MATH 918 LECTURE NOTES, SPRING 2023

Lecture of January 24, 2023

1. Derivations

1.1. **Definition and first examples.** Our goal will be to consider derivatives algebraically.

The usual notion of derivative of a function is a rule that turns certain real-valued or complex-valued functions into other real-valued or complex-valued functions as follows: at a given point x, we take

$$f'(x) = \lim_{y \to x} \frac{f(y) - f(x)}{y - x}.$$

This certainly gives us derivative functions on some rings, for example, the ring of infinitely-differentiable functions on $\mathbb{R}$:

$$\mathcal{C}^\infty(\mathbb{R}) \xrightarrow{\frac{d}{dx}} \mathcal{C}^\infty(\mathbb{R})$$

or the ring of *entire functions*, i.e., *holomorphic*, a.k.a. complex-differentiable, functions on the complex plane:

$$\mathrm{Holo}(\mathbb{C}) \xrightarrow{\frac{d}{dx}} \mathrm{Holo}(\mathbb{C}).$$

Neither of these is the sort of ring that we usually consider in commutative algebra. In particular, neither is Noetherian.

Using our familiar rules of differentiation, we might recall that the derivative of a polynomial is a polynomial, and the derivative of a rational function is a rational function. So, we get derivatives on much more manageable rings:

$$\mathbb{R}[x] \xrightarrow{\frac{d}{dx}} \mathbb{R}[x], \quad \mathbb{R}(x) \xrightarrow{\frac{d}{dx}} \mathbb{R}(x), \quad \mathbb{C}[x] \xrightarrow{\frac{d}{dx}} \mathbb{C}[x], \quad \mathbb{C}(x) \xrightarrow{\frac{d}{dx}} \mathbb{C}(x).$$

To unlock some of the applications of derivatives, we would like to be able to do this as much as possible over arbitrary rings. We might be optimistic about doing this for arbitrary polynomial rings at least, given the examples above. To do it, we certainly must get rid of this limit approach, since moving around in fields like $\mathbb{Q}$ or $\mathbb{F}_p$ we certainly will miss out on lots of limits. Of course, when we actually compute the derivative of a real or complex polynomial, we don't consider the limit definition anymore, but instead use rules of derivative. Namely, we have a sum rule, a scalar rule, a product rule, a quotient rule, and a power rule, and knowing all of these, we easily and limitlessly compute derivatives of any polynomial or rational function over $\mathbb{R}$ or $\mathbb{C}$. Since the quotient rule and power rule (mostly) follow from the product rule, we will hone in on the first three for our definition of algebraic notion of derivative.

So, our first approximation of the definition of *derivation*, our notion of derivative, is a function ∂ from a ring R to itself that satisfies a sum rule, a scalar rule, and a product rule:

- $\partial(r + s) = \partial(r) + \partial(s)$ for all $r, s \in R$,
- $\partial(cr) = c\partial(r)$ for all $r \in R$ and c "constant???",
- $\partial(rs) = r\partial(s) + s\partial(r)$ for all $r, s \in R$.

There is something we must change ("constant???") and something else less clear we can/should change. Let's be openminded. If R is a ring, let's let our constants be any reasonable set of elements of R: any subring A of R. But let's be even more openminded. Look at the right-hand sides above. To make sense of

them we have to be able to add our outputs together and multiply them by ring elements, but we don't have to multiply them with each other. They don't have to live in R—they just have to live in an R-module.

Definition 1.1. Let R be a ring and M be an R-module. A *derivation* from R to M is a function $\partial : R \to M$ such that

- $\partial(r+s) = \partial(r) + \partial(s)$ for all $r, s \in R$,
- $\partial(rs) = r\partial(s) + s\partial(r)$ for all $r, s \in R$.

If R is an A-algebra, then ∂ is a *derivation over* A or an *A-linear derivation* if in addition

- $\partial(ar) = a\partial(r)$ for all $a \in A$ and $r \in R$.

Remark 1.2. Recall that R is an A-algebra means that R is equipped with a ring homomorphism $\phi : A \to R$. In this case, every R-module is also an A-module by restriction of scalars: $am := \phi(a)m$; i.e., for A to act on M, just view elements of A as elements of R via ϕ and do the same action. This is what's going on in the right-hand side above. We'll circle back to restriction of scalars soon.

1.1.1. *Examples of derivations.* Let's consider some examples of derivations to buy into this notion.

First, let's construct the "usual derivative" for a polynomial or a power series ring, and show it is a derivation.

Definition 1.3. Let A be a ring and $R = A[x]$ a polynomial ring. We define $\frac{d}{dx} : R \to R$ by the rule

$$\frac{d}{dx}(\sum_{j=0}^{d} a_j x^j) = \sum_{j=1}^{d} j a_j x^{j-1}.$$

Similarly, for a power series ring, $R = A[\![x]\!]$, we define $\frac{d}{dx} : R \to R$ by the rule

$$\frac{d}{dx}(\sum_{j=0}^{\infty} a_j x^j) = \sum_{j=1}^{\infty} j a_j x^{j-1}.$$

Lemma 1.4. *The functions $\frac{d}{dx} : A[x] \to A[x]$ and $\frac{d}{dx} : A[\![x]\!] \to A[\![x]\!]$ are A-linear derivations.*

Proof. In either case, we have a well-defined function returning an object of the same type. The formulas are the same in both cases, just allowing infinite formal sums for power series, so we'll deal with both simultaneously.

Take $r = \sum_{j=0} a_j x^j$, $s = \sum_{j=0} b_j x^j$, and c with $a_j, b_j, c \in A$. Then

$$\frac{d}{dx}(r+s) = \frac{d}{dx}(\sum_{j=0}(a_j+b_j)x^j) = \sum_{j=1} j(a_j+b_j)x^{j-1} = \frac{d}{dx}(r) + \frac{d}{dx}(s),$$

$$\frac{d}{dx}(cr) = \frac{d}{dx}(\sum_{j=0}(ca_j)x^j) = \sum_{j=1} j(ca_j)x^{j-1} = c\frac{d}{dx}(r),$$

and

$$\begin{aligned} r\frac{d}{dx}(s) + s\frac{d}{dx}(r) &= (\sum_{i=0} a_i x^i)(\sum_{j=1} j b_j x^{j-1}) + (\sum_{j=0} b_j x^j)(\sum_{i=1} i a_i x^{i-1}) \\ &= \sum_{k=1}\sum_{i+j=k} (a_i j b_j) x^{i+j-1} + \sum_{k=1}\sum_{i+j=k} (i a_i b_j) x^{i+j-1} \\ &= \sum_{k=1}\sum_{i+j=k} k a_i b_j x^{i+j-1} \\ &= \frac{d}{dx}(\sum_{k=0}\sum_{i+j=k} (a_i b_j) x^k) = \frac{d}{dx}(rs). \quad \square \end{aligned}$$

Note that we could have written the formula above as $\frac{d}{dx}(\sum_{j=0}^{d} a_j x^j) = \sum_{j=1}^{d} j a_j x^{j-1}$ as well: it looks like we have something illegal when $j = 0$, but the coefficient of zero tells us to ignore it.

Proposition 1.5. *Let A be a ring, $\{X_\lambda \mid \lambda \in \Lambda\}$, and $R = A[X_\lambda \mid \lambda \in \Lambda]$ be a polynomial ring. Then the partial derivatives $\frac{d}{dX_\lambda}$ given by the rule*

$$\frac{d}{dx_\lambda}(\sum_\alpha a_\alpha X^\alpha) = \sum_\alpha \alpha_\lambda a_\alpha X^{\alpha - e_\lambda}$$

where $\alpha \in \mathbb{N}^\Lambda$ is an exponent tuple and e_λ is the unit vector in the λ coordinate, are A-linear derivations. Similarly for the power series ring $R = A[\![X_\lambda \mid \lambda \in \Lambda]\!]$.

Proof. Consider R as $R'[X_\lambda]$, with $R' = A[X_\mu \mid \mu \in \Lambda \smallsetminus \{\lambda\}]$. Then $\frac{d}{dX_\lambda}$ is just the "usual derivative" in this polynomial ring over R', so it is an R'-linear derivation of R. But since $A \subseteq R'$, this is an A-linear derivation as well. □

So we can differentiate over any polynomial ring now, e.g., over $R = \mathbb{F}_2[x]$. Let's not neglect our original derivatives.

Example 1.6. The standard derivatives

$$\mathcal{C}^\infty(\mathbb{R}) \xrightarrow{\frac{d}{dx}} \mathcal{C}^\infty(\mathbb{R})$$

and

$$\mathrm{Holo}(\mathbb{C}) \xrightarrow{\frac{d}{dx}} \mathrm{Holo}(\mathbb{C})$$

are $\mathbb{R}$-linear and $\mathbb{C}$-linear derivations, respectively.

We haven't seen examples where we take derivations into "actual" modules yet. It turns out that this is a natural thing to do. In fact, examples like this appear in calculus before derivations back into the ring!

Example 1.7. Let's return to old-fashioned derivatives of $\mathbb{C}^\infty$ functions. Before we get derivatives of functions as functions, we start with the notion of derivative at a point, which should just be a number. Let's try to realize "derivative at $x = x_0$" for some real number x_0, which we'll write as $\frac{d}{dx}|_{x=x_0}$, as a derivation on $\mathcal{C}^\infty(\mathbb{R})$. The target should be $\mathbb{R}$:

$$\frac{d}{dx}|_{x=x_0} : \mathcal{C}^\infty(\mathbb{R}) \to \mathbb{R},$$

so we need to view $\mathbb{R}$ as a $\mathcal{C}^\infty(\mathbb{R})$-module. A very $x = x_0$ flavored way of doing so is by the rule

$$f \cdot c = f(x_0)c.$$

Another useful way of thinking about this module structure is as the quotient $\mathcal{C}^\infty(\mathbb{R})/\mathfrak{m}_{x_0}$, where $\mathfrak{m}_{x_0}$ is the maximal ideal consisting of functions with $f(x_0) = 0$. Indeed, the evaluation at 0 map

$$\mathrm{ev}_{x_0}\mathcal{C}^\infty(\mathbb{R}) \to \mathbb{R}$$

has kernel $\mathfrak{m}_{x_0}$ by definition, and if $\mathbb{R}$ has the module structure given above, this map is $\mathcal{C}^\infty(\mathbb{R})$-linear: if $f \in \mathcal{C}^\infty(\mathbb{R})$ and $c \in \mathbb{R}$, then $\mathrm{ev}_{x_0}(fc) = f(x_0)c = f \cdot c$. Of course, if x_0 changed, we would get a different module structure.

Back to our derivative. Take $f, g \in \mathcal{C}^\infty(\mathbb{R})$ and $c \in \mathbb{R}$. Note that this c is an element of $\mathbb{R} \subseteq \mathcal{C}^\infty(\mathbb{R})$ as opposed to $\mathbb{R} \cong \mathcal{C}^\infty(\mathbb{R})/\mathfrak{m}_{x_0}$. Then

$$\frac{d}{dx}|_{x=x_0}\ (f+g) = \frac{d}{dx}|_{x=x_0}\ f + \frac{d}{dx}|_{x=x_0}\ g$$

$$\frac{d}{dx}|_{x=x_0}\ cf = c\frac{d}{dx}|_{x=x_0}\ f$$

and by the product rule

$$\frac{d}{dx}|_{x=x_0}\ (fg) = f(x_0)(\frac{d}{dx}|_{x=x_0}\ g) + g(x_0)(\frac{d}{dx}|_{x=x_0}\ f) = f\cdot(\frac{d}{dx}|_{x=x_0}\ g) + g\cdot(\frac{d}{dx}|_{x=x_0}\ f).$$

Lecture of January 26, 2023

Example 1.8. Other natural uses of derivatives actually take values in modules rather than the ring itself. Let's consider $R = \mathcal{C}^\infty(\mathbb{R}^3)$, the ring of infinitely differentiable real valued functions from $\mathbb{R}^3$ to $\mathbb{R}$, with pointwise operations. One has a notion of gradient ∇ of a function:

$$f(x,y,z) \mapsto \begin{bmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} & \frac{\partial f}{\partial z} \end{bmatrix}.$$

The output is a vector of three functions in R, so this is a function $\nabla : R \to R^3$. It follows from calculus that this is an $\mathbb{R}$-linear derivation.

Similarly, one sometimes talks about the *total derivative* of a function $f \in \mathcal{C}^\infty(\mathbb{R}^3)$ as

$$df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy + \frac{\partial f}{\partial z}dz.$$

This rule $f \mapsto df$ is a derivation from R to a free R-module with basis dx, dy, dz.

Example 1.9. Let's try out a slightly more interesting ring. Let's consider $R = \mathbb{C}[x,y]/(x^2 - y^3)$ and try out $\frac{d}{dx}$ on this ring. Of course, this is a quotient ring, so if this means anything, it means apply this rule to an equivalence class and take the class of the result. But this is a problem, since $0 = x^2 + y^3$ and $\frac{d}{dx}(0) = 0 \neq 2x = \frac{d}{dx}(x^2+y^3)$. So this derivation doesn't even make sense, and in hindsight, perhaps it looks a little bit silly to try. But we can actually get by with something surprisingly similar. Let's write $\frac{d}{dx}|_{(0,0)}$ for the rule

$$\frac{d}{dx}|_{(0,0)}(f) = \frac{d}{dx}(f)(0,0);$$

i.e., partial derivative with respect to x at the origin. It is in fact well-defined: we have

$$\begin{aligned}\frac{d}{dx}|_{(0,0)}(f + (x^2+y^3)g) &= \frac{d}{dx}|_{(0,0)}(f) + \frac{d}{dx}|_{(0,0)}((x^2+y^3)g)\\ &= \frac{d}{dx}|_{(0,0)}(f) + g|_{(0,0)}\frac{d}{dx}|_{(0,0)}(x^2+y^3) + (x^2+y^3)|_{(0,0)}\frac{d}{dx}|_{(0,0)}(g) = \frac{d}{dx}|_{(0,0)}(f)\end{aligned}$$

and, along the same lines as previous examples, is a $\mathbb{C}$-linear derivation to $\mathbb{C}$, viewed as a module via the rule $f \cdot c = f(0,0)c$.

Example 1.10. Let's end with a boring example. For any A-algebra R and any R-module M, the zero map is an A-linear derivation from R to M.

1.2. **Properties of derivations.** Let's collect some basic properties of derivations. The first includes the fact that constants go to zero.

Proposition 1.11. *Let $\partial : R \to M$ be a derivation.*

1. $\partial(0) = \partial(1) = 0$,
2. $\partial(-r) = -\partial(r)$,
3. *The kernel of ∂ is a subring of R,*
4. *For $A \subseteq R$, ∂ is A-linear if and only if $A \subseteq \ker(\partial)$.*

Proof. (1) $\partial(0) = \partial(0+0) = \partial(0) + \partial(0)$, and $\partial(1) = \partial(1\cdot 1) = 1\partial(1) + 1\partial(1) = \partial(1) + \partial(1)$; in each case we cancel.

(2) $0 = \partial(r - r) = \partial(r) + \partial(-r)$, and move $\partial(r)$ to the other side.
(3) If $\partial(r) = \partial(s) = 0$, then $\partial(r - s) = \partial(r) - \partial(s) = 0$ and $\partial(rs) = r\partial(s) + s\partial(r) = 0$.
(4) If $A \subseteq \ker(\partial)$, $a \in A$, and $r \in R$, then $\partial(ar) = a\partial(r) + r\partial(a) = a\partial(r)$, so ∂ is A-linear; conversely, if $\partial(ar) = a\partial(r)$ for all $a \in A$ and $r \in R$, then $r\partial(a) = 0$ for all $a \in A$ and $r \in R$, and in particular $\partial(a) = 1\partial(a) = 0$. □

Remark 1.12. It follows that every derivation of R into M is $\mathbb{Z}$-linear since every derivation is linear over its kernel, and its kernel is a subring.

There are lots of ways to make derivations out of other derivations.

Proposition 1.13. *Let $\alpha, \beta : R \to M$ be derivations over A, $t \in R$, and $\gamma : M \to N$ be an R-module homomorphism, and $\phi : S \to R$ an A-algebra homomorphism.*

(1) *$\alpha + \beta : R \to M$ is a derivation over A,*
(2) *$t\alpha : R \to M$ is a derivation over A,*
(3) *$\gamma \circ \alpha : R \to N$ is a derivation over A.*
(4) *$\alpha \circ \phi : S \to M$ is a derivation over A.*

Proof. In each case, the map under consideration is definitely A-linear, so we just need to check the product rule.

(1) $(\alpha + \beta)(rs) = \alpha(rs) + \beta(rs) = r\alpha(s) + s\alpha(r) + r\beta(s) + s\beta(r) = r(\alpha + \beta)(s) + s(\alpha + \beta)(r)$;
(2) $t\alpha(rs) = t(r\alpha(s) + s\alpha(r)) = r(t\alpha(s)) + s(t\alpha(r))$;
(3) $(\gamma \circ \alpha)(rs) = \gamma((r\alpha(s) + s\alpha(r)) = r\gamma \circ \alpha(s) + s\gamma \circ \alpha(r)$.
(4) $(\alpha \circ \phi)(rs) = \alpha(\phi(r)\phi(s)) = \phi(s)\alpha(\phi(r)) + \phi(r)\alpha(\phi(s)) = s(\alpha \circ \phi)(r) + r(\alpha \circ \phi)(s)$, where the last equality is just recalling that M is a module by restriction of scalars. □

Definition 1.14. Let R be a ring, and M be and R-module. We set $\mathrm{Der}_R(M)$ to be the *module of derivations* of R into M. If R is an A-algebra via $\phi : R \to M$, we set $\mathrm{Der}_{R|A}(M)$ or $\mathrm{Der}_\phi(M)$ to be the *module of A-linear derivations* of R into M.

These are R-modules as a consequence of the proposition above.

Example 1.15. If A is a ring and $R = A[x_1, \ldots, x_n]$ is a polynomial ring over A, then for any $f_1, \ldots, f_n \in R$,

$$\begin{aligned} \textstyle\sum_{i=1}^n f_i \frac{d}{dx_i} : \ & R \longrightarrow R \\ & r \longmapsto \textstyle\sum_{i=1}^n f_i \frac{dr}{dx_i} \end{aligned}$$

is an A-linear derivation on R.

If M is an R-module, then for any $m_1, \ldots, m_n \in M$, the map

$$\begin{aligned} m_i \tfrac{d}{dx_i} : \ & R \longrightarrow M \\ & r \longmapsto \tfrac{dr}{dx_i} m_i \end{aligned}$$

is an A-linear derivation, since it is the composition of the derivation $R \xrightarrow{\frac{d}{dx_i}} R$ and the R-linear map $R \xrightarrow{m} M$; adding these, the map

$$\begin{aligned} \textstyle\sum_{i=1}^n m_i \frac{d}{dx_i} : \ & R \longrightarrow M \\ & r \longmapsto \textstyle\sum_{i=1}^n \frac{dr}{dx_i} m_i \end{aligned}$$

is an A-linear derivation.

Example 1.16. Let's jack this example up. Let A be a ring, $R = A[X_\lambda \mid \lambda \in \Lambda]$ a polynomial ring over A, and $\{f_\lambda \mid \lambda \in \Lambda\}$ a sequence of elements in bijection with the variables then the formal sum

$$\sum_{\lambda\in\Lambda} f_\lambda \frac{d}{dX_\lambda} : R \to R$$

given by $r \mapsto \sum_{\lambda\in\Lambda} f_\lambda \frac{dr}{dX_\lambda}$ gives a well-defined map, since any $r \in R$ involves at most finitely many variables, and hence $\frac{dr}{dX_\lambda} = 0$ for all but finitely many $\lambda \in \Lambda$. This map is an A-linear derivation. Indeed, A-linearity is striaghtforward. To check the product rule, take $r, s \in R$; between the two, they involve only finitely many variables, and for these elements, the formula for this derivation agrees with the rule for the finitely many variables involved. By the last example, the product rule holds.

Similarly, for any R-module M and Λ-tuple of elements of M, there is a derivation

$$\sum_{\lambda\in\Lambda} m_\lambda \frac{d}{dX_\lambda} : R \to M$$

given by $f \mapsto \sum_{\lambda\in\Lambda} \frac{d}{dX_\lambda} m_\lambda$.

We would like to compute modules of derivations in some examples. The following lemma will help us recognize when we're done.

Lemma 1.17. *Let R be an A-algebra and $\{f_\lambda \mid \lambda \in \Lambda\}$ be a generating set of R as an A-algebra. Let M be an R-module. Then any A-linear derivation on R is determined by the images of f_λ. That is, $\alpha, \beta : R \to M$ are A-linear derivations with $\alpha(f_\lambda) = \beta(f_\lambda)$ for all λ, then $\alpha = \beta$.*

Proof. We need to show that $\alpha(r) = \beta(r)$ for any $r \in R$. Any element of R can be written as a sum of monomial expressions in the $f's$; i.e., a sum of terms of the form $r = af_{\lambda_1}^{\mu_1} \cdots f_{\lambda_n}^{\mu_n}$ with $a \in A$ so it suffices to show that α and β take e same value on such a monomial r. We proceed by induction on $k = \mu_1 + \cdots + \mu_n$. When $k = 0$, $r \in A$ so $\alpha(r) = 0 = \beta(r)$. For the inductive step, take $k > 0$, so WLOG $\mu_1 \neq 0$; then $r = r' f_{\lambda_1}$, and

$$\alpha(r' f_{\lambda_1}) = r'\alpha(f_{\lambda_1}) + f_{\lambda_1}\alpha(r')$$

and likewise for β. By the starting assumption, $\alpha(f_{\lambda_1}) = \beta(f_{\lambda_1})$ and by the induction hypothesis $\alpha(r') = \beta(r')$. The equality follows. □

Theorem 1.18. *Let A be a ring and $R = A[X_\lambda \mid \lambda \in \Lambda]$ be a polynomial ring over A. For any R-module M, the map*

$$\begin{aligned} \textstyle\prod_\Lambda M &\xrightarrow{\mu} \mathrm{Der}_{R|A}(M) \\ (m_\lambda)_\lambda &\longmapsto \textstyle\sum m_\lambda \frac{d}{dX_\lambda} \end{aligned}$$

is an isomorphism.

Proof. Consider the map $\nu : \mathrm{Der}_{R|A}(M) \to \prod_\Lambda M$ given by $\alpha \mapsto (\alpha(X_\lambda))_{\lambda\in\Lambda}$. The previous lemma shows that ν is injective. On the other hand,

$$(\nu \circ \mu)(m_\lambda)_\lambda = ((\sum_\lambda m_\lambda \frac{d}{dX_\lambda})(X_\lambda))_\lambda = (m_\lambda)_\lambda.$$

Thus, μ is injective. Then μ must be an isomorphism. Indeed, $\nu = (\nu\mu)\nu = \nu(\mu\nu)$ and ν injective implies $\mu\nu$ is the identity as well. □

Lecture of January 31, 2023

We can give a description the derivations on any ring now.

Proposition 1.19. *Let R be an A-algebra. Write $R = S/I$ with $S = A[X_\lambda \mid \lambda \in \Lambda]$ and $I = (f_\gamma \mid \gamma \in \Gamma)$. Let M be an R-module. Then every A-linear derivation ∂ from R to M can be written in the form*

$$\sum_{\lambda\in\Lambda} m_\lambda \overline{\frac{d}{dx_\lambda}}$$
$$r = [s] \mapsto \sum_\lambda \frac{d}{dx_\lambda}(s) m_\lambda$$

for some unique $(m_\lambda)_\lambda \in \prod_\Lambda M$. A tuple of elements $(m_\lambda)_\lambda$ induces a well-defined derivation from R to M if and only if the corresponding derivation $\widetilde{\partial} : S \to M$ has $\widetilde{\partial}(f_\gamma) = 0$ for all γ.

Proof. Let $\pi : S \to R$ be the quotient map. Given an A-linear derivation $\partial : R \to M$, there is an A-linear derivation $\pi \circ \partial : S \to M$ that can be written in the form above by the previous theorem, so any derivation has this form. Since derivations are addition, such a derivation is well-defined so long as $\widetilde{\partial}(I) = 0$. This certainly implies that $\widetilde{\partial}(f_\gamma) = 0$ for all γ; conversely, any element of I can be written as $\sum_i s_i f_i$ and $\widetilde{\partial}(\sum_i s_i f_i) = \sum_i s_i \widetilde{\partial}(f_i) + \sum_i f_i \widetilde{\partial}(s_i)$, and the first sum is zero by hypothesis and the second since M is an R-module which is necessarily killed by I. □

Example 1.20. Let's find some $\mathbb{C}$-linear derivations on $R = \frac{\mathbb{C}[x,y]}{x^2+y^3}$ to itself. Any such derivation must be a map of the form $\partial = r_1 \overline{\frac{d}{dx}} + r_2 \overline{\frac{d}{dy}}$ where $\widetilde{\partial} = r_1 \frac{d}{dx} + r_2 \frac{d}{dy} : \mathbb{C}[x,y] \to R$ has $\widetilde{\partial}(x^2+y^3) = 0$, or just as well $\partial' = r'_1 \frac{d}{dx} + r'_2 \frac{d}{dy} : \mathbb{C}[x,y] \to \mathbb{C}[x,y]$ has $\partial'(x^2+y^3) \in (x^2+y^3)$. Since $\partial'(x^2+y^3) = 2x\partial'(x) + 3y^2\partial'(y)$, we must have $2xr'_1 + 3y^2 r'_2 \in (x^2+y^3)$. Here are a couple:

$$3x\overline{\frac{d}{dx}} + 2y\overline{\frac{d}{dy}} \qquad \text{and} \qquad 3y^2\overline{\frac{d}{dx}} + 2x\overline{\frac{d}{dy}}.$$

Example 1.21. Let's look at something simpler: $\mathrm{Der}_{\mathbb{C}|\mathbb{R}}(\mathbb{C})$. We can write $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, so such a derivation is of the form $r\overline{\frac{d}{dx}}$ where $r\frac{d}{dx}(x^2+1) \in (x^2+1)$. Since $2x = \frac{d}{dx}(x^2+1)$ and x^2+1 are coprime in $\mathbb{R}[x]$, r must be a multiple of x^2+1, so the corresponding derivation must be the zero map. Thus, there are no $\mathbb{R}$-linear derivations on $\mathbb{C}$.

