# Wiles' numerical criterion

Josua Kugler

August 15, 2022

## Contents

**1 A brief sketch of the proof of Fermat's Last Theorem** **2**
1.1 Fermat's Last Theorem and the modularity conjecture . . . . . 2
1.2 Galois representations and modularity . . . . . 3
1.3 Ribet's theorem and the contradiction . . . . . 5
1.4 Wiles' proof of modularity: The 3-5 trick . . . . . 6
1.5 Wiles' proof of modularity: The main theorem . . . . . 6
1.6 Wiles' proof of modularity: $R = T$ and the numerical criterion . 7

**2 Wiles' numerical criterion** **8**
2.1 Introduction . . . . . 8
2.2 Preliminaries and examples . . . . . 8
2.3 Basic properties of the invariants . . . . . 14
2.4 Regular sequences and the Koszul complex . . . . . 18
2.5 Complete intersections and Gorenstein rings . . . . . 21
2.6 Explicit computation of $\eta$ for complete intersections . . . . . 28
2.7 Isomorphism theorems . . . . . 31
2.8 A resolution lemma . . . . . 35
2.9 A criterion for complete intersections . . . . . 36
2.10 Proof of Wiles' numerical criterion . . . . . 37

# 1 A brief sketch of the proof of Fermat's Last Theorem

## 1.1 Fermat's Last Theorem and the modularity conjecture

**Theorem 1.1** (Fermat's Last Theorem)**.** *There are no $a, b, c \in \mathbb{Z}$ with $abc \neq 0$ and $n \in \mathbb{N}, n \geq 3$ such that*

$$a^n + b^n = c^n.$$

Actually this is equivalent to

**Theorem 1.2.** *There are no $a, b, c \in \mathbb{Z}$ with $abc \neq 0$ and a prime number $p \geq 5$ such that*

$$a^p + b^p = c^p.$$

Indeed, let $a^n + b^n = c^n$ be a solution of the Fermat equation where $n \geq 3$. In the latter case, $n$ is always divided by a prime number $\geq 3$ or by 4. We can then write $n = \tilde{p} \cdot m$ where $\tilde{p} \in \{4\} \cup \{p | p \text{odd prime}\}$ and obtain

$$a^n + b^n = c^n \Leftrightarrow (a^m)^{\tilde{p}} + (b^m)^{\tilde{p}} = (c^m)^{\tilde{p}}.$$

The case $\tilde{p} = 4$ has been ruled out by Fermat himself and the case $\tilde{p} = 3$ was shown soon after, so any solution of the Fermat equation of exponent $n$ induces a solution of the Fermat equation for some prime number $p \geq 5$.

One of the key breakthroughs in the proof of FLT was to consider the

**Definition 1.1** (Frey-Hellegouarch-Curve)**.** From a solution of the Fermat equation we can with little technical modifications obtain a triple $(a, b, c)$ such that $a^p + b^p + c^p = 0$, $a \cong -1 \mod 4, 2|b$. Then define the elliptic curve

$$E_{a,b,c} \colon y^2 = x(x - a^p)(x + b^p).$$

This curve has weird properties in a sence that numerical invariants of this curve contradict several well-known conjectures (such as Serre's conjecture that was actually proved in 2008. See next section) and Frey conjectured that such a curve couldn't exist. He suggested to prove this by associating a modular form to this curve and showing that this modular form couldn't exist. The key point in this strategy was the following

**Theorem 1.3** (Modularity)**.** *Every semistable elliptic curve over $\mathbb{Q}$ is modular, i.e. there is a modular form $f$ "associated" to $E$ in a sence that will be made precise in the next sections.*

When Frey had the idea of using this to prove FLT, it still was a conjecture. It was finally proved by Andrew Wiles and Richard Taylor in 1995. (In the years until 1999 the semistability condition could be removed, so that the theorem holds for all elliptic curves.)

## 1.2 Galois representations and modularity

**Definitions** Let $A$ be coefficient ring, i.e. a complete noetherian local ring with finite residue field $k$. A continuous map of the form

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$$

is called a Galois representation, where $G_{\mathbb{Q}}$ is endowed with the Krull topology. By reducing to the residue field, we obtain the residual representation

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(k),$$

where the topology on $k$ is the discrete topology. A residual representation can have multiple lifts. Two such lifts $\rho, \rho'$ are called equivalent if $\rho = M\rho M^{-1}$ for $M \in \mathrm{GL}_2(A)$ s.t. $M \equiv \mathrm{id}_2 \mod \mathfrak{m}_A$. An equivalence class of lifts of $\rho_0$ is called deformation of $\rho$.

**Definition 1.2.** A Galois representation $\rho$ is **odd**, if $\rho(c) = -1$ where $c$ denotes the generator of $G_{\mathbb{Q}_\infty}$. Note that $G_{\mathbb{Q}_\infty}$ is canonically isomorphic to the decomposition subgroup associated to $\infty$ in $G_{\mathbb{Q}}$.

**Definition 1.3.** A Galois representation $\rho$ is **unramified** at $\ell$, if the inertia group $I_\ell$ is contained in the kernel of $\rho$. Being **flat** is a condition of similar nature, though considerably more technical.

**Galois representations for elliptic curves** As it is very difficult to come from an elliptic curve to a modular form directly, Wiles chose an indirect way via Galois representations. For each elliptic curve $E$ over $\mathbb{Q}$, we have an associated galois representation. Take the $p$-torsion subgroup $E[p]$ of $E$ (i.e. the kernel of $p$-multiplication on $E$). It is well known that we can choose a generating system $P, Q$ for $E[p]$ and obtain an isomorphism $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$. As $\mathbb{Q}(E[p])$ is a Galois number field, it is not hard to see that we have a Galois operation on $E[p]$, i.e. a morphism

$$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Completely analogous, we can construct compatible morphisms for $E[p^n]$ and in the limit we obtain a map.

$$\rho_{E,p} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p).$$

One can show that $\rho_{E,p}$ is also continuous with respect to the Krull- resp. $p$-adic topology, i.e. $\rho_{E,p}$ is a Galois representation.

**Proposition 1.1.** *[CSS97, chapter 1, theorem 2.11] Let $N_E$ be the conductor of $E$ and $\rho_{E,p}$ the representation described above. Then*

- $\det \circ \rho_{E,p} = \chi_p$
- *$\rho_{E,p}$ is unramified at primes not dividing $pN_E$*

- $\rho_{E,p}$ *is odd*

*If $E$ is semistable and $\Delta_E$ its minimal discriminant, we can further conclude that for*

$$\overline{\rho}_{E,p}\colon G_Q \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

*the following equivalences hold.*

- $\overline{\rho}_{E,p}$ *is flat at* $p \Leftrightarrow p|\operatorname{ord}_p(\Delta_E)$.
- *For any prime* $\ell \neq p$*:* $\overline{\rho}_{E,p}$ *is unramified at* $\ell \Leftrightarrow p|\operatorname{ord}_\ell(\Delta_E)$.

**Galois representations for modular forms** Now that we have seen how to associate a Galois representation to an elliptic curve, we want to do the same thing for a modular form. However, this is far more difficult and therefore beyond the scope of this thesis. The result that we need is that to a new cuspform $f$ of weight 2 we can associate a Galois representation $\rho_f$ [see DS07, section 9.5]. Now we can state Serre's conjecture that was mentioned in the introduction. Let

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be a continuous, odd, irreducible Galois representation. Then there exists a cuspidal eigenform $f$ , such that

$$\rho \cong \rho_f$$

the Galois representation associated to $f$. Serre even gives detailed formulas that assert a certain weight and level for $f$. In the case of $\rho_{E_{a,b,c},p}$ it predicts level two and weight two, a contradiction. That might be one of the reasons why Frey considered they Frey curve $E_{a,b,c}$ to be strange.

**Modularity** A Galois representation $\rho$ is modular if there is a newform $f$ of weight 2 such that

$$\rho \cong \rho_f.$$

For elliptic curves $E/\mathbb{Q}$ we have the following

**Theorem 1.4.** *[CSS97, chapter 1, theorem 5.1] An elliptic curve $E/\mathbb{Q}$ with conductor $N_E$ is modular if it satisfies the following equivalent conditions.*

1. *For some prime p,* $\rho_{E,p}$ *is modular.*
2. *For all primes p,* $\rho_{E,p}$ *is modular.*
3. *There is a newform $f$ of weight 2 and level $N_E$ s.t. $L(f,s) = L(E,s)$.*
4. *There is a non-constant morphism $\pi\colon X_0(N_E) \to E$ of algebraic curves over $\mathbb{Q}$.*
5. *There is an isogeny $E \to A_f$, where $A_f$ is the modular abelian variety associated to a weight 2 newform $f$ of conductor $N_E$.*

*The last three equivalences are of no further relevance to the thesis but might be of interest to the reader.*

## 1.3 Ribet's theorem and the contradiction

For a moment, let's believe that every elliptic curve is modular. In order to prove FLT, we need one more deep ingredient, namely

**Theorem 1.5** (Ribet's theorem)**.** *Let $f$ be a newform of weight 2 and level $N\ell$ for a prime $\ell$ s.t. $\ell \nmid N$. Suppose that the associated Galois representation $\overline{\rho}_f$ is absolutely irreducible and satisfies one of the following conditions.*

- *$\overline{\rho}_f$ is unramified at $\ell$*
- *$\ell = p$ and $\overline{\rho}_f$ is flat at $p$.*

*Then there is a newform of weight 2 and level $N$ such that*

$$\overline{\rho}_f \cong \overline{\rho}_g.$$

By the modularity theorem theorem 1.3 we find a newform $f$ of weight 2 such that

$$\overline{\rho}_{E_{a,b,c},p} \cong \overline{\rho}_f$$

We need the semistability of $E_{a,b,c}$ and the properties shown in proposition 1.1. Because of the specific properties of the Frey curve we have the following finer results for $\rho_{E_{a,b,c},p}$ [see CSS97, chapter 1, theorem 3.1].

- $\rho_{E_{a,b,c},p}$ is absolutely irreducible
- $\rho_{E_{a,b,c},p}$ is unramified outside $2p$ and flat at $p$

As $E$ is semistable, the conductor is squarefree,

$$N_E = 2 \cdot p \cdot \prod_{\ell \in S \text{ prime}} \ell$$

for a finite set $S$ of primes $\neq 2, p$. Let $\ell_0 \in S$. As $\overline{\rho}_{E_{a,b,c},p}$ is unramified at $\ell_0$, by Ribet's theorem we find a newform $f'$ of weight 2 and level

$$2 \cdot p \cdot \prod_{\ell \in S \setminus \{\ell_0\} \text{ prime}} \ell$$

such that $\overline{\rho}_{f'} \cong \overline{\rho}_{E_{a,b,c},p}$. By repeating this step, we obtain a newform $g'$ of weight 2 and level $2p$ whose reduced Galois representation is still equivalent to $\overline{\rho}_{E_{a,b,c},p}$. As $\overline{\rho}_{E_{a,b,c},p}$ is flat at $p$, we find a newform $g$ of weight 2 and level 2 such that

$$\overline{\rho}_{E_{a,b,c},p} \cong \overline{\rho}_g.$$

However, the only newform of weight 2 and level 2 is 0, so we obtain the desired contradiction.

## 1.4 Wiles' proof of modularity: The 3-5 trick

What remains now for the proof of FLT is the proof of the modularity theorem, i.e. that every semistable elliptic curve is modular. Wiles chose to proof version 1 of modularity as defined in theorem 1.4 Therefore we take a closer look at the $p$-adic representation $\rho_{E,p}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ associated to an elliptic curve $E/\mathbb{Q}$.

**Lemma 1.1.** *There is a prime $p$ such that the* mod $p$ *reduction of the galois representation $\rho_{E,p}$*

$$\overline{\rho}_{E,p}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

*satisfies the following properties.*

*(A)* $\det \overline{\rho}_{E,p} = \chi_p$

*(B)* $\overline{\rho}_{E,p}$ *is semistable*

*(C)* $\overline{\rho}_{E,p}$ *is absolutely irreducible*

*(D)* $\overline{\rho}_{E,p}$ *is modular, and* $\overline{\rho}_{E,p}|_{G_{\mathbb{Q}}(\sqrt{-3})}$ *is absolutely irreducible*

*Proof.* We have seen in proposition 1.1 that $\rho_{E,p}$ has determinant $\chi_p$. As $E$ is semistable we know that $\rho_{E,p}$ is semistable We now need to prove that there is a $p$ s.t. $\overline{\rho}_{E,p}$ is irreducible and modular. **Explain why absolute irreducibility of rhobar and of rhobarsqrt-3 are clear once modularity and irreducibility are shown.** Wiles proved the following

**Proposition 1.2.** *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Then at least one of $\overline{\rho}_{E,3}$ or $\overline{\rho}_{E,5}$ is irreducible.*

This allows us to make a case distinction.

- If $\overline{\rho}_{E,3}$ is irreducible, then by some group theoretical considerations we can apply the Langlands-Tunnel-theorem and conclude that $\overline{\rho}_{E,3}$ is modular.
- If $\overline{\rho}_{E,5}$ is irreducible, then Wiles has shown that there is another semistable elliptic curve $E'/\mathbb{Q}$ s.t.$\overline{\rho}_{E',3}$ is irreducible and $\overline{\rho}_{E',5} \cong \overline{\rho}_{E',5}$. Hence, we can apply the first case for $E'$ and obtain that $\overline{\rho}_{E',3}$ is modular. However, by theorem 1.4, then $\overline{\rho}_{E',5}$ and thereby also the equivalent representation $\overline{\rho}_{E,5}$ are modular.

In either case we have found a $p$ s.t. $\overline{\rho}_{E,p}$ is irreducible and modular. □

## 1.5 Wiles' proof of modularity: The main theorem

Let $A$ be a ring of coefficients **i.e. noetherian, local, Dedekind, ...?** and $k$ its quotient field. The goal of this part of the proof is to show that all lifts

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$$

of any galois representations $\rho_0\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ satisfying certain conditions are modular.

For each deformation type $\mathcal{D}$, we can define a universal deformation ring $R_{\mathcal{D}}$ together with a universal deformation

$$\rho_{\mathcal{D}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R_{\mathcal{D}}).$$

## 1.6 Wiles' proof of modularity: $R = T$ and the numerical criterion

# 2 Wiles' numerical criterion

## 2.1 Introduction

Wiles has discovered a criterion for two rings in a specific category to be isomorphic that only depends on some numerical invariants of these rings. The aim of this section is to prove that criterion in its purely algebraic form. In our presentation, we closely follow [DDT95, pp. 5.1 – 5.8].

