \in A/p^{i+1}A$ such that $\overline{a} = a_i$ modulo $p(A/p^{i+1}A)$ and a_i is in the image of $A^{p^i} \hookrightarrow A \to A/p^{i+1}A$. Indeed, since A/pA is perfect, there exists an $x \in A$ such that $\overline{a} = x^{p^i}$ modulo pA. Moreover, $(x+py)^{p^i} = x^{p^i}$ modulo $p^{i+1}A$ for arbitrary $y \in A$ (i.e. x is not unique). However, this means that x^{p^i} modulo $p^{i+1}A$ does not depend on x. Let us denote this element by a_i. Since $x^{p^i} \in A^{p^{i-1}} \subseteq A^{p^i}$ it follows that (x^{p^i} modulo p^iA) $=$ (a_i modulo $p^iA/p^{i+1}A$). The right hand side is a_{i-1} so x^{p^i} modulo p^iA is also a_{i-1} by uniqueness. Therefore, we can find a sequence $(a_i) \in \lim_{\leftarrow} A/p^{i+1}A$. Denote this element by $\rho(\overline{a})$. By construction, we know that $\rho(\overline{a}) = \overline{a}$ modulo pA.

We only need that $\rho(\overline{a}) \in A^{p^n}$ for all $n \in \mathbb{N}$. So fix $n > 0$: So let $\overline{b}_n \in A/pA$ be the unique element such that $(\overline{b}_n)^{p^n} = \overline{a}$ (such element exists since the ring is perfect). As before, there exists a $b_n \in A$ such that $\overline{b}_n = b_n$ modulo pA and (b_n modulo $p^{i+1}A$) comes from A^{p^i}. But then $b_n^{p^n}$ modulo $p^{i+1}A$ also comes from A^{p^i} for all i and it maps to $\overline{a}$ modulo pA. The uniqueness of a_i implies $b_n^{p^n} = \rho(\overline{a})$. □

Corollary 4.28. *Every $a \in A$ can be uniquely written as*

$$a = \sum_{i=0}^{\infty} \rho(\overline{a}_i)p^i$$

for some sequence $\overline{a}_i \in A/pA$.

Proof of Theorem 4.22. Part 2): Consider the multiplicative retractions $B_i \to A_i$ given by the Lemma 4.26. We have the diagram

$$\begin{array}{ccc} B_1 & \xrightarrow{\overline{\varphi}} & B_2 \\ \downarrow{\scriptstyle \rho_1} & & \downarrow{\scriptstyle \rho_2} \\ A_1 & \longrightarrow & A_2 \end{array}$$

which must be commutative since the property explained in the Lemma 4.26 is kept by the map $\overline{\varphi}$. So the only possibility for such a lift of $\overline{\varphi}$ is

$$\sum_{i=0}^{\infty} \rho_1(\overline{a}_i)p^i \mapsto \sum_{i=0}^{\infty} \rho_2(\overline{a}_i)p^i$$

since for finite quotients A/p^iA the image is given and $\cap p^iA$ is zero because it is a p-strict ring. What we still have to show is that it is a homomorphism.

We will show this by a universal construction: Consider families of variables $\{x_i\}_{i\in\mathbb{N}}$ and $\{y_i\}_{i\in\mathbb{N}}$. Define $x := \sum x_ip^i$ and $y := y_ip^i \in \mathbb{Z}(\{x_i, y_i\}, p^{-\infty})$. Note that $x_i = \rho(x_i)$ and $y_i = \rho(y_i)$ so there exist $\overline{s_j} \in \mathbb{F}_p[\{x_i, y_i \mid i \in \mathbb{N}\}, p^{-\infty}]$ such that

$$x + y = \sum_{i/=0}^{\infty} \rho(\overline{s_i})p^i$$

and similarly for the product $x \cdot y$. Therefore, given $a, b \in A_1$ there exists a homomorphism $\mathbb{Z}(\{x_i, y_i\}, p^{-\infty}) \to A_1$ such that $x \mapsto a$ and $y \mapsto b$: If $a = \sum \rho_1(\overline{a_i})p^i$, $b = \sum \rho_1(\overline{b_i})p^i$ then let $x_i \mapsto \rho(\overline{a_i})$ and $y_i \mapsto \rho(\overline{b_i})$ so by completion we indeed get such a homomorphism. Hence, by substitution

$$a + b = \sum \rho_1\big(\overline{s_j}(\{\overline{a_i}\}, \{\overline{b_i}\}\big)p^j$$

Now, we need to check that $\varphi(a+b) = \varphi(a) + \varphi(b)$. Let's write them all up by "power series":

$$\varphi(a) = \sum \rho_2(\overline{\varphi}(\overline{a_i}))p^i$$

$$\varphi(b) = \sum \rho_2(\overline{\varphi}(\overline{b_i}))p^i$$

$$\varphi(a+b) = \sum \rho_2\Big(\overline{\varphi}\big(\overline{s_j}(\{\overline{a_i}\},\{\overline{b_i}\})\big)\Big)p^j = \sum \rho_2\Big(\overline{s_j}\big(\{\overline{\varphi}(\overline{a_i})\},\{\overline{\varphi}(\overline{b_i})\}\big)\Big)p^j$$

because $\overline{\varphi}$ is a ring homomorphism. So we got additivity. Similar argument works, for multiplication.

Part 1): Observe that every perfect ring of charactersitic p is a quotient of some $\mathbb{F}_p[\{x_\alpha^{p^{-\alpha}}\}_{\alpha\in\Lambda}]$. This is the residue ring of $\mathbb{Z}[\{x_\alpha\}_{\alpha\in\Lambda}, p^\infty]$ so it is enough to prove that:

Lemma 4.29. *Assume given a surjective homomorphism $\overline{\varphi} : B_1 \to B_2$ of perfect rings if characteristic $p > 0$. If there exists a strict p-ring A_1 such that $B_1 \cong A_1/pA_1$ then there exists a strict p-ring A_2 such that $B_2 \cong A_2/pA_2$ such that the following diagram commutes:*

$$\begin{array}{ccc} B_1 & \xrightarrow{\overline{\varphi}} & B_2 \\ {\scriptstyle\rho_1}\downarrow & & \downarrow{\scriptstyle\rho_2} \\ A_1 & \longrightarrow & A_2 \end{array}$$

Proof. Consider

$$I = \left\{ \sum_{i=0}^{\infty} \rho_1(\overline{c_i})p^i \mid c_i \in \operatorname{Ker}(\overline{\varphi}) \right\}$$

where $\rho_1 : B_1 \to A_1$ is the multiplicative retraction. One can check (as in the proof of the second part) that $I \subseteq A_1$ is an ideal, using that $\operatorname{Ker}(\overline{\varphi})$ is an ideal. Define $A_2 := A_1/I$. Now, $A_2/pA_2 \overset{\cong}{\to} B_2$ since $\overline{\varphi}$ is surjective and we defined I in that way. Also ρ_1 induces a multiplicative retraction $\rho_2 : B_2 \to A_1$. Moreover, the filtration $\{p^iA_1\}$ induces a filtration $\{p^iA_2\}$ in the A_2. Therefore, we may write every $a_2 \in A_2$

$$a_2 = \sum_{i=0}^{\infty} \rho(\overline{a}_i)p^i \qquad \overline{a_i} \in B_2$$

hence $A_2$is a strict p-ring. ☐

Theorem 4.22 follows. ☐

Remark 4.30. *Witt vectors:* Assume that $\Bbbk$ is a perfect field and let A be a strict p-ring with residue field $\Bbbk$. Consider the map $A \to \Bbbk^{\mathbb{N}}$ bringing every element to (more or less) the sequence of "coefficients" of its power series:

$$\sum \rho(\overline{a_i})p^i \mapsto p^i\overline{a_i}$$

set theoretically, this is a bijection. So we can define a ring structure on $\Bbbk^{\mathbb{N}}$ making it a strict p-ring with residue field $\Bbbk$. (not proven) One can also show: in $\Bbbk^{\mathbb{N}}$ addition, multiplication are given by polynomials in $\mathbb{Z}[\{x_i\},\{y_i\}]$.

5 Depth

Definition 5.1. Let A be a ring, M and A-module, and $x = (x_1, \ldots, x_n) \in A^n$ is an *M-regular sequence* if

1. x_i is not a zero-divisor on $M/(x_1, \ldots, x_{i-1})M$ for all i.
2. $M/(x_1, \ldots, x_n)M \neq 0$

Remark 5.2. If $M \neq 0$ is finitely generated and A is local with maximal ideal $P \ni x_1, \ldots, x_n$ then 2) is automatic by Nakayama's lemma. Conversely, by 2) we have $x_i \in P$ for all i.

Remark 5.3. Let A be a Noetherian, local ring and M a finitely generated module. If $\{x_1, \ldots, x_n\}$ is a regular sequence for M then every permutation of x_i's is too. (This is a not really hard exercise, it is enough to prove it for transpositions.)

Definition 5.4. Let A be a Noetherian ring and $M \neq 0$ a finitely generated A-module. If $I \subseteq A$ is an ideal then

$$I-\mathrm{depth}(M) := \max \text{length of an } M\text{-regular sequence contained in } A$$

If A is local, $\mathrm{depth}(M) := P-\mathrm{depth}(M)$ where P is the maximal ideal.

5.1 Reminder: Associated primes

Assumptions: In the following, A will be a Noetherian ring and all modules are assumed to be finitely generated.

Definition 5.5. A $P \subseteq A$ is an *associated prime* ideal of M if there exists $m \in M$ such that

$$P = \mathrm{Ann}(m) = \{x \in A \mid xm = 0\}$$

The set of associated primes is denoted by $\mathrm{Ass}(M)$.

Proposition 5.6. *If $M \neq 0$ then a maximal element of $\{\mathrm{ann}(m) \mid m \in M\backslash\{0\}\}$ is a prime ideal. In particular, $\mathrm{Ass}(M) \neq \emptyset$.*

Proof. If $P = \mathrm{Ann}(m)$ is maximal then take $xy \in P$. Assume that $y \notin P$ then $ym \neq 0$ but $P \subseteq \mathrm{Ann}(ym)$ so $P = \mathrm{Ann}(ym)$ by maximality. Therefore, $x \in P$ since $xym = 0$. ☐

Proposition 5.7. *If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is an exact sequence of A-modules then*

$$\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

(This is an easy exercise.)

