Linear Differential Equations with Algebraic Solutions

Hélène Esnault, Freie Universität Berlin

Sackler Lectures, Nov. 2016

Acknowledgements

Thank you to

the mathematicians of Tel Aviv university for the kind invitation to deliver the Sackler Distinguished Lectures;

Acknowledgements

Thank you to

the mathematicians of Tel Aviv university for the kind invitation to deliver the Sackler Distinguished Lectures;

Mark Kisin for constructive remarks and comments on the slides, Yves André for historical references.

Table of Contents

Roots of unity and rational numbers

Question

Let a be a complex number, $a \neq 0$. How do we recognize whether a is a *root of unity*, that is satisfies an equation of the form

Roots of unity and rational numbers

Question

Let a be a complex number, $a \neq 0$. How do we recognize whether a is a *root of unity*, that is satisfies an equation of the form

$$a^n = 1$$

for some natural number n?

Roots of unity and rational numbers

Question

Let a be a complex number, $a \neq 0$. How do we recognize whether a is a *root of unity*, that is satisfies an equation of the form

$$a^n = 1$$

for some natural number n?

Answer

Well, write $a = \exp(2\pi\sqrt{-1}b)$ for some complex number b. Then b should be a *rational number*.

Roots of unity and rational numbers

Question

Let a be a complex number, $a \neq 0$. How do we recognize whether a is a *root of unity*, that is satisfies an equation of the form

$$a^n = 1$$

for some natural number n?

Answer

Well, write $a = \exp(2\pi\sqrt{-1}b)$ for some complex number b. Then b should be a *rational number*.

Too elementary!

Let us ask further, what makes the complex number a a root of unity, or equivalently the complex number b a rational number?

Kronecker's analytic answer

Theorem

Among the complex numbers a which satisfy an equation of the form $a^n + c_1 a^{n-1} + \ldots + c_n = 0$ for some integers $c_i \in \mathbb{Z}$, the roots of unity are those for which all the complex solutions have absolute value 1.

Kronecker's analytic answer

Theorem

Among the complex numbers a which satisfy an equation of the form $a^n + c_1 a^{n-1} + \ldots + c_n = 0$ for some integers $c_i \in \mathbb{Z}$, the roots of unity are those for which all the complex solutions have absolute value 1.

We could equivalently say: If $a \in \mathcal{O}_K$, the ring of integers of a number field K, then $a \in \mu_\infty$, the group of roots of unity, if and only if for all complex embeddings $\iota : K \hookrightarrow \mathbb{C}$, $|\iota(a)| = 1$.

Kronecker's analytic answer

Theorem

Among the complex numbers a which satisfy an equation of the form $a^n + c_1 a^{n-1} + \ldots + c_n = 0$ for some integers $c_i \in \mathbb{Z}$, the roots of unity are those for which all the complex solutions have absolute value 1.

We could equivalently say: If $a \in \mathcal{O}_K$, the ring of integers of a number field K, then $a \in \mu_\infty$, the group of roots of unity, if and only if for all complex embeddings $\iota : K \hookrightarrow \mathbb{C}$, $|\iota(a)| = 1$.

One needs $c_i \in \mathbb{Z}$

If a is algebraic, but not integral, the theorem does not hold. For example, we know there are more Weil numbers of weight 0 than roots of unity, e.g. $a = \frac{3+4\sqrt{-1}}{5}$, a is algebraic of degree 2, has norm 1 with respect to the two embeddings, but is not a root of unity.

Kronecker's arithmetic answer

Theorem

Among the complex numbers b which satisfy an equation of the form $b^m + q_1 b^{n-1} + \ldots + q_m = 0$ for some rational numbers $q_i \in \mathbb{Q}$, the rational numbers are those for which for all prime numbers p not dividing the denominators of the q_i, the mod p reduction of b satisfies

$$(b \bmod p)^p = (b \bmod p).$$

Kronecker's arithmetic answer

Theorem

Among the complex numbers b which satisfy an equation of the form $b^m + q_1 b^{n-1} + \ldots + q_m = 0$ for some rational numbers $q_i \in \mathbb{Q}$, the rational numbers are those for which for all prime numbers p not dividing the denominators of the q_i, the mod p reduction of b satisfies

$$(b \bmod p)^p = (b \bmod p).$$

We could equivalently say: If $b \in K$, a number field, then it lies in the ring $\mathcal{O}_{K,S}$ of integers except at finitely many places S; then

$$b \in \mathbb{Q} \subset K, \text{ the prime field of } K$$

if and only if for almost all prime numbers p,

$$(b \bmod p\mathcal{O}_{K,S}) \in \mathbb{F}_p \subset \mathcal{O}_{K,S}/p\mathcal{O}_{K,S}, \text{ the prime field of the residue ring}.$$