1.2.1. *Lie algebra structure on* $\mathrm{Der}_{R|A}(R)$. Even more than a module, there is extra structure on $\mathrm{Der}_{R|A}(R)$. Any two elements of $\mathrm{Der}_{R|A}(R)$ have the same source and target, so we can compose them. The result is essentially never a derivation though.

Example 1.22. In $\mathbb{C}[x]$,

$$\frac{d^2}{dx^2}(x \cdot x) = 2 \neq 0 = x\frac{d^2}{dx^2}(x) + x\frac{d^2}{dx^2}(x).$$

However:

Proposition 1.23. *Let R be an A-algebra, and $\alpha, \beta \in \mathrm{Der}_{R|A}(R)$. Then the map $\alpha \circ \beta - \beta \circ \alpha : R \to R$ is an A-linear derivation.*

Proof. A-linearity follows since we have linear combinations or compositions of A-linear maps. Given $r, s \in R$,

$$\begin{aligned}(\alpha\beta - \beta\alpha)(rs) &= \alpha(r\beta(s) + s\beta(r)) - \beta(r\alpha(s) + s\alpha(r)) \\ &= \alpha(r\beta(s)) + \alpha(s\beta(r)) - \beta(r\alpha(s)) - \beta(s\alpha(r)) \\ &= \alpha(r)\beta(s) + r\alpha\beta(s) + s\alpha\beta(r) + \alpha(s)\beta(r) - \beta(r)\alpha(s) - r\beta\alpha(s) - \alpha(r)\beta(s) - s\beta\alpha(r) \\ &= r\alpha\beta(s) + s\alpha\beta(r) - r\beta\alpha(s) - s\beta\alpha(r) \\ &= r(\alpha\beta - \beta\alpha)(s) + s(\alpha\beta - \beta\alpha)(r)\end{aligned}$$

□

We write $[\alpha, \beta] := \alpha \circ \beta - \beta \circ \alpha$ and call this the *commutator* of α and β. This operation isn't a product operation for a ring (we will see soon that it's not associative), but it gives the structure of a *Lie algebra*.

Definition 1.24. A *Lie algebra* over a ring A is an A-module M equipped with an operation $[-,-] : M \times M \to M$ such that, for all $l, m, n \in M$ and $a \in A$:

- $[l + m, n] = [l, n] + [m, n]$ and $[l, m + n] = [l, m] + [l, n]$,
- $[am, n] = a[m, n]$ and $[m, an] = a[m, n]$,
- $[m, m] = 0$,
- $[l, [m, n]] + [m, [n, l]] + [n, [l, m]] = 0$.

Example 1.25. If N is an A-module, then $E = \mathrm{End}_A(N)$ (the collection of A-linear *endomorphisms* of N) with bracket $[\alpha, \beta] := \alpha \circ \beta - \beta \circ \alpha$ is a Lie algebra over A. The first three conditions are straightforward. The third follows from associativity of composition: To avoid foiling all these out, note that each term after expanding is a triple involving l, m, n. The expression above is stable under the permutation $l \mapsto m \mapsto n \mapsto l$, so it suffices to check that the triples lmn and lnm appear a cancelling number of times. Indeed, lmn appears with $+1$ from the first and -1 from the second and lnm appears with -1 from the first and $+1$ from the second.

Proposition 1.26. *Let R be an A-algebra. The commutator operation endows $\mathrm{Der}_{R|A}(R)$ with the structure of a Lie algebra over A.*

Proof. $\mathrm{Der}_{R|A}(R)$ is a submodule of $\mathrm{End}_A(R)$ and the bracket operation is consistent with that on the Lie algebra $\mathrm{End}_A(R)$, so it suffices to note that it is closed under the bracket operation. □

1.3. **Derivations and ideals.**

Proposition 1.27. *Let R be a ring, and I an ideal. Let $\partial : R \to M$ be a derivation. Then $\partial(I^n) \subseteq I^{n-1}M$ for all $n \in \mathbb{N}$.*

Proof. We proceed by induction on n, with $n = 1$ trivial. Given $r \in I^n$, write $r = \sum_i a_i b_i$ with $a_i \in I^{n-1}$ and $b_i \in I$. Then

$$\partial(r) = \sum_i \partial(a_i b_i) = \sum_i a_i \partial(b_i) + \sum_i b_i \partial(a_i).$$

Clearly $a_i\partial(b_i) \in I^{n-1}M$, and by the induction hypothesis $\partial(a_i) \in I^{n-2}M$, so $b_i\partial(a_i) \in I^{n-1}M$. □

It follows that every A-linear derivation $\partial : R \to M$ gives rise, by restriction/quotient, to a well-defined A-linear map $\overline{\partial} : I^n/I^{n+1} \to I^{n-1}M/I^nM$, and in particular $\overline{\partial} : I/I^2 \to M/IM$.

Proposition 1.28. *Let R be an A-algebra, I an ideal, and M an R-module. If $IM = 0$, then there is an isomorphism*

$$\mathrm{Der}_{R|A}(M) \to \mathrm{Der}_{(R/I^2)|A}(M)$$

and a well-defined map

$$\mathrm{Der}_{R|A}(M) = \mathrm{Der}_{(R/I^2)|A}(M) \to \mathrm{Hom}_A(I/I^2, M)$$

induced by restriction.

In fact, this restriction map is better than one might expect!

Proposition 1.29. *Let R be an A-algebra, I an ideal, and M an R-module with $IM = 0$. Then the induced map $\overline{\partial} : I/I^2 \to M$ is R-linear. Thus, one obtains an R-module homomorphism*

$$\mathrm{Der}_{R|A}(M) = \mathrm{Der}_{(R/I^2)|A}(M) \to \mathrm{Hom}_R(I/I^2, M)$$

induced by restriction.

Proof. Given $r \in R$ and $a \in I/I^2$, we have $\overline{\partial}(ra) = r\overline{\partial}(a) + a\overline{\partial}(r) = r\overline{\partial}(a)$. □

Example 1.30. Consider $R = \mathbb{C}[x_1, \ldots, x_n]$ and $\mathfrak{m}$ maximal. We have the restriction map

$$\mathrm{Der}_{R|\mathbb{C}}(R/\mathfrak{m}) \xrightarrow{\text{res}} \mathrm{Hom}_R(\mathfrak{m}/\mathfrak{m}^2, R/\mathfrak{m}).$$

Since $\mathfrak{m}/\mathfrak{m}^2$ and $R/\mathfrak{m}$ are killed by $\mathfrak{m}$, these are $R/\mathfrak{m} = \mathbb{C}$-modules, so the target is just $(\mathfrak{m}/\mathfrak{m}^2)^*$, where $(-)^*$ denotes $\mathbb{C}$-linear dual. The map is an isomorphism! To see it, note that $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ for some vector a. Write $\widetilde{x_i} = x_i - a_i$. After a change of coordinates, we can consider R as a polynomial ring in the $\widetilde{x_i}$'s. Then $\mathfrak{m}/\mathfrak{m}^2$ is a vector space with basis given by the classes of the $\widetilde{x_i}$'s. By our proposition on derivations on polynomial rings, for any n-tuple of elements in $R/\mathfrak{m} \cong \mathbb{C}$, there is a unique derivation sending the corresponding variables there. That's what it means for the restriction to be an isomorphism! Concretely, the map

$$\sum_i \lambda_i \widetilde{x_i}^* \mapsto \sum_i \lambda_i \frac{d}{dx_i}|_{x=a}$$

is an inverse.

Lecture of February 2, 2023

We actually don't need the extremely strong hypothesis of polynomial ring in the last example. Let's party hard and figure out when, for a module with $IM = 0$, the map

$$\mathrm{Der}_{(R/I^2)|A}(M) \to \mathrm{Hom}_R(I/I^2, M)$$

is surjective (i.e., every homomorphism from the "I-top" extends to a derivation). A reasonable starting point is to take M to be I/I^2, which is the part of the ring R/I^2 itself that is definitely killed by I.

Theorem 1.31. *Let R be an A-algebra and I an ideal. Then an A-linear map $\alpha : R/I^2 \to I/I^2$ is an A-linear derivation if and only if the map*

$$\begin{aligned} R/I^2 &\xrightarrow{1+\alpha} R/I^2 \\ r &\longmapsto r + \alpha(r) \end{aligned}$$

is an A-algebra homomorphism.

Proof. We observe that the map $1 + \alpha$ is a sum of A-module homomorphisms, and hence A-linear. We just need to check that the product rule for α lines up with $1 + \alpha$ respecting multiplication. If α is a derivation, then

$$\begin{aligned} (1+\alpha)(rs) &= rs + \alpha(rs) = rs + r\alpha(s) + s\alpha(r) = rs + r\alpha(s) + s\alpha(r) + \alpha(r)\alpha(s) \\ &= (r + \alpha(r))(s + \alpha(s)) = (1+\alpha)(r)(1+\alpha)(s) \end{aligned}$$

where we used that $\alpha(r), \alpha(s) \in I/I^2$ so their product is zero. Conversely, following the equalities above, we must have $\alpha(rs) = r\alpha(s) + s\alpha(r)$ for the products to agree. □

This theorem gives an interesting and useful new way to think of derivations: they are "perturbations" of the identity map.

It also allows us to unlock many derivations.

Proposition 1.32. *Let R be an A-algebra and I an ideal. Suppose that the quotient map $\pi : R/I^2 \to R/I$ has an A-algebra right inverse, i.e., there is some A-algebra map $\tau : R/I \to R/I^2$ such that $\pi \circ \tau$ is the identity on R/I. Then for every R-module M with $IM = 0$, the map*

$$\mathrm{Der}_{R|A}(M) \xrightarrow{\text{res}} \mathrm{Hom}_R(I/I^2, M)$$

is surjective.

Proof. Consider the ring homomorphism $\tau \circ \pi : R/I^2 \to R/I^2$. Set $\alpha : R/I^2 \to R/I^2$ by $\tau \circ \pi - 1$. We claim that the image of α is in I/I^2. Indeed, for $r \in R/I^2$ we have $\pi\alpha(r) = \pi\tau\pi(r) - \pi(r) = \pi(r) - \pi(r) = 0$, so $\alpha : R/I^2 \to I/I^2$ has image in I/I^2. But $1 + \alpha = \tau\pi$ is a ring homomorphism, so α is a derivation, and α as well. Additionally, if $a \in I/I^2$, then $\pi(a) = 0$, so $-\alpha(a) = (\tau \circ \pi - 1)(-a) = a$. Thus, given $\phi : I/I^2 \to M$ R-linear, $\phi \circ -\alpha : R/I^2 \to M$ is an A-linear derivation on R/I^2 with restriction to I/I^2 being just ϕ. □

Example 1.33. Let R be a finitely generated $\mathbb{C}$-algebra, and $\mathfrak{m}$ a maximal ideal. Then $\mathbb{C} \subseteq R/\mathfrak{m}^2$ and $R/\mathfrak{m} \cong \mathbb{C}$, so there is a right inverse of the quotient map $R/I^2 \to R/I$. Moreover, $R/\mathfrak{m}^2$ is generated by $\mathfrak{m}/\mathfrak{m}^2$ as a $\mathbb{C}$-algebra, since $R/\mathfrak{m}^2 \cong \mathbb{C} \oplus \mathfrak{m}/\mathfrak{m}^2$ (or many other reasons). It follows that the map

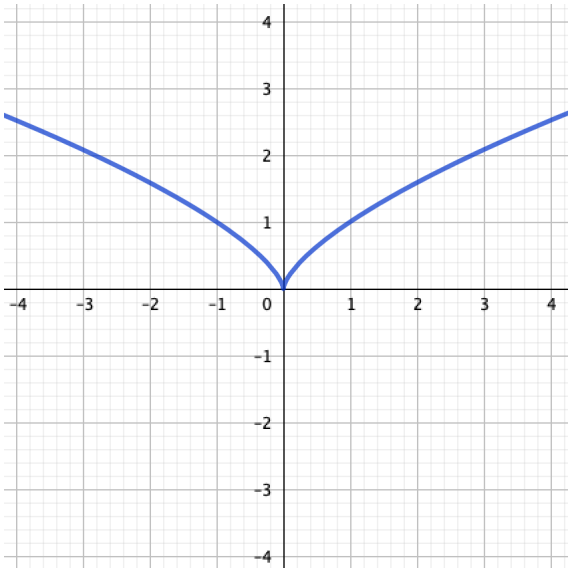
$$\mathrm{Der}_{R|\mathbb{C}}(R/\mathfrak{m}) \xrightarrow{\text{res}} \mathrm{Hom}_R(\mathfrak{m}/\mathfrak{m}^2, R/\mathfrak{m}) = (\mathfrak{m}/\mathfrak{m}^2)^*$$

is an isomorphism (where the last equality is just because the source and target are $(R/\mathfrak{m} = \mathbb{C})$-vector spaces).

1.4. **Quick review of affine varieties.** Many of the constructions and questions we will consider will be motivated geometrically, and we will want to compare and contrast many of our main theorems with things we encounter in multivariable calculus, manifold theory, analysis, and other disciplines. We'll want to remember how to think of rings and ring homomorphisms geometrically. Over $\mathbb{C}$ (or an algebraically closed field) we have the following correspondence:

algebra	geometry
$\mathbb{C}[x_1, \dots, x_n]$	$\mathbb{C}^n$
reduced finitely-generated $\mathbb{C}$-algebra	variety
$R = \dfrac{\mathbb{C}[x_1, \dots, x_n]}{(f_1, \dots, f_m)} =: \mathbb{C}[X]$	$X :=$ solution set of $f_1 = \cdots = f_m = 0$
maximal ideal $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n)$	point $a = (a_1, \dots, a_n)$
$r \in \mathbb{C}[X]$	polynomial function on X
going modulo $\mathfrak{m}_a$	evaluation at a
$\mathbb{C}$-algebra homomorphism $\mathbb{C}[X] \to \mathbb{C}[Y]$ $x_i \mapsto f_i((y))$	morphism of varieties $Y \to X$ $b \mapsto (f_1(b), \dots, f_n(b))$

Example 1.34. Take $R = \mathbb{C}[x, y]/(x^2 - y^3)$. Geometrically, this corresponds to the solution set of $x^2 = y^3$ in 2-space. We can only draw the "real" picture, and we'll have to live with that.



Note the corner at $(0,0)$; we will see later that this has something to do with our unexpected derivation in the example above.

Example 1.35. This business about maps of varieties going the wrong way is a bit disorienting. Let's try a couple of examples of this.

- Given a (radical) ideal $I \subset S = \mathbb{C}[x_1, \ldots, x_n]$, the quotient map $S \to S/I$ is given by sending $x_i \mapsto x_i$, so the corresponding map of varieties $V(I) \to \mathbb{C}^n$ is just the inclusion map.
- Consider $\mathbb{C}[x,y]/(x^2 - y^3) \cong \mathbb{C}[t^2, t^3]$ (via $x \mapsto t^3, y \mapsto t^2$) and take the inclusion of rings $\mathbb{C}[t^2, t^3] \subseteq \mathbb{C}[t]$. Under the composition $x \mapsto t^3, y \mapsto t^2$ in $\mathbb{C}[t]$, and corresponding map of varieties goes from $\mathbb{C} \mapsto V(x^2 - y^3)$ and sends $b \mapsto (b^3, b^2)$.

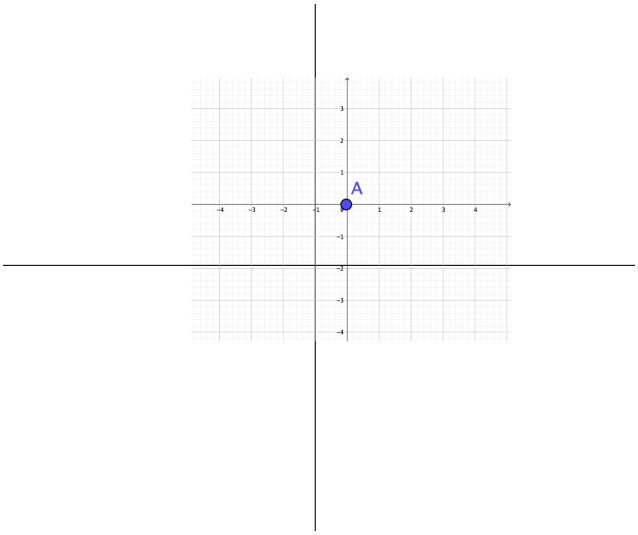
One important thing that is *not* included in this correspondence is the usual *Euclidean* topology on $\mathbb{C}^n$ or a subset $X \subseteq \mathbb{C}^n$ with an open basis given by $B_\varepsilon(a) = \{x \mid |x - a| < \varepsilon\}$ with the usual norm $|\cdot|$. We have the *Zariski* topology in which the closed sets are subvarieties, but this has no knowledge of what things are close in the Euclidean sense.

The magic making this all work out so nicely is the Nullstellensatz, which guarantees that maximal ideals of $\mathbb{C}[X]$ all correspond to points of X. In general, we just take the (instead of maximal) prime ideals to be our points and work from there.

algebra	"geometry"
ring	prime spectrum
R	$\mathrm{Spec}(R) = \{\mathfrak{p} \mid \mathfrak{p} \subset R \text{ prime ideal}\}$
prime ideal	point
maximal ideal	closed point
ring homomorphism $R \to S$	continuous map $Y \to X$
ϕ	$\mathfrak{q} \mapsto \phi^{-1}(\mathfrak{q})$

Whereas the correspondence between varieties and reduced f.g. $\mathbb{C}$-algebras was bijective above, the correspondence between rings and their spectra as topological spaces is far from: in particular, every field K has $\mathrm{Spec}(K)$ a singleton.

1.4.1. *Tangent spaces of varieties.* Let's get to the bottom of this corner business while we're at it. Let's define the *tangent space* of an affine variety X at a point a, $T_a(X)$. For starters, the tangent space of affine space $\mathbb{C}^n$ at a point a will be the vector space $\mathbb{C}^n$, thought of as centered at a.



We can recenter our coordinates there as $\widetilde{x_j} := x_j - a_j$. Now, given a variety $X = V(f_1, \dots, f_m)$, for each f_i we look at its *linear part* near a: we can take its Taylor expansion at a

$$f_i = f_i(a) + \sum_j \frac{d}{dx_j}|_{x=a}(f_i)(x_j - a_j) + \text{higher order terms}\ .$$

Since $a \in X$, $f_i(a) = 0$, and we have

$$f_i = \sum_j \frac{d}{dx_j}|_{x=a}(f_i)\widetilde{x_j} + \text{higher order terms}\ ,$$

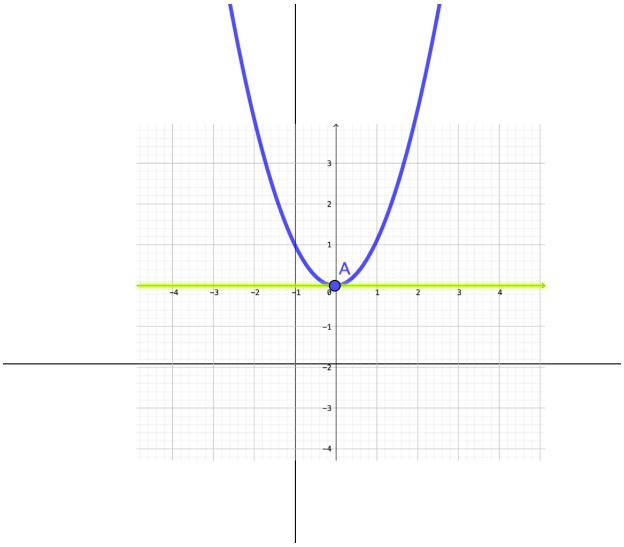
so the linear part of f is given by the linear functional $\nabla(f_i)|_{x=a} \cdot \widetilde{x}$. Then we take $T_a(X)$ to be the linear subspace of $T_a(\mathbb{C}^n)$ cut out by the linear equations $\nabla(f_1)|_{x=a}v = \cdots = \nabla(f_m)|_{x=a}v = 0$. In particular, $T_a(\mathbb{C}^n)$ is the kernel of the *Jacobian matrix*

$$J(f_1, \dots, f_m)|_{x=a} = \begin{bmatrix} \frac{d}{dx_1}|_{x=a}(f_1) & \cdots & \frac{d}{dx_n}|_{x=a}(f_1) \\ \vdots & \ddots & \vdots \\ \frac{d}{dx_1}|_{x=a}(f_m) & \cdots & \frac{d}{dx_n}|_{x=a}(f_m) \end{bmatrix},$$

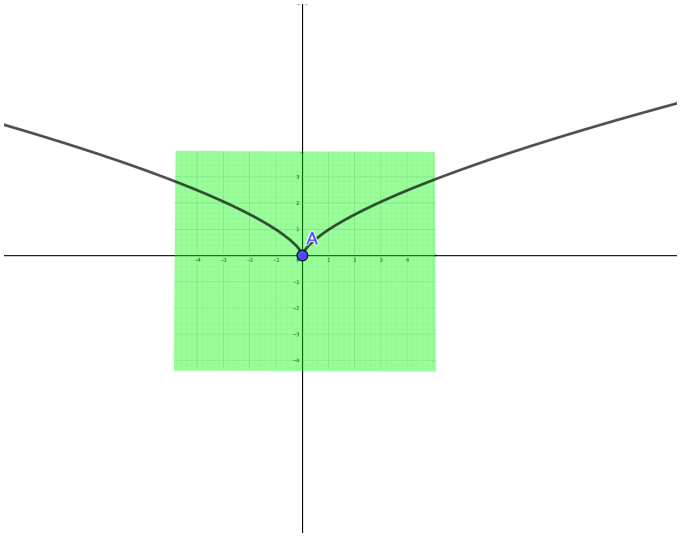
whose rows are the gradient vectors.

Lecture of February 6, 2023

Example 1.36. Take the parabola $X = V(y - (x-1)^2 - 2)$. To compute the tangent space at $a = (1, 2)$, take the gradient at $(1, 2)$, which is $\begin{bmatrix} -2(x-1) \\ 0 \end{bmatrix}|_{(1,2)} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, so the defining equation is $\widetilde{y} = 0$.



Example 1.37. Take the curve $X = V(y^2 - x^3)$. To compute the tangent space at $a = (0,0)$, take the gradient at $(0,0)$, which is $\begin{bmatrix} -3x^2 \\ 2y \end{bmatrix}|_{(0,0)} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, so the defining equation is the zero equation. Thus, the tangent space is all of $T_a(\mathbb{C}^2)$.



We want to understand this tangent space in terms of the algebra of the coordinate ring. Here's how.

Proposition 1.38. *Let $X = V(I)$ be a complex affine variety (with I reduced) and $a \in X$. Let $R = \mathbb{C}[x_1, \ldots, x_n]/I$ be the coordinate ring of X and $\mathfrak{m}$ the corresponding maximal ideal. Then there is a $\mathbb{C}$-vector space isomorphism $(\mathfrak{m}/\mathfrak{m}^2)^* \cong T_a(X)$, where $(-)^*$ denotes $\mathbb{C}$-vector space dual.*

Proof. Let $S = \mathbb{C}[x_1, \ldots, x_n]$ and $\mathfrak{n}$ be the preimage of $\mathfrak{m}$. Set $\widetilde{x_j} = x_j - a_j$; these are the generators of $\mathfrak{n}$. Then the images of the $\widetilde{x_j}$ form a vector space for $\mathfrak{n}/\mathfrak{n}^2$; we have essentially defined $T_a(\mathbb{C}^n)$ as the $\mathbb{C}$-vector space with coordinates $\widetilde{x_j}$; i.e., the dual space to $\mathfrak{n}/\mathfrak{n}^2$. So $T_a(\mathbb{C}^n)^* \cong \mathfrak{n}/\mathfrak{n}^2$. We will think of $T_a(\mathbb{C}^n)^* = \mathfrak{n}/\mathfrak{n}^2$ each as $1 \times n$ row vectors corresponding to the basis $\widetilde{x_j}$ and $T_a(\mathbb{C}^n)$ as $n \times 1$ column vectors.