Corollary 5.8. *If M is a finitely generated A-module then there exists a finite filtration $0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$ such that $M_i/M_{i+1} \cong A/P_i$ for some $P_i \subseteq A$ prime ideal. Moreover, $\mathrm{Ass}(M) \subseteq \{P_1, \ldots, P_n\}$. In particular $|\mathrm{Ass}(M)| < \infty$.*

Notation: $\mathrm{Supp}(M) := \{P \subseteq A \text{ prime} \mid P \supseteq \mathrm{Ann}(M)\}$

Proposition 5.9. (without proof) *Clearly, $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$ but these sets also have the same minimal elements.*

Proposition 5.10. *If I is an ideal consisting of zero-divisors on M then there exists an associated prime $P \in \mathrm{Ass}(M)$ such that $I \subseteq P$. Consequently,*

$$\bigcup_{p \in \mathrm{Ass}(M)} P = \{\mathrm{zero} - \mathrm{divisors}\} \cup \{0\}$$

Proof. For all $x \in I$ there exists $m \in M$ such that $x \in \mathrm{Ann}(m)$ implies $x \in P$ for some $P \in \mathrm{Ass}(M)$. But then $I \subseteq \bigcup\{P \mid P \in \mathrm{Ass}(M)\}$ where $|\mathrm{Ass}(M)| < \infty$ so $I \subseteq P$ for some of the P's. ☐

Seventh Lecture, 24th of February
[I was missing from this lecture, it is copied from Attila's notes. The statements are listed without proof.]

Remark 5.11. Reminder on Ext: It is a functor: for fixed $M \in A-\text{Mod}$ one has

$$A-\text{Mod} \ni N \to \text{Ext}^i_A(M,N) \in A-\text{Mod}$$

a covariant functor that takes short exact sequences into long exact sequences. It can be computed by projective resolutions of M. Similarly, for fixed $N \in A-\text{Mod}$ one has

$$A-\text{Mod} \ni M \to \text{Ext}^i_A(M,N) \in A-\text{Mod}$$

is a contravariant functor.

In particular, the multiplication by an $x \in A$ map $M \xrightarrow{\cdot x} M$ gives a map $\text{Ext}^i_A(M,N) \to \text{Ext}^i_A(M,N)$.

Proposition 5.12. *If A is a Noetherian local ring with residue field $\Bbbk$,*

$$\text{depth}(M) = \min\{i \mid \text{Ext}^i_A(\Bbbk, M) \neq 0\}$$

for all modules M finitely generated over A. Moreover, all maximal M-regular sequences have length $\text{depth}(M)$.

5.2 Cohen-Macauley rings

Lemma 5.13. *Let A be a Noetherian local ring, M a finitely generated module, $x_1, \dots, x_i$ an M-regular sequence. Then this sequence extends to an M-regular sequence $x_1, \dots, x_i, x_{i+1}$ if and only if* $\text{Hom}_A(\Bbbk, M_i) = 0$ *where $M_i = M/(x_1, \dots, x_i)M$.*

Corollary 5.14. *Let A be a Noetherian local ring and M a finitely generated module. If $x_1, \dots, x_r$ is a regular sequence for M then* $\text{depth}(M/(x_1, \dots, x_r)M) = \text{depth}(M) - r$.

Proposition 5.15. *Let A be a Noetherian local ring and M a finitely generated module. If $Q \in \text{Ass}(M)$ then* $\text{depth}(M) \leq \dim A/Q$.

Definition 5.16. $\dim M := \dim \big(A/\text{Ann}(M)\big)$

Corollary 5.17. *Let A be a Noetherian local ring and M a finitely generated module. Then* $\text{depth}(M) \leq \dim M$.

Definition 5.18. Let A be a Noetherian local ring and M a finitely generated module. Then M is called *Cohen-Macauley* (CM) if $\text{depth}(M) = \dim M$. Similarly, a ring A is called Cohen Macauley if $\text{depth}(A) = \dim A$. More generally, a Noetherian (not necessarily local ring) A is Cohen-Macauley, if A_Q is Cohen-Macauley for all maximal ideals $Q \lhd A$.

Remark 5.19. We will see later that if a local ring is CM then its localizations are also CM hence the definition is unambiguous and we can also say prime ideals in the above definition.

Proposition 5.20. *If A is a Noetherian local ring, M is a finitely generated CM-module, $Q \in \text{Ass}(M)$ then* $\dim A/Q = \dim M = \text{depth} M$. *Moreover, all $Q \in \text{Ass}(M)$ are minimal prime ideals in A containing* $\text{Ann}(M)$.

Proposition 5.21. *Let A be a Noetherian local ring, M a finitely generated module, $x_1, \dots, x_r$ an M-regular sequence. Then $M_r = M/(x_1, \dots, x_r)$ is CM if and only if M is CM.*

Example 5.22. For CM rings:

1. A regular local ring is CM.

2. A Noetherian ring of dimension zero is CM. (Indeed, then every localization has a nilpotent maximal ideal.)

3. A Noetherian integral domain of dimension 1 is CM. (Indeed, then the maximal ideals consists of non-zerodivisors hence $1 \leq \text{depth}(A) \leq \dim(A) \leq 1$.)

4. We will see later that if $\Bbbk$ is a field then $\Bbbk[x_1, \ldots, x_n]_P$ is a regular local ring for every prime hence $\Bbbk[x_1, \ldots, x_n]$ is CM.

5. One can show that if A is CM then $A[x_1, \ldots, x_n]$ is also CM hence most interesting CM rings are of the form $A/(x_1, \ldots, x_r)$ where A is regular local and or a polynomial ring and $x_1, \ldots, x_r$ is a regular sequence.

6. Counterexample for CM property: $A = \Bbbk[x, y]/(xy, y^2)$ is of dimension 1 and it is not CM. (Indeed, the maximal ideal in $A_{(x,y)}$ consists of zerodivisors hence it has depth zero but dimension 1 so not CM.

Definition 5.23. A Noetherian ring A satisfies the unmixedness theorem if for all ideals $I = (x_1, \ldots, x_r)$ of height r for any r, all prime ideals $P \in \text{Ass}(A/I)$ are minimal. (Here, $\text{ht}(I) = \min\{\text{ht}P \mid P \supseteq I\}$.

Eighth Lecture, 3rd of March

Definition 5.24. Let A be Noetherian and $I \subsetneq A$ be an ideal. The ideal is called *unmixed* if all associated primes of I are minimal.

A satisfies the unmixedness theorem if all ideals $I = (x_1, \ldots, x_r)$ of height r are unmixed, for all $r \geq 0$.

Theorem 5.25. *A Noetherian ring is Cohen-Macauley (CM) if and only if the unmixedness theorem holds in A.*

Corollary 5.26. (Macauley, 1916) *The unmixedness theorem holds in* $\Bbbk[t_1, \ldots, t_n]$.

Corollary 5.27. (Cohen, 1946) *The unmixedness theorem holds in a regular local ring.*

Lemma 5.28. (Lemma 0) *If A is a Cohen-Macauley ring then A_Q is also Cohen-Macauley for all prime ideals $Q \subseteq A$. Moreover,* $\text{depth}(A_Q) = Q{-}\text{depth}(A)$.

Proof. By the assumptions, we know that

$$\dim(A_Q) \geq \text{depth}(A_Q) \geq Q{-}\text{depth}(A)$$

so we have to prove that $\dim(A_Q) \leq Q{-}\text{depth}(A)$. We will do it by induction on $Q{-}\text{depth}(A)$: if it is zero then all elements of Q are zero-divisors so $Q \subseteq Q' \in \text{Ass}(A)$. But A is Cohen-Macauley so Q' is minimal hence $Q = Q'$. Therefore, A_Q has dimension zero.

Now, assume that $Q{-}\text{depth}(A) > 0$ and pick an $x \in Q$ which is not a zero-divisor. Set $A_1 := A/(x)$. We know that

$$Q{-}\text{depth}(A_1) \leq Q{-}\text{depth}(A) - 1$$

Since $A_1 \otimes_A A_Q \cong A_Q/xA_Q$ which is a nonzero ring as x is not a unit, we get $\dim A_Q/xA_Q = Q{-}\text{depth}(A_1)$ by induction. By Proposition 5.21: $\dim(A_1 \otimes_A A_Q) = \dim(A_Q) - 1$. Therefore,

$$Q - \text{depth}(A) \geq Q - \text{depth}(A_1) + 1 = \dim(A_1 \otimes_A A_Q) + 1 = \dim(A_Q)$$

and that proves the other inequality. □

Lemma 5.29. (Lemma 1) *Let A be a Cohen-Macauley local ring, $Q \subseteq A$ be a prime ideal with* $\text{ht}(Q) = r$. *Assume that Q is minimal above $(x_1, \ldots, x_r)$. Then $x_1, \ldots, x_r$ is a regular sequence.*

Remark 5.30. Locality is not needed in the proof, but the “permutation-invariance” of the regular sequence is only true in local rings so it is better to assume for a clearer statement.

Proof. By the previous lemma, A_Q is Cohen-Macauley so we may assume that Q is the maximal ideal of A. It is enough to show that x_1 is a non-zerodivisor. Then we can use induction on $A/(x_1)$ where the height of the image of Q is lower so we can find a regular sequence (by induction) that can be pulled back and extended by x_1.

If it is a zero-divisor then there exists a $Q' \in \operatorname{Ass}(A)$ such that $x_1 \in Q'$. We know that, A Cohen-Macauley so $\dim(A) = \dim(A/Q')$. But in A/Q' the ideal Q/Q' is minimal above the images of $x_2, \ldots, x_r$ so $\dim(A/Q') \leq r - 1$ by the Hauptidealsatz. □

Lemma 5.31. (Lemma 2) *Let A be a Noetherian ring and $P \subseteq A$ a prime ideal with $\operatorname{ht}(P) = r$. Then there exist $x_1, \ldots, x_r \in P$ such that $\operatorname{ht}\big((x_1, \ldots, x_i)\big) = i$ for all $1 \leq i \leq r$.*

Remark 5.32. Recall $\operatorname{ht}(I) = \min\{\operatorname{ht}(P) \mid P \supseteq I\}$.