## 2.2 Preliminaries and examples

Let $\mathcal{O}$ be the ring of integers of a finite extension $K$ of $\mathbb{Q}_\ell$. As $K$ is a local field, its ring of integers is a discrete valutation ring (DVR), i.e. $\mathcal{O}$ is a local, noetherian Dedekind ring with maximal ideal $\lambda$. It is complete with resp server usedect to the $\lambda$-adic topology, a principal ideal domain (PID) and has residue field $k \coloneqq \mathcal{O}/\lambda$ to name some properties that we will use in the course of the proof.

$\mathbb{Z}_\ell$ is the ring of integers of $\mathbb{Q}_\ell$ and $\mathbb{F}_\ell = \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$ its residue field. As $K/\mathbb{Q}_\ell$ is finite, the residue field of $\mathcal{O}$ is a finite extension of $\mathbb{F}_\ell$ and therefore finite.

**The categories $\mathcal{C}_\mathcal{O}$ and $\mathcal{C}_\mathcal{O}^\bullet$** In this section, we will mostly deal with very specific rings. Therefore we define the category $\mathcal{C}_\mathcal{O}$ where objects of $\mathcal{C}_\mathcal{O}$ are local complete noetherian $\mathcal{O}$-algebras with residue field $k$ and the morphisms are local $\mathcal{O}$-algebra morphisms. Often, we even need some extra structure. We obtain the category $\mathcal{C}_\mathcal{O}^\bullet$ from $\mathcal{C}_\mathcal{O}$ by equipping an object $A$ with an additional surjective $\mathcal{O}$-algebra homomorphism

$$\pi_A \colon A \twoheadrightarrow \mathcal{O},$$

the so-called augmentation map. Objects in $\mathcal{C}_\mathcal{O}^\bullet$ are often called *augmented rings*. The morphisms in $\mathcal{C}_\mathcal{O}^\bullet$ are local $\mathcal{O}$-algebra morphisms that respect the augmentation map structure, i.e. for a morphism $f \colon A \to B$ we have the commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ & {\scriptstyle \pi_A}\searrow \quad \swarrow{\scriptstyle \pi_B} & \\ & \mathcal{O} & \end{array} .$$

In order to state Wiles' criterion, we need some more definitions.

**Definition 2.1.** $A \in \mathcal{C}_\mathcal{O}$ is *finite flat*, if $A$ is finitely generated and torsion-free as an $\mathcal{O}$-module. Note that $\mathcal{O}$ is a PID and therefore being torsion-free is equivalent to being flat as an $\mathcal{O}$-module.

**Definition 2.2** (complete intersection)**.** [see DDT95, Def. 5.1] A finite flat ring $A \in \mathcal{C}_\mathcal{O}$ is called a *complete intersection*, if $A$ is isomorphic as an $\mathcal{O}$-algebra to a quotient

$$A \cong \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n),$$

where there are as many relations as there are variables.

Let's take a look at an example.

**Example 2.1.** [cf. DDT95, example 1] $A = \{(a,b) \in \mathcal{O}\times\mathcal{O},\ a \equiv b \pmod{\lambda^n}\} \cong \mathcal{O}[[T]]/(T(T-\lambda^n))$ is a finite flat complete intersection in $\mathcal{C}^\bullet_{\mathcal{O}}$. The projection $\pi_A$ is given by $\pi_A(a,b) = a$.

*Proof.* Consider the map

$$\begin{aligned}\phi\colon \mathcal{O}[[T]]/(T(T-\lambda^n)) &\to A\\ f &\mapsto (f(0), f(\lambda^n)).\end{aligned}$$

- $\phi$ **is welldefined and respects the $\mathcal{O}$-algebra structure:** Let $f_0$ be the constant term of a polynomial $f$ and $f_1 \coloneqq T^{-1}(f-f_0)$, s.t. $f = f_0 + T\cdot f_1(T)$. Because of

  $$f(0) - f(\lambda^n) = (f_0 + 0\cdot f_1(0)) - (f_0 + \lambda^n \cdot f_1(\lambda^n)) = -\lambda^n \cdot f_1(\lambda^n),$$

  $f(0) \equiv f(\lambda^n) \pmod{\lambda^n}$ as required. Furthermore,

  $$\phi(T(T-\lambda^n)) = (0(-\lambda^n), \lambda^n(\lambda^n - \lambda^n)) = (0,0).$$

  Finally, we need to think about series in $\mathcal{O}[[T]]$ with infinitely many terms. For the first component $f(0)$ this doesn't matter, as $\phi$ just takes the constant term. As $\mathcal{O}$ is complete with respect to the $\lambda$-adic topology, the map $\tilde{\phi}_2\colon \mathcal{O}[[T]] \to \mathcal{O},\ f \mapsto f(\lambda^n)$ is clearly welldefined and thus $\phi$ is welldefined. Let $o \in \mathcal{O}$. Then

  $$\phi(of) = ((of)(0), (of)(\lambda^n)) = (of(0), of(\lambda^n)) = o(f(0), f(\lambda^n)) = o\phi(f)$$

- **Injectivity:** Let $\phi(f) = 0$. Then $f(0) = 0 \implies T|f$ and $f(\lambda^n) = 0 \implies (T-\lambda)|f$. As a result, $f \in T(T-\lambda)$.

- **Surjectivity:** Let $(a,b) \in A$. As $a \equiv b \bmod \lambda^n$, we can write $b = a + b'\cdot\lambda^n$. Because of

  $$\phi(\overline{a + b'T}) = (a, a + b'\lambda^n) = (a,b),$$

  $\phi$ is surjective.

- $A \in \mathcal{C}^\bullet_{\mathcal{O}}$**:** $\mathcal{O}$ is noetherian, so $\mathcal{O}[T]/(T(T-\lambda^n))$ is noetherian as well. $(\lambda, T)$ is a maximal ideal in $\mathcal{O}[T]/(T(T-\lambda^n))$, because

  $$\left(\mathcal{O}[T]/(T(T-\lambda^n))\right)/(\lambda,T) = \mathcal{O}/(\lambda) = k.$$

  Therefore, the completion $\mathcal{O}[T]/(T(T-\lambda^n))^{\wedge(\lambda,T)}$ of $\mathcal{O}[T]/(T(T-\lambda^n))$ with respect to $(\lambda,T)$ is a local ring with maximal ideal $\widehat{(\lambda,T)}$. Consider the SES of finitely generated $\mathcal{O}$-modules

  $$0 \to (T(T-\lambda^n))\mathcal{O}[T] \to \mathcal{O}[T] \to \mathcal{O}[T]/(T(T-\lambda^n)) \to 0.$$

As completion of finitely generated $\mathcal{O}$-modules is exact (because $\mathcal{O}$ is noetherian), we get the SES

$$0 \to (T(T-\lambda^n))\mathcal{O}[[T]] \to \mathcal{O}[[T]] \to \mathcal{O}[T]/(T(T-\lambda^n))^{\wedge(\lambda,T)} \to 0.$$

by completing with respect to $(\lambda, T)$. As a result, we have

$$\mathcal{O}[T]/(T(T-\lambda^n))^{\wedge(\lambda,T)} = \mathcal{O}[[T]]/(T(T-\lambda^n)).$$

Hence, $\mathcal{O}[[T]]/(T(T-\lambda^n))$ is a local ring with maximal ideal $(\lambda, T)$. Therefore, its residue field is

$$\mathcal{O}[[T]]/(T(T-\lambda^n))/(\lambda,T) = \mathcal{O}[T]/(T(T-\lambda^n))/(\lambda,T) = \mathcal{O}/(\lambda) = k.$$

As $\mathcal{O}[T]/(T(T-\lambda^n))$ is noetherian, its $(\lambda, T)$-completion $\mathcal{O}[[T]]/(T(T-\lambda^n))$ is again noetherian [cf. AM69, theorem 10.26]. In total, we get that $A \cong \mathcal{O}[[T]]/(T(T-\lambda^n))$ is a local, complete, noetherian $\mathcal{O}$-algebra with residue field $k \implies A \in \mathcal{C}_{\mathcal{O}}$.

- $A$ **is a finite flat complete intersection:** $A$ is generated by $(1,1)$ and $0, \lambda^n$ because

$$(a,b) = a(1,1) + (0, \underbrace{b-a}_{\in\lambda^n}) = a(1,1) + c(0,\lambda^n).$$

Also, $A$ is torsion-free because $\mathcal{O}$ is an integral domain. As there is one variable and one relation in $A \cong \mathcal{O}[[T]]/(T(T-\lambda^n))$, $A$ is a complete intersection.

□

**Example 2.2.** [cf. DDT95, example 5] $U = \mathcal{O}[[X_1, \ldots, X_n]]$ with projection $\pi_U : U \to \mathcal{O},\ f \mapsto f(0)$ lies in $\mathcal{C}_{\mathcal{O}}^{\bullet}$.

*Proof.* $\mathcal{O}$ is noetherian, so $\mathcal{O}[X_1, \ldots, X_n]$ is noetherian as well. $(\lambda, X_1, \ldots, X_n)$ is a maximal ideal in $\mathcal{O}[X_1, \ldots, X_n]$, because

$$(\mathcal{O}[X_1, \ldots, X_n])/(\lambda, X_1, \ldots, X_n) = \mathcal{O}/(\lambda) = k.$$

Therefore, the completion

$$\mathcal{O}[X_1, \ldots, X_n]^{\wedge(\lambda, X_1, \ldots, X_n)} = \mathcal{O}[[X_1, \ldots, X_n]]$$

of $\mathcal{O}[X_1, \ldots, X_n]$ with respect to $(\lambda, X_1, \ldots, X_n)$ is a local ring with maximal ideal $(\lambda, \widehat{X_1, \ldots}, X_n)$. Its residue field is $\mathcal{O}[X_1, \ldots, X_n]/(\lambda, X_1, \ldots, X_n) = k$, as required. As $\mathcal{O}[X_1, \ldots, X_n]$ is noetherian, its $(\lambda, X_1, \ldots, X_n)$-completion is again noetherian. □

**Remark 2.1.** *In example 2.1 we could write $A$ as a quotient of $\mathcal{O}[[X]]$. This is possible in a more general setting, in fact every $A \in \mathcal{C}_{\mathcal{O}}$ can be written as a quotient of $U = \mathcal{O}[[X_1, \ldots, X_n]]$ for suitable $n$.*

*Proof.* As $A$ is a noetherian ring and $\ker \pi_A$ is an ideal in $A$, it is finitely generated and therefore also finitely generated as an $A$-module. Consider the map

$$\begin{aligned} \Phi \colon U = \mathcal{O}[[X_1, \dots, X_n]] &\to A \\ X_i &\mapsto a_i, \end{aligned}$$

where $\ker \pi_A = (a_1, \dots, a_n)$ and $\pi_U$ is given by $f \mapsto f(0)$. As $(X_1, \dots, X_n)$ generate the kernel of $\pi_U$, this is a map in $\mathcal{C}^\bullet_\mathcal{O}$. We have the short exact sequences

$$0 \to \ker \pi_A \to A \to \operatorname{im} \pi_A \cong \mathcal{O} \to 0$$

and

$$0 \to \ker \pi_U \to U \to \operatorname{im} \pi_U \cong \mathcal{O} \to 0$$

As both corresponding sequences split via the inclusion $\mathcal{O} \hookrightarrow A, x \mapsto x \cdot 1$ resp. $\mathcal{O} \hookrightarrow U$, we can write $U \cong \mathcal{O} \oplus \ker \pi_U$ and $A \cong \mathcal{O} \oplus \ker \pi_A$. $\Phi$ by definition induces an equality on the first component, a surjection on the second and therefore is surjective on the direct sum. □

**Remark 2.2.** *For a finite flat complete intersection $A \in \mathcal{C}^\bullet_\mathcal{O}$ we can choose the quotient*

$$U \xrightarrow{\alpha} U/(f_1, \dots, f_n) \cong A$$

*in such a way that the augmentation map $\pi_A$ is induced by*

$$\pi_U \colon \mathcal{O}[[X_1, \dots, X_n]] \to \mathcal{O}, \qquad f(X_1, \dots, X_n) \mapsto f(0, \dots, 0).$$

*Because $[f_i] = 0 \ \in A$, necessarily*

$$f_i(0) = \pi_U(f_i) = \pi_A(\Phi(f_i)) = \pi_A(0) = 0,$$

*i.e. the relations $f_i$ must not have a constant term.*

*Proof.* From remark 2.1 we know that we can express $A$ as a quotient of $U$,

$$A \cong \mathcal{O}[[X_1, \dots, X_n]]/(\ker \Phi).$$

Also By [Mat86, theorem 21.2] it follows that $\ker \Phi$ can be generated by $n$ elements. Hence we find $f_1, \dots, f_n$ s.t.

$$A \cong \mathcal{O}[[X_1, \dots, X_n]]/(f_1, \dots, f_n).$$

□

Note that whenever we write a complete intersection $A$ as a quotient of $U$, without loss of generality we can choose polynomials without constant term and assume that $\pi_A$ is induced by evaluation at 0 on $U$.

**Definition 2.3.** Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$. Then

$$\phi_A \coloneqq (\ker \pi_A)/(\ker \pi_A)^2.$$

The reader with background in algebraic geometry might notice that this can be thought of as a tangent space, in particular it is the cotangent space of the scheme spec$(A)$ at the point $\ker \pi_A$. However this point of view is not necessary in the following, it might be more a hint of how Wiles came to investigate this specific invariant.

**Example 2.3.** Remember the definition of $U$ in example 2.2. The tangent space $\phi_U = \ker \pi_U/(\ker \pi_U)^2$ is

$$\mathcal{O}X_1 \oplus \cdots \oplus \mathcal{O}X_n.$$

Indeed, elements of $f \in \ker \pi_U$ have no constant term as $f(0) = 0$ and therefore are multiples of $X$. Elements in $\ker \pi_U^2$ are multiples of $X^2$. As a result, we receive elements $\overline{f} \in \phi_U$ by cutting of all higher terms of a power series $f \in \ker \pi_U$.

**Remark 2.3.** *Write $A$ as a quotient of $U$, $A = U/(f_1, \ldots, f_m)$. This is possible because of remark 2.1. We then get $\phi_A = \phi_U/(\overline{f_1}, \ldots, \overline{f_m})$. As a quotient of $\phi_U$ its a finitely generated $\mathcal{O}$-module.*

*Proof.* Consider the following map of $\mathcal{O}$-modules

$$\begin{aligned} \Phi\colon \ker \pi_U &\to (\ker \pi_A)/(\ker \pi_A)^2 = \phi_A \\ f &\mapsto [f] \mod (\ker \pi_A)^2, \end{aligned}$$

where $[f]$ denotes the image of $f$ in $A$. Then, as $\pi_A([f]) = f(0)$, we get that $X_i \in \ker \pi_A \forall i$ and therefore $[f] \in \ker \pi_A \forall f \in \ker \pi_U$. Not only is $\Phi$ welldefined, we can conclude that $X_i \in \ker \pi_A \implies X_i^2 \in (\ker \pi_A)^2$ and therefore $\Phi$ is also surjective and $(\ker \pi_U)^2 \subset \ker \Phi$.

