Galois groups arising from arithmetic differential equations

ALEXANDRU BUIUM

University of New Mexico

1. Aim of the talk

1) Briefly introduce arithmetic differential equations (Reference: AB, Inventiones 1995; AB, book, AMS 2005)

2) Show how Galois groups arise in this context (Reference: book above + preprint by AB and A. Saha, 2009.)

2. p-derivations

A p-**derivation** $\delta : A \to A$ *on a ring* A *is a map such that*

$$\delta(x+y) = \delta x + \delta y + C_p(x,y),$$

$$\delta(xy) = x^p \delta y + y^p \delta x + p\delta x \delta y.$$

Here

$$C_p(X,Y) = \frac{X^p + Y^p - (X+Y)^p}{p}.$$

View δ *as a* "$\frac{d}{dp}$"

3. Examples

Example 1: Fermat quotient

$$A = \mathbb{Z}, \quad \delta x = \frac{x - x^p}{p}.$$

Example 2.

$$A = \hat{\mathbb{Z}}_p^{ur}, \quad \delta x = \frac{\phi(x) - x^p}{p}.$$

where ϕ on $A = \hat{\mathbb{Z}}_p^{ur}$ is the unique lift of Frobenius on A/pA and $\hat{}$ means p-adic completion.

From now on $R = \hat{\mathbb{Z}}_p^{ur}$, $\overline{R} = R/pR$

4. Examples, continued

Example 3: δ-polynomials

$$A = R\{x\} := R[x, x', x'', ...],$$

$$\delta x = x', \ \delta x' = x'', ...$$

Here x is a tuple of variables.

Example 4: δ-rational functions

$$A = \widehat{R\{x\}_{(p)}}, \ induced \ \ \delta$$

5. Galois groups

$A \subset B$ δ-*rings,* $pB \cap A = pA$

p-*ad. compl.,* p *non-zero div.*

$\overline{A} := A/pA \subset \overline{B} := B/pB$

$\rho : Aut_\delta(B/A) \to Aut(\overline{B}/\overline{A})$

Note: ρ *injective*

6. Γ-extensions

Let Γ *be a group.*

B/A *called a* Γ*-extension if*

1) $\Gamma \simeq Aut_{\delta}(B/A)$

2) ρ *iso*

3) $\overline{B}^{\Gamma} = \overline{A}$.

In particular $B^{\Gamma} = A$

7. δ-independence

For $u \in \widehat{R\{x\}_{(p)}}$ *say* u *is*

δ-independent

if $u, \delta u, \delta^2 u, \ldots$ *are algebraically independent in* $\overline{R}(x, x', x'', \ldots)$. *In this case we have*

$$A =: \widehat{R\{u\}_{(p)}} \subset \widehat{R\{x\}_{(p)}} := B$$

Write $F^\phi := F^p + p\delta F$ *for* $F \in B$

8. δ-rational functions

Theorem. Let x be one variable and $u := x^{\phi}/x \in B$.

1) u is δ- independent

2) B/A is a $\mathbb{Z}_p^{\times}$-extension.

9. Proof

Proof. $\delta^n(x^\phi/x) \mod p$ *equals*

$$x^{-p^n}(x^{(n)})^p - x^{p^{n+1}-2p^n}x^{(n)} + G_n,$$

$$G_n \in \overline{R}[x, x^{-1}, x', ..., x^{(n-1)}]$$

Then one uses (usual) Galois theory.

10. δ-rational functions, II

Theorem. *Let* x *be one variable and*

$$u := \frac{(x^{\phi^3} - x^{\phi})(x^{\phi^2} - x)}{(x^{\phi^3} - x^{\phi^2})(x^{\phi} - x)} \in B$$

1) u *is* δ*- independent*

2) B/A *is a* $PGL_2(\mathbb{Z}_p)$*-extension.*

Proof. *Same idea but more complicated.*

11. δ-functions on schemes

$X \subset \mathbb{A}^N$ *a closed subscheme* $/R$

$X(R) \subset R^N$ *set of* R*-points*

$f : X(R) \to R$ *called a* δ*-function if there exists* $F \in R[x, x', ..., x^{(r)}]\hat{}$, $r \geq 0$, x *an* N*-tuple of variables, such that*

$$f(a) = F(a, \delta a, ..., \delta^r a), \ a \in X(R)$$

View f *as an arithmetic differential equation*

12. Modular curves

$X_1(N) :=$ *modular curve over* R *of level* $\Gamma_1(N)$.

$L :=$ *line bundle on* $X_1(N)$ *s.t. sections of* $L^{\otimes n}$ *are the modular forms of weight* n.

$X \subset X_1(N)$ *affine open set disjoint from cusps and supersingular locus; restriction of* L *to* X *denoted again by* X.

13. Modular forms

S *ring of regular functions on* X

$V := Spec(\oplus_{n\in\mathbb{Z}} L^{\otimes n})/X$

M *ring of regular functions on* V

(ring of modular forms on X*)*

$\mathbb{G}_m$ *acts on* V/X *hence on* M/S

14. δ-modular forms

A δ-modular function (on X) is a δ-function

$$f : V(R) \to R$$

$M^\infty :=$ *δ-ring of δ-modular functions.*

$R^\times$ acts on V hence on M^∞

15. δ-Fourier expansion

$R((q))[q', q'', ..., q^{(n)}]\hat{}$: *rings*

$R((q))^\infty$ *their union: a* δ*-ring*

$M^\infty \to R((q))^\infty$ δ*-Fourier expansion map: the unique ring homomorphism extending usual Fourier expansion map* $M \to R((q))$ *and commuting with* δ

16. "δ-Igusa curve"

$S_{\dagger}^{\infty} := Im(M^{\infty} \to R((q))^{\infty})$

Morally viewed as the ring of functions on a "δ-Igusa curve" (which we do not define)

17. Motivation: Igusa curve

Let $\overline{S} := S/pS$, $\overline{M} := M/pM$

$\overline{S}_\dagger := Im(\overline{M} \to \overline{R}((q)))$

$Spec(\overline{S}_\dagger) \subset$ classical Igusa curve.

