A brief history of perfectoid spaces

Kiran S. Kedlaya

Department of Mathematics
University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

AMS Western Sectional Meeting
San Francisco State University
San Francisco, October 25, 2014

WHAT IS... a perfectoid space?

Short answer: see B. Bhatt, *Notices of the AMS*, October 2014.

Slightly longer answer: perfectoid spaces are a new class of objects in arithmetic algebraic geometry which provide a strong link between geometry in characteristic 0 and characteristic p.

This talk will not attempt to define perfectoid spaces. Instead, I will trace the genesis of these ideas through a series of key developments in arithmetic geometry over the past 50 years.

WHAT IS... a perfectoid space?

Short answer: see B. Bhatt, *Notices of the AMS*, October 2014.

Slightly longer answer: perfectoid spaces are a new class of objects in arithmetic algebraic geometry which provide a strong link between geometry in characteristic 0 and characteristic p.

This talk will not attempt to define perfectoid spaces. Instead, I will trace the genesis of these ideas through a series of key developments in arithmetic geometry over the past 50 years.

WHAT IS... a perfectoid space?

Short answer: see B. Bhatt, *Notices of the AMS*, October 2014.

Slightly longer answer: perfectoid spaces are a new class of objects in arithmetic algebraic geometry which provide a strong link between geometry in characteristic 0 and characteristic p.

This talk will not attempt to define perfectoid spaces. Instead, I will trace the genesis of these ideas through a series of key developments in arithmetic geometry over the past 50 years.

Contents

Ramification in geometry

Consider the following map from the complex plane to itself:

$$z \mapsto z^2.$$

For most points $z \in \mathbb{C}$, the inverse image of z consists of two distinct points. In fact, one can even find a neighborhood U of z whose inverse image consists of two disjoint copies of U.

However, for $z = 0$, the inverse image is a single point, and the local structure of neighborhoods of these points and their inverse images is a bit more complicated.

If we replace $\mathbb{C}$ with a field which is not algebraically closed, like $\mathbb{Q}$, then even when $t \neq 0$ the two points can fail to separate; but this will not bother us too much.

Ramification in geometry

Consider the following map from the complex plane to itself:

$$z \mapsto z^2.$$

For most points $z \in \mathbb{C}$, the inverse image of z consists of two distinct points. In fact, one can even find a neighborhood U of z whose inverse image consists of two disjoint copies of U.

However, for $z = 0$, the inverse image is a single point, and the local structure of neighborhoods of these points and their inverse images is a bit more complicated.

If we replace $\mathbb{C}$ with a field which is not algebraically closed, like $\mathbb{Q}$, then even when $t \neq 0$ the two points can fail to separate; but this will not bother us too much.

Ramification in geometry

Consider the following map from the complex plane to itself:

$$z \mapsto z^2.$$

For most points $z \in \mathbb{C}$, the inverse image of z consists of two distinct points. In fact, one can even find a neighborhood U of z whose inverse image consists of two disjoint copies of U.

However, for $z = 0$, the inverse image is a single point, and the local structure of neighborhoods of these points and their inverse images is a bit more complicated.

If we replace $\mathbb{C}$ with a field which is not algebraically closed, like $\mathbb{Q}$, then even when $t \neq 0$ the two points can fail to separate; but this will not bother us too much.

Ramification in geometry

Consider the following map from the complex plane to itself:

$$z \mapsto z^2.$$

For most points $z \in \mathbb{C}$, the inverse image of z consists of two distinct points. In fact, one can even find a neighborhood U of z whose inverse image consists of two disjoint copies of U.

However, for $z = 0$, the inverse image is a single point, and the local structure of neighborhoods of these points and their inverse images is a bit more complicated.

If we replace $\mathbb{C}$ with a field which is not algebraically closed, like $\mathbb{Q}$, then even when $t \neq 0$ the two points can fail to separate; but this will not bother us too much.

Ramification in algebra(ic geometry)

Using formal power series, we can give an algebraic reinterpretation of the previous discussion:

$$\frac{\mathbb{Q}[\![z-t]\!][x]}{(x^2-z)} \cong \begin{cases} \mathbb{Q}[\![x-\sqrt{t}]\!] \oplus \mathbb{Q}[\![x+\sqrt{t}]\!] & (t \neq 0, t = \square) \\ \mathbb{Q}(\sqrt{t})[\![z-t]\!] & (t \neq 0, t \neq \square) \\ \mathbb{Q}[\![x]\!] & (t = 0). \end{cases}$$

The key point: $z-t$ vanishes to order 1 in each factor when $t=1$, but to order 2 when $t=0$. Note that in $\mathbb{Q}[\![x-\sqrt{t}]\!]$ we have

$$\begin{aligned} \frac{1}{x+\sqrt{t}} &= \frac{1/(2\sqrt{t})}{1+(x-\sqrt{t})/(2\sqrt{t})} \\ &= \frac{1}{2\sqrt{t}} - \frac{x-\sqrt{t}}{(2\sqrt{t})^2} + \frac{(x-\sqrt{t})^2}{(2\sqrt{t})^3} - \cdots . \end{aligned}$$

Ramification in algebra(ic geometry)

Using formal power series, we can give an algebraic reinterpretation of the previous discussion:

$$\frac{\mathbb{Q}[\![z-t]\!][x]}{(x^2-z)} \cong \begin{cases} \mathbb{Q}[\![x-\sqrt{t}]\!] \oplus \mathbb{Q}[\![x+\sqrt{t}]\!] & (t \neq 0, t = \square) \\ \mathbb{Q}(\sqrt{t})[\![z-t]\!] & (t \neq 0, t \neq \square) \\ \mathbb{Q}[\![x]\!] & (t = 0). \end{cases}$$

The key point: $z-t$ vanishes to order 1 in each factor when $t=1$, but to order 2 when $t=0$. Note that in $\mathbb{Q}[\![x-\sqrt{t}]\!]$ we have

$$\begin{aligned} \frac{1}{x+\sqrt{t}} &= \frac{1/(2\sqrt{t})}{1+(x-\sqrt{t})/(2\sqrt{t})} \\ &= \frac{1}{2\sqrt{t}} - \frac{x-\sqrt{t}}{(2\sqrt{t})^2} + \frac{(x-\sqrt{t})^2}{(2\sqrt{t})^3} - \cdots . \end{aligned}$$

Ramification in algebra(ic geometry)

Using formal power series, we can give an algebraic reinterpretation of the previous discussion:

$$\frac{\mathbb{Q}[\![z-t]\!][x]}{(x^2-z)} \cong \begin{cases} \mathbb{Q}[\![x-\sqrt{t}]\!] \oplus \mathbb{Q}[\![x+\sqrt{t}]\!] & (t \neq 0, t = \square) \\ \mathbb{Q}(\sqrt{t})[\![z-t]\!] & (t \neq 0, t \neq \square) \\ \mathbb{Q}[\![x]\!] & (t = 0). \end{cases}$$

The key point: $z - t$ vanishes to order 1 in each factor when $t = 1$, but to order 2 when $t = 0$. Note that in $\mathbb{Q}[\![x-\sqrt{t}]\!]$ we have

$$\begin{aligned} \frac{1}{x+\sqrt{t}} &= \frac{1/(2\sqrt{t})}{1+(x-\sqrt{t})/(2\sqrt{t})} \\ &= \frac{1}{2\sqrt{t}} - \frac{x-\sqrt{t}}{(2\sqrt{t})^2} + \frac{(x-\sqrt{t})^2}{(2\sqrt{t})^3} - \cdots. \end{aligned}$$

Ramification in number theory

Let K be a number field, i.e., a field which is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is denoted $\mathfrak{o}_K$. E.g., if

$$K = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}, \text{ then } \mathfrak{o}_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

The analogue of a ring of formal power series (resp. formal Laurent series) is the completion of $\mathfrak{o}_K$ with respect to a prime ideal $\mathfrak{p}$, denoted $\mathfrak{o}_{K_\mathfrak{p}}$ (resp. the fraction field of this completion, denoted $K_\mathfrak{p}$). Elements of $\mathfrak{o}_K$ can be viewed as coherent sequences of residue classes modulo $\mathfrak{p}$, modulo $\mathfrak{p}^2$, etc.