Proof. We proceed by induction on i: if $i = 1$ then choose an $x_1 \in P$ that is not contained in any of the minimal prime ideals. Such an x_1 exists by the Prime Avoidance Lemma 1.11. Therefore, $\operatorname{ht}\big((x_1)\big) = 1$ by the Hauptidealsatz (it has height at most 1 but it is not contained in a minimal prime).

Assume that we have already constructed $x_1, \ldots, x_{i-1}$. By the Prime Avoidance Lemma 1.11, there must exists an $x_i \in P$ not contained in any of the minimal primes above (x_1), (x_1, x_2), …, $(x_1, x_2, \ldots, x_{i-1})$ since these have height at most $i - 1$ (by induction) hence they cannot contain P.

By the Hauptidealsatz we get $\operatorname{ht}\big((x_1, \ldots, x_i)\big) \leq i$, but, in fact, equality holds because a minimal prime above $(x_1, \ldots, x_i)$ is not minimal above $(x_1, \ldots, x_{i-1})$ by our choice. □

Proof of Theorem 5.25. $\Rightarrow$: Let $I = (x_1, \ldots, x_r)$ with $\operatorname{ht}(I) = r$. We have to show that all elements of $\operatorname{Ass}(A/I)$ are minimal. Assume that $P \in \operatorname{Ass}(A/I)$ is not minimal. By localizing at P we may assume that P is maximal. Notice the by Lemma 0, 5.28 we did not lose the Cohen-Macauley property and the set of associated primes behaves well under localization. If $Q \subseteq P$ is a minimal associated prime of $I = (x_1, \ldots, x_r)$ then it is a minimal prime above I because the minimal associated primes are minimal prime ideals (see Proposition 5.9). Therefore, $\operatorname{ht}(Q) = r$. Then we can apply Lemma 1, 5.29, implying that $x_1, \ldots, x_r$ is a regular sequence. So A/I is Cohen-Macauley by Proposition 5.21 so all associated primes are minimal.

Conversely, assume that A is Noetherian and the unmixedness theorem holds. Assume, moreover, that $P \subseteq A$ is a prime ideal with $\operatorname{ht}(P) = r$. Now, choose $x_1, \ldots, x_r \in P$ as in Lemma 2, 5.31. The unmixedness theorem implies that all associated primes of $A/(x_1, \ldots, x_i)$ are of height i. Therefore, they do not contain x_{i+1} by the higher height of $(x_1, \ldots, x_{i+1})$. This means that x_{i+1} is not a zero-divisor modulo $(x_1, \ldots, x_i)$ by Proposition 5.10, hence $x_1, \ldots, x_r$ is a regular sequence and $\operatorname{depth}(A_P) \geq r = \dim(A_P)$. This proves that A_P is Cohen-Macauley for all prime ideals P so we are done by definition. □

Remark 5.33. Every quotient of a Cohen-Macauley ring is *catenary*, i.e. if $P \subseteq Q$ are prime ideals then all chains of prime ideals between P and Q have the same length. (For this, it is enough to prove that Q being minimal over P have $\dim Q = \dim P + 1$. One can use Lemma 1, 5.29 to prove this.)

6 Homological dimension

Definition 6.1. If A is a ring, M is an A-module then the *projective dimension* of M is

$$\operatorname{pd}(M) := \inf\big\{i \mid \exists 0 \to P_i \to \cdots \to P_0 \to M \to 0,\ P_j \text{ is projective for all } j \leq i\big\}$$

Similarly,

$$\operatorname{gldim}(A) := \sup\{\operatorname{pd}(M) \mid M \text{ is an } A\text{-module}\}$$

where these can be infinite too.

Proposition 6.2. *The following are equivalent for an A-module M:*

1. $\mathrm{pd}(M) \leq d$,
2. $\mathrm{Ext}^i(M, N) = 0$ *for all A-modules N and $i > d$,*
3. $\mathrm{Ext}^{d+1}(M, N) = 0$ *for all A-modules N,*
4. *If* $0 \to M_d \to P_{d-1} \to \cdots \to P_0 \to M \to 0$ *is exact and P_i are projective then M_d is projective.*

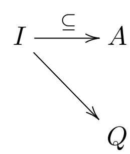
Proof. (Sketch) The implications 4) ⇒ 1) ⇒ 2) ⇒ 3) are straightforward by the definition of projective cover and the Ext-groups. For 3) ⇒ 4): Recall that if P is projective then $\mathrm{Ext}^i(P, N) = 0$ for $i > 0$. Using the assumption $\mathrm{Ext}^{d+1}(M, N) = 0$ we get that $\mathrm{Ext}^1(M_d, N) = 0$ for all N by dimension-shift. Therefore, M_d is projective since the functor $\mathrm{Hom}(M_d, .)$ is then exact. □

Lemma 6.3. *Let A be a ring and M, N be A-modules. Then* $\mathrm{Ext}^i(M, N) = 0$ *for all M, N if and only if* $\mathrm{Ext}^i(M, N) = 0$ *for all N and all finitely generated M.*

Corollary 6.4. $\mathrm{gldim}(A) = \sup\{\mathrm{pd}(M) \mid M$ *is a finitely generated A-module*$\}$.

Remark 6.5. Recall that $\mathrm{Ext}^i(M, N)$ can be calculated by taking injective coresolution $0 \to N \to Q_0 \to Q_1 \to \dots$.

Another important fact is Baer's criterion saying that an A-module Q is injective if and only if every diagram



can be completed in a commutative way with a morphism $A \to Q$.

Proof of Lemma 6.3. The implication ⇒ is trivial. So for ⇐ take an injective coresolution $0 \to N \to Q_0 \to Q_1 \to \dots$ where we know that $\mathrm{Ext}^j(M, Q_j) = 0$ for all modules M and for all $j > 0$. Now, we truncate the coresolution:

$$0 \to N \to Q_0 \to Q_1 \to \cdots \to Q_{i-2} \to N_{i-1} \to 0$$

then − as in the previous proof − we have $\mathrm{Ext}^i(M, N) \cong \mathrm{Ext}^1(M, N_{i-1})$. Then $\mathrm{Ext}^1(M, N_{i-1}) = 0$ for all M. This is equivalent to saying $\mathrm{Hom}(., N_{i-1})$ is an exact functor which is equivalent to N_{i-1} being injective. By Baer's criterion, this is equivalent to $\mathrm{Ext}^1(A/I, N_{i-1}) = 0$ using the short exact sequence $0 \to I \to A \to A/I \to 0$. This latter is equivalent to saying that $\mathrm{Ext}^i(A/I, N) = 0$. □

Proposition 6.6. *Let A be a Noetherian local ring with maximal ideal P and M a finitely generated A-module. Then* $\mathrm{pd}(M) \leq d$ *if and only if* $\mathrm{Tor}_{d+1}(M, \Bbbk) = 0$ *where* $\Bbbk = A/P$.

Corollary 6.7. *If A is a Noetherian local ring with residue field $\Bbbk$ then* $\mathrm{gldim}(A) = \mathrm{pd}(\Bbbk)$.

Proof of Corollary 6.7. This follows from the previous three propositions: the global dimension can be checked on finitely generated (first component) ones, so it is enough to check their pd. That is equivalent to $\mathrm{Tor}_{d+1}(M, \Bbbk) = 0$ for all M. However, this latter is clearly equivalent to $\mathrm{pd}(\Bbbk) \leq d$ by the symmetry of the Tor functor. □

Remark 6.8. Recall that $\mathrm{Tor}_i(M, N) = H_i(P_\bullet \otimes_A N)$ where $P_\bullet \to M$ is a projective resolution. This way from a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ we get a long exact sequence of Tor's.

Observe that if P is projective then $\mathrm{Tor}_i(P, N) = 0$ for all N and $i > 0$ by the above definition.

Proposition 6.9. *If $x \in A$ then* $\mathrm{Tor}_1\big(A/(x)\big) \cong \{m \in M \mid xm = 0\}$ *is called the x-torsion of M.*

Proof. Consider the exact sequence $0 \to A \to A \to A/(x) \to 0$ where the A's are clearly projective. This means that

$$0 = \mathrm{Tor}_1(A, M) \to \mathrm{Tor}_1\big(A/(x), M\big) \to M \to M \to M/(x) \to 0$$

So the statement follows. □

Proof of Proposition 6.6. The implication $\Rightarrow$ is clear. For $\Leftarrow$ we use induction on d where the $d = 0$ case is the hard one. We have to prove that if $\mathrm{Tor}_1(M, \Bbbk) = 0$ then M is projective. So take a basis of $M/PM \cong M \otimes_A \Bbbk$. Now, lift this basis to a set of elements $m_1, \dots, m_r \in M$. Consider the short exact sequence

$$0 \qquad N \longrightarrow A^r \xrightarrow{f} M \longrightarrow 0$$

where $f : (a_1, \dots, a_r) \mapsto \sum a_i m_i$. Now tensor it with $\Bbbk$:

$$0 = \mathrm{Tor}_1(M, \Bbbk) \longrightarrow N \otimes_A \Bbbk \longrightarrow \Bbbk^r \xrightarrow{f} M \otimes_A \Bbbk \longrightarrow 0$$

where –by construction – $\Bbbk^r \to M \otimes_A \Bbbk$ is an isomorphism. Therefore $N \otimes_A \Bbbk \cong N/PN = 0$ so $N = 0$ by Nakayama's lemma. Hence M is free, which is even stronger then the $d = 0$ step.

For the induction step assume that $d > 0$ and consider the same exact sequence:

$$0 \qquad N \longrightarrow A^r \xrightarrow{f} M \longrightarrow 0$$

By dimension shift (i.e. A^r is projective in this sequence) we get that $\mathrm{Tor}_d(N, \Bbbk) \cong \mathrm{Tor}_{d+1}(M; \Bbbk)$ so $\mathrm{pd}(M) \leq \mathrm{pd}(N) + 1$. This completes the induction noting that N is also finitely generated by the Noetherian property of the ring. □

Plan (for next time) We will prove a theorem of Serre: If A is a Noetherian local ring. Then it is regular if and only if its global dimension is finite. For this theorem we will use Theorem 6.6 i.e. it is enough to check the pd of $\Bbbk$. Afterward, we will prove the theorem of Auslander and Buchsbaum: If A is a Noetherian local rings and M is a finitely generated A-module then $\mathrm{depth}(A) = \mathrm{depth}(M) + \mathrm{pd}(M)$.

