

# Fermat's Last Theorem

Josua Kugler

July 18, 2022

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>An Overview of Wiles' proof</b>	<b>1</b>
<b>3</b>	<b>Wiles' numerical criterion</b>	<b>2</b>
3.1	Preliminaries and examples . . . . .	2
3.2	Basic properties of the invariants . . . . .	7
3.3	Regular sequences and the Koszul complex . . . . .	9
3.4	Complete intersections and the Gorenstein condition . . . . .	11

## 1 Introduction

## 2 An Overview of Wiles' proof

### 3 Wiles' numerical criterion

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.

#### 3.1 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 valuation ring (DVR), i.e.  $\mathcal{O}$  is a local, noetherian Dedekind ring with maximal ideal  $\lambda$ . It is complete with respect to the  $\lambda$ -adic topology, a principal ideal domain (PID) and has residue field  $k := \mathcal{O}/\lambda$  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 map

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

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  $f: A \rightarrow B$  we have the commutative diagram

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

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

**Definition 3.1.**  $A \in \mathcal{C}_\mathcal{O}$  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 3.2** (complete intersection). 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

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

where there are as many relations as there are variables.

Let's take a look at an example.

**Example 3.1.**  $A = \{(a, b) \in \mathcal{O} \times \mathcal{O}, a \equiv b \pmod{\lambda^n}\} \cong \mathcal{O}[[T]]/(T(T - \lambda^n))$  is a finite flat complete intersection in  $\mathcal{C}_{\mathcal{O}}^{\bullet}$ . The projection  $\pi_A$  is given by  $\pi_A(a, b) = a$ .

*Proof.* Consider the map

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

**$\phi$  is welldefined and respects the  $\mathcal{O}$ -algebra structure:** Let  $f_0$  be the constant term of a polynomial  $f$  and  $f_1 := T^{-1}(f - f_0)$ , 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  $\tilde{\phi}_2: \mathcal{O}[[T]] \rightarrow \mathcal{O}$ ,  $f \mapsto f(\lambda^n)$  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  $a \equiv b \pmod{\lambda^n}$ , 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.

$A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ :  $\mathcal{O}$  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

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

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

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

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

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

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

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

As a result,  $\mathcal{O}[[T]]/(T(T - \lambda^n))$  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.

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.  $\square$

**Example 3.2.**  $U = \mathcal{O}[[X_1, \dots, X_n]]$  with projection  $\pi_U: U \rightarrow \mathcal{O}$ ,  $f \mapsto f(0)$  lies in  $\mathcal{C}_{\mathcal{O}}^*$ .

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

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

Therefore, the completion

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

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

**Remark 3.1.** In example 3.1 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  $U = \mathcal{O}[[X_1, \dots, X_n]]$  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

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

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  $\mathcal{C}_{\mathcal{O}}^\bullet$ . We have the short exact sequences

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

and

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

As both corresponding sequences split via the inclusion  $\mathcal{O} \hookrightarrow A$  resp.  $\mathcal{O} \hookrightarrow U$ , we can write  $A \cong \mathcal{O} \oplus \ker \pi_A$  and  $A[[X_1, \dots, X_n]] \cong A \oplus \ker \pi_A$ .  $\Phi$  by definition induces an equality on the first component, a surjection on the second and therefore is surjective on the direct sum.  $\square$

**Definition 3.3.** Let  $A \in \mathcal{C}_{\mathcal{O}}^\bullet$ . Then

$$\phi_A := (\ker \pi_A) / (\ker \pi_A)^2.$$

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  $\operatorname{spec}(A)$  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 3.3.** Remember the definition of  $U$  in example 3.2. The tangent space  $\phi_U = \ker \pi_U / (\ker \pi_U)^2$  is

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

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  $\bar{f} \in \phi_U$  by cutting off all higher terms of a power series  $f \in \ker \pi_U$ .

**Remark 3.2.** Write  $A$  as a quotient of  $U$ ,  $A = U/(f_1, \dots, f_n)$ . We then get  $\phi_A = \phi_U/(\bar{f}_1, \dots, \bar{f}_n)$ . As a quotient of  $\phi_U$  its a finitely generated  $\mathcal{O}$ -module.