A Linear Differential Equation

Let us show that the Question above is *equivalent* to a question on rank one linear differential equations on the affine line minus a point.

A Linear Differential Equation

Let us show that the Question above is *equivalent* to a question on rank one linear differential equations on the affine line minus a point.

• Let $X := \mathbb{C} \setminus \{0\}$ be the complex affine line minus the origin, with parameter t.

A Linear Differential Equation

Let us show that the Question above is *equivalent* to a question on rank one linear differential equations on the affine line minus a point.

- Let $X := \mathbb{C} \setminus \{0\}$ be the complex affine line minus the origin, with parameter t.
- Linear differential equation

$$(\star)\ df = b \cdot f \cdot \frac{dt}{t}.$$

A Linear Differential Equation

Let us show that the Question above is *equivalent* to a question on rank one linear differential equations on the affine line minus a point.

- Let $X := \mathbb{C} \setminus \{0\}$ be the complex affine line minus the origin, with parameter t.
- Linear differential equation

$$(\star)\ df = b \cdot f \cdot \frac{dt}{t}.$$

- Solve in f, an analytic multivalued function on X.

A Linear Differential Equation

• *Solution:* $f = \lambda \cdot t^b$, for some $\lambda \in \mathbb{C}$; 1-dimensional vector space over $\mathbb{C}$ near any point.

A Linear Differential Equation

- *Solution:* $f = \lambda \cdot t^b$, for some $\lambda \in \mathbb{C}$; 1-dimensional vector space over $\mathbb{C}$ near any point.
- *Monodromy:* $\gamma : \exp(2\pi\sqrt{-1}\theta),\ \theta \in [0,1]$; follow solution f around $t = 1$ along the loop γ, so from $\theta = 0$ to $\theta = 1$. It transforms f to $\exp(2\pi\sqrt{-1}b)f = af$. So the local system is defined by:

$$\rho : \mathbb{Z} \cdot \gamma = \pi_1(X) \to \mathbb{C}^\times, \gamma \mapsto a.$$

A Linear Differential Equation

• *Solution:* $f = \lambda \cdot t^b$, for some $\lambda \in \mathbb{C}$; 1-dimensional vector space over $\mathbb{C}$ near any point.

• *Monodromy:* $\gamma : \exp(2\pi\sqrt{-1}\theta),\ \theta \in [0,1]$; follow solution f around $t = 1$ along the loop γ, so from $\theta = 0$ to $\theta = 1$. It transforms f to $\exp(2\pi\sqrt{-1}b)f = af$. So the local system is defined by:

$$\rho : \mathbb{Z} \cdot \gamma = \pi_1(X) \to \mathbb{C}^\times, \gamma \mapsto a.$$

• The datum of the local system ρ is equivalent to the datum of the linear differential equation $(\star)$: this is an instance of the Riemann-Hilbert correspondence, here valid as the solutions have moderate growth at infinity, or equivalently, $(\star)$ is regular singular.

Kronecker's theorems expressed with linear differential equations: analytic side

• Then the solution f is *algebraic* over the field of rational functions $\mathbb{C}(t)$ if and only if the monodromy a is a root of unity ("if" is clear, "only if" discussed later).

Kronecker's theorems expressed with linear differential equations: analytic side

• Then the solution f is *algebraic* over the field of rational functions $\mathbb{C}(t)$ if and only if the monodromy a is a root of unity ("if" is clear, "only if" discussed later).
• Note: to say $|a| = 1$ is to say that the monodromy is *unitary*, i.e. $\pi_1(X) \to U(1) = S^1 \subset \mathbb{C}^\times = GL(1, \mathbb{C})$. And to say a is *integral* is to say that $a \in GL(1, \mathcal{O}_K)$, where K is a number field and $\mathcal{O}_K$ is its ring of integers (called 'number ring').