Ninth Lecture, 10th of March

Recall the following corollary of Nakayama's Lemma:

Theorem 6.10. *Over a Noetherian local ring, finitely generated projective modules are free.*

Theorem 6.11. (Auslander-Buchsbaum) *If A is a Noetherian local ring and M is a finitely generated A-module with* $\mathrm{pd}(M) < \infty$ *then* $\mathrm{depth}(A) = \mathrm{depth}(M) + \mathrm{pd}(M)$.

Remark 6.12. As we will see later, in the regular case, $\mathrm{depth}(A) = \mathrm{gldim}(A)$ hence $\mathrm{depth}(M) = \mathrm{gldim}(A) - \mathrm{pd}(M)$. This is the reason why depth is sometimes called homological codimension. However, this makes sense only when the ring is regular.

Proposition 6.13. *Let A be any (commutative, unital) ring, $x \in A$ be a nonzero divisor and M is an $A/(x)$-module such that* $\mathrm{pd}_{A/(x)}(M) < \infty$. *Then* $\mathrm{pd}_A(M) = \mathrm{pd}_{A/(x)}(M) + 1$.

Proof. We proceed by induction on $\mathrm{pd}_{A/(x)}(M)$. If it is zero then M is a projective over $A/(x)$. Since x is a non-zerodivisor, we have a short exact sequence

$$0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow A/(x) \longrightarrow 0$$

This is a projective resolution of $A/(x)$ over A hence $\mathrm{pd}_A(A/(x)) \leq 1$. But $\mathrm{pd}_A(A/(x)) \neq 0$ because if it were zero then $A/(x)$ would be projective over A so it is a direct summand of a free A-module but that is impossible since x is a zero-divisor ring element on the module $A/(x)$ but it is a non-zerodivisor on the module A so on the module A^α as well. Hence, $\mathrm{pd}_A(A/(x)) = 1$ so $\mathrm{pd}_A(F) = 1$ for any free $A/(x)$-module F. Therefore, $\mathrm{pd}_A(M) = 1$ as M is a direct summand of a free $A/(x)$-module.

Now, for the inductive step, take an exact sequence of $A/(x)$-modules

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$$

where P is projective over $A/(x)$. Then by turning to homologies, we get two exact sequences (one by considering the above as an exact sequence of A-modules, the other by considering them as $A/(x)$-modules):

$$\mathrm{Ext}^i(P,N) \longrightarrow \mathrm{Ext}^i(K,N) \longrightarrow \mathrm{Ext}^{i+1}(M,N) \longrightarrow \mathrm{Ext}^{i+1}(P,N)$$

Here, over $A/(x)$ we have $\mathrm{Ext}^i(P,N) = 0$ for all $i > 0$ hence $\mathrm{Ext}^i_{A/(x)}(K,N) \cong \mathrm{Ext}^{i+1}_{A/(x)}(M,N)$ for all $i > 0$.

While, over A we have $\mathrm{Ext}^i(P,N) = 0$ for all $i > 1$ by $\mathrm{pd}_A(P) = 1$ (see the first step of the proof). Hence $\mathrm{Ext}^i_A(K,N) \cong \mathrm{Ext}^{i+1}_A(M,N)$ for all $i > 1$. Using the first equation, we get

$$\mathrm{pd}_{A/(x)}(M) = \mathrm{pd}_{A/(x)}(K) + 1 = \mathrm{pd}_A(K) \tag{6.1}$$

by the induction hypothesis. Therefore, by the equation interpreted over A, we get

$$\mathrm{pd}_A(M) = \mathrm{pd}_A(K) + 1$$

provided that $\mathrm{pd}_A(M) > 1$ since we only have the isomorphism in second equation for $i > 1$. Therefore, putting together the two equations, we proved the proposition for the case $\mathrm{pd}_A(M) > 1$.

So now we only have to show that $\mathrm{pd}_A(M) = 1$ and $\mathrm{pd}_{A/(x)}(M) > 0$ is impossible since all the other cases are handles by the above induction. So suppose indirectly that $\mathrm{pd}_A(M) = 1$ and consider again the exact sequence of Ext's:

$$\mathrm{Ext}^i(P,N) \longrightarrow \mathrm{Ext}^i(K,N) \longrightarrow \mathrm{Ext}^{i+1}(M,N) \longrightarrow \mathrm{Ext}^{i+1}(P,N)$$

but now the beginning of it. By the projectivity of P over $A/(x)$ we have

$$\mathrm{Ext}^i_A(P,N) = 0 \qquad (i = 2,3)$$

and $\mathrm{Ext}^3_A(M,N) = 0$ by $\mathrm{pd}_A(M) = 1$. Then, by the exact sequence we get $\mathrm{Ext}^2_A(K,N) = 0$ for all N, therefore $\mathrm{pd}_A(K) \leq 1$ where $\mathrm{pd}_A(K) = \mathrm{pd}_{A/(x)}(M)$ as we have seen in equation 6.1 (where no assumption like $\mathrm{pd}_A(M) > 1$ was used). So – by assuming $\mathrm{pd}_{A/(x)}(M) > 0$ – we reduced the case for $\mathrm{pd}_A(M) = \mathrm{pd}_{A/(x)}(M) = 1$.

So now choose an exact sequence of A-modules

$$0 \longrightarrow C \longrightarrow F \longrightarrow M \longrightarrow 0$$

where F is free. Then – since $\mathrm{pd}_A(M) = 1$ – we get that C is projective by Proposition 6.2. So this is, in fact, a projective resolution of M. Tensor this sequence with $A/(x)$ yielding

$$0 = \mathrm{Tor}^A_1(F, A/(x)) \longrightarrow \mathrm{Tor}^A_1(M, A/(x)) \longrightarrow C/xC \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0$$

where the first must be zero because F is free, moreover, $M/xM = M$ since M is an $A/(x)$-module hence $xM = 0$. Therefore, by $\mathrm{pd}_{A/(x)}(M) = 1 \leq 2$, we get $\mathrm{Tor}_1(M, A/(x))$ is projective over $A/(x)$ by Proposition 6.2 since C/xC and F/xF are already projective over $A/(x)$. However, in Proposition 6.9, we have seen the characterization of the Tor groups as $\mathrm{Tor}_1(M, A/(x)) = \{m \in M \mid xm = 0\}$ which is M in our case. So we got that M is projective what is a contradiction. □

Corollary 6.14. *If A is a Noetherian local ring, $x \in A$ is a non-unit non-zerodivisor on A and* $\operatorname{gldim}(A/(x)) < \infty$ *then* $\operatorname{gldim}(A) = \operatorname{gldim}(A/(x)) + 1$.

Proof. Apply the above proposition with $M = \Bbbk$ so – by Corollary 6.7 – we are done. ☐

Proposition 6.15. *Let A be a ring, M be an A-module and x a non-zerodivisor on M. Then*

$$\operatorname{pd}_A(M) \geq \operatorname{pd}_{A/(x)}(M/xM)$$

If, moreover, A is a Noetherian local ring, M is finitely generated and $x \in A$ is a non-unit non-zerodivisor on A then there is equality above.

Proof. We may assume that $d := \operatorname{pd}_A(M) < \infty$. We will do induction on d: For $d = 0$, M is projective over A so M/xM is projective over $A/(x)$. For $d > 0$, choose an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

with F being free. Then – as we have already seen in a previous argument – $\operatorname{pd}_A(K) = d - 1$. Therefore, $\operatorname{pd}_{A/(x)}(K/xK) \leq d - 1$ by induction. So apply $\otimes_A A/(x)$ on the sequence above:

$$\operatorname{Tor}_1^A(M, A/(x)) \longrightarrow K/xK \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0$$

where $\operatorname{Tor}_1^A(M, A/(x)) = \{m \in M \mid xm = 0\} = 0$ by Proposition 6.9. Therefore, $\operatorname{pd}_{A/(x)}(M/xM) = \operatorname{pd}_{A/(x)}(K/xK) + 1 \leq d$.

Now, assume that A is Noetherian, local, M is finitely generated and x is a non-unit. We prove by induction on $n = \operatorname{pd}_{A/(x)}(M/xM)$. If $n = 0$ then M/xM is projective over $A/(x)$ however then it is also free by Theorem 6.10. We claim that if M/xM is free over $A/(x)$ then M is free over A. This is enough to prove case $n = 0$ since then there are zeros on both sides of the equation in the statement.

So let $m_1, \ldots, m_r$ be a free $A/(x)$-generating system of M/xM so by Nakayama's lemma, it is also a generating system over A since $x \in P$ for the maximal ideal P. Now, assume that $\sum a_i m_i = 0$ for some $a_i \in A$. We know that $a_i \in (x)$ since module (x) there is no nontrivial relation. So there exists $a_i' \in A$ such that $a_i' \cdot x = a_i$. However, we know that x is a non-zerodivisor on M so $\sum a_i' \cdot m_i = 0$ since we can cancel x. Now, we can continue this process "forever" getting the sequence of equations

$$0 = \sum a_i' m_i = \sum a_i'' m_i = \ldots$$

where $x \cdot a_i'' = a_i'$ and so on. Therefore, $a_i \in \cap_n (x^n) \subseteq \cap_n P^n$ which is zero by Krull's Intersection Theorem, Corollary 3.18.

For the inductive step, assume that $n > 0$ and consider the exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

where F is free. We can tensor it with $A/(x)$ getting the exact sequence

$$\operatorname{Tor}_1^A(M, A/(x)) \longrightarrow K/xK \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0$$

where $\operatorname{Tor}_1^A(M, A/(x))$ is zero again by Proposition 6.9 and F/xF is free over $A/(x)$. So, if we interpret this sequence over $A/(x)$ then by $n = \operatorname{pd}_{A/(x)}(M/xM) > 0$ we get

$$\operatorname{pd}_{A/(x)}(M/xM) = \operatorname{pd}_{A/(x)}(K/xK) + 1$$

Moreover, if we interpret it over A then we get $\operatorname{pd}_A(M) = \operatorname{pd}_A(K) + 1$. By the first part of the theorem, we have $\operatorname{pd}_A(M) \geq n > 0$ hence, we are done by the induction. ☐

Proof of Theorem 6.11. : We proceed by a double induction on $\mathrm{depth}(A)$ and $\mathrm{depth}(M)$. As a first step, we prove that M is free provided that $\mathrm{depth}(A) = 0$. By this, $\mathrm{depth}(M) = 0$ follows because if all of the elements of the ideals of A are zero-divisors on A then they are zero-divisors on a free module as well.

