Étale cohomology of surfaces, degeneracy of Galois representations, and a conjectural geometric explanation for ramification

Nicolas Mascot

Trinity College Dublin

Atelier PARI/GP 2024 10 January 2024

### Goal

#### Let $C/\mathbb{Q}$ be a "nice" curve of genus g. Let J be its Jacobian, and fix a prime $\ell \in \mathbb{N}$ . Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $J(\overline{\mathbb{Q}})[\ell] \rightsquigarrow$ Galois representation

$$\rho_{\mathcal{C},\ell}: \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GSp}_{2g}(\mathbb{F}_{\ell}).$$

### Goal

Let  $C/\mathbb{Q}$  be a "nice" curve of genus g. Let J be its Jacobian, and fix a prime  $\ell \in \mathbb{N}$ . Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$  acts on  $J(\overline{\mathbb{Q}})[\ell] \rightsquigarrow$  Galois representation

$$\rho_{\mathcal{C},\ell}: \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GSp}_{2g}(\mathbb{F}_{\ell}).$$

Motivation(s):

• Point counting:

$$\rho(\mathsf{Frob}_p) \quad \rightsquigarrow \quad \#X(\mathbb{F}_p) \bmod \ell \\ \underset{\mathsf{CRT}}{\longrightarrow} \quad \mathsf{Get} \ \#X(\mathbb{F}_p) \ \mathsf{in} \ (\log p)^{O(1)}$$

- Modular curves → Galois representations attached to modular forms → Get a<sub>p</sub>(f) in (log p)<sup>O(1)</sup>.
- Interesting number-theoretic objects, e.g. polynomials with Galois group  $\subseteq GSp_{2g}(\mathbb{F}_{\ell})$  and with controlled ramification.

Suppose  $\alpha \in \mathbb{Q}(J)$  is defined and injective on  $J[\ell]$ .  $\rightsquigarrow$  "Division polynomial"

$$R_{C,\ell}(x) = \prod_{t \in J[\ell]} (x - \alpha(t)) \in \mathbb{Q}[x].$$

Splitting field =  $\mathbb{Q}(t|t \in J[\ell])$ . Galois group = Im  $\rho_{C,\ell} \leq \text{GSp}_{2g}(\mathbb{F}_{\ell})$ .

#### Theorem (Néron-Ogg-Shafarevic)

Unramified away from  $\ell$  and primes of bad reduction of C.

### *p*-adic algorithm to compute $\rho_{C,\ell}$

Fix a small-ish prime  $p \neq \ell$  of good reduction of C.

- Determine  $L_p(x) = \det (x \operatorname{Frob}_p |_J) \in \mathbb{Z}[x].$
- Solution Find  $q = p^a$  such that  $J(\overline{\mathbb{F}_p})[\ell] \subseteq J(\mathbb{F}_q)$ .
- Compute  $N = #J(\mathbb{F}_q) = \operatorname{Res}(L_p(x), x^a 1)$ . Write  $N = \ell^{\vee} N', \ell \nmid N'$ .
- Take random  $x \in J(\mathbb{F}_q)$   $\rightsquigarrow N'x \in J(\mathbb{F}_q)[\ell^{\infty}]$   $\rightsquigarrow \ell^{w_x} N'x \in J(\mathbb{F}_q)[\ell]$  for some  $w_x \leq v$ . Repeat until we get an  $\mathbb{F}_{\ell}$ -basis of  $J(\mathbb{F}_q)[\ell]$ .
- So Lift these points from  $J(\mathbb{F}_q)[\ell]$  to  $J(\mathbb{Z}_q/p^e)[\ell]$ ,  $e \gg 1$ .
- Form all linear combinations to get all the points of J(Z<sub>q</sub>/p<sup>e</sup>)[ℓ].

Oldentify 
$$R_{C,\ell}(x) = \prod_{t \in J[\ell]} (x - \alpha(t))$$
 in  $\mathbb{Q}[x]$ .

Nicolas Mascot

Take  $C: x^3y + y^3 + y^2 - x^2 - x = 0$ , investigate J[2].

R=CrvGalRep(x^3\*y+y^3+y^2-x^2-x,2,10,30)
polisirreducible(R[1])
factor(nfdisc(R[1]))

We get full image  $GSp_6(\mathbb{F}_2)$ , and ramification at 2, 71, 367.