E.g., for $K = \mathbb{Q}$, $\mathfrak{p} = (p)$, $\mathfrak{o}_{K_\mathfrak{p}} = \mathbb{Z}_p$ is Hensel's ring of *p-adic numbers* and $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. Formally, elements of $\mathbb{Z}_p$ may be viewed as "infinite base p numerals"

$$a_0 + a_1 p + a_2 p^2 + \cdots, \qquad a_i \in \{0, \ldots, p-1\}.$$

Ramification in number theory

Let K be a number field, i.e., a field which is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is denoted $\mathfrak{o}_K$. E.g., if

$$K = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}, \text{ then } \mathfrak{o}_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

The analogue of a ring of formal power series (resp. formal Laurent series) is the completion of $\mathfrak{o}_K$ with respect to a prime ideal $\mathfrak{p}$, denoted $\mathfrak{o}_{K_\mathfrak{p}}$ (resp. the fraction field of this completion, denoted $K_\mathfrak{p}$). Elements of $\mathfrak{o}_K$ can be viewed as coherent sequences of residue classes modulo $\mathfrak{p}$, modulo $\mathfrak{p}^2$, etc.

E.g., for $K = \mathbb{Q}$, $\mathfrak{p} = (p)$, $\mathfrak{o}_{K_\mathfrak{p}} = \mathbb{Z}_p$ is Hensel's ring of *p-adic numbers* and $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. Formally, elements of $\mathbb{Z}_p$ may be viewed as "infinite base p numerals"

$$a_0 + a_1 p + a_2 p^2 + \cdots, \qquad a_i \in \{0, \dots, p-1\}.$$

Ramification in number theory

Let K be a number field, i.e., a field which is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is denoted $\mathfrak{o}_K$. E.g., if

$$K = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}, \text{ then } \mathfrak{o}_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

The analogue of a ring of formal power series (resp. formal Laurent series) is the completion of $\mathfrak{o}_K$ with respect to a prime ideal $\mathfrak{p}$, denoted $\mathfrak{o}_{K_\mathfrak{p}}$ (resp. the fraction field of this completion, denoted $K_\mathfrak{p}$). Elements of $\mathfrak{o}_K$ can be viewed as coherent sequences of residue classes modulo $\mathfrak{p}$, modulo $\mathfrak{p}^2$, etc.

E.g., for $K = \mathbb{Q}$, $\mathfrak{p} = (p)$, $\mathfrak{o}_{K_\mathfrak{p}} = \mathbb{Z}_p$ is Hensel's ring of *p-adic numbers* and $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. Formally, elements of $\mathbb{Z}_p$ may be viewed as "infinite base p numerals"

$$a_0 + a_1 p + a_2 p^2 + \cdots, \qquad a_i \in \{0, \dots, p-1\}.$$

Ramification in number theory (continued)

What does $\mathbb{Z}_p[i]$ (or more precisely $\mathbb{Z}_p[i]/(i^2+1)$) look like?

- If $p \equiv 1 \pmod 4$, then it splits as two copies of $\mathbb{Z}_p$. For example, if $p = 5$, then $2 + i$ is divisible by 5 in one copy of $\mathbb{Z}_5$ but is invertible in the other.
- If $p \equiv 3 \pmod 4$, then $\mathbb{Z}_p[i]$ is an integral domain, and every nonzero ideal is a power of (p).
- If $p = 2$, then $\mathbb{Z}_p[i]$ is again an integral domain, but now the ideal $(1 + i)$ is not a power of (2).

We say that 2 is the unique *ramified prime* of the extension $\mathbb{Q}(i)/\mathbb{Q}$ of number fields. Similarly, for any finite extension L/K of number fields, we can identify a finite collection of *ramified prime ideals* of $\mathfrak{o}_K$ (or more precisely, of $\mathfrak{o}_L$).

Ramification in number theory (continued)

What does $\mathbb{Z}_p[i]$ (or more precisely $\mathbb{Z}_p[i]/(i^2+1)$) look like?

- If $p \equiv 1 \pmod 4$, then it splits as two copies of $\mathbb{Z}_p$. For example, if $p = 5$, then $2 + i$ is divisible by 5 in one copy of $\mathbb{Z}_5$ but is invertible in the other.
- If $p \equiv 3 \pmod 4$, then $\mathbb{Z}_p[i]$ is an integral domain, and every nonzero ideal is a power of (p).
- If $p = 2$, then $\mathbb{Z}_p[i]$ is again an integral domain, but now the ideal $(1 + i)$ is not a power of (2).

We say that 2 is the unique *ramified prime* of the extension $\mathbb{Q}(i)/\mathbb{Q}$ of number fields. Similarly, for any finite extension L/K of number fields, we can identify a finite collection of *ramified prime ideals* of $\mathfrak{o}_K$ (or more precisely, of $\mathfrak{o}_L$).

Ramification in number theory (continued)

What does $\mathbb{Z}_p[i]$ (or more precisely $\mathbb{Z}_p[i]/(i^2+1)$) look like?

- If $p \equiv 1 \pmod 4$, then it splits as two copies of $\mathbb{Z}_p$. For example, if $p = 5$, then $2 + i$ is divisible by 5 in one copy of $\mathbb{Z}_5$ but is invertible in the other.
- If $p \equiv 3 \pmod 4$, then $\mathbb{Z}_p[i]$ is an integral domain, and every nonzero ideal is a power of (p).
- If $p = 2$, then $\mathbb{Z}_p[i]$ is again an integral domain, but now the ideal $(1 + i)$ is not a power of (2).

We say that 2 is the unique *ramified prime* of the extension $\mathbb{Q}(i)/\mathbb{Q}$ of number fields. Similarly, for any finite extension L/K of number fields, we can identify a finite collection of *ramified prime ideals* of $\mathfrak{o}_K$ (or more precisely, of $\mathfrak{o}_L$).

Ramification in number theory (continued)

What does $\mathbb{Z}_p[i]$ (or more precisely $\mathbb{Z}_p[i]/(i^2+1)$) look like?