So, assume on the contrary that M is not free hence it is not projective since A is local (see Theorem 6.10). So $0 < \mathrm{pd}(M) < \infty$ and we can choose a projective resolution of minimal length:

$$0 \longrightarrow P_d \longrightarrow P_{d-1} \xrightarrow{\alpha} \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

where all the P_i's are finitely generated by Lemma 6.3. Here, we can take $K := \mathrm{Ker}\alpha$ which has $\mathrm{pd}(K) = 1$. Let us denote the maximal ideal of A by P and let $\Bbbk := A/P$. Pick a $\Bbbk$-basis of K/PK $\overline{u_1}, \ldots, \overline{u_m}$ and lift it to $u_1, \ldots, u_m \in K$. It also generates K by Nakayama's lemma. So let F be a free A-module of rank m and take the short exact sequence

$$0 \longrightarrow \tilde{P} \longrightarrow F \xrightarrow{f} K \longrightarrow 0$$

where $f(a_1, \ldots, a_m) \mapsto \sum a_i u_i$. Here, $\tilde{P}$ is projective by $\mathrm{pd}(K) = 1$ hence $\tilde{P}$ is free as A is Noetherian, local. By the construction $F/PF \cong K/PK$, therefore, $\tilde{P} \subseteq PF$. By $\mathrm{depth}(A) = 0$, P consists of zero-divisors so $P \in \mathrm{Ass}(A)$ so there exists an $a \in A$ such that $pa = 0$ for all $p \in P$ hence $a\tilde{P} \subseteq aPF = 0$. This contradicts the assumption that $\tilde{P}$ is free.

As a second step, we assume that $\mathrm{depth}(A) > 0$ and $\mathrm{depth}(M) = 0$. In this case, we know that $P \in \mathrm{Ass}(M)$ but there exists a non-zerodivisor $x \in P$. Therefore, there exists an $m \in M$ such that $P = \mathrm{Ann}(m)$. So we can take a short exact sequence

$$0 \longrightarrow K \longrightarrow F \xrightarrow{\varepsilon} M \longrightarrow 0$$

where F is a finitely generated free A-module. Choose $u \in F$ such that $\varepsilon(u) = m$. Then $Pu \subseteq K$ since $Pm = 0$. Therefore, $P(xu) \subseteq xK$. Also, $xu \in K$ as $x \in P$ but $xu \notin xK$ as $u \notin K$ and x is a non-zerodivisor on A hence on F as well. This means that $K/xK \neq 0$. But all elements of P are zero-divisors on K/xK by the definition of K (i.e. by the above short exact sequence) hence $\mathrm{depth}(K/xK) = 0$. Also, x is a non-zerodivisor on K because it is a sub of the free $F \supseteq K$. Therefore, by Proposition 6.15, $\mathrm{pd}_A(K) = \mathrm{pd}_{A/(x)}(K/xK)$ but M is not free as $\mathrm{depth}(M) = 0$ but $\mathrm{depth}(A) > 0$. This means that $\mathrm{pd}(M) > 0$ so $\mathrm{pd}_A(M) = \mathrm{pd}_A(K) + 1$.

On the other hand, we can apply the induction and obtain

$$\mathrm{depth}(A/(x)) = \mathrm{depth}(K/xK) + \mathrm{pd}_{A/(x)}(K/xK) = \mathrm{pd}_{A/(x)}(K/xK)$$

where $\mathrm{depth}(A/(x)) = \mathrm{depth}(A) - 1$ by Proposition 5.14, and $\mathrm{depth}(K/xK) = 0$ as we have seen. Therefore, by the previous paragraph, $\mathrm{pd}_{A/(x)}(K/xK) = \mathrm{pd}_A(K) = \mathrm{pd}_A(M) - 1$ so we are done with the case when $\mathrm{depth}(A) > 0$ and $\mathrm{depth}(M) = 0$.

Finally, we prove the general case when $\mathrm{depth}(M) > 0$ and $\mathrm{depth}(A) > 0$: Then $P \notin \mathrm{Ass}(M) \cup \mathrm{Ass}(A)$ by these positivity assumptions. By Prime Avoidance (Lemma 1.11) and the finiteness of the set of associated primes, we get that there exists an $x \in P$ non-zerodivisor on both M and A. We know that $\mathrm{depth}(A/(x)) < \mathrm{depth}(A)$ by Proposition 5.14 so we may use induction:

$$\mathrm{depth}(A/(x)) = \mathrm{depth}(M/xM) + \mathrm{pd}_{A/(x)}(M/xM)$$

where $\mathrm{depth}(A/(x)) = \mathrm{depth}(A) - 1$, $\mathrm{depth}(M/xM) = \mathrm{depth}(M) - 1$ and $\mathrm{pd}_{A/(x)}(M/xM) = \mathrm{pd}_A(M)$ by Proposition 6.15. □

Theorem 6.16. (Serre) *A Noetherian local ring A is regular if and only if* $\mathrm{gldim}(A) < \infty$*. In this case,* $\mathrm{gldim}(A) = \dim(A) = \mathrm{depth}(A)$.

Remark 6.17. The equality $\dim(A) = \mathrm{depth}(A)$ is not new, we have just seen that.

Proof. First, we prove $\Rightarrow$: We do induction on $d := \dim(A)$: If $d = 0$ then A is a field that clearly has global dimension zero. If $d = \operatorname{depth}(A) > 0$ then let $x \in P$ be a non-zerodivisor. Then $\operatorname{gldim}(A/(x)) = \operatorname{gldim}(A) - 1$ by Corollary 6.14 provided that $\operatorname{gldim}(A/(x)) < \infty$ which is true by the induction. Therefore, $\operatorname{gldim}(A) < \infty$. By induction, we know that $\dim(A/(x)) = \operatorname{gldim}(A/(x))$ so the same holds for A.

For $\Leftarrow$ we use induction on $\operatorname{gldim}(A)$. If it is zero then this means that all A-modules are projective hence free (since the ring is Noetherian local, see Theorem 6.10). In particular, the module $\Bbbk := A/P$ is free which is a field so $A = \Bbbk$, so the statement holds.

If $\operatorname{gldim}(A) > 0$ then $\operatorname{depth}(A) \neq 0$ by the proof of Case I in Theorem 6.11 of Auslander-Buchsbaum. So let $x \in P$ a non-zerodivisor and $x \notin P^2$. Such an element exists: apply the Prime Avoidance Lemma 1.11 for the associated primes, P^2 (which is not necessarily a prime ideal but it is not needed in the lemma) and P. Assume that we know that $\operatorname{gldim}(A/(x)) < \infty$ (we will get back to this point). Then by Corollary 6.14, $\operatorname{gldim}(A/(x)) = \operatorname{gldim}(A) - 1$ so we can apply the induction on $A/(x)$ hence it is regular. Therefore, P modulo (x) is generated by a regular sequence $\overline{y_1}, \dots, \overline{y_r}$. Lift $\overline{y_i}$ to $y_i \in P$: then $x, y_1, \dots, y_r$ is a regular sequence generating P. Hence A is regular.

It is left to prove that $\operatorname{gldim}(A/(x)) < \infty$ if $\operatorname{gldim}(A) < \infty$. This statement is equivalent to $\operatorname{pd}_{A/(x)}(\Bbbk) < \infty$ by Proposition 6.6 where $\Bbbk := A/P$. So consider the following exact sequence:

$$0 \longrightarrow P/(x) \longrightarrow A/(x) \longrightarrow \Bbbk \longrightarrow 0$$

Since $A/(x)$ is free hence projective, it is enough to prove that $\operatorname{pd}_{A/(x)}\big(P/(x)\big) < \infty$. By the second part of Proposition 6.15,

$$\operatorname{pd}_{A/(x)}\big(P/xP\big) = \operatorname{pd}_A(P) < \infty$$

The problem is that $P/(x) \leq A/(x)$ is not necessarily the same as P/xP.

To finish the proof, we claim that the exact sequence

$$0 \longrightarrow (x)/xP \longrightarrow P/xP \longrightarrow P/(x) \longrightarrow 0$$

splits. This is enough since then $P/(x)$ is a direct summand of P/xP and the projective dimension is additive so if $\operatorname{pd}(P/xP) < \infty$ then $\operatorname{pd}(P/(x)) < \infty$.

As $x \in P \backslash P^2$ there exist $x_2, \dots, x_r \in P$ such that $x, x_2, \dots, x_r$ modulo P^2 is a basis of P/P^2. Then $(x) \cap \big((x_2, \dots, x_r) + P^2\big) \subseteq xP$ since if not then there exists a $y \in (x_2, \dots, x_r) + P^2$ such that $y = xu$ where u is a unit. (This is exactly the negation of the previous statement since $A \backslash P$ is the set of units.) However, this means that $x = u^{-1}y \in (x_2, \dots, x_r) + P^2$ what contradicts the choice of $(x_2, \dots, x_r)$. Now, consider the following maps:

$$P/(x) \overset{=}{\to} \big((x) + (x_2, \dots, x_r) + P^2\big)/(x) \overset{\cong}{\to} \big((x_2, \dots, x_r) + P^2\big)/\big((x) \cap \big((x_2, \dots, x_r) + P^2\big)\big) \to P/xP \to P/(x)$$

where the big composition is the identity as one can check. This means exactly that P/xP can be retracted to $P/(x)$ and that was the goal. □

TENTH LECTURE, 17TH OF MARCH

Corollary 6.18. (Of Serre's Theorem 6.16) *Let A be a regular local ring and $Q \subseteq A$ be a prime ideal. Then A_Q is regular too.*

Proof. Since $\operatorname{gldim}(A) < \infty$we have a projective resolution $(P_i)_{i \leq d}$ of the A-module A/Q where P_i is in fact finitely generated and free because A is Noetherian, local. Now, we can tensor this projective resolution with A_Q what stays exact (because either A_Q is flat or because P_i is free hence the syzygies are split-exact). Moreover,

$$A/Q \otimes_A A_Q \cong A_Q/QA_Q$$

the residue field of A_Q. Hence we got a finite free resolution the residue field of A_Q over A_Q, in particular $\operatorname{pd}_{A_Q}(A_Q/QA_Q) < \infty$. By Proposition 6.7 it is equivalent to $\operatorname{gldim}(A_Q) < \infty$. □

Definition 6.19. A Noetherian ring A is *regular* if all localizations A_P (for all prime ideals $P \subseteq A$) are regular local maps.