With this knowledge we get a welldefined surjective map

$$\begin{aligned} \tilde{\Phi}\colon \phi_U = \mathcal{O}X_1 \oplus \cdots \oplus \mathcal{O}X_n &\to \phi_A \\ a_1X_1 + \cdots + a_nX_n \mod (\ker \pi_U)^2 &\mapsto [a_1X_1 + \cdots + a_nX_n] \mod (\ker \pi_A)^2. \end{aligned}$$

Elements in the kernel of this map are either generated by $X_i^2$ s.t. they become $0 \mod (\ker \pi_A)^2$ or they become 0 by sending them to $A = U/(f_i)$. As higher order terms of $f_i$ are vanishing anyways, the kernel of $\tilde{\Phi}$ is generated by the $\overline{f_i}$, i.e.

$$\phi_A \cong \phi_U/(\overline{f_i})$$

□

**Example 2.4.** We now compute $\phi_A$ where $A$ was defined in example 2.1. Remember that $f = T(T - \lambda^n) = -\lambda^n T + T^2$. Therefore,

$$\phi_A = \mathcal{O}T/(-\lambda^n T) = \mathcal{O}/\lambda^n.$$

**Definition 2.4.** Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$. Then

$$\eta_A \coloneqq \pi_A(\mathrm{Ann}_A(\ker \pi_A))$$

is an ideal in $\mathcal{O}$.

**Example 2.5.** We now compute $\eta_U$ for $U$ from example 2.2.

$$\begin{aligned}\eta_U &= \pi_U(\mathrm{Ann}\ker \pi_U)\\ &= \pi_U(\mathrm{Ann}\,\mathcal{O}X_1 \oplus \cdots \oplus \mathcal{O}X_n)\\ &= \pi_U(0) = 0.\end{aligned}$$

**Lemma 2.1.** *Let $\mathfrak{a} \subset \mathcal{O}$ be an ideal. Then*

$$\mathfrak{a} \neq 0 \implies \mathcal{O}/\mathfrak{a} \textit{ finite.}$$

*Proof.* As $\mathcal{O}$ is a DVR, $\mathfrak{a} = \lambda^n$ for some $n \in \mathbb{N}$ where $\lambda$ is the maximal ideal in $\mathcal{O}$. Therefore, $\mathcal{O}/\mathfrak{a} = \mathcal{O}/\lambda^n$.

Using the fact that $\lambda = (t)$ for some uniformizer $t$, we get $\forall i \geq 1$ the isomorphism $\lambda^i/\lambda^{i+1} \cong \mathcal{O}/\lambda = k$ and thereby also the short exact sequence

$$0 \to \mathcal{O}/\lambda \cong \lambda^i/\lambda^{i+1} \to \mathcal{O}/\lambda^{i+1} \to \mathcal{O}/\lambda^i \to 0.$$

As $k = \mathcal{O}/\lambda$ is finite, we can use induction

$$\#\mathcal{O}/\lambda^{i+1} = \#\mathcal{O}/\lambda \cdot \#\mathcal{O}/\lambda^i = \#k \cdot (\#k)^i = (\#k)^{i+1}$$

and get $\#\mathcal{O}/\mathfrak{a} = \#\mathcal{O}/\lambda^n = (\#k)^n$. □

**Example 2.6.** We now compute $\eta_A$ for $A$ from example 2.1.

$$\begin{aligned}\eta_A &= \pi_A(\mathrm{Ann}\ker \pi_A)\\ &= \pi_A(\mathrm{Ann}\{(0,b) \subset \mathcal{O} \times \mathcal{O} | b \equiv 0 \mod \lambda^n\})\\ &= \pi_A(\{(a,0) \subset \mathcal{O} \times \mathcal{O} | a \equiv 0 \mod \lambda^n\})\\ &= \pi_A((\lambda^n) \times \mathcal{O})\\ &= (\lambda^n)\end{aligned}$$

With these results at hand, we can state

**Theorem 2.1.** [DDT95, theorem 5.3] *Let $R \twoheadrightarrow T$ a surjective morphism of augmented rings, $T$ finite flat and $\eta_T \neq 0$ (i.e. $\mathcal{O}/\eta_T$ finite). Then the following are equivalent*

*(a)* $\#\phi_R \leq \#(\mathcal{O}/\eta_T)$,

*(b)* $\#\phi_R = \#(\mathcal{O}/\eta_T)$,

*(c) $R$ and $T$ are complete intersections, and $R \to T$ is an isomorphism.*

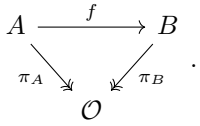
## 2.3 Basic properties of the invariants

In this subsection we prove the equivalence (a) $\Leftrightarrow$ (b) in theorem 2.1 by investigating the invariants $\phi_A$ and $\eta_A$ that we defined last section.

**Lemma 2.2.** *A morphism $f\colon A \to B \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ induces a homomorphism $\phi_A \to \phi_B$ of $\mathcal{O}$-modules. This induced map is surjective if and only if the morphism $A \to B$ is surjective.*

For the 'only if'-part, see [DDT95, lemma 5.5; Mat86, theorem 8.4; Har77, ch. II, lemma 7.4; Sta22, Tag 090T].

*Proof.* We have the commutative diagram




It follows from the diagram that the restriction of $f$ to $\ker\phi_A$ maps to $\ker\phi_B$, because $\forall x \in \ker\phi_A\colon\ \pi_B(f(x)) = \pi_A(x) = 0$. Concatenating this with the projection to the tangent space, we get a map

$$\tilde{f}\colon\ \ker\pi_A \to \ker\pi_B/(\ker\pi_B)^2 = \phi_B.$$

In order to see that $\tilde{f}\colon \phi_A \to \phi_B$ is welldefined, we need to show

$$f(\ker\pi_A)^2 \subset (\ker\pi_B)^2,$$

however this follows from the fact that $f(\ker\pi_A) \subset \ker\pi_B$ and that $f$ is an algebra homomorphism:

$$f(x^2) = \underbrace{f(x)}_{\in\ker\pi_B}\ \underbrace{f(x)}_{\in\ker\pi_B} \in (\ker\pi_B)^2$$

for any $x \in \ker\pi_A$.

First, let us assume that $A \to B$ is a surjective map. In this case, every element $x \in \ker\phi_B$ has a preimage in $\ker\pi_A$. Indeed, $\forall y \in f^{-1}(x) \subset A$:

$$\pi_A(y) = \pi_B(f(y)) = \pi_B(x) = 0.$$

As a result, the induced map $f\colon\ \ker\pi_A \to \ker\pi_B$ and its concatenation with the projection to $\phi_B$, $\tilde{f}\colon\ \ker\pi_A \to \ker\pi_B/(\ker\pi_B)^2$ are both surjective. In total, we obtain a surjective homomorphism $\tilde{f}\colon \phi_A \to \phi_B$.

Now, let the induced map $\phi_A \to \phi_B$ be surjective. Consider the ideal $I = f(\ker\pi_A)\cdot B$ in $B$. Let $x \in I$. Then $x = \sum_i f(x_i)\cdot b_i$ for $x_i \in \ker\pi_A$ and $b_i \in B$. Remember the commutative diagram from the beginning of the proof,

$$\pi_B(x) = \pi_B\left(\sum_i f(x_i)\cdot b_i\right) = \sum_i \pi_B(f(x_i))\cdot\pi_B(b_i) = \sum_i \pi_A(x_i)\cdot\pi_B(b_i) = 0.$$

As a result, $I \subset \ker \pi_B \subset \mathfrak{m}_B$. Note that

$$f(\ker \pi_A) \subset f(\ker \pi_A) \cdot B \implies f((\ker \pi_A)^n) = f(\ker \pi_A)^n \subset (f(\ker \pi_A) \cdot B)^n,$$

so we have $\phi((\ker \pi_A)^n) \cdot B \subset I^n$. As $B$ is $\mathfrak{m}_B$-adically complete and therefore Hausdorff, we get

$$\bigcap_{n \in \mathbb{N}} f((\ker \pi_A)^n) \cdot B \subset \bigcap_{n \in \mathbb{N}} I^n \subset \bigcap_{n \in \mathbb{N}} \mathfrak{m}_b^n = 0,$$

i.e. $B$ is separated with respect to the $I$-adic topology. Furthermore, $\ker \pi_A$ is finitely generated as an $A$-module, $\ker \pi_A = \langle a_1, \ldots, a_m \rangle$ because $A$ is noetherian. As $\ker \pi_A \to (\ker \pi_B)/(\ker \pi_B)^2$ is surjective, we have

$$(\ker \pi_B)/(\ker \pi_B)^2 = \langle \overline{f(a_1)}, \ldots, \overline{f(a_m)} \rangle_B.$$

As $A$ is $\mathfrak{m}_A$-adically complete, $\ker \pi_A$ is finitely generated over $A$ and $\ker \pi_A \subset \mathfrak{m}_A$, $A$ is $\ker \pi_A$-adically complete as well [cf. Sta22, lemma 10.96.8]. Furthermore, $I$ is separated with respect to the $I$-adic topology as a submodule of $B$. Together with the fact that $A$ is $\ker \pi_A$-adically complete, we can apply Nakayama's Lemma as in Mat, 8.4. It follows that the images $\langle f(a_1), \ldots, f(a_m) \rangle$ generate $\ker \pi_B$ as a $B$-module. We already know that $f(\ker \pi_A) \cdot B \subset \ker \pi_B$. In total we have

$$f(\ker \pi_A) \cdot B = \ker \pi_B.$$

Now we conclude that 1 is a generator of $B/I = B/f(\ker \pi_A)B = B/\ker \pi_B = \mathcal{O}$ as an $A/\ker \pi_A \cong \mathcal{O}$-module. Applying Nakayama's Lemma again, we get that 1 is a generator of $B$ as an $A$-module and hence, $f\colon A \to B$ is surjective. □

**Corollary 2.1.** *Let $A, B \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ and $\phi_A$ be finite. Then $\phi_B$ is finite as well and $A \to B$ is surjective if and only if*

$$\#\phi_A \geq \#\phi_B.$$

**Lemma 2.3.** *If $f\colon A \to B$ is surjective, then*

$$\eta_A \subset \eta_B, \quad \textit{i.e. if } \eta_A \neq 0, \quad \#(\mathcal{O}/\eta_A) \geq \#(\mathcal{O}/\eta_B). \tag{1}$$

*Proof.* As we have seen in the proof of lemma 2.2, a surjective map $f$ induces a surjective map on the kernels, $f\colon \ker \pi_A \to \ker \pi_B$. Now let $x \in \operatorname{Ann}_A \ker \pi_A$, i.e. $x \cdot a = 0 \ \ \forall a \in \ker \pi_A$. For all $b \in \ker \pi_B$ and any preimage $a \in \ker \pi_A$ we have

$$f(x) \cdot b = f(x) \cdot f(a) = f(x \cdot a) = f(0) = 0.$$

As a result, $f(x) \in \operatorname{Ann}_B \ker \pi_B$ and we obtain a map

$$\tilde{f}\colon \operatorname{Ann}_A \ker \pi_A \to \operatorname{Ann}_B \ker \pi_B.$$

In order to show $\eta_A \subset \eta_B$, let $x \in \eta_A = \pi_A(\operatorname{Ann}_A \ker \pi_A)$, i.e. $x = \pi_A(y)$ for some $y \in \operatorname{Ann}_A \ker \pi_A$. By the commutative diagram

$$\begin{array}{ccc} \operatorname{Ann}_A \ker \pi_A & \xrightarrow{\tilde{f}} & \operatorname{Ann}_B \ker \pi_B \\ & {\scriptstyle \pi_A} \searrow \quad \swarrow {\scriptstyle \pi_B} & \\ & \mathcal{O} & \end{array},$$

we get

$$x = \pi_A(y) = \pi_B(\tilde{f}(y)) \in \pi_B(\operatorname{Ann}_B \ker \pi_B) \implies x \in \eta_B,$$

as desired. □

**Definition 2.5.** Let $M$ be a finitely generated $R$-module. Then $M$ is a quotient

$$P \colon R^n \longrightarrow M = R^n / \ker P$$

We define $\operatorname{Fitt}_R(M) \coloneqq \langle \det(v_1, \dots, v_n) | v_i \in \ker P \rangle_R \subset R$. This is independent of the choice of the surjection (see e.g. stacks project).