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

$$\begin{aligned} \Phi: \ker \pi_U = \mathcal{O}X_1 \oplus \dots \oplus \mathcal{O}X_n &\rightarrow (\ker \pi_A) / (\ker \pi_A)^2 = \phi_A \\ a_1X_1 + \dots + a_nX_n &\mapsto [a_1X_1 + \dots + a_nX_n] \mod (\ker \pi_A)^2, \end{aligned}$$

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

$$\begin{aligned} \tilde{\Phi}: \phi_U &\rightarrow \phi_A \\ a_1X_1 + \dots + a_nX_n \mod (\ker \pi_U)^2 &\mapsto [a_1X_1 + \dots + a_nX_n] \mod (\ker \pi_A)^2. \end{aligned}$$

Elements in the kernel of this map are either generated by  $X_i^2$  s.t. they become  $0 \pmod{(\ker \pi_A)^2}$  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 3.4.** We now compute  $\phi_A$  where  $A$  was defined in example 3.1. 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 3.4.** Let  $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ . Then

$$\eta_A := \pi_A(\text{Ann}_A(\ker \pi_A))$$

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

**Example 3.5.** We now compute  $\eta_U$  for  $U$  from example 3.2.

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

**Lemma 3.1.** Let  $\mathfrak{a} \subset \mathcal{O}$  be an ideal. Then

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

*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

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

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 3.6.** We now compute  $\eta_A$  for  $A$  from example 3.1.

$$\begin{aligned} \eta_A &= \pi_A(\text{Ann } \ker \pi_A) \\ &= \pi_A(\text{Ann}\{(0, b) \in \mathcal{O} \times \mathcal{O} \mid b \equiv 0 \pmod{\lambda^n}\}) \\ &= \pi_A(\{(a, 0) \in \mathcal{O} \times \mathcal{O} \mid a \equiv 0 \pmod{\lambda^n}\}) \\ &= \pi_A((\lambda^n) \times \mathcal{O}) \\ &= (\lambda^n) \end{aligned}$$

With these results at hand, we can state

**Theorem 3.1** (Wiles' numerical criterion). *Let  $R \rightarrow T$  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  $R \rightarrow T$  is an isomorphism.

### 3.2 Basic properties of the invariants

In this subsection we prove the equivalence (a)  $\Leftrightarrow$  (b) in theorem 3.1 by investigating the invariants  $\phi_A$  and  $\eta_A$  that we defined last section.

**Lemma 3.2.** *A morphism  $f: A \rightarrow B \in \mathcal{C}_{\mathcal{O}}^{\bullet}$  induces a homomorphism  $\phi_A \rightarrow \phi_B$  of  $\mathcal{O}$ -modules. This induced map is surjective if and only if the morphism  $A \rightarrow B$  is surjective.*

*Proof.* We have the commutative diagram

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

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

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

In order to see that  $\tilde{f}: \phi_A \rightarrow \phi_B$  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  $A \rightarrow B$  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  $f: \ker \pi_A \rightarrow \ker \pi_B$  and its concatenation with the projection to  $\phi_B$ ,  $\tilde{f}: \ker \pi_A \rightarrow \ker \pi_B / (\ker \pi_B)^2$  are both surjective. In total, we obtain a surjective homomorphism  $\tilde{f}: \phi_A \rightarrow \phi_B$ .