For an element $f \in \mathfrak{n}$, we can write $f = \nabla(f)|_{x=a}\widetilde{x}$ in $\mathfrak{n}/\mathfrak{n}^2$, so $\nabla(f)|_{x=a}$ is its row vector.

Then $T_a(X)^*$ corresponds to quotient of the linear functionals on $T_a(\mathbb{C}^n) \to \mathbb{C}$ modulo the ones that vanish on $T_a(X)$. But since $T_a(X)$ is just the set of vectors v such that $\nabla(f_i)|_{x=a}v = 0$ for all i, a linear

functional in $T_a(\mathbb{C}^n)^*$ vanishes on $T_a(X)$ if and only if it is in the (row) span of $\nabla(f_i)|_{x=a}$. Thus, we have

$$T_a(X)^* \cong \frac{\mathfrak{n}/\mathfrak{n}^2}{((f_1,\dots,f_m)+\mathfrak{n}^2)/\mathfrak{n}^2} \cong \frac{\mathfrak{n}}{\mathfrak{n}^2+I}.$$

Finally, by some basic isomorphism theorems, we can identify $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{n}/(\mathfrak{n}^2+I)$: namely,

$$\frac{\mathfrak{m}}{\mathfrak{m}^2} \cong \frac{\mathfrak{n}/I}{(\mathfrak{n}^2+I)/I} \cong \frac{\mathfrak{n}}{\mathfrak{n}^2+I}.$$ □

Corollary 1.39. *Let $R = \mathbb{C}[X]$ be the coordinate ring of an affine variety and $a \in X$ with associated maximal ideal $\mathfrak{m}$. Then there is an isomorphism $\mathrm{Der}_{R|\mathbb{C}}(R/\mathfrak{m}) \cong T_a(X)$.*

This description of the tangent space of a variety like so is useful; in fact, in many situations, one defines the tangent space to an object by using derivations! Clearly this has some advantages as it naturally arises from X rather than thinking about X inside of $\mathbb{C}^n$ cut out by some equations.

We say that an irreducible affine variety X is *nonsingular* at a if $\dim_{\mathbb{C}} T_a(X) = \dim X$, and *singular* otherwise (in which case ">" happens).

Lecture of February 9, 2023

From the geometric definition of tangent space, we have the following.

Theorem 1.40 (Jacobian criterion for varieties)**.** *Let $X \subseteq \mathbb{C}^n$ be an irreducible affine variety of dimension $d = n - h$. Then*

$$\{a \in X \mid X \text{ is singular at } a\}$$

is equal to the vanishing locus of the $h \times h$-minors of $J(f_1,\dots,f_m)$ in X.

Proof. We have that $T_a(X) = \ker(J(f_1,\dots,f_m)|_{x=a})$, so $\dim(T_a(X)) = n - \mathrm{rank}(J(f_1,\dots,f_m)|_{x=a})$, and so X is singular at a if and only if the rank of $J(f_1,\dots,f_m)|_{x=a}$ is less than h. This is equivalent to the all of the $h \times h$ minors of the matrix $J(f_1,\dots,f_m)|_{x=a}$ vanishing. This happens at a point a if and only if each $h \times h$ minor of $J(f_1,\dots,f_m)$ evaluated at a is zero; i.e., $a \in X$ is in the vanishing locus of each $h \times h$ minor. □

Example 1.41. Consider $X = V(x^3 - y^2, z - xy)$. The Jacobian matrix is

$$\begin{bmatrix} 3x^2 & -2y & 0 \\ -y & -x & 1 \end{bmatrix}.$$

Since X has dimension 1 in 3 space, we consider the 2×2-minors

$$-3x^3 - 2y^2, 3x^2, -2y$$

so $x = 0, y = 0$, and using $z = xy$, $z = 0$, and this is the unique singular point on the curve.

Motivated by the geometric case, for a local ring $(R, \mathfrak{m}, k)$ we define $\mathfrak{m}/\mathfrak{m}^2$ to be the *cotangent space* and $\mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$ to be the *tangent space* of R. We recall that a local ring $(R, \mathfrak{m}, k)$ is *regular* $\dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

Example 1.42. If $R = \mathbb{C}[x_1,\dots,x_n]/I$ is a reduced finitely generated $\mathbb{C}$-algebra, and $\mathfrak{m}$ is a maximal ideal, then $R_{\mathfrak{m}}$ is regular if and only if the variety $X = V(I)$ is nonsingular at $a = V(\mathfrak{m})$.

Example 1.43. Let $R = \mathbb{Z}_{(2)}$. This is a local ring with maximal ideal (2). The dimension of R is the height of (2) in $\mathbb{Z}$, which is one, and the maximal ideal is generated by one element, so R is regular.

Example 1.44. Let $R = \mathbb{Z}[\sqrt{5}]_{(2,1+\sqrt{5})}$. Note that $2, 1+\sqrt{5}$ generates a maximal ideal in $\mathbb{Z}[\sqrt{5}]$. The ring $\mathbb{Z}[\sqrt{5}]$ has dimension one, since it is integral over $\mathbb{Z}$, and we see that R has dimension one as well. One can check that the maximal ideal $(2, 1+\sqrt{5})$ cannot be generated by one element; equivalently that these elements are $\mathbb{Z}/2\mathbb{Z}$-linearly independent modulo the square of this ideal. Thus, R is not regular.

Remark 1.45. It is often handy to use the following fact:

Let R be a ring and $\mathfrak{m}$ be a maximal ideal. Let M be an R-module such that for every $x \in M$, there is some n such that $\mathfrak{m}^n x = 0$. Then the localization map $M \to M_{\mathfrak{m}}$ is an isomorphism.

To see it, first note that for any $v \notin \mathfrak{m}$ and and $n \in \mathbb{N}$, there is some $w \notin \mathfrak{m}$ with $vw - 1 \in \mathfrak{m}^n$. Indeed, since the image of v in $R/\mathfrak{m}$, $v + \mathfrak{m}$, is a unit, there is some $u + \mathfrak{m} \in R/\mathfrak{m}$ that is its inverse, so $vu + \mathfrak{m} = 1 + \mathfrak{m}$. For an arbitrary representative u, we have $vu = 1 - a$ for some $a \in \mathfrak{m}$. Take $w = u(1 + a + a^2 + \cdots + a^{n-1})$. Then

$$vw = vu(1 + a + a^2 + \cdots + a^{n-1}) = (1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1 - a^n,$$

with $a^n \in \mathfrak{m}^n$.

Now, to show that the localization map is injective, we need to check that for any $x \neq 0$, $\mathfrak{x}1$ is nonzero as well, so $vx \neq 0$ for any $v \notin \mathfrak{m}$. Take n such that $\mathfrak{m}^n x = 0$, and $w \notin \mathfrak{m}$ with $vw - 1 \in \mathfrak{m}^n$. In particular, $(vw - 1)x - 0$ so $x = vwx$. Then $0 \neq x = vwx$ so $vw \neq 0$. To show that the localization map is surjective, we show that for any $x \in M$ and $v \notin \mathfrak{m}$, there is some $y \in M$ with $\frac{x}{v} = \frac{y}{1}$. With n and w as above, take $y = wx$: since $vwx = x$, the equality holds.

1.5. **Localization.** We include one more property of derivations.

Proposition 1.46. *Let R be an A-algebra. Let $W \subseteq R$ be a multiplicative set and $V = W \cap A$. For any $W^{-1}R$ module M, any A-linear derivation $\partial : R \to M$ extends uniquely to an A-linear derivation $W^{-1}R \to M$ given by the rule*

$$\widetilde{\partial}\left(\frac{r}{w}\right) = \frac{w\partial(r) - r\partial(w)}{w^2},$$

and this extension is $V^{-1}A$-linear. Conversely, any A-linear derivation from $W^{-1}R \to M$ is of this form.

That is, there are isomorphisms

$$\mathrm{Der}_{R|A}(M) \to \mathrm{Der}_{W^{-1}R|A}(M) \to \mathrm{Der}_{W^{-1}R|V^{-1}A}(M).$$

Proof. We omit the verification that the rule for the map $W^{-1}R \to M$ is well-defined, that this is $V^{-1}A$-linear, and satisfies the product rule.

If $\alpha : W^{-1}R \to M$ is an A-linear derivation, by restriction through the localization map, we get a derivation $\partial : R \to M$ with $\widetilde{\partial} \circ i = \partial$. We claim that $\alpha = \widetilde{\partial}$. Indeed,

$$\partial(r) = \alpha(r) = \alpha(\frac{r}{w}w) = w\alpha(\frac{r}{w}) + \frac{r}{w}\alpha(w) = w\alpha(\frac{r}{w}) + \frac{r}{w}\partial(w),$$

so

$$\alpha(\frac{r}{w}) = \frac{\partial(r) - \frac{r}{w}\partial(w)}{w} = \widetilde{\partial}(\frac{r}{w}).$$

□

Lecture of February 14, 2023

1.6. **Left-exact sequences.** We now encode many of the key properties of derivations in some left-exact sequences. Recall that a sequence of maps of R-modules is a *left exact sequence* is an exact sequence of R-module maps of the form

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N.$$

That is, α and β are R-module homomorphisms such that with α is injective and $\ker(\beta) = \mathrm{im}(\alpha)$.

Proposition 1.47. *Let R be an A-algebra and*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

be a left exact sequence of R-modules. Then

$$0 \to \mathrm{Der}_{R|A}(L) \xrightarrow{\alpha_*} \mathrm{Der}_{R|A}(M) \xrightarrow{\beta_*} \mathrm{Der}_{R|A}(N)$$

is a left exact sequence, where $\alpha_*(\partial) = \alpha \circ \partial$ and likewise with β_*.

Proof. First we observe that α_* is R-linear, since $\alpha_*(\partial + \partial') = \alpha_*\partial + \alpha_*\partial'$ and $\alpha_*(r\partial) = r\alpha_*\partial$.

Since α is injective, if $\partial \neq 0$, then $\alpha_*\partial \neq 0$. If $\beta_*(\partial) = 0$, then $\beta\partial(r) = 0$ for all $r \in R$, so $\partial(r) \in \ker(\beta) = \mathrm{im}(\alpha)$ for all $r \in R$, and since α is injective, there is an R-linear map $\alpha^{-1} : \mathrm{im}(\alpha) \to L$; then $\partial = \alpha_*(\alpha^{-1} \circ \partial) \in \mathrm{im}(\alpha_*)$. □

Proposition 1.48. *Let $A \to R \xrightarrow{\phi} S$ be ring homomorphisms, and M be an S-module. Then there is a left exact sequence*

$$0 \to \mathrm{Der}_{S|R}(M) \xrightarrow{\mathrm{inc}} \mathrm{Der}_{S|A}(M) \xrightarrow{\phi^*} \mathrm{Der}_{R|A}(M)$$

where inc *is the inclusion map and ϕ^* is precomposition with ϕ.*

Proof. We start by noting that $\mathrm{Der}_{S|R}(M)$ naturally includes in $\mathrm{Der}_{S|A}(M)$, since any R-linear map is automatically linear over the image of A.

If $\partial = \mathrm{inc}(\theta)$, then $\phi^*(\partial) = \partial \circ \phi$ is an R-linear derivation on R, which must be zero. Conversely, if $\phi^*(\partial) = \partial \circ \phi$ is zero, then $\phi(R)$ is in the kernel of ∂, so ∂ is R-linear, and hence i the image of inc. □

Proposition 1.49. *Let $A \to R \xrightarrow{\pi} R/I$ be ring homomorphisms, and M be an R/I-module. Then there is a left exact sequence*

$$0 \to \mathrm{Der}_{R/I|A}(M) \xrightarrow{\pi^*} \mathrm{Der}_{R|A}(M) \xrightarrow{\mathrm{res}} \mathrm{Hom}_R(I/I^2, M).$$

Proof. First, we have π^* is injective, since if $\partial([r]) = 0$, then $\pi^*(\partial)(r) = \partial\pi(r) = \partial([r]) \neq 0$.

If $\partial = \pi^*(\theta)$, then $\mathrm{res}(\partial)([a]) = \theta \circ \pi([a]) = \theta(0)$ for $[a] \in I/I^2$, so $\mathrm{res} \circ \pi^* = 0$. Conversely, if $\mathrm{res}(\partial) = 0$, then $\partial(a) = 0$ for all $a \in I$, so ∂ yields a well-defined derivation from $R/I \to M$; i.e., is in the image of π^*. □

Proposition 1.50. *Let $A \to R \xrightarrow{\pi} R/I$ be ring homomorphisms, and suppose that there is an A-algebra homomorphism $\tau : R/I \to R/I^2$ such that $\tau\pi : R \to R/I^2$ is just the quotient map. Then the sequence*

$$0 \to \mathrm{Der}_{R/I|A}(M) \xrightarrow{\pi^*} \mathrm{Der}_{R|A}(M) \xrightarrow{\mathrm{res}} \mathrm{Hom}_R(I/I^2, M) \to 0$$

is exact.

Proof. Follows from the previous, plus proposition on surjectivity of res. □

2. Kahler differentials

2.1. **Restriction and extension of scalars.**

2.1.1. *Hom.*

Definition 2.1. Let L, M, N be R-modules.

- The *module of homomorphisms* from M to N is
$$\mathrm{Hom}_R(M,N) := \{\phi : M \to N \mid \phi \text{ is } R\text{-linear}\}.$$
The R-module structure is given by the rule $r \cdot \phi$ is the homomorphism $m \mapsto r\phi(m) = \phi(rm)$.
- If $\alpha : M \to N$ is a module homomorphism, we define a map $\mathrm{Hom}_R(L,\alpha)$ or α_* from $\mathrm{Hom}_R(L,M) \to \mathrm{Hom}_R(L,N)$ by the rule
$$\alpha_*(\phi) = \alpha \circ \phi;$$
i.e.,
$$\alpha_* : \quad (\ L \xrightarrow{\phi} M\ ) \ \mapsto \ (\ L \xrightarrow{\alpha} M \xrightarrow{\phi} N\ ).$$
- If $\alpha : M \to N$ is a module homomorphism, we define a map $\mathrm{Hom}_R(\alpha,L)$ or α^* from $\mathrm{Hom}_R(N,L) \to \mathrm{Hom}_R(M,L)$ by the rule
$$\alpha^*(\phi) = \phi \circ \alpha;$$
i.e.,
$$\alpha^* : \quad (\ N \xrightarrow{\phi} L\ ) \ \mapsto \ (\ M \xrightarrow{\alpha} N \xrightarrow{\phi} L\ ).$$

Thus, given a fixed R-module L, $F(-) := \mathrm{Hom}_R(L,-)$ is a rule that assigns to any R-module M another R-module $F(M)$, and to any homomorphism $M \xrightarrow{\phi} N$ a homomorphism $F(M) \xrightarrow{F(\phi)} F(N)$. This plus the fact that F takes the identity map to the identity map and compositions to compositions makes F a *covariant functor* from R-modules to R-modules.

Similarly, given a fixed R-module L, $G(-) := \mathrm{Hom}_R(-,L)$ is rule that assigns to any R-module M another R-module $G(M)$, and to any homomorphism $G(M) \xrightarrow{\phi} G(N)$ a homomorphism $G(N) \xrightarrow{G(\phi)} G(M)$. This plus the fact that F takes the identity map to the identity map and compositions to compositions makes G a *contravariant functor* from R-modules to R-modules. The covariant vs. contravariant bit refers to whether the directions of maps have changed.

Given maps $L \xrightarrow{\alpha} L'$ and $M \xrightarrow{\beta} M'$, we likewise get a map $\mathrm{Hom}_R(L',M) \xrightarrow{\mathrm{Hom}_R(\alpha,\beta)} \mathrm{Hom}_R(L,M')$, by combining the constructions above.

Example 2.2. $\mathrm{Hom}_R(R,M) \cong M$ by $\phi \mapsto \phi(1)$, and under this isomorphism, $M \xrightarrow{\alpha} N$ corresponds to $1 \mapsto m \rightsquigarrow 1 \mapsto \alpha(m)$ under this isomorphism.

If I is an ideal, $\mathrm{Hom}_R(R/I,M) \cong \mathrm{ann}_M(I)$ by the same map: the image of 1 in R/I must map to something killed by I, and there is a unique R-linear map that does this. The same recipe for maps as above holds. Thus, we can identify $\mathrm{Hom}_R(R/I,-)$ with the functor that sends modules M to $\mathrm{ann}_M(I)$, and sends maps to their restrictions to these submodules.

We recall that a sequence of maps of R-modules is *split-exact* if it is of the form
$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$
with α injective, β surjective, $\ker(\beta) = \mathrm{im}(\alpha)$ and α has a left inverse (i.e., there is a map ρ such that $\rho\alpha$ is the identity on L). It is equivalent if we replace the last condition with β has a right inverse (i.e., there is a map ι such that $\beta\iota$ is the identity on N.

Theorem 2.3. (1) *A sequence of maps*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

is exact if and only if, for all R-modules X, the sequence

$$0 \to \mathrm{Hom}_R(X, L) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, M) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, N)$$

is exact.

(2) *A sequence of maps*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

is split-exact if and only if, for all R-modules X, the sequence

$$0 \to \mathrm{Hom}_R(X, L) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, M) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, N) \to 0$$

is exact.

(3) *A sequence of maps*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

is right-exact if and only if, for all R-modules X, the sequence

$$0 \to \mathrm{Hom}_R(N, X) \xrightarrow{\beta^*} \mathrm{Hom}_R(M, X) \xrightarrow{\alpha^*} \mathrm{Hom}_R(L, X)$$

is left-exact.

(4) *A sequence of maps*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

is split-exact if and only if, for all R-modules X, the sequence

$$0 \to \mathrm{Hom}_R(N, X) \xrightarrow{\beta^*} \mathrm{Hom}_R(M, X) \xrightarrow{\alpha^*} \mathrm{Hom}_R(L, X) \to 0$$

is exact.

Proof. (1) Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ be exact, and X be an R-module.

- α_* is injective: if $X \xrightarrow{\phi} L$ is nonzero, $X \xrightarrow{\phi} L \xrightarrow{\alpha} M$ is as well, since a nonzero element in the image of ϕ goes to something nonzero in the composition.
- $\ker(\beta_*) = \mathrm{im}(\alpha_*)$: $X \xrightarrow{\phi} M \xrightarrow{\beta} N$ is zero if and only if $\mathrm{im}(\phi) \subseteq \ker(\beta) = \mathrm{im}(\alpha)$, which happens if and only if ϕ factors through L; i.e., $\phi \in \mathrm{im}(\alpha_*)$.

The other direction of the first part follows from the example above; we can use $X = R$.

(2) Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be split-exact, and X be an R-module. In particular, $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is a left exact sequence, so

$$0 \to \mathrm{Hom}_R(X, L) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, M) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, N)$$

is exact. We just need to see that $\mathrm{Hom}_R(X, M) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, N)$ is surjective. Let ι be such that $\beta\iota$ is the identity on N. Then $\beta_*\iota_*$ is the identity on $\mathrm{Hom}_R(X, M)$, so β_* must be surjective.

For the converse, take $X = N$. Then the identity map in $\mathrm{Hom}_R(N, N)$ is in the image of β_*, so there is a map $\rho \in \mathrm{Hom}_R(M, N)$ such that $\beta\rho = \beta_*(\rho)$ is the identity on N, as required.

(3) Let $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a right-exact sequence, and X be an R-module.

- β^* is injective: if $N \xrightarrow{\phi} X$ is nonzero, pick $n \in N$ not in the kernel, and $m \in M$ that maps to n. Then, the image of m under $M \xrightarrow{\beta} N \xrightarrow{\phi} X$ is nonzero.

- $\ker(\alpha^*) = \operatorname{im}(\beta_*)$: $L \xrightarrow{\alpha} M \xrightarrow{\phi} X$ is zero if and only if $\operatorname{im}(\alpha) \subseteq \ker(\phi)$, which happens if and only if ϕ descends to a map of the form $N \cong M/\operatorname{im}(\alpha) \to X$; i.e., $\phi \in \operatorname{im}(\alpha^*)$.

Let $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a sequence of maps, and suppose that it is exact after applying $\operatorname{Hom}_R(-, X)$ for all X.

- β is surjective: if not, let $X = N/\operatorname{im}(\beta)$. There is a nonzero projection map $N \xrightarrow{\phi} X$, but $M \xrightarrow{\beta} N \xrightarrow{\phi} X$ is zero, contradicting injectivity of β^*.
- $\ker(\beta) \supseteq \operatorname{im}(\alpha)$: Take $X = N$, and $N \xrightarrow{\mathrm{id}} X$. Since $\ker(\alpha^*) \supseteq \operatorname{im}(\beta^*)$, $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \xrightarrow{\mathrm{id}} X = L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is zero.
- $\ker(\beta) \subseteq \operatorname{im}(\alpha)$: Take $X = M/\operatorname{im}(\alpha)$, and $M \xrightarrow{\phi} X$ the projection map. Since $L \xrightarrow{\alpha} M \xrightarrow{\phi} X$ is zero, ϕ is in the image of β^*, so it factors through β. This is equivalent to the stated containment.

(4) Similar to (2). □

In short, $\operatorname{Hom}_R(X, -)$ is kernel-preserving, and $\operatorname{Hom}_R(-, X)$ turns cokernels into kernels.

Given a ring homomorphism $\phi : R \to S$, we can use ϕ to turn S-modules and S-algebras into R-modules and R-algebras with *restriction of scalars* and vice versa with *extension of scalars*.

2.1.2. *Restriction of scalars.* Given $\phi : R \to S$ and an S-module N, we get an R-module $\phi_*(N)$ by *restriction of scalars* by keeping the same set and same addition, so $\phi_*(N) = N$ as additive groups, and the R-module action $r \cdot n := \phi(r) \cdot n$, where the left-hand side is the action in $\phi_*(N)$ and the right hand side is the original S-action. When $\phi : R \to S$ is just an inclusion map $R \subseteq S$, this restriction of scalars is literally just restricting which scalars we consider in the module action.

For example, consider $R = \mathbb{C} \subseteq S = \mathbb{C}[x]$ and $N = \mathbb{C}[x]/(x^3)$. N is a cyclic S-module killed by some stuff, but we can also "forget about the action of x" and consider N as a $\mathbb{C}$-vectorspace; as such it is just a free 3-generated R-module.

Given a homomorphism of S-modules $\alpha : N \to N'$, we can call $\phi_*(\alpha)$ the same map from $\phi_*(N) \to \phi*(N)$, which is a homomorphism of R-modules.

We can think of this restriction of scalars ϕ_* as the "demotion" functor, when demotes modules from a "bigger" (target of ϕ) ring to a "smaller" (source of ϕ) ring.

In the same way, we can demote S-algebras to R-algebras: if T is an S-algebra with structure map $\psi : S \to T$ take $\phi_*(T)$ to be the same ring T with structure map $\psi \circ \phi : R \to T$.

To promote a module or an algebra, we have to do something a bit more interesting. For example, consider $R = \mathbb{C} \subseteq S = \mathbb{C}[x]$ and $M = \mathbb{C}^3$, a free R-module of rank 3. There is no "obvious" or "natural" R-module structure on M, so we'll end up changing our underlying set. The "right" way of going about this is by using tensor products, but we'll take a barehanded approach using presentations, and everyone is encouraged to reconcile the two approaches now if they know tensors and, if not, later when they do.

2.1.3. *Presentations of modules.* Let M be an R-module.

Given a generating set $\{m_\lambda\}_{\lambda \in \Lambda}$ for M, there is a surjection from a free module onto M:

$$\begin{array}{ccc} \{m_\lambda\}_{\lambda\in\Lambda} & \rightsquigarrow & R^{\oplus\Lambda} \to M \to 0 \\ \text{generating set} & & e_\lambda \mapsto m_\lambda \end{array}$$

and conversely any such surjection yields a generating set (consisting of the images of the basis vectors).

The kernel of this map is a submodule of $R^{\oplus\Lambda}$ which are the relations on these generators. We can take a subset $\{v_\gamma\}_{\gamma\in\Gamma}$ that generates the module of relations (a set of *defining relations*) and map a free module

onto them:

$$\begin{array}{ccccc} \{m_\lambda\}_{\lambda\in\Lambda} & + & \{v_\gamma\}_{\gamma\in\Gamma} & \rightsquigarrow & R^{\oplus\Gamma} \longrightarrow R^{\oplus\Lambda} \longrightarrow M \to 0 \\ \text{generating set} & & \text{defining relations} & & e'_\gamma \mapsto v_\gamma \quad e_\lambda \mapsto m_\lambda \end{array}$$

Conversely, any such right exact sequence is a recipe for a set of generators and defining relations on M. The map between free modules is given by multiplication by a (possibly infinite) matrix A whose γ column consists of the λ-coordinates of v_γ; concretely, each column is a relation on the m_λ's. When Λ and Γ are finite, we'll just write something like

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

and A will be an actual $n \times m$ matrix, standing for the map of multiplication (on the left) by A. We will call this (either in the finite or infinite case) a *presentation matrix* for M.

Given a presentation matrix, we can recover M up to isomorphism as $M \cong R^n/\operatorname{im}(A)$ (i.e., the *cokernel* of the map A) coming from the first isomorphism theorem, since the map from $R^n \to M$ is surjective with kernel $\operatorname{im}(A)$. The rows of the presentation matrix correspond to generators, and the columns correspond to relations.