**Lemma 2.4.** *For a finitely generated $R$-module $M$ we have*

$$\operatorname{Fitt}_R(M) \subset \operatorname{Ann}_R(M).$$

*Proof.* $M$ is generated by $\overline{e_1}, \dots, \overline{e_n}$ where $\overline{x}$ may denote the residue class of $x$ mod $\ker P$. Now let $[v_1 | \dots | v_n]$ be a matrix with $v_i \in \ker P$. Then this matrix annihilates $M$ because it annihilates all the generators $\overline{e_i}$,

$$[v_1 | \dots | v_n] \cdot e_i = v_i \in \ker P.$$

Let $A$ be the adjugate matrix of $[v_1 | \dots | v_n]$, i.e.

$$A[v_1 | \dots | v_n] = \det[v_1 | \dots | v_n] \cdot I_{n \times n}.$$

Let $m \in M$ and $(m_i)_{i=1}^n$ a lift in $R^n$. Then we have

$$\begin{aligned} \det[v_1 | \dots | v_n] \cdot m &= \det[v_1 | \dots | v_n] \cdot I_{n \times n} (m_i)_{i=1}^n \\ &= A[v_1 | \dots | v_n] \left( \sum_{i=1}^n m_i e_i \right) \\ &= A \cdot \sum_{i=1}^n m_i v_i \in A \cdot \ker P \subset \ker P \end{aligned}$$

Therefore $\operatorname{Fitt}_R(M) \subset \operatorname{Ann}_R(M)$. □

**Remark 2.4** (Fitting ideals and $\otimes$)**.** *Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ and $M$ a finitely generated $A$-module. Note that $\mathcal{O}$ has an $A$-module structure via $\pi_A$. We have*

$$\pi_A(\operatorname{Fitt}_A(M)) = \operatorname{Fitt}_{\mathcal{O}}(M \otimes_A \mathcal{O}).$$

*This follows from the fact that $- \otimes_A \mathcal{O}$ is right exact. Hence, from the exact sequence*

$$\ker P \longrightarrow A^n \longrightarrow M \longrightarrow 0$$

*we get the exact sequence*

$$\ker P \otimes_A \mathcal{O} \longrightarrow A^n \otimes_A \mathcal{O} = \mathcal{O}^n \longrightarrow M \otimes_A \mathcal{O} \longrightarrow 0.$$

*The remaining details are left as an exercise to the reader.*

**Remark 2.5** (Fitting ideals for finitely generated $O$-modules)**.** *Let $M$ be a finitely generated $O$-module. As $O$ is a PID, there are unique $r, s \in \mathbb{N}$ and $n_1 \geq \cdots \geq n_s \in \mathbb{N}$ s.t.*

$$M = \mathcal{O}^r \oplus \mathcal{O}/\lambda^{n_1} \oplus \cdots \oplus \mathcal{O}/\lambda^{n_s}.$$

*If $r > 0$ then every $v \in \ker P \subset \mathcal{O}^{r+s}$ has $r$ zero components. Therefore, $\mathrm{Fitt}_R(M) = 0$ for $r > 0$. If $r = 0$ the $i$-th component of $v \in \ker P \subset \mathcal{O}^s$ lies in the kernel of $\mathcal{O} \to \mathcal{O}/\lambda^{n_i}$, i.e. $v_i \in \lambda^{n_i}$. Using the Leibniz formula for computing the determinant, we get $\mathrm{Fitt}_{\mathcal{O}}(M) = \lambda^{n_1} \cdot \cdots \cdot \lambda^{n_s} = \lambda^{n_1+\cdots+n_s}$.*

**Corollary 2.2.** *Let $M$ be a finite $\mathcal{O}$-module. Then*

$$\#M = \#(\mathcal{O}/\operatorname{Fitt}_{\mathcal{O}}(M)).$$

*Proof.* As $M$ is finite, we get

$$M = \mathcal{O}/\lambda^{n_1} \oplus \cdots \oplus \mathcal{O}/\lambda^{n_s}$$

and

$$\mathrm{Fitt}_{\mathcal{O}}(M) = \lambda^{n_1+\cdots+n_s}.$$

From the proof of lemma 2.1 it follows that

$$\#M = (\#k)^{n_1} \cdot \cdots \cdot (\#k)^{n_s} = (\#k)^{n_1+\cdots+n_s}$$

and

$$\#(\mathcal{O}/\operatorname{Fitt}_{\mathcal{O}}(M)) = \#(\mathcal{O}/\lambda^{n_1+\cdots+n_s}) = (\#k)^{n_1+\cdots+n_s}.$$

□

**Lemma 2.5.** *Let $A \in \mathcal{C}_{\mathcal{O}}$ s.t. $\phi_A$ finite and $\eta_A \neq 0$. Then*

$$\#\phi_A \geq \#(\mathcal{O}/\eta_A).$$

*Proof.* As $\mathcal{O} = A/\ker \pi_A$, we have

$$\ker \pi_A \otimes_A \mathcal{O} = \ker \pi_A \otimes_A A/\ker \pi_A \cong \ker \pi_A/(\ker \pi_A) \ker \pi_A = \phi_A.$$

We therefore have

$$\mathrm{Fitt}_{\mathcal{O}}(\phi_A) = \mathrm{Fitt}_{\mathcal{O}}(\ker \pi_A \otimes_A \mathcal{O}) = \pi_A(\mathrm{Fitt}_A(\ker \pi_A))$$

where the second equality follows from remark 2.4. Applying lemma 2.4 to the RHS, we get

$$\mathrm{Fitt}_{\mathcal{O}}(\phi_A) \subset \pi_A(\mathrm{Ann}_A(\ker \pi_A)) = \eta_A.$$

As $\phi_A$ is finite, we can apply corollary 2.2 to $M = \phi_A$ and obtain

$$\#\phi_A = \#(\mathcal{O}/\mathrm{Fitt}_{\mathcal{O}}(\phi_A)) \geq \#(\mathcal{O}/\eta_A).$$

□

**Proposition 2.1.** [cf. DDT95, corollary 5.6] *(a) ⇔ (b) in theorem 2.1.*

*Proof.* By assumption, $R \to T$ is a surjective morphism in $\mathcal{C}_{\mathcal{O}}^{\bullet}$. With corollary 2.1 it follows that $\#\phi_R \geq \#\phi_T$. Lemma 2.5 tells us that $\#\phi_T \geq \#(\mathcal{O}/\eta_T)$. The inequalities combine to

$$\#\phi_R \geq \#(\mathcal{O}/\eta_T).$$

In both cases the finiteness of $\mathcal{O}/\eta_T$ implies the finiteness of $\phi_R$ and from that we obtain the finiteness of $\#\phi_T$.

(a) $\Longrightarrow$ (b) (a) gives us $\#\phi_R \leq \#(\mathcal{O}/\eta_T)$, so combined with the inequality $\#\phi_R \geq \#(\mathcal{O}/\eta_T)$ we have just proven we conclude that (b) must hold.

(b) $\Longrightarrow$ (a) Obvious.

□

## 2.4 Regular sequences and the Koszul complex

Let $A$ be a finite flat complete intersection. Hence we can write

$$A = \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n).$$

The goal of this section is to prove some technical lemmata and to introduce the Koszul complex that we will use to construct two $\mathcal{O}[[X]]$-free resolutions for $A$. This will turn out to be crucial in the next section.

We start with a few definitions from commutative algebra, closely following [DDT95, sec. 5.3]

**Definition 2.6** (primary ideal)**.** Let $R$ be a local ring and $\mathfrak{a} \subsetneq R$ an ideal. $\mathfrak{a}$ is said to be primary if every zero divisor in $R/\mathfrak{a}$ is nilpotent.

Recall that the dimension of a ring is given by

$$\sup\{n | \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq R,\ \mathfrak{p}_i \text{ prime}\}.$$

**Definition 2.7** (system of parameters)**.** Let $x_1, \ldots, x_n$ generate a primary ideal of $R$. If $n = \dim R$ then $x_1, \ldots, x_n$ is called a system of parameters.

**Lemma 2.6.** [DDT95, lemma 5.10] *The sequence $(f_1, \ldots, f_n, \lambda)$ is a system of parameters for $U$ (cf. example 2.2).*

*Proof.* First, we show that $\dim U = n+1$. We have an ascending chain of prime ideals

$$(0) \subsetneq (\lambda) \subsetneq \cdots \subsetneq (\lambda, X_1, \ldots, X_n),$$

so by definition of the dimension we get $\dim U \geq n+1$. Let $\mathfrak{m} = (\lambda, X_1, \ldots, X_n)$. We have seen that this is the maximal ideal in $U$. Now we can conclude

$$\dim U \leq \dim_{U/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\lambda/\lambda^2 \oplus kX_1 \oplus \cdots \oplus kX_n).$$

As $\lambda/\lambda^2 \cong k$ (cf. lemma 2.1), the above expression evaluates to $n+1$ and taking both inequalities together we obtain $\dim U = n+1$. It remains to show that $(f_1, \ldots, f_n, \lambda)$ generate a primary ideal of $U$. $U$ is local and therefore the quotient ring

$$\tilde{U} \coloneqq U/(f_1, \ldots, f_n, \lambda)$$

is local as well. Also, $\tilde{U}$ is a $k$-vector space (because it's an $\mathcal{O}$-module and $\lambda$-operation annihilates it). As $A = U/(f_1, \ldots, f_n)$ is a finitely generated $\mathcal{O}$-module, we can find $(x_1, \ldots, x_N)$ that generate $A$ as $\mathcal{O}$-module. These $x_i$ then generate $\tilde{U}$ as a $k$-vector space. As $k$ is finite, the whole vector space is finite. As a result, the chain of powers of $\mathfrak{m}_{\tilde{U}}$ must stabilize,

$$\mathfrak{m}_{\tilde{U}}^n = \mathfrak{m}_{\tilde{U}}^{n+1}$$

By Nakayama's lemma it follows that $\mathfrak{m}_{\tilde{U}}^n = 0$. As a result, every element of the maximal ideal is nilpotent. Zero-divisors are never units. Hence they are contained in the maximal ideal and, a fortiori, nilpotent. In total, $f_1, \ldots, f_n, \lambda$ generate a primary ideal of $U$. □

**Definition 2.8** (regular sequence)**.** [cf. Mat86, §16] A sequence $(x_1, \ldots, x_n)$ is said to be a regular sequence if $\forall\, i = 1, \ldots, n$:

$$x_i \text{ is not a zero-divisor in } R/(x_1, \ldots, x_{i-1}).$$

**Lemma 2.7.** [DDT95, lemma 5.11] *The sequence $(f_1, \ldots, f_n)$ is a regular sequence for $U$.*

*Proof.* The sequence $(\lambda, X_1, \ldots, X_n)$ is a regular sequence for $U$ because $U/\lambda = k[[X_1, \ldots, X_n]]$ and $U/(\lambda, X_1, \ldots, X_{i-1}) = k[[X_i, \ldots, X_n]]$ are integral domains (hence obviously $X_i$ can't be a zero-divisor in these rings). As we have seen in the previous lemma, it's as well a system of parameters. Therefore, the depth of $U$ (i.e. the maximal lenth of any regular sequence in $U$) is bigger than the length of the particular regular sequence $(\lambda, X_1, \ldots, X_n)$. In total we get $\operatorname{depth} U \geq \dim U$, because $(\lambda, X_1, \ldots, X_n)$ is a system of parameters as well. In general, we have $\operatorname{depth} R \leq \dim R$ for a noetherian local ring $R$, so combined we have

$$\operatorname{depth} U = \dim U$$

and hence, $U$ is Cohen-Macaulay. As $(f_1, \ldots, f_n, \lambda)$ is a system of parameters and $U$ is Cohen-Macaulay it follows by [Matsumura, Theorem 17.4] that $(f_1, \ldots, f_n, \lambda)$ is a regular sequence. A fortiori, the sequence $(f_1, \ldots, f_n)$ is also a regular sequence. □

**Corollary 2.3.** [DDT95, corollary 5.12] *Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ be finitely generated and of the form*

$$A \cong \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n).$$

*Then $A$ is flat.*

*Proof.* Assume that $A$ is not flat, i.e. there is a $\lambda^n u \in \mathcal{O}$ and a

$$0 \neq g(X_1, \ldots, X_n) \in A \qquad \text{s.t. } \lambda^m u \cdot g(\underline{X}) = 0.$$

Consider $g' = \lambda^{m-1} u g$. Either $g' \neq 0$ s.t. $\lambda \cdot g' = 0$ with $g' \neq 0$ or $g' = 0 \in A$. Then repeat the last step with $g'$ instead of $g$. After finitely many steps we find a $0 \neq g \in A$ s.t. $\lambda g = 0$, i.e.

$$\lambda \cdot g(\underline{X}) = c_1(\underline{X}) f_1(\underline{X}) + \cdots + c_n(\underline{X}) f_n(\underline{X}).$$

Without loss of generality we can choose the $c_i(\underline{X})$ in such a way that $c_i(\underline{X})$ is never divisible by any of the $f_j(\underline{X})$ for $j < i$. (In such a case one would have to add a suitable multiple of $f_i$ to $c_j$.) Furthermore, $\exists i \colon\ 0 \neq c_i \mod \lambda$. Otherwise we could divide the whole equation by $\lambda$ and obtain $g = 0 \mod (f_1, \ldots, f_n)$, a contradiction. Let $i_0$ be the biggest such $i$. In the proof of lemma 2.6 we have never used that $A$ is flat, only that it is finitely generated. Therefore we know that $\lambda, f_1, \ldots, f_n$ is a system of parameters for $U$. From the proof of lemma 2.7 (where we also haven't used that $A$ is flat) we can deduce that $\lambda, f_1, \ldots, f_n$ is also a regular sequence for $U$ and, a fortiori, $f_{i_0}$ is not a zero-divisor in $U/(\lambda, f_1, \ldots, f_{i_0-1})$. If we consider the equation

$$\lambda \cdot g(\underline{X}) = c_1(\underline{X}) f_1(\underline{X}) + \cdots + c_n(\underline{X}) f_n(\underline{X}).$$

mod $(\lambda, f_1, \ldots, f_{i_0-1})$ we obtain

$$0 = 0 + c_{i_0} f_{i_0} + 0,$$

as all other terms are in the ideal $(\lambda, f_1, \ldots, f_{i_0-1})$. We know that $c_{i_0}$ is not divisible by any of $\lambda, f_1, \ldots, f_{i_0}$. Therefore $f_{i_0}$ is a zero-divisor in $U/(\lambda, f_1, \ldots, f_{i_0-1})$. This is a contradiction, so our assumption must be false. □

**Definition 2.9** (Koszul complex)**.** [DDT95, ch. 5.3; Mat86, §16] The Koszul complex associated to a sequence $\underline{x} = (x_1, \ldots, x_n)$ contained in the maximal ideal of a local ring is given by the complex

$$0 \to K_n(\underline{x}, R) \xrightarrow{d_n} K_{n-1}(\underline{x}, R) \to \cdots \to K_0(\underline{x}, R) \to 0,$$

where

$$K_p(\underline{x}, R) \coloneqq \bigoplus_{i_1 < \cdots < i_p} R \cdot u_{i_1} \wedge \cdots \wedge u_{i_p}$$

for symbols $u_1, \ldots, u_n$. The differential map $d_p \colon K_p(\underline{x}, R) \to K_{p-1}(\underline{x}, R)$ is given by

$$d_p(u_{i_1} \wedge \cdots \wedge u_{i_p}) = \sum_{t=1}^{p} (-1)^t x_{i_t} \cdot u_{i_1} \wedge \cdots \wedge \widehat{u_{i_t}} \wedge \cdots \wedge u_{i_p}.$$

As usual, we denote by $H_p(\underline{x}, R)$ the $p$-th homology group of this complex.

**Remark 2.6.** [DDT95, proposition 5.13; Mat86, theorem 16.5 (i)] *We note* $K_0(\underline{x}, R) = R$ *and therfore compute*

$$H_0(\underline{x}, R) = K_0(\underline{x}, R)/(\operatorname{im} d_1) \cong R/(x_1, \ldots, x_n) = R/(\underline{x}).$$

*Furthermore, one can show that if* $(\underline{x})$ *is a regular sequence, then the complex is exact. As it consists of free* $R$*-modules, homological algebra shows that we then get a resolution of* $H_0(\underline{x}, R) = R/(\underline{x})$ *by free* $R$*-modules.*

## 2.5 Complete intersections and Gorenstein rings

Let $A$ be a finite flat complete intersection in $\mathcal{C}_{\mathcal{O}}^{\bullet}$. The goal of this section is to show that $A$ satisfies a Gorenstein condition, i.e. a specific form of self-duality. This fact can then be used to show (c) $\implies$ (b) in theorem 2.1. Although there is a very general notion of Gorenstein rings, for the purpose of this proof we only need a special case,

**Definition 2.10.** Let $A \in \mathcal{C}_{\mathcal{O}}$ be finite flat. $A$ is called Gorenstein, if there is an isomorphism of $A$-modules

$$\Psi\colon \operatorname{Hom}_{\mathcal{O}}(A, \mathcal{O}) \cong A.$$

Our goal therefore reduces to constructing an $A$-module isomorphism

$$\operatorname{Hom}_{\mathcal{O}}(A, \mathcal{O}) \to A.$$

We start with some useful constructions and conventions.

