Étale and smooth extension

Contents

Chapter 0

Weierstrass Preparation Theorem

0.1 01/18/2022

Convention: all local rings are assumed to be noetherian.

Theorem 0.1.1 . Suppose (R, m) is a complete local ring. M is an m-adically Hausdorff R-module (i.e. $\bigcap m^n M = 0$). If $\bar{x}_1, ..., \bar{x}_1$ generate M/mM over R/mR, $x_1, ..., x_n$ generate M over R.

Proof. Take $y \in M$. Assume $\bar{y} = \Sigma \bar{\lambda}_i \bar{x}_i$ in M/mM, in which $\lambda \in R$ and $x_i \in M$. Then $y = \Sigma \lambda_i x_i + y_1$ where $y_1 = \Sigma \mu_i \alpha_i$ in mM. We can write α_i as $\alpha_i = \Sigma \lambda_{ij} x_j + \beta_i$, $\beta_i \in mM$. Combining the equations, we get $y = \Sigma(\lambda_i + \mu_i \lambda_{ij}) x_i + \Sigma \mu_i \beta_i$. Note that $\Sigma \mu_i \beta_i \in m^2 M$. By continuing the process and taking the limit, we get the equation $y = \Sigma \gamma_i x_i$, $\gamma_i \in R$, since R is complete and M is Hausdorff. □

Theorem 0.1.2 (Weierstrass preparation theorem WPT)**.**
Let (R, m) be a complete local ring, $f \in R[[x]]$. Assume that h is the smallest integer such that $a_h \notin m$ where $f = \Sigma a_i x^i$ (known as the order of f in $R[[x]]$). Then any $g \in R[[x]]$ can be written uniquely as $g = qf + r$, $q \in R[[x]]$, $r \in R[x]$ and $deg(r) < h$.

Proof. Let $M = R[[x]]/(f)$. Since R is m-adically complete, $R[[x]]$ is (m, x)-adically complete and noetherian. Therefore (f) is closed in $R[[x]]$, which is equivalent to say M is Hausdorff as an $R[[x]]$-module, and thus as an R-module. Note that $M/mM \simeq k[[x]]/(x^h)$. Apply Theorem 0.1.1 to M, we conclude that M is generated by $1, \bar{x}, ..., \bar{x}^{h-1}$ as an R-module. Given any element $g \in R[[x]]$, we have $g = qf + r$ where $r = \sum_{i<h} p_i x^i$, $p_i \in R$. To prove the uniqueness statement, it suffices to prove that if $qf = r$, $r \in R[x]$, $deg(r) < h$, then $q = 0$. Suppose that $q = \sum_n b_n x^n$, i is the largest integer such that all a_n sit inside m^i (exits since $R[[x]]$ is Hausdorff), and j is the smallest number such that $b_j \notin m^{i+1}$. The coefficient of qf in degree $h+j$ is $b_j a_h + \sum_{i \neq j} b_i a_{h+j-i}$. Note that $b_j a_h \in m^i - m^{i+1}$, $\sum_{i \neq j} b_i a_{h+j-i} \in m^{i+1}$. So this term is not 0, which is a contradiction since the coefficient of r in degree $h + j$ is 0. □

Exercise 0.1.3. f as above. Is $R[[x]]/(f)$ a free R-mod with basis $1, \bar{x}, ..., \bar{x}^{h-1}$?

Proof. We have the exact sequence

$$0 \to K \to R^h \to M \to 0$$

Tensoring by R/mR, we get

$$0 \to K/mK \to k^h \to M/mM \to 0$$

Since we can write down a projective resolution for this particular M (e.g. $0 \to R[[x]] \to R[[x]] \to M \to 0$, note that multiplication by f is injective), $Tor_1^R(k, M) = 0$. And this shows that the above sequence is exact. □

Corollary 0.1.4 . f as above. Then $f = qf^*$ where $f^* = x^h + \sum_{i<h} \gamma_i x^i$, $\gamma_i \in m$, q is a unit in $R[[x]]$.

Proof. WPT implies $x^h = qf + r$, $r \in R[x]$, $deg(r) < h$. A similar argument as the uniqueness part of the proof of Theorem 0.1.2 shows that $i = 0, j = 0$. So q is a unit. □

Definition 0.1.5. Suppose $f = qf^*$ as above. f^* is called the polynomial associated with f. Note that $(f) = (f^*)$.

Exercise 0.1.6. f^* is unique, i.e., if $f = qf^*$ and $f = q'g$, $g \in R[x]$, $g = x^h - \sum g_i x^i$, then $g = f^*$.

Proof. By the solving equations $f = qf^*$ and $f = q'g$, we have $x^h = q^{-1}f - \sum_{i<h} a_i x^i$ and $x^h = q'^{-1}f - \sum_{i<h} g_i x^i$. Thus $q = q'$, $f^* = g$ by the uniqueness of factorization. □

0.2 01/20/2022

Exercise 0.2.1. Let $f_1, ...f_t \in R[[x]]$, each regular with respect to x of certain order. Then $(f_1 \cdots f_t)^* = f_1^* \cdots f_t^*$. (Follows from exercise 0.1.6).

Proof. By corollary 0.1.4, $f_i = q_i f_i^*$. So $f_1 \cdots f_t = q_1^* \cdots q_t^* f_1^* \cdots f_t^*$. On the other hand, $f_1 \cdots f_t = q(f_1 \cdots f_t)^*$. Thus the conclusion follows from exercise 0.1.6. □

Corollary 0.2.2 . Let $R_n = k[[x_1, ..., x_n]]$, $f \in R_n$. Suppose f is regular with respect to x_n of order h (i.e. f is considered as an element in $R_{n-1}[[x_n]]$). By WPT, we have the following,

(i) For $g \in R_n$, $g = qf + r$, where $r \in R_{n-1}[x_n]$ and $deg(r) < h$.

(ii) $f = qf^*$, where $f^* = x_n^h + \sum r_i x^i$, $r_i \in R_{n-1}$.

(iii) Given $f_1, ..., f_n \in R_n$, each regular with respect to x_n. Then $(f_1 \cdots f_t)^* = f_1^* \cdots f_t^*$.

Corollary 0.2.3 . Let $\mathbb{C}\{x_1, ..., x_n\}$ be ring of convergent power series of n variables. Then WPT holds over $\mathbb{C}\{x_1, ..., x_n\}$, i.e., given f of degree h in x_n. For any $g \in \mathbb{C}\{x_1, ..., x_n\}$,

(i) there is a unique way to write g as $g = qf + r$, $r \in R_{n-1}[x_n]$, $deg(r) < h$.

(ii) $f = qf^*$, $f^* \in R_{n-1}[x_n]$, $f^* = x_n^h + \sum r_i x^i$.

Proof. See [Zariski, Samuel, Commutative Algebra, Vol3] $\square$

Theorem 0.2.4 . Given $f \in k[[x_1, ..., x_n]]$. k is a field. There exists an automorphism ϕ of R_n such that $\phi(f)$ is regular with respect to x_n.

Proof.
Case 1 $|k| = \infty$.
Claim: There exists a *linear automorphism* $\phi : R_n \to R_n$ such that $\phi(f)$ is regular with respect to x_n.
Assume that $\phi(x_i) = \sum \lambda_{ij} x_j$, $\lambda_{ij} \in k$, $1 \leq i \leq n$. We will determine λ_{ij} by requiring $\phi(f)$ is regular with respect to x_n. $f = f_d + f_{d+1} + ...$ where f_d is the first nonzero homogeneous component. $f_d = \sum_{i_1+\cdots+i_n=d} a_{i_1,...,i_n} x^{i_1} \cdots x_n^{i_n}$. Applying ϕ to f_d, we get $\phi(f_d) = \sum_{i_1+\cdots+i_n=d} a_{i_1,...,i_n} \prod_k (\sum \lambda_{kj} x_j)^{i_k}$. Note that this is the first homogeneous component of $\phi(f)$. The coefficient of x_n^d in $\phi(f_d)$ is $\sum_{i_1+\cdots+i_n=d} a_{i_1,...,i_n} \lambda_{1n}^{i_1} \cdots \lambda_{nn}^{i_n}$. We want to choose λ_{in} such that this coefficient is not zero. By exercise 0.2.5, we can always find $\lambda_{in} \in k$ such that $f_d(\lambda_{1n}, ..., \lambda_{nn}) \neq 0$. Now complete the non-singular matrix $[\lambda_{ij}]$ with fixed last column. This matrix is the desired linear transformation.
Case 2 $|k| < \infty$.
The following proof doesn't require k to be a field and irrespective of the cardinality of k. Assume that $\phi(x_1) = x_1 + x_n^{u_1}$, $\phi(x_2) = x_2 + x_n^{u_2}, \ldots, \phi(x_{n-1}) = x_{n-1} + x_n^{u_{n-1}}$, $\phi(x_n) = x_n$. Let $x_1^{a_1} \cdots x_n^{a_n}$ be the smallest term of f_d (in lexicographic order). Set $u_{n-1} > a_n$, $u_{n-2} > a_{n-1}u_{n-1} + a_n$, $u_i > a_{i+1}u_{i+1} + a_{i+2}u_{i+2} + \cdots + a_n, \ldots$. We also have $\phi(x_1^{a_1} \cdots x_n^{a_n}) = (x_1 + x_n^{u_1})^{a_1} \cdots x_n^{a_n}$. The highest power of x_n in this term is $a_1 u_1 + ... + a_{n-1}u_{n-1} + a_n$. The corresponding power in the term $x_1^{b_1} \cdots x_n^{b_n}$ of larger lexicographic order is $b_1 u_1 + ... + b_{n-1}u_{n-1} + b_n$. It is clear that $(b_1 - a_1)u_1 + ... + (b_{n-1} - a_{n-1})u_{n-1} + (b_n - a_n) > 0$ due to the way we choose u_i. Why do we not consider $f_{d+1}, f_{d+2}, ...$?.

$\square$

Exercise 0.2.5. Let $T_1, ..., T_n$ be n subsets of a infinite field k such that $|T_i| = \infty$ for $1 \leq i \leq n$. Then f can't vanish on $T_1 \times T_2 \times \cdots \times T_n$.

Proof. The case $n = 1$ is clear. The general case follows by induction. $\square$

Corollary 0.2.6 . Suppose $f_1, ..., f_t \in k[[x_1, ..., x_n]]$. Then there exists an automorphism $\phi : R_n \to R_n$ such that $\phi(f_i)$ is regular with respect to x_n for all i.

Proof. Take $f = f_1 \cdots f_t$. And apply theorem 0.2.4 to f. $\square$

Exercise 0.2.7. Let $R_n = \mathbb{C}[[x_1, ..., x_n]]$, $\{f_t\}_{1 \leq t \leq \infty} \in R_n$. Show that there exist a linear automorphism $\phi : R_n \to R_n$ such that $\phi(f_t)$ is regular with respect to x_n for $1 \leq t \leq \infty$.

Proof. By case 1 of theorem 0.2.4, it suffices to choose $(\lambda_{1n}, ..., \lambda_{nn}) \in \mathbb{C}^n$ that sits inside the intersection of all non-vanishing locus of f_t for $1 \leq t \leq \infty$. To start with, we may pick a point $s_1 \in \mathbb{C}^n$ such that f_1 doesn't vanish in the (closed) ball B_1 centered at s_1 of radius ϵ_1. Then pick a point $s_2 \in B_1$ such that f_2 doesn't vanish in the ball B_2 centered at s_1 of radius ϵ_2 with $\epsilon_2 < 1/2\epsilon_1$. By continuing this process, we get an infinite sequence $\{s_i\}$. Take $(\lambda_{1n}, ..., \lambda_{nn}) = \lim_{i \to \infty} s_i$. $\square$

Application 0.2.8.

(i) Suppose $R_n = \mathbb{C}\{x_1, ..., x_n\}$ or $\mathbb{C}[[x_1, ..., x_n]]$. Then R_n is noetherian.
Take an ascending chain of ideals $0 \neq I_1 \subsetneq I_2 \subsetneq ...$ in R_n. Pick $0 \neq f \in I_1$. By applying ϕ, we can assume that f is regular with respect to x_n. By WPT, $R_n/(f)$ is finitely generated over R_{n-1}. Thus is noetherian by the induction hypothesis. Consider the following ascending chain of ideals in $R_n/(f)$,
$$\frac{I_1}{(f)} \subsetneq \frac{I_2}{(f)} \subsetneq ...$$
This chain has to be stable at certain stage. Say $I_n/(f) = I_{n+1}/(f) = ...$ Then $I_n = I_{n+1} = ...$ So R_n is noetherian.

(ii) The ring of entire functions (i.e., convergent everywhere in $\mathbb{C}^n$) is **not** noetherian.
It suffices to prove for the case $n = 1$. Let R be the ring of entire functions. Consider I_n $=\{f \in R |\ f$ vanishes on $2^n\mathbb{Z}\}$. Then $I_n \subset I_{n-1}$. Since $sin(\pi\mathbb{Z}/2^n) \in I_n$ but $sin(\pi\mathbb{Z}/2^n) \notin I_{n-1}$, $I_n \subsetneq I_{n-1}$. So R is not noetherian.

Theorem 0.2.9 . Suppose $R_n = \mathbb{C}\{x_1, ..., x_n\}$ or $\mathbb{C}[[x_1, ..., x_n]]$. Then R_n is a UFD.

Proof. R_n is a noetherian domain. Then R_n is a UFD if and only if every irreducible element of R_n is a prime element. Let f be a irreducible element in R_n. Suppose that $f|uv$ for $u, v \in R_n$. We will show that $f|u$ or $f|v$. Assume $fg = uv$, where $g \in R_n$. Then $(fg)^* = (uv)^*$, i.e., $f^*g^* = u^*v^*$, for $f^*, g^*, u^*, v^* \in R_{n-1}[x_n]$. All of then are monic and all coefficients of lower terms are in $m_{R_{n-1}}$. By induction on n, $R_{n-1}[x_n]$ is a UFD. We claim that f^* is irreducible in $R_{n-1}[x_n]$. If not, $f^* = \alpha(x_n)\beta(x_n)$ and $f^* = x_n^h$ mod $(x_1, ..., x_{n-1})$. $\alpha(x_n), \beta(x_n)$ are monic since f is monic. Thus the coefficient of the lower degree terms of both $\alpha(x_n)$ and $\beta(x_n)$ are in $(x_1, ..., x_{n-1})$. This shows that $\alpha(x_n)$ and $\beta(x_n)$ are not units in R_n, which leads to a contradiction since $f = qf = q\alpha(x_n)\beta(x_n)$. We have proved the claim that f^* is irreducible. To prove the theorem, note that f^* is prime in $R_{n-1}[x_n]$. So $f^*|u^*$ or $f^*|v^*$, which is equivalent to $f|u$ or $f|v$. $\square$

Chapter 1

Cohen's Structure Theorem

1.1 01/25/2022

Proposition 1.1.1 . The following statements are equivalent,

(i) Assume (A,m) is a local ring. $k=A/m$. $F(x)\in A[x]$ is a monic polynomial. $f(x)=im(F(x))\in k[x]$. Suppose $f(x)=g(x)h(x)$ such that $(g(x),h(x))=1$. Then there exist polynomials $G(x),H(x)$ such that $F(x)=G(x)H(x)$ and $g(x)=im(G(x))$, $h(x)=im(H(x))$.

(ii) Assume (A,m) is a local ring. $k=A/m$. $F_1,...,F_n\in A[x_1,...,x_n]$. $f_i=\bar{F_i}\in k[x_1,...,x_n]$ for all $1\leq i\leq n$. If there exists $(\lambda_i,...,\lambda_n)\in k^n$ such that $f_i(\lambda_1,...,\lambda_n)=0$ fpr $1\leq i\leq n$ and $det(\partial f_i/\partial x_j(\lambda_1,...,\lambda_n))\neq 0$. Then we can find $(a_i)_i\in k^n$ such that
(a) $F_i(a_1,...,a_n)=0$.
(b) $a_i=\lambda_i$ mod m.

Definition 1.1.2. Any local ring (A,m) (quasi-local suffices) satisfies the conditions in proposition 1.1.1 is called a *Henselian* ring.

Theorem 1.1.3 (Hensel's lemma)**.** Suppose (A,m) is a complete local ring. Then A satisfies the statement (ii) of proposition 1.1.1, i.e., A is Henselian.

Proof. There exist a lift $(\alpha_1,...,\alpha_n)\subset A$ such that $f_i(\alpha_1,...,\alpha_n)=0$ mod m and $\alpha_i=\lambda_i$ for all i. Note that $|\partial F_i/\partial x_j(x_1,...,x_n)|\neq 0$ mod m. So the matrix $[\partial F_i/\partial x_j(\alpha_1,...,\alpha_n)]_{ij}$ is invertible over A, i.e., there exists B such that $[\partial F_i/\partial x_j(\alpha_1,...,\alpha_n)]_{ij}\cdot B=\mathbf{1}$. Suppose we have constructed $(\alpha_1^r,...,\alpha_n^r)$ satisfying $F_i(\alpha_1^r,...,\alpha_n^r)=0$ mod m^r and $\alpha_i^r=\alpha_i$ mod m for $1\leq i\leq n$. We want to produce $(\alpha_1^{r+1},...,\alpha_n^{r+1})$. Suppose $\alpha_i^{r+1}=\alpha_i^r+\epsilon_i$, $\epsilon_i\in m^r$. By Taylor expansion, $F_i(\alpha_1^{r+1},...,\alpha_n^{r+1})=F_i(\alpha_1^r,...,\alpha_n^r)+\sum_j\partial F_i/\partial x_j(\alpha_1^r,...,\alpha_n^r)\epsilon_j$ mod m^{r+1}. Take $\epsilon_j=-\sum_k B_{ij}F_k(\alpha_1^r,...,\alpha_n^r)$ for $1\leq i\leq n$. Then we have $F_i(\alpha_1^{r+1},...,\alpha_n^{r+1})=0$ mod m^{r+1} and $\alpha_i^{r+1}=\alpha$ mod m. let $a_i=\lim_{r\to\infty}\alpha_i^r$. By the continuity of polynomials, it follows that $F_i(a_1,...a_n)=0$ and $\bar{a}_i=\lambda_i\in k$. $\square$

Definition 1.1.4. Suppose (A,m) is a local ring. k is a field in A. Then A is *equi-characteristic*. In contrary, if $char(A)\neq char(A/m)$, A is of *mixed characteristic*.
The followings are the only cases that are possible:

(i) A and $K = A/m$ are both of characteristic 0.

(ii) A and K are both of characteristic p.

(iii) A has characteristic 0, K has characteristic p.

(iv) A has characteristic p^k, K has characteristic p. (Note that the characteristic of A has to be a power of a prime.)

Theorem 1.1.5 . Suppose (A, m) is a complete local ring containing a field k (thus equi-charateristic). Let $K = A/m$ then A contains a copy of K.