2.1.4. *Extension of scalars for modules.* We're now ready to describe *extension of scalars*, or *promotion* of a module along a ring homomorphism. Let $\phi : R \to S$ be a ring homomorphism and M be an R-module. We define the extension of scalars of M, denoted $\phi^*(M)$ or $S \otimes_R M$ as follows. Take a presentation of M:

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

then $\phi^*(M)$ is the S-module with the same presentation

$$S^m \xrightarrow{\phi(A)} S^n \to \phi^*(M) \to 0.$$

Lecture of February 16, 2023

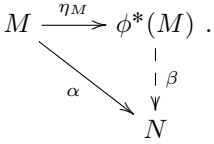
It's not clear that what we did does not depend on the choice of presentation. However, we will show that the $\phi^*(M)$ satisfies an important universal property and use that to show it is well-defined.

First we note that there is an R-module homomorphism from $\eta_M : M \to \phi^*(M)$ (or more properly, to $\phi_*\phi^*(M)$). Given $r \in R$ write $m = \sum_i r_i[e_i]$, where the e_i's are the standard basis in R^n. For convenience, set $\mathbf{e}$ to be the row vector with entries $e_1, \ldots, e_n$ and $\mathbf{r}$ be the column vector of $r_1, \ldots, r_n$ so $m = \mathbf{er}$. We map m to $\mathbf{e}\phi(\mathbf{r}) = \sum_i \phi(r_i)[e_i]$. If m also equals $\sum_i r'_i[e_i] = \mathbf{er'}$, then $\mathbf{e}(\mathbf{r} - \mathbf{r'}) = 0$ so $\mathbf{r} - \mathbf{r'} = A\mathbf{v}$ for some $\mathbf{v}$, and hence

$$\mathbf{e}\phi(\mathbf{r}) - \mathbf{e}\phi(\mathbf{r'}) = \mathbf{e}\phi(\mathbf{r} - \mathbf{r'}) = \mathbf{e}\phi(A\mathbf{v}) = \mathbf{e}\phi(A)\mathbf{v},$$

so this is zero in $\phi^*(M)$. It is then clear to see that this is R-linear.

Proposition 2.4. *Let $\phi : R \to S$ be a ring homomorphism. Let M be an R-module, N be an S-module, and $\alpha : M \to \phi_*(N)$ be an R-module homomorphism. Then there exists a unique S-module homomorphism $\beta : \phi_*(M) \to N$ that makes the diagram commute:*



Proof. We will abuse notation and drop the ϕ to identify elements in R with their images in S.

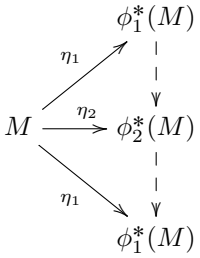
Let $\alpha([e_i]) = n_i$ and write $\mathbf{n}$ for the row vector $[n_1, \ldots, n_t]$. We define $\beta(\sum_i s_i[e_i']) = \sum_i s_i n_i$, or $\beta(\mathbf{es}) = \mathbf{ns}$ for short. To see that this is well-defined, suppose that $\sum_i s_i[e_i'] = \sum_i s_i'[e_i']$, and write $\mathbf{s}$ and $\mathbf{s}'$ for the column vectors of s_i and s_i'. We need to show that $\mathbf{ns} = \mathbf{ns}'$. By construction of $\phi^*(M)$, we have that $\mathbf{s} - \mathbf{s}' = A\mathbf{v}$ for some vector $\mathbf{v}$ with entries in S. Since α is well-defined, we must have that for any columns of A, the corresponding combination of basis vectors maps to zero, so the corresponding combination of the n's is zero; i.e., $\mathbf{n}A = 0$. But then $\mathbf{n}A\mathbf{v} = \mathbf{n}(\mathbf{s} - \mathbf{s}')$, and this shows the claim. Checking S-linearity is straightforward from the construction. For uniqueness, $\phi^*(M)$ is generated by $[e_i]$, and $n_i = \alpha([e_i]) = \beta\eta_M([e_i]) = \beta([e_i'])$, so the generators must go to the same place, and hence there can only be one map. □

In other words, the proposition says that for any R-module M and S-module N, there is an isomorphism

$$\mathrm{Hom}_S(\phi^* M, N) \xrightarrow{\eta_M^*} \mathrm{Hom}_R(M, \phi_* N).$$

Corollary 2.5. *$\phi : R \to S$ be a ring homomorphism, and M be an R-module. Fix two presentations for M, and let $(\phi_1^*(M), \eta_1^M)$ and $(\phi_2^*(M), \eta_2^M)$ be the two modules and morphisms constructed above for each presentation. Then $\phi_1^*(M) \cong \phi_2^*(M)$ as S-modules. Moreover, there is a unique S-module isomorphism θ for which $\eta_2^M = \theta \circ \eta_1^M$.*

Proof. It suffices to show that there is an isomorphism that makes $\eta_2^M = \theta \circ \eta_1^M$, for the uniqueness will follow from the proposition applied with $\alpha = \eta_2$. Consider the diagram



The universal property yields unique S-module dotted maps making the triangles commute. The double down composition and the identity map on $\phi_1^*(M)$ are two maps that make the big triangle commute. Applying the uniqueness in the proposition with $\alpha = \eta_1$, we get that the composition is the identity. We can switch the roles of ϕ_1^* and ϕ_2^* to get that the other composition is the identity. Thus, the induced map is an isomorphism. □

Corollary 2.6. *Let $\phi : R \to S$ be a ring homomorphism. For any R-module homomorphism $\alpha : M \to N$, there is a unique S-module homomomorphism $\phi^*\alpha : \phi^* M \to \phi^* N$ such that $\phi^*\alpha \circ \eta_M = \eta_N \circ \alpha$.*

Proof. Apply the universal property of $(\phi^* M, \eta_M)$ to $\eta_N \circ \alpha$. □

Tracing the proof of the universal property, we see that $\phi^*\alpha$ can be computed as follows: take presentations for M and N, and lift α to a matrix from the free modules over M and N; then use the same matrix for $\phi^*\alpha$.

Lemma 2.7. *Under the isomorphisms $\mathrm{Hom}_S(\phi^* M, N) \xrightarrow{\eta_M^*} \mathrm{Hom}_R(M, \phi_* N)$, the map $\mathrm{Hom}_S(\phi^*\alpha, N)$ corresponds to $\mathrm{Hom}_R(\alpha, N)$. That is, for an R-module homomorphism $\alpha : L \to M$ and S-module N, there is a*

commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_S(\phi^*M, N) & \xrightarrow{\mathrm{Hom}_S(\phi^*\alpha, N)} & \mathrm{Hom}_S(\phi^*L, N) \\ \cong \downarrow \eta_M^* & & \cong \downarrow \eta_L^* \\ \mathrm{Hom}_R(M, N) & \xrightarrow{\mathrm{Hom}_R(\alpha, N)} & \mathrm{Hom}_R(L, N) \end{array}$$

Proof. First, by construction of $\phi^*\alpha$, we have a commutative diagram:

$$\begin{array}{ccc} \phi^*M & \xleftarrow{\phi^*\alpha} & \phi^*L \\ \uparrow \eta_M & & \uparrow \eta_L \\ M & \xleftarrow{\alpha} & L \end{array}$$

Then using this commutativity, given an S-linear map $\theta : \phi^*M \to N$, we have that

$$(\eta_L^* \circ \mathrm{Hom}(\phi^*\alpha, N))(\theta) = \theta \circ \phi^*\alpha \circ \eta_L = \theta \circ \alpha \circ \eta_M = (\mathrm{Hom}(\alpha, N) \circ \eta_M^*)(\theta). \qquad \square$$

Proposition 2.8. *Let $\phi : R \to S$ be a ring homomorphism, and*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

be a right exact sequence of R-modules. Then the sequence of S-modules

$$\phi^*L \xrightarrow{\phi^*\alpha} \phi^*M \xrightarrow{\phi^*\beta} \phi^*N \to 0$$

is exact.

Proof. Let X be an arbitrary S-module. Applying Hom into X to the sequence above, we have a sequence:

$$0 \to \mathrm{Hom}_S(\phi^*N, X) \xrightarrow{\mathrm{Hom}(\phi^*\beta, X)} \mathrm{Hom}_S(\phi^*M, X) \xrightarrow{\mathrm{Hom}(\phi^*\alpha, X)} \mathrm{Hom}_S(\phi^*L, X).$$

We have isomorphisms

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_S(\phi^*N, X) & \xrightarrow{\mathrm{Hom}(\phi^*\beta, X)} & \mathrm{Hom}_S(\phi^*M, X) & \xrightarrow{\mathrm{Hom}(\phi^*\alpha, X)} & \mathrm{Hom}_S(\phi^*L, X) \\ \| & & \| & & \| & & \| \\ 0 & \longrightarrow & \mathrm{Hom}_R(N, X) & \xrightarrow{\mathrm{Hom}(\beta, X)} & \mathrm{Hom}_R(M, X) & \xrightarrow{\mathrm{Hom}(\alpha, X)} & \mathrm{Hom}_R(L, X) \end{array}$$

The last row is exact, by left exactness of Hom (part (3) in the forward implication). But then by left exactness of Hom again, since this is true for all X, the sequence we consider is exact. $\square$

In general, exact sequences (or left exact sequences) no longer remain exact. We say that a ring homomorphism $\phi : R \to S$ is *flat* if it has the special property that extension of scalars preserves exact sequences.

Proposition 2.9. *Let R be a ring and W be a multiplicative set. Let $\phi : R \to W^{-1}R$ be the localization map. Then $\phi^*(M) \cong W^{-1}M$ for any R-module M.*

Proof. Let $\eta : M \to W^{-1}M$ be the localization map. We will show that $(W^{-1}M, \eta)$ satisfies the universal property of ϕ^*M. If N is any $W^{-1}R$-module, and $\alpha : M \to N$ is a homomorphism, define $\beta : W^{-1}M \to N$ by sending $\beta(\frac{m}{w}) = \frac{\alpha(m)}{w}$. The check that this β is well-defined and $W^{-1}R$-linear is straightforward; that it is the unique map making the diagram commute follows from the fact that the image of M generates $W^{-1}M$ as a $W^{-1}R$-module. $\square$

2.1.5. *Presentations of algebras.* We can play a similar game with algebras. Let S be an R-algebra, so there is some $\phi : R \to S$. Given a generating set for S as an algebra, we get a surjection from a polynomial ring:

$$\begin{array}{ccc} \{s_\lambda\}_{\lambda\in\Lambda} & \rightsquigarrow & R[\{x_\lambda\}_{\lambda\in\Lambda}] \to S \to 0 \\ \text{algebra generating set} & & x_\lambda \mapsto s_\lambda \end{array}$$

The kernel is an ideal I, for which we can pick generators ($\{f_\gamma\}_{\gamma\in\Gamma}$) and we get

$$\begin{array}{ccccc} \{s_\lambda\}_{\lambda\in\Lambda} & + & \{f_\gamma\}_{\gamma\in\Gamma} & \rightsquigarrow & R[\{x_\lambda\}_{\lambda\in\Lambda}]^{\oplus\Gamma} \longrightarrow R[\{X_\lambda\}_{\lambda\in\Lambda}] \longrightarrow S \to 0 \\ \text{algebra generating set} & & \text{defining relations} & & e'_\gamma \mapsto f_\gamma \qquad e_\lambda \mapsto s_\lambda \end{array}$$

Note that we have *polynomial* relations rather than linear relations now, so we can't use a matrix to describe them anymore.

Given an R-algebra S with an algebra presentation $S \cong R[x_1, \dots, x_n]/(f_1, \dots, f_m)$, we can also ask what S looks like as an R-module. As a generating set, we can take the monomials $\{x_1^{a_1} \cdots x_n^{a_n} \mid a_i \in \mathbb{N}\}$. The relations are generated as an $R[x_1, \dots, x_n]$-module by $f_1, \dots, f_m$; to find an R-module generating set of the relations, we can take $\{x_1^{a_1} \cdots x_n^{a_n} f_j \mid a_i \in \mathbb{N}, j = 1, \dots, m\}$ and collect the coefficients of the monomials, and this gives a presentation. That is, if $f_j = \sum_a c_{a,j} x^a$ for some tuples a, then $\{\sum_a c_{a,j} x^{a+b} \mid b \in \mathbb{N}^n, j = 1, \dots, m\}$ is a defining set of relations.

For example, consider $R = \mathbb{Z}[x]/(2x^2-5)$. Let's find a $\mathbb{Z}$-module presentation of this ring. As a generating set, we have $1, x, x^2, x^3, \dots$; the relations are given by $2x^2-5, 2x^3-5x, 2x^4-5x^2, \dots$; the presentation matrix is

$$\begin{bmatrix} -5 & 0 & \cdots & & \\ 0 & -5 & 0 & \cdots & \\ 2 & 0 & -5 & 0 & \cdots \\ 0 & 2 & 0 & -5 & \ddots \\ & \ddots & \ddots & \ddots & \ddots \end{bmatrix}$$

2.1.6. *Base change for algebras.* Let's promote some algebras too. We'll follow the same recipe: take a presentation (as an algebra) and upgrade the base ring. That is, let $\phi : R \to S$ be a ring homomorphism and T be an R-algebra. We define the *extension of scalars* or *base change* of T as follows. Write

$$R[X_1, \dots, X_n]^m \xrightarrow{[f_1,\dots,f_m]} R[X_1, \dots, X_n] \to T \to 0;$$

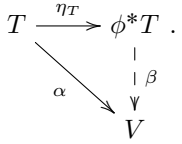
then $\phi^*(T)$ is the S-algebra with presentation

$$S[X_1, \dots, X_n]^m \xrightarrow{[\phi(f_1),\dots,\phi(f_m)]} S[X_1, \dots, X_n] \to \phi^*(T) \to 0.$$

Note that we are using the same notation as module extension of scalars, though it is not immediately clear these should be related. For starters, in analogy with the module extension of scalars, one has:

Proposition 2.10. *For a ring homomorphism $\phi : R \to S$ and an R-algebra T, the base change ϕ^*T admits an R-algebra homomorphism $\eta_T : T \to \phi^*T$ that satisfies the universal property that for any S-algebra V and R-algebra homomorphism $\alpha : R \to V$, there is a unique S-algebra homomorphism $\beta : \phi^*T \to V$ that*

makes the diagram commute:



Consequently, ϕ^*T is well-defined (independent of the choice of presentation) up to isomorphism.

Proof. Omitted; similar to what we did with modules. □

Another key point is that this base change operation for algebras agrees with that for modules. Namely:

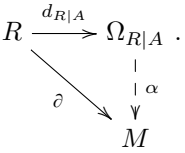
Proposition 2.11. *Let $\phi : R \to S$ be a ring homomorphism and T an R-algebra. Then the S-algebra ϕ^*T obtained by extension of scalars of R-algebras along ϕ, considered as an S-module, is isomorphic to the extension of scalars of T considered as an S-module.*

Proof. Take a presentation of T as an R-algebra, and take the presentation as an R-module obtained from it as discussed above, i.e., with relations $\{\sum_a c_{a,j}x^{a+b} \mid b \in \mathbb{N}^n, j = 1, \dots, m\}$ for an algebra generating set $f_j = \sum_a c_{a,j}x^a$. If we take algebra extension of scalars of T, then we get the same presentation as an S-module by this formula. □

Lecture of February 23, 2023

2.2. **Kahler differentials.**

Definition 2.12. Let R be an A-algebra. A derivation $d_{R|A} : R \to \Omega_{R|A}$ to some R-module $\Omega_{R|A}$ is called a *universal derivation* of R over A if for any A-linear derivation $\partial : R \to M$ to any R-module M, there is a unique R-module homomorphism $\alpha : \Omega_{R|A} \to M$ such that $\partial = \alpha \circ d_{R|A}$:



We call the target module $\Omega_{R|A}$ a *module of differentials* or module of *Kahler differentials* of R over A.

Theorem 2.13. *Let R be an A-algebra. There exists a universal derivation of R over A. Given two universal derivations $d_{R|A} : R \to \Omega_{R|A}$ and $d'_{R|A} : R \to \Omega'_{R|A}$ of R over A, there is a unique isomorphism $\alpha : \Omega_{R|A} \cong \Omega'_{R|A}$ such that $\alpha d = d'$. In particular, there exists a module of differentials that is unique up to isomorphism.*

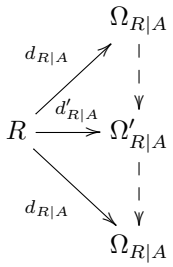
Proof. **Existence of universal derivation:** Let F be a free module with basis $\{dr \mid r \in R\}$, and $d : R \to F$ be function $d(r) = dr$. (Note that this function is not a homomorphism in any sense, just a function.) Let J be the submodule of F generated by the elements of the form

- $d(r + s) - dr - ds$, $r, s \in R$,
- $d(rs) = rds - sdr$, $r, s \in R$,
- $d(ar) = adr$, $a \in A$, $r \in R$,

and set $\Omega = F/J$, and by abuse of notation d the map $R \to \Omega$. First, we observe that d is an A-linear derivation: the relations in J force each rule to hold. Now, suppose that $\partial : R \to M$ is a derivation. We need to see that there is exactly one R-module homomorphism $\alpha : \Omega \to M$ such that $\alpha \circ d = \partial$. There is at most

one, since Ω is generated by the elements dr and $\alpha(dr) = \alpha(d(r)) = \partial(r)$, so the images of the generators are determined. To see that the map $\alpha : F \to M$ given on the generators dr as $\alpha(dr) = \partial(r)$ gives a well-defined R-module homomorphism $\alpha : \Omega \to M$, we just need to check that $\alpha(J) = 0$, or equivalently that α maps each of the generators of J to zero. But $\alpha(d(r+s) - dr - ds) = \partial(r+s) - \partial(r) - \partial(s) = 0$, and similarly for the other rules since ∂ is an A-linear derivation. Thus, such a map α exists (and, still, is unique). This shows that $d : R \to \Omega$ is a universal derivation.

Uniqueness of universal derivation: This is the analogous to the proof for extension of scalars: Uniqueness of the isomorphism (if it exists) is immediate from the universal property. Consider the diagram



The identity map on $\Omega_{R|A}$ makes the big triangle commute, and by uniqueness, the vertical maps must compose to the identity. Switch roles to get that the two maps compose to the identity the other way. □

From the definition of module of differentials, we have:

Lemma 2.14. *For any R-algebra A and R-module M, there is an isomorphism*

$$\mathrm{Hom}_R(\Omega_{R|A}, M) \xrightarrow{d^*_{R|A}} \mathrm{Der}_{R|A}(M),$$

where $d^*_{R|A}$ is precomposition by $d_{R|A}$.

Thus, the single module $\Omega_{R|A}$ contains all of the information about all of the A-linear derivations from R to any R-module! Of course, translating back and forth may be challenging in general.

It turns out that we have computed the module of differentials is a relatively broad setting already.

Theorem 2.15. *Let A be a ring, and $R = A[x_\lambda \mid \lambda \in \Lambda]$ be a polynomial ring over A. The module of differentials $\Omega_{R|A}$ of R over A is a free R-module with basis $\{dx_\lambda \mid \lambda \in \Lambda\}$, and the universal derivation is given by*

$$d_{R|A}(f) = \sum_{\lambda \in \Lambda} \frac{df}{dx_\lambda}\, dx_\lambda.$$

Proof. We know that this is a valid derivation based on our earlier computation of derivations on polynomial rings. Let us see that it is universal. Given any R-module M, we have that every derivation $\partial : R \to M$ can be written uniquely in the form $\sum_{\lambda \in \Lambda} \frac{df}{dx_\lambda} m_\lambda$. If $\partial = \alpha \circ d$, then $m_\lambda = \partial(x_\lambda) = \alpha(dx_\lambda)$, and this uniquely determines α, so there is at most one homomorphism that makes the diagram commute in the universal property. On the other hand, if we take the R-linear map given by this equation, then $\alpha \circ d$ is a derivation that agree with ∂ on the x_λ's, and since a derivation is uniquely determined by its values on a generating set, the map we have $\partial = \alpha \circ d$. Thus, the universal property holds. □

To compute modules of differentials in general, we will bootstrap off of this case. To get started, we will need to set up some functoriality properties.

Proposition 2.16. (1) *Let $A \xrightarrow{\psi} B$ be a ring homomorphism and R be a B-algebra. There there is a unique R-module homomorphism $d_{R|\psi}$ such that the diagram commutes:*

$$\begin{array}{ccc} \Omega_{R|A} & \xrightarrow{d_{R|\psi}} & \Omega_{R|B} \\ & {\scriptstyle d_{R|A}}\nwarrow \quad \nearrow{\scriptstyle d_{R|B}} & \\ & R & \end{array}$$

(2) *Let A be a ring, and $\phi : R \to S$ be an A-algebra homomorphism. Then there is a unique R-module homomorphism $d_{\phi|A} : \Omega_{R|A} \to \Omega_{S|A}$ such that the diagram commutes*

$$\begin{array}{ccc} \Omega_{R|A} & \xrightarrow{d_{\phi|A}} & \Omega_{S|A} \\ {\scriptstyle d_{R|A}}\uparrow & & \uparrow{\scriptstyle d_{S|A}} \\ R & \xrightarrow{\phi} & S \end{array}$$

(3) *Let A be a ring, and $\phi : R \to S$ be an A-algebra homomorphism. Then there is a unique S-module homomorphism $S \otimes d_{\phi|A} : S \otimes_R \Omega_{R|A} \to \Omega_{S|A}$ such that the diagram commutes*

$$\begin{array}{ccc} S \otimes_R \Omega_{R|A} & \xrightarrow{S \otimes d_{\phi|A}} & \Omega_{S|A} \\ {\scriptstyle \eta}\uparrow & & \\ \Omega_{R|A} & & \uparrow{\scriptstyle d_{S|A}} \\ {\scriptstyle d_{R|A}}\uparrow & & \\ R & \xrightarrow{\phi} & S \end{array}$$

Proof. (1) The map $d_{R|B}$, since it is B-linear, is an A-linear derivation when viewed via restriction of scalars along ψ. Apply the universal property of $\Omega_{R|A}$ and $d_{R|A}$ to this derivation.

(2) The map $d_{S|A} \circ \phi$ is an A-linear derivation from R to $\Omega_{S|A}$. Apply the universal property of $\Omega_{R|A}$ and $d_{R|A}$ to this derivation.

(3) Apply the universal property of extension of scalars to the map $d_{\phi|A}$. □

Theorem 2.17 (First fundamental sequence)**.** *Let $A \xrightarrow{\psi} R \xrightarrow{\phi} S$ be ring homomorphisms. Then there is a right exact sequence of S-modules*

$$S \otimes_R \Omega_{R|A} \xrightarrow{S \otimes d_{\phi|R}} \Omega_{S|A} \xrightarrow{d_{S|\psi}} \Omega_{S|R} \to 0.$$

Proof. By the Theorem on exactness of Hom, it suffices to show that for every S-module M there is a left exact sequence

$$0 \longrightarrow \mathrm{Hom}_S(\Omega_{S|R}, M) \xrightarrow{d^*_{S|\psi}} \mathrm{Hom}_S(\Omega_{S|A}, M) \xrightarrow{(S \otimes d_{\phi|R})^*} \mathrm{Hom}_S(S \otimes_R \Omega_{R|A}, M) \ .$$

This is just the left exact sequence on derivations from before! Precisely, we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_S(\Omega_{S|R}, M) & \xrightarrow{d^*_{S|\psi}} & \mathrm{Hom}_S(\Omega_{S|A}, M) & \xrightarrow{(S \otimes d_{\phi|R})^*} & \mathrm{Hom}_S(S \otimes_R \Omega_{R|A}, M) \\ & & \cong \downarrow {\scriptstyle d^*_{S|R}} & & \cong \downarrow {\scriptstyle d^*_{S|A}} & & \cong \downarrow {\scriptstyle d^*_{R|A} \circ \eta^*} \\ 0 & \longrightarrow & \mathrm{Der}_{S|R}(M) & \xrightarrow{\mathrm{inc}} & \mathrm{Der}_{S|A}(M) & \xrightarrow{\phi^*} & \mathrm{Der}_{R|A}(M) \end{array}$$

Let's check them: for $\Omega_{S|R} \xrightarrow{\theta} M$, we have

$$d^*_{S|A} d^*_{S|\psi} \theta = \theta \circ d_{S|\psi} \circ d_{S|A} = \theta d_{S|R} = d^*_{S|R}\theta = \mathrm{inc} d^*_{S|R}\theta$$

and for $\Omega_{S|A} \xrightarrow{\theta} M$, we have

$$d^*_{R|A} \circ \eta^* \circ (S \otimes d_{\phi|R})^* \theta = \theta \circ (S \otimes d_{\phi|R}) \circ \eta \circ d_{R|A} = \theta \circ d_{S|A} \circ \phi = \phi^* d^*_{S|A}\theta. \qquad \square$$

Lecture of February 28, 2023

Theorem 2.18 (Second fundamental sequence)**.** *Let $A \to R \xrightarrow{\pi} R/I$ be ring homomorphisms. Then there is a right exact sequence of R/I-modules*

$$I/I^2 \xrightarrow{\overline{d_{R|A}}} R/I \otimes_R \Omega_{R|A} \xrightarrow{R/I \otimes d_{\pi|A}} \Omega_{R/I\,|A} \to 0,$$

where $\overline{d_{R|A}}$ is the map obtained from $d_{R|A}$ by postcomposing with the quotient map π and taking restriction.