Now, let the induced map  $\phi_A \rightarrow \phi_B$  be surjective. Consider the ideal  $\mathfrak{a} = \mathfrak{m}_A B \subset B$ . As  $B$  is a local ring with maximal ideal  $\mathfrak{m}_B$ , by definition  $\mathfrak{a} \subset \mathfrak{m}_B$ . We know by assumption that  $\ker \pi_A / (\ker \pi_A)^2 \rightarrow \ker \pi_B / (\ker \pi_B)^2$  is surjective. **Why is now  $\mathfrak{a} = \mathfrak{m}_B$ ? Why is  $B$  a finitely generated  $A$ -module?** The  $A/\mathfrak{m}_A = k$ -module  $B/\mathfrak{m}_A B = B/\mathfrak{m}_B \cong k$  is obviously generated by 1. Therefore, by Nakayama's Lemma, the finitely generated  $A$ -module  $B$  is also generated by 1, i.e. the map  $A \rightarrow B$  is surjective.  $\square$

**Corollary 3.1.**  *$A \rightarrow B$  is surjective if and only if*

$$\phi_A \geq \phi_B.$$

**Lemma 3.3.** *If  $f: A \rightarrow B$  is surjective, then*

$$\eta_A \subset \eta_B, \quad \text{i.e.,} \quad \#(\mathcal{O}/\eta_A) \geq \#(\mathcal{O}/\eta_B). \quad (1)$$

*Proof.* As we have seen in the proof of lemma 3.2, a surjective map  $f$  induces a surjective map on the kernels,  $f: \ker \pi_A \rightarrow \ker \pi_B$ . Now let  $x \in \text{Ann}_A \ker \pi_A$ , i.e.  $x \cdot a = 0 \quad \forall a \in \ker \pi_A$ . 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,  $f(x) \in \text{Ann}_B \ker \pi_B$  and we obtain a map

$$\tilde{f}: \text{Ann}_A \ker \pi_A \rightarrow \text{Ann}_B \ker \pi_B.$$

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

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

we get

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

as desired.  $\square$

**Lemma 3.4.** *Let  $A \in \mathcal{C}_{\mathcal{O}}$ . Then*

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

*Proof.* We have  $\#M = \#(\mathcal{O}/\text{Fitt}_{\mathcal{O}}(M))$  for finite  $\mathcal{O}$ -modules and

$$\text{Fitt}_R(M) \subset \text{Ann}_R(M)$$



for any  $R$ -module  $M$ . Furthermore, if  $M$  is a finitely generated  $A$ -module for  $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ , then:

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

and

$$\phi_A = \ker \pi_A \otimes_A \mathcal{O},$$

where  $\mathcal{O}$  becomes an  $A$ -module via the map  $\pi_A: A \rightarrow \mathcal{O}$ . Bringing all this together, we get

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

with  $M = \ker \pi_A$  it follows

$$\begin{aligned} &= \pi_A(\text{Fitt}_A(\ker \pi_A)) \\ &\subset \pi_A(\text{Ann}_A(\ker \pi_A)) \\ &= \eta_A \end{aligned}$$

Using  $\#M = \#(\mathcal{O}/\text{Fitt}_{\mathcal{O}}(M))$  for  $M = \phi_A$ , we finally obtain

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

□

**Proposition 3.1.** *(a)  $\Leftrightarrow$  (b) in theorem 3.1.*

*Proof.* By assumption,  $R \rightarrow T$  is a surjective morphism in  $\mathcal{C}_{\mathcal{O}}^{\bullet}$ . With corollary 3.1 it follows that  $\#\phi_R \geq \#\phi_T$ . lemma 3.4 tells us that  $\#\phi_T \geq \#(\mathcal{O}/\eta_T)$ . The inequalities combine to

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

(a)  $\Rightarrow$  (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)  $\Rightarrow$  (a) Obvious.

□

### 3.3 Regular sequences and the Koszul complex

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

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

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.

**Definition 3.5** (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 3.6** (system of parameters). Let  $x_1, \dots, x_n$  generate a primary ideal of  $R$ . If  $n = \dim R$  then  $x_1, \dots, x_n$  is called a system of parameters.