*Notation.* For any ring $R$ write $R[[\underline{X}]] \coloneqq R[[X_1, \ldots, X_n]]$.

Let $a_1, \ldots, a_n$ be the images in $A$ of $X_1, \ldots, X_n$ by the natural map

$$\alpha\colon \mathcal{O}[[\underline{X}]] \to A = \mathcal{O}[[\underline{X}]]/(f_1, \ldots, f_n),$$

and let

$$\beta\colon A[[\underline{X}]] \to A$$

be the natural map which sends $X_i$ to $a_i$. A polynomial $f \in A[[\underline{X}]]$ is sent to 0 exactly when $f(a_1, \ldots, a_n) = 0$. Therefore, $\exists i\colon\ (X_i - a_i) | f$ and hence, the sequence $g_i = (X_i - a_i)$ generates the kernel of $\beta$. View the $f_i$ as polynomials in $A[[\underline{X}]]$ via the inclusion $O \hookrightarrow A$. Then $\forall i = 1, \ldots, n\colon$

$$\beta(f_i) = f_i(a_1, \ldots, a_n) = 0 \in \mathcal{O}[[\underline{X}]]/(f_1, \ldots, f_n).$$

Therefore every of the $f_i$ is element of $\ker \beta$ and hence can be written as an $A[[X]]$-linear combination of the $g_i$,

$$(f_1, \ldots, f_n) = (g_1, \ldots, g_n)M,$$

where $M$ is an $n \times n$ matrix with coefficients in $A[[\underline{X}]]$. Let $D = \det(M) \in A[[\underline{X}]]$. The projection $\mathcal{O}[[\underline{X}]] \to A$ induces an $\mathcal{O}[[\underline{X}]]$-module structure on $A$.

**Lemma 2.8.** [see DDT95, lemma 5.14] *The map*

$$\Phi\colon \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(A[[\underline{X}]], \mathcal{O}[[\underline{x}]]) \to A \qquad f \mapsto \alpha(f(D))$$

*is an $\mathcal{O}[[\underline{X}]]$-linear surjection.*

*Proof.* As shown in lemma 2.7, $(\underline{f}) = (f_1, \ldots, f_n)$ is a regular sequence for $\mathcal{O}[[\underline{X}]]$. In the ring $A[[\underline{X}]]/(X_1 - a_1, \ldots, X_{i-1} - a_{i-1})$, there are no relations in $X_i$, i.e. it can be written as $R[X_i]$ for a ring $R$. Therefore $(X_i - a_i)$ can't be a zero-divisor. As this holds for all $i = 1, \ldots, n$, $(\underline{g}) = (g_i) = (X_i - a_i)$ is a regular sequence for $A[[\underline{X}]]$.

Let now $K(\underline{f}, \mathcal{O}[[\underline{X}]])$ and $K(\underline{g}, A[[\underline{X}]])$ be the associated Koszul complexes. We have that $K(\underline{f}, \mathcal{O}[[\underline{X}]])$ is a resolution of

$$A = H_0(\underline{f}, \mathcal{O}[[\underline{X}]]) = \mathcal{O}[[\underline{X}]]/(f_1, \ldots, f_n)$$

by free $\mathcal{O}[[\underline{X}]]$-modules and analogous that $K(\underline{g}, A[[\underline{X}]])$ is a resolution of

$$A = H_0(\underline{g}, A[[\underline{X}]]) = A[[\underline{X}]]/(X_1 - a_1, \ldots, X_n - a_n)$$

by free $A[[\underline{X}]]$-modules. Every free $A[[\underline{X}]]$-module has a canonical $\mathcal{O}[[\underline{X}]]$-module structure (take the canonical inclusion $\mathcal{O} \hookrightarrow A, x \mapsto x \cdot 1$ and extend it to a map $\mathcal{O}[[\underline{X}]] \hookrightarrow A[[\underline{X}]]$).

In the following, we want to construct a map of complexes

$$\Phi\colon K(\underline{f}, \mathcal{O}[[\underline{X}]]) \to K(\underline{g}, A[[\underline{X}]]).$$

On the 0-th level, we define

$$\phi_0\colon K_0(\underline{f}, \mathcal{O}[[\underline{X}]]) = \mathcal{O}[[\underline{X}]] \to K_0(\underline{g}, A[[\underline{X}]]) = A[[\underline{X}]]$$

to be just the canonical inclusion $\mathcal{O}[[\underline{X}]] \hookrightarrow A[[\underline{X}]]$ as explained above. On the first level, let

$$\Phi_1\colon K_1(\underline{f}, \mathcal{O}[[\underline{X}]]) = \bigoplus_{i=1}^{n} R \cdot u_i \to K_1(\underline{g}, A[[\underline{X}]]) = \bigoplus_{i=1}^{n} R \cdot v_i$$

be the map defined by

$$(\Phi_1(u_1), \ldots, \Phi_1(u_n)) = (v_1, \ldots, v_n)M.$$

By skew-linearity this can be extended to a map of exterior algebras. In the following we proof that $\Phi$

1. is a morphism of complexes,
2. induces the identity on $A = H_0(\underline{f}, \mathcal{O}[[\underline{X}]])$

3. and satisfies
$$\Phi_n(u_1 \wedge \cdots \wedge u_n) = D \cdot v_1 \wedge \cdots \wedge v_n.$$

1. $\Phi$ **is a morphism of complexes.** It is clear by definition that $\Phi$ is welldefined on every level. We have to show that $\Phi$ commutes with the differentials of the complex,
$$\begin{aligned}\Phi_{p-1}(d(u_{i_1}\wedge\ldots\wedge u_{i_p})) &= \Phi_{p-1}\left(\sum_{t=1}^{p}(-1)^t x_{i_t} u_{i_1}\wedge\ldots\wedge\widehat{u_{i_t}}\wedge\ldots\wedge u_{i_p}\right)\\ &= \sum_{t=1}^{p}(-1)^t x_{i_t}\Phi_1(u_{i_1})\wedge\ldots\wedge\widehat{\Phi_1(u_{i_t})}\wedge\ldots\wedge\Phi_1(u_{i_p})\\ &= d(\Phi_1(u_{i_1})\wedge\cdots\wedge\Phi_1(u_{i_p}))\\ &= d(\Phi_p(u_{i_1}\wedge\cdots\wedge u_{i_p})).\end{aligned}$$

2. $\Phi$ **induces the identity on** $A = H_0(\underline{f}, \mathcal{O}[[\underline{X}]])$
We have the following commutative diagram
$$\begin{array}{ccccccc}\bigoplus_{i=1}^n u_i\mathcal{O}[[\underline{X}]] = K_1(\underline{f},\mathcal{O}[[\underline{X}]]) & \xrightarrow{d_1} & K_0(\underline{f},\mathcal{O}[[\underline{X}]]) = \mathcal{O}[[\underline{X}]] & \xrightarrow{d_0} & 0\\ \downarrow{\scriptstyle\Phi_1} & & \downarrow{\scriptstyle\Phi_0} & & \\ \bigoplus_{i=1}^n v_i A[[\underline{X}]] = K_1(\underline{g},A[[\underline{X}]]) & \xrightarrow{d_1} & K_0(\underline{g},A[[\underline{X}]]) = A[[\underline{X}]] & \xrightarrow{d_0} & 0\end{array}.$$
As
$$H_0(\underline{f},\mathcal{O}[[\underline{X}]]) = \frac{\ker d_0}{\operatorname{im} d_1} = \frac{\mathcal{O}[[\underline{X}]]}{(f_1,\ldots,f_n)}$$
and
$$H_0(\underline{g},A[[\underline{X}]]) = \frac{\ker d_0}{\operatorname{im} d_1} = \frac{A[[\underline{X}]]}{(g_1,\ldots,g_n)}$$
we can take a look at the map
$$\mathcal{O}[[\underline{X}]] \to \frac{A[[\underline{X}]]}{(X_1-a_1,\ldots,X_n-a_n)} = A.$$
This map sends $X_i$ to $a_i \in A$. By definition of $A = \mathcal{O}[[\underline{X}]]/(f_1,\ldots,f_n)$ and $a_i$ as image of $X_i$ under $\alpha$ this is exactly the map $\alpha$. Hence, the induced map
$$A = \mathcal{O}[[\underline{X}]]/(f_1,\ldots,f_n) \to \frac{A[[\underline{X}]]}{(X_1-a_1,\ldots,X_n-a_n)} = A$$
is identity.

3. Let $M = (M_{i,j})_{i,j}$. Then we have

$$\begin{aligned}\Phi_n(u_1 \wedge \cdots \wedge u_n) &= \Phi(u_1) \wedge \cdots \wedge \Phi(u_n) \\ &= \sum_{j=1}^{n} v_j M_{j,1} \wedge \cdots \wedge \sum_{j=1}^{n} v_j M_{j,n} \\ &= \underbrace{\sum_{\sigma \in \mathfrak{S}(n)} (-1)^{\operatorname{sgn}(\sigma)} \prod_{i=1}^{n} M_{i,\sigma(i)}}_{=\det M} \cdot v_1 \wedge \cdots \wedge v_n \\ &= D \cdot v_1 \wedge \cdots \wedge v_n,\end{aligned}$$

where $\mathfrak{S}(n)$ may denote the group of permutations.

In the following we write $K_\bullet(\underline{f}) = K_\bullet(\underline{f}, \mathcal{O}[[\underline{X}]])$ and $K_\bullet(\underline{g}) = K_\bullet(\underline{g}, A[[\underline{X}]])$ By applying the functor $\operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(-, \mathcal{O}[[\underline{X}]])$ to the two free resolutions, we get the following commutative diagram

$$\begin{array}{ccccccc} \xrightarrow{d_{n-1}^*} & \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_{n-1}(\underline{f}), \mathcal{O}[[\underline{X}]]) & \xrightarrow{d_n^*} & \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{f}), \mathcal{O}[[\underline{X}]]) & \longrightarrow & 0 \\ & \uparrow{\scriptstyle \Phi_{n-1}^*} & & \uparrow{\scriptstyle \Phi_n^*} & & \\ \xrightarrow{d_{n-1}^*} & \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_{n-1}(\underline{g}), \mathcal{O}[[\underline{X}]]) & \xrightarrow{d_n^*} & \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{g}), \mathcal{O}[[\underline{X}]]) & \longrightarrow & 0 \end{array}.$$

As both resolutions are free and, a fortiori, projective we can use the fact from homological algebra that there exists a homotopy equivalence that induces identity on the zero-th homology groups. Consider the following commutative diagram with exact rows

$$\begin{array}{ccccccc} \bigoplus_{i=1}^n u_i \mathcal{O}[[\underline{X}]] & \xrightarrow{d_1} & \mathcal{O}[[\underline{X}]] & \xrightarrow{\alpha} & A & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ \bigoplus_{i=1}^n v_i A[[\underline{X}]] & \xrightarrow{d_1} & A[[\underline{X}]] & \xrightarrow{X_i \mapsto a_i} & A & \longrightarrow & 0 \end{array}.$$

From projectiveness we can conclude that there is a lift of the map $\mathrm{id} \circ \alpha$ to a map $\mathcal{O}[[\underline{X}]] \to A[[\underline{X}]]$ along the map $X_i \mapsto a_i$. As both maps send $X_i \mapsto a_i$, our lift is given by $X_i \mapsto X_i$, i.e. it is exactly $\Phi_0$. By commutativity, $(f_1, \ldots, f_n) = \operatorname{im} d_1 = \ker \alpha$ maps to the kernel of $X_i \mapsto a_i$. Therefore, we can lift the map $\Phi_0 \circ d_1$ along the surjective map

$$d_1 \colon \bigoplus_{i=1}^{n} v_i A[[\underline{X}]] \to \operatorname{im} d_1 = \ker(X_i \mapsto a_i) = (g_1, \ldots, g_n).$$

Using $(f_1, \dots, f_n) = (g_1, \dots, g_n)M$, we obtain for the induced map $f$

$$\begin{aligned} d_1(f(u_i)) = \Phi_0(d_1(u_i)) = \Phi_0(-f_i) &= -\sum_{j=1}^{n} g_j m_{ji} \\ &= \sum_{j=1}^{n} d_1(v_j) m_{j_i} = d_1\left(\sum_{j=1}^{n} v_j m_j\right). \end{aligned}$$

We note that $f = \Phi_1$. As the higher maps are then uniquely defined by skew linearity, we get that $\Phi$ needs to be a homotopy equivalence. Hence, we have an isomorphism on the $n$-th cohomology,

$$\Phi_n^* \colon \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{g}), \mathcal{O}[[\underline{X}]])/(\operatorname{im} d_n^*) \to \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{f}), \mathcal{O}[[\underline{X}]])/(\operatorname{im} d_n^*).$$

We know that

$$\begin{aligned} K_n(\underline{f}) &= \bigoplus_{i=1}^{n} \mathcal{O}[[\underline{X}]] \cdot u_1 \wedge \cdots \wedge u_n \cong \mathcal{O}[[\underline{X}]] \qquad \text{and} \\ K_n(\underline{g}) &= \bigoplus_{i=1}^{n} A[[\underline{X}]] \cdot u_1 \wedge \cdots \wedge u_n \cong A[[\underline{X}]]. \end{aligned}$$

Therefore, we can make the identification

$$\operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{f}), \mathcal{O}[[\underline{X}]]) \cong \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(\mathcal{O}[[\underline{X}]], \mathcal{O}[[\underline{X}]]) \cong \mathcal{O}[[\underline{X}]],$$

where the second isomorphism sends $f \mapsto f(1)$. The lift of 1 under the first isomorphism is $u_1 \wedge \cdots \wedge u_n$. Hence in total we send a map $f$ to $f(u_1 \wedge \cdots \wedge u_n)$. As a next step, we compute the image of $d_n^*$ in $\mathcal{O}[[\underline{X}]]$. Let $\varphi \in \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_{n-1}(\underline{f}), \mathcal{O}[[\underline{X}]])$. Then we have

$$d_n^*(\varphi) = \varphi \circ d_n \colon K_n(\underline{f}) \xrightarrow{d_n} K_{n-1}(g) \xrightarrow{\varphi} \mathcal{O}[[\underline{X}]],$$

where the composition is given by

$$\varphi(d_n(u_1 \wedge \cdots \wedge u_n)) = \sum_{t=1}^{n} (-1)^t f_t \varphi(v_1 \wedge \cdots \wedge \widehat{v_t} \wedge \cdots \wedge v_n),$$

as $\varphi$ is $\mathcal{O}[[\underline{X}]]$-linear. By our identification we then send the whole map to

$$\varphi \circ d_n(u_1 \wedge \cdots \wedge u_n) = \sum_{t=1}^{n} (-1)^t f_t \varphi(v_1 \wedge \cdots \wedge \widehat{v_t} \wedge \cdots \wedge v_n) \in \mathcal{O}[[\underline{X}]].$$

