Fermat's Last Theorem

Josua Kugler

July 25, 2022

Contents

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 valutation ring (DVR), i.e. $\mathcal{O}$ is a local, noetherian Dedekind ring with maximal ideal λ. It is complete with resp server usedect to the λ-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

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

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

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi_A"'] & & B \arrow[dl, "\pi_B"] \\ & \mathcal{O} & \end{tikzcd}.$$

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 π_A is given by $\pi_A(a,b) = a$.

Proof. Consider the map

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

ϕ 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 ϕ just takes the constant term. As $\mathcal{O}$ is complete with respect to the λ-adic topology, the map $\tilde{\phi}_2\colon \mathcal{O}[[T]] \to \mathcal{O},\ f \mapsto f(\lambda^n)$ is clearly welldefined and thus ϕ 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

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

ϕ 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. (λ, 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 (λ, 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 (λ, 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 (λ, 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 (λ, 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. □

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

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

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

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. □

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

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

where $\ker \pi_A = (a_1, \dots, a_n)$ and π_U is given by $f \mapsto f(0)$. As $(X_1, \dots, X_n)$ generate the kernel of π_U, this is a map in $\mathcal{C}_{\mathcal{O}}^{\bullet}$. 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 $A \cong \mathcal{O} \oplus \ker \pi_A$ and $A[[X_1, \dots, X_n]] \cong A \oplus \ker \pi_A$. Φ by definition induces an equality on the first component, a surjection on the second and therefore is surjective on the direct sum. □

Definition 3.3. 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 though 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 $\overline{f} \in \phi_U$ by cutting of 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 $\phi_A = \phi_U/(\overline{f_1}, \dots, \overline{f_n})$. As a quotient of ϕ_U its a finitely generated $\mathcal{O}$-module.*

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

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

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 Φ welldefined, we can conclude that $X_i \in \ker \pi_A \implies X_i^2 \in (\ker \pi_A)^2$ and therefore Φ is also surjective and $(\ker \pi_U)^2 \subset \ker \Phi$.

With this knowledge we get a welldefined surjective map

$$\begin{gathered}\tilde{\Phi}\colon \phi_U \to \phi_A \\ a_1X_1 + \dots + a_nX_n \mod (\ker \pi_U)^2 \mapsto [a_1X_1 + \dots + a_nX_n] \mod (\ker \pi_A)^2.\end{gathered}$$

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 3.4. We now compute ϕ_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

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

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

Example 3.5. We now compute η_U for U from example 3.2.

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

Lemma 3.1. *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 λ 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 3.6. We now compute η_A for A from example 3.1.

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

With these results at hand, we can state

Theorem 3.1 (Wiles' numerical criterion)**.** *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.

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 ϕ_A and η_A that we defined last section.

Lemma 3.2. *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.*

Proof. We have the commutative diagram

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, two heads, "\pi_A"'] & & B \arrow[dl, two heads, "\pi_B"] \\ & \mathcal{O} & \end{tikzcd} .$$

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 ϕ_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.

Why is A complete with respect to the $\ker\pi_A$-adic topology? 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, $\ker\pi_A = \langle a_1,\dots,a_m\rangle$ because A is noetherian. As $\ker\pi_A \to (\ker\pi_B)/(\ker\pi_B)^2$ is surjective, we have

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

As A is complete and I is separated with respect to the I-adic topology as a submodule of B, we can apply Nakayama's Lemma as in Mat, 8.4. It follows that the images $\langle f(a_1),\dots,f(a_m)\rangle$ generate $\ker\pi_B$ as a B-module. We already know that $f(\ker\pi_A)\cdot B \subset \ker\pi_B$. Together 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 3.1. *$A \to B$ is surjective if and only if*

$$\phi_A \geq \phi_B.$$

Lemma 3.3. *If $f\colon A \to B$ is surjective, then*

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

Proof. As we have seen in the proof of lemma 3.2, a surjective map f induces a surjective map on the kernels, $f\colon \ker \pi_A \to \ker \pi_B$. 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

$$\begin{tikzcd} \operatorname{Ann}_A \ker \pi_A \arrow[rr, "\tilde{f}"] \arrow[dr, two heads, "\pi_A"'] & & \operatorname{Ann}_B \ker \pi_B \arrow[dl, two heads, "\pi_B"] \\ & \mathcal{O} & \end{tikzcd},$$

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 3.5. 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 3.4. *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 3.3 (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 π_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 3.4 (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 $n_1 \geq dots \geq n_s \in \mathbb{N}$ 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, $\operatorname{Fitt}_R(M) = 0$ 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 $\operatorname{Fitt}_{\mathcal{O}}(M) = \lambda^{n_1} \cdot \cdots \cdot \lambda^{n_s} = \lambda^{n_1 + \cdots + n_s}$.