If we also have that the quotient map $R/I^2 \to R/I$ admits an A-algebra right inverse, then

$$0 \to I/I^2 \xrightarrow{\overline{d_{R|A}}} R/I \otimes_R \Omega_{R|A} \xrightarrow{R/I \otimes d_{\pi|A}} \Omega_{R/I\,|A} \to 0$$

is split exact.

Proof. By the Theorem on exactness of Hom it suffices to show that for every R/I-module M there is a left exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(\Omega_{R/I|A}, M) \xrightarrow{(R/I \otimes d_{\pi|A})^*} \mathrm{Hom}_R(\Omega_{R|A}, M) \xrightarrow{\overline{d_{R|A}}^*} \mathrm{Hom}_R(I/I^2, M)\ .$$

and that the last map is surjective under the hypothesis that the quotient map $R/I^2 \to R/I$ admits an A-algebra right inverse. This is just the other left exact sequence on derivations from before!

Precisely, we have a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_{R/I}(\Omega_{R/I|A}, M) & \xrightarrow{(R/I \otimes d_{\pi|A})^*} & \mathrm{Hom}_{R/I}(\Omega_{R|A}, M) & \xrightarrow{\overline{d_{R|A}}^*} & \mathrm{Hom}_{R/I}(I/I^2, M) \\
 & & \cong \downarrow d^*_{R/I|A} & & \cong \downarrow d^*_{R|A} \circ \eta^* & & \| \\
0 & \longrightarrow & \mathrm{Der}_{R/I|A}(M) & \xrightarrow{\pi^*} & \mathrm{Der}_{R|A}(M) & \xrightarrow{\mathrm{res}} & \mathrm{Hom}_R(I/I^2, M)
\end{array}$$

The first square is just a special case of the second square in the previous proof and the second is easily checked too. The last map on the bottom is also surjective under the bonus hypothesis, so the top row extends to a short exact sequence in this case. $\square$

We can now write everything about differentials in concrete terms. We recall that the *Jacobian* of a set of elements $f_1, \ldots, f_m$ in a polynomial ring $A[x_1, \ldots, x_n]$ is the matrix

$$J(f_1, \ldots, f_m) = \begin{bmatrix} \frac{df_1}{dx_1} & \cdots & \frac{df_1}{dx_n} \\ \vdots & \ddots & \vdots \\ \frac{df_m}{dx_1} & \cdots & \frac{df_m}{dx_n} \end{bmatrix}.$$

Let's also call this the *row Jacobian* to indicate that the elements f_i correspond to rows. The *column Jacobian* is its transpose:

$$J(f_1,\dots,f_m)^T = \begin{bmatrix} \frac{df_1}{dx_1} & \dots & \frac{df_m}{dx_1} \\ \vdots & \ddots & \vdots \\ \frac{df_1}{dx_n} & \dots & \frac{df_m}{dx_n} \end{bmatrix}.$$

Corollary 2.19. *Let $A \xrightarrow{\psi} R \xrightarrow{\phi} S$ be maps of rings. Concretely, let*

- *R be the A-algebra with generators x_i and relations f_j,*
- *S be the A-algebra with generators y_i and relations g_j,*
- *$\phi(x_i) = h_i(y)$.*

Then,

(1) *$\Omega_{R|A}$ is the R-module with generators dx_i and relations $df_j = \sum_i \frac{df_j}{dx_i} dx_i$. In particular (if the set of generators and relations are finite), the presentation matrix of $\Omega_{R|A}$ is the column Jacobian $J(f_1,\dots,f_m)^T$.*

(2) *The universal derivation $d_{R|A}$ maps $r \in R$ to $\sum_i \frac{dr}{dx_i} dx_i$.*

(3) *The map $d_{\phi|A}$ maps the $dx_k \in \Omega_{R|A}$ to the element $\sum_i \frac{dh_k}{dy_i} dy_i \in \Omega_{S|A}$. In particular (if the set of generators and relations on both sides are finite), the matrix of the map in the given generating sets is the column Jacobian $J(h_1,\dots,h_\ell)^T$.*

(4) *The map $d_{S|\psi}$ is a quotient map from $\Omega_{S|A} \to \Omega_{S|R}$ given by killing the elements of the form $\sum_i \frac{dh_k}{dy_i} dy_i$ for all k. That is, with respect to the given generators (if all are finite), the map is quotienting by the image of the column Jacobian $J(h_1,\dots,h_\ell)^T$.*

Proof. For (1), we can write $R = T/I$ with $T = A[\{x_i\}]$ and $I = (\{f_j\})$. Then $\Omega_{T|A}$ is the free T-module with basis $\{dx_i\}$, and $R \otimes_T \Omega_{T|A}$ is the free R-module on the same basis. The image of the R-linear map $I/I^2 \xrightarrow{\overline{d_{T|A}}} R \otimes_T \Omega_{T|A}$ is generated by the elements $\overline{d_{T|A}}(f_j)$, which are just the df_j elements above. The second fundamental sequence then gives the result. For (2), if $\pi : T \to R$ is the quotient map, in the isomorphism above, we have identified $\Omega_{R|A}$ with a quotient of $R \otimes_T \Omega_{T|A}$, so $R \otimes_T d_{\pi|A}$ is a quotient map. Then $d_{R|A} \circ \pi = R \otimes_T d_{\pi|A} \circ \eta \circ d_{T|A}$, so for $r' \in T$ with $\pi(r') = r$, we have $d_{R|A}(r) = d_{R|A}(r') = \sum_i \frac{dr}{dx_i} dx_i$. For (3), we have

$$d_{\phi|A}(dx_k) = d_{\phi|A} d_{R|A}(x_k) = d_{S|A}\phi(x_k) = d_{S|A}(h_k) = \sum_i \frac{dh_k}{dy_i} dy_i.$$

For (4), from the first fundamental sequence, we have that $\Omega_{S|R}$ is the quotient of $\Omega_{S|A}$ by the image of $S \otimes_R d_{\phi|A}$. This is generated by the images of dx_i under this map, which are as above. □

Example 2.20. Let K be a field.

(1) For a polynomial ring $R = K[x,y,z]$, we have $\Omega_{R|K} = Rdx \oplus Rdy \oplus Rdz$. This is free of rank 3.

(2) For $R = K[x]/(x^2)$, if the characteristic of K is not 2, then $\Omega_{R|K} = Rdx/(2xdx) \cong R/(x)$. If the characteristic is 2, then $\Omega_{R|K} = Rdx$.

(3) For $R = K[x,y,z]/(x^n + y^n + z^n)$ with $n > 1$ we have $\Omega_{R|K} = \dfrac{Rdx \oplus Rdy \oplus Rdz}{(nx^{n-1}dx + ny^{n-1}dy + nz^{n-1}dz)}$.

In particular, if K has characteristic zero we get a free module of rank three quotiented out by a relation with entries in the maximal ideal $\mathfrak{m} = (x,y,z)$. If we invert the nonzero elements in R in our relation we can divide by the coefficient of dx and write it as a combination of the others, so $(\Omega_{R|K})_{(0)}$ is a free module over the quotient field of rank two. That is $\Omega_{R|K}$ has rank two as an R-module. However, $\Omega_{R|K}$ is not free; in particular $(\Omega_{R|K})_{\mathfrak{m}}$ is not, since $(\Omega_{R|K})_{\mathfrak{m}}/\mathfrak{m}(\Omega_{R|K})_{\mathfrak{m}}$

is a three dimensional K-vector space on the basis dx, dy, dz. This all works as long as n is not a multiple of the characteristic of K.

If K has characteristic p and $n = p$, then the relation is trivial, so $\Omega_{R|K}$ is free of rank three.

(4) For $R = K[x,y,z]/(x^n + y^n + z^n - 1)$, we have $\Omega_{R|K} = \dfrac{Rdx \oplus Rdy \oplus Rdz}{(nx^{n-1}dx + ny^{n-1}dy + nz^{n-1}dz)}$. We claim that, if the characteristic of K is zero, $\Omega_{R|K}$ is a locally free/projective module of rank two. Since (x,y,z) generate the unit ideal of R, there is no maximal ideal containing all of them, so any maximal ideal fails to contain at least one. Let $\mathfrak{m}$ be a maximal ideal; WLOG say $x \notin \mathfrak{m}$. Then by an argument similar to above, we get that $(\Omega_{R|K})_{\mathfrak{m}}$ is free of rank two. Depending on K and n, this module is not necessarily (globally) free. For example, if $K = \mathbb{R}$ and $n = 2$, this is impossible. Prove it!

Lecture of March 2, 2023

Recall that a module P is *projective* if the equivalent conditions hold:

- For any surjection of R-modules $M \xrightarrow{p} N \to 0$ and homomorphism $P \xrightarrow{\beta} N$, there is a map $P \xrightarrow{\alpha} M$ such that $\beta = p\alpha$;
- Every short exact sequence of the form $0 \to A \to B \to P \to 0$ is split exact;
- There is a module Q such that $P \oplus Q$ is free.

If P is finitely generated and R is Noetherian, these are equivalent to

- P is *locally free*: for every maximal ideal $\mathfrak{m}$ (equivalently, every prime ideal $\mathfrak{p}$), $P_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module (resp., $P_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module).

We can also show that modules of differentials localize.

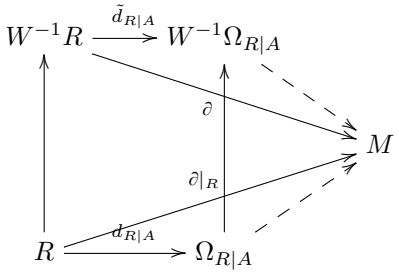
Proposition 2.21. *Let R be an A-algebra and $W \subseteq R$ a multiplicative set. Then there are isomorphisms*

$$W^{-1}\Omega_{R|A} \cong \Omega_{W^{-1}R|A}.$$

Proof. First, note that there is a natural R-linear map $\eta : \Omega_{R|A} \to W^{-1}\Omega_{R|A}$

$$\begin{array}{ccc} W^{-1}R & \xrightarrow{\tilde{d}_{R|A}} & W^{-1}\Omega_{R|A} \\ \uparrow & & \uparrow{\scriptstyle \eta} \\ R & \xrightarrow{d_{R|A}} & \Omega_{R|A} \end{array}$$

which induces a unique A-linear derivation from $W^{-1}R$ to $W^{-1}\Omega_{R|A}$ making the diagram commute. We claim this is a universal derivation. Let M be an $W^{-1}R$-module and $\partial : W^{-1}R \to M$ an A-linear derivation. Then, restricting to R we get a derivation $\partial|_R$, so the universal property of $\Omega_{R|A}$ yields an R-linear map α with $\alpha d_{R|A} = \partial$. But then the universal property of extension of scalars yields a unique $W^{-1}R$-linear map $\beta : W^{-1}\Omega_{R|A} \to M$ with $\beta\eta = \alpha$.



Then $\beta\tilde{di} = \beta\eta d = \alpha d = \partial|_R$ and since two derivations on $W^{-1}R$ with the same restriction to R must be the same by the lemma on derivations and localization we must have $\beta\tilde{d} = \partial$. Moreover, since the image of d generates $\Omega_{R|A}$, the image of $\tilde{d}$ generates $W^{-1}\Omega_{R|A}$, and since β is unique determined by its values on a generating set, the map β must be unique. This verifies the universal property. □

Definition 2.22. We say that a ring homomorphism $R \xrightarrow{\phi} S$ is

- *essentially algebra-finite* if ϕ factors as an algebra-finite map followed by a localization. Concretely, $S = W^{-1}(R[x_1, \ldots, x_n]/I)$ for some ideal I and multiplicatively closed set W.
- *finitely presented* if it is algebra-finite and the kernel is a finitely generated ideal. Concretely, $S = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Note that if R is Noetherian, then algebra-finite and finitely presented are equivalent by Hilbert Basis Theorem.
- *essentially finitely presented* if ϕ factors as an finitely presented map followed by a localization. Concretely, $S = W^{-1}(R[x_1, \ldots, x_n]/(f_1, \ldots, f_m))$ multiplicatively closed set W.

Corollary 2.23. *Let $S = W^{-1}R[x_1, \ldots, x_n]/I$ and $I = (f_1, \ldots, f_m)$. Then $\Omega_{S|R}$ is the S module with generators $dx_1, \ldots, dx_n$ and relations $df_j = \sum_i \frac{df_j}{dx_i} dx_i$. In particular, $\Omega_{S|R}$ is finitely generated.*

2.3. **Jacobi-Zariski sequence.**

Definition 2.24. Let R be an A-algebra. Write $R = S/I$ with $S = A[X]$. We define $\Gamma_{R|A}$ to be the kernel of the map $I/I^2 \xrightarrow{\overline{d_{S|I}}} R \otimes_S \Omega_{S|A}$.

We will call the map $I/I^2 \xrightarrow{\overline{d_{S|I}}} R \otimes_S \Omega_{S|A}$ the *conormal map* associated with the presentation $R = A[X]/I$. Thus, there is an exact sequence

$$0 \to \Gamma_{R|A} \to I/I^2 \xrightarrow{\overline{d_{S|I}}} \bigoplus Rdx \to \Omega_{R|A} \to 0.$$

We need to see that $\Gamma_{R|A}$ is well-defined.

Proposition 2.25. *Different presentations of R as an A-algebra yield isomorphic R-modules $\Gamma_{R|A}$.*

(To prove next time).

Theorem 2.26 (Jacobi-Zariski sequence)**.** *Let $A \to R \to S$ be ring homomorphisms. Then there is an exact sequence*

$$\Gamma_{S|A} \to \Gamma_{S|R} \to S \otimes_R \Omega_{R|A} \to \Omega_{S|A} \to \Omega_{S|R} \to 0.$$

(To prove next time).

Remark 2.27. Both of the fundamental sequences are special cases of this! The tail is just the first fundamental sequence. If we have $R \to S = R/I$, then we don't need any variables at all to present R/I; i.e., we can take $R[X]$ in the presentation $R[X] \to R/I$ to be just R itself. Thus, the sequence defining $\Gamma_{R/I|R}$ reads

$$0 \to \Gamma_{R/I|R} \to I/I^2 \to 0 \to \Omega_{R/I|R} \to 0,$$

so $\Gamma_{R/I|R} \cong I/I^2$ and $\Omega_{R/I|R} = 0$. Thus, we obtain the second fundamental sequence as the tail of the Jacobi-Zariski sequence in this case.

Lecture of March 7, 2023

Lemma 2.28 (Snake Lemma)**.** *Given a commutative diagram with exact rows*

$$\begin{array}{ccccccc} A & \longrightarrow & B & \longrightarrow & C & \xrightarrow{c} & 0 \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \end{array}$$

there is an exact sequence

$$\ker(a) \to \ker(b) \to \ker(c) \to \operatorname{coker}(a) \to \operatorname{coker}(b) \to \operatorname{coker}(c).$$

If in addition the top row has $0 \to$ *on the left or the bottom row has* $\to 0$ *on the right, then one can add* $0 \to$ *or* $\to 0$ *respectively to the exact sequence.*

Proposition 2.29. *Different presentations of* R *as an* A*-algebra yield isomorphic* R*-modules* $\Gamma_{R|A}$*.*

Proof. Unfortunately, we do not have a snappy universal property to help us here, so we proceed directly. Suppose we are given polynomial rings $A[X]$ and $A[Y]$ with surjections $\pi : A[X] \to R$ and $\pi' : A[Y] \to R$. Then there is a surjection $\pi'' : A[X, Y] \to R$ given by sending $\pi''(x_i) = \pi(x_i)$ and $\pi''(y_i) = \pi'(y_i)$.

$$\begin{array}{ccc} A[X,Y] & \xleftarrow{\supset} & A[Y] \\ \cup\uparrow & \searrow^{\pi''} & \downarrow{\scriptstyle \pi'} \\ A[X] & \xrightarrow{\pi} & R \end{array}$$

If we show that π and π'' yield isomorphic Γ modules, then by symmetry, π and π' do as well.

For each $y_i \in Y$, we can choose some $g_i \in A[X]$ with $\pi(g_i) = \pi'(y_i)$. Let $I = \ker(\pi)$; we'll sometimes write $I(x)$ for I to indicate this consists of polynomials in the X variables. Note that

$$J := \ker(\pi'') = (I(x), \{y_i - g_i\})A[X, Y].$$

We can take a change of variables in $A[X, Y]$ replacing y_i by $y_i - g_i$; then without loss of generality, we can assume that $J = (I(x), Y)A[X, Y]$.

The inclusion maps $I \subseteq J$ and $I^2 \subseteq J^2$ induce a map $I/I^2 \to J/J^2$. Since

$$J^2 \cap I = (I(x)^2, I(x)Y, (Y)^2)A[X, Y] \cap I \subseteq (I(x)^2, I(x)Y, (Y)^2)A[X, Y] \cap A[X] = I(x)^2,$$

this map is injective. The cokernel is

$$\frac{(I(x), Y)A[X, Y]}{(I(x), Y)^2A[X, Y] + I(x)} \cong \frac{(I(x), Y)S''}{(I(x)^2, I(x)Y, (Y)^2)A[X, Y] + I(x)} \cong \frac{(I(x), Y)A[X, Y]}{(I(x), (Y)^2)A[X, Y]},$$

since $I(x)A[X, Y] = I(x) + I(x)YA[X, Y]$. We claim that this is a free R-module with basis $\{[y_i]\}$. Indeed, it is generated by these as an S''-module, and given an R-linear relation on these classes, this pulls back to an $A[X, Y]$-linear relation $\sum_j p_j(x, y)y_j \in (I(x), (Y)^2)A[X, Y]$: the terms in p_j without any y's must also be in I, so each $p_j(x, y) \in (I(x), Y)A[X, Y]$, and hence is the trivial relation over R.

We then have a

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ I/I^2 & \xrightarrow{d} & \bigoplus Rdx_i \\ \downarrow & & \downarrow \\ J/J^2 & \xrightarrow{d} & \bigoplus Rdx_i \oplus \bigoplus Rdy_i \\ \downarrow & & \downarrow \\ \bigoplus Ry_i & \xrightarrow{d} & \bigoplus Rdy_i \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

with exact rows, where the bottom map sends y_i to dy_i. We claim that this commutes. For the top square, for $a \in I(x)$, under the $\to$ then $\downarrow$ composition, we have $[a] \mapsto \sum_i \frac{da}{dx_i} dx_i \mapsto \sum_i \frac{da}{dx_i} dx_i$ and under the $\downarrow$ then $\to$ composition, we have $[a] \mapsto [a] \mapsto \sum_i \frac{da}{dx_i} dx_i$. For the bottom square, it suffices to check for a elements in a generating set, so for y_i and for $a \in I(x)$. For $a \in I(x)$, under the $\to$ then $\downarrow$ composition, we have $[a] \mapsto \sum_i \frac{da}{dx_i} dx_i \mapsto 0$, and under the $\downarrow$ then $\to$ composition, we have $[a] \mapsto 0 \mapsto 0$. For y_i, under the $\to$ then $\downarrow$ composition, we have $[y_i] \mapsto dy_i \mapsto dy_i$, and under the $\downarrow$ then $\to$ composition, we have $[y_i] \mapsto [y_i] \mapsto dy_i$.

The map on cokernels is an isomorphism. The Snake Lemma, then says that

$$0 \to \ker\left(I/I^2 \xrightarrow{d} \bigoplus Rdx_i\right) \to \ker\left(J/J^2 \xrightarrow{d} \bigoplus Rdx_i \oplus \bigoplus Rdy_i\right) \to 0 \to \cdots$$

is exact, so these modules are isomorphic. □

Proposition 2.30. *Let $A \xrightarrow{\phi} R$ be a homomorphism and $W \subseteq R$ be a multiplicative set. Then $W^{-1}\Gamma_{R|A} \cong \Gamma_{W^{-1}R|A}$.*

Proof. Let $R = A[X]/I$. We have that $W^{-1}R \cong R[Y]/(\{wy_w - 1\})$ for a set of variables in bijection with W; one can see this by verifying the latter quotient satisfies the universal property of localization. We then obtain the presentation $W^{-1}R = A[X, Y]/J$ with $J = IA[X, Y] + (\{wy_w - 1\})$.

The inclusions $I \subseteq J$ and $I^2 \subseteq J^2$ induce a map $I/I^2 \to J/J^2$, and thus by the universal property of localization, $W^{-1}(I/I^2) \to J/J^2$. As J/J^2 is a $W^{-1}R$-module, we can rewrite

$$J/J^2 = \frac{(I, \{wy_w - 1\})W^{-1}R}{(I, \{wy_w - 1\})^2 W^{-1}R} = \frac{(I, \{y_w - w^{-1}\})W^{-1}R}{(I, \{y_w - w^{-1}\})^2 W^{-1}R}.$$

We can then take a change of coordinates and replace $y_w - w^{-1}$ by y_w, and the rest of the argument proceeds as in the previous one. □

We recall that a ring homomorphism $R \xrightarrow{\phi} S$ is *flat* if the corresponding extension of scalars functor $S \otimes_R -$ turns injective maps into injective maps. This is true for polynomial maps and localizations.

Theorem 2.31. *Let $A \to R \to S$ be ring homomorphisms. Then there is an exact sequence*

$$\Gamma_{S|A} \to \Gamma_{S|R} \to S \otimes_R \Omega_{R|A} \to \Omega_{S|A} \to \Omega_{S|R} \to 0.$$

If $R \to S$ is flat, then one can extend the sequence one further to the left by $S \otimes_R \Gamma_{R|A}$.

Proof. Take $R = A[X]/I$ and $S = R[Y]/J$. Let's write $A[X] \xrightarrow{\pi} R$ and $R[Y] \xrightarrow{\pi'} S$ for these surjections, and just to keep track of things, write $I(x) = I$ and $J(y) = J$ to remember that they are polynomials in x and y respectively. Then the quotient map $A[X] \xrightarrow{\pi} R$ induces by extension of scalars $A[Y] \otimes_A -$ a quotient map $A[X,Y] \xrightarrow{A[Y]\otimes_A \pi} R[Y]$, which has kernel $I(x)A[X,Y]$, generated by the images of $I(x)$. We then get an algebra presentation of S over A by composing $\pi'' : A[X,Y] \xrightarrow{A[Y]\otimes_A \pi} R[Y] \xrightarrow{\pi'} S$. If we set $J'(y) = (A[Y] \otimes_A \pi)^{-1}(J(y))$ to be the preimage of $J(y)$ in $A[X,Y]$ (which is generated by polynomials in just the y's also), then the kernel π'' is $L = I(x)A[X,Y] + J'(y)$.

We claim that there is a right exact sequence

$$S \otimes_R I/I^2 \to L/L^2 \to J/J^2 \to 0.$$

First, we have $(A[Y] \otimes_A \pi)(L) = J$ and likewise with L^2 and J^2 so we get a valid surjection on the right. Since $I \subseteq L$, we also have $I^2 \subseteq L^2$, and there is a valid map R-module map $I/I^2 \to L/L^2$. Then the universal property of extension of scalars gives the first map above.

As $S \otimes_R I/I^2$ is generated by images of elements in I, to see that the composition above is zero, it suffices to check for elements of I, but $\pi(I) = 0$. On the other hand, the kernel of the map corresponds to classes of elements in L with $(A[Y] \otimes_A \pi)(f) \in J(y)^2$, which corresponds to classes of elements in $J'(y)^2 + I(x)A[X,Y]$. But this is contained in $L^2 + I(x)A[X,Y]$, so the kernel of the map $L/L^2 \to J/J^2$ is generated by classes of elements in the image of I. This shows the sequence is right exact.

We then get a commutative diagram

$$\begin{array}{ccccccc} S \otimes_R I/I^2 & \longrightarrow & L/L^2 & \longrightarrow & J/J^2 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 \longrightarrow \bigoplus Sdx_i & \longrightarrow & \bigoplus Sdx_i \oplus \bigoplus Sdy_i & \longrightarrow & \bigoplus Sdy_i & \longrightarrow & 0 \end{array}$$

with exact rows. We note that the first column comes from the map giving $\Omega_{R|A}$ as cokernel and $\Gamma_{R|A}$ and kernel affter extension of scalars to S. In the case $R \to S$ is flat, we have that the kernel of $S \otimes_R I/I^2 \to \bigoplus Sdx_i$ is $S \otimes_R \Gamma_{R|A}$, and we get one more from the snake lemma. □

2.4. **Unramified, smooth, and étale maps.**

Definition 2.32. Let $R \xrightarrow{\phi} S$ be a ring homomorphism. We say that ϕ is

- *formally unramified* if $\Omega_{S|R} = 0$,
- *formally étale* if $\Omega_{S|R} = 0$ and $\Gamma_{S|R} = 0$,
- *formally smooth* if $\Gamma_{S|R} = 0$ and $\Omega_{S|R}$ is projective.