The image of $d_n^*$ is therefore generated by the $f_t$ and we get

$$\operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{f}), \mathcal{O}[[\underline{X}]])/(\operatorname{im} d_n^*) \cong \mathcal{O}[[\underline{X}]]/(f_1, \dots, f_n) = A.$$

As a result, $\Phi_n^*$ induces a $\mathcal{O}[[\underline{X}]]$-linear surjection

$$\Phi\colon \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(A[[\underline{X}]], \mathcal{O}[[\underline{X}]]) \cong \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(K_n(\underline{g}), \mathcal{O}[[\underline{X}]]) \twoheadrightarrow A.$$

$\Phi$ takes a $\mathcal{O}[[\underline{X}]]$-linear map and applies $\Phi_n^*$ to $f$, resulting in

$$f \circ \Phi_n\colon \mathcal{O}[[\underline{X}]] \xrightarrow{\Phi_n} K_n(g) \xrightarrow{f} \mathcal{O}[[\underline{X}]].$$

After that it uses our previous identification $\operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(\mathcal{O}[[\underline{X}]], \mathcal{O}[[\underline{X}]]) \cong \mathcal{O}[[\underline{X}]]$ and sends $f \circ \Phi_n$ to its value on 1. Using the identifications $K_n(\underline{f}) \cong \mathcal{O}[[\underline{X}]]$ and $K_n(\underline{g}) \cong A[[\underline{X}]]$, we obtain

$$f \circ \Phi_n(1) = f \circ \Phi_n(u_1 \wedge \cdots \wedge u_n) = f(D \cdot v_1 \wedge \cdots \wedge v_n) = f(D).$$

Finally we have to take the residue class $\bmod (f_1, \ldots, f_n)$. That is done by applying the projection map $\alpha$. In total we get

$$\Phi(f) = \alpha(f(D)),$$

as desired. □

**Lemma 2.9.** [DDT95, lemma 5.15] *Let*

$$\tilde{\cdot}\colon \operatorname{Hom}_{\mathcal{O}}(A, \mathcal{O}) \to \operatorname{Hom}_{\mathcal{O}[[\underline{X}]]}(A[[\underline{X}]], \mathcal{O}[[\underline{X}]])$$

*be the map that assigns an $\mathcal{O}[[\underline{X}]]$-homomorphism $\tilde{f}\colon A[[\underline{X}]] \to \mathcal{O}[[\underline{X}]]$ to the $\mathcal{O}$-homomorphism $f\colon A \to \mathcal{O}$ by extending it with $X \mapsto X$. Then define*

$$\Psi\colon \operatorname{Hom}_{\mathcal{O}}(A, \mathcal{O}) \to A$$

*via $\Psi(f) = \alpha(\tilde{f}(D))$. This is an $A$-module isomorphism where the $A$-module structure on $\operatorname{Hom}_{\mathcal{O}}(A, \mathcal{O})$ is given by $a \cdot f = (x \mapsto f(ax))$. In total we get that $A$ is Gorenstein.*

*Proof.* 1. $\Psi$ is $A$-linear. For any $a \in A, a' \in \mathcal{O}[[\underline{X}]]$ we have by definition of $\Psi$

$$\Psi(af) = \alpha(\tilde{f}(aD)) = \alpha(\tilde{f}((a-a')D + a'D)) = \alpha(\tilde{f}((a-a')D)) + \alpha(\tilde{f}(a'D)),$$

where in the last step we have used the linearity of $\tilde{f}$ and $\alpha$. Now choose $a' \in \alpha^{-1}(a) \subset \mathcal{O}[[\underline{X}]]$, as $\alpha$ is surjective. We can also understand $a'$ as an element of $A[[\underline{X}]]$ via the inclusion $\iota\colon \mathcal{O}[[\underline{X}]] \hookrightarrow A[[\underline{X}]]$. It follows $\beta(\iota(a')) = \alpha(a') = a = \beta(a)$. Therefore, $a - \iota(a') \in \ker \beta$. By definition of the $g_i$ as generators of $\ker \beta$, we can write $a - \iota(a')$ as an $A[[\underline{X}]]$-linear combination of the $g_i$. We further have

$$(f_1, \ldots, f_n) = (g_1, \ldots, g_n) \cdot M.$$

Multiplying with the adjugate matrix $M'$ we get

$$(f_1, \ldots, f_n) \cdot M' = (g_1, \ldots, g_n) \cdot \underbrace{M \cdot M'}_{= D \cdot I_{n \times n}}.$$

Hence, we can write $g_i \cdot D$ (and therefore also $(a - \iota(a')) \cdot D$) as an $A[[\underline{X}]]$-linear combination of the $f_i$,

$$(a - \iota(a')) \cdot D = \sum_{i=1}^{n} a_i f_i.$$

Using the $\mathcal{O}[[\underline{X}]]$-linearity of $\tilde{f}$, we compute

$$\begin{aligned}\alpha(\tilde{f}((a-a')D)) &= \alpha\left(\tilde{f}\left(\sum_{i=1}^{n} a_i f_i\right)\right) \\ &= \alpha\left(\sum_{i=1}^{n} f_i \tilde{f}(a_i)\right) = \sum_{i=1}^{n} \alpha(f_i \cdot \tilde{f}(a_i)) = 0,\end{aligned}$$

as $f_i \in \ker \alpha$. Putting our results together, we obtain

$$\Psi(af) = \alpha(\tilde{f}((a-a')D)) + \alpha(\tilde{f}(a'D)) = \alpha(\tilde{f}(a'D)),$$

and again by $\mathcal{O}[[\underline{X}]]$-linearity of $\tilde{f}$ we conclude

$$\Psi(af) = \alpha(a'\tilde{f}(D)) = a\alpha(\tilde{f}(D)) = a\Psi(f).$$

2. $\Psi$ is surjective. As $A$ is a finite flat $O$-algebra, we know by the classification of finitely generated modules over principal ideal domains that $A$ consists of a free part and a torsion part. Because it is flat, however, the torsion part is 0 and therefore $A$ is a free $O$-module. Therefore we have $\mathcal{O}$-module-isomorphisms

$$\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}^r, \mathcal{O}) \cong \mathcal{O}^r,$$

where $r$ may denote the rank of $\mathcal{O}$. Therefore $A$ and $\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ are both free $A$-modules of the same finite rank $r$. Let $f_1, \ldots, f_r$ be a generating system of $\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ over $\mathcal{O}$. Then, the extended maps $\tilde{f}_1, \ldots \tilde{f}_r$ form a generating system of $\mathrm{Hom}_{\mathcal{O}[[X]]}(A[[\underline{X}]], \mathcal{O}[[\underline{X}]])$ over $\mathcal{O}$. Indeed, let $f \in \mathrm{Hom}_{\mathcal{O}[[X]]}(A[[\underline{X}]], \mathcal{O}[[\underline{X}]])$. Then

$$f(X_i) = X_i \cdot f(1) = X_i \cdot \sum_{i=1}^{n} f_i(1) = \sum_{i=1}^{n} X_i \cdot f_i(1) = \sum_{i=1}^{n} \tilde{f}_i(X_i).$$

We have seen that the map

$$\Phi\colon \mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(A[[\underline{X}]], \mathcal{O}[[\underline{x}]]) \to A$$

is surjective. Therefore, $\forall a \in A\colon \exists p_1, \ldots, p_r \in \mathcal{O}[[\underline{X}]]$ s.t.

$$a = \Phi(p_1\tilde{f}_1 + \cdots + p_r\tilde{f}_r).$$

Now we can use the linearity of the involved maps,

$$a = \alpha((p_1\tilde{f}_1 + \cdots + p_r\tilde{f}_r)(D)) = \Psi(\alpha(p_1)f_1 + \cdots + \alpha(p_r)f_r).$$

3. $\Psi$ is injective. Analogous to the theorem for vector spaces, we know that a surjective homomorphism between two free modules of the same finite rank is also injective. As this condition is satisfied by $\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ and $A$, the lemma follows.

□

## 2.6 Explicit computation of $\eta$ for complete intersections

In this section, $A$ is always a finite flat complete intersection $\in \mathcal{C}^{\bullet}_{\mathcal{O}}$, i.e. $A \cong \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$. The goal of this section is to find explicit formulas for $\eta_A$ and $\phi_A$ using the relations $f_i$. This allows us to show that (c) $\implies$ (b) in theorem 2.1. We closely follow [DDT95, chapter 5.4].

*Notation.* $A^\vee \coloneqq \mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ and similarly, $\pi_A^\vee \colon \mathcal{O}^\vee \to A^\vee$ may denote the dual map associated to $\pi_A \colon A \to \mathcal{O}$.

As we have seen in the last section, $A^\vee \cong A$ as $A$ is a complete intersection. We choose one $A$-module isomorphism $\Psi \colon A^\vee \to A$.

**Lemma 2.10.** *Any two $A$-module isomorphisms $\Psi, \Psi' \colon A^\vee \to A$ differ by a unit.*

*Proof.* The composition $\Psi' \circ \Psi^{-1} \colon A \to A$ is an $A$-module isomorphism from $A$ to $A$. Such an isomorphism is uniquely defined by its value on 1,

$$\Psi' \circ \Psi^{-1}(x) = x \cdot \Psi' \circ \Psi^{-1}(1).$$

As we have the same fact for the inverse map, we find that $\Psi' \circ \Psi^{-1}(1) \in A^\times$. $\Psi \circ \Psi^{-1}(1) = 1$, so $\Psi' \circ \Psi^{-1} = x \cdot \Psi \circ \Psi^{-1}$. We conclude $\Psi = x \cdot \Psi'$. □

**Lemma 2.11.** *Regardless of the choice of $\Psi$, we have $\Psi\pi_A^\vee(\mathcal{O}^\vee) = \mathrm{Ann}_A \ker \pi_A$ and, a fortiori*

$$\eta_A = \pi_A \Psi \pi_A^\vee(\mathcal{O}^\vee).$$

*Proof.* We first show $\Psi\pi_A^\vee(\mathcal{O}^\vee) \subset \mathrm{Ann}_A \ker \pi_A$. Let therefore $\phi \colon \mathcal{O} \to \mathcal{O} \in \mathcal{O}^\vee$ and $x \in \ker \pi_A$. It suffices to show that $\Psi\pi_A^\vee(\phi) \cdot x = 0$. Taking into account the $A$-module structure of $\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ and the fact that $\Psi$ is an $A$-module-isomorphism, we obtain

$$\Psi\pi_A^\vee(\phi) \cdot x = \Psi(\phi \circ \pi_A) \cdot x = \Psi(x \cdot \phi \circ \pi_A) = \Psi((y \mapsto \phi \circ \pi_A(x \cdot y))) = 0,$$

as $x \in \ker \pi_A$. In order to prove $\Psi\pi_A^\vee(\mathcal{O}^\vee) \supset \mathrm{Ann}_A \ker \pi_A$, let $a \in \mathrm{Ann}_A \ker \pi_A$ and $f \in \mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ s.t. $\Psi(f) = a$. Then $\forall x \in \ker \pi_A$,

$$0 = \Psi(f) \cdot x = \Psi((y \mapsto f(x \cdot y))) \implies f(x \cdot y) = 0 \quad \forall y \in A \implies f(x) = 0.$$

A fortiori, $\ker \pi_A \subset \ker f$ and we get an induced map $\tilde{f} \colon \mathcal{O} \cong A/\ker \pi_A \to \mathcal{O}$ s.t. $f = \tilde{f} \circ \pi_A$. As a result, we can write

$$a = \Psi(f) = \Psi(\tilde{f} \circ \pi_A) = \Psi(\pi_A^\vee(\tilde{f})) \in \Psi(\pi_A^\vee(\mathcal{O}^\vee)).$$

□

**Lemma 2.12.** *Let*

$$\tilde{\cdot}\colon \mathrm{Hom}_{\mathcal{O}}(A,\mathcal{O}) \to \mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(A[[\underline{X}]],\mathcal{O}[[\underline{X}]])$$

*and $\Psi$ be the maps known from lemma 2.9 and $D = \det M$ as defined in the previous section. Then,*

$$\pi_A \Psi \pi_A^\vee(\mathcal{O}^\vee) = \langle \pi_A \alpha \tilde{\pi}_A(D)\rangle_{\mathcal{O}}.$$

*Proof.* Let $\phi \in \mathcal{O}^\vee = \mathrm{Hom}_{\mathcal{O}}(\mathcal{O},\mathcal{O})$. Then $\phi(x) = x \cdot \phi(1) \in \mathcal{O}$. Therefore

$$\Psi(\pi_A^\vee(\phi)) = \Psi(\phi \circ \pi_A) = \alpha(\tilde{\phi} \circ \tilde{\pi_A}(D)) = \alpha(\phi(1) \cdot \tilde{\pi_A}(D)).$$

Using the $\mathcal{O}$-linearity of $\alpha$ and $\pi_A$, we get

$$\pi_A(\Psi(\pi_A^\vee(\phi))) = \phi(1) \cdot \pi_A \alpha \tilde{\pi_A}(D) \in \langle \pi_A \alpha \tilde{\pi}_A(D)\rangle_{\mathcal{O}}.$$

For the other inclusion, let $x \cdot \pi_A \alpha \tilde{\pi}_A \in \langle \pi_A \alpha \tilde{\pi}_A(D)\rangle_{\mathcal{O}}$ with $x \in \mathcal{O}$. Then define $\phi(y) = y \cdot x \in \mathcal{O}^\vee$. By the calculations we have done so far it becomes clear that this is the required preimage. □

**Proposition 2.2.** *[DDT95, proposition 5.19]*

$$\eta_A = (\det(\partial f_i/\partial X_j(0))).$$

*Proof.* We have

$$\eta_A = \pi_A \Psi \pi_A^\vee(\mathcal{O}^\vee) = \pi_A \alpha \tilde{\pi}_A(D).$$

