We review the construction, starting with the monoid $\mathbb{N}$ of natural numbers, of the ring $\mathbb{Z}$ of integers, of the field $\mathbb{Q}$ of rational numbers, of the locally compact fields $\mathbb{R}$ and $\mathbb{Q}_p$ of real and $p$-adic numbers ($p$ being a prime number), and of the complete closed fields $\mathbb{C}$ and $\mathbb{C}_p$. We introduce Fontaine’s rings of periods and, finally, indicate the need for going beyond them for the purposes of outer galoisian actions.

1. (Numbers as sums). Mathematics starts with

**Definition 1.** — *The monoid $\mathbb{N}$ is the free monoid on one generator, denoted 1.*

We grant that such a monoid exists. The elements of $\mathbb{N}$ are $0$, $1$, $1 + 1$, $1 + 1 + 1$, . . . ; they are to be added for example as

$$(1 + 1) + (1 + 1 + 1) = 1 + 1 + 1 + 1 + 1$$

with the requirement that $n + 0 = n$ and $0 + n = n$ for every $n \in \mathbb{N}$. Given any monoid $M$ and an element $m \in M$, there is a unique morphism of monoids $f : \mathbb{N} \to M$ such that $f(1) = m$.

**Summary:** $(\mathbb{N}, 1)$ is the initial object in the category of pointed monoids.

2. (Numbers as products). Let $\text{End}(\mathbb{N})$ be the additive monoid of endomorphisms of $\mathbb{N}$:

$$(f + g)(n) = f(n) + g(n).$$

The map $e : \text{End}(\mathbb{N}) \to \mathbb{N}$, $f \mapsto f(1)$ is an isomorphism of monoids; the reciprocal is the morphism $1 \mapsto (1 \mapsto 1)$, i.e. the unique morphism which sends $1$ to $\text{Id}_\mathbb{N}$.

An endomorphism $f$ is injective if and only if $f(1) \neq 0$, bijective if and only if $f(1) = 1$. As the composite of two injective maps is injective, $e$ can be used to make the set $\mathbb{N}^*$ (the complement of 0 in $\mathbb{N}$) into a monoid, by transport of structure; it is commutative.

For $m, n \in \mathbb{N}^*$, we say that $m$ divides $n$, and write $m | n$, if the endomorphism $1 \mapsto n$ factors via the endomorphism $1 \mapsto m$. 
Definition 2. — A number \( p \in \mathbb{N}^* \) is called prime if \( p \neq 1 \) and if the only divisors of \( p \) are 1 and \( p \).

The set of prime numbers is denoted by \( P \). The first few primes are 2, 3, 5, 7, 11, \ldots\) Multiples of 2 are called even numbers, the others are called odd. In particular, every prime \( \neq 2 \) is odd.

Theorem 1. — The map \( \mathbb{N}^{(P)} \to \mathbb{N}^* \) which send \( f \) to \( \prod_{p \in P} p^{f(p)} \) is an isomorphism, i.e. \( \mathbb{N}^* \) is the free commutative monoid on the set \( P \).

In other words, given any commutative monoid \( M \) and any map \( f : P \to M \), there is a unique morphism \( \mathbb{N}^* \to M \) which extends \( f \). Moreover, \( P \) is the only subset of \( \mathbb{N}^* \) with this property.

Theorem 2. — The monoid \( \mathbb{N}^* \) is not finitely generated: \( P \) is infinite.

Proof (Euclid) : Suppose that \( P \) were finite, and consider the number \( n = 1 + \prod_{p \in P} p \), which is \( > 1 \). If \( n \) is prime, we get a contradiction because \( P \) does not contain \( n \). If \( n \) is not a prime, we also get a contradiction, because it does not have any prime divisor: no \( p \in P \) is a divisor of \( n \).

Summary: \( \mathbb{N}^* \) is the monoid of injective endomorphisms of the monoid \( \mathbb{N} \); it is free commutative; the elements of its basis are called prime numbers.

3. (Numbers as differences). If \( f : \mathbb{N} \to M \) is a morphism of monoids such that \( f(1) \) has an (additive) inverse, then \( f(n) \) has an inverse for every \( n \in \mathbb{N} \). Conversely, if \( f(n) \) is invertible for some \( n \neq 0 \), then \( f(1) \) is invertible.