If S is a finitely presented R-algebra, we drop the "formally" and say *unramified/étale/smooth* if the corresponding condition holds. If S is essentially finitely-presented over R, and the corresponding condition holds, we say *essentially unramified/essentially étale/essentially smooth*.

Lecture of March 9, 2023

Note that formally étale is formally unramified plus formally smooth.

To get a sense of where these conditions come from, let's throw them into the Jacobi-Zariski sequence: given a map of A-algebra $R \xrightarrow{\phi} S$, we can ask whether for every S-module M the map

$$\mathrm{Der}_{S|A}(M) \xrightarrow{\phi^*} \mathrm{Der}_{R|A}(M)$$

is injective, surjective, or bijective.

If $R \to S$ is formally unramified, $\Omega_{S|R} = 0$, so $S \otimes_R \Omega_{R|A} \xrightarrow{S\otimes d_{\phi|A}} \Omega_{S|A}$ is surjective, and by exactness of Hom, $\mathrm{Hom}_S(\Omega_{S|A}, M) \cong \mathrm{Der}_{S|A}(M) \xrightarrow{\phi^*} \mathrm{Der}_{R|A}(M) \cong \mathrm{Hom}_S(S \otimes_R \Omega_{R|A}, M)$ is injective for all M.

If $R \to S$ is formally étale, $\Omega_{S|R} = 0$ and $\Gamma_{S|R} = 0$, so $S \otimes_R \Omega_{R|A} \xrightarrow{S\otimes d_{\phi|A}} \Omega_{S|A}$ is an isomorphism, and $\mathrm{Hom}_S(\Omega_{S|A}, M) \cong \mathrm{Der}_{S|A}(M) \xrightarrow{\phi^*} \mathrm{Der}_{R|A}(M) \cong \mathrm{Hom}_S(S \otimes_R \Omega_{R|A}, M)$ is an isomorphism for all M.

If $R \to S$ is formally smooth, $\Omega_{S|R}$ is projective and $\Gamma_{S|R} = 0$, so $S \otimes_R \Omega_{R|A} \xrightarrow{S\otimes d_{\phi|A}} \Omega_{S|A}$ is a split injection, and $\mathrm{Hom}_S(\Omega_{S|A}, M) \cong \mathrm{Der}_{S|A}(M) \xrightarrow{\phi^*} \mathrm{Der}_{R|A}(M) \cong \mathrm{Hom}_S(S \otimes_R \Omega_{R|A}, M)$ is a surjection for all M.

In particular, if $\psi : X \to Y$ is a map of complex affine varieties, and $\psi^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ is the map on coordinate rings, then

- If ψ^* is unramified, then the induced map on tangent spaces is injective at every point;
- If ψ^* is étale, then the induced map on tangent spaces is bijective at every point;
- If ψ^* is smooth, then the induced map on tangent spaces is surjective at every point.

We note:

Proposition 2.33. *Let $R \xrightarrow{\phi} S$ be a ring homomorphism. Write $S = R[X]/I$ for some polynomial ring $R[X]$ and ideal I.*

1. *ϕ is formally unramified if and only if the conormal map $I/I^2 \xrightarrow{d} \bigoplus S dx_\lambda$ is surjective.*
2. *ϕ is formally étale if and only if the conormal map $I/I^2 \xrightarrow{d} \bigoplus S dx_\lambda$ is bijective.*
3. *ϕ is formally smooth if and only if the conormal map $I/I^2 \xrightarrow{d} \bigoplus S dx_\lambda$ is a split injection.*

Example 2.34.

1. If $R \to R/I$ is surjective, then is formally unramified, and if R is Noetherian, plain old unramified. In this case, $\Gamma_{R/I|R} = I/I^2$. A surjection is almost never formally smooth/formally étale: this would require $I = I^2$, which (at least if I is finitely generated) I to be generated by an idempotent. That is, a smooth surjection must be killing a factor in a direct product.
2. If R is a ring and W is a multiplicative set, then $W^{-1}R$ is formally étale over R. Indeed, we have $\Gamma_{W^{-1}R|R} \cong W^{-1}\Gamma_{R|R} = 0$ and likewise with Ω.
3. Let K be a field and $R = K[x, y, z]$. Then $\Omega_{R|K}$ is free of rank 3 and $\Gamma_{R|K} = 0$, so R is smooth over K. R is not unramified or étale.
4. Let $K = \mathbb{R}$ and $R = K[x, y, z]/(x^2 + y^2 + z^2)$. Then $\Omega_{R|K}$ localized at (x, y, z) is not free, so $\Omega_{R|K}$ is not projective, and hence R is not smooth over K. Note that, trivially, every K-linear derivation on K extends to R. R is not unramified or étale.

   We remark that if T is a ring and f is a nonzerodivisor, then $(f)/(f^2)$ is a free $T/(f)$-module with basis element $[f]$: if $tf = sf^2$ then $t = sf \in (f)$, so the annihilator as a T-module is just f.
5. Let $K = \mathbb{R}$ be a field of characteristic zero and $R = K[x, y, z]/(x^2 + y^2 + z^2 - 1)$. We have seen that $\Omega_{R|K}$ is locally free, and hence projective. By definition,
$$\Gamma_{R|K} = \ker\left((f)/(f^2) \xrightarrow{d} R dx \oplus R dy \oplus R dz\right),$$
where $f = x^2 + y^2 + z^2 - 1$. Given $s \in S$ and $[sf] \in (f)/(f^2)$, we have $d([sf]) = 0$ implies $s(2x dx + 2y dy + 2z dz) = 0$ in $R dx \oplus R dy \oplus R dz$, which implies $sx \in (f)S$, so $f|s$. Thus, the map d is injective, and $\Gamma_{R|K} = 0$. We conclude that R is smooth over K. R is not unramified or étale.
6. Let $K = \mathbb{F}_p$ and $R = K[x]/(x^p)$. Then $\Omega_{R|K} = R dx$ is free of rank 1, but the map $I/I^2 \xrightarrow{d} R dx$ maps the generator x^p to zero, so $\Gamma_{R|K} = (x^p)/(x^p)^2 \cong R$ is nonzero. Thus R is not smooth over K, even though $\Omega_{R|K}$ is free.

(7) Let $K = \mathbb{F}_p(t)$ and $R = K(t^{1/p}) \cong K[x]/(x^p - t)$. Then $\Omega_{R|K} = Rdx$ is free of rank 1 and the $I/I^2 \xrightarrow{d} Rdx$ maps the generator to zero as above. We again have that R is not smooth over K, even though R is a field (and hence regular).

(8) For a nontrivial étale map, let $R = \mathbb{Z}_2$ and $S = \mathbb{Z}[i]_2$. Then $S = R[x]/(x^2+1)$ so the conormal map is $(x^2+1)/(x^2+1)^2 \xrightarrow{d} Rdx$ with the generator mapping to $2i$ in Rdx. Since $2i$ is a unit, this map is surjective, and bijective as well.

Lecture of March 21, 2023

2.5. **Regular rings revisited.** Recall that a Noetherian local ring $(R, \mathfrak{m}, k)$ is regular if $\dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. In particular, a zero-dimensional local ring is regular if and only if it is a field.

Proposition 2.35. *Let $(R, \mathfrak{m}, k)$ be a regular local ring.*

(1) *If $f \in \mathfrak{m}/\mathfrak{m}^2$, then $R/(f)$ is a regular local ring.*
(2) *$(R, \mathfrak{m}, k)$ is a domain.*
(3) *If I is an ideal, then R/I is regular if and only if the minimal generators of I are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$ (i.e., the map $I/\mathfrak{m}I \to \mathfrak{m}/\mathfrak{m}^2$ induced by inclusion is injective).*

Proof. (1) Set $d = \dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. We have

$$\dim_k\left(\frac{\mathfrak{m}R/(f)}{\mathfrak{m}^2R/(f)}\right) = \dim_k\left(\frac{\mathfrak{m}}{(f,\mathfrak{m}^2)}\right) = d-1,$$

so

$$d-1 \leqslant \dim(R/(f)) \leqslant \dim_k\left(\frac{\mathfrak{m}R/(f)}{\mathfrak{m}^2R/(f)}\right) \leqslant d-1,$$

so equality holds and $R/(f)$ is regular.

(2) By induction on $d = \dim R$, where R is a regular local ring. If $d = 0$, then R must be a field, and thus a domain. If $d > 0$, consider $f \in \mathfrak{m} \setminus \left(\mathfrak{m}^2 \cup \bigcup_{\mathfrak{p}\in\mathrm{Min}(R)} \mathfrak{p}\right)$. (Here we are using the strong version of prime avoidance where we can avoid one or two arbitrary ideals and a finite number of prime ideals.) By the first part, $R/(f)$ is regular. By the induction hypothesis, this is a domain, so (f) is prime. By choice of f, this is not a minimal prime. Given a prime ideal $0 \subseteq \mathfrak{p} \subsetneqq (f)$, if $y \in \mathfrak{p}$, we can write $y = rf$ for some $r \in R$, and since $f \notin \mathfrak{p}$, $r \in \mathfrak{p}$. Thus $\mathfrak{p} = f\mathfrak{p} \subseteq \mathfrak{m}\mathfrak{p}$, which by NAK implies that $\mathfrak{p} = 0$. Thus 0 is prime, so R is a domain.

(3) From the first part, if $f_1, \ldots, f_t$ be a minimal generating set for I and their images are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$, by induction on t we get that R/I is regular. Conversely, if the images of the f's are not linearly independent in $\mathfrak{m}/\mathfrak{m}^2$ suppose that the images of $f_1, \ldots, f_a$ form a basis for the image; subtracting off copies of these, we may suppose the rest are in $\mathfrak{m}^2$. Then $R/(f_1, \ldots, f_a)$ is a regular local ring, and $R/I \cong R'/J$ for $R' = R/(f_1, \ldots, f_a)$ some ideal J in the maximal ideal $\mathfrak{m}R'$. Since R' is a domain and $J \neq 0$, $\dim(R'/J) < \dim(R')$, and

$$\dim(\mathfrak{m}(R/I)/\mathfrak{m}^2(R/I)) = \dim(\mathfrak{m}R'/\mathfrak{m}^2R') = \dim(R'),$$

so $R/I \cong R'/J$ is not regular. □

Recall that for a ring R and a prime $\mathfrak{p}$, the *residue field* of R at $\mathfrak{p}$ is $\kappa(\mathfrak{p}) := R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. For a ring homomorphism $R \xrightarrow{\phi} S$ and a prime $\mathfrak{p} \in \mathrm{Spec}(R)$, the *fiber ring* of ϕ over $\mathfrak{p}$ is $\kappa(\phi, \mathfrak{p}) := (R \setminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$. Since localization and quotienting are special cases of extension of scalars, we can also write this as $\kappa(\phi, \mathfrak{p}) = \kappa(\mathfrak{p}) \otimes_R S$. The point of this construction is that the induced map on Spec from $S \to \kappa(\phi, \mathfrak{p})$ induces a

bijection

$$\operatorname{Spec}(\kappa(\phi,\mathfrak{p})) \xrightarrow{\sim} \{\mathfrak{q} \in \operatorname{Spec}(S) \mid \phi^*(\mathfrak{q}) = \mathfrak{p}\}.$$

Lemma 2.36. *Let R be a Noetherian ring. Let $\mathfrak{q}$ be a prime ideal of $R[x]$ and set $\mathfrak{p} = \mathfrak{q} \cap R$. Then either*

(1) *$\mathfrak{p}R[x]$, with $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p})$, or*
(2) *$\{g(x) \mid \exists a \in R \smallsetminus \mathfrak{p}$ with $ag(x) \in \mathfrak{p}R[x] + (f(x))\}$ for some $f(x) \in \mathfrak{q}$, with $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p}) + 1$.*

Proof. First, we show every other prime is of the form above. We compute $\kappa(\phi,\mathfrak{p}) = \kappa(\mathfrak{p}) \otimes_R R[x] \cong \kappa(\mathfrak{p})[x]$. Every prime in this ring is zero or principal. The preimage of 0 in $R[x]$ is $\mathfrak{p}R[x]$. The preimage of some $(\overline{f}(x))$ for $\overline{f}(x) \in \kappa(\mathfrak{p})[x]$ is the set of $g(x) \in R[x]$ that end up in $\mathfrak{p}R[x] + (f(x))$ after localizing at $R \smallsetminus \mathfrak{p}$, which is the formula above.

The height of $\mathfrak{p}[x]$ is at least that of $\mathfrak{p}$ (say h), since a chain

$$\mathfrak{r}_0 \subsetneqq \mathfrak{r}_1 \subsetneqq \mathfrak{r}_2 \subsetneqq \cdots \subsetneqq \mathfrak{r}_h = \mathfrak{p}$$

yields a chain

$$\mathfrak{r}_0[x] \subsetneqq \mathfrak{r}_1[x] \subsetneqq \mathfrak{r}_2[x] \subsetneqq \cdots \subsetneqq \mathfrak{r}_h[x] = \mathfrak{p}[x].$$

Consequently, a prime of the second type has height at least $\operatorname{ht}(\mathfrak{p}) + 1$.

Finally, we compute the heights. Note that $\operatorname{ht}(\mathfrak{p}[x]) = \operatorname{ht}(\mathfrak{p}R_{\mathfrak{p}}[x]$ since any prime contained in $\mathfrak{p}[x]$ does not meet $R \smallsetminus \mathfrak{p}$. Take a system of parameters $(z_1, \ldots, z_h)$ for $R_{\mathfrak{p}}$. Then $\mathfrak{p}R_{\mathfrak{p}}$ is nilpotent modulo $(z_1, \ldots, z_h)$. But then $\mathfrak{p}R_{\mathfrak{p}}[x]$ is nilpotent modulo $(z_1, \ldots, z_h)R_{\mathfrak{p}}[x]$ as well, since a polynomial with nilpotent coefficients is nilpotent. Thus, $\sqrt{\mathfrak{p}R_{\mathfrak{p}}[x]} \subseteq \sqrt{(z_1, \ldots, z_h)R_{\mathfrak{p}}[x]} \subseteq \sqrt{\mathfrak{p}R_{\mathfrak{p}}[x]}$, so equality holds, and $\operatorname{ht}(\mathfrak{p}R_{\mathfrak{p}}[x]) \leqslant h = \operatorname{ht}(\mathfrak{p}R_{\mathfrak{p}}) = \operatorname{ht}(\mathfrak{p})$, and this gives the formula in case (1).

For a prime of case (2), we note that $\frac{R_{\mathfrak{p}}}{(z_1,\ldots,z_h)}[x]$ has dimension one, since killing the ideal of nilpotents $\mathfrak{p}R_{\mathfrak{p}}[x]$ yields a polynomial ring over a field, which has dimension one. Then, since $\frac{R[x]_{\mathfrak{q}}}{(z_1,\ldots,z_h)}$ is a localization of $\frac{R_{\mathfrak{p}}}{(z_1,\ldots,z_h)}[x]$, we have

$$\operatorname{ht}(\mathfrak{q}) = \dim(R[x]_{\mathfrak{q}}) \leqslant h + \dim\left(\frac{R[x]_{\mathfrak{q}}}{(z_1,\ldots,z_h)}\right) + h \leqslant \dim\left(\frac{R_{\mathfrak{p}}}{(z_1,\ldots,z_h)}[x]\right) + h = h + 1$$

and we are done. □

Lecture of March 23, 2023

Proposition 2.37. *Let R a Noetherian ring and suppose that $R_{\mathfrak{p}}$ is a regular local ring for every prime ideal $\mathfrak{p}$. Then for every prime ideal $\mathfrak{q}$ of $R[x]$, the local ring $R[x]_{\mathfrak{q}}$ is a regular local ring.*

Proof. Let $\mathfrak{q}$ be prime in $R[x]$ and $\mathfrak{p} = \mathfrak{q} \cap R$. Let $h = \operatorname{ht}(\mathfrak{p})$ and $e_1, \ldots, e_h \in \mathfrak{p}$ be a basis for $\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}^2R_{\mathfrak{p}}$, so for any $p \in \mathfrak{p}$, there is $p' \in \mathfrak{p}^2R_{\mathfrak{p}}$, and $r_j \in R_{\mathfrak{p}}$ with $p = \sum_j r_j e_j + p'$ in $R_{\mathfrak{p}}$.

If $\mathfrak{q} = \mathfrak{p}R[x]$, take $q = \sum_i p_i s_i(x) \in \mathfrak{p}R[x]$; then as above we have $q = \sum_i (\sum_j r_{i,j}e_j + p_i')s_i(x)$ in $R_{\mathfrak{p}}[x]$ so $\mathfrak{q}R_{\mathfrak{p}}[x] = ((e_1, \ldots, e_h) + \mathfrak{q}^2)R_{\mathfrak{p}}[x]$, so $\mathfrak{q}R[x]_{\mathfrak{q}} = ((e_1, \ldots, e_h) + \mathfrak{q}^2)R[x]_{\mathfrak{q}}$, and hence $\mathfrak{q}R[x]_{\mathfrak{q}}/\mathfrak{q}^2R[x]_{\mathfrak{q}}$ is generated by $e_1, \ldots, e_h$. Thus, $R[x]_{\mathfrak{q}}$ is regular.

If $\mathfrak{q} = \{g(x) \mid \exists a \in R \smallsetminus \mathfrak{p}$ with $ag(x) \in \mathfrak{p}R[x] + (f(x))\}$ with $f(x) \in \mathfrak{q}$, take $q = \sum_i p_i s_i(x) + f(x)s_0(x) \in \mathfrak{p}R[x]$. Proceeding the same way as above, we get that $\mathfrak{q}R[x]_{\mathfrak{q}}/\mathfrak{q}^2R[x]_{\mathfrak{q}}$ is generated by $e_1, \ldots, e_h, f(x)$, so $R[x]_{\mathfrak{q}}$ is regular. □

Corollary 2.38. *If K is a field, $R = K[x_1, \ldots, x_n]$ is a polynomial ring, and $\mathfrak{p} \subset R$ is prime, then $R_{\mathfrak{p}}$ is regular. Likewise, if $R = \mathbb{Z}[x_1, \ldots, x_n]$ is a polynomial ring, and $\mathfrak{p} \subset R$ is prime, then $R_{\mathfrak{p}}$ is regular.*

2.6. **Smoothness vs regularity.**

Lemma 2.39. *Let $(R, \mathfrak{m}, k)$ be a local ring. Let B be an $m \times n$ matrix with entries in R. Then the following are equivalent:*

(1) *$R^n \xrightarrow{B} R^m$ is a split injection,*
(2) *$K^n \xrightarrow{\overline{B}} K^m$ is injective,*
(3) *$m \geqslant n$ and some $n \times n$ minor of B is a unit.*

Proof. (1) $\Rightarrow$ (2): If $AB = I$, then $\overline{AB} = \overline{I}$, so $\overline{B}$ is injective.

(2) $\Rightarrow$ (3): From linear algebra, the rank of a matrix is the size of its largest nonvanishing minor.

(3) $\Rightarrow$ (1): Without loss of generality, say that B' is the matrix of the first n rows of B, and $\det(B')$ is a unit. Then $A' = \det(B')^{-1}\mathrm{adj}(B')$ satisfies $A'B' = I$, so $[A'|0]B = I$. □

Theorem 2.40. *Let K be a field, $S = K[x_1, \ldots, x_n]$ a polynomial ring over S, and $R = S/I$ for an ideal I. Let $\mathfrak{p}$ be a prime ideal of R and $\mathfrak{q}$ its preimage in S. Suppose that*

(1) *K is algebraically closed and $\mathfrak{p} = \mathfrak{m}$ is a maximal ideal, or*
(2) *more generally, there is a K-algebra right inverse to the projection map $S_\mathfrak{q}/\mathfrak{q}^2 S_q \to S_\mathfrak{q}/\mathfrak{q}S_\mathfrak{q}$.*

Then the following are equivalent:

- *$R_\mathfrak{p}$ is regular.*
- *The map $K \to R_\mathfrak{p}$ is essentially smooth.*
- *The column Jacobian on a minimal generating set for $IS_\mathfrak{q}$, viewed as a matrix in $\kappa(\mathfrak{q}) = S_\mathfrak{q}/\mathfrak{q}S_\mathfrak{q}$ is injective.*

Proof. First we observe that case (1) is a special case of case (2). Now let's rock.

Under the hypothesis of (2), the map $\frac{\mathfrak{q}S_\mathfrak{q}}{\mathfrak{q}^2 S_\mathfrak{q}} \xrightarrow{d} \kappa(\mathfrak{q}) \otimes_S \Omega_{S|K}$ is injective, so the map $\frac{IS_\mathfrak{q}}{I\mathfrak{q}S_\mathfrak{q}} \xrightarrow{d} \kappa(\mathfrak{q}) \otimes_S \Omega_{S|K}$ is injective if and only if the map $\frac{IS_\mathfrak{q}}{I\mathfrak{q}S_\mathfrak{q}} \to \frac{\mathfrak{q}S_\mathfrak{q}}{\mathfrak{q}^2 S_\mathfrak{q}}$ is injective. Since $S_\mathfrak{q}$ is regular, this happens if and only if $R_\mathfrak{p}$ is regular. But the map $\frac{IS_\mathfrak{q}}{I\mathfrak{q}S_\mathfrak{q}} \xrightarrow{d} \kappa(\mathfrak{q}) \otimes_S \Omega_{S|K}$ is just the map given by the column Jacobian of the generators of I viewed in $\kappa(\mathfrak{q})$. This shows the equivalence of the first with the last.

On the other hand, we have the commutative diagram

$$\begin{array}{ccc} R_\mathfrak{p}^{\oplus t} & \xrightarrow{\quad J(f)^T \quad} & R_\mathfrak{p} \otimes_{S_\mathfrak{q}} \Omega_{S|K} \\ & {\scriptstyle q} \searrow \quad \nearrow {\scriptstyle d} & \\ & IS_\mathfrak{q}/I^2 S_\mathfrak{q} & \end{array}$$

where $R_\mathfrak{p}^{\oplus t}$ is a free module with basis in bijection with the minimal generators of $IS_\mathfrak{q}$, q mapping each basis element to the class of one generator. If $K \to R_\mathfrak{p}$ is smooth, then d is a split injection, so $IS_\mathfrak{q}/I^2 S_\mathfrak{q}$ is free, and hence the map q is an isomorphism. Then $J(f)^T$ is a split injection, so by the lemma, the column Jacobian must be injective modulo $\mathfrak{q}S_\mathfrak{q}$, yielding the last condition.

Conversely, if the map $J(f)^T$ is injective modulo $\mathfrak{q}S_\mathfrak{q}$, it is split injective by the lemma, forcing q to be an isomorphism, and then forcing d to be a split injection, and hence forcing $R_\mathfrak{p}$ to be essentially smooth over K. □

Corollary 2.41. *If R is a finitely generated algebra over an algebraically closed field K, then $R_\mathfrak{p}$ is regular for all primes $\mathfrak{p}$ if and only if $K \to R$ is smooth.*

3. Coefficient fields and complete local rings

3.1. **Transcendence bases and p-bases.** Let $K \subseteq L$ be fields. Recall that $l \in L$ is *algebraic* over K if it satisfies a nonzero polynomial equation over K and *transcendental* otherwise. An algebraic element is *separable* if it is a simple root if its minimal polynomial, and *inseparable* otherwise. The only way an algebaric element can be inseparable is if the its minimal polynomial and the derivative of the minimal polynomial are not coprime, and since the minimal polynomial is irreducible and the degree of the derivative is lower, this forces the derivative to be zero. Thus, inseparable elements can only occur in positive characteristic, and the degree of any inseparable element must be a multiple of p, since its minimal polynomial can only contain exponents that are multiples of p. So algebraic extensions in characteristic zero are always separable.

Lecture of March 28, 2023

An algebraic extension is *separable* if every element is separable. We recall that by the primitive element theorem, every finite separable extension is generated by one element. We then have the following.

Proposition 3.1. *If $K \subseteq L$ is a separable algebraic extension of fields, then L is formally étale over K.*

Proof. If $K \subseteq L$ is finite separable, then we can write $L = K[x]/(f(x))$ with $f'(x)$ a unit in L. Then the conormal map is

$$(f(x))/(f(x))^2 \xrightarrow{d} L dx \quad [f(x)] \mapsto f'(x)dx.$$

The source of this map is a one-dimensional L-vector space generated by $[f(x)]$, so this map is an isomorphism, and thus L is étale over K.

If $K[f_1, \dots, f_n] \subseteq L$ is a finitely generated K-algebra, then since each L is algebraic over K, each f_i is integral over K, so $K \subseteq K[f_1, \dots, f_n]$ is integral, and since $K[f_1, \dots, f_n] \subseteq L$ is a domain, it is a field. Since it is finitely generated as an algebra, by Zariski's lemma, it is a finite extension of K, and thus étale over K. The statement then follows from the following lemma. □

Lemma 3.2. *Let R be an A-algebra. If every finitely generated A-subalgebra of R is formally unramified or formally étale, then the same is true for R.*

Proof. Let $X = \{x_r \mid r \in R\}$ be a set of indeterminates in bijection with R, and map $A[X] \to R$ by sending $x_r \mapsto r$, with kernel I. For any finite subset $T \subseteq R$, take $X_T = \{x_t \mid t \in T\}$ and let I_T be the kernel of the map $A[X_T] \to A[T] \subseteq R$. We then have a commutative diagram of inclusions

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_T & \longrightarrow & A[X_T] & \longrightarrow & A[T] & \longrightarrow & 0 \\ & & \downarrow\cap & & \downarrow\cap & & \downarrow\cap & & \\ 0 & \longrightarrow & I & \longrightarrow & A[X] & \longrightarrow & R & \longrightarrow & 0 \end{array}$$

Since $A[X] = \bigcup_T A[X_T]$ and $I_T = I \cap A[X_T]$, we have that $I = \bigcup_T I_T$ and likewise $I^2 = \bigcup_T I_T^2$.