Kronecker's theorems expressed with linear differential equations: analytic side

• Then the solution f is *algebraic* over the field of rational functions $\mathbb{C}(t)$ if and only if the monodromy a is a root of unity ("if" is clear, "only if" discussed later).
• Note: to say $|a| = 1$ is to say that the monodromy is *unitary*, i.e. $\pi_1(X) \to U(1) = S^1 \subset \mathbb{C}^\times = GL(1, \mathbb{C})$. And to say a is *integral* is to say that $a \in GL(1, \mathcal{O}_K)$, where K is a number field and $\mathcal{O}_K$ is its ring of integers (called 'number ring').

Analytic characterization

The linear differential equation $(\star)$ has *finite* monodromy if and only if the monodromy is both unitary and defined over a number ring.

Kronecker's theorems expressed with linear differential equations: arithmetic side

• Then the solution f is *algebraic* over the field of rational functions $\mathbb{C}(t)$ if and only if b is a rational number (again "if" clear and "only if" discussed later).

Kronecker's theorems expressed with linear differential equations: arithmetic side

- Then the solution f is *algebraic* over the field of rational functions $\mathbb{C}(t)$ if and only if b is a rational number (again "if" clear and "only if" discussed later).
- Note: solution (f mod p) is a finite expansion $f = \sum_i \lambda_i t^i$ for λ_i in ($\mathcal{O}_{K,S}$ mod p) satisfying

$$(\sum i\lambda_i t^{i-1}) = \frac{b\lambda_0}{t} + (\sum_{i\neq 0} b\lambda_i t^{i-1})$$

Kronecker's theorems expressed with linear differential equations: arithmetic side

• Then the solution f is *algebraic* over the field of rational functions $\mathbb{C}(t)$ if and only if b is a rational number (again "if" clear and "only if" discussed later).

• Note: solution (f mod p) is a finite expansion $f = \sum_i \lambda_i t^i$ for λ_i in ($\mathcal{O}_{K,S}$ mod p) satisfying

$$(\sum i\lambda_i t^{i-1}) = \frac{b\lambda_0}{t} + (\sum_{i\neq 0} b\lambda_i t^{i-1})$$

• Compute: f solution if and only if $b = 0$, or $\lambda_0 = 0$ and $b = i \in (\mathbb{Z} \text{ mod } p) \setminus \{0\}$ for some i.

Kronecker's theorems expressed with linear differential equations: arithmetic side

• We conclude: $b \in \mathbb{Q}$ if and only if the solution $(f \mod p)$ exists for almost all p.

Kronecker's theorems expressed with linear differential equations: arithmetic side

- We conclude: $b \in \mathbb{Q}$ if and only if the solution ($f \bmod p$) exists for almost all p.
- Discussion "only if": $b \in \mathbb{Q}$ is equivalent to $f = t^b$ $\left(\text{and thus to } f = \lambda t^b, \forall \lambda \in \mathbb{C}\right)$ being algebraic over $\mathbb{C}(t)$.

Kronecker's theorems expressed with linear differential equations: arithmetic side

- We conclude: $b \in \mathbb{Q}$ if and only if the solution ($f \bmod p$) exists for almost all p.
- Discussion "only if": $b \in \mathbb{Q}$ is equivalent to $f = t^b$ $\left(\text{and thus to } f = \lambda t^b, \forall \lambda \in \mathbb{C}\right)$ being algebraic over $\mathbb{C}(t)$.
- Easy direction: if $b = \frac{n}{m}, m, n \in \mathbb{Q}, (n, m) = 1$, the minimal equation of f is $(X^m - t^n) \in \mathbb{C}(t)[X]$ as this is an irreducible polynomial. Vice-versa: an algebraic equation $(t^b)^N + \varphi_1(t)(t^b)^{N-1} + \ldots + \varphi_0(t) = 0$ with $\varphi_i(t) \in \mathbb{C}(t)$ implies that $b \in \mathbb{Q}$.