Proof.
Case 1 $char(k) = 0$.
Denote by $\eta : A \to A/m = K$. Let F be the maximal field in A containing k. We will prove that $\eta(F) = K$. If not, we pick an element $\alpha \in K/\eta(F)$. If α is transcendental over $\eta(F)$, we can find $a \in A$ such that $\eta(a) = \alpha$ and a is transcendental over F. Consider the map $\eta : F[a] \to K$. This map is injective because α is transcendental. Thus all nonzero elements in $F[a]$ are units in A. The fraction field $F(a) \subset A$ is strictly larger than F so this contradicts with the maximality of F. If α is algebraic over $\eta(F)$, denote by $g(x)$ the minimal polynomial of α over $\eta(F)$. Since $char(k) = 0$, we have $g'(\alpha) \neq 0$. Let $G(x)$ be a lift of $g(x)$, there is a such that $G(a) = 0$ and $\eta(a) = \alpha$ by Hensel's lemma. It is clear that $G[x]$ is the minimal polynomial of a over F. So $F[a]$ is a field strictly containing F, which contradicts the maximality of F.
Case 2 $char(k) = p$, K is perfect.
Let $F = \bigcap A^{p^n}$. We will prove $\eta(F) = K$. It suffices to prove that for every $x \neq 0 \in K$, there exists a unique $y \in F$ such that $\eta(y) = x$. Suppose $\eta(y_n) = x^{1/p^n}$ for all n, $y_n \in A$. We have $\eta(y_n) = \eta(y_{n+1}^p) = x^{1/p^n}$. So $y_n - y_{n+1}^p = 0 \bmod m$. $(y_n - y_{n+1}^p)^{p^n} = y_n^{p^n} - y_{n+1}^{p^{n+1}} = 0 \bmod m^{p^n}$. The sequence $y_n^{p^n}$ is a Cauchy sequence. Take $y = \lim_{n\to\infty} y_n^{p^n}$. Then $y \in F$ and $\eta(y) = x$. For the uniqueness part, suppose y' is another element in F such that $\eta(y') = x$. Suppose $z_n^{p^n} = y$ and $z_n'^{p^n} = y'$ (exists because $y, y' \in F$). Then $\eta(z_n) = \eta(z'_n) = x^{1/p^n}$, i.e., $z_n - z'_n \in m$. $y - y' = (z_n - z'_n)^{p^n} \in m^{p^n}$ for all n. Since $\bigcap m^n = 0$ (followed by the explicit formula of limits $(..., 0, 0, 0)$), $y - y' = 0$.
Case 3 general case. (01/27/2022)
a) Suppose $m^2 = 0$. So $m^p = 0$ for $p \geq 2$. We observe that A^p is a field. Suppose that $x \in A^p$ and $x = y^p$, $y \in A$. Then $y \notin m$ since $y^p \notin m^p = 0$, y is a unit in A. So $x = y^p$ is a unit in A^p. A^p is a field. Let F be a maximal subfield of A containing A^p. If $\eta(F) \neq K$, let $\alpha \in K - \eta(F)$. Let $a \in A$ be a lift of α. $a^p \in A^p \subset F$. So $\alpha^p \in \eta(F)$, which means α is purely inseparable over $\eta(F)$. The minimal polynomial for α over $\eta(F)$ is $x^p - \alpha^p$. So $x^p - a^p$ is irreducible over F. Then we may conclude that $F[a]$ is a field strictly containing F, which contradicts with the maximality of F. Thus $\eta(F) = K$.
b) In general, if A is a complete local ring, $A = \varprojlim A/m^n$. By induction, we may assume that there is a field $K_n on A/m^n$ such that $\eta_n(K_n) = K_{n-1}$, where η_n is the connecting map in the limit. We want to find a similar K_{n+1} such that $\eta_{n+1}(K_{n+1}) = K_n$. Denote by $R = \eta_n^{-1}(K_n)$. $\eta_n^{-1}(0) = m^n/m^{m+1}$. Note that $\eta_n^{-1}(0)^2 = 0$, $R/\eta_n^{-1}(0) = K_n$. If we can show that R is local, we may apply a) to get the desired field K_{n+1}. Now we show that R is local. Let $x \neq \eta_n^{-1}(0)$ in R. Let $y = \eta(x) \neq 0 \in K_n$. Suppose that $y \cdot u = 1 \in K_n$. Take $v \in R$ such that $\eta(v) = u$.

So $x \cdot v = 1 + w$ in R where $w \in m^n$. Also note that $1 + w$ is a unit in R since, for example, $(1+w) \cdot (1-w) = 1 - w^2 = 1$ mod m^{n+1}. Thus x is a unit in R. R is a local ring. And this finish the proof.

□

1.2 01/27/2022

Corollary 1.2.1 (Cohen structure theorem)**.** Suppose $(R, m, K = R/m)$ is a complete local ring containing a field. Then $A \simeq k[[x_1, ..., x_n]]/I$, i.e. , A is the image of a power series ring over K. More generally, suppose $A \subset R$ is a subring such that $A \to R \to K$ is onto. Then R is the image of $A[[x_1, ..., x_n]]$ for some n.

Proof. By assumption, $R = A + m$. So $m = Am + m^2$, ..., $m^n = Am^n + m^{n+1}$...
$R = A + Am + Am^2 + ... + Am^n + m^{n+1}$.
Take a generating set $(f_1, ..., f_n)$ of m. Consider the map

$$A[[x_1, ..., x_n]] \to R, \quad x_i \mapsto f_i.$$

This map is clearly surjective. □

Corollary 1.2.2 . Suppose $(R, m, K = R/m)$ is a complete *regular* local ring of dimension n containing a field. Then $R \simeq K[[x_1, ..., x_n]]$.

Proof. We may assume that m is minimally generated by a regular system of parameter $(x_1, ..., x_n)$ where $n = dim(R)$. Consider the map

$$B = K[[x_1, ..., x_n]] \xrightarrow{\eta} R, \quad x_i \mapsto x_i.$$

We need to show that the map η is an isomorphism. It is clear that η is surjective. To show the injectivity, note that R is an integral domain. So $\eta^{-1}(0)$ is a prime ideal of R. So $dim(R) = dim(B) - ht(\eta^{-1}(0)) = n$. So $\eta^{-1} = 0$. □

Corollary 1.2.3 . Suppose $(R, m, K = R/m)$ is a complete local ring of dimension n containing a field. Then R is a module finite extension of $K[[x_1, ..., x_n]]$.

Proof. Take a system of parameter $(x_1, ..., x_n)$ of R. By definition, $length(R/(x_1, ..., x_n)R) \leq \infty$. Consider the map

$$A = K[[x_1, ..., x_n]] \xrightarrow{\eta} R, \quad x_i \mapsto x_i.$$

Let m_A be the maximal ideal of A. Since $R/m_A R$ is of finite length over R, it has finite length over A (R and A have the same residue field). By theorem 0.1.1, R is a finitely generated R module. So $dim(A) = n$. If $ker(\eta) \neq 0$, $dim(A/ker(\eta)) < dim(A) = n$. But R is finitely generated over $A/ker(\eta)$, $dim(R) = dim(A/ker(\eta)) = n$. This leads to a contradiction. So η is injective. This completes the proof. □

1.2.1 Mixed characteristic

Theorem 1.2.4 (Cohen structure theorem)**.** Suppose $(R, m, K = R/m)$ is a complete local ring of mixed characteristic p, i.e., $char(K) = p$, $char(R) \neq p$.

(i) p is not nilpotent in R, then R contains a complete discrete valuation ring (dvr) V with maximal ideal pV and $V/pV \simeq R/m = k$.

(ii) p is nilpotent. Let n be the smallest integer such that $p^n \mathbf{1}_R = 0$, then R contains a local ring T of the form V/p^nV where V is a complete dvr. The maximal ideal m_V of V is generated by p and $T/pT \simeq R/m$.

Corollary 1.2.5 . Suppose $(R, m, K = R/m)$ is a complete local ring of mixed characteristic p. Then R is the image of a power series ring $V[[x_1, ..., x_n]]$ where V is a complete dvr such that m_V is generated by p and $V/pV \simeq R/m = K$.

Proof. See the proof of corollary 1.2.1 □

Corollary 1.2.6 . Suppose $(R, m, K = R/m)$ is a complete local ring of mixed characteristic p. $p \cdot \mathbf{1}_R$ is a parameter in R. (This implies p is not nilpotent). Then there exists a complete dvr V with $m_V = (p)$. And given any system of parameter $(p, x_2, ...x_n)$ where $n = dim(R)$, there exists an injective homomorphism

$$A = V[[x_2, ..., x_n]] \to R$$

such that R is a module finite extension of A.

Proof. See the proof of corollary 1.2.3. □

Corollary 1.2.7 . Suppose $(R, m, K = R/m)$ is a complete *regular* local ring of mixed characteristic p. Then

(i) If $p \notin m^2$, $R \simeq V[[x_2, ..., x_n]]$ where $dim(R) = n$

(ii) If $p \in m^2$, $R \simeq S[x_n]/(f(x_n))$, in which $S = V[[x_1, ..., x_{n-1}]]$, $f(x_n)$ is an Eisenstein polynomial over S, i.e. , $f(x_n) = x_n^t + a_1 x_n^{t-1} + a_2 x_n^{t-2} + ... + a_t$ where $a_i \in m_S$ for $1 \leq i \leq t$. $a_t \in m_S - m_S^2$. (Nagata, Local rings).

Example 1.2.8. $\widehat{\mathbb{Z}_p}[[x_1, ..., x_n]]/(p - x_1^2 - x_2^2 - ... - x_n^2)$.

1.3 02/01/2022

We will use proposition 1.3.1 in the proof of case (ii) of corollary 1.2.7.

Proposition 1.3.1 . Suppose that (A, m) is a Henselian local domain. B is also a domain. $A \to B$ is an integral extension. Then

(i) If x is a nonzero nonunit element in B, there exists a polynomial $f(x) = x^t + a_1 x^{t-1} + ... + a_t \in A[x]$ such that $f(x) = 0$, $a_i \in m$ for $1 \leq i \leq t$.

(ii) B is quasi-local.

Proof. (i) Given $x \neq 0 \in B$. Let $f(x) = x^t + a_1x^{t-1} + ... + a_t \in A[x]$ be of minimal degree such that $f(x) = 0$. We claim that $a_i \in m$ for $1 \leq i \leq t$. To prove the claim, take a maximal ideal $q \subset B$ that contains x. $q \cap A = m$ since $A \to B$ is integral. By the equation $x^t + a_1x^{t-1} + ... = -a_t$, $a_t \in A \cap q = m$. Let i be the largest number such that $a_i \notin m$. So in $A/m[x]$, $\bar{f}(x) = x^t + \bar{a}_1x^{t-1} + ... + \bar{a}_ix^{t-i} = x^{t-i}g(x)$, where $(x^{t-i}, g(x)) = 1$. Since A is henselian, this factorization lifts. We get $f(x) = H(x) \cdot G(x)$, where $H(x)$ is monic of degree $t - i$. $G(x)$ is monic of degree i. Since B is a domain, one of $H(x)$, $G(x)$ has to be 0. And this contradicts with the assumption that f is the minimal polynomial.
(ii) Suppose m_1 and m_2 are two different maximal ideals in B. Let $x \in m_1 - m_2$. Since $x^t = -(a_1x^{t-1} + ... + a_t)$ with $a_i \in m$, $x^t \in mB$. $x^t \in m_2$ implies $x \in m_2$ and this leads to a contradiction. □

Proof. proof of corollary 1.2.7.

(i) $p \notin m^2$.
Take a set of regular system of parameters of R, say $(p, x_1, ..., x_{n-1})$. Consider the onto map:

$$S = V[[x_1, ..., x_{n-1}]] \xrightarrow{\eta} R$$

Note that $dim(S) = dim(R) = n$, S is a domain. So $ker(\eta) = 0$.

(ii) $p \in m^2$.
$dim(R/pR) = dim(R) - 1$. Choose a system of parameters $(\bar{x}_1, ..., \bar{x}_{n-1})$ of R/pR such that by adding x_n, $(x_1, ..., x_{n-1}, x_n)$ forms a minimal set of generators of m. Consider the map:

$$S = V[[x_1, ..., x_{n-1}]] \xrightarrow{\eta} R$$

Note that R/m_SR is of finite length (as an S-module) and thus is generated by $1, \bar{x}_n, ..., \bar{x}_n^{t-1}$. So R is an S-module generated by $1, x_n, ...x_n^{t-1}$ (Theorem 0.1.1). Since R is integral over S, S is Henselian, x_n is a root of the polynomial of minimal degree $f(x) = x^t + a_1x^{t-1} + ... + a_t$, $a_i \in m_S$. It suffices to show that $a_t \in m_S - m_S^2$. By assumption $p \in m^2$. So $p = \sum \lambda_i x_i$ where $\lambda_i \in m$. $\lambda_i = \sum_j c_{ij}x_n^j$ where $c_{ij} \in S$ for $j \geq 1$ and $c_{i0} \in m \cap S = m_S$ (R is generated by x_n^j as S-module). By combining these equations, we get $p = b_0 + \sum_{1 \leq i \leq n} b_i x_n^i$, where $b_0 = \sum_{1 \leq i \leq n-1} c_{i0}x_i \in m_S^2$ (Note that the index i here is strictly less than n. This is why we need to combine the equations, rather than just using the fact that R is generated by x_n^i). Now consider the function $g(x) = \sum_{1 \leq i \leq n} b_i x_n^i + b_0 - p$. It is clear that x_n is a root of $g(x)$ and the constant term of $b_0 - p$ is in $m_S - m_S^2$ (since $p \in m_S - m_S^2$). Being the minimal polynomial of x_n, $f(x)|g(x)$. So $a_t|b_0 - p$, $a_t \in m_S - m_S^2$. This completes the proof.

□

Definition 1.3.2. Suppose $(A, m, K = A/m)$ is a complete local ring. Then

(i) If A is equi-characteristic, any copy of $K \subset A$ is called a coefficient field of A.

(ii) If A is of mixed-characteristic $p \geq 0$, a copy of V (resp. $T = V/p^nV$) is called a coefficient ring of A.

Exercise 1.3.3.

1. Suppose $(A, m, K = A/m)$ is local. $char(A) = p \geq 0$. $L = \bigcap A^{p^n}$. Is L a field? (Hint: $L \cap m = ?$).

   Proof. $L \cap m = \bigcap m^{p^n} = 0$. The second equality holds by Krull's intersection theorem. ☐

2. If $A = \mathbb{C}[[x]]$, prove that A has an automorphism ψ such that $\psi(\pi) = \pi + x$, $\psi(x) = x$.

   Proof. ☐

Chapter 2

Zariski's Main Theorem

2.1 02/01/2021

Let $X = \mathbb{C}[x_1, ...x_n]/I = V(I) \in \mathbb{C}^n$. X has Zariski topology and complex topology (denoted by $\tilde{X}$). We can define the sheaf $\mathcal{O}_{\tilde{X}}$ by $\Gamma(U, \mathcal{O}_{\tilde{X}}) = \{f : U \to \mathbb{C} |\ \forall x \in U\ \exists$ open $V \subset \mathbb{C}^n$ and an analytic function $g : V \to \mathbb{C}$ such that $g\big|_{U \cap V} = f\}$.

Note that $\Gamma(U, \mathcal{O}_X) \subset \Gamma(U, \mathcal{O}_{\tilde{X}})$.

For an affine variety X, $(\tilde{X}, \mathcal{O}_{\tilde{X}})$ is called an *analytic set*. If X is a variety over C, $(\tilde{X}, \mathcal{O}_{\tilde{X}})$ is called an *analytic space*.

Definition 2.1.1. Let $(\tilde{X}, \mathcal{O}_{\tilde{X}})$ be a variety over $\mathbb{C}$. $(\tilde{X}, \mathcal{O}_{\tilde{X}})$ is the corresponding analytic space. S is the set of all singular points in X. For $x \in S$ a closed point, take a complex neighborhood U of x. We can write U as the union of its complex connected components $U - U \cap S = V_1 \cup V_2 \cup \ldots \cup V_n$. Then $\overline{V_1}, ..., \overline{V_n}$ are called *branches* of x in X.

Example 2.1.2. $X = V(y^2 - x^2(1 + x))$.

Example 2.1.3. $X = V(z^2 - xy)$. $A = \mathbb{C}[x, y, z]/(z^2 - xy)$.

Exercise 2.1.4. Show that A in 2.1.3 is normal. (Hint: Serre's criterion).

2.2 02/03/2022

There are different versions of Zariski's Main Theorem.

1. (Original version) Suppose that X and X' are varieties over k. X is normal. If $f : X' \to X$ os a birational morphism with finite fibres. Then f is a open immersion.

2. (Topological version) Suppose that X is a normal variety over $\mathbb{C}$. S is the set of all singular points. x is a closed point. Then x has a fundamental system of open (complex) neighborhoods U_i such that $U_i - U_i \cap S$ is connected.

3. (Power series form) Suppose X is a normal variety over k. x is a closed point. Then $\mathcal{O}^{\wedge}_{X,x}$ is a normal domain.

4. (Grothendieck form) Suppose that X and X' are varieties over k. $f : X' \to X$ is a morphism with finite fiber. Then we have a factorization of f, $X' \xrightarrow{f'} Y \xrightarrow{g} X$ where f' is an open immersion and g is a finite morphism.

5. (Connectedness form) Suppose X' and X are varieties over k. $S = X' \to X$ is a birational proper morphism. $x \in X$ is a closed point. Assume that X is normal at x, i.e., $\mathcal{O}_{X,x}$ is normal. Then $f^{-1}(X)$ is connected.

Theorem 2.2.1 (Zariski's Main Theorem due to C. Peskine)**.** Suppose $A \subset B$ are commutative rings such that A is integrally closed in B. And there exists $t_1, ..., t_n \in B$ such that B is integral over $A[t_1, ..., t_n]$. Let $Q \in Spec(B)$ and $P = Q \cap A$ in $Spec(A)$. Suppose that Q is isolated in the fibre over P (i.e., Q is both maximal and minimal in $f^{-1}(P) = Spec(k(p) \otimes_A B)$). Then there exists an element $c \in A - P$ such that $A_c = B_c$.