We also have commutative diagrams

$$\begin{array}{ccc} I_T & \xrightarrow{d_T} & \bigoplus_{t\in T} A[T]dx_t \\ \downarrow\cap & & \downarrow\cap \\ I & \xrightarrow{d} & \bigoplus_{r\in R} R dx_r \end{array}$$

and the union over T of the top rows is the bottom row. It is easy to see that the image of d is the union of the images of d_T and likewise for the kernel. So, if each d_T is injective, the same holds for d, and if each d_T is bijective, the same holds for d. This establishes the claim. □

Let $K \subseteq L$. A subset $\{l_\lambda\}$ of elements of L is *algebraically independent* if the K-algebra map $K[\{x_\lambda\}] \to L$ given by $x_\lambda \mapsto l_\lambda$ is injective; i.e., there are no nontrivial relations on the elements over K. In this case, there is an injective map from the field of rational function $K(\{x_\lambda\}) \to L$ with image $K(\{l_\lambda\}) \subseteq L$. If $L = K(\{l_\lambda\})$ for an algebraically independent subset $\{l_\lambda\}$, we that L is a *purely transcendental* extension of K.

Definition 3.3. Let $K \subseteq L$ be fields. We say that a subset $\{l_\lambda\}$ is a *transcendence basis* for L over K if it is algebrically independent and every element of L is algebraic over $K(\{l_\lambda\})$.

We say $\{l_\lambda\}$ is a *transcendence basis* for L (without any K) if it is a transcendence basis over the ground field ($\mathbb{Q}$ or $\mathbb{F}_p$).

Lemma 3.4. *Let $K \subseteq L$ be fields.*

(1) *A subset of L is a transcendence basis over K if and only if it is a maximal algebraically independent subset of L.*
(2) *Every algebraically independent subset of L is contained in a transcendence basis.*

Proof. (1) If $\{l_\lambda\}$ and $l \in L$, then l is algebraic over $K(\{l_\lambda\})$, so there is a nonzero polynomial relation $l^n + r_1 l^{n-1} + \cdots + r_n = 0$ with $r_i \in K(\{l_\lambda\})$. Writing $r_i = \frac{p_i}{q_i}$ and multiplying by the product of the q_i's gives a nonzero polynomial relation on the l_λ's and l. Thus, $\{l_\lambda\}$ is a maximal algebraic subset. The converse is similar.

(2) Given a nested union of algebraically independent subsets, the union is as well, since a relation on one of these sets involves finitely many elements, all of which must occur in one of the sets in the chain. The claim then follows from Zorn's Lemma. □

Example 3.5. (1) Let $K = \mathbb{Q}(x^2, xy, y^2)$. Then $K = \mathbb{Q}(x^2, xy)$, since $y^2 = (xy/x^2)^2$, and x^2, xy are algebraically independent, since given a polynomial $F(u, v)$ with $F(x^2, xy) = 0$, there must be no v terms (because of y) and then no u terms (because of x). Thus, x^2, xy is a transcendence basis (and K is purely transcendental). Also, $\mathbb{Q}(x^2, y^2) \subseteq K$ is algebraic, since $(xy)^2 - (x^2)(y^2)$ is a relation, so x^2, y^2 is also a transcendence basis.

(2) Let $K = \mathbb{C}$. We claim that any transcendence basis for $\mathbb{C}$ is uncountable. Note first that a polynomial ring in countably many variables over a field is a countable dimensional vector space: there are countably many monomials. Then, since $\mathbb{Q}$ is countable, $\mathbb{Q}[x_1, x_2, \dots]$ is a countable $\mathbb{Q}$-vector space, so is countable. Then $\mathbb{Q}(x_1, x_2, \dots)$ is classes of polynomials over polynomials, and there are countably many pairs of polynomials. Finally, the algebraic closure of a countable field is countable, since there is an injection from the set of polynomials in one variable to over that field to it. So any field of countable transcendence degree over $\mathbb{Q}$ is again countable, which $\mathbb{C}$ is not.

Let $K \subseteq L$ be fields of characteristic $p > 0$. Recall that $L^p = \{l^p \mid l \in L\}$ is a subfield of L. For a subset $T = \{l_\lambda\}$ of elements of L, we write

$$T^{[<q]} = \{t_{\lambda_1}^{a_1} \cdots t_{\lambda_m}^{a_m} \mid 0 \leqslant a_i < q\}.$$

Definition 3.6. Let $K \subseteq L$ be fields of characteristic $p > 0$. A subset $T = \{l_\lambda\}$ is

- *p-independent* over K if $T^{[<p]}$ is linearly independent over $K(L^p)$.
- *p-spanning* over K if $T^{[<p]}$ spans over $K(L^p)$.
- a *p-basis* over K if $T^{[<p]}$ is a basis for $K(L^p)$.

We say $T = \{l_\lambda\}$ is a *p-basis* for L (without any K) if it is a p-basis over the ground field ($\mathbb{F}_p$).

Lemma 3.7. *Let $K \subseteq L$ be fields of characteristic $p > 0$.*

(1) *A subset of L is a p-basis over K if and only if it is a maximal p-independent subset of L.*
(2) *Every p-indepdendent subset of L is contained in a p-basis.*

Proof. (1) It is clear that a p-basis is a maximal p-independent set. For the other direction, by maximality, if $l \in L$, there is a relation $l^{p-1}f_{p-1} + \cdots + lf_1 + f_0 = 0$ with $f_i \in K(L^p) \cdot T^{[<p]} \subseteq K(L^p)(T)$. This implies that $[K(L^p)(T)(l) : K(L^p)(T)] < p$. Since the minimal polynomial divides $x^p - l^p$, and this factors as $(x-l)^p$ over L, it must be a power of $x-l$, but if $1 < a < p$, $(x-l)^a \in K^p[x]$, its derivative is nonzero and a is a root, contradicting that it is the minimal polynomial, so $l \in K(L^p)(T)$. But using the relations $l^p \in L^p$, we have $K(L^p)(T) = K(L^p)T^{[<p]}$, so T is a p-basis.
(2) Straightforward application of Zorn's Lemma. □

Definition 3.8. $K \subseteq L$ is an extension of fields of positive characteristic, the *p-degree* of the extension, written $p\text{-deg}_K(L)$ is the cardinality of a p-basis for the extension.

Note that if T is a finite p-basis, then $[L : K(L^p)] = p^{|T|}$, and if T is an infinite p-basis, $[L : K(L^p)] = |T| = p^{|T|}$. Thus, the p-degree is well-defined, and $p^{p\text{-}\deg_K(L)} = [L : K(L^p)]$.

Lecture of March 30, 2023

Example 3.9. (1) If K is perfect, then $K = K^p$, so the empty set is a p-basis. In particular, this is true for any finite field. In particular, the p-degree is zero.
(2) If K is perfect and $L = K(t)$ then $L^p = K^p(t^p) = K(t^p)$ so $L = K(L^p) \cdot \{1, t, \ldots, t^{p-1}\}$. Thus, t is a p-basis for L over K, and the p-degree is one. Similarly, for a purely transcendental extension of a perfect field, the transcendence basis forms a p-basis. In particular, the field $F_p(t_1, t_2, \ldots)$ has infinite p-degree.
(3) Let F be perfect. For the field extension $F(t) \subseteq F(t^{1/p^e})$, the element t^{1/p^e} forms a p-basis, but no element of the form $t^{1/p^{e'}}$ with $e' < e$ does. In particular, for the tower $\mathbb{F}_p(t) \subseteq \mathbb{F}_p(t^{1/p}) \subseteq \mathbb{F}_p(t^{1/p^2})$, each intermediate extension has p-degree one, and the composition has p-degree one as well.

Remark 3.10. Let T be a p-basis for L over K. Then any element of L can be written uniquely as a monomial in $T^{[<p]}$ with coefficients in $K(L^p)$. For $t_0 \in T$, define $\frac{d}{dt_0}$ to be the $K(L^p)$-linear map that maps the monomial $t_0^{a_0}t_1^{a_1}\cdots t_j^{a_j}$ to $a_0 t_0^{a_0-1}t_1^{a_1}\cdots t_j^{a_j}$. Note that this depends not just on t but the choice of an entire p-basis. We claim that this is a K-linear derivation. By construction, it is well-defined, additive, and kills K, so we just need to check the product rule, and by additivity, again just on monomials in $T^{[<p]}$, which is then clear.

Moreover, one can take formal combinations of these derivations (as we did with polynomial rings) since every element is expressed in terms of finitely many elements of the p-basis. So there are derivations of the form

$$\sum_{t \in T} l_t \frac{d}{dt},$$

which map t to l_t.

On the other hand, any K-linear derivation on L is zero on L^p, so $K(L^p)$ is in the kernel, and hence is $K(L^p)$-linear. L is generated as a $K(L^p)$-algebra by T, so derivations are uniquely determined by their values on T. Thus, every derivation is of this form.

Theorem 3.11. *Let $K \subseteq L$ be an extension of fields. Let $T \subseteq L$.*

(1) *If K and L have characteristic zero, then $\{dt \mid t \in T\}$ is a vectorspace basis for $\Omega_{L|K}$ if and only if T is a transcendence basis for L over K.*

(2) *If K and L have characteristic $p > 0$, then $\{dt \mid t \in T\}$ is a vectorspace basis for $\Omega_{L|K}$ if and only if T is a p-basis for L over K.*

Proof. (1) If T is a transcendence basis, we have $K \subseteq K(T) \subseteq L$ with $K(T)$ a field of rational functions in the t's and $K(T) \subseteq L$ separable algebraic. We have $\Omega_{K[T]|K}$ is free over $K[T]$ in the basis dt, since it is a polynomial ring, and by localization $\Omega_{K(T)|K}$ is a vectorspace on the same basis. Furthermore, $\Gamma_{K(T)|K} = 0$ by the same steps. From the Jacobi-Zariski sequence

$$\Gamma_{L|K(T)} \to L \otimes_{K(T)} \Omega_{K(T)|K} \to \Omega_{L|K} \to \Omega_{L|K(T)} \to 0$$

plus the fact that L is étale over $K(T)$ we get that $\Gamma_{L|K(T)} = \Omega_{L|K(T)} = 0$ and $L \otimes_{K(T)} \Omega_{K(T)|K} \cong \Omega_{L|K}$, so $\Omega_{L|K}$ is free on dt.

For the other direction, suppose that $\{dt\}$ is a basis for $\Omega_{L|K}$. If $F(x_1, \ldots, x_m)$ is a polynomial such that $F(t_1, \ldots, t_m) = 0$ is a relation of smallest degree, then for some i, $\frac{dF}{dx_i} \neq 0$ and has lower degree than F, so $\frac{\partial F}{\partial x_i}(t) \neq 0$ for some i . Then $0 = dF = \sum_i \frac{dF}{dx_i}(t)dt_i$ is a nonzero relation on the t_i's. Thus, T is algebraically independent. If not a transcendence basis, we can properly include T in a transcendence basis, and by the first direction, we get that dt is a proper subset of a basis, so it does not span $\Omega_{L|K}$. Thus, since it spans, T is a transcendence basis.

(2) Suppose that T is a p-basis. To show that $\{dt \mid t \in T\}$ is a basis for the vectorspace $\Omega_{L|K}$, it suffices to show that for any function $f : T \to L$, there is a unique L-linear map $\phi : \Omega_{L|K} \to L$ such that $\phi|_T = f$. This follows from the discussion above.

On other hand, if $\{dt\}$ is a basis for $\Omega_{L|K}$, we claim that T is p-independent. Indeed, if not, we can take $t_1, \ldots, t_n \in T$ such that $\{t_1, \ldots, t_n\}^{[<p]}$ are linearly independent over $K(L^p)$ and so, without loss of generality (saying some monomial with t_1 occurs), the degree of t_1 over $K(L^p, t_2, \ldots, t_n)$ is less than p, so $t_1 \in K(L^p, t_2, \ldots, t_n) = K(L^p) \cdot \{t_2, \ldots, t^n\}^{[<p]}$. So, $t_1 = G(t_2, \ldots, t_n)$ for some polynomial $G(x_2, \ldots, x_n) \in K(L^p)[x_2, \ldots, x_n]$. We then have $dt_1 = \sum_{i>1} \frac{dG}{dx_i}(t)dt_i$, contradicting linear independence. If not a p-basis, then we can properly include T in a p-basis, obtaining a contradiction as in the previous case. □

3.2. **Completion.** Let R be a ring, I an ideal, and M an R-module.

Define

$$d_I(m, m') = \frac{1}{\inf\{e > 0 \mid m \not\equiv m' \mod I^e M\}},$$

with the convention $1/\infty = 0$. This is a measure of how close m and m' are in terms of powers of I, scaled so that close in the sense of high powers makes this distance smaller. This function satisfies most of the axioms of a metric: clearly $d_I(m, m') \geqslant 0$ with equality if $m = m'$, and if $d_I(m, m''), d_I(m', m'') < 1/e$ so $m - m'', m' - m'' \in I^e M$, then $m - m' \in I^e M$ and $d_I(m, m') < 1/e$, so

$$d_I(m, m') \leqslant \max\{d_I(m, m''), d_I(m', m'')\} (\leqslant d_I(m, m'') + d_I(m', m'')).$$

However, $m \neq m'$ does not always guarantee $d_I(m, m') > 0$: for example, in a ring $R \times S$ considered as a module over itself, with the ideal $I = 0 \times S$, we have $I = I^e$ for all e, so $d_I((r, s), (r, s')) = 0$.

Definition 3.12. Let R be a ring, I an ideal, and M an R-module. The *I-adic topology* on M is the topology with open basis $\{m + I^a M \mid m \in M, a \in \mathbb{N}\}$; that is, the topology whose open sets are arbitrary unions of sets of the form $m + I^a M$; this is the topology arising from the pseudometricspace structure from the function d_I.

The central case is when $M = R$, so the basic open sets are of the form $r + I^n$. The point of the I-adic topology is that two elements are close if they are congruent modulo a large power of I.

Let us translate some basic topological notions into this topology.

Proposition 3.13. *Let R be ring, I an ideal, and M an R-module. Let $\{a_n\}$ be a sequence of elements in M and $a \in M$.*

- *$\lim m_n = m$ in the I-adic topology if and only if for any $e \in \mathbb{N}$, there is some $d \in \mathbb{N}$ such that for all $n \geqslant d$, $m_n \equiv m \mod I^e M$.*
- *In particular, $\lim m_n = 0$ in the I-adic topology if and only if for any $e \in \mathbb{N}$, there is some $d \in \mathbb{N}$ such that for all $n \geqslant d$, $m_n \in I^e M$.*
- *$\{a_n\}$ is Cauchy if and only if for any $e \in \mathbb{N}$, there is some $d \in \mathbb{N}$ such that for all $n, n' \geqslant N$, $m_n \equiv m'_n \mod I^e M$.*
- *If S is another ring, J ideal of S, and N an S-module, a function $f : M \to N$ is continuous with respect to the two topologies if for any $e \in \mathbb{N}$, there is some $d \in \mathbb{N}$ such that $m \equiv m' \mod I^d M$ implies $f(m) \equiv f(m') \mod J^e N$; that is, $f(m + I^d M) \subseteq f(m) + J^e N$.*

  In particular, if $\phi : R \to S$ is a ring homomorphism and $\phi(I) \subseteq J$, then ϕ is continuous (w.r.t. I and J topologies), any R-module homomorphism $\alpha : M \to N$ is continuous (w.r.t. I topologies), and any derivation $\theta : R \to M$ is continuous (w.r.t. I topologies).

Definition 3.14. We say that a module M is *I-adically separated* if $\bigcap_{n\in\mathbb{N}} I^n M = 0$.

If $(R, \mathfrak{m})$ is local, we simply say M is *separated* to mean $\mathfrak{m}$-adically separated.

This is equivalent to saying that limits are unique in the I-adic topology. Indeed, $m \in \bigcap_{n\in\mathbb{N}} I^n M$, then the limit of the constant sequence $\{m\}$ is both 0 and m, so unique limits implies separated, and conversely, if $\lim m_n = m$ and $\lim m_n = m'$ then $m - m' \in \bigcap_{n\in\mathbb{N}} I^n M$ so separated implies unique limits. By the Krull Intersection Theorem, any finitely generated module over a local ring $(R, \mathfrak{m})$ is $\mathfrak{m}$-adically separated.

Definition 3.15. We say that a module M is *I-adically complete* if every Cauchy sequence in M has a unique limit.

If $(R, \mathfrak{m})$ is local, we simply say M is *complete* to mean $\mathfrak{m}$-adically complete. In particular, a complete local ring is a local ring that is complete with respect to its maximal ideal.

Example 3.16.

(1) Let $(R, \mathfrak{m})$ be an Artinian local ring, so $\mathfrak{m}^t = 0$ for some t. Then any Cauchy sequence is eventually constant: taking $e = t$, there is a d such that for $n, n' \geqslant d$, $r_n \equiv r_{n'} \mod \mathfrak{m}^e$ so $r_n = r_{n'}$. Thus an Artinian local ring is complete.

(2) Let A be a ring and $R = A[x_1, \ldots, x_t]$. Then R is not $(x_1, \ldots, x_t)$-adically complete, since the sequence $(\sum_{i=0}^n x^i)$ is Cauchy but has no limit: the limit would have arbitrarily large degree.

(3) Let A be a ring and $R = A[\![x_1, \ldots, x_t]\!]$. We claim that R is $(x_1, \ldots, x_t)$-adically complete. Indeed the condition for a sequence $\{f_n(x)\}$ to be Cauchy is that for any e, there is some d such that for $n, n' \geqslant d$, the coefficients up to degree e in $f_n(x)$ and $f_{n'}(x)$ agree. That is, the $x_1^{a_1} \cdots x_t^{a_t}$-coefficient of $f_n(x)$ for n sufficiently large (greater than the d coming from $e = a_1 + \cdots + a_t$) is well-defined. The unique power series with these coefficients is the unique limit of $\{f_n(x)\}$. In particular, a power series ring over a field is a complete local ring.

(4) If R is I-adically complete, and J is an ideal of R, then R/J is $I(R/J)$-adically complete. In particular, a quotient of a power series ring over a field is a complete local ring.

Lemma 3.17. *Let R be a ring, I an ideal, and M an R-module. Let $\{r_n\}$, $\{s_n\}$ be sequences in R and $\{m_n\}$, $\{l_n\}$ be sequences in M.*

1. *If $\{r_n\}$ and $\{s_n\}$ are Cauchy, then so are $\{r_n + s_n\}$ and $\{r_n s_n\}$.*
2. *If $\lim r_n = 0$ or $\lim s_n = 0$, then $\lim r_n s_n = 0$.*
3. *If $\{m_n\}$ and $\{l_n\}$ are Cauchy, so is $\{m_n + l_n\}$.*
4. *If $\{r_n\}$ and $\{m_n\}$ are Cauchy, then so is $\{r_n m_n\}$.*
5. *If $\lim m_n = 0$ or $\lim r_n = 0$, then $\lim r_n m_n = 0$.*

Proof. Note that (1) and (2) are special cases of the rest. If $\{m_n\}$, $\{l_n\}$, and $\{r_n\}$ are Cauchy, fix e and take a d that "works" for all three sequences (taking the max). Then for $n, n' > d$, $(m_n + l_n) - (m_{n'} + l_{n'}) = (m_n - m_{n'}) + (l_n - l_{n'}) \in I^e M$, and $r_n m_n - r_{n'} m_{n'} = r_n m_n - r_{n'} m_n + r_{n'} m_n - r_{n'} m_{n'} = (r_n - r_{n'}) m_n + r_{n'}(m_n - m_{n'}) \in I^e M$, so this d works for each.

If $\lim m_n = 0$, fix e and take a d that "works". Then for $n > d$, $r_n m_n \in r_n I^e M \subseteq I^e M$; similarly if $\lim r_n = 0$. □

It follows from this lemma that given a ring R, and ideal I, the set of Cauchy sequences with pointwise addition and multiplication forms a ring, and the set of sequences that converge to zero forms an ideal in this ring. There is a homomorphism from R to this ring that sends an element to the associated constant sequence.

Definition 3.18. Let R be a ring and I an ideal. The I-adic completion of R is the ring $\hat{R}^I$ given by the quotient of the ring of Cauchy sequences by the ideal of sequences that converge to zero. This is an R-algebra given by the map sending an element to the class of a constant sequence.

If M is an R-module, the set of Cauchy sequences in M is a module over the ring of Cauchy sequences in R, and the set of sequences converging to zero is a submodule. One can check that this induces a well-defined module action of $\hat{R}^I$ on the set of equivalence classes of Cauchy sequences on M modulo sequences converging to zero.

Definition 3.19. Let R be a ring, I an ideal, and M a module. The I-adic completion of M is the $\hat{R}^I$-module $\hat{M}^I$ given by the quotient of the ring of Cauchy sequences by sequences converging to zero in M.

Remark 3.20. Let R be a ring, I an ideal, and M a module. Given a Cauchy sequence (a_n) in M, by passing to a subsequence, we can assume that for any e, and any $n, m \geqslant e$, $a_n - a_m \in I^e M$; we just keep skipping to the "dth term." Thus, we can write $a_e = a_0 + (a_1 - a_0) + (a_2 - a_1) + \cdots + (a_e - a_{e-1})$ with $a_e - a_{e-1} \in I^{e-1} M$. In this way, we can represent any element in $\hat{M}^I$ as a power series with nth term in $I^n M$; conversely, any such series is clearly Cauchy, so represents an element of the completion.

Remark 3.21. The following alternative description of completion is also useful. Consider the set of sequences $(\bar{r}_n)$ with $\bar{r}_n \in R/I^n$ such that the image of $\bar{r}_{n+1}$ under the quotient map $R/I^{n+1} \to R/I^n$ is $\bar{r}_n$ for all n. The sum or product of two such sequences is again of the same form, so this is a ring, and there is an obvious map from R to this ring.

Lecture of April 6, 2023

Let's say that a sequence in $R/I \times R/I^2 \times R/I^3 \times \cdots$ is *consistent* if for any n, the image of the nth component under the quotient map $R/I^n \to R/I^{n-1}$ equals the $n-1$st component. We claim that there is an isomorphism from $\hat{R}^I$ to the ring of consistent sequences. To define it, note that for a sequence (r_n) and any e, the Cauchy condition implies that the value of r_n modulo I^e stabilizes at some point; set $\bar{r}_e$ to be

that value. Then $(\bar{r}_e)$ satisfies the compatibility condition above. Given Cauchy sequences (r_n), (s_n), it is straightforward to see that the associated sequences respect sum and product. Furthermore, a sequence (r_n) converges to zero if and only if the stable value of r_n modulo I^e is zero for all e, so this map is well-defined from the completion, and injective. Given any sequence in the target, taking arbitrary lifts for the elements to R yields a Cauchy sequence, so this map is surjective.

The same construction works just as well for modules. One advantage of these constructions is that we have well-defined representatives for objects.

We summarize:

Proposition 3.22. *Let R be a ring, I an ideal, and M a module. There is an R-algebra isomorphism*

$$\hat{R}^I \cong \{(\bar{r}_1, \bar{r}_2, \bar{r}_3, \dots) \in R/I \times R/I^2 \times R/I^3 \times \cdots \mid \bar{r}_{n+1} \equiv \bar{r}_n \mod I^n\}$$

and isomorphism of $\hat{R}^I$-modules

$$\hat{M}^I \cong \{(\bar{m}_1, \bar{m}_2, \bar{m}_3, \dots) \in M/IM \times M/I^2M \times M/I^3M \times \cdots \mid \bar{m}_{n+1} \equiv \bar{m}_n \mod I^nM\}.$$

Example 3.23.

(1) If $R = A[x_1, \dots, x_n]$, then $\hat{R}^{(x)} \cong A[\![x_1, \dots, x_n]\!]$.
(2) The I-adic completion of $R^{\oplus n}$ is $(\hat{R}^I)^{\oplus n}$. Indeed, Cauchy implies Cauchy in each coordinate using nothing, and Cauchy in each coordinate implies Cauchy, since for each e, we can take a d for each coordinate, and the max of these "works". Similarly, converging to zero means converging to zero in each coordinate.
(3) The I-adic completion of $R^{\oplus \mathbb{N}}$ contains $(\hat{R}^I)^{\oplus \mathbb{N}}$ by the same argument as the interesting direction above, and can be identified with a subset of $\prod_{\mathbb{N}} \hat{R}^I$ by the same argument as the boring direction. However, it is strictly between the direct sum and direct product. Indeed, an element of the completion corresponds to a sequence of elements in $\hat{R}^I$ such that for every e, there are at most finitely many entries that are not in $I^e(\hat{R}^I)$.
(4) The (x)-adic completion of the $K[x]$-module $K[x, x^{-1}]$ is zero, since $\bigcap_{n\in\mathbb{N}} x^n K[x, x^{-1}] = K[x, x^{-1}]$.