Kronecker's theorems expressed with linear differential equations: arithmetic side

- We conclude: $b \in \mathbb{Q}$ if and only if the solution (f mod p) exists for almost all p.
- Discussion "only if": $b \in \mathbb{Q}$ is equivalent to $f = t^b$ $\left(\text{and thus to } f = \lambda t^b, \forall \lambda \in \mathbb{C}\right)$ being algebraic over $\mathbb{C}(t)$.
- Easy direction: if $b = \frac{n}{m}, m, n \in \mathbb{Q}, (n, m) = 1$, the minimal equation of f is $(X^m - t^n) \in \mathbb{C}(t)[X]$ as this is an irreducible polynomial. Vice-versa: an algebraic equation $(t^b)^N + \varphi_1(t)(t^b)^{N-1} + \ldots + \varphi_0(t) = 0$ with $\varphi_i(t) \in \mathbb{C}(t)$ implies that $b \in \mathbb{Q}$.

Arithmetic characterization

The linear differential equation $(\star)$ has *algebraic solutions* if and only if it is defined over a number field K, and for almost all p, it has a full set of solutions modulo p.

Generalization of the analytic theorem

• We can reinterpret Kronecker's analytic theorem as follows: writing $\prod(\iota) : K \hookrightarrow V_{\mathbb{C}}$ for an r-dimensional vector space over $\mathbb{C}$, where r equals the number of real embeddings plus twice the number of complex embeddings, and $\mathcal{O}_K$ as a lattice $V_{\mathbb{Z}} \subset V_{\mathbb{C}}$, then $\mathcal{O}_K^{\times} \subset GL(V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$. The condition $|\iota(a)| = 1 \ \forall \iota$ says $a \in \mathrm{diag}(S^1 \times \ldots \times S^1) \cap GL(r, V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$.

Generalization of the analytic theorem

- We can reinterpret Kronecker's analytic theorem as follows: writing $\prod(\iota) : K \hookrightarrow V_{\mathbb{C}}$ for an r-dimensional vector space over $\mathbb{C}$, where r equals the number of real embeddings plus twice the number of complex embeddings, and $\mathcal{O}_K$ as a lattice $V_{\mathbb{Z}} \subset V_{\mathbb{C}}$, then $\mathcal{O}_K^{\times} \subset GL(V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$. The condition $|\iota(a)| = 1 \ \forall \iota$ says $a \in \mathrm{diag}(S^1 \times \ldots \times S^1) \cap GL(r, V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$.
- In $GL(V_{\mathbb{C}})$ endowed with the complex topology, the subgroup $\mathrm{diag}(S^1 \times \ldots \times S^1)$ is compact, while the subgroup $GL(r, V_{\mathbb{Z}})$ is discrete.

Generalization of the analytic theorem

- We can reinterpret Kronecker's analytic theorem as follows: writing $\prod(\iota) : K \hookrightarrow V_{\mathbb{C}}$ for an r-dimensional vector space over $\mathbb{C}$, where r equals the number of real embeddings plus twice the number of complex embeddings, and $\mathcal{O}_K$ as a lattice $V_{\mathbb{Z}} \subset V_{\mathbb{C}}$, then $\mathcal{O}_K^{\times} \subset GL(V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$. The condition $|\iota(a)| = 1 \ \forall \iota$ says $a \in \mathrm{diag}(S^1 \times \ldots \times S^1) \cap GL(r, V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$.
- In $GL(V_{\mathbb{C}})$ endowed with the complex topology, the subgroup $\mathrm{diag}(S^1 \times \ldots \times S^1)$ is compact, while the subgroup $GL(r, V_{\mathbb{Z}})$ is discrete.
- Thus $\mathrm{diag}(S^1 \times \ldots \times S^1) \cap GL(r, V_{\mathbb{Z}})$ is finite.