Proof.
Step 1
In this step, we will show that it suffices to prove the theorem in the case $n = 1$.
Assume that the theorem holds for $n = 1$. Denote by B_0 the integral closure of $A[t_1, ..., t_{n-1}]$ in B. Define $Q_0 = Q \cap B_0$. Consider $B_0 \hookrightarrow B_0[t_n] \hookrightarrow B$. Then Q is isolated over Q_0 because Q is isolated over P. By assumption, there exist $\lambda \in B_0 - Q_0$ such that $B_{0\lambda} = B_\lambda$. We claim that Q_0 is isolated over P. To prove the minimality, assume that $\tau \subset Q_0$ is a prime lying over P. Since $B_{0\lambda} = B_\lambda$. There is a unique prime ideal $\tilde{\tau} \in B$ such that $\tilde{\tau} \cap B_0 = \tau$. So $\tilde{\tau}$ lies over P. This contradicts the minimality of Q. To prove the maximality, assume that $Q_0 \subset S_0$ is a prime lying over P. Consider the maps $k(p) \hookrightarrow k(p) \otimes Q_0 \hookrightarrow k(p) \otimes B/Q$. Since B is integral over $A[t_1, ..., t_n]$, $k(p) \otimes B/Q$ is integral over $k(p)[\bar{t}_1, ..., \bar{t}_n]$. Note that $k(p) \otimes B/Q$ is a field (since Q is isolated). Thus $k(p)[\bar{t}_1, ..., \bar{t}_n]$ is a finite algebraic field extension of $k(p)$. (We are using the fact that $k[x_1, ..., x_n] = k(x_1, ..., x_n)$ if and only if $x_1, ..., x_n$ are algebraic over k, which follows form Noether normalization). Since $k(p) \otimes B_0/Q_0$ is integral over the field $k(p)[\bar{t}_1, ..., \bar{t}_{n-1}]$, $k(p) \otimes B_0/Q_0$ is a field. So $S_0 = Q_0$. By induction on n, we know that there exists $\mu \in A - P$ such that $A_\mu = B_{0\mu}$. Take $\lambda \in B_{0\mu} = A_\mu$. Then $A_{\mu\lambda} = B_{\mu\lambda}$.
Step 2
By step 1, we may assume that $n = 1$. Let $J = Ann_{A[t]} B/A[t]$. Note that J is the largest among the ideals of $A[t]$ that are also ideals of B. Consider the case $J \not\subset Q$, $A \hookrightarrow A[t] = B$. Without loss of generality, by localizing at P, we may assume that A is local. We want to show that $A = B$ in this case. Consider the map $k(p) \to k(p)[\bar{t}]$. If $\bar{t}$ is transcendental over $k(p)$, $\overline{Q}$ cannot be isolated over 0. So $\bar{t}$ is algebraic over $k(p)$. Denote the maximal ideal of A by m. $\bar{t}^r = \overline{a_1}\bar{t}^{r-1} + ... + \overline{a_r} = 0$ in B/mB. Equivalently, $t^r + a_1 t^{r-1} + ... + a_r = \sum_i u_i t^i$, where $u_i \in m$. So $\alpha_{n+1} t^{n+1} + ... + a_0 = 0$ in B. One of α_i for $i \geq 1$ is a unit. If $n = 0$, $\alpha_1 t + \alpha_0 = 0$. Thus $t = \alpha_0/\alpha_1 \in A$. $A = B$. If $n \geq 0$. By multiplying α_{n+1}^n, $\alpha_{n+1} t$ is integral over A. Since A is integrally closed in B, $\alpha_{n+1} t \in A$. If α_{n+1} is a unit in A, $A = B$ follows trivially. If α_{n+1} is not a unit in A but $\alpha_{n+1} t$ is a unit in A, $(\alpha_{n+1} t)^{-1} \alpha_{n+1} = t^{-1} \in A$. If $t^{-1} \in m \subset A$, $t^{-1} \in Q \subset B$, which leads to a contradiction. So $t^{-1} \notin m$. And thus $A = B$. If $\alpha_{n+1} t$ is not a unit of A. We have $(\alpha_{n+1} t + \alpha_n) t^n + ... + \alpha_1 t + \alpha_0 = 0$. Note that one of the coefficients of positive degree terms is a unit. We may repeat the above argument and conclude that $A = A[t] = B$. This finish the proof for the case $J \not\subset Q$ and $A[t] = B$. For the case $J \not\subset Q$ and $A[t] \hookrightarrow B$ is an integral extension

(02/08/2022), denoted by $q = Q \cap A[t]$. Since Q is maximal in the fiber over p and $A[t] \hookrightarrow B$ is integral, q is maximal in the fiber over p in $A[t]$. Also note that $J \not\subset q$. $A[t]_q = B_q$ (recall that $J = Ann_{A[t]}B/A[t]$). So q is also a minimal prime in the fiber over p in $A[t]$. We may apply the previous case and conclude that there exists an element $c \in A - p$. $A_c = A[t]_c$. B_c is integral over $A[t]_c = A_c$. A_c is integrally closed in B_c. So $A_c = B_c$. This finished the proof of the case $J \not\subset Q$. Now it suffices to prove that the case $J \subset Q$ is impossible. In particular, we will show that Q is not isolated in this case.

By proposition 2.3.2, we may assume that B is a finitely generated $A[t]$-module. Let $n \subset B$ be a minimal prime containing J and contained in Q. $m = n \cap A$. Consider the maps $A/m \to A/m[t] \to B/n$. We claim that $\bar{t}$ is transcendental over A/m. To prove the claim, we suppose that $\bar{t}$ is lagebraic over A/m. By localizing at m, we may assume A is local, $J = Ann_{A_m[t]}(B_m/A_m[t])$ (Note that this is not true for B that is not finitely generated). A/m is a field. Consider $A/m \to A/m[\bar{t}] \to B/n$. And $\bar{t}$ satisfies a monic polynomial $\bar{f}(x)$ in A/m. In other words, there exists a polynomial $F(x) \in A[x]$ such that $F(t) \in n$. Since nB_n is a minimal prime containing JB_n. $F(t)^r \in JB_n$. Thus there exists $v \in B - n$ such that $vF(t)^r \in J$. Let $D = A[t, vB] \subset B$. Since A is integrally closed in B, A is integrally closed in $D = A[t, vB]$. Note that $F(t)^r D \subset A[t]$ (since J is an ideal in both $A[t]$ and B). By lemma 2.3.1, $A[t] = D$, i.e., $vB \subset A[t]$. So $v \in J$. But this is a contradiction since $v \in B - n$, $J \subset n$. This shows that $\bar{t}$ is transcendental over A/m. Now we will do the last part of the proof. We have prime ideals $m \subset A$, $n \subset B$ as above. By abusing of notations, we write $A = A/m$ and $B = B/n$. Note that A and B are integral domains. Assume that A^* (resp. $A[\bar{t}]^*$, B^*) are the integral closure of A (resp. $A[\bar{t}]$, B). Let Q^* be the prime ideal lying over Q. Let $p^* = Q^* \cap A^*$. Then Q^* is isolated in the fiber of p^*. Since $A[\bar{t}]$ is a polynomial ring ($\bar{t}$ is transcendental). There doesn't exists any isolated prime in $A[\bar{t}]$ lying over p^*. So Q^* is not isolated in the fiber of p^* since B^* is integral over $A^*[t]$. This completes the proof of the theorem.

□

2.3 02/08/2022

Lemma 2.3.1. Suppose that we have $A \hookrightarrow A[t] \hookrightarrow B$. A is integrally closed in B. The map $A[t] \hookrightarrow B$ is integral. Assume that there exists a polynomial $F(t)$ such that $F(t)B \subset A[t]$. Then $B = A[t]$.

Proof. Take $0 \neq b \in B$. Then $F(t)b = G(t) \in A[t]$. By division algorithm, $G(t) = F(t)q(t) + r(t)$, where $deg(r(t)) < deg(F(t))$. Let $s = b - q(t) \in B$. $F(t)s = r(t)$. $F(t) = (1/s)r(t)$. Thus t is integral over $A[1/s]$. Since s is integral over $A[t]$ and $A[t]$ is integral over $A[1/s]$, s is integral over $A[1/s]$. Thus s is integral over A by clearing the denominators. $s \in A$ since A is integrally closed. Then $b \in A[t]$. $B = A[t]$. □

Proposition 2.3.2 (Reduction to the finitely generated case)**.** Suppose that we have $A \hookrightarrow A[t] \hookrightarrow B$. A is integrally closed in B. The map $A[t] \hookrightarrow B$ is integral. $J = Ann_{A[t]}(B/A[t]) \subset Q$. Then to prove the theorem 2.2.1, it suffices to prove it for finitely generated $A[t]$-module B.

Proof. Denote $q = A[t] \cap Q$. $k = k(p) = A_p/pA_p$. Consider the maps $k \to k[\bar{t}] \to B_p/pB_p = k \otimes_A B$. Then $\bar{q} = (f(\bar{t}))$, i.e., generated by one element. $f(\bar{t}) \in QB_p/pB_p$. $QB_p/pB_p \to$

B_Q/pB_Q. Since QB_Q is the minimal prime containing pB_Q, QB_Q is nilpotent in pB_Q. So $f(\bar{t})^r = 0$ for some r. $F(t)^r \in pB_Q$. $vF(t)^r \in pB$ with $v \in B - Q$. Thus we have the equality $vF(t)^r = \sum_{1\leq i\leq n} p_i b_i$. Consider the ring $\tilde{B} = A[t, v, b_1, ..., B_n] \subset B$. Let $\tilde{Q} = Q \cap \tilde{B}$. Since $\tilde{B}$ is a finitely generated $A[t]$-algebra and B is integral over $A[t]$, $\tilde{B}$ is a finitely generated $A[t]$-module. Now in order to applying the assumption, we show that $\tilde{Q}$ is minimal in the fiber over p (Note that it is maximal due to the integrability). By contradiction, assume that there is a prime ideal $\tau \subset \tilde{Q}$ lying over p. $p\tilde{B} \subset \tau$. So $vF(t)^r \in \tau$ for $v \notin \tilde{Q}$. Then $F(t)^r \in \tau$. $F(t) \in \tau$. So τ lies over q. But this is a contradiction since $A[t] \to \tilde{B}$ is integral. The by assuming the theorem for the finitely generated case. We conclude that $A_C = \tilde{B}_c \to B_c$. Since A_c is integrally closed in B_c, $A_c = B_c$. ☐

In the rest of this section, we will explore the relations between different versions of Zariski's main theorem.

Remark 2.3.3. Theorem 2.2.1 implies [1. original version].
It suffices to argue locally. Assume that $A \to B$ is a map of rings. B is a finitely generated A-algebra. $K(A) = K(B)$ since the map is birational. Then A is integrally closed in B. So there exits $c \in A - p$ such that $A_c = B_c$. $A_p = B_Q$. If Q' is another isolated prime over p. $A_p = B_{Q'}$. For any reduced irreducible separated scheme X, given two distinct points x and y, there is no local ring $\mathcal{O} \subset K(X)$ containing both $\mathcal{O}_{X,x}$ and $\mathcal{O}_{X,y}$. So the fiber of p in B contains only one point. And this shows that $Spec(B) \to Spec(A)$ is an open immersion.

Remark 2.3.4. [3. Power series form] implies [2. Topological form].
Note that $\mathcal{O}_{\tilde{X},x} \hookrightarrow \mathcal{O}^{\wedge}_{X,x}$ is a domain.
Theorem (Gunning and Rossi) If $\mathcal{O}_{\tilde{X},X}$ is a domain, X has a fundamental system of open neighborhoods U_i such that $U_i - U_i \cap S$ is connected.

For [3. Power series form] implies [1. original form], we will prove the following.

Proposition 2.3.5 . Let $(A, m) \subset (A'm')$ be local domains. $K(A) = K(A')$. A is normal. Suppose the followings are true,

(i) A is analytically irreducible, i.e., $A^{\wedge}$ is a domain.

(ii) $dim(A) = dim(A')$.

(iii) length$_{A'}(A'/mA')$ is finite (This imples length$_A(A'/mA')$ is finite by (ii)).

Then $A = A'$.

Proof. (02/10/2022) Denote the inclusion $A \to A'$ by ϕ. Denote the induced map $A^{\wedge} \to A'^{\wedge}$ by $\phi^{\wedge}$. (iii) implies that length$_{A^{\wedge}}(A'^{\wedge}/mA'^{\wedge}) < \infty$. Since $A^{\wedge}$ is complete. $A'^{\wedge}$ is a finitely generated $A^{\wedge}$-module (Theorem 0.1.1). So $dim(A'^{\wedge}) = dim(A^{\wedge}/ker(\phi^{\wedge})) \leq dim(A^{\wedge}) = dim(A) = dim(A') = dim(A'^{\wedge})$. By (i), $A^{\wedge}$ is an integral domain. So $ker(\phi^{\wedge}) = 0$. Take an element $x \in A'$. We will show that $x \in A$. Since $K(A) = K(A')$, $x = b/c$ where $b, c \in A$. Note that x is integral over $A^{\wedge}$ (since $A'^{\wedge}$ is a finitely generated over $A^{\wedge}$). We have $(b/c)^n + \alpha_1(b/c)^{n-1} + ... + \alpha_n = 0$ where $\alpha_i \in A^{\wedge}$. By clearing the denominators, $b^n + \alpha_1 b^{n-1}c + ... + \alpha_n c^n = 0$. So $b^n \in (b^{n-1}c, ..., c^n)A^{\wedge}$. Since the map $A \to A^{\wedge}$ is faithfully flat, $b^n \in (b^{n-1}c, ..., c^n)A$. There exists $a_1, ..., a_n \in A$ such that $x^n + a_1 x^{n-1} + ... + a_n = 0$. Equivalently, x is integral over A. Since $K(A) = K(A')$ and A is normal, $x \in A$.

☐

Remark 2.3.6. [3. Power series form] implies [1. original version] Let $f : X' \to X$ be a birational map with finite fiber. X is a normal scheme. Assume that f takes $x', x'' \in X'$ to $x \in X$. By proposition 2.3.5, $\mathcal{O}_{X,x} = \mathcal{O}_{X',x'}$ and $\mathcal{O}_{X,x} = \mathcal{O}_{X',x''}$. So $x' = x''$. f is an open immersion.

Remark 2.3.7.
Not all integral domains are analytically irreducible. For example, let $A = k[x,y]/(y^2 - x^2(1+x))$. $A^\wedge = k[[x,y]]/(y - x\sqrt{1+x})(y + x\sqrt{1+x})$.

2.4 02/10/2022

2.4.1 Generalization of [4. Grothendieck form]

Theorem 2.4.1 . Let $f : X \to Y$ be a morphism of preschemes. Y is locally noetherian prescheme. If f is proper, $f_*\mathcal{O}_X$ is a coherent $\mathcal{O}_Y$-algebra and there exists a commutative diagram

$$\begin{tikzcd} X \arrow[r, "f'"] \arrow[dr, "f"'] & Y' \arrow[d, "g"] \\ & Y \end{tikzcd}$$

where g is a finite map, f' is proper and $\mathcal{O}_{Y'} = f_*(\mathcal{O}_X)$ (as $\mathcal{O}_Y$-modules). Furthermore, for every $y' \in Y'$, ${f'}^{-1}(y')$ is connected and nonempty.

Corollary 2.4.2 . The number of connected components of $f^{-1}(f(x))$ equals the number of points in $g^{-1}(f(x))$.

Theorem 2.4.3 (Zariski's Main Theorem)**.** In the same setup with theorem 2.4.1, let $X' = \{x' \in X | x' \text{ is isolated in the fiber } f^{-1}(f(x'))\}$. Then X' is open in X and $f'\big|_{X'}$ is an isomorphism with image U' an open set in Y'. Moreover, $f'^{-1}(U') = X'$.

Theorem 2.4.4 (Zariski's Main Theorem)**.** Let $f : X \to Y$ be a quasi-projective morphism. Assume that Y is a scheme. Then X' (the same as in theorem 2.4.3) is isomorphic to an open subset in Y' where Y' is finite over Y. (Applying theorem 2.4.3 to $\mathbb{P}_Y(\mathcal{E}) \to Y$ as the diagram below.)

$$\begin{tikzcd} X \arrow[r, hook, "\text{open}"] \arrow[dr, "f"'] & \mathbb{P}_Y(\mathcal{E}) \arrow[r] \arrow[d, "\text{finite}"] & Y' \arrow[dl, "g"] \\ & Y & \end{tikzcd}$$

Corollary 2.4.5 . Let $X = Spec(B)$, $Y = Spec(A)$ (in fact Y can be any noetherian scheme). Let $f : A \to B$ be a map of commutative rings. B is a finitely generated A-module via this map. Assume that A is noetherian. Denote by q a point in $Spec(B)$. Denote by $p = A \cap q$. If q is isolated in the fiber over p, there exists a module finite extension $Y' = Spec(A')$ of $Spec(A)$ such that $A'_{q'} = A_q$.

2.4.2 Generalization of [5. Connectedness form]

Theorem 2.4.6 (Stein Factorization)**.** Let Y be a quasi-compact scheme. $f : X \to Y$ a separated map of finite type with finite fiber. Then we can factor the map f as follows,

$$\begin{tikzcd}
X \arrow[r, "f'"] \arrow[dr, "f"'] & Y' \arrow[d, "g"] \\
& Y
\end{tikzcd}$$

where f' is an open immersion and g is finite.

Chapter 3

Derivations and Smoothness

3.1 02/10/2022

Definition 3.1.1. Suppose R is a commutative ring. M is an R-module. $D : R \to M$ is called a *derivation* if D is additive and satisfies the Leibniz rule, i.e., $D(b_1b_2) = b_1D(b_2) + D(b_1)b_2$.

Remark 3.1.2. If $A = ker(D)$ is a ring, D is A-linear.

This intrigues us to make the relative definition as follows:

Definition 3.1.3. Suppose R is a commutative A-algebra. M is an R-module. Then $D : R \to M$ is a derivation over A if D is A-linear and D satisfies the Leibniz rule. Note that this implies $D(A) = 0$. Let $Der_A(R, M)$ denote the set of all A derivations of R to M.

Remark 3.1.4. If $char(R) = p > 0$, $D(x^p) = px^{p-1}D(x) = 0$. So $R^p \in ker(D)$. D vanishes on AR^p.

Lemma 3.1.5. R is an integral domain. L is a field contains R. Suppose that $R \to L$ is a derivation. Then D can be extended to a derivation $D' : Q(R) \to L$.

Proof. Define $D(r/s) = (sD(r) - D(s)r)/s^2$. Check that this is well-defined. □

Lemma 3.1.6. If $D : R \to S$ is a derivation. D can be extended to a derivation $D' : R[x_1, ..., x_n] \to S[x_1, ..., x_n]$.

Proof. $D'(f(x_1, ..., x_n)) = \sum a_{i_1,...,i_n} x^{i_1} \cdots x_n^{i_n}$. Take $D'(f(x_1, ..., x_n)) = \sum D(a_1, ..., a_n)x^{i_1} \cdots x_n^{i_n}$. Check that this satisfies the Leibniz rule. □

Proposition 3.1.7 . $Der_{R[x_1,...,x_n]/R}$ is a free $R[x_1, ..., x_n]$-module with basis $\{\partial/\partial x_i, i = 1, ..., n\}$.

Proof. If $\sum f_i \frac{\partial}{\partial x_i} = 0$ for some $f_i \in R[x_1, ..., x_n]$, $\sum f_i \frac{\partial}{\partial x_i}(x_i) = f_i = 0$. So $\frac{\partial}{\partial x_i}$ are linearly independent over A. Take $D \in D_{A/R}$. Consider $D' = D - \sum D(x_i)\frac{\partial}{\partial x_i}$. Note that $D'(x_i) = 0$ for all $1 \le i \le n$. So $D' = 0$. $D = \sum D(x_i)\frac{\partial}{\partial x_i}$. □

Remark 3.1.8. If $f : R \to S$ is a map of commutative rings over A, $Der_A(R, S)$ is an S-module.

Exercise 3.1.9. Let $A = R[x_a]_{a \in I}$ where $|I| = \infty$. $\{D_a = \frac{\partial}{\partial x_a}\} \subset D_{R/A}$ is linearly independent over A. Do they span $D_{R/A}$?