The trouble is that there is no \( n \in \mathbb{N} \) such that \( n + 1 = 0 \), i.e. the difference \( 0 - 1 \) does not exist. Nor does the difference \( 8 - 9 \), which is essentially the same. The way to make them exist is to declare these differences \( m - n \) (\( m, n \in \mathbb{N} \)) themselves as being new numbers and to identify any two differences which are essentially the same.

Formally, consider the equivalence relation \( \sim \) on the monoid \( \mathbb{N} \times \mathbb{N} \) of all pairs, defined as
\[
(m, n) \sim (m', n') \iff m + n = m' + n.
\]
Then the class of \((0, 1)\) is the same as the class of \((8, 9)\), and so on; it is denoted \(-1\). The pairs \((1, 0), (9, 8), \text{ etc.}, \) have the same class, which is identified with 1. Thus the equivalence classes consist of \( \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \) and we have obtained the group \( \mathbb{Z} \) of integers as the group of differences of the monoid \( \mathbb{N} \).
Theorem 3. — The group $\mathbb{Z}$ is free on one generator; 1 and $-1$ are the only generators.

Summary: $\mathbb{N} \rightarrow \mathbb{Z}$ is the group of differences of $\mathbb{N}$, i.e. the initial object in the category of maps of the monoid $\mathbb{N}$ into groups.

4. (Numbers as products, bis). Consider the ring $\text{End}(\mathbb{Z})$ of endomorphisms of the group $\mathbb{Z}$. The map $\text{End}(\mathbb{Z}) \rightarrow \mathbb{Z}$, $f \mapsto f(1)$ is an isomorphism of additive groups, allowing us to make the commutative group $\mathbb{Z}$ into a ring; extending the multiplication from $\mathbb{N}$ to $\mathbb{Z}$. This ring is commutative and integral, i.e., if $xy = 0$ ($x,y \in \mathbb{Z}$), then $x = 0$ or $y = 0$. Moreover, the sum and the product of two positive numbers is again positive.

Theorem 4. — The ring $\mathbb{Z}$ is principal, i.e., every ideal can be generated by one element.

Given any ring $A$, there is a unique homomorphism of rings $\mathbb{Z} \rightarrow A$, a fact which is expressed by saying that the ring $\mathbb{Z}$ is the initial object in the category of rings.

Theorem 5. — For every prime $p$, the ideal $p\mathbb{Z}$ is prime, indeed maximal. Conversely, every maximal ideal of $\mathbb{Z}$ is generated by a prime number.

Notice that 0 is the only prime ideal of $\mathbb{Z}$ which is not maximal. For every prime $p$, the field $\mathbb{Z}/p\mathbb{Z}$ is denoted $\mathbb{F}_p$.

Summary: The ring $\mathbb{Z}$ is the ring of endomorphisms of the (commutative) group $\mathbb{Z}$. It is principal and the maximal ideal correspond to prime numbers.

5. (Numbers as fractions). We notice that fractions do not exist in $\mathbb{Z}$: there is no $x$ such that $2x = 1$. In order to remedy this, we proceed as with difference: on the set $\mathbb{Z} \times \mathbb{Z}^*$ of pairs $(m,n)$ ($n \neq 0$), we define an equivalence relation $\sim$ as

$$(m,n) \sim (m',n') \Leftrightarrow mn' = m'n.$$ 

The equivalence class of $(m,n)$ is written $m/n$; they are to be added and multiplied as

$$\frac{m}{n} + \frac{m'}{n'} = \frac{mn' + m'n}{nn'}, \quad \frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'}.$$ 

These classes form a field $\mathbb{Q}$, called the field of fractions of the (integral) ring $\mathbb{Z}$. 

3
Consider the multiplicative group $\mathbb{Q}^\times$ of the field $\mathbb{Q}$, and its subgroup $\mathbb{Z}^\times$, which happens to be the torsion subgroup. One identifies $P$ with its image in $\mathbb{Q}^\times/\mathbb{Z}^\times$.