- If $p \equiv 1 \pmod 4$, then it splits as two copies of $\mathbb{Z}_p$. For example, if $p = 5$, then $2 + i$ is divisible by 5 in one copy of $\mathbb{Z}_5$ but is invertible in the other.
- If $p \equiv 3 \pmod 4$, then $\mathbb{Z}_p[i]$ is an integral domain, and every nonzero ideal is a power of (p).
- If $p = 2$, then $\mathbb{Z}_p[i]$ is again an integral domain, but now the ideal $(1+i)$ is not a power of (2).

We say that 2 is the unique *ramified prime* of the extension $\mathbb{Q}(i)/\mathbb{Q}$ of number fields. Similarly, for any finite extension L/K of number fields, we can identify a finite collection of *ramified prime ideals* of $\mathfrak{o}_K$ (or more precisely, of $\mathfrak{o}_L$).

Ramification in number theory (continued)

What does $\mathbb{Z}_p[i]$ (or more precisely $\mathbb{Z}_p[i]/(i^2+1)$) look like?

- If $p \equiv 1 \pmod 4$, then it splits as two copies of $\mathbb{Z}_p$. For example, if $p = 5$, then $2 + i$ is divisible by 5 in one copy of $\mathbb{Z}_5$ but is invertible in the other.
- If $p \equiv 3 \pmod 4$, then $\mathbb{Z}_p[i]$ is an integral domain, and every nonzero ideal is a power of (p).
- If $p = 2$, then $\mathbb{Z}_p[i]$ is again an integral domain, but now the ideal $(1 + i)$ is not a power of (2).

We say that 2 is the unique *ramified prime* of the extension $\mathbb{Q}(i)/\mathbb{Q}$ of number fields. Similarly, for any finite extension L/K of number fields, we can identify a finite collection of *ramified prime ideals* of $\mathfrak{o}_K$ (or more precisely, of $\mathfrak{o}_L$).

Contents

Ramification and traces

Let L/K be an extension of number fields, let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$, and let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}_L$ appearing in the prime factorization of $\mathfrak{p}$ (i.e, $\mathfrak{q} \cap \mathfrak{o}_K = \mathfrak{p}$). Then $L_\mathfrak{q}$ is a finite extension of $K_\mathfrak{p}$.

For $x \in L_\mathfrak{q}$, the *trace* of x is the trace of multiplication-by-x as a $K_\mathfrak{p}$-linear transformation on $L_\mathfrak{q}$. (It is also the sum of the Galois conjugates of x.)

Lemma

The trace map takes $\mathfrak{o}_{L_\mathfrak{q}}$ into $\mathfrak{o}_{K_\mathfrak{p}}$, and is surjective if and only if $\mathfrak{q}$ is not a ramified prime.

For example, take $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathfrak{p} = (2)$, $\mathfrak{q} = (1+i)$. Then

$$\mathrm{Trace}(a+bi) = (a+bi) + (a-bi) = 2a$$

so the image of $\mathrm{Trace} : \mathbb{Z}_2[i] \to \mathbb{Z}_2$ lands in the ideal (2). By contrast, if $\mathfrak{p} = (p)$ for $p \equiv 3 \pmod 4$, then 2 is invertible in $\mathbb{Z}_p$; if $p \equiv 1 \pmod 4$, there are two choices for $\mathfrak{q}$, and in both cases $\mathfrak{o}_{L_\mathfrak{q}} \cong \mathfrak{o}_{K_\mathfrak{p}} \cong \mathbb{Z}_p$.

Ramification and traces

Let L/K be an extension of number fields, let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$, and let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}_L$ appearing in the prime factorization of $\mathfrak{p}$ (i.e, $\mathfrak{q} \cap \mathfrak{o}_K = \mathfrak{p}$). Then $L_\mathfrak{q}$ is a finite extension of $K_\mathfrak{p}$.

For $x \in L_\mathfrak{q}$, the *trace* of x is the trace of multiplication-by-x as a $K_\mathfrak{p}$-linear transformation on $L_\mathfrak{q}$. (It is also the sum of the Galois conjugates of x.)

Lemma

The trace map takes $\mathfrak{o}_{L_\mathfrak{q}}$ into $\mathfrak{o}_{K_\mathfrak{p}}$, and is surjective if and only if $\mathfrak{q}$ is not a ramified prime.

For example, take $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathfrak{p} = (2)$, $\mathfrak{q} = (1+i)$. Then

$$\mathrm{Trace}(a+bi) = (a+bi) + (a-bi) = 2a$$

so the image of $\mathrm{Trace} : \mathbb{Z}_2[i] \to \mathbb{Z}_2$ lands in the ideal (2). By contrast, if $\mathfrak{p} = (p)$ for $p \equiv 3 \pmod 4$, then 2 is invertible in $\mathbb{Z}_p$; if $p \equiv 1 \pmod 4$, there are two choices for $\mathfrak{q}$, and in both cases $\mathfrak{o}_{L_\mathfrak{q}} \cong \mathfrak{o}_{K_\mathfrak{p}} \cong \mathbb{Z}_p$.

Ramification and traces

Let L/K be an extension of number fields, let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$, and let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}_L$ appearing in the prime factorization of $\mathfrak{p}$ (i.e, $\mathfrak{q} \cap \mathfrak{o}_K = \mathfrak{p}$). Then $L_\mathfrak{q}$ is a finite extension of $K_\mathfrak{p}$.

For $x \in L_\mathfrak{q}$, the *trace* of x is the trace of multiplication-by-x as a $K_\mathfrak{p}$-linear transformation on $L_\mathfrak{q}$. (It is also the sum of the Galois conjugates of x.)

Lemma

The trace map takes $\mathfrak{o}_{L_\mathfrak{q}}$ into $\mathfrak{o}_{K_\mathfrak{p}}$, and is surjective if and only if $\mathfrak{q}$ is not a ramified prime.

For example, take $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathfrak{p} = (2)$, $\mathfrak{q} = (1+i)$. Then

$$\mathrm{Trace}(a+bi) = (a+bi) + (a-bi) = 2a$$

so the image of $\mathrm{Trace} : \mathbb{Z}_2[i] \to \mathbb{Z}_2$ lands in the ideal (2). By contrast, if $\mathfrak{p} = (p)$ for $p \equiv 3 \pmod 4$, then 2 is invertible in $\mathbb{Z}_p$; if $p \equiv 1 \pmod 4$, there are two choices for $\mathfrak{q}$, and in both cases $\mathfrak{o}_{L_\mathfrak{q}} \cong \mathfrak{o}_{K_\mathfrak{p}} \cong \mathbb{Z}_p$.

Ramification and traces

Let L/K be an extension of number fields, let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$, and let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}_L$ appearing in the prime factorization of $\mathfrak{p}$ (i.e, $\mathfrak{q} \cap \mathfrak{o}_K = \mathfrak{p}$). Then $L_\mathfrak{q}$ is a finite extension of $K_\mathfrak{p}$.

For $x \in L_\mathfrak{q}$, the *trace* of x is the trace of multiplication-by-x as a $K_\mathfrak{p}$-linear transformation on $L_\mathfrak{q}$. (It is also the sum of the Galois conjugates of x.)

Lemma

The trace map takes $\mathfrak{o}_{L_\mathfrak{q}}$ into $\mathfrak{o}_{K_\mathfrak{p}}$, and is surjective if and only if $\mathfrak{q}$ is not a ramified prime.