Proof. No. Clearly the derivation δ defined as $\delta(x_a) = 1$ for all $a \in I$ is not in the span. □

3.2 02/15/2022

Definition 3.2.1. Suppose that A is a noetherian commuative ring. A is called pseudo-geometric if for all $p \in Spec(A)$ and all finite field extension L over $k(p)$, the integral closure of A/p in L is a finitely generated A/p-module.

Theorem 3.2.2 (Nagata-Zariski)**.** Let A be a pseudo-geometric dedekind domain. Let R be a local domain essentially of finite type over A (i.e., it is a localization of a finitely generated A-algebra). Then the integral closure R' of R in $Q(R)$ is a finitely generated R-module and R is analytically unramified (i.e. $R^\wedge$ does not have any nilpotent element). If R is normal, then so is $R^\wedge$.

Corollary 3.2.3 (corollary of proposition 3.1.7)**.** Suppose $L = k(x_1, ..., x_n)/k$ has transcendental degree n. $Der_k(L, K) = D_{L/K}$ is a free F-module of dimension n with basis $\frac{\partial}{\partial x_1}, ... \frac{\partial}{\partial x_n}$.

Proposition 3.2.4 . Let $k(x_1, ..., x_n) \subset L$ be a finitely generated field extension over k. Suppose that D is a derivation on k, $D : k \to L$. Given any $u_1, ..., u_n \in L$. Then there exists an extension $D' : k(x_1, ..., x_n) \to L$ such that $D'(x_i) = u_i$ for $1 \leq i \leq n$ if and only if for all $f \in k[x_1, ..., x_n]$ such that $f(x_1, ..., x_n) = 0$, $f^D(x_1, ..., x_n) + \sum u_i \frac{\partial f}{\partial x_i}(x_1, ..., x_n) = 0$. Moreover, such an extension is unique.

Proof. ($\Rightarrow$) Suppose that $f(x_1, ..., x_n) = 0$. $D'f(x_1, ..., x_n) = f^D(x_1, ..., x_n) + \sum u_i \frac{\partial f}{\partial x_i}(x_1, ..., x_n) = 0$. ($\leftarrow$) For $f(x_1, ..., x_n) \in k[x_1, ..., x_n]$. Define $D'(f) = f^D + \sum u_i \frac{\partial f}{\partial x_i}(x_1, ..., x_n) = 0$. Note that $f(x_1, ..., x_n) = g(x_1, ..., x_n)$ implies $(f - g)(x_1, ..., x_n) = 0$ and thus $D'(f) = D'(g)$. D' is well-defined. D' is unique by definition. $\square$

Corollary 3.2.5 .

- (i) Consider $k(x)/k$ where x is transcendental over k. $D : k \to L$ is a derivative. Given any $u \in L$, there exist a unique extension D' of D such that $D'(x) = u$.
- (ii) Suppose that $K = k(S)$ is an transcendental extension of k where S is a set of transcendental generators $(x_\alpha)_{\alpha \in I}$. Given any $(u_\alpha)_{\alpha \in I}$, there exists a unique extension $D' \in Der_k(K, L)$ such that $D'(x_\alpha) = u_\alpha$ for all α. (by Zorn's Lemma).
- (iii) Consider $k(x)/k$ where x is separable over k. Then $k(x) = k[x]/(f(x))$ where $f'(x) \neq 0$. For $u \in L$ such that $f^D(x) + uf'(x) = 0$, i.e. $u = -f^D(x)/f'(x)$. Thus D has a unique extension to $k(x)$.
- (iv) Consider $k(x_\alpha)_{\alpha \in I} = K$ a separable extension of k. Then $D \in Der_k(k, L)$ has a unique extension $D' : K \to L$ such that $D'(x_\alpha) = u_\alpha$ where u_α are uniquely determined. (by Zorn's Lemma).
- (v) Consider $K = k(x)/k$ where x is purely inseparable over k ($char(p) > 0$, for $x \notin k$, $x^{p^n} \in k$). $k(x) = k[x]/(x^{p^n} - a)$. That $u \in L$, there exists extension $D' \in Der_k(K, L)$ of D if and only if $p^n x^{p^n - 1} u - D(a) = 0$, i.e. $D(a) = 0$.

(vi) Consider $k(x_\alpha)_{\alpha\in I} = K$ a purely inseparable extension of k. Suppsoe $D(a_\alpha) = 0$. Then given $(u_\alpha)_{\alpha\in I}$. There exists a unique extension D' of D such that $D'(x_\alpha) = u_\alpha$.

Remark 3.2.6. Note that for any field extension K/k, there is a tower $k \overset{tr}{\hookrightarrow} k(x_\alpha) \overset{sep}{\hookrightarrow} F \overset{insep}{\hookrightarrow} K$.

Theorem 3.2.7 . Suppose that $char(k) = p > 0$. F/k a finite field extension. Assume $[F : K] = p^n$ and $F^p \in k$. Then we have the following,

(i) There exists $x_1, ..., x_n \in F$ such that $F = k(x_1, ..., x_n)$ where $x_{j+1} \notin k(x_1, ..., x_j)$.

(ii) There exists $D_1, ..., D_n \in D_{F/k}$ such that $D_i(x_i) = 1$, $D_i(x_j) = 0$ for $i \neq j$ and rank$(D_{F/k}) = n$. $D_1, ..., D_n$ form a basis of $D_{F/k}$.

Proof. (i) Take $x_1 \in F - k$, $x_1^p \in k$ and $[k(x_1) : k] = p$ (note that $[k(x_1) : k]$ is at most p). Suppose that $k(x_1, ..., x_j)$ have been constructed. Then takle $x_{j+1} \in F - k(x_1, ..., x_j)$. Since $F^p \subset k(x_1, ..., x_j)$.
(ii) Apply corollary 3.2.5 (v) to construct D_i. The proof of the rest of the statement is the same as in proposition 3.1.7. ☐

Remark 3.2.8. $x_1^{i_1} \cdots x_n^{i_n}$ for $1 \leq i_j < p$ form a basis pf F/k. Such a basis is called a *p-basis* of F/k. p-basis satisfies property (ii).

Corollary 3.2.9 . Suppose $char(L) = p$. $D \in Der_k(L, F)$. Note that D vanishes on $K(L^p) \subset L$. Then $K(L^p) = \{x \in L \ such\ that\ all\ D \in D_{L/k}\ vanish\ on\ x\}$.

Proposition 3.2.10 . Suppose that $K = k(x_1, ..., x_n)$ is a finitely generated field extension of k. Then K/k is a separably algebraic extension if and only if 0 is the only k-derivation of k.

Proof. ($\Rightarrow$) done above.
($\Leftarrow$) Let j be the largest integer such that K is not separable over $k(x_1, ..., x_j)$. If x_{j+1} is either transcendental or inseparable over $k(x_1, ..., x_j)$. If x_{j+1} is transcendental over $k(x_1, ..., x_j)$, then there is a nonzero extension D. And D can be extended uniquely to K. This leads to a contradiction. If x_i is inseparable. Then $k(x_1, ..., x_j) \overset{sep}{\hookrightarrow} k(x_1, ..., x_j, x_{j+1}^{p^t}) \overset{purely\ insep}{\hookrightarrow} k(x_1, ..., x_j, x_{j+1}) \overset{sep}{\hookrightarrow} K$. Thus we may choose a nonzero extension for the second inclusion above. ☐

Exercise 3.2.11. Let $K = k(x_1, ..., x_n) = k[x_1, ..., x_n]/(f_1, ..., f_n)$ be an algebraic field extension over k. Then K/k is separable if and only if $det(\frac{\partial}{\partial x_j}(x_1, ..., x_n)) \neq 0$.

Proof. By proposition 3.2.4, $\sum u_i \frac{\partial f_j}{\partial x_i} = 0$. So u_i have to be 0 since the Jacobian is invertible. Then by proposition 3.2.10, K is separable over k. The converse is just similar. ☐

3.3 02/17/2022

Theorem 3.3.1 . Let $K = k(x_1, ..., x_n)$ be a finitely generated field extension of k. Then $\text{rank}(D_{K/k}) = s$ where s is the smallest integer such that there exists $u_1, ..., u_s \in K$ and $K/k(u_1, ..., u_s)$ is a separably algebraic extension.

Proof. If $char(k) = 0$, the assertion follows easily by taking $u_1, ..., u_s$ a transcendental basis of K/k. Assume $char(k) = p$. If K is a separably algebraic extension of $k(v_1, ..., v_t)$, then $D_{K/k} \le t$. Note that there is an tower $k \hookrightarrow k(K^p) \xhookrightarrow{purely\ insep} K$. So $D_{K/k} = D_{K/k(K^p)}$. By the theorem 3.2.7, there exists $u_1, ..., u_s \in K$ such that $K/k(K^p) = k(K^p)(u_1, ..., u_s)$ and $[K : k(K^p)] = p^s$. A basis of derivations is $D_1, ..., D_s \in D_{K/k(K^p)}$. $\text{rank}(D_{K/k}) = s$. Now we need to show that K is separably algebraic over $k(u_1, ..., u_s)$ i.e., we need to show that 0 is the only $k(u_1, ..., u_s)$-derivation of K. Suppose that there exists a derivation $D' : K \to L \in Der_k(K, L)$ such that $D'|_{k(u_1,...,u_s)} = 0$. $D' = \sum D'(u_i)D_i$ since $D' \in D_{K/k(K^p)}$. Thus $D' = 0$. $\square$

Remark 3.3.2. If $char(K) = p$. Let K/k be a finitely generated field extension. Then $K = k(K^p)$ implies that K is a separably algebraic extension over k. However, this is not true if K/k is infinitely generated.

3.3.1 Module of differentials

Let $A \to B$ be a map of commutative rings. The *module of differential* of B over A is a B-module $\Omega_{B/A}$ with (A-)derivation $d : B \to \Omega_{B/A}$ such that for any B-module M, $Hom_B(\Omega_{B/A}, M) \simeq Der_A(B, M)$ ($\star$). In other words, $Der_A(B, -)$ is (co)represented by $\Omega_{B/A}$ in $Mod(B)$.

We may take the standard construction of $\Omega_{B/A}$ as follows. Consider the short exact sequence

$$0 \to I \to B \otimes_A B \xrightarrow{\eta} B \to 0$$

Note that I is generated by $\{1 \otimes b - b \otimes 1 | b \in B\}$ as an ideal. Indeed, if $\eta(\sum b_i \otimes c_i) = \sum b_i c_i = 0$, $\sum b_i \otimes c_i = \sum b_i \otimes c_i - (\sum b_i c_i) \otimes 1 = \sum b_i \otimes 1(1 \otimes c_i - c_i \otimes 1)$.

Definition 3.3.3. $\Omega_{B/A} = I/I^2$. This is a B-module with module structure given by multiplication $b(1 \otimes x - x \otimes 1) = b \otimes x - bx \otimes 1$. The derivation $d : B \to I/I^2$ is defined by $d(b) = \overline{1 \otimes b - b \otimes 1}$ in I/I^2. Note that $d(b_1 b_2) = b_1 d(b_2) + b_2 d(b_1)$.

Given $D \in Der_A(B, M)$, there is $\phi_D : cdb \mapsto cD(b)$, $\phi_D \in Hom_B(\Omega_{B/A}, M)$. This induces an isomorphism between $Der_A(B, M)$ and $Hom_B(\Omega_{B/A}, M)$. We may also define $\Omega_{X/Y} = \mathcal{I}/\mathcal{I}^2$ for schemes X and Y.

There is another way to define $\Omega_{B/A}$. Namely, $\Omega_{B/A} = B \otimes_A B/R$ where R is a left B-module given by $\{1 \otimes bb' - b \otimes b' - b' \otimes b |\ b,\ b' \in B\}$. The differential is defined by $d : B \to \Omega_{B/A}, d(b) = \overline{1 \otimes b}$. Consider the short exact sequence

$$0 \to I \to B \otimes_A B \to B \to 0$$

This sequence admits a splitting $B \to B \otimes_A B$, $b \mapsto b \otimes 1$. So $B \otimes_A B \simeq B \otimes id \oplus I$ as a B-module. In $B \otimes_A B/R$, $0 = 1 \otimes b \cdot 1 - b \otimes 1 - 1 \otimes b = -b \otimes 1$. So $b \otimes 1 \in R$. Then $B \otimes_A B/R \simeq (B \oplus I)/R = I/I^2$.

Example 3.3.4. Note that $\Omega_{B/A}$ is generated by db as a B-module. If B is an A-algebra, $B = A[x_\alpha]_{\alpha\in I}$. Then $\Omega_{B/A}$ is a B-module generated by $\{dx_\alpha\}_{\alpha\in I}$.

Example 3.3.5. If $B = A[x_\alpha]_{\alpha\in I}$, $(x_\alpha)_{\alpha\in I}$ are transcendental elements. Then $\Omega_{B/A}$ is a free B-module generated by $\{dx_\alpha\}_{\alpha\in I}$. It remains to show that $\{dx_\alpha\}_{\alpha\in I}$ are linearly independent. Let $D_\alpha : B \to B$ be the derivation such that $D_\alpha(x_\alpha) = 1$, $D_\alpha(x_\beta) = 0$. Consider the finite sum $\sum f_\alpha dx_\alpha = 0$. Since the is a map of B-modules $\Omega_{B/A} \xrightarrow{\tilde{D_\alpha}} B$ where $\tilde{D_\alpha}(dx_\alpha) = 1, \tilde{D_\alpha}(dx_\beta) = 0$. By applying $\tilde{D_\alpha}$ to the equation, we get $f_\alpha = 0$.

Remark 3.3.6. Suppose $A \to B$ is a map of commutative rings. If $B = A/I$. Then $D_{B/A} = 0$.

Exercise 3.3.7. Consider the commutative square

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d] \\
A' \arrow[r] & B'
\end{tikzcd}$$

There is a natural map $\phi : \Omega_{B/A} \otimes B' \to \Omega_{B'/A'}$, $db \otimes b' \to b'db$. Show that the following statements are true

1. Suppose that $B' = B \otimes_A A'$. Then ϕ is an isomorphism.
2. Suppose that S is a multiplicative subset of B. Then $\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A}$.

Proposition 3.3.8 . If $A \to B \to C$ are ring homomorphisms. We have the exact sequence

$$\Omega_{B/A} \otimes C \xrightarrow{u} \Omega_{C/A} \xrightarrow{v} \Omega_{C/B} \to 0 \quad (\star)$$

Moreover, u has a left inverse if and only if any A-derivation of B into a C-module T can be extended to an A-derivation of C into T.

Proof. $(\star)$ is exact if and only if for all C-module T, $0 \to Hom_C(\Omega_{C/B}, T) \to Hom_C(\Omega_{C/A}, T) \to Hom_C(\Omega_{B/A} \otimes C, T)$ is exact. Or equivalently, if and only if $0 \to Der_B(C, T) \to Der_A(C, T) \to Der_A(B, T)$ is exact. This is straightforward. u splits in $(\star)$ if and only if for all C-module T, $Hom_C(\Omega_{C/A}, T) \to Hom_C(\Omega_{B/A} \otimes C, T) \to 0$ is exact. Equivalently, $Der_A(C, T) \to Der_A(B, T)$ is onto. ☐

Exercise 3.3.9.

1. Suppose that $A \to B$ is a map. $B = B_1 \oplus B_2$. Then $\Omega_{B/A} \simeq \Omega_{B_1/A} \oplus \Omega_{B_2/A}$.
2. $$\begin{tikzcd}
A \arrow[r] \arrow[d] & B_1 \arrow[d] \\
B_2 \arrow[r] & B_1 \otimes_A B_2
\end{tikzcd}$$

   Show that $\Omega_{B/A} \simeq \Omega_{B_1/A} \otimes B \oplus \Omega_{B_2/A} \otimes B$.

Theorem 3.3.10 . Suppose that $A \to B \to C = B/I$. Then we have the following

(i) $I/I^2 \overset{\bar{d}}{\to} \Omega_{B/A} \otimes C \to \Omega_{C/A} \to 0$ is exact, where $\bar{d}(x) = dx \otimes 1$.

(ii) $\Omega_{\frac{B}{I^2}/A} \otimes C \simeq \Omega_{B/A} \otimes C$.

(iii) $\bar{d}$ has a left inverse if and only if in the sequence $0 \to I/I^2 \to B/I^2 \overset{\eta}{\to} B/I = C \to 0$, η has a A-algebra splitting: $C \to B/I^2$.

Proof. (i) $\bar{d}$ is well-defined. For $x, y \in I$, $d(xy) = xdy + ydx$. So $d(xy) = 0 \in C$. For exactness, show that fpr all C-module T, $0 \to Hom_C(\Omega_{C/A}, T) \to Hom_C(\Omega_{B/A}, T) \to Hom_C(I/I^2, T)$ is exact. Equivalently, $0 \to Der_A(C, T) \to Der_A(B, T) \to Hom_B(I, T)$ is exact.

(ii) Note that for any $C = B/I$-module T, $Der_A(B, T) = Der_A(B/I^2, T)$.

(iii) Due to (ii), we can assume that $B = B/I^2$. Suppose that $\bar{d}$ has a left inverse v. Then $D : B \xrightarrow{d \otimes id_C} \Omega_{B/A} \otimes C \overset{v}{\to} I$ is a derivation such that $D\big|_I = id_I$. Take $u = id_B - D$. Note that u is an A-algebra map. Indeed, $u(xy) = xy - D(xy) = xy - xD(y) - yD(x) = (x - D(x))(y - D(y)) = u(x)u(y)$ since $D(x)D(y) \in I^2 = 0$. Moreover, $u\big|_I = 0$. Thus u factor through $\bar{u} : B/I \to B$. It is clear that $\eta\bar{u} = id_C$. Conversely, given a splitting $\bar{u}$ of η. Take $u = B \to B/I \overset{\bar{u}}{\to}\!\!\to B$. $D = u - id_B$. We can show that D is a derivation in $Der_A(B, I) \simeq Hom_B(\Omega_{B/A}, I) \simeq Hom_C(\Omega_{B/A} \otimes C, I)$. The image of D under the isomorphism above is a splitting of $\bar{d}$.

□

Exercise 3.3.11. B is a commutative ring. $\phi : B^m \to B^n$ is a map of B-modules. Show that $coker(\phi) = 0$ if and only if the $n \times n$ minors of ϕ generates the unit ideal of B.

3.4 02/22/2022

Example 3.4.1. Consider the map $A \to B = A[x_1, ..., x_n] \to C = A[x_1, ..., x_n]/(f_1, ..., f_m) = B/I$. By theorem 3.3.10, there is an exact sequence $I/I^2 \overset{\bar{d}}{\to}\!\!\to \Omega_{B/A} \otimes C \to \Omega_{C/A} \to 0$. Recall that $\Omega_{B/A}$ is a free B-module of rank n that is generated by $dx_1, ..., dx_n$. $\bar{d}(f) = \sum_{1 \leq i \leq n} \frac{\partial f}{\partial x_j} dx_j \otimes 1$. Therefore, $\Omega_{C/A} = coker(C^m \overset{J}{\to} C^n)$ where $J = [\frac{\partial f_i}{\partial x_j}]$ is the Jacobian matrix. By exercise 3.3.11, $\Omega_{C/A} = 0$ if and only if the $n \times n$ minors of J generate the unit ideal of C. In particular, if $m < n$, $\Omega_{C/A} = 0$.