So we can compute with  $J[\ell] \approx H^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$ .

Next natural step:  $H^2_{\acute{e}t}(Surface, \mathbb{Z}/\ell\mathbb{Z})$ .

So we can compute with  $J[\ell] \approx H^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$ . Next natural step:  $H^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$ .

Solution: dévissage by Leray's spectral sequence  $``{\sf H}^p({\sf H}^q) \Rightarrow {\sf H}^{p+q}"\,.$ 

So we can compute with  $J[\ell] \approx H^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$ . Next natural step:  $H^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$ .

Solution: dévissage by Leray's spectral sequence  $``{\sf H}^p({\sf H}^q) \Rightarrow {\sf H}^{p+q}".$ 

#### Theorem (M., 2019)

Let  $S/\mathbb{Q}$  be a regular surface. For every  $\rho \subset H^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$ , one can construct a curve  $C/\mathbb{Q}$  such that  $\rho \subset \text{Jac}(C)[\ell]$  (up to twist by the cyclotomic character).

#### Theorem (M., 2019)



#### Theorem (M., 2019)



#### Theorem (M., 2019)



#### Theorem (M., 2019)



#### Theorem (M., 2019)



#### Theorem (M., 2019)



#### Theorem (M., 2019)



# Strategy

We have sketched a *p*-adic algorithm Curve  $C/\mathbb{Q} \rightsquigarrow \ell$ -division polynomial  $R_{C,\ell}(x) \in \mathbb{Q}[x]$ .

This can be generalised to Curve  $C/\mathbb{Q}(t) \rightsquigarrow \ell$ -division polynomial  $R_{C,\ell}(x,t) \in \mathbb{Q}(t)[x]$ , by lifting  $\ell$ -torsion points (p, t)-adically.

Now suppose we want to compute  $\rho \subset H^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$ .

- Pick  $\pi : S \longrightarrow B$ , where  $B = \mathbb{P}^1_{\mathbb{Q}}$  with coordinate  $t \\ \rightsquigarrow$  view S as a curve S over  $\mathbb{Q}(t)$ .
- ② Compute *ℓ*-division polynomial  $R_{S,\ell}(x,t) \in \mathbb{Q}(t)[x]$ .  $\rightsquigarrow C : R_{S,\ell}(x,t) = 0$  contains  $\rho$  in its Jacobian.
- Isolate *ρ* in *T* ⊂ Jac(*C*)[*ℓ*] by characterising *T* by the action of Frob<sub>*p*</sub> for a well-chosen *p*.

All this requires handling singular plane models f(x, y) = 0 of curves over  $\mathbb{Q}$  or  $\mathbb{Q}(t)$ .

Personal PARI/GP implementation, relies on Puiseux expansions ( $\approx$  factorisation in  $\mathbb{Q}((x))[y]$ ) to resolve singularities.

```
C=CrvInit(y^12-x^4*(x-1)^9);
CrvPrint(C)
CrvHyperell(C)
CanProj(C)
```

### Families of Galois representations

The division polynomial  $R_{S,\ell}(x,t) \in \mathbb{Q}(t)[x]$  defines a <u>family</u> of Galois representations parametrised by  $t \in \mathbb{P}^1_{\mathbb{Q}}$ . For good fibres  $t_0 \in \mathbb{P}^1_{\mathbb{Q}}$ ,  $R_{S,\ell}(x,t=t_0)$  describes  $\operatorname{Jac}(S_{t_0})[\ell]$ 



### Families of Galois representations

The division polynomial  $R_{S,\ell}(x,t) \in \mathbb{Q}(t)[x]$  defines a family of Galois representations parametrised by  $t \in \mathbb{P}^1_{\mathbb{Q}}$ . For good fibres  $t_0 \in \mathbb{P}^1_{\mathbb{Q}}$ ,  $R_{S,\ell}(x, t = t_0)$  describes  $Jac(S_{t_0})[\ell]$ 



But what happens at bad fibres?

## Understanding / computing degeneracy

We would like to predict <u>geometrically</u> the ramification of the degenerate Galois representation, but cannot invoke usual Néron-Ogg-Shafarevic, because we are now working over a 2-dimensional base (1 geometric + 1 arithmetic).