**Theorem 6.** — The map $\mathbb{Z}^{(P)} \to \mathbb{Q}^\times/\mathbb{Z}^\times$ which sends $f$ to $\prod_{p \in P} p^{f(p)}$ is an isomorphism, i.e. $\mathbb{Q}^\times/\mathbb{Z}^\times$ is the free $\mathbb{Z}$-module on the set $P$.

In other words, $\mathbb{Q}^\times/\mathbb{Z}^\times$ is the group of “differences” of the monoid $\mathbb{N}^*$.

**Corollary.** — The map $\{1, -1\} \times \mathbb{Z}^{(P)} \to \mathbb{Q}^\times$ which sends $(\varepsilon, f)$ to $\varepsilon \prod_{p \in P} p^{f(p)}$ is an isomorphism of $\mathbb{Z}$-modules.

Sometimes it is more convenient to use the isomorphism which sends $-1$ to $-1$ and $e_p$ to $p^*$ for every prime $p$, where $(e_p)_{p \in P}$ is the canonical basis of $\mathbb{Z}^{(P)}$ and

$$2^* = 2, \quad p^* = p^{\frac{p-1}{2}} \quad (p \neq 2).$$

Summary: $\mathbb{Z} \to \mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, i.e. the initial object in the category of injective homomorphisms of the ring $\mathbb{Z}$ into fields. $\mathbb{N}^* \to \mathbb{Q}^\times/\mathbb{Z}^\times$ is the “group of differences” of $\mathbb{N}^*$.

6. *(Numbers as limits).* We notice that there are sequences $(x_n)_n$ of rational numbers which do not have a limit in $\mathbb{Q}$, although $|x_m - x_n|$ can be made as small as we please by taking $m, n$ large enough. For example,

$$x_n = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}$$

In order to make such limits exist, we consider the space of all fundamental sequences, i.e. sequences $(x_n)_n$ of rational numbers such that $|x_n - x_m|$ can be made as small as we please by taking $m, n$ large enough. They can be added and multiplied, so they form a ring. Those fundamental sequences which tend to 0, i.e. such that $|x_n|$ is as small as we please for $n$ large enough, form a maximal ideal of this ring. The quotient field $\mathbb{R}$ has a natural order, hence a uniformity and a topology.

**Theorem 7.** — The space $\mathbb{R}$ is connected, locally connected, locally compact and complete.

7. *(Numbers as roots).* The polynomial $X^2 + 1$ is irreducible over $\mathbb{R}$ because $x^2 + 1 > 0$ for every $x \in \mathbb{R}$. Adjoining a root of this polynomial, we obtain the field $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ of complex numbers. Something miraculous happens:
Theorem 8. — The field \( \mathbb{C} \) of complex numbers is algebraically closed.

The proof rests on the fact that every real number \( > 0 \) has a square root, and that every real polynomial of odd degree has a root in \( \mathbb{R} \).

The group of \( \mathbb{R} \)-automorphisms of \( \mathbb{C} \) is generated by the involution \( i \mapsto -i \), where \( i \) is the image of \( X \) in \( \mathbb{C} \).

The field \( \mathbb{C} \) comes with an absolute value \( |\cdot|_{\infty} \) extending the one on \( \mathbb{R} \), which can be used to give it a uniformity, and hence a topology. Another miracle happens:

Theorem 9. — The space \( \mathbb{C} \) is simply connected, locally compact and complete.

Let us mention the field \( \mathbb{H} \) of quaternions, which is not commutative. It was discovered by Hamilton, who was trying to find an even bigger number system than \( \mathbb{C} \). It can now be defined as the unique (4-dimensional) \( \mathbb{R} \)-algebra \( A \), other than \( M_2(\mathbb{R}) \), such that \( A \otimes_{\mathbb{R}} \mathbb{C} \) is \( \mathbb{C} \)-isomorphic to \( M_2(\mathbb{C}) \). The absolute value \( |\cdot|_{\infty} \) extends to \( \mathbb{H} \), with respect to which it is complete.

Theorem 10. — The only fields complete with respect to an archimedean absolute value are \( \mathbb{R} \), \( \mathbb{C} \) and \( \mathbb{H} \).