Generalization of the analytic theorem

- We can reinterpret Kronecker's analytic theorem as follows: writing $\prod(\iota) : K \hookrightarrow V_{\mathbb{C}}$ for an r-dimensional vector space over $\mathbb{C}$, where r equals the number of real embeddings plus twice the number of complex embeddings, and $\mathcal{O}_K$ as a lattice $V_{\mathbb{Z}} \subset V_{\mathbb{C}}$, then $\mathcal{O}_K^{\times} \subset GL(V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$. The condition $|\iota(a)| = 1 \ \forall \iota$ says $a \in \mathrm{diag}(S^1 \times \ldots \times S^1) \cap GL(r, V_{\mathbb{Z}}) \subset GL(V_{\mathbb{C}})$.
- In $GL(V_{\mathbb{C}})$ endowed with the complex topology, the subgroup $\mathrm{diag}(S^1 \times \ldots \times S^1)$ is compact, while the subgroup $GL(r, V_{\mathbb{Z}})$ is discrete.
- Thus $\mathrm{diag}(S^1 \times \ldots \times S^1) \cap GL(r, V_{\mathbb{Z}})$ is finite.
- Thus a is a root of unity.

Generalization of the analytic theorem

Theorem (Nobody's theorem, it is obvious: same topological argument)

Let X be a complex manifold, $\rho : \pi_1(X) \to GL(r, \mathbb{C})$ be a local system. Then it has finite monodromy if it is definable over $\mathbb{Z}$ and is unitary.

Generalization of the analytic theorem

Theorem (Nobody's theorem, it is obvious: same topological argument)

Let X be a complex manifold, $\rho : \pi_1(X) \to GL(r, \mathbb{C})$ be a local system. Then it has finite monodromy if it is definable over $\mathbb{Z}$ and is unitary.

• Later on, we shall interpret unitary local systems as polarizable variations of Hodge structure of weight 0. We keep this in mind.

Restricted formulation of Grothendieck's p-curvature conjecture

Grothendieck's p-curvature conjecture, restricted formulation

Let X be a smooth variety defined over a number field K. Then a system of linear differential equations M has *algebraic solutions* if and only if it has a full set of solutions modulo p for almost all p.

Restricted formulation of Grothendieck's p-curvature conjecture

Grothendieck's p-curvature conjecture, restricted formulation

Let X be a smooth variety defined over a number field K. Then a system of linear differential equations M has *algebraic solutions* if and only if it has a full set of solutions modulo p for almost all p.

- This is the precise generalization of the 'Arithmetic Formulation' of Kronecker's theorem translated for $(X, M) = (\mathbb{G}_m, (\star))$.

Restricted formulation of Grothendieck's p-curvature conjecture

Grothendieck's p-curvature conjecture, restricted formulation

Let X be a smooth variety defined over a number field K. Then a system of linear differential equations M has *algebraic solutions* if and only if it has a full set of solutions modulo p for almost all p.

• This is the precise generalization of the 'Arithmetic Formulation' of Kronecker's theorem translated for $(X, M) = (\mathbb{G}_m, (\star))$.

Small historical remark by Yves André

The problem of characterizing which linear differential equations have algebraic solutions goes back to Fuchs (1875), followed by Schwarz, Jordan, Poincaré...Landau "Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gausschen Differentialgleichung" (Crelle (1904)).

More precise formulation

- We should be more precise.

More precise formulation

- We should be more precise.
- To say that ($M \bmod p$) has a *full set of solutions* means the following.

More precise formulation

- We should be more precise.
- To say that $(M \bmod p)$ has a *full set of solutions* means the following.
- Locally on U Zariski open in X with local coordinates $(x_1, \dots, x_n)$, M is defined by

$$(\star\star) \quad \partial_{x_s} f_i = \sum_{j=1}^{r} a_{ij} f_j,$$

for $s = 1, \dots, n$, $i, j = 1, \dots, r$, a_{ij} regular functions. Then there are r r-vectors of functions $g^j := (g_1^j, \dots, g_r^j)$, $j = 1, \dots, r$ in $(\mathcal{O}(U) \bmod p)$ such that any r-vector with entries in $(\mathcal{O}(U) \bmod p)$ is a linear combination of the vectors g^j with coefficients in $(\mathcal{O}(U) \bmod p)$.

More precise formulation

• To say that (X, M) is *defined over a number field* means X is defined by algebraic equations with coefficients in a number field, K say, and $(\star\star)$ has coefficients $a_{ij} \in \mathcal{O}(U_K)$.