## Understanding / computing degeneracy

We would like to predict <u>geometrically</u> the ramification of the degenerate Galois representation, but cannot invoke usual Néron-Ogg-Shafarevic, because we are now working over a 2-dimensional base (1 geometric + 1 arithmetic).

Degenerate representation: cannot simply set  $t = t_0$  in  $R_{S,\ell}(x,t)$ ; instead, resolve singularity by factoring over  $\mathbb{Q}((t-t_0))$ .  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ Nicolas Mascot Degeneracy of Galois representations

We would like to predict <u>geometrically</u> the ramification of the degenerate Galois representation, but cannot invoke usual Néron-Ogg-Shafarevic, because we are now working over a 2-dimensional base (1 geometric + 1 arithmetic).

Degenerate representation: cannot simply set  $t = t_0$  in  $R_{S,\ell}(x, t)$ ; instead, resolve singularity by factoring over  $\mathbb{Q}((t - t_0))$ .

Similarly, to understand the bad fibre, we do not simply take  $\pi^{-1}(t_0)$ ; instead we consider the minimal regular model of S/B.

$$\mathcal{H}: y^2 = x^6 - x^4 + (t-1)(x^2 + x), \quad \ell = 3.$$

$$Q: x^4 + (2-t)y^4 + 2x^3 + x(x+y) + (t-1)(y+x^2+x) = 0, \quad \ell = 2.$$

tPlace decompositionRamification1 $\mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathcal{K}_8^1 \cdot \mathcal{K}_8^1 \cdot \mathcal{K}_8^{\prime 2} \cdot \mathcal{K}_8^{\prime 2} \cdot \mathcal{K}_{12}^1$ 2,2292 $\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}(\sqrt{2})^4 \cdot \mathbb{Q}(\sqrt{2}, \sqrt{15})^8$ 2,3,5 $\infty$  $\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot \mathcal{K}_3^2 \cdot \mathcal{K}_3^4 \cdot \mathcal{K}_6^1 \cdot \mathcal{K}_8^{\prime\prime\prime 4}$ 2,23

2

$$\begin{array}{c|c} \mathcal{H} : y^2 = x^0 - x^4 + (t-1)(x^2 + x), \quad \ell = 3. \\ \hline t & \text{Place decomposition} & \text{Ramification} \\ \hline 1 & \mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot \left(\mathbb{Q}(\zeta_9)^+(\sqrt{-1})\right)^9 \cdot \left(\mathbb{Q}(\zeta_{36})^+\right)^3 & 2,3 \\ \hline -1 & \mathbb{Q}(\sqrt{-21})^1 \cdot K_6^1 \cdot K_{18}^1 \cdot K_{18}'^3 & 2,3,7,11 \\ \hline \frac{283}{256} & \mathbb{Q}(\sqrt{-14})^1 \cdot K_{18}''^3 \cdot K_{24}^1 & 2,3,7,11 \\ \hline \infty & \mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12} & 2,3 \end{array}$$

Special fibre at t = -1 of minimal regular model of  $\mathcal{H}$  in characteristic  $\notin \{2, 7, 11\}$ :



$$\begin{aligned} \mathcal{H} : y^2 &= x^6 - x^4 + (t-1)(x^2 + x), \quad \ell = 3. \\ \hline t & \text{Place decomposition} & \text{Ramification} \\ \hline 1 & \mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot \left(\mathbb{Q}(\zeta_9)^+(\sqrt{-1})\right)^9 \cdot \left(\mathbb{Q}(\zeta_{36})^+\right)^3 & 2,3 \\ \hline -1 & \mathbb{Q}(\sqrt{-21})^1 \cdot \mathcal{K}_6^1 \cdot \mathcal{K}_{18}^1 \cdot \mathcal{K}_{18}'^3 & 2,3,7,11 \\ \hline 283 \\ 256 & \mathbb{Q}(\sqrt{-14})^1 \cdot \mathcal{K}_{18}''^3 \cdot \mathcal{K}_{24}^1 & 2,3,7,11 \\ \hline \infty & \mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12} & 2,3 \end{aligned}$$