For example, take $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathfrak{p} = (2)$, $\mathfrak{q} = (1+i)$. Then

$$\mathrm{Trace}(a+bi) = (a+bi) + (a-bi) = 2a$$

so the image of $\mathrm{Trace} : \mathbb{Z}_2[i] \to \mathbb{Z}_2$ lands in the ideal (2). By contrast, if $\mathfrak{p} = (p)$ for $p \equiv 3 \pmod 4$, then 2 is invertible in $\mathbb{Z}_p$; if $p \equiv 1 \pmod 4$, there are two choices for $\mathfrak{q}$, and in both cases $\mathfrak{o}_{L_\mathfrak{q}} \cong \mathfrak{o}_{K_\mathfrak{p}} \cong \mathbb{Z}_p$.

Almost disappearing ramification

Tate discovered that ramification "almost disappears" if one makes certain *infinite* extensions of number fields.

E.g., for any prime p, let $\mathbb{Z}_p[\zeta_{p^\infty}]$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) be the ring obtained from $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) by adjoining primitive p^n-th roots of unity ζ_{p^n} for all n. (Note that $\mathbb{Z}_p[\zeta_{p^\infty}]$ is the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty})$.)

Theorem (example of a theorem of Tate)

Let F be a finite extension of $\mathbb{Q}_p(\zeta_{p^\infty})$. Let $\mathfrak{o}_F$ be the integral closure of $\mathbb{Z}_p$ in F. Then $\mathrm{Trace} : \mathfrak{o}_F \to \mathbb{Q}_p(\zeta_{p^\infty})$ *has image in $\mathbb{Z}_p[\zeta_{p^\infty}]$ and is* **almost** *surjective: its image contains the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

That maximal ideal is generated by $1 - \zeta_{p^n}$ for $n = 1, 2, \dots,$ and

$$(1-\zeta_p)^{p-1} = p \times (\mathrm{unit}), \qquad (1-\zeta_{p^{n+1}})^p = (1-\zeta_{p^n}) \times (\mathrm{unit}).$$

So any element "divisible by p^ϵ for some $\epsilon > 0$" is a trace.

Almost disappearing ramification

Tate discovered that ramification "almost disappears" if one makes certain *infinite* extensions of number fields.

E.g., for any prime p, let $\mathbb{Z}_p[\zeta_{p^\infty}]$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) be the ring obtained from $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) by adjoining primitive p^n-th roots of unity ζ_{p^n} for all n. (Note that $\mathbb{Z}_p[\zeta_{p^\infty}]$ is the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty})$.)

Theorem (example of a theorem of Tate)

Let F be a finite extension of $\mathbb{Q}_p(\zeta_{p^\infty})$. Let $\mathfrak{o}_F$ be the integral closure of $\mathbb{Z}_p$ in F. Then $\mathrm{Trace} : \mathfrak{o}_F \to \mathbb{Q}_p(\zeta_{p^\infty})$ has image in $\mathbb{Z}_p[\zeta_{p^\infty}]$ and is **almost** *surjective: its image contains the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

That maximal ideal is generated by $1 - \zeta_{p^n}$ for $n = 1, 2, \ldots$, and

$$(1-\zeta_p)^{p-1} = p \times (\mathrm{unit}), \qquad (1-\zeta_{p^{n+1}})^p = (1-\zeta_{p^n}) \times (\mathrm{unit}).$$

So any element "divisible by p^ϵ for some $\epsilon > 0$" is a trace.

Almost disappearing ramification

Tate discovered that ramification "almost disappears" if one makes certain *infinite* extensions of number fields.

E.g., for any prime p, let $\mathbb{Z}_p[\zeta_{p^\infty}]$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) be the ring obtained from $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) by adjoining primitive p^n-th roots of unity ζ_{p^n} for all n. (Note that $\mathbb{Z}_p[\zeta_{p^\infty}]$ is the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty})$.)

Theorem (example of a theorem of Tate)

Let F be a finite extension of $\mathbb{Q}_p(\zeta_{p^\infty})$. Let $\mathfrak{o}_F$ be the integral closure of $\mathbb{Z}_p$ in F. Then $\mathrm{Trace} : \mathfrak{o}_F \to \mathbb{Q}_p(\zeta_{p^\infty})$ has image in $\mathbb{Z}_p[\zeta_{p^\infty}]$ and is **almost** *surjective: its image contains the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

That maximal ideal is generated by $1 - \zeta_{p^n}$ for $n = 1, 2, \dots$, and

$$(1 - \zeta_p)^{p-1} = p \times (\text{unit}), \qquad (1 - \zeta_{p^{n+1}})^p = (1 - \zeta_{p^n}) \times (\text{unit}).$$

So any element "divisible by p^ϵ for some $\epsilon > 0$" is a trace.

Almost disappearing ramification

Tate discovered that ramification "almost disappears" if one makes certain *infinite* extensions of number fields.

E.g., for any prime p, let $\mathbb{Z}_p[\zeta_{p^\infty}]$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) be the ring obtained from $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) by adjoining primitive p^n-th roots of unity ζ_{p^n} for all n. (Note that $\mathbb{Z}_p[\zeta_{p^\infty}]$ is the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty})$.)

Theorem (example of a theorem of Tate)

Let F be a finite extension of $\mathbb{Q}_p(\zeta_{p^\infty})$. Let $\mathfrak{o}_F$ be the integral closure of $\mathbb{Z}_p$ in F. Then $\mathrm{Trace} : \mathfrak{o}_F \to \mathbb{Q}_p(\zeta_{p^\infty})$ has image in $\mathbb{Z}_p[\zeta_{p^\infty}]$ and is **almost** *surjective: its image contains the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

That maximal ideal is generated by $1 - \zeta_{p^n}$ for $n = 1, 2, \ldots,$ and

$$(1 - \zeta_p)^{p-1} = p \times (\text{unit}), \qquad (1 - \zeta_{p^{n+1}})^p = (1 - \zeta_{p^n}) \times (\text{unit}).$$

So any element "divisible by p^ϵ for some $\epsilon > 0$" is a trace.

Almost disappearing ramification

Tate discovered that ramification "almost disappears" if one makes certain *infinite* extensions of number fields.

E.g., for any prime p, let $\mathbb{Z}_p[\zeta_{p^\infty}]$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) be the ring obtained from $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) by adjoining primitive p^n-th roots of unity ζ_{p^n} for all n. (Note that $\mathbb{Z}_p[\zeta_{p^\infty}]$ is the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty})$.)

Theorem (example of a theorem of Tate)

Let F be a finite extension of $\mathbb{Q}_p(\zeta_{p^\infty})$. Let $\mathfrak{o}_F$ be the integral closure of $\mathbb{Z}_p$ in F. Then $\mathrm{Trace} : \mathfrak{o}_F \to \mathbb{Q}_p(\zeta_{p^\infty})$ has image in $\mathbb{Z}_p[\zeta_{p^\infty}]$ and is **almost** *surjective: its image contains the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

That maximal ideal is generated by $1 - \zeta_{p^n}$ for $n = 1, 2, \dots$, and

$$(1-\zeta_p)^{p-1} = p \times (\text{unit}), \qquad (1-\zeta_{p^{n+1}})^p = (1-\zeta_{p^n}) \times (\text{unit}).$$

So any element "divisible by p^ϵ for some $\epsilon > 0$" is a trace.