More complete formulation of Grothendieck's p-curvature conjecture

We wish to be free of the assumption that (X, M) be defined over a number field. It goes as follows. If not, that is if (X, M) is only defined over $\mathbb{C}$, then it is indeed defined over a $\mathbb{Z}$-algebra of finite type, R say, which contains all the coefficients of the equations defining X, so $a_{ij} \in \mathcal{O}(U_R)$ in $(\star\star)$. One writes $(X, M) = (X, M)_R \otimes_R \mathbb{C}$. For all specializations $R \to K$, where K is a number field, (called *K-valued points*), $(X, M) \otimes_R K$ is defined over the number field K. For specializations $R \to \kappa$, where κ is a finite field, (called *closed points*), $(X, M) \otimes_R \kappa$ is defined over a finite field.

More complete formulation of Grothendieck's p-curvature conjecture

Grothendieck's p-curvature conjecture, more general formulation

Let X be a smooth complex variety. Then a system of linear differential equations M has *algebraic solutions* if and only if $M \otimes_R \kappa$ as a full set of solutions for all closed points κ of a ring of definition R.

Easy direction

Theorem (Easy direction)

If M has algebraic solutions, then $M \otimes_R \kappa$ has a full set of solutions for all closed points κ of a ring of definition R.

Easy direction

Theorem (Easy direction)

If M has algebraic solutions, then $M \otimes_R \kappa$ has a full set of solutions for all closed points κ of a ring of definition R.

Proof.

• There is an easy argument which relies on the notion of *p-curvature* which we carefully avoided up to now (even though the conjecture carries this name).

Easy direction

Theorem (Easy direction)

If M has algebraic solutions, then $M \otimes_R \kappa$ has a full set of solutions for all closed points κ of a ring of definition R.

Proof.

• There is an easy argument which relies on the notion of *p-curvature* which we carefully avoided up to now (even though the conjecture carries this name).

• One has to show that when we take the mod p reduction of a finite étale cover $Y \to X$ which trivializes the differential equation M_Y, then the solutions of the differential equation on (Y mod p) come from (X mod p). The solutions on (Y mod p) form a bundle on the Frobenius twist of (Y mod p), and because M_Y comes from M, this bundle comes from the Frobenius twist of (X mod p). This bundle is the sheaf of solutions.

Two examples of global problems and theorems understood via localization/specialization, and local-global considerations

Theorem of Minkowski-Hasse

Minkowski: if a quadratic form defined over $\mathbb{Q}$ has a real zero and zeros in all the p-adic completions $\mathbb{Q}_p$ of $\mathbb{Q}$, then it has a zero on $\mathbb{Q}$. (Hasse more generally: replace $\mathbb{Q}$ by a number field, and $\mathbb{R}$ and $\mathbb{Q}_p$ by the completion at all places).

Differences

Minkowski-Hasse consider *all* the *completions*, Grothendieck considers *almost all non-archimedian specializations*. Also, while a p-adic zero yields a zero (mod p), it is true vice-versa only if the quadric has good reduction.

Two examples of global problems and theorems understood via localization/reduction, and local-global considerations

Theorem of Deligne-Sullivan

On X complex manifold, the $\mathcal{C}^\infty$-vector bundle associated to a local system $\rho : \pi_1^{\mathrm{top}}(X) \to GL(r, A)$, where A is a finite type over $\mathbb{Z}$, is trivial if $\rho \otimes_A \kappa_i$, $i = 1, 2$, are trivial for two closed points with $\mathrm{char}(\kappa_1) \neq \mathrm{char}(\kappa_2)$.

Differences

We have here specializations, not localizations, but of the monodromy, not of the underlying algebraic vector bundle; in addition, one needs only two specializations.

Two other classical examples

Additive version

Let X_S be smooth over an open S of a number ring, ω be a regular differential form. Then ω is d-exact if and only if it is mod p for almost all p.

Two other classical examples

Additive version

Let X_S be smooth over an open S of a number ring, ω be a regular differential form. Then ω is d-exact if and only if it is mod p for almost all p.

Multiplicative version

Let X_S be smooth an open S of a number ring, ω be a regular differential form. Then ω is $d\log$-exact if and only if it is mod p for almost all p.

Two other classical examples

Additive version

Let X_S be smooth over an open S of a number ring, ω be a regular differential form. Then ω is d-exact if and only if it is mod p for almost all p.

Multiplicative version

Let X_S be smooth an open S of a number ring, ω be a regular differential form. Then ω is $d\log$-exact if and only if it is mod p for almost all p.