Given a ring homomorphism $\alpha : R \to S$ with $\phi(I) \subseteq J$, there is an induced map $\hat{\alpha} : \hat{R}^I \to \hat{S}^J$. Indeed, a continuous map sends a Cauchy sequence to a Cauchy sequence, and a sequence converging to zero to another converging to zero. It is easy to see this is a ring homomorphism. Likewise, a module homomorphism $\alpha : M \to N$ induces a module homomorphism $\hat{\alpha} : \hat{M}^I \to \hat{N}^I$.

Lemma 3.24. *Let R be a ring, I be a finitely generated ideal, and M be an R-module. Then there are equalities*

$$\begin{aligned} I^e\hat{M}^I &= \{ \textit{ equivalence classes of Cauchy sequences with entries in } I^eM\} \\ &= \{ \textit{ consistent sequences with first } e \textit{ components equal to zero } \}. \end{aligned}$$

Proof. We start with the first equality. Clearly any sequence in $I^e\hat{M}^I$ is represented by a sequence with entries in I^eM, so the other containment needs to be shown. Let $x \in\in \hat{M}^I$ be represented by a Cauchy sequence with entries in I^eM. Take a series representation: $x = \sum_{n=0}^{\infty} a_n$ with $a_n \in I^nM$. We must have $a_i = 0$ for $i \leqslant e$, since $x \equiv \sum_{n=0}^{i} a_i \mod I^i$. Let $I^e = (f_1, \dots, f_t)$. We can write $a_n = \sum f_j b_{n,j}$ with $b_{n,j} \in I^{n-e}M$ for all $n \geqslant e$. Then each sequence $s_n^{(j)} = \sum_{k=e}^{n} b_{k,j}$ is a Cauchy sequence in M, and $x = \sum_j f_j s_n^{(j)}$.

The second equality is straightforward: if each entry is in I^e, then the stable value modulo I^m for $m \leqslant d$ is zero, and conversely if the stable value modulo I^e is zero, by passing to a subsequence, we can assume that all elements are in I^e. □

Proposition 3.25. *Let R be a ring, I be a finitely generated ideal, and M be an R-module. The completion $\hat{M}^I$ is $I\hat{R}^I$-adically complete.*

Proof. Given a Cauchy sequence in $\hat{R}^I$, for any e, there is a stable value for modulo $I^e\hat{R}^I$, so the first e coordinates stabilize. Take the sequence of stable values; this satisfies the consistency condition, so this is an element of the completion. It is then clear this is the limit. □

Proposition 3.26. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then $\hat{R}$ (the $\mathfrak{m}$-adic completion of R) is a complete local ring with maximal ideal $\mathfrak{m}\hat{R}$, and for any R-module M, $\hat{M}$ is complete.*

Proof. Since $\mathfrak{m}$ is finitely generated, we know that $\mathfrak{m}\hat{R}$ is the set of Cauchy sequences whose stable value mod $\mathfrak{m}$ is nonzero; by passing to a subsequence, we can assume any such sequence (a_n) has elements that are all units. Now, if $a_n - a_{n'} \in \mathfrak{m}^e$, then $a_n^{-1} - a_{n'}^{-1} = \frac{a_{n'} - a_n}{a_n a_{n'}} \in \mathfrak{m}^e$, so (a_n^{-1}) is a Cauchy sequence, and its class is an inverse for (a_n). This shows that $\hat{R}$ is local with maximal ideal $\mathfrak{m}\hat{R}$. From the previous proposition, $\hat{R}$ and $\hat{M}$ are then complete. □

Proposition 3.27.
(1) *If $R \to S$ is surjective, and $J = IS$, then the induced map $\hat{R}^I \to \hat{S}^J$ on completions is surjective.*
(2) *If $M \to N$ is a surjective map of R-modules, then the induced map $\hat{M}^I \to \hat{N}^I$ on completions is surjective.*
(3) *The completion of a Noetherian ring with respect to any ideal is Noetherian.*

Proof. Given an element of $s \in \hat{S}^J$, we can write $s = \sum_{n=0}^{\infty} s_n$ with $s_n \in J^n$. We can then choose a preimage of s_n that is in I^n, and inductively, we get a sequence of preimages that is Cauchy. Thus the induced map on completions is surjective.

The second statement is similar.

For the last, let $I = (f_1, \dots, f_n)$ and take the induced map on completions from $R[x_1, \dots, x_n] \to R$ sending $x_i \mapsto f_i$. This expresses the I-adic completion as a quotient of a power series ring in finitely many variables over a Noetherian ring, which is again Noetherian. □

Lecture of April 11, 2023

3.3. **Three main technical things about completion.**

3.3.1. *Flatness.* The key to exactness properties of completion is the Artin-Rees lemma.

Theorem 3.28 (Artin-Rees Lemma)**.** *Let R be a Noetherian ring, I an ideal, and $L \subseteq M$ finitely generated R-modules. Then there exists a constant c such that for all n, $I^n M \cap L \subseteq I^{n-c}L$.*

The proof is in the 902 notes.

Theorem 3.29. *Let R be a Noetherian ring.*
(1) *If $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is an exact sequence of finitely generated R-modules, then $0 \to \hat{L}^I \xrightarrow{\hat{\alpha}} \hat{M}^I \xrightarrow{\hat{\beta}} \hat{N}^I \to 0$ is exact.*
(2) *If M is a finitely generated R-module, then $\hat{R}^I \otimes_R M \cong \hat{M}^I$.*
(3) *$\hat{R}^I$ is a flat R-algebra.*

Proof. (1) We have already seen that $\hat{\beta}$ is surjective. We identify L with $\alpha(L)$ and N with M/L.

To see that $\hat{\alpha}$ is injective, let (l_n) be a Cauchy sequence in L. If $\lim l_n = 0$ in M, then for any e, there is d such that for $n \geqslant d$, $l_n \in I^e M$. Take c such that $I^n M \cap L \subseteq I^{n-c}L$ by Artin-Rees. Then

for any $e' = e + c$, there is d such that for $n \geqslant d$, $l_n \in I^{e+c}M \cap L \subseteq I^e L$, so (l_n) represents the zero element in $\hat{L}^I$. This shows injectivity.

We also need Artin-Rees for exactness in the middle. Let (m_n) be a Cauchy sequence representing an element in the kernel of $\hat{\beta}$. Then for any e, there is some d such that for $n \geqslant d$, $\beta(m_n) \in I^e N$. This implies that $m_n \in I^e M + L$, so write $m_n = m'_n + l_n$ for each n, with $m'_n \in I^e M$. It suffices to show that (l_n) is a Cauchy sequence in L. But $l_n = m_n - m'_n$ is Cauchy viewed as a sequence in M; then given $e' = e + c$, there is d such that for all $n, n' \geqslant d$, $l_n - l_{n'} \in I^{e+c}M \cap L \subseteq I^e L$, so it is Cauchy in L. Thus, (m_n) represents an element in the image.

(2) Take a presentation:

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

We can apply base change or completion; since the completions are $\hat{R}^I$-modules, there are maps via the universal property of extension of scalars:

$$\begin{array}{ccccccc} \hat{R}^I \otimes_R R^m & \xrightarrow{A} & \hat{R}^I \otimes_R R^n & \longrightarrow & \hat{R}^I \otimes_R M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \hat{R^m}^I & \longrightarrow & \hat{R^n}^I & \longrightarrow & \hat{M}^I & \longrightarrow & 0 \end{array}$$

The top rows is exact by definition of extension of scalars, the bottom by part (1). The first two down arrows are isomorphisms by earlier example. The last map must then be an isomorphism.

(3) From parts (1) and (2), it follows that for any inclusion of finitely generated modules, the extension of scalars to the completion is injective. Given a general inclusion of modules, $L \subseteq M$, if $\hat{R}^I \otimes_R L \to \hat{R}^I \otimes_R M$ is not injective, take an element in the kernel. Take a generating set for L and one for M that contains it; then one can take a generating set of relations for L and extend it to a generating set of relations on M. An element in the kernel of $\hat{R}^I \otimes_R L \to \hat{R}^I \otimes_R M$ is a linear combination of finitely many generators $S \subseteq L$, and a combination of finitely many relations on the generators of M. Let L' be the submodule of L generated by S and M' the submodule of M generated by the elements occurring in the relations on generators of M making the element zero. Then the element is in the kernel of the corresponding map. □

Example 3.30. (1) Let $R = K[x]$, $M = K[x, x^{-1}]/K[x]$, and

$$0 \to K \cdot \frac{1}{x} \to M \xrightarrow{x} M \to 0.$$

Then the completion is just

$$0 \to K \to 0 \to 0 \to 0,$$

which is no longer exact.

(2) Let $R = K[x]$, and consider the sequence

$$0 \to \bigoplus_n R \xrightarrow{\mu} \bigoplus_n R \xrightarrow{\pi} \bigoplus_n R/x^n \to 0,$$

where $\mu(e_i) = x^i e_i$ and π is the projection map. Then the element $(x, x^2, x^3, \dots)$ is a valid element of $\widehat{\bigoplus_n R}$ and is in the kernel of $\hat{\pi}$, but is not in the image of $\hat{\mu}$, since $(x, x, x, \dots)$ is not a valid element of $\widehat{\bigoplus_n R}$.

Corollary 3.31. *If A is Noetherian and $R = A[x_1, \dots, x_n]/I$, then $\hat{R}^{(x)} \cong A[\![x_1, \dots, x_n]\!]/IA[\![x_1, \dots, x_n]\!]$.*

Proof. First, we note that the (x)-adic completion of R as a ring is the same as the (x)-adic completion of R as an $A[x_1, \dots, x_n]$-module: Cauchy and convergent sequences are the same in either. Then, the (x)-adic completion of R is the $A[\![x_1, \dots, x_n]\!]$-module with the same presentation; i.e., $A[\![x_1, \dots, x_n]\!]/IA[\![x_1, \dots, x_n]\!]$. □

3.3.2. *Super NAK.*

Theorem 3.32 (Complete NAK)**.** *Let $(R, \mathfrak{m}, k)$ be a complete local ring, and M be a separated R-module. Then, for $m_1, \dots, m_t \in M$, we have*

$$M = \sum_i Rm_i \qquad \iff \qquad M/\mathfrak{m}M = \sum_i k\overline{m_i}.$$

Proof. The implication $(\Rightarrow)$ is clear.

For the other implication, we have that $M = \sum_i Rm_i + \mathfrak{m}M$. Consequently, $\mathfrak{m}M = \sum_i \mathfrak{m}m_i + \mathfrak{m}^2 M$, etc. Then, for $m \in M$, write

$$\begin{aligned} m &= \sum_i r_{i,0}m_i + t_1, && r_{i,0} \in R,\ t_1 \in \mathfrak{m}M \\ t_1 &= \sum_i r_{i,1}m_i + t_2, && r_{i,1} \in \mathfrak{m},\ t_2 \in \mathfrak{m}^2 M \\ t_2 &= \sum_i r_{i,2}m_i + t_3, && r_{i,2} \in \mathfrak{m}^2,\ t_3 \in \mathfrak{m}^3 M \\ &\vdots && \vdots \end{aligned}$$

The sequences $\{r_{i,0}, r_{i,0}+r_{i,1}, r_{i,0}+r_{i,1}+r_{i,2}, \dots\}$ for each i are Cauchy, so we obtain elements $r_i = \sum_j r_{i,j} \in R$. Consider the element $\tilde{m} = \sum_i r_i m_i \in M$. To compute $m - \tilde{m}$ modulo $\mathfrak{m}^n M$, we may replace r_i by $\sum_{j=0}^{n-1} r_{i,j}$, and we see the difference is congruent to t_n, which is hence congruent to zero. Thus $m - \tilde{m} \in \mathfrak{m}^n M$ for each n. Thus, $m = \tilde{m}$, so $M = \sum_i Rm_i$. □

3.3.3. *Hensel's Lemma.*

Theorem 3.33 (Hensel's lemma)**.** *Let $(R, \mathfrak{m}, k)$ be a complete local ring. Let $F \in R[x]$ be monic. Suppose that the image of f of F in $k[x]$ factors as $f = gh$ with $g, h \in k[x]$ monic and $(g, h) = 1$. Then there exist $G, H \in R[x]$ monic with images $g(x), h(x) \in k[x]$ respectively and $F = GH$.*

Proof. The idea is to inductively solve modulo $\mathfrak{m}^n$, where the base case is the given hypothesis. Suppose we have $G_n, H_n \in R[x]$ such that $\overline{G_n} = g, \overline{H_n} = h$ and $F - G_n H_n \in \mathfrak{m}^n[x]$. Note that the leading coefficients cancel, so this difference has degree less than that of F. Thus, we can write

$$F - G_n H_n = \sum_i U_i V_i \qquad U_i \in \mathfrak{m}^n, V_i \in R[x], \deg V_i < \deg(F).$$

Since $(g, h) = 1$, we can write $a_i g + b_i h = \overline{V_i}$ with $a_i, b_i \in k[x]$; after replacing a_i with the remainder modulo h and changing b_i appropriately, we can assume that $\deg(a_i) < \deg(h)$. Then,

$$\deg(hb_i) = \deg(\overline{V_i} - a_i g) < \deg(f) = \deg(g) + \deg(h), \quad \text{so } \deg(b_i) < \deg(g).$$

Now, pick $A_i, B_i \in R[x]$ with $\overline{A_i} = a_i, \deg(A_i) = \deg(a_i)$ (likewise with B's), and set $G_{n+1} = G_n + \sum_i U_i B_i$, $H_{n+1} = H_n + \sum_i U_i A_i$. These polynomials then satisfy the same hypotheses (modulo $\mathfrak{m}^{n+1}$). Indeed:

$$\begin{aligned} F - G_{n+1}H_{n+1} &= F - (G_n + \sum U_i B_i)(H_n + \sum U_i A_i) \\ &= F - G_n H_n - \sum U_i B_i H_n - \sum U_i A_i G_n - (\sum U_i B_i)(\sum U_i A_i) \\ &= \sum_i U_i V_i - \sum U_i B_i H_n - \sum U_i A_i G_n - (\sum U_i B_i)(\sum U_i A_i) \end{aligned}$$

The last term is in $\mathfrak{m}^{2n}[x] \subseteq \mathfrak{m}^{n+1}[x]$. Thus, modulo $\mathfrak{m}^{n+1}[x]$ we have

$$\sum_i U_i(V_i - B_i H_n - A_i G_n).$$

Since $U_i \in \mathfrak{m}^n[x]$ and $V_i - B_i H_n - A_i G_n \in \mathfrak{m}[x]$, this difference is zero.

The elements $\{G_n\}$ and $\{H_n\}$ then form a Cauchy sequence converging to the required elements. □

Corollary 3.34. *Let $(R, \mathfrak{m}, k)$ be a complete local ring, and $F \in R[x]$. If $f = \overline{F} \in k[x]$ has a simple root α in k, then F has a simple root $a \in R$ with $a \bmod \mathfrak{m} = \alpha$.*

Proof. If $\overline{f}$ has a simple root in k, then it factors in k as $(x-\alpha)g$, with g coprime to $x - \alpha$. We can lift this factorization by Hensel's lemma, to get the same type of factorization in R, yielding a simple root. □

Example 3.35. We can use Hensel's Lemma to show that the polynomial $1 + x$ has a square root in $R = \mathbb{C}[\![x]\!]$. This is the same as showing that $T^2 - x - 1$ has a root. Going modulo x we get $T^2 - 1$, which has $T = 1$ as a simple root. By Hensel's Lemma, we get a root in R.

Example 3.36. The hypothesis of simple root is necessary. Indeed, over $R = \mathbb{C}[\![x, y]\!]$, the polynomial $T^2 - xy$ has 0 as a simple root modulo (x, y), but no root in R, since xy is not a square.

Example 3.37. Consider the ring $R = \mathbb{C}[x, y]/(y^2 - x^2 - x^3)$. This ring is a domain, and $S = R_{(x,y)}$ is as well. Geometrically, this corresponds to a curve with a crossing at the origin. Even locally, this is irreducible. However, in the completion $\hat{S} = \frac{\mathbb{C}[\![x,y]\!]}{(y^2-x^2-x^3)}$ the element $x^2 - x^3 = x^2(1 + x)$ is a square, so the equation factors, and $\hat{S}$ has two minimal primes corresponding to the two branches of the curve near the origin.

3.4. **Coefficient fields and Cohen Structure Theorem.**

Definition 3.38. Let $(R, \mathfrak{m}, k)$ be a local ring. A *coefficient field* for R is a field $K \subseteq R$ such that the map $K \subseteq R \to k$ is an isomorphism.

Note that a local ring can have a coefficient field only if it contains a field, which is equivalent to having equal characteristic. In this case, the map from any subfield to the residue field is always injective.

Example 3.39.

(1) Let $R = \mathbb{R}[x]_{(x^2+1)}$. Then $R/\mathfrak{m} \cong \mathbb{C}$, but there is no coefficient field for R, since any element in R is a rational function over $\mathbb{R}$, which squares to an element that is a nonnegative function, so there is no solution to $z^2 + 1 = 0$ in R.

(2) Let $R = \mathbb{C}[x, y]_{(x)}$. Then $\mathbb{C}(y)$ and $\mathbb{C}(x + y)$ are two different coefficient fields for R.

(3) Let $R = \mathbb{F}_p(t)\widehat{[x]}_{(x^p-t)}$. This is a complete local ring, with residue field $\mathbb{F}_p(t)[x]/(x^p - t) \cong \mathbb{F}_p(t^{1/p})$.

We claim that no coefficient field contains t. Suppose otherwise that K is a coefficient field containing t, and hence $\mathbb{F}_p(t)$. Then there is an element $r \in K \subseteq R$ with $r^p = t$. Going modulo $(x^p - t)$, there is a unique pth root of t in the residue field, so we must have $r \equiv x \mod (x^p - t)$, so $r = x + (x^p - t)g$. But then $r^p = x^p + (x^p - t)^p g^p \equiv x^p \mod (x^p - t)^2$, but $x^p \not\equiv t \mod (x^p - t)^2$, a contradiction.

However, we claim that $\mathbb{F}_p(x) \subseteq R$ is a coefficient field. First, we note that the field of rational functions of x is contained in $\mathbb{F}_p(t)[x]_{(x^p-t)} = \mathbb{F}_p[t,x]_{(x^p-t)}$, since $\mathbb{F}_p[x] \cap (x^p - t)\mathbb{F}_p[t,x] = 0$, so every element of $\mathbb{F}_p[x]$ maps to a unit in $\mathbb{F}_p(t)[x]_{(x^p-t)}$, and a local ring injects into its completion. But $x \in R$ maps to $t^{1/p}$ in the residue field, so this is a surjective map of fields, and hence an isomorphism.

Lemma 3.40. *Let $(R, \mathfrak{m}, k)$ be a local ring of equal characteristic. Then any subfield of R is contained in a maximal subfield, and if K is a maximal subfield, the extension $K \subseteq k$ is algebraic.*

Proof. The first part is a straightforward application of Zorn's lemma. For the second, let $K \subseteq R$ be a maximal subfield. Suppose that $\theta \in k$ is transcendental over K, and let $r \in R$ be a lift of θ. For any nonzero polynomial $f(x) \in K[x]$, we must have that $f(\theta) \neq 0$ in k, so $f(r)$ is not in $\mathfrak{m}$; i.e., is a unit. Thus the map $K[x] \to R$ is mapping x to r is injective and extends to a map $K(x) \cong K(r) \subseteq R$. This contradicts the maximality of K. □

Theorem 3.41. *Let $(R, \mathfrak{m}, k)$ be a local ring of equal characteristic zero. Then every maximal subfield of R is a coefficient field. In particular, every subfield of R is contained in a coefficient field.*

Proof. Let K be a maximal subfield. By the lemma, $K \subseteq k$ is algebraic, and by the hypothesis of characteristic zero, is separable algebraic. Suppose that there is some $\theta \in k \smallsetminus K$. Then $\alpha \in k$ is a simple root of some irreducible monic polynomial $f \in K[x]$. We have $f \in K[x] \subseteq R[x] \to k[x]$, so we can apply Hensel's lemma. Thus, f has a simple root θ in R that has image α in k. Then $K[x]/(f(x)) \cong K[\theta] \subseteq R$ is a larger subfield of R, contradicting minimality. □

Lemma 3.42. *If Θ is a p-basis for k, then $\Theta^{[<p^e]}$ is a basis for k over k^{p^e}.*

Theorem 3.43. *Let $(R, \mathfrak{m}, k)$ be a local ring of equal characteristic $p > 0$. Let Θ be a p-basis for k. Then for any lift T of Θ to R, there is a coefficient field of R containing T, namely $K = \bigcap_{e\in\mathbb{N}} R^{p^e}[T]$.*

Proof. First we observe that any coefficient field must contain some lifting of Θ. Also, note that K is a subring of R that contains T.

Note that $R^{p^e}[T] = R^{p^e} \cdot T^{[<p^e]}$. Now observe that $R^{p^e}[T] \cap \mathfrak{m} \subseteq \mathfrak{m}^{p^e}$. Indeed, write $u \in \mathfrak{m}$ as an R^{p^e}-linear combination of $T^{[<p^e]}$. Taking images of this linear combination module $\mathfrak{m}$ gives a k^{p^e}-linear combination of $\Theta^{[<p^e]}$ that is zero, so by the lemma, each coefficient is zero in k^{p^e}, and hence in the original combination, each coefficient is in $\mathfrak{m} \cap R^{p^e} \subseteq \mathfrak{m}^{p^e}$. Thus

$$K \cap \mathfrak{m} = \bigcap_e (R^{p^e}[T] \cap \mathfrak{m}) \subseteq \bigcap_e \mathfrak{m}^{p^e} = 0.$$

Thus, K injects into k.

Now we show that the map $K \to k$ is surjective. We define a set theoretic function $\ell : k \to R$ such that $\pi \circ \ell$ is the identity on k as follows: Fix $\lambda \in k$. Since $k = k^{p^e}[\Theta]$, for any e we can pick some $r_e \in R^{p^e}[T]$ that maps to λ. Then $r_{e+1} - r_e \in \mathfrak{m}$ since their images coincide in k, and $r_{e+1} - r_e \in R^{p^e}[T] \cap \mathfrak{m} \subseteq \mathfrak{m}^{p^e}$, so (r_e) is a Cauchy sequence in R. Let $\ell(\lambda) = \lim_e r_e$. To see that ℓ is well-defined, given (r'_e) with r'_e mapping to λ, $r_e - r'_e \in R^{p^e}[T] \cap \mathfrak{m} \subseteq \mathfrak{m}^{p^e}$, so the difference converges to 0. The image of $\ell(\lambda)$ in k is λ, since this is true for each r_e.

Now we show that for any λ and any n, $\ell(\lambda) \in R^{p^n}[T]$; this will show that $\ell(\lambda) \in K$ so the map $K \to k$ is surjective.

Given e, write λ as an element of $k^{p^n}\Theta^{[<p^n]}$:

$$\lambda = \sum_\mu c_\mu^{p^n}\theta^\mu,$$

where μ runs over all exponent tuples with each exponent bounded by p^n. For every μ and e, pick some $c_{\mu,e} \in R^{p^e}[T]$ such that $c_{\mu,e}$ maps to c_μ in k, so $(c_{\mu,e})$ is a Cauchy sequence with limit $\ell(c_\mu)$. Let

$$w_e = \sum_\mu c_{\mu,e}^{p^n} t^\mu.$$

Then $w_e \in R^{p^e}[T]$ and the $w_e \equiv \lambda \mod \mathfrak{m}$. Again by well-definedness of ℓ, we have

$$\lim_e w_e = \ell(\lambda).$$

On the other hand,

$$\lim_e w_e = \sum_\mu \lim_e (c_{\mu,e}^{p^n}) t^\mu = \sum_\mu \lim_e (c_{\mu,e})^{p^n} t^\mu = \sum_\mu \ell(c_\mu)^{p^n} t^\mu \in R^{p^n}[T]. \qquad \square$$

Theorem 3.44 (Cohen Structure Theorem)**.** *Let $(R, \mathfrak{m}, k)$ be a local ring containing a field. Then $R \cong k[\![x_1, \ldots, x_n]\!]/I$ for some ideal I.*

Proof. Let $\mathfrak{m} = (a_1, \ldots, a_n)$. Consider the homomorphism $k[\![x_1, \ldots, x_n]\!] \to R$ induced by map $k[x_1, \ldots, x_n] \to R$ mapping x_i to a_i. We claim that this is surjective. The image if (x) in R is contained in $\mathfrak{m}$, so R is (x)-adically separated. Then since the image 1 generates $R/(x)R$ as a $k[\![x_1, \ldots, x_n]\!]/(x)$ vector space, 1 generates R as a $k[\![x_1, \ldots, x_n]\!]$-module. This means that the map is surjective. $\square$