Exercise 3.4.2. Let k be a ring. Consider the rings $k \to A \to B = A[x_1, ..., x_n] \to C = B/I$ where $I = (f_1, ..., f_n)$. Determine $\Omega_{C/k}$.

Exercise 3.4.3.

1. K is a finitely generated separably algebraic field extension over k if and only if $\Omega_{K/k} = 0$.

2. Use the results of derivations to conclude about the rank of $\Omega_{K/k}$, K is a finitely generated field extension.

Exercise 3.4.4. Consider field extensions $k \hookrightarrow K \hookrightarrow L$. If L/K is a finitely generated extension. Show that $rank(\Omega_{L/K}) \geq rank(\Omega_{K/k}) + trdeg(L/K)$. The equality holds if and only if L is separably generated over K.

Exercise 3.4.5. Let $A = k[x, y]/(y^2 - x^3)$ where k is a field. Show that $\Omega_{A/k}$ has torsion (as an A-module).

Exercise 3.4.6. Suppose $A \to B_\lambda$ are commutative rings. $B = \varinjlim B_\lambda$. Then $\Omega_{B/A} = \varinjlim \Omega_{B_\lambda/A}$.

Remark 3.4.7. *What we are not covering in this notes.*
If A, B are topological rings. $A \to B$ is a continuous map. $B \otimes_A B$ has the tensor product topology. Then I/I^2 has the induced topology. And $\Omega_{B/A}$ is a topological module over B. $d : B \to \Omega_{B/A}$ is a continuous derivation. However, $\Omega_{B/A}$ is not necessarily Hausdorff. For example, consider $k \to k[[x]]$. $\Omega_{k[[x]]/k}$ is not Hausdorff (in characteristic 0, $rank(\Omega_{k[[x]]/k}) = \infty$) and $\Omega^\wedge_{k[[x]]/k} \simeq k[[x]]$.

3.4.1 Separability

Lemma 3.4.8. Let $k \hookrightarrow K$ be an algebraic field extension. Then the following are equivalent,

(i) K is separable over k.

(ii) $K \otimes_k K'$ is reduced for any field extension K' of k.

(iii) $K \otimes_k K'$ is reduced for any algebraic field extension K' of k.

(iv) $K \otimes_k K'$ is reduced for any finite field extension K' of k.

Proof. (i) ⇒ (ii). Take $x = \sum_{1 \leq i \leq n \lambda_i \otimes u_i} \in K \otimes_k K'$. It is clear that we may assume that K is a finitely generated extension over k. Since K is separable over k, by taking primitive elements y, $K = k(y) = k[Y]/(f(Y))$ where $f'(Y) = 0$. Note that there exists an embedding of the algebraic closure $\overline{K'} \hookrightarrow \bar{k}$. Thus $K \otimes_k K' = K'[Y]/(f(Y)) = K'[Y]/(f_1(Y) \cdots f_n(Y))$ in which $f_i(Y)$ are distinct irreducible polynomials in K'. By Chinese remainder theorem, $K'[Y]/(f_1(Y) \cdots f_n(Y)) = \oplus K'[Y]/(f_i(Y))$. It is reduced since all the summands are fields. (ii) ⇒ (iii) ⇒ (iv) are obvious. For (iv) ⇒ (i). We may assume that K is generated by an algebraic element x over k. If K is not separable, there exists a tower of fields $k \hookrightarrow k(x^{p^t}) \hookrightarrow k(x)$ where the first injection is separable. So there exists a minimal polynomial of x such that $f(x^{p^t}) = 0$. By adjoining p^t-th roots of coefficients of f, we have $g(x)^{p^t} = 0$. Note that it is not possible that all p^t-th roots of coefficients in f are already in k. So K' is strictly larger than k. $g(x) \neq 0 \in K \otimes_k K'$. □

Definition 3.4.9. Let k be a field. Let A be a k-algebra. A is a *separable* k-algebra if $A \otimes_k k'$ is reduced for every algebraic field extension k' over k.

Remark 3.4.10. If A is separable over k, any k-subalgebra of A is separable over k. Conversely, if every finitely generated k-subalgebra is separable over k, A is separable over k.

Lemma 3.4.11. Let K/k be a separably generated field extension. If A is a reduced k-algebra, $K \otimes_k A$ is reduced.

Proof. We may assume that A is a finitely generated k-algebra. Since A is reduced, $0 = p_1 \cap p_2 \cap \cdots \cap p_i$. There is an inclusion $A \hookrightarrow \oplus A/p_i \hookrightarrow \oplus Q(A/p_i) = \oplus k_i$. It suffices to prove that $K \otimes_k k'$ is reduced. For any finitely generated field extension k' over k. Since K is separably generated over k. We can find a set of transcendental basis $\{x_\alpha\}$ such that K is separable over $k(x_\alpha)$. $K \otimes_k k' = (K \otimes_{k(x_\alpha)} k(x_\alpha)) \otimes_k k' \hookrightarrow K \otimes_{k(x_\alpha)} k'(x_\alpha)$. The right hand side is reduced by assumption. □

Corollary 3.4.12 . K is separably generated over k implies that K is a *separable k-algebra*.

Remark 3.4.13. Suppose that k is perfect. Then a k-algebra A is separable if and only if A is reduced.

3.5 02/24/2022

Theorem 3.5.1 . Let $k \to K$ be a finitely generated field extension. The followings are equivalent,

(i) K is separable over k.

(ii) $K \otimes_k k^{1/p}$ is reduced.

(iii) K is separably generated over k.

Proof. (i) $\Rightarrow$ (ii) follows by definition. (iii) $\Rightarrow$ (i) is clear. Now we prove (ii) $\Rightarrow$ (iii). Let $r = trdeg_k(K)$. Suppose that $K = k(x_1, ..., x_r, x_{r+1}, ..., x_n)$ where $x_1, ..., x_r$ is a transcendental basis of K. Assume that $x_{r+1}, ..., x_q$ are separably algebraic over $k(x_1, ..., x_r)$ and $x_{q+1}, ..., x_n$ are not separably algebraic over $k(x_1, ..., x_n)$. Let $y = x_{q+1}$. Denote the minimal polynomial of y by $F(\underline{x}, Y^p) \in k(\underline{x})[Y]$. $F(\underline{x}, Y^p) = \sum a_i(\underline{x})/b_i(\underline{x}) Y^{p^i}$. By clearing the denominators and by Gauss' lemma, we can assume that $F(\underline{x}, Y^p) \in k[\underline{x}, y]$. We claim that for some $1 \leq i \leq r$, $\frac{\partial F}{\partial x_i} \neq 0$. If $\frac{\partial F}{\partial x_i} = 0$ for all i, $F(\underline{x}, y^p) = G(\underline{x}^p, y^p)$. Let $\{a_{i_1 \ldots i_r}\}$ be the coefficient of F. $k' = k(a_{i_1 \ldots i_r}^{1/p}) \hookrightarrow k^{1/p}$. By assumption, $k[x_1, ..., x_r, y]/(F(\underline{x}, y^p)) \otimes k' \hookrightarrow K \otimes_k k^{1/p}$ is reduced. Note that $k[x_1, ..., x_r, Y]/(G(\underline{x}^p, Y^p)) \otimes k = k'[x_1, ..., x_n, y]/(G(\underline{x}, y))^p$. The fact that $G(\underline{x}, y)$ is nilpotent leads to a contradiction. This proves the claim. If $\frac{\partial F}{\partial x_i} \neq 0$, x_i is separably algebraic over $k(x_1, ..., x_{i-1}, x_{i+1}, ..., x_r, y)$. So $k(x_1, ..., x_r, x_{r+1}, ..., x_q, y)$ is separably algebraic over $k(x_1, ..., x_{i-1}, x_{i+1}, x_r, y)$. Note that y is transcendental over k. So we may repeat this process. It follows that k is separably algebraic by this 'changing of transcendental basis' technique. □

Exercise 3.5.2. Let K/k be a finitely generated extension. Suppose that K is not separable over k. Then show that there exists a finite extension k' of k in $k^{1/p}$ such that $K(k')$ is separable over k'.

Proof. Note that it suffices to prove for K/k having one inseparable algebraic generator. Take the same k' as in the proof of theorem 3.5.1. Unlike the proof of the theorem, $\frac{\partial F}{\partial x_i} = 0$ for all i since the contrary shows K/k is separable. Then $K(k') = k'[x_1, ..., x_n, Y]/G(x, Y)$. Thus $K(k')$ is separable over k'. ☐

Corollary 3.5.3 . Suppose that A is separable over k. Then for any extension k' of k. $A \otimes_k k'$ is reduced.

Proof. $A \otimes_k k' \hookrightarrow A \otimes_k \bar{k}' = A \otimes_k \bar{k} \otimes_{\bar{k}} \bar{k}'$. Note that $A \otimes_k \bar{k}$ is reduced and $\bar{k}$ is perfect. So $A \otimes_k \bar{k} \otimes_{\bar{k}} \bar{k}'$ is reduced by remark 3.4.13. ☐

Exercise 3.5.4. Let k be a field. $K = k(x, x^{1/p}, x^{1/p^2}, ...)$. Show that K is separable over k but not separably generated.

Proof. For any $k \hookrightarrow k'$ finite extension of k, we have $K \otimes k' = k'(x, x^{1/p}, x^{1/p^2}, ...)$ is reduced hence K/k is separable.

Note that x is transcendental, $x^{1/p}$ is algebraic over $k(x)$, and x^{1/p^2} is algebraic over $k(x, x^{1/p})\ldots.$ So Trdeg $K/k = 1$. Suppose we take any transcendental basis $y = a_0x + a_1x^1/p + \ldots a_nx^{1/p^n}$. Consider $x^{1/p^{n+1}}$ which satisifes $a_nz^p + a_{n-1}z^{p^2} + \cdots + a_0z^{p^{n+1}} - y = 0$, hence it's inseparable. So we can not find a transcendental basis $\{y\}$ so that K is separable over $k(y)$. ☐

Exercise 3.5.5. Consider $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$. Show that $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is reduced and $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is not noetherian.

Proof. $\mathbb{Q}$ is perfect. So $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is reduced. $0 \to I \to \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \overline{\mathbb{Q}} \to 0$. If $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is noetherian, $\Omega_{\overline{\mathbb{Q}}/\mathbb{Q}}$ is a finite $\overline{Q}$-vector space, i.e., $Der_{\mathbb{Q}}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}})$ is a finite dimensional $\overline{\mathbb{Q}}$ vector space. However, we know that $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is infinite. trying to relate the galois group to the derivatives

If $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is noetherian, $\Omega_{\overline{\mathbb{Q}}/\mathbb{Q}} = \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}/R$ is noetherian. Why does being noetherian imply $\Omega_{\overline{\mathbb{Q}}/\mathbb{Q}}$ is a finite $\overline{Q}$-vector space? ☐

Definition 3.5.6. Consider $k \hookrightarrow K$ a field extension and $char(k) = p > 0$. Then K is called linearly disjoint if

$$K \otimes_k k^{1/p} \xrightarrow{\phi} K(k^{1/p}),\ x \otimes y \mapsto xy$$

ϕ is an isomorphism.

Exercise 3.5.7. $k \hookrightarrow K$ is separable if and only if K, $k^{1/p}$ are linearly disjoint.

Proof. If $k \hookrightarrow K$ is not separable, then take any finite extension $k \subset L \subset K$, L is finite separable over k, by Proposition 3.5, $L \otimes_k k^{1/p}$ is not reduced. Since $L \otimes_k k^{1/p} \hookrightarrow K \otimes_k k^{1/p}$, $K \otimes_k k^{1/p}$ is not reduced thus ϕ can't be an isomorphism.

Suppose $k \hookrightarrow K$ is separable. Note that ϕ is surjective since $K, K^{1/p} \subset Im\phi$. Suppose $x = \Sigma a_i x_i$, $y = \Sigma b_j y_j$ such that $xy = 0$, then $(xy)^p = \Sigma a_i^p x_i^p b_j^p y_j^p = 0$. Then

$$(\Sigma a_i x_i \otimes \Sigma b_j y_j)^p = (\Sigma a_i^p x_i^p b_j^p y_j^p) \otimes 1 = 0$$

since $y_j \in k^{1/p} \Rightarrow y_j^p \in k$. But $K \otimes_k k^{1/p}$ is reduced, hence ϕ is injective. ☐

Definition 3.5.8. Let $A \to B$ be a ring homomorphism. B is called finitely presented over A if there exists a set of generators (as a A-algebra) $x_1, ..., x_n$ over B such that the kernel of the map $\eta : A[x_1, ..., x_n] \xrightarrow{\eta} B$ is a finitely generated ideal of A.

Exercise 3.5.9. Suppose B is finitely presented with respect to a set of generators. Then B is finitely presented with respect to another set of generators.

Definition 3.5.10. Let $A \to B$ be a ring homomorphism. B is called essentially of finite type over A if B is a localization of a finitely presented A-algebra.

Definition 3.5.11. Let $A \to B$ be a ring homomorphism. B is called essentially finite over A if B is a localization of a finitely presented A-module.

Theorem 3.5.12 (Another version of ZMT)**.** Let $(A.m) \hookrightarrow (B, n)$ be a quasi-local extension essentially of finite type. Suppose that B/mB is a finite dimensional vector space over A/m. Then B is essentially finite over A.

Definition 3.5.13. Let $f : A \to B$ be a (resp. finitely presented) ring homomorphism. Then B is called *quasi-unramified* (resp. *unramified*) over A if given any A-algebra C and an ideal I of C such that $I^2 = 0$ and a map $h : B \to C/I$ making the following diagram commute,

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "h"] \arrow[dl, "\tilde{\eta}"] \\
C \arrow[r, "\eta"'] & C/I
\end{tikzcd}$$

there exists *at most one* lift of h such that $\eta \circ \tilde{h} = h$. In other words, the map $Hom_A(B, C) \to Hom_A(B, C/I)$ is injective.

Definition 3.5.14. B is called *quasi-smooth* (resp. *smooth*) if for $I^2 = 0$, $Hom_A(B, C) \to Hom_A(B, C/I)$ is surjective.

Definition 3.5.15. B is called *quasi-étale* (resp. *étale*) if for $I^2 = 0$, $Hom_A(B, C) \to Hom_A(B, C/I)$ is bijective.

Theorem 3.5.16 . $A \to B$ is quasi-étale (resp. étale) if and only if it is quasi-unramified (resp. unramified) and quasi-smooth (resp. smooth).

Proposition 3.5.17 . Let $A \xrightarrow{f} B \xrightarrow{g} E$ be ring homomorphisms. If f, g are quasi-unramified, quasi-smooth, quasi-étale (resp. unramified, smooth, étale), $g \circ f$ is also quasi-unramified, quasi-smooth, quasi-étale (resp. unramified, smooth, étale).

Proposition 3.5.18 . Being quasi-unramified, quasi-smooth, quasi-étale (resp. unramified, smooth, étale) is stable under pushout (tensor product of rings). In particular, if $A \to B$ is quasi-unramified, quasi-smooth, quasi-étale (resp. unramified, smooth, étale), the scheme theoretic fiber $k(p) \to k(p) \otimes_A B$ over $p \in Spec(A)$ is also quasi-unramified, quasi-smooth, quasi-étale (resp. unramified, smooth, étale).

Remark 3.5.19. (Some facts)

(i) Suppose M is a projective (resp. finitely presented) A module. Then $S_A(M)$ (symmetric algebra) is quasi-smooth (resp. smooth) over A. In particular, $A[x_\alpha]_{\alpha\in I}$ is quasi-smooth (smooth) for $|I| < \infty$.

(ii) $A \to B$ is quasi-unramified (unramified) if and only if $\Omega_{B/A} = 0$.
($\Rightarrow$)

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d, "id"] \arrow[dl, shift right, "\phi_1"'] \arrow[dl, shift left, "\phi_2"] \\
B \otimes_A B/I^2 \arrow[r] & B \otimes_A B/I
\end{tikzcd}$$

$\phi_1 : b \mapsto 1 \otimes \bar{b}$, $\phi_2 : b \mapsto \bar{b} \otimes 1$. By assumption, $\phi_1 = \phi_2$. So $1 \otimes b - b \otimes 1 \in I^2$. $I = I^2$ and thus $\Omega_{B/A} = 0$.
($\Leftarrow$) Assume that $\Omega_{B/A} = 0$. Suppose g has two lifts g_1 and g_2. Then $\eta(g_1 - g_2) = 0 \in C/I$. $g_1 - g_2 : B \to I$ is a A-linear derivation of B into I since $I^2 = 0$. So $Hom_B(\Omega_{B/A}, I) \simeq Der_A(B, I) \neq 0$. This leads to a contradiction since $\Omega_{B/A} = 0$.

(iii) $A \to S^{-1}A$ is quasi-étale (étale). Note that $1+a$ for $a \in I$ is a unit in C since $(1+a)(1-a) = 1 - a^2 = 1$.

Remark 3.5.20. (Timmy) The definition of smoothness here coincides with the definition involving the naive cotangent complex (See definition 10.137.1 of The Stacks Project) due to theorem 3.3.10 (iii).

3.6 03/01/2022

Example 3.6.1. Let $k \xrightarrow{i} k(x)$ be a finite separable extension. Then i is a étale morphism. Assume $k(x) = k[x]/(f(x))$, $f'(x) \neq 0$. Consider the diagram

$$\begin{tikzcd}
k \arrow[r] \arrow[d] & k[x]/(f(x)) \arrow[d, "g"] \arrow[dl] \\
C \arrow[r, "\eta"] & C/I
\end{tikzcd}$$

Note that $g(f'(x))$ is a unit in C/I. Since $I^2 = 0$, any preimage of $g(f'(x))$ in C is a unit. Assume $x \mapsto u \in C$, $f'(u)$ is a unit in C. Suppose that $f(u) \neq 0$. By solving the equation $f(u + \delta) = 0$ for $\delta \in I$, we get $\delta = -f(u)/f'(u)$. Then there exists a unique lift $\tilde{g}$ of g such that $\eta \circ \tilde{g} = g$.

Corollary 3.6.2 .

(i) Let $k \hookrightarrow K$ be a finitely generated field extension. Suppose that K/k is separable. Then K/k is smooth.

$$k \xhookrightarrow{tran} k(x_1, ..., x_n) \xhookrightarrow{f.sep} K.$$

$$k \xhookrightarrow{smooth} k[x_1, ..., x_n] \xhookrightarrow{étale} k(x_1, ..., x_n) \xhookrightarrow{étale} K$$

(ii) Let X be a variety over k. k is a perfect field. Then $k \hookrightarrow k(X)$ is separable and $k \hookrightarrow k(X)$ is smooth.

Remark 3.6.3. Ley $k \hookrightarrow K$ be a separable field extension. $K = \varinjlim K_i$ where K_i is finitely generated over k. Then K_i are smooth over k. It is true that K is also smooth over k. We may prove this by using Hochschild homology.