Consider the equation

$$(f_1,\ldots,f_n) = (X_1 - [X_1],\ldots,X_n - [X_n]) \cdot (m_{i,j})_{i,j}.$$

Applying $\tilde{\pi}_A$ to the whole equation leaves the $f_i$ unchanged because $\tilde{\pi}_A(X_i) = X_i$ and the coefficients of the $f_i$ are elements of $\mathcal{O}$ that are not affected by $\pi_A$ because of its $\mathcal{O}$-linearity. In the following we make use of remark 2.2. On the RHS, we get $\tilde{\pi}_A(X_i - [X_i]) = X_i - \pi_A([X_i]) = X_i$, as $\pi_A$ is the evaluation at 0 for preimages of $A$ in $\mathcal{O}[[X_1,\ldots,X_n]]$. Denote the image of $m_{i,j}$ under $\tilde{\pi}_A$ with $\tilde{m}_{i,j} \in \mathcal{O}[[X_1,\ldots,X_n]]$. Now compute

$$\frac{\partial f_i}{\partial X_j}(0) = \frac{\partial \sum_{k=1}^n X_k \tilde{m}_{k,i}}{\partial X_j}(0) = \tilde{m}_{j,i}(0) + \sum_{k=1}^n X_k \frac{\partial \tilde{m}_{k,i}}{\partial X_j}\bigg|_0 = \tilde{m}_{j,i}(0).$$

The composition $\pi_A \circ \alpha$ is given by the evaluation at 0. Because computing the determinant is a linear operation, we get

$$\pi_A \alpha \tilde{\pi}_A(D) = \det(\pi_A \alpha \tilde{m}_{i,j})_{i,j} = \det(\tilde{m}_{i,j}(0))_{i,j} = \det \frac{\partial f_i}{\partial X_j}(0).$$

□

**Corollary 2.4.** *[DDT95, corollary 5.20] Remembering that we assumed $A$ to be a finite flat complete intersection $\in \mathcal{C}^{\bullet}_{\mathcal{O}}$, we obtain*

$$\#\Phi_A = \#(\mathcal{O}/\eta_A),$$

*i.e. (c) $\Longrightarrow$ (b) in theorem 2.1.*

*Proof.* From remark 2.3 we know that

$$\Phi_A \cong \Phi_U/(\overline{f_1}, \ldots, \overline{f_n}),$$

where $\overline{f}$ denotes the degree one term of a polynomial. More explicitly, we get

$$\Phi_A \cong \mathcal{O}X_1 \oplus \cdots \oplus \mathcal{O}X_n/(a_{f_1,1}X_1 + \cdots + a_{f_1,n}X_n, \ldots, a_{f_n,1}X_1 + \cdots + a_{f_n,n}X_n).$$

Applying the isomorphism $\Phi_U = \mathcal{O}^n$ we obtain

$$\Phi_A \cong \mathcal{O}^n/(v_1, \ldots, v_n),$$

where $v_i \coloneqq (a_{f_i,1}, \ldots, a_{f_i,n})$. If we interpret $V = [v_i]_i$ as a matrix and hence an $\mathcal{O}^n$-endomorphism, then $\operatorname{im} V = (v_1, \ldots, v_n)$. Clearly

$$a_{f_i,j} = \frac{\partial f_i}{\partial X_j}(0)$$

and hence

$$V = (\frac{\partial f_i}{\partial X_j}(0))_{i,j}.$$

As $\mathcal{O}$ is a PID, we know that there exist invertible $\mathcal{O}$-matrices $S, T$ s.t.

$$V = SDT$$

for some diagonal matrix

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

(Smith normal form). As the endomorphisms enduced by $S$ and $T$ are isomorphisms, we compute

$$\mathcal{O}^n/(SDT)\mathcal{O}^n = \mathcal{O}^n/D\mathcal{O}^n = \mathcal{O}/d_1\mathcal{O} \oplus \cdots \oplus \mathcal{O}/d_n\mathcal{O}$$

For Dedekind rings we know that $A/\mathfrak{a}A \cong \mathfrak{b}/\mathfrak{a}\mathfrak{b}$ if $0 \neq \mathfrak{a}, \mathfrak{b}$ are ideals of $A$. We conclude

$$\#\mathcal{O}/\mathfrak{a}\mathfrak{b} \cong \#\mathcal{O}/\mathfrak{b} \cdot \#\mathfrak{b}/\mathfrak{a}\mathfrak{b} \cong \#\mathcal{O}/\mathfrak{b} \cdot \#\mathcal{O}/\mathfrak{a}$$

and obtain

$$\#\mathcal{O}^n/D\mathcal{O}^n = \#\mathcal{O}/d_1\mathcal{O} \cdot \cdots \cdot \#\mathcal{O}/d_n\mathcal{O} = \#\mathcal{O}/d_1 \cdot \cdots \cdot d_n\mathcal{O} = \#\mathcal{O}/\det D\mathcal{O}$$

As the ideal generated by units is the whole ring, this is the same as $\#\mathcal{O}/\det V\mathcal{O}$. However, we compute

$$\det V\mathcal{O} = \det(\frac{\partial f_i}{\partial X_j}(0))\mathcal{O} = \eta_A.$$

We conclude

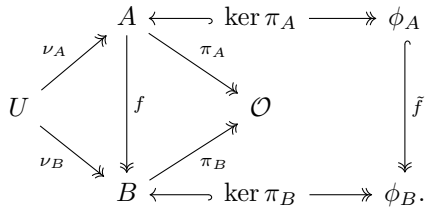
$$\#\Phi_A = \#\mathcal{O}^n/V\mathcal{O}^n \#\mathcal{O}/\det V\mathcal{O} = \#\mathcal{O}/\eta_A.$$

□

## 2.7 Isomorphism theorems

**Proposition 2.3.** *[DDT95, theorem 5.21] Let $f\colon A \twoheadrightarrow B$ be a $\mathcal{C}^\bullet_\mathcal{O}$-morphism and $B$ a finite flat complete intersection. If the tangent spaces $\phi_A, \phi_B$ are finite and the induced morphism $\tilde{f}\colon \phi_A \to \phi_B$ is an isomorphism, then $f$ is an isomorphism.*

*Proof.* Consider the following commutative diagram




The projection $\nu_B$ arises from the fact that we can write every object in $\mathcal{C}^\bullet_\mathcal{O}$ as a quotient of $U$ (remark 2.1). As $B$ is a complete intersection, we find $n$ generators $f_i \in U$ s.t. $\ker \nu_B = (f_1, \ldots, f_n)$. Note that we need to choose the $f_i$ in such a way that they have no constant term (cf. remark 2.2) Define $b_i \coloneqq \nu_B(X_i) \in \ker \pi_B$ and choose preimages $a_i \in A$ s.t. $f(a_i) = b_i$. As the triangle involving $A, B$ and $\mathcal{O}$ commutes, we conclude that $\pi_A(a_i) = \pi_B(b_i) = 0$, i.e. $a_i \in \ker \pi_A$.

As $X_1, \ldots, X_n$ generate $\phi_U$ and $\nu_B$ is surjective, it is easy to see that $b_1, \ldots, b_n$ generate $\phi_B$. We know that $\tilde{f}$ is an isomorphism, so $a_1, \ldots, a_n$ generate $\phi_A$. Define

$$\nu_A\colon \mathcal{O}[[X_1, \ldots, X_n]] \to A$$

via $\nu_A(X_i) = a_i$. As all generators lie in the image of $\nu_A$, this induces a surjection on $\phi_A$. By lemma 2.2 it follows that $\phi$ is surjective.

Finally, we want to show that $\ker \nu_A = \ker \nu_B$. Let $x \in \ker \nu_A$, i.e. $0 = f(0) = f(\nu_A(x)) = \nu_B(x)$, i.e. $x \in \ker \nu_B$. Therefore it remains to prove the inclusion $\ker \nu_B \subset \ker \nu_A$.

The kernel of

$$\overline{\nu_A}\colon \phi_U \to \phi_A$$

is a submodule of the finitely generated $\mathcal{O}$-module of rank $n$ $\phi_U$. As $\mathcal{O}$ is a PID, we know that any submodule is finitely generated of rank $n' \leq n$. Independent

of $n'$, we can choose $n$ possibly linear dependent generators $\overline{g_1}, \dots \overline{g_n}$ of the above kernel and then extend these generators to $g_1, \dots, g_n \in \ker \nu_A$. A fortiori, the $g_i$ do not have constant terms.

As the kernel of $\nu_B$ is generated by $f_1, \dots, f_n$ and $\ker \nu_A \subset \ker \nu_B$, we find a $U$-linear combination that can be written in the form

$$(g_1, \dots, g_n) = (f_1, \dots, f_n) \cdot M,$$

where $M$ is a $n \times n$ matrix with entries in $U$. The $g_i$ and the $f_i$ both have no constant terms. Hence, forgetting all monomials of degree bigger than one (equivalently considering the residue classes $\mod \ker \pi_A^2$ resp. $\ker \pi_B^2$, denoted by $\bar{\cdot}$) forces us to take the constant terms $\overline{M}$ of $M$,

$$(\overline{g_1}, \dots, \overline{g_n}) = (\overline{f_1}, \dots, \overline{f_n})\overline{M}.$$

As the tangent spaces are isomorphic, both $(\overline{g_1}, \dots, \overline{g_n})$ and $(\overline{f_1}, \dots, \overline{f_n})$ generate the same $\mathcal{O}$-submodule of $\phi_U$. Indeed, $\overline{f_1}, \dots, \overline{f_n} = \ker(\ker \pi_U / \ker \pi_U^2 \to \ker \pi_B / \ker \pi_B^2)$. As a result, we can express each of the $\overline{f_1}, \dots, \overline{f_n}$ as a $\mathcal{O}$-linear combination of $(\overline{g_1}, \dots, \overline{g_n})$. This gives us an inverse to $\overline{M}$ and we deduce that $\det \overline{M}$ is invertible in $\mathcal{O}$. A power series is invertible if its constant term is invertible so as a result $\det M$ is invertible as well and we conclude that

$$f_1, \dots, f_n \in \langle g_1, \dots, g_n \rangle_U = \ker \nu_B$$

and, a fortiori,

$$\ker \nu_A = \langle f_1, \dots, f_n \rangle_U \subset \ker \nu_B.$$

In total we obtain $\ker \nu_A = \ker \nu_B$ and we can define the map

$$\nu_A \nu_B^{-1} \colon B \to A.$$

This is indeed welldefined: For a given $x \in B$ choose $y, y' \in U$ s.t. $\nu_B(y) = \nu_B(y') = x$. It follows $y' - y \in \ker \nu_B$. Then $\nu_A(y') = \nu_A(y' - y) + \nu_A(y) = 0 + \nu_A(y)$ because $\ker \nu_A = \ker \nu_B$. From the commutativity of the above diagram we get that this is indeed an inverse for $f$ and hence, $f$ is an isomorphism. □

**Lemma 2.13.** *Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ be finite flat. Then the canonical map*

$$A \to A^{\vee\vee}$$

*is injective. As a corollary we have*

$$A \neq 0 \implies A^{\vee} \neq 0.$$

*Proof.* As $\mathcal{O}$ is local, every finitely generated torsion-free $\mathcal{O}$-module is free and, a fortiori projective. For projective modules we have the existence of a dual basis, i.e. a set of functions

$$\{f_i \colon i \in I, f_i \in A^{\vee} = \mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})\}$$

together with a set of of elements

$$\{a_i \colon i \in I, a_i \in A\}$$

satisfying the properties

1. $\forall a \in A\colon \quad \#\{i \in I\colon f_i(a) \neq 0\} < \infty$ and
2. $\forall a \in A\colon \quad a = \sum_{i\in I} f(a) \cdot a_i$.

Now let $0 = (\phi \mapsto \phi(a))$, i.e. $\phi(a) = 0 \forall \phi \in A^\vee$. Then, a fortiori, $f_i(a) = 0 \forall i \in I$. We conclude

$$a = \sum_{i\in I} f_i(a) \cdot a_i = 0$$

and hence, $A \to A^{\vee\vee}$ is injective. If $A^\vee = 0$ then obviously any homomorphism from $A^\vee$ is 0, a fortiori, $A^\vee\vee = 0$. By the injectivity of $A \to A^{\vee\vee}$ this yields $A = 0$ and we have proved the second part of the lemma. □

**Lemma 2.14.** *Let $A \in \mathcal{C}^\bullet_\mathcal{O}$ be finite flat. Then*

$$\ker \pi_A \cap \operatorname{Ann}_A \ker \pi_A = 0.$$

*Proof.* Let $0 \neq x \in \eta_A$ and $x' \in \operatorname{Ann}_A \ker \pi_A$ s.t. $\pi_A(x') = x$. Interpret $x \cdot 1$ as an element of the $\mathcal{O}$-module $A$. Then,

$$\pi_A(x \cdot 1 - x') = x \cdot \pi_A(1) - \pi_A(x') = x - x = 0 \implies x \cdot 1 - x' \in \ker \pi_A$$

Take $a \in \ker \pi_A \cap \operatorname{Ann}_A \ker \pi_A$. Then $ax' = 0$, because $a \in \ker \pi_A$ and $x' \in \operatorname{Ann}_A \ker \pi_A$. Together we obtain

$$0 = a \cdot (x \cdot 1 - x') = x \cdot a,$$

i.e. $a$ is $\mathcal{O}$-torsion. However, $A$ is flat and, a fortiori, torsion-free. Hence, $a$ is 0. □

**Proposition 2.4.** *[DDT95, theorem 5.24] Let $f\colon A \twoheadrightarrow B$ be a $\mathcal{C}^\bullet_\mathcal{O}$-morphism, $A$ and $B$ finite flat and $B$ a complete intersection. If $\eta_A = \eta_B \neq 0$, then $f$ is an isomorphism.*

*Proof.* By lemma 2.9, $A$ is Gorenstein, i.e.

$$A^\vee = \operatorname{Hom}_\mathcal{O}(A, \mathcal{O}) \cong A \quad \text{as } A\text{-modules},$$

where the $A$-module structure is given via $a \cdot \phi = (x \mapsto \phi(a \cdot x))$. By lemma 2.14 $\ker \pi_A \cap \operatorname{Ann}_A \ker \pi_A = 0$ and likewise for $B$. The fundamental theorem of homomorphisms gives us an isomorphism

$$\operatorname{Ann}_A \ker \pi_A = \operatorname{Ann}_A \ker \pi_A / (\ker \pi_A \cap \operatorname{Ann}_A \ker \pi_A) \xrightarrow[\sim]{\pi_A} \eta_A$$

respectively

$$\operatorname{Ann}_B \ker \pi_B = \operatorname{Ann}_B \ker \pi_B / (\ker \pi_B \cap \operatorname{Ann}_B \ker \pi_B) \xrightarrow[\sim]{\pi_B} \eta_B.$$

In total we obtain

$$\operatorname{Ann}_A \ker \pi_A \cong \eta_A \xrightarrow{f} \eta_B \cong \operatorname{Ann}_B \ker \pi_B.$$