Remark 6.20.

- It is enough to require that A_P is regular for P being maximal, since the others are further localizations of them.
- Regular rings are Cohen-Macauley.

Example 6.21. Regular rings:

1. A Dedekind domain (integrally closed Noetherian domain of dimension 1) is regular since all localization are discrete valuation domains that are clearly regular.
2. If X is a smooth affine variety over a field then the coordinate ring $\mathcal{A}_X$ is regular. The converse is also true provided that the field is perfect.

Proposition 6.22. *If A is a regular ring then $A[t]$ is regular too.*

Corollary 6.23. *If A is a field (or Dedekind ring) then $A[t_1, \dots, t_n]$ is regular.*

Proof of Proposition 6.22. : Let $P \subseteq A[t]$ be a maximal ideal and take $Q = P \cap A$. Then $A[t]_P$ is a localization of $A_Q[t]$ where A_Q is regular. Hence, we can assume that A is local with maximal ideal Q. Then P maps to $(\overline{f}) \subseteq \Bbbk[t]$ modulo Q. Now, lift this $\overline{f}$ to $f \in A[t]$. Then clearly, $P = (Q, f)$ where f is not a zero-divisor modulo Q, hence $\operatorname{depth}_{A[t]}(P) \geq \operatorname{depth}_A(Q) + 1$. Moreover,

$$\dim A[t]_P = \operatorname{ht}(P) \geq \operatorname{depth}(P) \geq \operatorname{depth}(Q) + 1 = \operatorname{ht}(Q) + 1 = \dim(A) + 1$$

where we used regularity of A at the penultimate equality. However,

$$\dim A[t]_P = \operatorname{ht}(P) \leq \operatorname{ht}(Q) + 1 = \dim A + 1$$

Therefore, we got that $\dim A[t]_P = \dim(A) + 1$ while $\operatorname{depth}(A[t]) = \operatorname{depth}(A) + 1$ by Proposition 5.14 hence – by the regularity of A – we get $A[t]_P$ is regular. □

To prove Auslander Buchsbaum's theorem, we first prove the following:

Theorem 6.24. *If A is a Noetherian ring of finite dimension d then A is regular if and only if* $\operatorname{gldim}(A) \leq d$.

Corollary 6.25. (Hilbert syzygy theorem) $\operatorname{gldim}\big(\Bbbk[t_1, \dots, t_d]\big) \leq d$.

Remark 6.26.

- Actually, $\operatorname{gldim}\big(\Bbbk[t_1, \dots, t_d]\big) = d$ what can be proved by induction: $d = 0$ is clear and for the induction step one can use Corollary 6.14.
- In fact, over a $\Bbbk[t_1, \dots, t_d]$ every finitely generated projective module is free. It was a conjecture of Serre, solved by Quillen and Suslin. Consequently, every finitely generated module has a finitely generated free resolution.

Proof of Theorem 6.24. $\Leftarrow$: If $P \subseteq A$ is maximal then $\operatorname{gldim}(A_P) \leq \operatorname{gldim}(A) \leq d$ by the argument using the tensoring with A_P on the projective resolution of A/P. This direction of the statement follows.

For $\Rightarrow$: let M be a finitely generated module over A and take a truncated projective resolution of M:

$$0 \longrightarrow M_d \longrightarrow P_{d-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

Here, all the P_i's are finitely generated by Noetherian property. We need to prove that M_d is projective too. If $P \subseteq A$ is maximal then we can tensor the whole sequence by A_P getting again an exact sequence by flatness of A_P. Here, $P_i \otimes A_P$ is projective over A_P since it is a direct summand of a free.

The ring A_P is regular of dimension d since A is regular (hence Cohen-Macauley) of dimension d too and depth is preserved there. Therefore, $\mathrm{gldim}(A_P) \leq d$ hence $M_A \otimes_A A_P$ is free over A_P. The statement can be deduced from the following proposition:

Proposition 6.27. *Let A be a Noetherian ring, M a finitely generated A-module. Then M is projective if and only if $M \otimes_A A_P$ is free for all $P \subseteq A$ prime. In fact, it is enough to investigate maximal P's.*

Lemma 6.28. *Let A be a Noetherian ring:*

1. *A finitely generated A-module is zero if and only if $M \otimes_A A_P = 0$ for all maximal ideals P.*
2. *A morphism $\varphi : M_1 \to M_2$ of finitely generated modules is surjective if and only if $\varphi \otimes \mathrm{id}_{A_P}$ is surjective for all maximal ideals P.*

Proof. 1) $\Rightarrow$ 2): Apply $a)$ to the cokernel of φ and use the right exactness of the tensor product.

Direction $\Rightarrow$ of 1) is trivial, while to get $\Leftarrow$, assume that there exists a maximal ideal $m \neq 0$ such that $\mathrm{Ann}(m) \subseteq A$ is a proper ideal. Therefore, there exists a maximal $P \subseteq A$ containing $\mathrm{Ann}(m)$ but then $m \neq 0$ in $M \otimes_A A_P$. □

Proof of the proposition by the lemma. : Direction $\Rightarrow$ is clear by Theorem 6.10 since a localization of a projective is projective (it is still a summand of a free). To get $\Leftarrow$, take an exact sequence $0 \to K \to F \xrightarrow{f} M \to 0$ for a free generator F of M. Then it is enough to show that this sequence splits, for which it is enough to show that the dual map

$$\mathrm{Hom}(M, f) : \mathrm{Hom}(M, F) \to \mathrm{Hom}(M, M)$$

is surjective. Indeed, if $s \in \mathrm{Hom}(M, F)$ is a preimage of id_M then this s must be a section of the sequence $0 \to K \to F \to M \to 0$ by definition.

So take the localization of $\mathrm{Hom}(M, F) \to \mathrm{Hom}(M, M)$ giving

$$\mathrm{Hom}(M \otimes_A A_P, F \otimes_A A_P) \cong \mathrm{Hom}(M, F) \otimes_A A_P \to \mathrm{Hom}(M, M) \otimes_A A_P \cong \mathrm{Hom}(M \otimes_A A_P, M \otimes_A A_P)$$

Here, we know that $M \otimes_A A_P$ is projective hence $\mathrm{Hom}(M \otimes_A A_P, F \otimes_A A_P) \to \mathrm{Hom}(M \otimes_A A_P, M \otimes_A A_P)$ is surjective because it is equivalent to the splitting of

$$0 \to K \otimes_A A_P \to F \otimes_A A_P \xrightarrow{f \otimes_A A_P} M \otimes_A A_P \to 0$$

so we can apply part b) of Lemma 6.28 on $\mathrm{Hom}(M, f)$. □

□

Theorem 6.29. (Auslander - Buchsbaum) *A regular local ring is a unique factorization domain.*

Remark 6.30. In a unique factorization domain, every prime ideal of height 1 is principal. Therefore, if S is a smooth variety over a field, then A is a local ring at P, and $Y \subseteq X$ is of codimension 1. Hence, Y defines a prime ideal of height 1 in A so it is principal. This means that locally, around P, it is defined by one equation.

Lemma 6.31. (Nagata) *If A is a Noetherian integral domain and $x \in A$ is a prime element and $A_{(x)}$ is a unique factorization domain then A is a unique factorization domain.*

Recall the following proposition:

Proposition 6.32. *A Noetherian integral domain A is a unique factorization domain if and only if every height 1 prime ideal in it is principal.*

Proof. If A is a unique factorization domain and P is a prime ideal of height 1 then for all $a \in P \backslash \{0\}$ we have $a = u \cdot \prod p_i^{\alpha_i}$ so there exists i such that $p_i \in P$ by primeness. But then (p_i) is a prime ideal contained in P hence $(p_i) = P$ by $\mathrm{ht}(P) = 1$. Conversely, if every height 1 prime ideal is principal then we want to conclude that every irreducible element is prime. So assume that p is irreducible and take a minimal prime P containing P. Then – by the Hauptidealsatz – $\mathrm{ht}(P) \leq 1$ but it is nonzero hence $\mathrm{ht}(P) = 1$. The assumption says that $P = (b)$ for some $b \in A$. Therefore $P = (p)$ because p was irreducible. □

Proof of Lemma 6.31. By this proposition, it is enough to prove that every height 1 prime ideal is principal. So take a $P \subseteq A$ prime ideal with $\mathrm{ht}(P) = 1$. If $x \in P$ then $P = (x)$ since x is a prime element and $\mathrm{ht}(P) = 1$ so we are done. The other case is $x \notin P$. In this case, there exists a $p \in P$ such that $PA_x = pA_x$ for some $p \in A$ since A_x is a unique factorization domain. We may assume that $(p) \subseteq A$ is maximal with this property. Then $p \notin (x)$, because otherwise there exists an $a \in A$ such that $p = ax$. Here, $a \in P$ as $x \notin P$ but $p \in P$ and $(a) \supsetneq (p)$, hence $pA_x = x^{-1}pA_x = aA_x$ which is a contradiction.