Contents

The field of norms equivalence

Fontaine put Tate's result into a broader context, by (partially) isolating a key relevant property of the infinite extensions appearing in Tate's theorem. In the process, he discovered an amazing relationship between Galois theory in characteristic 0 and characteristic p.

Theorem (example of a theorem of Fontaine-Wintenberger)

There is an explicit isomorphism between the absolute Galois groups of $\mathbb{Q}_p(\zeta_{p^\infty})$ *and* $\mathbb{F}_p((\pi))$.

In retrospect, this constitutes the first example of a *tilting equivalence* between perfectoid spaces.

The field of norms equivalence

Fontaine put Tate's result into a broader context, by (partially) isolating a key relevant property of the infinite extensions appearing in Tate's theorem. In the process, he discovered an amazing relationship between Galois theory in characteristic 0 and characteristic p.

Theorem (example of a theorem of Fontaine-Wintenberger)

There is an explicit isomorphism between the absolute Galois groups of $\mathbb{Q}_p(\zeta_{p^\infty})$ *and* $\mathbb{F}_p((\pi))$.

In retrospect, this constitutes the first example of a *tilting equivalence* between perfectoid spaces.

The field of norms equivalence

Fontaine put Tate's result into a broader context, by (partially) isolating a key relevant property of the infinite extensions appearing in Tate's theorem. In the process, he discovered an amazing relationship between Galois theory in characteristic 0 and characteristic p.

Theorem (example of a theorem of Fontaine-Wintenberger)

There is an explicit isomorphism between the absolute Galois groups of $\mathbb{Q}_p(\zeta_{p^\infty})$ *and* $\mathbb{F}_p((\pi))$.

In retrospect, this constitutes the first example of a *tilting equivalence* between perfectoid spaces.

Artin-Schreier theory

One consequence of the previous theorem is that one can use special tools from characteristic p to study Galois theory in characteristic 0. One of the most powerful of these is the Artin-Schreier construction.

For any ring R of characteristic p, the map $x \mapsto x^p$ on R is a ring homomorphism, called *Frobenius* and denoted φ.

For any R-module M, we can twist the action of R on M to define a new R-module $M \otimes_\varphi R$:

$$rm \otimes 1 = m \otimes \varphi(r).$$

We define a *φ-module* over R to be a finite projective R-module M equipped with an R-linear isomorphism $F : M \otimes_\varphi R \cong M$. The map $\Phi : M \to M$ given by $\Phi(m) = F(m \otimes 1)$ is *φ-semilinear*:

$$\Phi(r_1 m_1 + r_2 m_2) = \varphi(r_1)\Phi(m_1) + \varphi(r_2)\Phi(m_2).$$

Artin-Schreier theory

One consequence of the previous theorem is that one can use special tools from characteristic p to study Galois theory in characteristic 0. One of the most powerful of these is the Artin-Schreier construction.

For any ring R of characteristic p, the map $x \mapsto x^p$ on R is a ring homomorphism, called *Frobenius* and denoted φ.

For any R-module M, we can twist the action of R on M to define a new R-module $M \otimes_\varphi R$:

$$rm \otimes 1 = m \otimes \varphi(r).$$

We define a *φ-module* over R to be a finite projective R-module M equipped with an R-linear isomorphism $F : M \otimes_\varphi R \cong M$. The map $\Phi : M \to M$ given by $\Phi(m) = F(m \otimes 1)$ is *φ-semilinear*:

$$\Phi(r_1 m_1 + r_2 m_2) = \varphi(r_1)\Phi(m_1) + \varphi(r_2)\Phi(m_2).$$

Artin-Schreier theory

One consequence of the previous theorem is that one can use special tools from characteristic p to study Galois theory in characteristic 0. One of the most powerful of these is the Artin-Schreier construction.

For any ring R of characteristic p, the map $x \mapsto x^p$ on R is a ring homomorphism, called *Frobenius* and denoted φ.

For any R-module M, we can twist the action of R on M to define a new R-module $M \otimes_\varphi R$:

$$rm \otimes 1 = m \otimes \varphi(r).$$

We define a *φ-module* over R to be a finite projective R-module M equipped with an R-linear isomorphism $F : M \otimes_\varphi R \cong M$. The map $\Phi : M \to M$ given by $\Phi(m) = F(m \otimes 1)$ is *φ-semilinear*:

$$\Phi(r_1 m_1 + r_2 m_2) = \varphi(r_1)\Phi(m_1) + \varphi(r_2)\Phi(m_2).$$

Artin-Schreier theory

One consequence of the previous theorem is that one can use special tools from characteristic p to study Galois theory in characteristic 0. One of the most powerful of these is the Artin-Schreier construction.

For any ring R of characteristic p, the map $x \mapsto x^p$ on R is a ring homomorphism, called *Frobenius* and denoted φ.

For any R-module M, we can twist the action of R on M to define a new R-module $M \otimes_\varphi R$:

$$rm \otimes 1 = m \otimes \varphi(r).$$

We define a *φ-module* over R to be a finite projective R-module M equipped with an R-linear isomorphism $F : M \otimes_\varphi R \cong M$. The map $\Phi : M \to M$ given by $\Phi(m) = F(m \otimes 1)$ is *φ-semilinear*:

$$\Phi(r_1 m_1 + r_2 m_2) = \varphi(r_1)\Phi(m_1) + \varphi(r_2)\Phi(m_2).$$

φ-modules and Galois representations

Let F be a field of characteristic p with absolute Galois group G_F. The group G_F is a compact profinite topological group, and the Galois groups of finite separable extensions of E occur as open subgroups.

Theorem (Katz)

The functors

$$V \mapsto (V \otimes_{\mathbb{F}_p} F^{\mathrm{sep}})^{G_F}, \qquad D \mapsto (D \otimes_F F^{\mathrm{sep}})^{\varphi}$$

define equivalences of categories

$$\left\{ \begin{matrix} \textit{continuous}^a\ G_F\textit{-representations} \\ \textit{on finite } \mathbb{F}_p\textit{-vector spaces } V \end{matrix} \right\} \leftrightarrow \{\varphi\textit{-modules } D \textit{ over } F\}.$$

[a] I.e., representations of Galois groups of finite separable extensions of F.

(And something similar for representations on modules over $\mathbb{Z}_p$ or $\mathbb{Q}_p$.)

φ-modules and Galois representations

Let F be a field of characteristic p with absolute Galois group G_F. The group G_F is a compact profinite topological group, and the Galois groups of finite separable extensions of E occur as open subgroups.

Theorem (Katz)

The functors

$$V \mapsto (V \otimes_{\mathbb{F}_p} F^{\text{sep}})^{G_F}, \qquad D \mapsto (D \otimes_F F^{\text{sep}})^{\varphi}$$

define equivalences of categories

$$\left\{ \begin{matrix} \textit{continuous}^{a}\ G_F\textit{-representations} \\ \textit{on finite } \mathbb{F}_p\textit{-vector spaces } V \end{matrix} \right\} \leftrightarrow \{\varphi\textit{-modules } D \textit{ over } F\}.$$

[a] I.e., representations of Galois groups of finite separable extensions of F.

(And something similar for representations on modules over $\mathbb{Z}_p$ or $\mathbb{Q}_p$.)