In fact, these are the only locally compact connected fields. Notice that these three fields are different, as \( \mathbb{R} \) is commutative but not algebraically closed, \( \mathbb{C} \) is commutative and algebraically closed, whereas \( \mathbb{H} \) is not commutative.

Summary: \( \mathbb{Q} \to \mathbb{R} \) is the completion of \( \mathbb{Q} \) in the \( \infty \)-adic uniformity. It is connected, locally connected, locally compact and complete. \( \mathbb{R} \to \mathbb{C} \) is a quadratic extension and an algebraic closure, with a chosen 4\(^{th}\) root of 1.

8. (Numbers as limits, bis). It was noticed at the end of the XIX\(^{th}\) century that \( |\cdot|_{\infty} \) is not the only absolute value on \( \mathbb{Q} \). For every prime \( p \), there is an absolute value \( |\cdot|_p \) for which the sequence

\[
x_n = 1 + p + p^2 + p^3 + \cdots + p^n
\]

is a fundamental sequence! It is the unique homomorphism \( \mathbb{Q}^\times \to \mathbb{R}^\times \) (into the multiplicative group of real numbers \( > 0 \)) such that \( |p|_p = 1/p \) and \( |l|_p = 1 \) for every prime \( l \neq p \) (cf. Corollary to Theorem 6).
Theorem 11. — *Leaving aside the trivial one, every absolute value on $\mathbb{Q}$ is equivalent to $| |_\infty$ or to $| |_p$ for some prime $p \in \mathbb{P}$.*

That none of these absolute values can be neglected is illustrated by the following result (the “product formula”) — almost a tautology — in which $\tilde{\mathbb{P}}$ denoted the set $\mathbb{P}$ together with an additional element $\infty$:

Theorem 12. — *For every $x \in \mathbb{Q}^\times$, one has $|x|_v = 1$ for almost all $v \in \tilde{\mathbb{P}}$ and $\prod_{v \in \tilde{\mathbb{P}}} |x|_v = 1$.*

Indeed, it is sufficient to verify this for $x = -1$ and $x = p$ ($p \in \mathbb{P}$), cf. Corollary to Theorem 6.

There are fundamental sequences with respect to $| |_p$ which do not converge in $\mathbb{Q}$, for example the sequence $x_n = 2^{5^n}$ for $p = 5$, whose limit would be a primitive $4$th root of $1$.

As in the construction of real numbers, we can consider the ring of all fundamental sequences; those which converge to 0 form a maximal ideal. The quotient field $\mathbb{Q}_p$ comes with an absolute value $| |_p$ (extending the one on $\mathbb{Q}$), hence a metric.

Theorem 13. — *The space $\mathbb{Q}_p$ is locally compact, totally disconnected, and complete.*

The disc $|x|_p \leq 1$ is a compact subring $\mathbb{Z}_p$, with group of units $\mathbb{Z}_p^\times$ the circle $|x|_p = 1$. Another simplification occurs in the multiplicative group (cf. Theorem 6).

Theorem 14. — *The valuation $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ induces an isomorphism $\mathbb{Q}_p^\times / \mathbb{Z}_p^\times \to \mathbb{Z}$.*

Choosing a section of $v_p$, i.e. an element $e_p \in \mathbb{Q}_p^\times$ such that $v_p(e_p) = 1$ (for example $e_p = p$), we get an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \to \mathbb{Q}_p^\times$. For $p$ odd, the torsion subgroup $W$ of $\mathbb{Z}_p^\times$ is cyclic of order $p - 1$; the quotient $\mathbb{Z}_p^\times / W$ is a commutative pro-$p$-group, i.e. a $\mathbb{Z}_p$-module; it is free of rank 1; the image of $1 + e_p$ is a basis. What happens for $p = 2$?

What is the archimedean analogue of this theorem? The analogue of the units would be the kernel of the absolute value, i.e. the 0-sphere $\{1, -1\}$ in $\mathbb{R}$, the 1-sphere $\mathbb{S}_1$ in $\mathbb{C}$ and the 3-sphere $\mathbb{S}_3$ in $\mathbb{H}$.