The converse of the above is also true. If K/k is smooth, then K/k is separable. To prove this we need the notion of formal smoothness.

Definition 3.6.4. Consider topoligical rings A, B. Suppose that C and C/I has discrete topology. Consider the following commutative diagram of continuous ring homomorphisms

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "h"] \\
C \arrow[r, "\eta"'] & C/I
\end{tikzcd}$$

where $I^2 = 0$. Then $A \to B$ is called formally unramified (resp. formally smooth, formally étale) if and only if

$$Hom_A^{cont}(B, C) \to Hom_A^{cont}(B, C/I)$$

is injective (resp. surjective, bijective).

Exercise 3.6.5. Suppose B has J-adic topology where J is an ideal of B. Then quasi-unramified (resp. quasi-smooth, quasi-étale) implies formal unramified (resp. formal-smooth, formal-étale).

Proof. It suffices to prove for any ring map $\tilde{g} : B \to C$ a solution of lifting problem, $\tilde{g}$ is continuous. Suppose that $\tilde{g}(b) = c$ and $g(b) = c'$ where $b \in B$, $c \in C$, $c' \in C/I$. Since $g^{-1}(c')$ is open. There exists an neighborhood $b + J^n$ such that $g(b + J^n) = c'$, i.e., $\tilde{g}(J^n) \subset I$. So $\tilde{g}(J^{2n}) \subset I^2 = 0$. Then we have $\tilde{g}(b + J^{2n}) = c$. This proves the continuity of $\tilde{g}$. $\square$

Example 3.6.6. Let $k \hookrightarrow k[[x_1, ..., x_n]]$ be formally smooth with $(x_1, ..., x_n)$-adic topology.

$$\begin{tikzcd}
k \arrow[r, "f"] \arrow[d] & k[x_1, ..., x_n] = B \arrow[r, "h"] & k[[x_1, ..., x_n]] = A \arrow[d, "g"] \\
C \arrow[rr, "\eta"'] & & C/I
\end{tikzcd}$$

Since g is continuous, $\hat{m}^t \subset g^{-1}(0)$. Note that B is quasi-smooth hence formally smooth. So there is a map $\eta' : B \to C$ which makes the diagram commute. Again η' factor through $B/m^s \simeq A/\hat{m}^s$. There is a map $\tilde{\eta} = A \to A/\hat{m}^n \simeq B/m^n \xrightarrow{\eta'} C$ for some large n.

Theorem 3.6.7 . let k be a field. $k \hookrightarrow A$ a noetherian local ring equipped with m-adic topology. Suppose $k \hookrightarrow A$ is formally smooth. Then A is regular local.

Theorem 3.6.8 . If $k \hookrightarrow K$ is smooth, K/k is separable.

Proof. It suffices to prove that for any finite field extension k' of k, $k' \otimes_k K$ is reduced. It is clear that $k' \otimes_k K$ is a finite vector space over K. So $k' \otimes_k K$ is Artinian. It follows that $k' \otimes_k K = A_1 \times \cdots \times A_n$ where A_i are local rings. The assumption that $k \to K$ is smooth implies that $k' \to k' \otimes_k K$ is smooth. Therefore $k' \to A_i$ is smooth. By theorem 3.6.7, A_i is regular local. So each A_i is a domain. And $k' \otimes_k K$ is reduced. ☐

Lemma 3.6.9. (idempotent lifting) Let A be a commutative ring. I is a nilpotent ideal. Then $\{Indempotents\ of\ A\} \xleftrightarrow{bijection} \{Idempotents\ of\ A/I\}$.

Proof. We want to show that every idempotent $\bar{e} \in A/I$ has a unique lift as an idempotent in A. Suppose that e is a preimage of $\bar{e}$ under the map $A \xrightarrow{\eta} A/I$. Let $f = 1 - e$. So $ef \in I$. $(ef)^n = 0$ for some n. Then $1 = (e+f)^{2n+1} = e^n(e^{n+1} + efs) + f^n(f^{n+1} + eft)$. Let $e' = e^n(e^{n+1} + efs)$ and $f' = f^n(f^{n+1} + eft)$. $e'(1-e') = e'f' = e^n f^n (e^{n+1} + efs)(f^{n+1} + eft) = 0$. So e' is also an idempotent. $\eta(e') = \bar{e}^n(\bar{e}^{n-1} + \bar{e}\bar{f}\bar{s}) = \bar{e}^{2n-1} = \bar{e}$. This proves the existence of the lifting. For the uniqueness, suppose that there exists two lifts e, e' of $\bar{e}$. It is clear that $e = e' + u$, $u \in I$. So $e = e^n = (e' + u)^n = e'u'$. Similarly, $e' = ev$. Thus $e = e'u' = e'e'u' = e'e = eve = ev = e$. ☐

Exercise 3.6.10. The map $A \to B_1 \times B_2 \times \cdots \times B_n$ is unramified/smooth/étale if and only if $A \to B_i$ is unramified/smooth/étale for all $1 \leq i \leq n$.

Proof. It follows by checking the lifting diagram componentwise. ☐

Theorem 3.6.11 . Let A be a finitely generated k-algebra. The followings are equivalence,

(i) A is étale over k.

(ii) A is unramified over k.

(iii) $A \simeq k_1 \times k_2 \times \cdots k_n$ where each k_n is a finitely separated extension.

(iv) $\bar{k} \otimes_k A \simeq \bar{k} \oplus \bar{k} \oplus \cdots \oplus \bar{k}$.

Proof. (i) $\Rightarrow$ (ii) and (iii) $\Rightarrow$ (iv) are clear. (ii) $\Rightarrow$ (iii). let p be a prime ideal of A. We claim that p is a maximal ideal. Note that both $k \to A$ and $A \to A/p$ are unramified. Since $A/p \to k(p)$ is étale, $k \to k(p)$ is unramified. And thus $k(p)/k$ is a finite separable extension (see exercise 3.4.3 and remark 3.5.19 (ii)). A/p is a finite dimensional k-subspace of $k(p)$. So A/p is a field (if $s \in A/p$ is not invertible, $A/p[1/s]$ would be infinite dimensional). This proves the claim and equivalently, A is Artinian. A can be written as a product of local rings $A = A_1 \times \cdots \times A_n$ where A_i is unramified over k (see exercise 3.6.10). Let m_i be the maximal ideal of A_i. We will show that $m_i = 0$. We claim that the following exact sequence splits,

$$m_i/m_i^2 \xrightarrow{d} \Omega_{A_i/k} \otimes A_i/m_i \to \Omega_{\frac{A_i}{m_i}/k} \to 0$$

By theorem 3.3.10 (iii), d splits if and only if η splits as a k-algebra map in the following sequence,

$$0 \to m_i/m_i^2 \to A_i/m_i \xrightarrow{\eta_i} A_i/m_i(= L_i) \to 0$$

Since A_i/m_i^2 is a complete local k-algebra ($m_i^2 = 0$), it contains a copy of L_i by theorem 1.1.5. This provides us a splitting in the above sequence. Moreover, since $\Omega_{A_i/k}$ and $\Omega_{\frac{A_i}{m_i}/k}$ are 0, $m_i/m_i^2 = 0$ and thus $m_i = 0$.
(iii) ⇒ (i) by example 3.6.1. It remains to prove (iv) ⇒ (iii). Note that $A \to A \otimes_k \bar{k} = \oplus \bar{k}$ is integral since $k \to \bar{k}$ is integral. By going up, all prime ideal of A are maximal. Since A is reduced, by Chinese remainder theorem, $A \simeq A/m_1 \oplus \cdots \oplus A/m_n$ where m_i is a maximal ideal of A. It is also clear that A (thus A_i) is a finite dimensional k-vector space. Since $K \otimes_k A$ is reduced for all algebraic extension K/k, each A/m_i is a finite separable extension of A. Thus A is étale over k. □

3.7 03/03/2022

Definition 3.7.1. If $B = (A[x]/(F(x)))_g$ and $F'(x)$ is a unit in B, we say that B is a *standard étale extension* over A.

Proposition 3.7.2 . Let $A \to B$ be a map of commutative rings.

(i) $B = (A[x]/(F(x)))_g$ such that $F'(x)$ is a unit in B. Then B is étale over A.

(ii) $B = (A[x_1, ..., x_n]/(F_1(x), F_2(x), ..., F_n(x)))_g$ such that $det(\frac{\partial F_i}{\partial x_j})$ is a unit in B. Then B is étale over A.

Proof. We will prove (ii). It suffices to assume $g = det(\frac{\partial F_i}{\partial x_j})$.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "l"'] & B \arrow[d, "h"] \\
C \arrow[r, "\eta"'] & C/I
\end{tikzcd}$$

Suppose that $h(x_i) = d_i$ in C/I. Then $g(d_1, ..., d_n)$ is a unit. For any $c_1, ..., c_n$ set of lifts of $d_1, ..., d_n$, $g(c_1, ..., c_n)$ is a unit since $I^2 = 0$. Consider the following equations for $\delta_i \in I$,

$$\eta(c_i + \delta_i) = d_i, \quad F_i(c_1 + \delta_1, c_2 + \delta_2, ..., c_n + \delta_n) = 0$$

for all $1 \leq i \leq n$. It follows that $F_i(c_1+\delta_1, c_2+\delta_2, ..., c_n+\delta_n) = F_i(c_1, ..., c_n) + \sum \delta_i \frac{\partial F_j}{\partial x_i}(c_1, ..., c_n)$. Since $g(c_1, ..., c_d) = det(\frac{\partial F_i}{\partial x_j})(c_1, ..., c_d)$ is a unit in C, the above equation has a unique solution for $\delta_1, ..., \delta_n$. Thus $A \to B$ is étale.

□

Remark 3.7.3.

(i) If $\Omega_{B/A}$ is a finitely generated B-module, $\Omega_{B_p/A} = (\Omega_{B/A})_p$ for any prime ideal $p \in Spec(B)$. If moreover $\Omega_{B_p/A} = (\Omega_{B/A})_p = 0$, there exists $s \in B/p$ such that $\Omega_{B_s/A} = 0$. So $A \to B_s$ is unramified. Being unramified is local.

(ii) Let $A \to B$ be a map. Q is a prime ideal in B and $Q \cap A = P$. If $(\Omega_{B/A})_Q = 0$, $\Omega_{B_Q/A} = 0$ and thus $\Omega_{B_Q/A_P} = 0$.

(iii) As in (i), $\Omega_{B_s/A} = 0$. So $\Omega_{B_P/A_P} = 0$. So $\Omega_{B \otimes_A k(p)/k(p)} = 0$, $B \otimes_A k(p) = \oplus k_i$ each k_i is finite separable extension of $k(p)$ (theorem 3.6.11). Every prime in the fiber of p along the map $A \to B_s$ is isolated.

Exercise 3.7.4. let (A, m), (B, n) be local rings. $A \to B$ is a local map essentially of finite type. Then $A \to B$ is essentially unramified if and only if $mB = n$, $A/m \to B/n$ is a finite separable extension.

Proof. Let $A \to B = C_p$ where $p \in \operatorname{spec} C$, C a finitely generated$A$-algebra. Suppose $A \to B$ is essentially unramified, then B is a localization of an unramified A-algebra, say D. $A \to B = D_q$, $q \in \operatorname{spec} D$, $A \to D$ is unramified, $\Omega_{D/A} = 0 \Rightarrow \Omega_{D_q/A} = 0 \Rightarrow \Omega_{C_p/A} = 0 \Rightarrow (\Omega_{C/A})_p = 0 \Rightarrow \exists s \in C \setminus p, \Omega_{C_s/A} = 0$. By replacing C with C_s, we may assume $A \to C$ unramified and C a finitely generated A-algebra. Then $A/m \hookrightarrow C/mC$ is a finitely generated k-algebra. By the previous proposition, $C/mC \cong C_1 \times C_2 \times \cdots \times C_n$, C_i finite separable extension over k. $B/mB = C_p/mC_p = (C/mC)_p \cong C_{ip} \cong C_i$ for some i. Thus $mB = n$ and $B/mB = C_i$ a finite separable extension of k.

Conversely, if $mB = n$, $A/m \hookrightarrow B/mB$ is a finite separable extension. Since $A \to B$ essentially of finite type, $A \to B = C_p$ where C is a finitely generated A-algebra, then $k = A/m \hookrightarrow B/mB = C_p/pC_p$ a finitely generated k-algebra, unramified.

Thus $\Omega_{\frac{(C/mC)_p}{A/m}} = 0 \Rightarrow \exists s \notin p, \Omega_{\frac{(C/mC)_s}{A/m}} = 0$.

From the following,

$$\begin{tikzcd} A \arrow[r] \arrow[d] & C_s \arrow[d] \\ A/m \arrow[r] & C_s/mC_s \end{tikzcd}$$

, $\Omega_{\frac{(C/mC)_s}{A/m}} \cong \Omega_{C_s/A} \otimes_{C_s} C_s/mC_s = 0$. Since $\Omega_{C_s/A}$ is a finitely generated C_s-algebra. By Nakayama's, $\Omega_{C_s/A} = 0$. Thus $A \to C_s$ is unramified, $A \to B$ is essentially unramified.

We may freely drop the word 'essentially' since everything is local. Let $k = A/m$ and $K = B/n$. Then ($\Rightarrow$) by remark 3.7.3. ($\Leftarrow$) $\Omega_{K/k} = \Omega_{B/A} \otimes_A k = 0$. So $\Omega_{B/A} \otimes_A k \otimes_k K = \Omega_{B/A} \otimes_B K = 0$. By the fact that $\Omega_{B/A}$ is a finitely generated B-module and Nakayama's lemma, $\Omega_{B/A} = 0$.

□

Remark 3.7.5. The equivalence condition in exercise 3.7.4 is definition 41.3.1. of The Stacks Project. Nagata's definition only requires $mB = n$ and $A/m \to B/n$ is a separable *algebraic* extension.

Definition 3.7.6. Assume that $A \to B$ is finitely generated/finitely presented. We say that B is unramified over A near Q if there exists $b \in B - Q$, $a \in A - P$ such that $A_a \to B_b$ is unramified. (Note that this is equivalent to the condition $A \to B_b$ is unramified since $A \to A_a$ is unramified anyway).

Note that if $f : A \to B$ is unramified, so is $A/f^{-1}(0) \to B$. Because $B \otimes_A B = B \otimes_{A/f^{-1}(0)} B$.

Lemma 3.7.6. (Corollary of ZMT) Suppose that $A \to B$ is a finitely generated map. $Q \in Spec(B)$. $P = Q \cap A$. Suppose that Q is isolated over P. Then there exists a module finite subextension B' of B and $c' \in B - Q \cap B'$ such that $B'_{c'} = B_{c'}$.

Proof. Let C be the integral closure of A in B. Assume $\tilde{Q} = Q \cap C$. Then Q is isolated over $\tilde{Q}$, C is integrally closed in B and B is a finitely generated C-algebra. By theorem 2.2.1 (ZMT), there exists $c' \in C - \tilde{Q}$ such that $C_{c'} = B_{c'}$. $B = A[x_1, ..., x_n]$ for $x_i = c_i/c^{t_i}$. Take $B' = A[c_1, ..., c_n, c']$. Since $c_1, ..., c_n, c$ are integral over A, B' is a finite extension over A. And $B'_{c'} = C_{c'} = B_{c'}$. ☐

Lemma 3.7.7. Let k be a field. A is a finitely generated Artinian algebra over k. let $m_1, ..., m_n$ be the maximal ideals of A. $A = A_{m_1} \times \cdots \times A_{m_n} = A_1 \times \cdots \times A_n$. Assume that $A_1 = k(\alpha)$ is a finite extension of k. Let $\gamma = (\alpha, 0, 0, ..., 0) \in A$. Let $q = m_1 \cap k[\gamma]$. Then $k[\gamma]_q = A_q = A_{m_1} = A_1$. (Warning: If $A = B \times C$, the prime ideals in A are of the form $P \times C$ or $B \times Q$.)

Proof. content... ☐

Theorem 3.7.8 [SGA 1]**.** If $A \to B$ is a finitely generated map. $Q \in Spec(B)$ and $p = Q \cap A$. B is unramified near Q if and only if there exists $b \in B - Q$ and $a \in A - p$ such that

$$C = A_a[x]/(F(x))_g \to B_b$$

where C is standard étale over A_a, is onto.

Proof. It suffices to show $\Rightarrow$. If we can show that there exists a standard étale algebra over A_P such that

$$A_P[x]/(F(x))_g \to B_{bP}$$

is onto, then there exists $a \in A_P$ such that $A_a[x]/(F(x))_g \to B_{ab}$ is onto. Hence we can assume A is local and $Q \cap A = m$. By lemma 3.7.6, we can assume that B is a finitely generated A-module. So $k = k(p) \to B/mB$ is Artinian. Using a general fact of Artinian rings, $B/mB = L_1 \times L_2 \times L_3 \times \cdots \times L_n$. Then $(B/mB)_Q = L$ is a local ring which is also unramified over k. Thus L is a finite separated field extension of k. (One may argue that the finitely generated condition here is unnecessary because one may pass to a principle localization of B/mB which is already unramified over k. However, we need the finitely generated condition in the following.) By the above, we may assume $B/mB = L \times L_1 \times L_2 \times \cdots \times L_n$ where $L = k(\alpha)$. Let $\gamma = (\alpha, 0, 0, ..., 0)$. Choose a lift θ of γ in B. *We claim that* if $A[\theta]_q = B_Q$ for $q = A[\theta] \cap Q$. This claim will allow us to pass to $A[\theta]$, i.e., generated by a single element. Now we prove the claim. First note that $A[\theta]/mB \cap A[\theta] = k[\gamma] \hookrightarrow B/mB$. By lemma 3.7.7, $k[\gamma]_{\bar{q}} = (B/mB)_q = (B/mB)_Q = L$. By Nakayama's lemma, $A[\theta]_q = B_q$ since $A[\theta]_q \to B_q$ is finite. Thus B_q is local and $B_q = B_Q = A[\theta]_q$. This proves the claim. We may assume that $B = A[\theta]$. It is clear that $A[\theta]/mA[\theta] = k[\theta]$ is a finite dimensional vector space over k. By Nakayama's lemma again, we may assume that $1, \theta, ..., \theta^{t-1}$ generates $A[\theta]$ as an A-module. So $\theta^t = \sum_{1 \le i \le t-1} a_i \theta^i$. Consider the following map,

$$C = A[x]/(F(x)) \xrightarrow{\eta} A[\theta] = B$$

Denote $n = \eta^{-1}(Q)$ where $Q \subset B$. By comparing the dimensions, $C/mC = k[x]/(F(x)) \simeq A[\theta]/mA[\theta]$, i.e., $k \otimes_A C \simeq k \otimes_A B$. So $L \otimes_A C \simeq L \otimes_A B$ where $k \to L = k(\alpha)$. Then $\Omega_{C/A} \otimes_A k = \Omega_{\frac{C}{mC}/k} = \Omega_{\frac{B}{mB}/k} = \Omega_{B/A} \otimes_A k$. Moreover, $\Omega_{C_n/A} \otimes C_n/nC_n \simeq \Omega_{B_Q/A} \otimes B_Q/QB_Q = 0$. By Nakayama, $\Omega_{C_n/A} = 0$ since it is a finitely generated C_n-module. By the exact sequence

$$(F)/(F)^2 \xrightarrow{d} \Omega_{A[x]/A} \otimes C \to \Omega_{C/A} \to 0$$

$\Omega_{C/A} = C/(F'(x))$. Since $(\Omega_{C/A})_n = 0$, $F'(x) \notin n$. Therefor, there exists an onto map

$$(A[x]/F(x))_n \to B_Q$$

such that $F'(x) \notin n$. This proves the theorem by choosing an element in n.