φ-modules and Galois representations

Let F be a field of characteristic p with absolute Galois group G_F. The group G_F is a compact profinite topological group, and the Galois groups of finite separable extensions of E occur as open subgroups.

Theorem (Katz)

The functors

$$V \mapsto (V \otimes_{\mathbb{F}_p} F^{\mathrm{sep}})^{G_F}, \qquad D \mapsto (D \otimes_F F^{\mathrm{sep}})^{\varphi}$$

define equivalences of categories

$$\left\{ \begin{array}{l} \textit{continuous}^a\ G_F\textit{-representations} \\ \textit{on finite } \mathbb{F}_p\textit{-vector spaces } V \end{array} \right\} \leftrightarrow \{\varphi\textit{-modules } D \textit{ over } F\}.$$

[a] I.e., representations of Galois groups of finite separable extensions of F.

(And something similar for representations on modules over $\mathbb{Z}_p$ or $\mathbb{Q}_p$.)

Related developments

In related work, Fontaine formalized an observation of Tate and conjectured the form of a *comparison isomorphism* between étale and de Rham cohomology for smooth proper algebraic varieties over finite extensions of $\mathbb{Q}_p$.

Fontaine also introduced the concept of a (φ, Γ)-*module*, which allows the theorem of Katz to be applied to finite extensions of $\mathbb{Q}_p$ (whose absolute Galois groups do not directly appear in characteristic p).

These developments form the heart of *p-adic Hodge theory*, one of the most active branches of arithmetic geometry at present. But I digress...

Related developments

In related work, Fontaine formalized an observation of Tate and conjectured the form of a *comparison isomorphism* between étale and de Rham cohomology for smooth proper algebraic varieties over finite extensions of $\mathbb{Q}_p$.

Fontaine also introduced the concept of a (φ, Γ)-*module*, which allows the theorem of Katz to be applied to finite extensions of $\mathbb{Q}_p$ (whose absolute Galois groups do not directly appear in characteristic p).

These developments form the heart of *p-adic Hodge theory*, one of the most active branches of arithmetic geometry at present. But I digress...

Related developments

In related work, Fontaine formalized an observation of Tate and conjectured the form of a *comparison isomorphism* between étale and de Rham cohomology for smooth proper algebraic varieties over finite extensions of $\mathbb{Q}_p$.

Fontaine also introduced the concept of a (φ, Γ)-*module*, which allows the theorem of Katz to be applied to finite extensions of $\mathbb{Q}_p$ (whose absolute Galois groups do not directly appear in characteristic p).

These developments form the heart of *p-adic Hodge theory*, one of the most active branches of arithmetic geometry at present. But I digress...

Contents

Almost purity

Faltings discovered that the results of Tate and Fontaine-Wintenberger generalize to a large class of rings which are not fields.

For example, let R be the p-adic completion of

$$\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Let R' be the π-adic completion of

$$\mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Theorem (example of a theorem of Faltings)

There is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$. In particular, the **étale fundamental groups** *of these rings are isomorphic.*

Almost purity

Faltings discovered that the results of Tate and Fontaine-Wintenberger generalize to a large class of rings which are not fields.

For example, let R be the p-adic completion of

$$\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Let R' be the π-adic completion of

$$\mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Theorem (example of a theorem of Faltings)

There is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$. In particular, the **étale fundamental groups** *of these rings are isomorphic.*

Almost purity

Faltings discovered that the results of Tate and Fontaine-Wintenberger generalize to a large class of rings which are not fields.

For example, let R be the p-adic completion of

$$\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Let R' be the π-adic completion of

$$\mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Theorem (example of a theorem of Faltings)

There is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$. In particular, the **étale fundamental groups** *of these rings are isomorphic.*

Almost purity

Faltings discovered that the results of Tate and Fontaine-Wintenberger generalize to a large class of rings which are not fields.

For example, let R be the p-adic completion of

$$\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Let R' be the π-adic completion of

$$\mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots].$$

Theorem (example of a theorem of Faltings)

There is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$. In particular, the **étale fundamental groups** *of these rings are isomorphic.*

Almost purity (continued)

Theorem (example of a theorem of Faltings)

For R as before, let S be the integral closure of R in a finite étale extension of $R[1/p]$. Then $\mathrm{Trace} : S \to R$ is **almost** *surjective: its cokernel is killed by every element of the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

Similarly, let S' be the integral closure of R' in a finite étale extension of $R'[1/\pi]$. Then $\mathrm{Trace} : S' \to R'$ is **almost** surjective: its cokernel is killed by π^{1/p^n} for any n. However...

... this is **almost** trivial: the cokernel is killed by some power of π, but is also invariant under φ^{-1}.

The first statement is ultimately proved by reducing to the second statement, using the previous theorem. (We'll see this process again later.)

Almost purity (continued)

Theorem (example of a theorem of Faltings)

For R as before, let S be the integral closure of R in a finite étale extension of $R[1/p]$. Then $\mathrm{Trace} : S \to R$ is **almost** *surjective: its cokernel is killed by every element of the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

Similarly, let S' be the integral closure of R' in a finite étale extension of $R'[1/\pi]$. Then $\mathrm{Trace} : S' \to R'$ is **almost** surjective: its cokernel is killed by π^{1/p^n} for any n. However...

... this is **almost** trivial: the cokernel is killed by some power of π, but is also invariant under φ^{-1}.

The first statement is ultimately proved by reducing to the second statement, using the previous theorem. (We'll see this process again later.)

Almost purity (continued)

Theorem (example of a theorem of Faltings)

For R as before, let S be the integral closure of R in a finite étale extension of $R[1/p]$. Then $\mathrm{Trace} : S \to R$ is **almost** *surjective: its cokernel is killed by every element of the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

Similarly, let S' be the integral closure of R' in a finite étale extension of $R'[1/\pi]$. Then $\mathrm{Trace} : S' \to R'$ is **almost** surjective: its cokernel is killed by π^{1/p^n} for any n. However...

... this is **almost** trivial: the cokernel is killed by some power of π, but is also invariant under φ^{-1}.

The first statement is ultimately proved by reducing to the second statement, using the previous theorem. (We'll see this process again later.)

Almost purity (continued)

Theorem (example of a theorem of Faltings)

For R as before, let S be the integral closure of R in a finite étale extension of $R[1/p]$. Then $\mathrm{Trace} : S \to R$ is **almost** *surjective: its cokernel is killed by every element of the maximal ideal of $\mathbb{Z}_p[\zeta_{p^\infty}]$.*

Similarly, let S' be the integral closure of R' in a finite étale extension of $R'[1/\pi]$. Then $\mathrm{Trace} : S' \to R'$ is **almost** surjective: its cokernel is killed by π^{1/p^n} for any n. However...

... this is **almost** trivial: the cokernel is killed by some power of π, but is also invariant under φ^{-1}.

The first statement is ultimately proved by reducing to the second statement, using the previous theorem. (We'll see this process again later.)

Contents

What is really going on here?

In the mid-2000s, I tried to understand the proofs of the theorems of Fontaine-Wintenberger and Faltings. Failing to do so, I decided to try to come up with my own proofs. (Some progress was reported at ICM 2010; subsequent progress includes joint work with Ruochuan Liu and with Chris Davis.)