Theorem 15. — *The maps $(\varepsilon, x) \mapsto \varepsilon e^x$, $\{1, -1\} \times \mathbb{R} \to \mathbb{R}^\times$, $\mathbb{S}_1 \times \mathbb{R} \to \mathbb{C}^\times$ and $\mathbb{S}_3 \times \mathbb{R} \to \mathbb{H}^\times$ are isomorphisms of real-analytic groups.*

In other words, the topological groups $\mathbb{R}^\times / \{1, -1\}$, $\mathbb{C}^\times / \mathbb{S}_1$ and $\mathbb{H}^\times / \mathbb{S}_3$ are 1-dimensional vector spaces over $\mathbb{R}$, with canonical basis $\bar{e}$; they are
the same as the multiplicative group $\mathbb{R}^\times$ of reals $> 0$.

Further, there is a unique $\pi > 0$ in $\mathbb{R}$ such that $2i\pi \mathbb{Z}$ is the kernel of $e^{(\cdot)} : 2i\pi \mathbb{R} \to S_1$, i.e. one has the exact sequence

$$\{0\} \to 2i\pi \mathbb{Z} \to 2i\pi \mathbb{R} \to S_1 \to \{1\}.$$ 

What is the analogue for $S_3$? What is the liegebra $\mathfrak{s}_3$? What are the groups $\mathbb{C}^\times/\mathbb{R}^\times$, $\mathbb{H}^\times/\mathbb{R}^\times$, $\mathbb{H}^\times/\{1, -1\}$, $S_1/\{1, -1\}$, $S_3/\{1, -1\}$?

In all fairness, we should give a similar description of the multiplicative group of all fields complete with respect to the $p$-adic absolute value, and not just $\mathbb{Q}_p$. Let us leave that aside.

Summary : $\mathbb{Q} \to \mathbb{Q}_p$ is the completion of $\mathbb{Q}$ in the $p$-adic uniformity; it is locally compact and totally disconnected. The closed unit disc $\mathbb{Z}_p$ is a compact subring; the quotient $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times$ is $\mathbb{Z}$.

9. (*Numbers as roots and limits, bis*). We saw that there is a drastic reduction in the number of irreducible polynomials when we completed $\mathbb{Q}$ with respect to $| \cdot |_\infty$. The reduction is not so drastic when we complete with respect to $| \cdot |_p$ : there are irreducible polynomials of every degree, but essentially only finitely many of them:

**Theorem 16.** — The field $\mathbb{Q}_p$ has only finitely many extensions in each degree.

For example, the only quadratic extensions of $\mathbb{Q}_5$ are $\mathbb{Q}_5(\sqrt{5})$, $\mathbb{Q}_5(\sqrt{2})$ and $\mathbb{Q}_5(\sqrt{10})$.

Central simple $\mathbb{Q}_p$-algebras are classified by the group $\mathbb{Q}/\mathbb{Z}$, whereas central simple $\mathbb{R}$-algebras are classified by the group $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. There is a very precise local-to-global principle in terms of these groups, of which a special case reads :

**Theorem 17.** — An $n^2$-dimensional central simple $\mathbb{Q}$-algebra $A$ is isomorphic to $\mathbf{M}_2(\mathbb{Q})$ if $A \otimes_\mathbb{Q} \mathbb{Q}_p$ is isomorphic to $\mathbf{M}_2(\mathbb{Q}_p)$ for every $p \in P$ ; $A \otimes_\mathbb{Q} \mathbb{R}$ is then necessarily isomorphic to $\mathbf{M}_2(\mathbb{R})$.

Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$ ; the group $\text{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$, being pro-solvable, is simpler than $\text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, but it is considerably more complicated than the order-2 group $\text{Gal}(\mathbb{C}|\mathbb{R})$. The absolute value $| \cdot |_p$ extends uniquely to $\overline{\mathbb{Q}}_p$. Here is a minor embarrassment :

**Theorem 18.** — The field $\overline{\mathbb{Q}}_p$ is not complete (and not locally compact).
But we can complete $\overline{\mathbb{Q}}_p$ with respect to $| \cdot |_p$ to obtain a field $\mathbb{C}_p$, to which $| \cdot |_p$ extends uniquely, with the same group of values.

**Theorem 19.** — The field $\mathbb{C}_p$ is algebraically closed.

So we don’t need to start all over again, taking an algebraic closure, etc.