Corollary 3.2. *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

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

From the proof of lemma 3.1 it follows that

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

and

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

$\square$

Lemma 3.5. *Let $A \in \mathcal{C}_{\mathcal{O}}$ **s.t.** ϕ_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 3.3. Applying lemma 3.4 to the RHS, we get

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

As ϕ_A is finite, we can apply corollary 3.2 to $M = \phi_A$ and obtain

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

$\square$

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

Proof. By assumption, $R \to T$ is a surjective morphism in $\mathcal{C}_{\mathcal{O}}^{\bullet}$. With corollary 3.1 it follows that $\#\phi_R \geq \#\phi_T$. lemma 3.5 tells us that $\#\phi_T \geq \#(\mathcal{O}/\eta_T)$. The inequalities combine to

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

(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.

$\square$

3.3 Regular sequences and the Koszul complex

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

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

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.

Definition 3.6 (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 3.7 (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 3.6. *The sequence $(f_1, \ldots, f_n, \lambda)$ 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
$$(0) \subsetneq (\lambda) \subsetneq \cdots \subsetneq (\lambda, X_1, \ldots, X_n),$$
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 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 $(f_1, \ldots, f_n, \lambda)$ generate a primary ideal of U. U is local and therefore the quotient ring
$$\tilde{U} := U/(f_1, \ldots, f_n, \lambda)$$
is local as well. Also, $\tilde{U}$ is a k-vector space (because it's an $\mathcal{O}$-module and λ-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. $\square$

Definition 3.8 (regular sequence)**.** 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 3.7. *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 $(f_1, \dots, f_n, \lambda)$ 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. □

Corollary 3.3. *Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$ be finitely generated and of the form*

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

Then A is flat.

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

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

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 λ and obtain $g = 0 \mod (f_1, \dots, f_n)$, a contradiction. Let i_0 be the biggest such i. In the proof of lemma 3.6 we have never used that A is flat, only that it is finitely generated. Therefore we know that $\lambda, f_1, \dots, f_n$ is a system of parameters for U. From the proof of lemma 3.7 (where we also haven't used that A is flat) we can deduce that $\lambda, f_1, \dots, f_n$ is also a regular sequence for U and, a fortiori, f_{i_0} is not a zero-divisor in $U/(\lambda, f_1, \dots, f_{i_0 - 1})$. 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 $(\lambda, f_1, \dots, f_{i_0 - 1})$ we obtain

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

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

Definition 3.9 (Koszul complex)**.** The Koszul complex associated to a sequence $\underline{x} = (x_1, \dots, x_n)$ 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 3.5. *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.

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 3.10. 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 β. View the f_i as polynomials in $A[[\underline{X}]]$ via the inclusion $O \hookrightarrow A$. Then $\forall i = 1, \ldots, n$:

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

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 3.8. *The map*

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

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

Proof. As shown in lemma 3.7, $(\underline{f}) = (f_1, \ldots, f_n)$ 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

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

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

1. is a morphism of complexes,
2. induces the identity on $A = H_0(\underline{f}, \mathcal{O}[[\underline{X}]])$
3. and satisfies
$$\Phi_n(u_1 \wedge \dots \wedge u_n) = D \cdot v_1 \wedge \dots \wedge v_n.$$

1. **Φ is a morphism of complexes.** It is clear by definition that Φ is welldefined on every level. We have to show that Φ commutes with the differentials of the complex,

$$\begin{aligned}
\Phi_{p-1}(d(u_{i_1} \wedge \ldots \wedge u_{i_p})) &= \Phi_{p-1}\left(\sum_{t=1}^{p}(-1)^t x_{i_t} u_{i_1} \wedge \ldots \wedge \widehat{u_{i_t}} \wedge \ldots \wedge u_{i_p}\right) \\
&= \sum_{t=1}^{p}(-1)^t x_{i_t} \Phi_1(u_{i_1}) \wedge \ldots \wedge \widehat{\Phi_1(u_{i_t})} \wedge \ldots \wedge \Phi_1(u_{i_p}) \\
&= d(\Phi_1(u_{i_1}) \wedge \dots \wedge \Phi_1(u_{i_p})) \\
&= d(\Phi_p(u_{i_1} \wedge \dots \wedge u_{i_p})).
\end{aligned}$$