□

3.8 03/08/2022

Theorem 3.8.1 (Structure Theorem for Étale Extensions)**.** Let S be a *finitely presented* R-algebra. The followings are equivalent,

(i) $R \to S$ is étale.

(ii) $R \to S$ is flat and unramified.

(iii) $R \to S$ is flat and $\Omega_{R/S} = 0$.

(iv) For any $Q \in Spec(S)$, $P = Q \cap R$, there exists $b \in S - Q$ and $a \in R - P$ such that $S_b = R_a[x]/(F(x))_g$ where $F(x)$ is monic and $F'(x)$ is a unit.

Proof. (ii) ⇔ (iii) is clear. (iv) ⇒ (iii) by the fact that flatness is a local property.
(iii) ⇒ (iv). By theorem 3.7.8., $R_a[x]/(F(x))_g \xrightarrow{\eta} S_b$ is onto. Let $I = ker(\eta)$, $n = \eta^{-1}(Q)$. We have the exact sequence

$$0 \to I_n \to C_n \to S_Q \to 0$$

Since $R_p \to S_Q$ is flat,

$$0 \to I_n \otimes k(p) \to C_n \otimes k(p) \xrightarrow{\eta} S_Q \otimes k(p) \to 0$$

By the construction of η in theorem 3.7.8, η is an isomorphism. So $I_n/mI_n = 0$. By Nakayama's lemma, $I_n = 0$.
(i) ⇒ (iv). There is a exact sequence,

$$0 \to I \to R_a[x]/(F(x))_g = C \to S_Q \to 0$$

Localizing it at Q, we get

$$0 \to I_n/I_n^2 \to C_n/I_n^2 C_n \to S_Q \to 0$$

Consider the following diagram

$$\begin{tikzcd}
R_p \arrow[r, "\textit{étale}"] \arrow[d] & S_Q \arrow[dl, dashed, "\tilde{\eta}"] \arrow[d, equal] \\
C_n/I_n^2C_n \arrow[r, "\eta"] & S_Q
\end{tikzcd}$$

This gives us a splitting of the exact sequence above. And by theorem 3.3.10 (iii), there is a split exact sequence,

$$0 \to I_n/I_n^2 \to \Omega_{C_n/R} \otimes C_n/IC_n \to \Omega_{S_Q/R} \to 0$$

Since $\Omega_{C_n/R} = 0$ and $\Omega_{S_Q/R} = 0$, $I_n/I_n^2 = 0$. Thus $I_n = 0$.
(iv) $\Rightarrow$ (i). The existence of a lifting is local. $\square$

Exercise 3.8.2. Suppose that R and S are local rings. The map $R \to S$ is flat and essentially étale, i.e., $(R[x]/F(x))_n = S$ where n is a maximal ideal. Then

1. R is reduced if and only if S is reduced.
2. R is regular if and only if S is regular.
3. If R satisfies S_i (for all prime ideal p in R, if $ht(p) \leq i$, R_p is Cohen-Macaulay. If $ht(p) > i$, $depth(R_p) \geq i$), S satisfies S_i.
4. R is Gorenstein if and only if S is Gorenstein.
5. R is normal if and only if S is normal. (Hint: Serre's criterion)

Exercise 3.8.3. B is a normal local ring if and only if $B = B_1 \times \cdots \times B_r$ where each B_i is a normal domain.

3.9 03/10/2022

Let R be a commutative ring. Consider the map $\phi : R^n \to R^m$ where $\phi = (r_{ij})_{n\times m}$. Denote the ideal generated by $t \times t$ minors of ϕ by $I_t\phi$. Then $I_t(\phi \circ \psi) \subset I_t(\phi)I_t(\psi)$. Indeed, $\wedge^t(\phi \circ \psi) = \wedge^t(\phi) \circ \wedge^t(\psi)$.

If $u : R^n \to R^n$ is invertible, $I_t(u) = R$. Indeed, $R = I_t(id) = I_t(uu^{-1}) \subset I_t(u)I_t(u^{-1})$. Moreover, $I_t(u\phi) \subset I_t(u)I_t(\phi) = I_t(\phi) = I_t(u^{-1}u\phi) \subset I_t(u^{-1})I_t(u\phi) = I_t(u\phi)$. So $I_t(u\phi) = I_t(\phi)$. Similarly, $I_t(\phi u) = I_t(\phi)$. In particular, $I_t(\phi)$ is invariant under column operations.

Suppose that R is a local ring. $\phi : R^n \to R^m$. If ϕ does not have all entries in m. Then by row and column operations, ϕ can be transformed into

$$\left[\begin{array}{c|c} I & 0 \\ \hline 0 & W \end{array}\right]$$

where I is the identity matrix and W has all entries in m. It is also clear that $coker(\phi) = coker(W)$.

Exercise 3.9.1. Let (R, m) be a local ring. $\phi : R^m \to R^n$ is a ring map. Then $coker(\phi)$ is free of rank d if and only if $I_{n-d}(\phi) = R$ and $I_{n-d+1}(\phi) = 0$. Moreover, the following are equivalent,

1. The rank of $coker(\phi)$ is $n - m$.
2. $I_m = R$.
3. Some $m \times m$ minor of ϕ is a unit.
4. Some $m \times m$ minor of $\bar{\phi} \neq 0$ in k.
5. rank $\bar{\phi} = m$.
6. There exists a free submodule R^m of as a complement of $coker(\phi)$.

Proof. If $coker(\phi)$ is free of rank d, by considering mod m case, I has to be a $(n-d) \times (n-d)$ matrix. Since $coker(\phi) = coker(W)$, $W = 0$. This proves the first statement. Then it is clear that 1-5 are equivalent. 6 implies 5 by considering mod m. ☐

Exercise 3.9.1 is simple but it plays a very important role in the proof of many theorems below.

Exercise 3.9.2. Let R be a commutative ring. M is a finitely presented R-module. Assume that M_p is free of rank t over R_p. Then there exists $s \in R - p$ such that M_s is a free R_s module of rank t.

Lemma 3.9.2. Let $R \to S$ be a map of commutative rings. Suppose that $R \to T$ is quasi-smooth and $S = T/I$. Then S is quasi-smooth over R if and only if $\eta : T/I^2 \to T/I = S$ has a R-algebra splitting, i.e., $\eta \circ v = Id_S$.

Proof. $(\Rightarrow)$

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & T/I = S \arrow[d, "Id"] \arrow[dl, dashed, "g"'] \\
T/I^2 \arrow[r, "\eta"'] & S
\end{tikzcd}$$

$(\Leftarrow)$

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d] & T \arrow[r, "\eta"] \arrow[dl, dashed, "g"'] & S \arrow[d, "f"] \\
C \arrow[rr, "\lambda"'] & & C/J
\end{tikzcd}$$

In the diagram, $\eta \circ f = \lambda \circ g$. So $g(I) \subset J$. $g(I^2) \subset J^2 = 0$. In other words, g factor through $\bar{g} : T/I^2 \to C$. Take $\tilde{g} = \bar{g} \circ v : S \to C$. ☐

Definition 3.9.3. Let $R \to S$ be finitely presented. $q \in Spec(S)$. $p = q \cap R$. We say that S is *smooth* near q over R if there exists $a \in R - p$ and $b \in S - q$ such that $R_a \to S_b$ is smooth.

Definition 3.9.4. Let $R \to S$ be finitely presented. Q a prime ideal in S. Suppose that we choose a presentation $S = R[x_1, ..., x_n]/I$ where I is finitely generated. Let $\tilde{Q}$ be a lift of Q in $R[x_1, ..., x_n]$. Let $h(Q)$ be the minimal number of generators of $I_{\tilde{Q}}$ in $R[x_1, ..., x_n]_{\tilde{Q}}$.

Theorem 3.9.5 (Jacobian criterion for smoothness)**.** Let $R \to S$ be finitely presented. Q a prime ideal in S. Then S is smooth near Q over R if and only if $(\Omega_{S/R})_Q = \Omega_{S_Q/R}$ is a free S_Q module of rank $n - h(Q)$ if and only if S_Q is essentially smooth over R.

Proof. Replacing S by S_b and R by R_a. We can assume that $R \to S$ is smooth. On the other hand, by lemma 3.9.2, $R \to S$ is smooth if and only if for $T = R[x_1, ..., x_n]$,

$$0 \to I/I^2 \to T/I^2 \to T/I = S$$

splits. Equivalently, by theorem 3.3.10,

$$0 \to I/I^2 \to \Omega_{T/R} \otimes S = S^n \to \Omega_{S/R} \to 0$$

splits. Localizing at Q. it follows that $I_{\tilde{Q}}/I_{\tilde{Q}}^2$ is a free S_Q-module of rank $h(Q)$. So $\Omega_{S_Q/R}$ is free and $rank(\Omega_{S_Q/R}) = n - h(Q)$. The other direction is very similar. $\square$

Example 3.9.6. Let $R = k[x]/(x^p - a)$. Then $\Omega_{R/k} = R$ since $I/I^2 \xrightarrow{d} \Omega_{k[x]/k} \otimes R \to \Omega_{R/k} \to 0$ is exact and $d = 0$.

Theorem 3.9.7 (Structure of Smooth Extension)**.** Let $R \to S$ be a finitely presented ring homomorphism. The following are equivalent,

(i) $R \to S$ is smooth.

(ii) For all $Q \in S$, $P = Q \cap R$, there exists $a \in R - P$ and $b \in S - Q$ such that $R_a \to S_b$ is obtained by first taking a polynomial extension of R_a then taking an étale extension.

(iii) For all $Q \in S$, $P = Q \cap R$, $R_P \to S_Q$ is obtained by first taking a polynomial extension of R_P then taking an étale extension.

Proof. From the proof of theorem 3.9.5, the sequence

$$0 \to I_{\tilde{Q}}/I_{\tilde{Q}}^2 \to S_Q^n \to \Omega_{S_Q/R} \to 0$$

splits. $rank(I_{\tilde{Q}}/I_{\tilde{Q}}^2) = h(Q)$ and $rank(\Omega_{S_Q/R}) = n - h(Q)$. Let $t = h(Q)$. Suppose that $F_1, ..., F_t$ generate $I_{\tilde{Q}}/I_{\tilde{Q}}^2$ minimally. Consider the map

$$I_{\tilde{Q}}/I_{\tilde{Q}}^2 \to \Omega_{T_{\tilde{Q}}/R} \otimes S_{\tilde{Q}}, \quad F_i \mapsto \sum_{1 \le j \le n} \frac{\partial F_i}{\partial x_j} dx_j$$

Denote the Jacobian in S by $J = (\frac{\partial F_j}{\partial x_i})$. Note that $\Omega_{S_Q/R} = coker(J_Q)$. Since the above sequence splits if and only if there exists a $t \times t$ invertible minor of J_Q, we may choose $x_1, ..., x_t$ such that $det(\frac{\partial F_j}{\partial x_i})_{1 \le j \le t, 1 \le i \le t}$ is a unit in S_Q. By delocalizing, we get

$$R_a \to A = R_a[x_{t+1}, ..., x_n] \xrightarrow{\acute{e}tale} A[x_1, ..., x_t]/(F_1, ..., F_t)_{det(\frac{\partial F_j}{\partial x_i})} \to S_b$$

The second map is étale since the Jacobian is invertibe (hence the extension is finite separable). The third map is a localization. $\square$

3.10 03/22/2022

Corollary 3.10.1 . If $R \to S$ is smooth, $R \to S$ is flat.

Proof. This follows from theorem 3.9.7 and the fact that being étale is local property. ☐

Remark 3.10.2. Let (R, m) be a local ring. $dim(R) = d$. The following are equivalent,

(i) R is regular local.

(ii) $G_m(R) = R/m \oplus m/m^2 \oplus m^2/m^3 \oplus \cdots \oplus m^n/m^{n+1} \cdots$. Then there exists $s > 0$ such that $k[x_1, ..., x_s] \simeq G_m(R)$.

(iii) $k[x_1, ..., x_d] \simeq G_m(R)$.

(iv) $pd_R(k) < \infty$.

(v) $gldim_R(A) = sup\, pd_R(M) = dimR < \infty$.

Exercise 3.10.3.

(i) $k[x_1, ..., x_n]_(x_1, ..., x_n)$ is regular local.

(ii) $R = k[x, y, u, v]/(xy - uv)_{(x,y,u,v)}$ is not regular local.

Proof. For (i), apply remark 3.10.2 (ii). For (ii), note that $dim(R) = 3$ while $dim_k(m/m^2) = 4$. ☐

Corollary 3.10.4 . If R is regular local, R is a domain.

Proof. Remark 3.10.2 (ii). ☐

Theorem 3.10.5 . If R is regular local, so is R_p for all prime p in R.

Definition 3.10.6. (R, m) regular local ring of dimension n. Any minimal set of generators $\{x_1, ..., x_n\}$ of m is called a regular system of parameters.

Exercise 3.10.7. Suppose (R, m) regular local ring of dimension n. $\{x_1, ..., x_n\}$ is a subset of m. The following are equivalent,

(i) $x_1, ..., x_n$ form a part of regular system of parameters of R.

(ii) $R/(x_1, ..., x_i)$ is a regular local ring of dimension $dim(R) - i$.

Proof. (i) ⇒ (ii). Note that $(x_{i+1}, ..., x_n)$ generates $m/(x_1, ..., x_i)$ minimally. This implies that $dim(R/(x_1, ..., x_i)) \leq n - i$. On the other hand, $dim(R/(x_1, ..., x_i)) \geq n - i$ by counting the primes. Therefore $dim(R/(x_1, ..., x_i)) = n - i$ and $(x_{i+1}, ..., x_n)$ forms a regular system of parameter of $R/(x_1, ..., x_i)$.
(ii) ⇒ (i). $R/(x_1, ..., x_n)$ is a regular local ring of dimension 0. Thus is a field. So $(x_1, ..., x_n)$ is the maximal ideal of R. ☐

Exercise 3.10.8. Suppose that R is regular local ring. And that $J \subset m$ is an ideal. Then R/J is a regular local ring if and only if $J = (x_1, ..., x_i)$ where $x_1, ..., x_i$ forms a part of regular system of parameters.

Proof. ($\Leftarrow$) follows directly from exercise 3.10.7. ($\Rightarrow$). Suppose R/J is regular, we may pick a regular system of parameters $\{x_1, ..., x_n\}$ of R such that $\{x_1, ..., x_i\}$ are contained in J. Consider $R/(x_1, ..., x_i)$. This ring is regular of dimension $n - i$ by exercise 3.10.7. Moreover, by exercise 3.10.7 again, $x_{i+1,...,x_n}$ is a regular system of parameter of R/J. So $dim(R/(x_1, ..., x_i, x_{i+1})) = dim(R/(J + x_{i+1})) = n - i - 1$. So $dim(R/J) = n - i - 1 + 1 = n - i = dimR/(x_1, ..., x_i)$. Therefore $J = (x_1, ..., x_i)$ since R/J and $R/(x_1, ..., x_i)$ are regular. ☐

Theorem 3.10.9 (Smoothness over algebraically closed fields)**.** Suppose that k is an algebraically closed field. R is a finitely generated k-algebra. Then the following are equivalent,

(i) $k \to R$ is smooth.

(ii) For all maximal ideal q of R, R_q is a regular local ring.

(iii) $\Omega_{R_q/k} = (\Omega_{R/k})_q$ is a free R_q-module of rank $dim(R_q)$.

Proof. (i) $\Rightarrow$ (ii). Suppose $R = k[x_1, ..., x_n]/I$. We want to show that R_q is a regular local ring. By exercise 3.10.8, it suffices to show I_Q is generated by a part of regular system of parameters of $k[x_1, ..., x_n]_Q$. Suppose I_Q is generated by $\{f_1, ..., f_r\}$. Note that in Q/Q^2, $f_i = l_i$ where l_i is the linear term. $f_1, ..., f_r$ form a part of regular system of parameters if and only if $l_1, ..., l_r$ form a linearly independent set of in Q/Q^2. $d(f_i) = \sum \frac{\partial f_i}{\partial x_j} dx_j = \sum \frac{\partial l_i}{\partial x_j} dx_j + ... = \sum a_{ij} dx_j$. ($d : I_Q/I_Q^2 \to \Omega_{k[x_1,...,x_n]/k} \otimes_{k[x_1,...,x_n]} R/q = \oplus_{1 \le i \le n} k$). Since $k \to R$ is smooth, by the proof of Jacobian criterion, $[a_{ij}]$, i.e., d has independent columns. Therefore $f_1, ..., f_r$ form a part of regular system of parameters.

(ii) $\Rightarrow$ (iii). Reverse the argument in the previous step.
(iii) $\Rightarrow$ (i). Suppose that $rank(\Omega_{R_q/k}) = dim(R_q) = n - ht(I_Q)$. Let $t = ht(I_Q)$, $(f_1, ..., f_r)$ generates I_Q minimally ($t \le r$). We will show that $t = r$. Note that $J = [\frac{\partial f_j}{\partial x_i}]_{r \times t}$ has full rank t. Thus by the same argument in the first part of the proof, $f_1, ..., f_t$ form a part of regular system of parameters. Consider the quotient map $k[x_1, ..., x_n]_Q/(f_1, ..., f_t) \to k[x_1, ..., x_n]_Q/I_Q$. Note that both rings are regular and have the same dimension $n - t$. So they are isomorphic. $I_Q = (f_1, ..., f_t)$. Then (i) follows from the Jacobian criterion. ☐

3.11 03/24/2022

Definition 3.11.1. Let k be a field. R is a finitely generated k-algebra. R is called geometrically regular if for all finite field extension k' over k, $k' \otimes_k R$ is regular. Equivalently, for all field extension k' over k, $k' \otimes_k R$ is regular.

Remark 3.11.2. If R is not a k-algebra essentially of finite type. Then we define the geometric regularity by considering finite field extensions over k.

Example 3.11.3. For example, $\mathbb{Q} \to \overline{\mathbb{Q}}$ is not essentially of finite type. And $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is not even noetherian. (See exercise 3.5.5).

Suppose that (R, m) is a regular local ring over k where k is a field of characteristic 0. $K = R/m$. And $[k' : k] < \infty$. Then $A = k' \otimes_k K = A_{m_1} \oplus ... \oplus A_{m_n}$ is Artinian. Since $k' \otimes_k K$ is reduced (lemma 3.4.11), $A = k_1, ..., k_n$ is a field. $mR' = m'_1 \cap ... \cap m'_n$ where $R' = k' \otimes_k R$ and m'_i are the maximal ideals of R' lifting m_i. So the maximal ideal of $R'_{m'_1}$ is generated by $mR'_{m'_1}$. Since R' is a finitely generated R-module, $dim(R_m) = dim(R'_{m'_1})$. By considering the number of minimal generators of m'_1, we may conclude that $R'_{m'_1}$ is also regular. Thus, in characteristic 0, regularity is equivalent to geometric regularity.