Summary : $\overline{\mathbb{Q}}_p$ is an algebraic closure of $\mathbb{Q}_p$. $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$ in the $p$-adic uniformity; it is algebraically closed.

10. *(Numbers as periods).* Varieties have periods. Let us return briefly to the archimedean world of $\mathbb{R}$ and $\mathbb{C}$ to illustrate this.

A considerable effort has been spent, following Grothendieck’s insights, in the search for a universal cohomology theory for varieties over $\mathbb{Q}$. It was noticed that the various known cohomology theories share a number of properites, which led Grothendieck to suspect that there must be a universal cohomology theory — a theory of motives —, of which the known choosing theories are but various different “avatars”. In other words, the motive of a variety should carry every bit of cohomological information about the variety.

To be specific, let us take a smooth, projective, absolutely connected curve $X$ of genus $g$ over $\mathbb{R}$. Then $H^1(X(\mathbb{C}), \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $2g$, so all it knows about $X$ is its genus. However, the $\mathbb{C}$-space $H^1(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$ has a natural filtration which carries much more information about $X$, and indeed enough information to recover the jacobian $J$ of $X$. What I want to emphasize is that you need to tensor with $\mathbb{C}$ to get this additional structure.

The miracle is that tensoring with $\mathbb{C}$ suffices for varieties over $\mathbb{R}$. Another way of saying this is that the field $\mathbb{C}$ contains the periods of all smooth projective $\mathbb{R}$-varieties. This is a miracle because $\mathbb{C}$ was not designed to serve this purpose; it was merely designed to have a square root of $-1$.

11. *(Numbers as periods, bis).* Varieties over $\mathbb{Q}_p$ have their periods too. The major difference with the archimedean world is that you have to go way beyond $\mathbb{C}_p$ to get all the periods. Fontaine has pursued relentlessly this quest for the $p$-adic analogue of $2i\pi$; his solution is to construct several rings carrying many structures which play the role of rings of periods for different kinds of varieties : those with smooth reduction, those with semistable reduction, all (smooth proper) varieties.
The rings $\mathcal{B}$ constructed by Fontaine are $\mathbb{Q}_p$-algebras which carry — among other structures — a representation of $G_\mathbb{Q} = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$: the invariants $\mathcal{B}^{G_\mathbb{Q}}$ are a field. A $p$-adic representation $E$ of $G_\mathbb{Q}$, i.e. a finite-dimensions vector $\mathbb{Q}_p$-space with a continuous linear action of $G_\mathbb{Q}$, is called $\mathcal{B}$-admissible if the dimension of $(\mathcal{B} \otimes \mathbb{Q}_p E)^{G_\mathbb{Q}}$ (as a vector space over $\mathcal{B}^{G_\mathbb{Q}}$) is the same as the dimension of $E$ (as a vector space over $\mathbb{Q}_p$).

Notable examples of $p$-adic representations are provided by the $p$-adic étale cohomology of varieties over $\mathbb{Q}_p$ — the analogue of the singular cohomology of varieties over $\mathbb{R}$ and $\mathbb{C}$.

The rings of Fontaine have proved their utility beyond any doubt. A theorem of Colmez gives an idea of their coherence as $p$ varies: he proves a product formula (cf. Theorem 12) for the periods of abelian varieties having complex multiplications, periods which may be transcendental!

I have chosen to illustrate their utility by taking for $\mathcal{B}$ the crystalline ring of Fontaine; $\mathcal{B}$-admissible representations of $G_\mathbb{Q}$ are called crystalline.

**Theorem (Faltings).** — *For a smooth projective variety $X$ having smooth reduction over $\mathbb{Q}_p$, the representation $H^n(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ is crystalline.*

The converse need not hold. Nevertheless, in the light of the Serre-Tate criterion (see below), one has a right to expect it to hold for abelian varieties.