A construction of Fontaine

For any ring R, the ring $R/(p)$ is of characteristic p, so it has a Frobenius map φ. We can then define

$$R' = \varprojlim_{\varphi} R/(p);$$

that is, R' consists of sequences $(\dots, x_1, x_0)$ in $R/(p)$ such that $x_{n+1}^p = x_n$. The ring R' is again of characteristic p, but now φ is bijective: its inverse is the map $(\dots, x_1, x_0) \to (\dots, x_2, x_1)$.

Theorem (Fontaine)

If R is the integral closure of $\mathbb{Z}_p$ in an algebraic closure of $\mathbb{Q}_p$, then R' is a valuation ring in an algebraically closed field.

But what about smaller R? For example, if $R = \mathbb{Z}_p[\zeta_{p^\infty}]$, then R' is the π-adic completion of $\mathbb{F}_p[\pi, \pi^{1/p}, \dots]$.

A construction of Fontaine

For any ring R, the ring $R/(p)$ is of characteristic p, so it has a Frobenius map φ. We can then define

$$R' = \varprojlim_{\varphi} R/(p);$$

that is, R' consists of sequences $(\dots, x_1, x_0)$ in $R/(p)$ such that $x_{n+1}^p = x_n$. The ring R' is again of characteristic p, but now φ is bijective: its inverse is the map $(\dots, x_1, x_0) \to (\dots, x_2, x_1)$.

Theorem (Fontaine)

If R is the integral closure of $\mathbb{Z}_p$ in an algebraic closure of $\mathbb{Q}_p$, then R' is a valuation ring in an algebraically closed field.

But what about smaller R? For example, if $R = \mathbb{Z}_p[\zeta_{p^\infty}]$, then R' is the π-adic completion of $\mathbb{F}_p[\pi, \pi^{1/p}, \dots]$.

A construction of Fontaine

For any ring R, the ring $R/(p)$ is of characteristic p, so it has a Frobenius map φ. We can then define

$$R' = \varprojlim_{\varphi} R/(p);$$

that is, R' consists of sequences $(\dots, x_1, x_0)$ in $R/(p)$ such that $x_{n+1}^p = x_n$. The ring R' is again of characteristic p, but now φ is bijective: its inverse is the map $(\dots, x_1, x_0) \to (\dots, x_2, x_1)$.

Theorem (Fontaine)

If R is the integral closure of $\mathbb{Z}_p$ in an algebraic closure of $\mathbb{Q}_p$, then R' is a valuation ring in an algebraically closed field.

But what about smaller R? For example, if $R = \mathbb{Z}_p[\zeta_{p^\infty}]$, then R' is the π-adic completion of $\mathbb{F}_p[\pi, \pi^{1/p}, \dots]$.

The Fontaine-Wintenberger equivalence revisited

The following is in some sense a *maximal* generalization of the Fontaine-Wintenberger theorem.

Theorem

Let K be the completion of an algebraic extension of $\mathbb{Q}_p$. Suppose that:

(a) *the valuation on K is not discrete (so $[K : \mathbb{Q}_p] = \infty$);*

(b) *the map $\varphi : \mathfrak{o}_K/(p) \to \mathfrak{o}_K/(p)$ is surjective.*

Then the ring $(\mathfrak{o}_K)'$ is a valuation ring in a field K' of characteristic p, and there is a canonical isomorphism of Galois groups $G_K \cong G_{K'}$.

The Fontaine-Wintenberger equivalence revisited

The following is in some sense a *maximal* generalization of the Fontaine-Wintenberger theorem.

Theorem

Let K be the completion of an algebraic extension of $\mathbb{Q}_p$. Suppose that:

(a) *the valuation on K is not discrete (so $[K : \mathbb{Q}_p] = \infty$);*

(b) *the map $\varphi : \mathfrak{o}_K/(p) \to \mathfrak{o}_K/(p)$ is surjective.*

Then the ring $(\mathfrak{o}_K)'$ is a valuation ring in a field K' of characteristic p, and there is a canonical isomorphism of Galois groups $G_K \cong G_{K'}$.

More on the Fontaine-Wintenberger equivalence

For any ring S of characteristic p on which φ is bijective, there is a unique p-adically separated and complete ring $W(S)$ such that $W(S)/(p) \cong S$. It can be built explicitly using *Witt vectors*. For instance, if $S = \mathbb{F}_p$, then $W(S) \cong \mathbb{Z}_p$, but with a more exotic description.

Fontaine showed that for R, R' as before, there is an explicit map $\theta : W(R') \to R$. The conditions of the theorem imply that $\theta : W(\mathfrak{o}_{K'}) \to \mathfrak{o}_K$ is surjective. One then shows that for every finite extension L' of K',

$$L = W(\mathfrak{o}_{L'}) \otimes_{W(\mathfrak{o}_{K'}),\theta} K$$

is a finite extension of K, *and* this accounts for all of the finite extensions of K. (This last step reduces to: if K' is algebraically closed, then so is K.)

More on the Fontaine-Wintenberger equivalence

For any ring S of characteristic p on which φ is bijective, there is a unique p-adically separated and complete ring $W(S)$ such that $W(S)/(p) \cong S$. It can be built explicitly using *Witt vectors*. For instance, if $S = \mathbb{F}_p$, then $W(S) \cong \mathbb{Z}_p$, but with a more exotic description.

Fontaine showed that for R, R' as before, there is an explicit map $\theta : W(R') \to R$. The conditions of the theorem imply that $\theta : W(\mathfrak{o}_{K'}) \to \mathfrak{o}_K$ is surjective. One then shows that for every finite extension L' of K',

$$L = W(\mathfrak{o}_{L'}) \otimes_{W(\mathfrak{o}_{K'}),\theta} K$$

is a finite extension of K, *and* this accounts for all of the finite extensions of K. (This last step reduces to: if K' is algebraically closed, then so is K.)

The Fontaine construction for rings

Let R be a ring which is p-torsion-free and integrally closed in $R[1/p]$ (e.g., we rule out $\mathbb{Z}_p[px, x^2]$ because x is missing). Suppose also that:

(a) there exists $x \in R$ such that $x^p \equiv p \pmod{p^2}$;

(b) $\varphi : R/(p) \to R/(p)$ is surjective.

Again, the map $W(R') \to R$ is surjective. Let $\pi \in R'$ be any element of the form $(\dots, x, p)$; we will then compare $R[1/p]$ and $R'[1/\pi]$ in the same way that we compared K and K' in the previous theorem.

For example, the rings from the example of Faltings's theorem:

$$R = (\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots])_p^\wedge,$$
$$R' = \mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots]_\pi^\wedge,$$

are a pair of this form with $\pi = (\dots, 1 - \zeta_{p^2}, 1 - \zeta_p, 0)$.

The Fontaine construction for rings

Let R be a ring which is p-torsion-free and integrally closed in $R[1/p]$ (e.g., we rule out $\mathbb{Z}_p[px, x^2]$ because x is missing). Suppose also that:

(a) there exists $x \in R$ such that $x^p \equiv p \pmod{p^2}$;

(b) $\varphi : R/(p) \to R/(p)$ is surjective.