2. **Φ induces the identity on** $A = H_0(\underline{f}, \mathcal{O}[[\underline{X}]])$
We have the following commutative diagram

$$\begin{array}{ccccc}
\bigoplus_{i=1}^n u_i \mathcal{O}[[\underline{X}]] = K_1(\underline{f}, \mathcal{O}[[\underline{X}]]) & \xrightarrow{d_1} & K_0(\underline{f}, \mathcal{O}[[\underline{X}]]) = \mathcal{O}[[\underline{X}]] & \xrightarrow{d_0} & 0 \\
\downarrow \Phi_1 & & \downarrow \Phi_0 & & \\
\bigoplus_{i=1}^n v_i A[[\underline{X}]] = K_1(\underline{g}, A[[\underline{X}]]) & \xrightarrow{d_1} & K_0(\underline{g}, A[[\underline{X}]]) = A[[\underline{X}]] & \xrightarrow{d_0} & 0
\end{array}.$$

As
$$H_0(\underline{f}, \mathcal{O}[[\underline{X}]]) = \frac{\ker d_0}{\operatorname{im} d_1} = \frac{\mathcal{O}[[\underline{X}]]}{(f_1, \dots, f_n)}$$
and
$$H_0(\underline{g}, A[[\underline{X}]]) = \frac{\ker d_0}{\operatorname{im} d_1} = \frac{A[[\underline{X}]]}{(g_1, \dots, g_n)}$$
we can take a look at the map

$$\mathcal{O}[[\underline{X}]] \to \frac{A[[\underline{X}]]}{(X_1 - a_1, \dots, X_n - a_n)} = A.$$

This map sends X_i to $a_i \in A$. By definition of $A = \mathcal{O}[[\underline{X}]]/(f_1, \dots, f_n)$ and a_i as image of X_i under α this is exactly the map α. **Really?** Hence, the induced map

$$A = \mathcal{O}[[\underline{X}]]/(f_1, \dots, f_n) \to \frac{A[[\underline{X}]]}{(X_1 - a_1, \dots, X_n - a_n)} = A$$

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

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

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. As this map is then uniquely defined by skew linearity, we get that Φ needs to be a homotopy equivalence. **might be not so uniquely defined?** 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

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

$$K_n(\underline{g}) = \bigoplus_{i=1}^{n} A[[\underline{X}]] \cdot u_1 \wedge \cdots \wedge u_n \cong A[[\underline{X}]].$$

Therefore, we can make the identification

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

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 $\varphi \in \mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(K_{n-1}(\underline{f}), \mathcal{O}[[\underline{X}]])$. 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 φ 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

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

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

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

Φ takes a $\mathcal{O}[[\underline{X}]]$-linear map and applies Φ_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 $\mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(\mathcal{O}[[\underline{X}]], \mathcal{O}[[\underline{X}]]) \cong \mathcal{O}[[\underline{X}]]$ 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 α. In total we get

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

as desired. □

Lemma 3.9. *Let*

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

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

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

where in the last step we have used the linearity of $\tilde{f}$ and α. Now choose $a' \in \alpha^{-1}(a) \subset \mathcal{O}[[\underline{X}]]$, as α 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. Ψ is surjective. Let $f_1, \dots, f_r$ be a $\mathcal{O}$-basis of $\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$. **Why is that a free module?** Then, the extended maps $\tilde{f}_1, \dots \tilde{f}_r$ form a basis for $\mathrm{Hom}_{\mathcal{O}[[X]]}(A[[\underline{X}]], \mathcal{O}[[\underline{X}]])$. 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, $\forall a \in A\colon \exists p_1, \dots, p_r \in \mathcal{O}[[\underline{X}]]$ s.t.

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

Now we can use the linearity of the involved maps,

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

by using linearity multiple times.

3. Ψ 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 (**Why?**), the lemma follows.

$\square$