Fermat's Last Theorem

Josua Kugler

July 4, 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

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 respect to the λ-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 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

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

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.

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.

Definition 3.4. Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$. Then

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

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

Lemma 3.1. *Let $A \in \mathcal{C}_{\mathcal{O}}^{\bullet}$.*

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

Proof. As $0 \neq \eta_A$ is an ideal in the DVR $\mathcal{O}$, $\eta_A = \lambda^n$ for some $n \in \mathbb{N}$ where λ is the maximal ideal in O. Therefore, $\mathcal{O}/\eta_T = \mathcal{O}/\lambda^n$.

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 $\#\mathcal{O}/\eta_A = \#\mathcal{O}/\lambda^n = (\#k)^n$. □

With these definitions 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 $\eta_T \neq 0$. 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 ϕ_A and η_A

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 week.