**Theorem (Coleman-Iovita).** — *Let $A$ be an abelian $\mathbb{Q}_p$-variety. If the $p$-adic representation $H^1(A_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ is crystalline, then $A$ has abelian reduction.*

If we compare these two theorems with what goes on for $l$-adic étale cohomology, where $l$ is a prime $\neq p$, the similarity is striking:

**Theorem (Grothendieck).** — *For a smooth projective variety $X$ having smooth reduction over $\mathbb{Q}_p$, the representation $H^n(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$ is unramified.*

**Theorem (Serre-Tate).** — *Let $A$ be an abelian $\mathbb{Q}_p$-variety. If the $l$-adic representation $H^1(A_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$ is unramified, then $A$ has abelian reduction.*

Summary: For abelian varieties over a finite extension of $\mathbb{Q}_p$, there is an $l$-adic and a $p$-adic criterion for abelian reduction.

12. (*Anabelian periods*). These criteria of Serre-Tate and Coleman-Iovita fail for curves. Indeed, it is not very difficult to construct smooth
proper absolutely connected curves $C$ over $\mathbb{Q}_p$ which do not have smooth reduction but whose jacobian has abelian reduction. For such a curve $C$, the $l$-adic étale cohomology $H^1(C_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$ is unramified and the $p$-adic étale cohomology $H^1(C_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ is crystalline, because these groups are the same for $C$ and its jacobian.

Is there a criterion for the smooth reduction of curves? A very striking theorem was proved by Takayuki Oda, who gives an anabelian $l$-adic criterion. He replaces $H^1(C_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$ by the maximal pro-$l$-quotient $\pi_1^{(l)}(C_{\overline{\mathbb{Q}}_p})$ of the fundamental group $\pi_1(C_{\overline{\mathbb{Q}}_p})$ of $C_{\overline{\mathbb{Q}}_p}$ (there is a choice of a base point involved; it will turn out to be immaterial). The fundamental group carries a natural outer action of the Galois group, i.e. there is a natural homomorphism $G_p \to \text{Out} \pi_1^{(l)}(C_{\overline{\mathbb{Q}}_p})$.

**Theorem** (Takayuki Oda). — *Let $C$ be a smooth proper absolutely connected $\mathbb{Q}_p$-curve of genus $> 1$. If the the outer action $G_p \to \text{Out} \pi_1^{(l)}(C_{\overline{\mathbb{Q}}_p})$ on the pro-$l$ $\pi_1$ is unramified, then $C$ has smooth reduction.***

In fact, his theorem works over any finite extension of $\mathbb{Q}_p$.

**Summary**: For curves, there is an anabelian $l$-adic criterion for smooth reduction.

**13. (Anabelian periods, bis)**. Let me end with a problem which I would very much like to solve. Anyone who has read this account cannot fail to ask himself: Is there an anabelian $p$-adic criterion for smooth reduction of curves over $\mathbb{Q}_p$? I happened to mention this to Kazuya Kato, and he said that this problem “goes straight to the heart”.

**Problem.** — *Give a necessary and sufficient condition on the outer action $G_p \to \text{Out} \pi_1^{(p)}(C_{\overline{\mathbb{Q}}_p})$ for the (smooth, projective, absolutely connected) $\mathbb{Q}_p$-curve $C$ (of genus $> 1$) to have smooth reduction.*

In other words, one should complete the square:

| $l$ | $l \neq p$ | $l = p$ |
|-----|-------------|---------|
| abelian varieties | Serre-Tate (1968, “unramified”) | Coleman-Iovita (1999, “crystalline”) |
| curves of genus $> 1$ | Takayuki Oda (1995, “unramified”) | ??? (???) |

The problem should be studied not just over $\mathbb{Q}_p$, but over every finite extension thereof.
Summary: Find an anabelian $p$-adic criterion for smooth reduction of curves.

14 (Semistable reduction). Notice that there is already a $p$-adic criterion for semistable reduction of curves and abelian varieties in terms of Fontaine's semistable ring. In effect, Fontaine has proved that if an abelian $K$-variety has semiabelian reduction, $K$ being a finite extension of $\mathbb{Q}_p$, then the representation $H^1(A_K, \mathbb{Q}_p)$ of $\text{Gal}(\overline{K}|K)$ is semistable, $\overline{K}$ being an algebraic closure of $K$. Later, Breuil proved the converse, at least for $p \neq 2$. Earlier, Deligne and Mumford had proved that for a curve to have semistable reduction, it is necessary and sufficient for its jacobian to have semiabelian reduction.