Again, the map $W(R') \to R$ is surjective. Let $\pi \in R'$ be any element of the form $(\dots, x, p)$; we will then compare $R[1/p]$ and $R'[1/\pi]$ in the same way that we compared K and K' in the previous theorem.

For example, the rings from the example of Faltings's theorem:

$$R = (\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots])_p^\wedge,$$
$$R' = \mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots]_\pi^\wedge,$$

are a pair of this form with $\pi = (\dots, 1 - \zeta_{p^2}, 1 - \zeta_p, 0)$.

The Fontaine construction for rings

Let R be a ring which is p-torsion-free and integrally closed in $R[1/p]$ (e.g., we rule out $\mathbb{Z}_p[px, x^2]$ because x is missing). Suppose also that:

(a) there exists $x \in R$ such that $x^p \equiv p \pmod{p^2}$;

(b) $\varphi : R/(p) \to R/(p)$ is surjective.

Again, the map $W(R') \to R$ is surjective. Let $\pi \in R'$ be any element of the form $(\dots, x, p)$; we will then compare $R[1/p]$ and $R'[1/\pi]$ in the same way that we compared K and K' in the previous theorem.

For example, the rings from the example of Faltings's theorem:

$$R = (\mathbb{Z}_p[\zeta_{p^\infty}][T_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots])_p^\wedge,$$
$$R' = \mathbb{F}_p[\![\pi]\!][\pi^{1/p^n}, \overline{T}_i^{\pm 1/p^n} : i = 1, \dots, m; n = 0, 1, \dots]_\pi^\wedge,$$

are a pair of this form with $\pi = (\dots, 1 - \zeta_{p^2}, 1 - \zeta_p, 0)$.

The Faltings almost purity theorem revisited

The following theorem is in some sense a *maximal* generalization of the Faltings almost purity theorem.

Theorem

Let R, R' be as on the previous slide.

(a) *If R is p-adically separated and complete[a], then there is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$.*

(b) *Let S be the integral closure of R in some finite étale $R[1/p]$-algebra. Then $\mathrm{Trace} : S \to R$ is almost surjective.*

[a] Or even just henselian with respect to p.

Again, (b) follows from (a) using the surjection $\theta : W(R') \to R'$ and the map φ^{-1} on $R'[1/\pi]$. To prove (a), one reduces to the preceding theorem using a glueing argument in nonarchimedean analytic geometry.

The Faltings almost purity theorem revisited

The following theorem is in some sense a *maximal* generalization of the Faltings almost purity theorem.

Theorem

Let R, R' be as on the previous slide.

(a) *If R is p-adically separated and complete*[a]*, then there is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$.*

(b) *Let S be the integral closure of R in some finite étale $R[1/p]$-algebra. Then $\mathrm{Trace}: S \to R$ is almost surjective.*

[a] Or even just henselian with respect to p.

Again, (b) follows from (a) using the surjection $\theta : W(R') \to R'$ and the map φ^{-1} on $R'[1/\pi]$. To prove (a), one reduces to the preceding theorem using a glueing argument in nonarchimedean analytic geometry.

The Faltings almost purity theorem revisited

The following theorem is in some sense a *maximal* generalization of the Faltings almost purity theorem.

Theorem

Let R, R' be as on the previous slide.

(a) *If R is p-adically separated and complete[a], then there is an explicit equivalence of categories of finite étale algebras over $R[1/p]$ and $R'[1/\pi]$.*

(b) *Let S be the integral closure of R in some finite étale $R[1/p]$-algebra. Then $\mathrm{Trace} : S \to R$ is almost surjective.*

[a] Or even just henselian with respect to p.

Again, (b) follows from (a) using the surjection $\theta : W(R') \to R'$ and the map φ^{-1} on $R'[1/\pi]$. To prove (a), one reduces to the preceding theorem using a glueing argument in nonarchimedean analytic geometry.

Contents

A humbling development

Everything I just reported was independently rediscovered by Peter Scholze as a PhD student in Bonn. In addition:

- he introduced a good framework for globalizing the results using Huber's theory of *adic spaces* (and coined the term *perfectoid spaces* for the result);
- he used this to give a simplified derivation of the étale-de Rham comparison isomorphism in p-adic Hodge theory;
- he discovered several new applications that seem to have very little to do with p-adic Hodge theory! E.g., he constructs representations of the Galois groups of number fields out of certain systems of torsion cohomology classes of arithmetic groups. These had been predicted by the Langlands program but were previously untouchable by existing techniques (dating back to Deligne).

A humbling development

Everything I just reported was independently rediscovered by Peter Scholze as a PhD student in Bonn. In addition:

- he introduced a good framework for globalizing the results using Huber's theory of *adic spaces* (and coined the term *perfectoid spaces* for the result);
- he used this to give a simplified derivation of the étale-de Rham comparison isomorphism in p-adic Hodge theory;
- he discovered several new applications that seem to have very little to do with p-adic Hodge theory! E.g., he constructs representations of the Galois groups of number fields out of certain systems of torsion cohomology classes of arithmetic groups. These had been predicted by the Langlands program but were previously untouchable by existing techniques (dating back to Deligne).

A humbling development

Everything I just reported was independently rediscovered by Peter Scholze as a PhD student in Bonn. In addition:

- he introduced a good framework for globalizing the results using Huber's theory of *adic spaces* (and coined the term *perfectoid spaces* for the result);
- he used this to give a simplified derivation of the étale-de Rham comparison isomorphism in p-adic Hodge theory;
- he discovered several new applications that seem to have very little to do with p-adic Hodge theory! E.g., he constructs representations of the Galois groups of number fields out of certain systems of torsion cohomology classes of arithmetic groups. These had been predicted by the Langlands program but were previously untouchable by existing techniques (dating back to Deligne).

A humbling development

Everything I just reported was independently rediscovered by Peter Scholze as a PhD student in Bonn. In addition:

- he introduced a good framework for globalizing the results using Huber's theory of *adic spaces* (and coined the term *perfectoid spaces* for the result);
- he used this to give a simplified derivation of the étale-de Rham comparison isomorphism in p-adic Hodge theory;
- he discovered several new applications that seem to have very little to do with p-adic Hodge theory! E.g., he constructs representations of the Galois groups of number fields out of certain systems of torsion cohomology classes of arithmetic groups. These had been predicted by the Langlands program but were previously untouchable by existing techniques (dating back to Deligne).

The story continues...

A number of experts are assembled at MSRI this semester to study the fallout from these developments. Scholze is giving a course on some even newer ideas, adapting the work of Drinfeld, L. Lafforgue, and V. Lafforgue on the Langlands correspondence in positive characteristic to the case of local fields of mixed characteristic (like $\mathbb{Q}_p$).

For more of the story, see Scholze's 2014 ICM[1] lecture.

[1] And perhaps the 2018 or 2022 ICM proceedings?

The story continues...

A number of experts are assembled at MSRI this semester to study the fallout from these developments. Scholze is giving a course on some even newer ideas, adapting the work of Drinfeld, L. Lafforgue, and V. Lafforgue on the Langlands correspondence in positive characteristic to the case of local fields of mixed characteristic (like $\mathbb{Q}_p$).

For more of the story, see Scholze's 2014 ICM[1] lecture.

[1] And perhaps the 2018 or 2022 ICM proceedings?