Theorem 3.11.4 (Smoothness over a field)**.** Let R be a finitely generated k-algebra. The followings are equivalent,

(i) R is a smooth over k.

(ii) For all field extension L over k, the map $L \to L \otimes_k R$ is smooth.

(iii) There exists algebraic closed field $\bar{k}$ such that $\bar{k} \otimes_k R$ is regular.

(iv) For all field extension L over k, $L \otimes_k R$ is regular, i.e., R is geometric regular over k.

(v) For all maximal ideal Q of $Spec(R)$, $\Omega_{R_Q/k}$ is a free R_Q-module of rank $dim(R_Q)$.

Proof. It is clear that (i) and (ii) are equivalent. (ii) implies (iii) by theorem 3.10.9.
(iii) $\Rightarrow$ (iv) It is enough to show that for any finite field extension L over k, $L \otimes_k R$ is regular. Since $\bar{k}$ is algebraically closed over k, we may assume that L is contained in $\bar{k}$. Since $L \to \bar{k}$ is faithfully flat, $A = L \otimes_k R \to A' = \bar{k} \otimes_k R$ is also faithfully flat. Let Q be a maximal ideal of A, Q' be a prime ideal of A' lying over Q (This is possible because $A \to A'$ is an integral extension). Let $F = A_Q/m$. Since $A'_{Q'}/mA'_{Q'}/m$ is a local ring of dimension 0, $A'_{Q'}/mA'_{Q'} = A'_{Q'}/Q'A'_{Q'} = G$. Then $Tor_i^{A'_{Q'}}(G, G) = 0$ for $i >> 0$ since $A'_{Q'}$ is regular (and hence G has finite projective dimension). Moreover, since $Tor_i^{A'_{Q'}}(G, G) = Tor_i^{A_Q}(F, F) \otimes A'_{Q'} = 0$ for $i >> 0$, $Tor_i^{A_Q}(F, F) = 0$ for $i >> 0$ by the fact that $A_Q \to A'_{Q'}$ is faithfully flat. And this implies that $L \otimes_k R$ is regular for all L.
(iv) $\Rightarrow$ (v) Recall that $A' = \bar{k} \otimes_k R$ is finitely generated over $\bar{k}$ and is regular. Thus the map $\bar{k} \to A'$ is smooth. Note that the map $R \to A'$ is integral. For any maximal ideal $q \subset R$, we can find a maximal ideal $Q \subset A'$ lying over it. By theorem 3.10.9, $\Omega_{A'_Q/\bar{k}}$ is a free A'_Q module of rank $dim(A'_Q) = dim(R_Q)$ (integral extension). On the other hand, $\Omega_{R_q/k} \otimes_{R_q} A'_Q = \Omega_{R_q/k} \otimes_k k' \otimes_{k'} A'_Q = \Omega_{A'_Q/\bar{k}}$. Hence by lemma 3.11.5, $\Omega_{R_q/k}$ is a free R_q-module of rank $dim(R_q)$.
(v) $\Rightarrow$ (i). Let $R = k[x_1, ..., x_n]/I$. Let q be a maximal ideal of R, Q be a lift of q in $k[x_1, ..., x_n]$. Consider the sequence,

$$I_Q/I_Q^2 \to \oplus_{1 \leq i \leq n} R_q \to \Omega_{R_q/k} \to 0 \quad (\star)$$

where by assumption, $\Omega_{R_q/k}$ is free of rank $dim(R_q)$. By tensoring with $A'_{Q'}$, we have

$$I_{Q'}/I_{Q'}^2 \to \oplus_{1 \leq i \leq n} A'_{Q'} \to \Omega_{A'_{Q'}/\bar{k}} \to 0$$

This sequence is split exact since $rank_{A'_{Q'}}(\Omega_{A'_{Q'}}) = rank_{R_q}(\Omega_{R_q}) = dim(A'_{Q'}) = dim(R_q)$. By faithfully flatness, $(\star)$ splits. □

Lemma 3.11.5. Let $A \to A'$ be a faithfully flat local map. Suppose that M is a finitely generated A-module. Then $M \otimes_A A'$ is free of rank n if and only if M is free of rank n.

Proof. Suppose that $M \otimes_A A'$ is free of rank n. Then $(M \otimes_A A') \otimes_{A'} A'/m'$ is an n-dimensional vector space over A'/m'. Note that $dim(M \otimes_A A/m \otimes_{A/m} A'/m') = dim_{A/m}(M/mM) = n$. By Nakayama's lemma, M is generated by n elements. So we have the following exact sequence,

$$0 \to N \to \oplus_{1 \leq i \leq n} Ae_i \to M \to 0$$

Tensoring with A', the following sequence is exact

$$0 \to N \otimes_A A' \to \oplus_{1 \leq i \leq n} A'e_i \to M \otimes_A A' \to 0$$

By assumption, $N \otimes_A A' = 0$. So $N = 0$ by faithfully flatness. □

3.12 03/29/2022

Definition 3.12.1. Let $f : R \to S$ be a finitely presented ring map. S is called *geometrically regular* over R if f is flat and for all $p \in Spec(R)$, $k(p) \to k(p) \otimes_R S$ is geometrically regular. (flat + geometric regular in fibers).

Theorem 3.12.2 (Smoothness over arbitrary rings)**.** Let $f : R \to S$ be a finitely presented ring map. The following are equivalent,

(i) $R \to S$ is smooth.

(ii) f is flat and for all $p \in Spec(R)$. $k(p) \to k(p) \otimes_R S$ is smooth, i.e., $R \to S$ is geometrically regular.

(iii) f is flat and for all maximal ideals q of S, let $p = q \cap R$, $\Omega_{S_q/R}$ is a free S_q-module of rank $dim(S_q/pS_q)$. (flat + has the 'correct' relative dimension).

Proof. (i) ⇒ (ii) is clear by corollary 3.10.1 and theorem 3.11.4.
(ii) ⇒ (iii) by theorem 3.11.4.
(iii) ⇒ (i) Suppose that $S = R[x_1, ..., x_n]/I$. Q is the lift of Q in $R[x_1, ..., x_n]$. Note that the sequence $0 \to I_Q \to R[x_1, ..., x_n]_Q \to S_q \to 0$ is exact. Since S is a flat R-module, S_q is a flat R_p-module. Then $Tor_1^{R_p}(k(p), S_q) = 0$. So by tensoring with $k(p)$, the sequence

$$0 \to I_Q/pI_Q \to k(p)[x_1, ..., x_n]_Q \to S_q/pS_q \to 0$$

is exact. By assumption, $rank_{S_q}(\Omega_{S_q/R}) = rank(\Omega_{\frac{S_q}{pS_q}/R}) = rank(\Omega_{\frac{S_q}{pS_q}/k(p)}) = dim(S_q/pS_q)$. So the sequence comparing the modules of differentials

$$0 \to I_Q/(pI_Q + I_Q^2) \to \bigoplus_n \frac{S_q}{pS_q} \to \Omega_{\frac{S_q}{pS_q}/k(p)} \to 0 \quad (\star)$$

is split exact. Note that $I_Q/(pI_Q + I_Q^2)$ is a free $\frac{S_q}{pS_q}$-module being projective over a local ring. By exercise 3.9.1, $(\star)$ is split exact if and only if the corresponding mod-Q sequence is split exact. And this is true if and only if the following mod-0 sequence is split exact by exercise 3.9.1 again,

$$0 \to I_Q/I_Q^2 \to \bigoplus_n S_q \to \Omega_{S_q/R} \to 0$$

Thus S_q is smooth over R for all maximal ideal q. Since smoothness if a local property, S is smooth over R.

□

Exercise 3.12.3. Let $S = k[x_1, ..., x_n]$. Take $f_1, ..., f_n \in S$ and denote $k[f_1, ..., f_n]$ by R. Suppose that $det(\frac{\partial f_i}{\partial x_j})$ is a unit in k. Show that $R \to S$ is étale (i.e., flat + unramified). Moreover, show that $f_1, ..., f_n$ are algebraically independent over k.

Remark 3.12.4. For a map of varieties $f : X \to Y$ over $\mathbb{C}$. Mumford showed that f is étale if and only if $\tilde{f}$ is a local isomorphism where $\tilde{f}$ is the induced map on the complex analytic space. So exercise 3.12.4 is the analogue of the implicit function theorem.

Exercise 3.12.5. Prove the statement of remark 3.12.4 in *The Red Book in Algebraic Geometry* by Mumford on étale and smooth morphism independently.

Definition 3.12.6. Let $f : (A, m) \to (B, n)$ be a local map. B is essentially of finite type over A. Then B is called a *pointed étale morphism* if

(i) f is étale.

(ii) $A/m \simeq B/n$.

Recall that f is étale if and only if $n = mB$ and $A/m \to B/n$ is a finite separable extension.

Exercise 3.12.7. If $A \to B$ is a pointed étale extension, $\hat{A} \simeq \hat{B}$.

Proof. Consider the natural map $f_i : A/m^i \to B/n^i$. We will show that there is an inverse of f_i for all i. We construct this map inductively. For $i = 1$, take $g_1 : B/n \to A/m$. For $i \geq 2$, consider the following lifting problem,

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d] & B \arrow[d, "g_{i-1}"] \arrow[dl, dashed, "g_i"'] \arrow[ddl, dashed] \\
A/m^i \arrow[r] \arrow[d, "f_i"] & A/m^{i-1} \arrow[d, "f_{i-1}"] \\
B/n^i \arrow[r] & B/n^{i-1}
\end{tikzcd}$$

Both the upper and lower squares have a unique solution g_i and η since $A \to B$ is étale. Note that g_i factor through B/n^i since $g_i(m^iB) = g_i(n^iB)$ vanishes. By abuse of notation, we also call the factor $g_i : B/n^i \to A/m^i$. It is clear that $g_i : B/n^i \to A/m^i$ is compatible with $g_{i-1} : B/n^{i-1} \to A/m^{i-1}$ by tracing the upper square. Moreover, $f_i \circ g_i : B/n^i \to B/n^i$ is the identity map by the uniqueness of η. This shows that g_i is a compatible system of inverse of f_i. And in particular, $\hat{A} \simeq \hat{B}$.

□

Chapter 4

Henselian Rings and Henselization

4.1 03/29/2022

Definition 4.1.1. (Henselian local rings) See proposition 1.1.1.

Definition 4.1.2. S is a *semilocal ring* if it has only finitely many maximal ideals. We say that S *decomposes* if $S = S_1 \times S_2 \times \cdots \times S_n$ where S_i is a local ring. Note that in this case, if $m_1, ..., m_n$ are the maximal ideals of S, $S_i = S_{m_i}$.

Let (R, m) be a local ring. Suppose that $R \to S$ is a module finite extension. Then S is semi-local. Indeed, let $k = R/m$. Then S/mS is a finite dimensional k-vector space. So S/mS is Artinian. $S/mS = (S/mS)_{m_1} \times \cdots \times (S/mS)_{m_n}$. So $m_1, ..., m_n$ are the only maximal ideals of S.

Suppose that $S = S_1 \times \cdots \times S_n$. Then $S_i/mS_i = (S/mS)_{m_i}$. This shows that S_i is local. Therefore, to show that S decomposes, it suffices to show that then idempotents associated to $(S/mS)_{m_1}$ lifts to orthogonal idempotents in S.

Consider a special case $S = R[x]/(F(x))$. Let $k = R/m$. $S/mS = k[x]/(f(x)) = \oplus k[x]/(g_i(x))$ where g_i are the coprime factors of $f(x)$. In this case, we have

Proposition 4.1.3 . S decomposes if and only if $F = G_1 \cdots G_r$ where $\overline{G_i} = g_i$.

Proof. ($\Rightarrow$) This direction is clear by Nakayama's lemma.
($\Leftarrow$) Suppose that $S = S_1 \times \cdots \times S_r$. Then $S_i/mS_i = k[x]/((g_i(x)))$ where $deg(g_i(x)) = d_i$. So $\{1, x, ..., x^{d_i-1}\}$ form a basis of S_i/mS_i. Then S_i is generated by $\{1, x, ..., x^{d_i-1}\}$ as an R-module (by Nakayama). $x^d = \sum_{i=0}^{d_i-1} r_i x^i$ in S_i. Let $G_i(x) = x^d - \sum_{i=0}^{d_i-1} r_i x^i$. Consider the map $R[x] \to S - i, x \mapsto x$. We have short exact sequence,

$$0 \to L_i \to R[x]/G_i(x) \to S_i \to 0$$

Note that S is a free R-module. Then S_i is also a free R-module since it is projective over the local ring R. In particular, S_i is R-flat. $Tor_1^R(S_i, R/m) = 0$. So by tensoring with R/m,

$$0 \to L_i/mL_i \to k[x]/\overline{G_i}(x) \to S_i/mS_i \to 0$$

The quotient map above is actually an isomorphism. So $L_i = mL_i$. $L_i = 0$. This implies that $R[x]/G_i(x) \simeq S_i$. And thus $\overline{G_i}(x) = g_i(x)$. Let $H(x) = G_i(x)...G_r(x)$. Then $H(x) = 0 \in S$. $H(x)$ is monic and have the same degree with $F(x)$. So $F(x) = H(x)$. This completes the proof. $\square$

4.2 03/31/2022

Theorem 4.2.1 (Henselian local rings)**.** Let (R, m, k) be a quasi-local ring. The following are equivalent,

1. R is Henselian.
2. Every module finite extension S of R decomposes.
3. Every module finite free extension S of R decomposes.
4. Let $S = R[x]/(F(x))$. F is monic in $R[x]$. S decomposes.
5. Suppose that $F(x)$ is monic in $R[x]$. If $f(x) = F(x)\ mod\ m$ has a simple root λ in k, $F(x)$ has a root α in R such that $\alpha\ mod\ m = \lambda$.
6. Let $f : R \to S$ be a local map between local rings. Suppose that S is a pointed étale extension of R. Then f is an isomorphism.
7. For all $n > 0$, given that $F_1, ..., F_n \in R[x_1, ..., x_n]$. If there exists $(\lambda_1, ...\lambda_n) \in k^n$ such that $f_i(\lambda_1, ..., \lambda_n) = 0$ and $det(\frac{\partial f_i}{\partial x_j})(\lambda_i, ..., \lambda_n) \neq 0$. Then $F_1 = F_2 = ... = F_n = 0$ has a unique root $(\alpha_1, ..., \alpha_n) \in R^n$ such that $\alpha_i = \lambda_i\ mod\ m$.

Proof. content... ☐

4.3 04/05/2021

Exercise 4.3.1.

1. Let R be a quasi-local integral domain. S is a domain. Let $R \to S$ be a integral extension. We proved in proposition 1.3.1 that S is quasi-local. Conversely, suppose that S is a quasi-local integral domain. $R \to S$ is integral and S is local. Then show that R is Henselian.
2. Let R be a quasi-local Henselian domain. $R \to S$ is integral. Then show that S is also Henselian.
3. Let (R, m) be a quasi-local Henselian domain. $R \to S$ be a local map. Suppose that S is quasi-local and S is integral over R. Then S is Henselian.
4. Let (R, m) be a local normal domain. $p \in Spec(R)$ and $p \neq m$. Then R_p is not Henselian.
5. Prove that the convergent power series ring $\mathbb{C}\{x_1, ..., x_n\}$ is Henselian. (Hint: use either WPT or inverse function theorem).

4.3.1 Henselization

Recall that for a local ring (R, m), $R \to \hat{R}$ is injective and faithfully flat. For a quasi-local ring, the map exists but may fail to be injective or faithfully flat.

Here are some facts about the henselian local rings and pointed étale extension.

1. Consider the following diagram of quasi-local rings

$$\begin{tikzcd}
R \arrow[r, "p.e.n"] \arrow[d] & S \arrow[d] \arrow[dl, dashed, "g"] \\
T \arrow[r, shift right] & (T \otimes_R S)_{m_T \otimes_R S + T \otimes_R m_S} \arrow[l, dashed, shift right, "h"']
\end{tikzcd}$$

   Suppose that the map $R \to S$ is a pointed étale extension and T is Henselian. Then h is a pointed étale extension and hence an isomorphism by theorem 4.2.1. So g exists. Moreover, $Hom_R(S, T) \simeq Hom_T((T \otimes_R S)_n, T) \simeq Hom_T(T, T) = id$. So h is unique.

2. The family of pointed étale extensions of (R, m) forms a directed family.

$$\begin{tikzcd}
R \arrow[r, "p.e.n"] \arrow[d, "p.e.n"] & S_1 \arrow[d, "p.e.n"] \\
S_2 \arrow[r, "p.e.n"] & (S_1 \otimes_R S_2)_{m_{S_1} \otimes_R S_2 + S_2 \otimes_R m_{S_1}}
\end{tikzcd}$$

3. Consider the diagram

$$\begin{tikzcd}
R \arrow[r, "p.e.n"] \arrow[d, "p.e.n"'] & S \arrow[dl, dashed, "g"] \\
T &
\end{tikzcd}$$

   There exists at most one local R-algebra map $S \to T$ making the diagram commute.
   (Noetherian case)

$$\begin{tikzcd}
R \arrow[r, "p.e.n"] \arrow[d, "p.e.n"'] & S \arrow[dl, shift right, "\phi_1"'] \arrow[dl, shift left, "\phi_2"] \arrow[d, "f"] \\
T \arrow[r, "g"] & \hat{R}
\end{tikzcd}$$

   f and g are the unique maps in part 1. They are injections since $\hat{S} = \hat{R} = \hat{T}$. So $\phi_1 = \phi_2$.
   (Non-noetherian case)

$$\begin{tikzcd}
R \arrow[r, "p.e.n"] \arrow[d] & S \arrow[d] \arrow[dl, shift right, "\phi_1"'] \arrow[dl, shift left, "\phi_2"] \\
T/m_T^2 \arrow[r] & T/m_T = S/m_S = R/m_R
\end{tikzcd}$$

   $\phi_1 - \phi_2$ is a map $S \to m_T/m_T^2$. Check that $\phi_1 - \phi_2$ is a R-derivation. Since $\Omega_{S/R} = 0$, $Hom(\Omega_{S/R}, m_T/m_T^2) = Der_R(S, m_T/m_T^2) = 0$. So $\phi_1 = \phi_2$. Not Proved Yet.

Definition 4.3.2. The Henselization of R, denoted by R^h, is defined by $R^h = \varinjlim_{S\ p.e.n/R} S$.

Some properties of henselization.

1. R^h is quasi-local. $R^h/mR^h = \varinjlim S/mS = k$. Thus $R \to R^h$ is a flat local unramified extension. (not étale because R^h is not finitely generated in general.)
2. R^h admits a unique R-module map to $\hat{R}$ such that $\hat{R}^h = \hat{R}$. Note that if $R \to S$ is a pointed étale extension, $\hat{R} = \hat{S}$.