So $PA_x = pA_x$ i.e. for all $y \in P$ there exists $a \in A$ and $m, n > 0$ such that $\frac{y}{x^n} = p \cdot \frac{a}{x^m}$ since A is a domain. This means that $x^l y \in (p)$ for big enough l. Therefore, it is enough to show that $xy \in (p)$ implies $y \in (p)$. If $xy = ap$ then $a \in (x)$ as (x) is a prime ideal and $p \notin (x)$. Therefore, $a = bx$ for some b hence $xy = ap = bxp$ so $y = bp$ because A is a domain. □

Lemma 6.33. (Kaplansky) *If A is a domain and $I \subseteq A$ is an ideal such that $I \oplus A^n \cong A^{n+1}$ as A-modules then I is principal i.e. $I \cong A$ as A-modules. (proof: next time)*

Lemma 6.34. (Serre) *If A is a ring and P is a projective A-module such that there exists a finite free resolution of length n then P is stably free, i.e. there exists free modules F and F' such that $P \oplus F' \cong F$. If, moreover, A is Noetherian and P is finitely generated then we may find finitely generated F and F'.*

Proof. The resolution is denoted as

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \dots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} P \longrightarrow 0$$

As P is projective, φ_0 has a retraction so $F_0 \cong P \oplus \mathrm{Im}(\varphi_1)$ hence $\mathrm{Im}(\varphi_1)$ is projective. We can iterate this giving that $F_i \cong \mathrm{Im}(\varphi_i) \oplus \mathrm{Im}(\varphi_{i+1})$ for all i hence

$$P \oplus F := P \oplus \bigoplus_{i=1}^{n} \mathrm{Im}(\varphi_i) \cong P \oplus \bigoplus_{i \text{ odd}} F_i \cong \bigoplus_{i \text{ even}} F_i =: F'$$

so the statement holds. □

Proof of Theorem 6.29. : Let A be a regular local domain of dimension d. We proceed by induction on $\dim(A)$: the case $\dim(A) = 0$ is clear. Pick an $x \in P \backslash P^2$. We know that $A/(x)$ is again regular, local by Proposition 2.4. Therefore, by Theorem 2.6, it is again an integral domain. This means that (x) is a prime ideal. Therefore, by Lemma 6.31, it is enough to prove that A_x is a unique factorization domain, i.e. by Lemma 6.32, every prime ideal $Q \subseteq A_x$ of height 1 is principal.

If M is a maximal ideal of A_x then $(A_x)_M$ is also a localization of A by a prime ideal hence it is also regular by Corollary 6.18. Also, $\dim(A_x)_M < \dim A$ as $x \notin M$ so $M \cap A$ is not maximal. Therefore, by induction, $(A_x)_M$ is a unique factorization domain, hence, $Q(A_x)_M$ is principal since it keeps its height. Therefore, $Q(A_x)_M$ is a free module of rank 1 over $(A_x)_M$. However, it is true for all localizations at a maximal ideal, i.e. $Q(A_x)_M$ is a locally free module. This means – by Proposition 6.27 – that Q is projective as an A_x-module.

On the other hand, there exists $Q' \subseteq A$ such that $Q = Q'A_x$ by definition. By the regularity of A we know that every finitely generated A-module has a finite free resolution since A is local with finite global dimension. In particular, Q' has a finite resolution too. Therefore, Q also has a finite free resolution since we can tensor the resolution of Q' with A_x. Therefore, by Lemma 6.34, Q is stably free as an A_x-module, i.e. there exists an m and n such that $Q \oplus (A_x)^m \cong (A_x)^n$. We claim that $m = n - 1$ as we can tensor this equation by $(A_x)_M$ yielding

$$Q(A_x)_M \oplus (A_x)_M^m \cong (A_x)_M^n$$

where $Q(A_x)_M$ is a free module of rank 1 so $n = m - 1$ by picking a module-basis. Hence, we can apply Lemma 6.33 to complete the proof. □

Eleventh Lecture, 24th of March

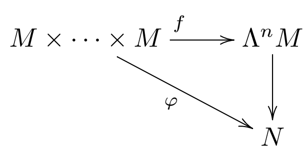
7 Koszul complex

Definition 7.1. Let A be a ring, M is an A-module and $n \geq 0$. Then the n-th exterior power of M is:

$$\Lambda^0 M := A; \qquad \Lambda^1 M := M$$

$$\Lambda^n M := M^{\otimes n} / \langle m_1 \otimes \cdots \otimes m_n \mid \exists 1 \leq i < j \leq n : m_i = m_j \rangle$$

It is characterized by the following universal property: for all A-modules N and for all n-linear maps $\varphi : M \times \cdots \times M \to N$ such that $\varphi(m_1, \ldots, m_n) = 0$ if $m_i = m_j$ for some $i \neq j$ there exists a factorization



where f is the natural surjection.

Notation: the image of $m_1 \otimes \cdots \otimes m_n$ in $\Lambda^n M$ is denoted by $m_1 \wedge \cdots \wedge m_n$.

Remark 7.2.

1. Alternative definition: Consider the tensor algebra $T(M) = \oplus M^{\otimes n}$ which is a graded A-algebra with the usual (tensor-)multiplication. Then we can take

$$\Lambda(M) = T(M)/(m \otimes m \mid m \in M)$$

where the latter is a generated two-sided ideal. The n-th homogeneous component of $\Lambda(M)$ is the same as the above $\Lambda^n M$.

2. There is a multiplication $\Lambda^n M \otimes \Lambda^m M \to \Lambda^{n+m} M$, the induced multiplication from $\Lambda(M)$.

3. Moreover, all A-module map $M \to N$ extends to a map $\Lambda(M) \to \Lambda(N)$ of graded A-algebras. In, particular, there exists maps $\Lambda^n M \to \Lambda^n N$ for all $n \geq 0$ since the map is graded.

4. In $\Lambda^n M$ we have the relation

$$m_1 \wedge \cdots \wedge m_i \wedge m_{i+1} \wedge \cdots \wedge m_n = (-1) \cdot m_1 \wedge \cdots \wedge m_{i+1} \wedge m_i \wedge \cdots \wedge m_n$$

5. If M and N are A-modules then

$$\Lambda^n(M \otimes N) \cong \bigoplus_{i+j=n} \Lambda^i M \otimes \Lambda^j N$$

what property follows from the analogous property for the tensor product.

6. If $M \cong A^n$ is free of rank r then $\Lambda^n M$ is free of rank $\binom{r}{n}$. If $e_1, \dots, e_r$ is a basis of M then

$$\left\{ e_{i_1} \wedge \cdots \wedge e_{i_n} \mid 1 \leq i_1 < i_2 < \cdots < i_n \leq r \right\}$$

is a basis of $\Lambda^n M$. The idea for this is that one can take the determinant as a nonzero multilinear map and reduce an indirectly existing relation to a relation $\det = 0$ which is a contradiction hence the above elements are independent.

Proposition 7.3. *If A is a domain $I_1, \dots, I_n, J_1, \dots, J_n \subseteq A$ ideals such that*

$$\bigoplus_{i=1}^{n} I_i \cong \bigoplus_{i=1}^{n} J_i$$

as A-modules then $I_1 \cdot \dots \cdot I_n \cong J_1 \cdot \dots \cdot J_n$ as A-modules.

Corollary 7.4. *Lemma 6.33 where $I_1 = I$, $I_i = A$ for $i \geq 2$ and $J_i = A$ for all i.*

Proof of Proposition 7.3. First, we prove that

$$I_1 \cdot \dots \cdot I_n \cong \Lambda^n\big(I_1 \oplus \cdots \oplus I_n\big)/T$$

where T is a torsion submodule. This is enough since the right hand side is the same for both I_i's and J_i's by the assumption.

For this, take $K = \mathrm{Frac}(A)$ and let us denote $M = I_1 \oplus \cdots \oplus I_n$. Then $M \otimes_A K \cong K^n$ since $I \otimes K = K$ for all ideals I. Then

$$\Lambda^n M \otimes_A K \cong \Lambda^n(M \otimes_A K)$$

hence there exists a map

$$\begin{array}{ccc} \Lambda^n M & \xrightarrow{\varphi} & K \\ & {\scriptstyle \alpha \mapsto \alpha \otimes 1} \searrow & \uparrow \\ & & \Lambda^n M \otimes K \end{array}$$

by the universal property. The kernel of this map φ is exactly T by construction.

We claim that in this case $\mathrm{Im}(\varphi) = I_1 \cdot \dots \cdot I_n \subseteq K$ proving the statement. Let $e_1, \dots, e_n$ be the standard basis of K^n. If $m_i \in M = \oplus_{i=1}^n I_i$ then we can write

$$m_i = \sum_{i,j} a_{ij} e_j \qquad a_{ij} \in I_j$$

hence we can rearrange the elements of $\Lambda^n M$ as

$$m_1 \wedge \cdots \wedge m_n = \det((a_{ij})) \cdot e_1 \wedge \cdots \wedge e_n \in \Lambda^n K^n = K$$

Conversely, $I_1 \cdot \dots \cdot I_n = \langle \det((a_{ij})) \mid a_{ij} \in I_j \rangle \subseteq K$. □

Definition 7.5. Let A be a ring, M and A-module, $f : M \to A$ an A-linear map. Then the *Koszul complex* $K(f)$ of f is defined as

$$\dots \longrightarrow \Lambda^n M \xrightarrow{\mathrm{d}_f^n} \Lambda^{n-1} M \xrightarrow{\mathrm{d}_f^{n-1}} \dots \longrightarrow \Lambda^2 M \xrightarrow{\mathrm{d}_f^2} M \xrightarrow{\mathrm{d}_f} A \longrightarrow 0$$

where $\mathrm{d}_f = f$ and

$$\mathrm{d}_f^n(m_1 \wedge \dots \wedge m_n) = \sum_{i=1}^{n} (-1)^{i+1} \cdot f(m_i) \cdot m_1 \wedge \dots \wedge \hat{m}_i \wedge \dots \wedge m_n$$

which map exists by the universal property. Moreover, one can check that $\mathrm{d}_f^{n-1} \circ \mathrm{d}_f^n$ even for $n = 2$.

Remark 7.6. On $\Lambda(M)$ the d_f^n induce a map of graded algebras $\mathrm{d}_f : \Lambda(M) \to \Lambda(M)$ of degree -1 satisfying $\mathrm{d}_f \circ \mathrm{d}_f = 0$. Moreover, if $x \in \Lambda^i M$ and $y \in \Lambda^j M$ such that

$$\mathrm{d}_f(x \wedge y) = \mathrm{d}_f(x) \wedge y + (-1)^i x \wedge \mathrm{d}_f(y)$$

Such that graded algebras are called differential graded algebras (in short, DGA).

Example 7.7. Let $M = A$ so every $f : A \to A$ module homomorphism is multiplication by an element $x := f(1)$. Then the homology in degree zero of the above sequence is A/xA, in degree 1 it is zero if and only if x is a non-zerodivisor.

Definition 7.8. Let $C_\bullet$ and $D_\bullet$ two chain complexes concentrated in nonnegative degrees. Then the tensor product of them is

$$(C \otimes D)_n = \bigoplus_{i+j=n} C_i \otimes D_j$$

gets a natural differentiation by the formula $\mathrm{d}_n^{C\otimes D}(x \otimes y) = \mathrm{d}_i^C(x) \otimes y + (-1)^i x \otimes d_j^D(y)$.