We shall see later that those last two statements are true as a corollary of one of the rare instances where one has a solution to the conjecture.

Number field condition

Theorem of André-Hrushovski

The more general formulation of Grothendieck's p-curvature conjecture reduces to the restricted formulation. More precisely: Let R be a ring of finite type over $\mathbb{Q}$. If $M_R \otimes_R K$ has a full set of algebraic solutions for all points with values in number fields K, then M itself has a full set of algebraic solutions. *So one may assume that* (X, M) *is defined over a number field*.

Number field condition

Theorem of André-Hrushovski

The more general formulation of Grothendieck's p-curvature conjecture reduces to the restricted formulation. More precisely: Let R be a ring of finite type over $\mathbb{Q}$. If $M_R \otimes_R K$ has a full set of algebraic solutions for all points with values in number fields K, then M itself has a full set of algebraic solutions. *So one may assume that* (X, M) *is defined over a number field*.

Hrushovski: model theory

I'm incompetent to comment.

Number field condition

André: pure algebraic geometry and group theory

• Camille Jordan's theorem, proved in fact in connection with Fuchs' problem (1878): any finite subgroup of $GL(r, \mathbb{C})$ has a normal abelian subgroup of index bounded in term of r, thus independently of the complex linear representations associated to the various complex embeddings of K for the specializations $M \otimes K$. .

Number field condition

André: pure algebraic geometry and group theory

• Camille Jordan's theorem, proved in fact in connection with Fuchs' problem (1878): any finite subgroup of $GL(r, \mathbb{C})$ has a normal abelian subgroup of index bounded in term of r, thus independently of the complex linear representations associated to the various complex embeddings of K for the specializations $M \otimes K$. .

• This reduces the problem to the case where the monodromies are all finite abelian groups.

Number field condition

André: pure algebraic geometry and group theory

• Camille Jordan's theorem, proved in fact in connection with Fuchs' problem (1878): any finite subgroup of $GL(r, \mathbb{C})$ has a normal abelian subgroup of index bounded in term of r, thus independently of the complex linear representations associated to the various complex embeddings of K for the specializations $M \otimes K$. .

• This reduces the problem to the case where the monodromies are all finite abelian groups.

• One uses algebraic geometry and the representability of the Pic-functor to conclude.

First Katz' theorem: conditions at infinity

Theorem (Katz)

Let X be a smooth variety defined over a number field, let M be a system of linear differential equations which has a full set of algebraic solutions mod p for almost all p. Then after replacing X by a finite cover, M extends to a good compactification. In other words, one may assume that X is projective.

Lefschetz' and Belyi's theorems

• The Lefschetz theorem reduces the problem to X being a smooth projective curve, defined over a number field.

Lefschetz' and Belyi's theorems

- The Lefschetz theorem reduces the problem to X being a smooth projective curve, defined over a number field.
- Belyi's theorem according to which smooth projective curves defined over a number field ramify over the projective line $\mathbb{P}^1$ in three (rational) points reduces the problem to X being $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, defined over a number field.

Résumé

To summarize:

Grothendieck's p-curvature conjecture predicts:

(i) If X is a smooth projective curve defined over a number field, (M mod p) has a full set of solutions for almost all p; or

(ii) if $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ over a number field, (M mod p) has a full set of solutions for almost all p;

then M has a full set of algebraic solutions.

Résumé

To summarize:

Grothendieck's p-curvature conjecture predicts:

(i) If X is a smooth projective curve defined over a number field, (M mod p) has a full set of solutions for almost all p; or

(ii) if $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ over a number field, (M mod p) has a full set of solutions for almost all p;

then M has a full set of algebraic solutions.

Comment

(i) suggests perhaps the use of techniques of global algebraic geometry;
(ii) suggests perhaps the use of p-adic analysis.

Second Katz' theorem: Gauß-Manin connections and the use of Nobody's analytic theorem

Theorem (Katz)

Gauß-Manin connections verify Grothendieck's p-curvature conjecture.

Second Katz' theorem: Gauß-Manin connections and the use of Nobody's analytic theorem

Theorem (Katz)

Gauß-Manin connections verify Grothendieck's p-curvature conjecture.