Theorem. (well known)

$\overline{S}_\dagger$ is a $(\mathbb{Z}/p\mathbb{Z})^\times$-extension of $\overline{S}$

18. Result for "δ-Igusa curve"

Theorem.

$\widehat{S^{\infty}_{\dagger}}$ *is a* $\mathbb{Z}_p^{\times}$*-extension of* $\widehat{S^{\infty}}$

19. Proof. *x basis of L on X;* $M = S[x, x^{-1}]$.

Barcau (Compositio 2003):

there exists $f \in M^{\infty}$

$f = \varphi x^{\phi}/x \mapsto 1 \in R((q))^{\infty}$.

Get surjection

$$Q^{\infty} := \frac{\overline{S^{\infty}\{x,x^{-1}\}}}{(\delta^i(f-1))} \to \overline{S^{\infty}_{\dagger}}$$

20. Proof, continued

By computation in the proof of theorem about x^ϕ/x *one gets* Q^∞ *is a* $\mathbb{Z}_p^\times$*-extension of* $\overline{\widehat{S^\infty}}$

left to prove: above surjection an isomorphism

enough to show: Q^∞ *an integral domain because* $\overline{S^\infty} \to Q^\infty \to \overline{S^\infty_\dagger}$ *is injective and first map is an integral extension*

21. Proof, continued

The latter follows from an analysis of the $\mathbb{Z}_p^\times$*-equivariant map*

$M^\infty \to \mathbb{W}$

$\mathbb{W}$= *Katz's ring of generalized* p*-adic modular forms.*

argument is geometric; needs auxiliary construction

22. Application to classical modular forms

Corollary. *Any divided congruence in* $\mathbb{Z}_p[[q]]$ *(in the sense of Katz) can be represented as a restricted power series in classical modular forms over* R *and their (iterated) Fermat quotients of various orders.*

23. Fermat quotient on $R((q))$

Here the Fermat quotient operator on $R((q))\hat{}$ *is defined as*

$$\delta(\sum a_n q^n) = \frac{\sum a_n^{\phi} q^{np} - (\sum a_n q^n)^p}{p}$$

24. Moral

The above (plus other results, cf. AB, book, AMS 2005) suggest that:

Some of Number Theory is governed by a "new" geometry (δ-geometry). The latter is obtained from algebraic geometry by replacing algebraic equations with arithmetic differential equations

25. δ-geometry

Objects: *δ-sets*: *sets* X_δ + *monoid* S + *subsets* (X_s), $s \in S$ + *rings* $(\mathcal{O}_s)$ *of functions* $X_s \to R$, *such that* $\delta(\mathcal{O}_s) \subset \mathcal{O}_s$.

Morphisms: *naturally defined.*

Define ring $R\langle X_\delta \rangle := \cup \mathcal{O}_s$ *of δ-rational functions*

25. Alg. geo $\subset$ δ-geo.

X/R *smooth scheme,*

L/X *line bundle*

Define δ*-sections of* L^w, $w \in \mathbb{Z}[\phi]$;
Zariski locally: δ*-functions.*

Define $R(X) = \cup \mathcal{O}(X')$, X' *mod* $p \neq \emptyset$, *ring of rational functions*

26. Alg. geo $\subset$ δ-geo. II

$X_\delta := X(R)$

$S := \{\delta\text{-sections} \not\equiv 0 \mod p\}$

X_s locus where s invertible

$\mathcal{O}_s$ quotients of δ-sections $\frac{f}{s^v}$

Often $R(X) \subset R\langle X_\delta \rangle$

27. Correspondences

$X \leftarrow C \rightarrow X$ *correspondence in alg.geo /*R*; assume etale and assume* L *line bundle on* X *with iso pull backs on* C*.*

Get $X_\delta \leftarrow C_\delta \rightarrow X_\delta$ *correspondence in* δ*-geometry.*

28. Quotients

X/C *cat. quot. in* {*schemes*}

X_δ/C_δ *cat. quot. in* {δ*-sets*}

N.B. There are interesting cases when X/C *is trivial but* X_δ/C_δ *is not*

29. Cases with X_δ/C_δ non-triv

Spherical: $X = \mathbb{P}^1$, C *graphs of automorphisms in* $SL_2(\mathbb{Z})$.

Flat: $X = \mathbb{P}^1$, C *graph of a post-critically finite dynamical system* $\mathbb{P}^1 \longrightarrow \mathbb{P}^1$ *with negative orbifold Euler char.*

Hyperbolic: X *a modular curve,* C *a Hecke correspondence.*

30. Galois groups

$A := (R(X) \text{“}\cdot\text{”} R\langle X_\delta/C_\delta\rangle)\hat{}$

$B := R\langle X_\delta\rangle\hat{}$

Theorem

In all 3 cases B/A is a Γ-extension with Γ profinite (often computable)