As $f$ is a $\mathcal{C}_{\mathcal{O}}^{\bullet}$-map, we have the commutativity $\pi_A = \pi_B f$. Hence, for all $x \in \ker f$ we compute $\pi_A(x) = \pi_B(f(x)) = \pi_B(0) = 0$, i.e. $x \in \ker \pi_A$. We thereby have shown that $\ker f \subset \ker \pi_A$ and with lemma 2.14 we conclude

$$\ker f \cap \operatorname{Ann}_A \ker \pi_A \subset \ker \pi_A \cap \operatorname{Ann}_A \ker \pi_A = 0.$$

A fortiori, we get an exact sequence of $A$-modules

$$0 \longrightarrow \ker f \oplus \operatorname{Ann}_A \ker \pi_A \longrightarrow A \longrightarrow A/\ker f \oplus \operatorname{Ann}_A \ker \pi_A \longrightarrow 0. \qquad (*)$$

We have

$$A/\ker f \oplus \operatorname{Ann}_A \ker \pi_A \xrightarrow[\sim]{f} B/f(\operatorname{Ann}_A \ker \pi_A) \cong B/\operatorname{Ann}_B \ker \pi_B$$

and via $[b] \mapsto (x \mapsto b \cdot x)$ we get a canonical injection

$$B/\operatorname{Ann}_B \ker \pi_B \hookrightarrow \operatorname{End}_{\mathcal{O}}(\ker \pi_B)$$

As $B$ and therefore $\ker \pi_B$ are torsion-free, we show that $\operatorname{End}_{\mathcal{O}}(\ker \pi_B)$ is torsion-free as well. For, let $0 \neq \phi \in \operatorname{End}_{\mathcal{O}}(\ker \pi_B)$ and $x \in \mathcal{O}$ s.t. $0 = x \cdot \phi = (y \mapsto x \cdot \phi(y))$. As $\phi \neq 0$, there is at least one $\tilde{y} \in \ker \pi_B$ s.t. $\phi(\tilde{y}) \neq 0$. As $\ker \pi_B$ is torsion-free and $x \cdot \phi(\tilde{y}) = 0$ it follows that $x = 0$, i.e. $\operatorname{End}_{\mathcal{O}}(\ker \pi_B)$ is torsion-free. As $O$ is a Dedekind ring, torsion-freeness implies flatness. Over any local ring, finitely generated flat modules are free and a fortiori projective. Hence, the short exact sequence $(*)$ splits. Functors preserve split exact sequences and therefore applying the contravariant functor $\operatorname{Hom}_{\mathcal{O}}(-, \mathcal{O})$ yields

$$0 \longrightarrow (A/\ker f \oplus \operatorname{Ann}_A \ker \pi_A)^\vee \longrightarrow A^\vee \longrightarrow (\ker f \oplus \operatorname{Ann}_A \ker \pi_A)^\vee \longrightarrow 0.$$

The direct sum of modules is a colimit, so it commutes with the $\operatorname{Hom}_{\mathcal{O}}(-, \mathcal{O})$-functor and becomes a limit, in this case a product. However, a finite product is isomorphic to the finite coproduct in the category of $\mathcal{O}$-modules and together with the fact that $A$ is Gorenstein, we obtain

$$A \longrightarrow (\ker f)^\vee \oplus (\operatorname{Ann}_A \ker \pi_A)^\vee \longrightarrow 0.$$

The functor $- \otimes_A k$ (where we interpret $k$ as an $A$-module via the canonical projection $A \xrightarrow{\pi_A} \mathcal{O} \twoheadrightarrow \mathcal{O}/\lambda = k$) is right exact (because it's left adjoint to the corresponding Hom-functor). Taking the dimension of the resulting exact sequence gives us

$$1 = \dim_k(A \otimes_A k) \geq \dim_k((\ker f)^\vee \otimes_A k) + \dim_k((\operatorname{Ann}_A \ker \pi_A)^\vee \otimes_A k), \quad (**)$$

because taking the dimension commutes with direct sums. It is clear that

$$\eta_A = \pi_A \operatorname{Ann}_A \ker \pi_A \neq 0 \implies \operatorname{Ann}_A \ker \pi_A \neq 0.$$

By lemma 2.13, $(\operatorname{Ann}_A \ker \pi_A)^\vee \neq 0$. Now let's assume $(\operatorname{Ann}_A \ker \pi_A)^\vee \otimes_A k = 0$, i.e.

$$0 = (\operatorname{Ann}_A \ker \pi_A)^\vee \otimes_A A/\lambda = (\operatorname{Ann}_A \ker \pi_A)^\vee / \lambda (\operatorname{Ann}_A \ker \pi_A)^\vee,$$

which is equivalent to $(\mathrm{Ann}_A \ker \pi_A)^\vee = \lambda(\mathrm{Ann}_A \ker \pi_A)^\vee$ and by Nakayama's lemma for the local ring $\mathcal{O}$ we could conclude that $(\mathrm{Ann}_A \ker \pi_A)^\vee = 0$, contradiction. Therefore $\dim_k(\mathrm{Ann}_A \ker \pi_A)^\vee > 0$ and by $(**)$ we have $(\ker f)^\vee \otimes_A k = 0$. Again,

$$0 = (\ker f)^\vee \otimes_A A/\lambda = (\ker f)^\vee/\lambda(\ker f)^\vee \xrightarrow{Nakayama} (\ker f)^\vee = 0.$$

Taking the dual and applying lemma 2.13 finally yields $\ker f = 0$. □

## 2.8 A resolution lemma

**Lemma 2.15.** *[DDT95, theorem 5.26] Let $A \in \mathcal{C}^\bullet_\mathcal{O}$ be finite flat. Then there is a $\mathcal{C}^\bullet_\mathcal{O}$-morphism $f\colon \tilde{A} \to A$ where $\tilde{A}$ is a finite flat complete intersection and $f$ induces an isomorphism on the tangent spaces, $\tilde{f}\colon \phi_{\tilde{A}} \xrightarrow{\sim} \phi_A$.*

*Proof.* First, we notice that $\ker \pi_A$ is a finitely generated $O$-module. This follows from the fact that submodules of finitely generated modules over PIDs are finitely generated again. Let $a_1, \ldots, a_n$ be generators of $\ker \pi_A$. Then define

$$\phi\colon V \coloneqq \mathcal{O}[X_1, \ldots, X_n] \to A$$

via $\phi(X_i) = a_i$. We have seen in the proof of remark 2.1 that $A = \ker \pi_A \oplus \mathcal{O}$. Defining $\pi_V$ via $X_i \mapsto 0 \quad \forall i$ we get $V = \ker \pi_V \oplus \mathcal{O}$. $\phi$ then induces an isomorphism on the second component, a surjection on the first and is therefore surjective. It is clear that

$$\phi_V \coloneqq \ker \pi_V/(\ker \pi_V)^2 = \mathcal{O}X_1 \oplus \cdots \oplus \mathcal{O}X_n$$

is a finitely generated $\mathcal{O}$-module of rank $n$. Therefore the kernel of the projection $\phi_V \to \phi_A$ is also finitely generated of rank $n' \leq n$. Independent of $n'$, we can choose $n$ possibly linearly dependent linear polynomials $\overline{f_i} \in \ker(\phi_V \to \phi_A)$ without constant term that generate $\ker \phi_V \to \phi_A$. Now consider a system $(f_1, \ldots, f_n)$ of lifts to $V$ and denote their maximal degree with $m$. All elements of $\ker \pi_A$ can be written as a linear combination of the generators $a_i$, so a fortiori we find linear polynomials $h_i(X_1, \ldots, X_n)$ s.t. $a_i^2 = h_i(a_1, \ldots, a_n)$. With these additional relations we can replace the relations $f_i$ by modified relations

$$f_i + X_i^m h_i - X_i^{m+2}.$$

Now we see that $V/(f_1, \ldots, f_n)$ is a finitely generated $\mathcal{O}$-module, because it is generated by the images of monomials of degree $\leq n(m+1)$. Indeed, any monomial of higher degree must contain one of the $X_i$ at least with potence $m+2$. Then, using the relation $f_i + X_i^m h_i - X_i^{m+2}$, it can be expressed as a sum of monomials of lower degree. Therefore we get a surjection

$$\mathcal{O}[X_1, \ldots, X_n]/(f_1, \ldots, f_n) \to A.$$

The completion of the left side is still a finitely generated $\mathcal{O}$-module. Indeed, the submodule $M$ generated by the generators of $\mathcal{O}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$

contains the dense subset of all polynomials in $\mathcal{O}[[X_1,\dots,X_n]]/(f_1,\dots,f_n)$. Once we can show that the $\mathcal{O}$-submodules generated by a single polynomial are closed in $\mathcal{O}[[X_1,\dots,X_n]]/(f_1,\dots,f_n)$, it follows that $M$ is closed as a finite union of closed submodules. Consider the submodule $f\cdot\mathcal{O}$. For any family of elements $(F_i)_{i\in I}$ of $f\cdot\mathcal{O}$, we have a family $(x_i)_{i\in I}$ with $x_i\in\mathcal{O}\ \forall i\in I$ s.t. $F_i = f\cdot x_i\ \forall i\in I$. Then

$$\lim_{i\in I} f\cdot x_i = f\cdot\lim_{i\in I} x_i = f\cdot x\in f\cdot\mathcal{O},$$

because $x\in\mathcal{O}$ as $\mathcal{O}$ is complete. Hence, $f\cdot\mathcal{O}$ is closed. We obtain that the finite generating set of $A$ generates a dense and closed subset in $\tilde{A}$, i.e. it generates $\tilde{A}$. Hence, $\tilde{A}$ is a finitely generated $\mathcal{O}$-module $\in\mathcal{C}^\bullet_{\mathcal{O}}$. From corollary 2.3 we then conclude that its flat as well and therefore is a complete intersection where the tangent space is the completion of

$$\phi_A = \phi_{V/(f_1,\dots,f_n)} = \phi_V/(\overline{f_1},\dots,\overline{f_n}).$$

As $\overline{f_1},\dots,\overline{f_n}$ generate $\ker\phi_V\to\phi_A$, they also generate the completion $\ker\phi_U\to\phi_A$ (Analogous to the above argumentation **provide details**). Therefore, using remark 2.3, we have an isomorphism of the tangent spaces

$$\phi_{\tilde{A}} = \phi_U/(\overline{f_1},\dots,\overline{f_n})\to\phi_A,$$

as desired. □

## 2.9 A criterion for complete intersections

**Proposition 2.5.** *[DDT95, theorem 5.27] Let $A\in\mathcal{C}^\bullet_{\mathcal{O}}$ be finite flat. If $\#\phi_A\le\#(\mathcal{O}/\eta_A)<\infty$, then $A$ is a complete intersection.*

*Proof.* Take the morphism $\phi\colon\tilde{A}\to A$ from lemma 2.15. As $\#\phi_A$ is finite, we can apply corollary 2.1 and because $\phi$ induces an isomorphism on the tangent spaces, i.e. $\#\phi_{\tilde{A}} = \#\phi_A$, it is surjective. By lemma 2.5 we also now that $\#\phi_{\tilde{A}}\ge\#(\mathcal{O}/\eta_{\tilde{A}})$. Starting with the assumption and then using both of the previous facts, we obtain

$$\#(\mathcal{O}/\eta_A)\ge\#\phi_A = \#\phi_{\tilde{A}}\ge\#(\mathcal{O}/\eta_{\tilde{A}}).$$

As $\tilde{A}\twoheadrightarrow A$ is surjective, we apply lemma 2.3 and deduce

$$\eta_{\tilde{A}}\subset\eta_A,\ \ \#(\mathcal{O}/\eta_{\tilde{A}})\ge\#(\mathcal{O}/\eta_A).$$

All in all, we have $\#(\mathcal{O}/\eta_A) = \#(\mathcal{O}/\eta_{\tilde{A}})$ and because of $\eta_{\tilde{A}}\subset\eta_A$ we conclude $\eta_{\tilde{A}} = \eta_A$. By proposition 2.4 it follows that $\phi$ is an isomorphism. Since $\tilde{A}$ is a complete intersection, so is $A$. □

## 2.10 Proof of Wiles' numerical criterion

**Proposition 2.6.** *[DDT95, theorem 5.28] Let $R, T \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ such that $T$ is finite flat and $\phi\colon R \twoheadrightarrow T$ is a surjective $\mathcal{C}_{\mathcal{O}}^{\bullet}$-morphism. If $\#\phi_R \leq \#(\mathcal{O}/\eta_T) < \infty$, then $R$ and $T$ are complete intersections, and $\phi$ is an isomorphism. A fortiori, (a) $\Longrightarrow$ (c) in theorem 2.1.*

*Proof.* Concatenating the inequalities from lemma 2.5, corollary 2.1 which is applicable because of the surjectivity of $\phi$ and from the assumption, we obtain

$$\#(\mathcal{O}/\eta_T) \leq \#\phi_T \leq \#\phi_R \leq \#(\mathcal{O}/\eta_T).$$

All inequalities must be equalities and from $\#\phi_T = \#(\mathcal{O}/\eta_T)$ we conclude with proposition 2.5 that $T$ is a complete intersection. From $\#\phi_T = \#\phi_R$ we see that $\phi$ induces an isomorphism on the tangent spaces. From proposition 2.3 it follows that $\phi\colon R \to T$ is an isomorphism and, a fortiori $R$ is a complete intersection as well. □

Now we can put all results together and complete the proof of theorem 2.1.

*Proof.* The equivalence of (a) and (b) has been established in proposition 2.1. Corollary 2.4 shows that (c) $\Longrightarrow$ (b) in theorem 2.1. Finally, proposition 2.6 gives us the implication (a) $\Longrightarrow$ (c). □

# References


[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison Wesley Publishing Company, 1969, pp. I–IX, 1–128. ISBN: 978-0-201-40751-8.

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens. *Modular Forms and Fermat's Last Theorem*. New York, NY: Springer New York, 1997. I-XIX, 1-582. ISBN: 9781461219743. URL: http://dx.doi.org/10.1007/978-1-4612-1974-3.

[DDT95] H. Darmon, F. Diamond, and R. Taylor. "Fermat's last theorem". In: *Current developments in mathematics* 1995.1 (1995), pp. 1–154.

[DS07] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer, 2007, p. 451. ISBN: 9780387232294.

[Har77] R. Hartshorne. *Algebraic geometry*. Vol. 52. Graduate texts in mathematics. Springer, 1977. ISBN: 978-3-540-90244-7. DOI: 10.1007/978-1-4757-3849-0.

[Mat86] H. Matsumura. *Commutative ring theory*. @Cambridge studies in advanced mathematics 8. Cambridge: Cambridge Univ. Press, 1986. XIII, 320. ISBN: 0521259169.

[Sta22] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2022.