**Definition 3.7** (regular sequence). A sequence  $(x_1, \dots, x_n)$  is said to be a regular sequence if  $\forall i = 1, \dots, n$ :

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

**Lemma 3.5.** *The sequence  $(f_1, \dots, f_n, \lambda)$  is a system of parameters for  $U$  (cf. example 3.2).*

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

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

so by definition of the dimension we get  $\dim U \geq n + 1$ . Let  $\mathfrak{m} = (\lambda, X_1, \dots, X_n)$ . 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 3.1), the above expression evaluates to  $n + 1$  and taking both inequalities together we obtain  $\dim U = n + 1$ . It remains to show that  $(f_1, \dots, f_n, \lambda)$  generate a primary ideal of  $U$ .  $U$  is local and therefore the quotient ring

$$\tilde{U} := U/(f_1, \dots, f_n, \lambda)$$

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  $A = U/(f_1, \dots, f_n)$  is a finitely generated  $\mathcal{O}$ -module, we can find  $(x_1, \dots, x_N)$  that generate  $A$  as  $\mathcal{O}$ -module. These  $x_i$  then generate  $\tilde{U}$  as a  $k$ -vector space. Every element in the maximal ideal of  $\tilde{U}$  is nilpotent **because ??**  $\square$

**Lemma 3.6.** *The sequence  $(f_1, \dots, f_n)$  is a regular sequence for  $U$ .*

*Proof.* The sequence  $(\lambda, X_1, \dots, X_n)$  is a regular sequence for  $U$  because  $U/\lambda = k[[X_1, \dots, X_n]]$  and  $U/(\lambda, X_1, \dots, X_{i-1}) = k[[X_i, \dots, X_n]]$  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 length of any regular sequence in  $U$ ) is bigger than the length of the particular regular sequence  $(\lambda, X_1, \dots, X_n)$ . In total we get  $\text{depth } U \geq \dim U$ , because  $(\lambda, X_1, \dots, X_n)$  is a system of parameters as well. In general, we have  $\text{depth } R \leq \dim R$  for a noetherian local ring  $R$ , so combined we have

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

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

### 3.4 Complete intersections and the Gorenstein condition

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 3.1. Although there is a very general notion of Gorenstein rings, for the purpose of this proof we only need a special case,

**Definition 3.8.** Let  $A \in \mathcal{C}_{\mathcal{O}}$  be finite flat.  $A$  is called Gorenstein, if there is an isomorphism of  $A$ -modules

$$\Psi: \text{Hom}_{\mathcal{O}}(A, \mathcal{O}) \cong A.$$

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

$$\text{Hom}_{\mathcal{O}}(A, \mathcal{O}) \rightarrow A.$$

We start with some useful constructions and conventions.

*Notation.* For any ring  $R$  write  $R[[\underline{X}]] := R[[X_1, \dots, X_n]]$ .

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

$$\alpha: \mathcal{O}[[\underline{X}]] \rightarrow A = \mathcal{O}[[\underline{X}]]/(f_1, \dots, f_n),$$

and let

$$\beta: A[[\underline{X}]] \rightarrow A$$

be the natural map which sends  $X_i$  to  $a_i$ . The sequence  $g_i = (X_i - a_i)$  generates the kernel of  $\beta$ . **Why?** View the  $f_i$  as polynomials in  $A[[\underline{X}]]$  via the inclusion  $\mathcal{O} \hookrightarrow A$ . Then  $\forall i = 1, \dots, n$ :

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

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

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

where  $M$  is an  $n \times n$  matrix with coefficients in  $A[[\underline{X}]]$ . Let  $D = \det(M) \in A[[\underline{X}]]$ .

The projection  $\mathcal{O}[[\underline{X}]] \rightarrow A$  induces an  $\mathcal{O}[[\underline{X}]]$ -module structure on  $A$ .

**Lemma 3.7.** *The map*

$$\begin{aligned} \Phi: \text{Hom}_{\mathcal{O}}[[\underline{X}]](A[[\underline{X}]], \mathcal{O}[[\underline{x}]]) &\rightarrow A \\ f &\mapsto \alpha(f(D)) \end{aligned}$$

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

*Proof.* As shown in lemma 3.6,  $(\underline{f}) = (f_1, \dots, f_n)$  is a regular sequence for  $\mathcal{O}[[\underline{X}]]$ . In the ring  $A[[\underline{X}]]/(X_1 - a_1, \dots, X_{i-1} - a_{i-1})$   $\square$