Method of proof

• By definition, the monodromy is integral, i.e. lies in $GL(r, \mathbb{Z})$, and in some $U(p, q)$ (up to conjugacy), as a variation of Hodge structure. Show: in fact it is unitary, i.e. in $U(r, \mathbb{C})$, and apply Nobody's theorem.

Second Katz' theorem: Gauß-Manin connections and the use of Nobody's analytic theorem

Theorem (Katz)

Gauß-Manin connections verify Grothendieck's p-curvature conjecture.

Method of proof

• By definition, the monodromy is integral, i.e. lies in $GL(r, \mathbb{Z})$, and in some $U(p, q)$ (up to conjugacy), as a variation of Hodge structure. Show: in fact it is unitary, i.e. in $U(r, \mathbb{C})$, and apply Nobody's theorem.

• To this: use geometry. Show "full sets of solutions mod p" implies (F-filtration mod p) stable under the connection, thus stable to start with.

Theorems of Honda, Chudnovsky-Chudnovsky, André: p-adic analysis

Theorem (Honda, Chudnovsky-Chudnovsky, André)

Grothendieck's p-curvature conjecture is true for M being a successive extension of rank 1 connections.

Theorems of Honda, Chudnovsky-Chudnovsky, André: p-adic analysis

Theorem (Honda, Chudnovsky-Chudnovsky, André)

Grothendieck's p-curvature conjecture is true for M being a successive extension of rank 1 connections.

Additive and multiplicative examples fall under this theorem

For any system: to have a full set of algebraic solutions is a property one checks locally Zariski on X. Then the multiplicative example is precisely the case of a rank 1 system of differential equations, while the additive example if precisely the case of an extension of the trivial rank 1 system of differential equations by itself.

Theorems of Honda, Chudnovsky-Chudnovsky, André: p-adic analysis

Method of proof

- Honda-Chudnovsky[2]: Dwork's criterion for a p-adic function to be a rational function;

Theorems of Honda, Chudnovsky-Chudnovsky, André: p-adic analysis

Method of proof

- Honda-Chudnovsky[2]: Dwork's criterion for a p-adic function to be a rational function;
- Extension by André: criterion for a p-adic function to be algebraic.

Theorems of Honda, Chudnovsky-Chudnovsky, André: p-adic analysis

Method of proof

- Honda-Chudnovsky[2]: Dwork's criterion for a p-adic function to be a rational function;
- Extension by André: criterion for a p-adic function to be algebraic.
- Tannakian considerations.

End of general knowledge/understanding

This is essentially all we know on Grothendieck's p-curvature conjecture, without reinforcing the assumptions.

End of general knowledge/understanding

This is essentially all we know on Grothendieck's p-curvature conjecture, without reinforcing the assumptions.

The résumé suggested to try to use algebraic geometry and start with X being a smooth projective curve. This is what we shall do in the next lecture, based on joint work with Mark Kisin.

Outlook

• A generalisation: M with algebraic solutions is a special instance of an M which is a Gauß-Manin connection, that is of an M which comes from the variation of Betti cohomology of a fibration $Y \to X$ over $\mathbb{C}$. The case of algebraic solutions is equivalent to $Y \to X$ finite.

• The generalization of the p-curvature conjecture is to say that Gauß-Manin connections and their summands are characterized by their p-curvatures as in the previous case, except that here one requires the M on (X mod p) to be filtered so that the graded pieces have a full set of solutions. Again the 'easy' direction is known (and due to Deligne): if M is a summand of a Gauß-Manin, then mod p for almost all p, M is filtered with graded having a full set of solutions.

Simpson

A very recent development is based on *Simpson's earlier conjecture*: a local system which is *rigid* (i.e. isolated in its moduli) should be a summand of a Gauß-Manin connection. He proved this with Corlette in full generality for $SL(2)$-local, and with various restrictions with Langer for $SL(3)$-local systems.

Outlook: a conjecture

Conjecture

Let (X, M) be a system of linear differential equations on X smooth over $\mathbb{C}$. Assume M is simple, has quasi-nilpotent monodromies at infinity and is rigid. Then there is S affine over $\mathbb{Z}$ and a model (X_S, M_S) such that for all $s \in S$, M_s is filtered and grM_s has a full set of solutions.