Example 7.9. Let f_1, f_2 be two $A \to A$ module homomorphisms. Then $K(f_1) \otimes K(f_2)$ is the following:

$$A \longrightarrow A \oplus A \longrightarrow A$$

where the second map if $(x, y) \mapsto f_1(x) + f_2(y)$ and the first is

$$A \cong A \otimes A \ni x \otimes y \mapsto (f_2(y)x, f_1(x)y$$

Therefore, using the canonical isomorphism between $A \otimes A$ and $\Lambda^2(A \oplus A)$ we get $K(f_1) \otimes K(f_2) \cong K(f_1, f_2)$ where $(f_1, f_2) : A \oplus A \to A$ is an A-linear map.

More generally,

Proposition 7.10. *If M_1, M_2 are A-modules $f_i : M_i \to A$ then define*

$$f = (f_1, f_2) : M_1 \oplus M_2 \to A$$

Then $K(f) \cong K(f_1) \otimes K(f_2)$.

Proof. Recall that $\Lambda^n(M_1 \oplus M_2) \cong \bigoplus_{i+j=n} \Lambda^i M_1 \otimes \Lambda^j M_2$ where the latter is nothing else but the n-th term of $K(f)$. To compare d_f with $\mathrm{d}_{f_1} \otimes \mathrm{d}_{f_2}$ view them as degree -1 maps $\Lambda(M_1 \oplus M_2) \to \Lambda(M_1 \oplus M_2)$. They coincide in degree 1 and satisfy the same equation $\mathrm{d}(x \wedge y) = \mathrm{d}(x) \wedge y + (-1)^i x \wedge \mathrm{d}y$. □

Let $f = (f_1, \dots, f_r) : A^r \to A$ and take $f_i(1) =: x_i$ since f is the same as sum of multiplications by x_i's. Let

$$K(\underline{x}) = K(x_1, \dots, x_n) := K(f)$$

so it is a complex of length r of free A-modules of rank $\binom{r}{n}$. If M is an A-module then define $K(\underline{x}, M) := K(\underline{x}) \otimes_A M$.

Theorem 7.11. *If $\underline{x} = (x_1, \dots, x_n)$ is an M-regular sequence then $K(\underline{x}, M)$ is acyclic (i.e. it has no homology in positive degrees). In particular, for $M = A$, $K(\underline{x})$ is a free resolution of $A|_{(x_1,\dots,x_r)}$.*

Corollary 7.12. *The $\mathbb{k}[x_1, \dots, x_n]$-module $\mathbb{k}$ has a finite free resolution of length n, in particular, $\mathrm{pd}_{\mathbb{k}[x_1,\dots,x_n]}(\mathbb{k}) \leq n$.*

Similarly, if A is a regular local ring of dimension n then $\mathrm{gldim}(A) \leq n$.

Corollary 7.13. *If $I = (x_1, \dots, x_n)$ then*

$$\mathrm{Tor}_i(A/I, M) \cong H_i(K(\underline{x}) \otimes_A M)$$

$$\mathrm{Ext}^i(A/I, M) \cong H^i\mathrm{Hom}(K(\underline{x}), M)$$

Lemma 7.14. *If $C_\bullet$ is any complex of A-modules and $x \in A$ then there exists an exact sequence of complexes*

$$0 \longrightarrow C_\bullet \longrightarrow C_\bullet \otimes_A K(x) \longrightarrow C_\bullet[-1] \longrightarrow 0$$

where $(C_\bullet[-1])_i = C_{i-1}$. Moreover, in the corresponding long exact sequence

$$\dots \longrightarrow H_i(C_\bullet) \longrightarrow H_i\big(C_\bullet \otimes_A K(x)\big) \longrightarrow H_{i-1}(C_\bullet) \longrightarrow H_{i-1}(C_\bullet) \longrightarrow \dots$$

the map $H_{i-1}(C_\bullet) \to H_{i-1}(C_\bullet)$ is multiplication by $(-1)^{i-1}x$.

Corollary 7.15. *There exists an exact sequence*

$$0 \longrightarrow H_i(C_\bullet)/xH_i(C_\bullet) \longrightarrow H_i\big(C_\bullet \otimes_A K(x)\big) \longrightarrow \mathrm{Ker}\Big(H_{i-1}(C_\bullet) \xrightarrow{x\cdot} H_{i-1}(C_\bullet)\Big) \longrightarrow 0$$

Proof of Lemma 7.14. : We know that $K(x) = A \xrightarrow{x\cdot} A$. The Corresponding exact sequence is

$$0 \longrightarrow A \longrightarrow K(x) \longrightarrow A[-1] \longrightarrow 0$$

what we can tensor with $C_\bullet$, where the following term appears:

$$\big(C_\bullet \otimes K(x)\big) = (C_i \otimes_A A) \oplus (C_{i-1} \otimes_A A) \cong C_i \oplus C_{i-1}$$

with the differential $C_i \oplus C_{i-1} \to C_{i-1} \oplus C_{i-2}$ given by

$$\begin{bmatrix} \partial & (-1)^{i-1}x \\ 0 & \partial \end{bmatrix}$$

where ∂ is the differential of $C_\bullet$. Then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_i & \longrightarrow & C_i \oplus C_{i-1} & \longrightarrow & C_{i-1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C_{i-1} & \longrightarrow & C_{i-1} \oplus C_{i-2} & \longrightarrow & C_{i-2} & \longrightarrow & 0 \end{array}$$

To compute the connecting homomorphism in the long exact sequence can be computed by applying the Snake lemma on the above diagram. In details, take $\alpha \in \mathrm{Ker}(C_{i-1} \to C_{i-2})$, lift it to $(0, \alpha) \in C_i \oplus C_{i-1}$ and map it into $((-1)^{i-1}x\alpha, 0) \in C_{i-1} \oplus C_{i-2}$ by applying the matrix above. □

Proof of Theorem 7.11. : We proceed by induction. Recall that $K(\underline{x}, M) = [M \xrightarrow{x\cdot} M]$. Then $H_1\big(K(x), M\big) = \operatorname{Ker}(M \xrightarrow{x\cdot} M)$ and $H_0\big(K(x), M\big) = M/xM$ so the induction starts.

Now, assume that $r > 1$ and apply the above argument and the Corollary 7.15 of the Lemma 7.14 to $H_{i-1}(C_\bullet)$ and $H_i(C_\bullet)$. We get that

$$0 \longrightarrow H_0\big(K(x) \otimes H_i(C)\big) \longrightarrow H_i\big(K(x) \otimes C_\bullet\big) \longrightarrow H_1\big(K(x) \otimes H_{i-1}(C_\bullet)\big) \longrightarrow 0$$

For the inductive step, let $C_\bullet = K(x_1, \dots, x_r) \otimes_A M$ and $x = x_r$ hence

$$H_i\big(K(x), M\big) \cong H_i\big(C_\bullet \otimes_A K(x)\big)$$

since $K(x) = K(x_1) \otimes \cdots \otimes K(x_r)$ by Proposition 7.10. The induction hypothesis says that $H_i(C_\bullet) = 0$ for all $i > 0$ hence – by the above short exact sequence – we get $H_i\big(K(x, M)\big) = 0$ for all $i > 1$.

Let's determine the terms in the short exact sequence: for $i = 1$

$$H_1\big(K(x, M)\big) \cong H_1\big(K(x) \otimes H_0(C_\bullet)\big) \cong H_1\big(K(x) \otimes M/(x_1, \dots, x_{r-1})M\big) = \operatorname{Ker}\Big(N_{r-1} \xrightarrow{x_r\cdot} M_{r-1}\Big) = 0$$

which is zero since $\underline{x}$ is a regular sequence. □

Theorem 7.16. *Let A be a Noetherian local ring, M be a finitely generated A-module and $x_1, \dots, x_r \in P$ where P is the maximal ideal of A. Then the following are equivalent:*

1. $(x_1, \dots, x_r)$ *is an M-regular sequence*
2. $H_i\big(K(\underline{x}, M)\big) = 0$ *for* $i > 0$
3. $H_1\big(K(\underline{x}), M)\big) = 0$

Remark 7.17. Under the assumption of the theorem, this implies that every permutation of an M-regular sequence is M-regular.

Proof. 1) ⇒ 2) is the previous theorem, 2) ⇒ 3) is trivial and 3) ⇒ 1): In the case $r = 1$, the assumption says that $\operatorname{Ker}\big(M \xrightarrow{x\cdot} M\big) = 0$ hence it is a non-zerodivisor.

For $r > 1$: set $C_\bullet := K(x_1, \dots, x_{r-1}) \otimes_A M$. By the Lemma

$$\dots \longrightarrow H_1(C_\bullet) \longrightarrow H_1(C_\bullet) \longrightarrow H_1\big(K(x_r) \otimes C\big) = H_1\big(K(x), M\big) = 0$$

It means that $H_1(C_\bullet) \xrightarrow{x_r\cdot} H_1(C_\bullet)$ is surjective. But $x_r \in P$ hence $H_1(C_\bullet) = 0$ by Nakayama. Therefore, the induction hypothesis says that $x_1, \dots, x_{r-1}$ is M-regular but

$$0 = H_1(K(\underline{x}, M) \cong \operatorname{Ker}\Big(M/(x_1, \dots, x_{r-1})M \xrightarrow{x_r\cdot} M/(x_1, \dots, x_{r-1})M\Big)$$

proving that $\underline{x}$ is a regular sequence. □

Definition 7.18. (Grothendieck) A Noetherian local ring A is a *complete intersection ring* if there exists a regular complete local ring R such that $\hat{A} \cong R/I$ where I is generated by a regular sequence.

Fact: Regular ⇒ complete intersection ⇒ Cohen-Macauley

Theorem 7.19. (J. Tate, Assumus) *Let A be a Noetherian local ring and $x_1, \dots, x_r$ is a minimal system of generators of the maximal ideal. Then A is a complete intersection ring if and only if the following graded A-algebras are isomorphic, i.e.*

$$\bigoplus_{i=0}^{\infty} H_i\big(K(\underline{x})\big) \cong \Lambda\big(H_1(K(\underline{x}))\big)$$