Special fibre at t = -1 of minimal regular model of  $\mathcal{H}$  in characteristic 11:



$$\begin{array}{c|c} \mathcal{H}: y^2 = x^6 - x^4 + (t-1)(x^2 + x), \quad \ell = 3. \\ \hline t & \text{Place decomposition} & \text{Ramification} \\ \hline 1 & \mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot \left(\mathbb{Q}(\zeta_9)^+(\sqrt{-1})\right)^9 \cdot \left(\mathbb{Q}(\zeta_{36})^+\right)^3 & 2, 3 \\ \hline -1 & \mathbb{Q}(\sqrt{-21})^1 \cdot K_6^1 \cdot K_{18}^1 \cdot K_{18}'^3 & 2, 3, 7, 11 \\ \hline \frac{283}{256} & \mathbb{Q}(\sqrt{-14})^1 \cdot K_{18}''^3 \cdot K_{24}^1 & 2, 3, 7, 11 \\ \hline \infty & \mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12} & 2, 3 \end{array}$$

Special fibre at t = -1 of minimal regular model of  $\mathcal{H}$  in characteristic 7:



$$\mathcal{Q}: x^4 + (2-t)y^4 + 2x^3 + x(x+y) + (t-1)(y+x^2+x) = 0, \quad \ell = 2.$$

tPlace decompositionRamification1
$$\mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot K_8^1 \cdot K_8^1 \cdot K_8^{\prime 2} \cdot K_8^{\prime \prime 2} \cdot K_{12}^{\prime 1}$$
2,2292 $\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}(\sqrt{2})^4 \cdot \mathbb{Q}(\sqrt{2}, \sqrt{15})^8$ 2,3,5 $\infty$  $\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot K_3^2 \cdot K_3^4 \cdot K_6^1 \cdot K_8^{\prime \prime \prime 4}$ 2,23

Special fibre at t = 2 of minimal regular model of Q in characteristic  $\notin \{3,5\}$ :



$$\mathcal{Q}: x^4 + (2-t)y^4 + 2x^3 + x(x+y) + (t-1)(y+x^2+x) = 0, \quad \ell = 2.$$

t	Place decomposition	Ramification
1	$\mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathcal{K}_8^1 \cdot \mathcal{K}_8^1 \cdot \mathcal{K}_8^{\prime  2} \cdot \mathcal{K}_8^{\prime  2} \cdot \mathcal{K}_{12}^{\prime  2}$	2,229
2	$\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}(\sqrt{2})^4 \cdot \mathbb{Q}(\sqrt{2},\sqrt{15})^8$	2, 3, 5
$\infty$	$\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot K_3^2 \cdot K_3^4 \cdot K_6^1 \cdot K_8^{\prime\prime\prime}$	2,23

Special fibre at t = 2 of minimal regular model of Q in characteristic 5:



$\mathcal{H}: y^2 = x^6 - x^4 + (t-1)(x^2 + x),  \ell = 3.$				
t	Place decomposition	Ramification		
1	$\left[ \mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot \left( \mathbb{Q}(\zeta_9)^+ (\sqrt{-1})  ight)^9 \cdot \left( \mathbb{Q}(\zeta_{36})^+  ight)^3  ight]$	2,3		
-1	$\mathbb{Q}(\sqrt{-21})^1\cdot  extsf{K}_6^1\cdot  extsf{K}_{18}^1\cdot  extsf{K}_{18}^{\prime 3}$	2, 3, 7, 11		
283 256	$\mathbb{Q}(\sqrt{-14})^1\cdot {K_{18}''}^3\cdot K_{24}^1$	2, 3, 7, 11		
$\infty$	$\mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12}$	2,3		

Special fibre at  $t = \infty$  of (minimal regular model of)  $\mathcal{H}$  in any characteristic:



$$\mathcal{H}: y^2 = x^6 - x^4 + (t-1)(x^2 + x), \quad \ell = 3.$$

t	Place decomposition	Ramification
1	$\mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot \left(\mathbb{Q}(\zeta_9)^+(\sqrt{-1}) ight)^9 \cdot \left(\mathbb{Q}(\zeta_{36})^+ ight)^3$	2,3
-1	$\mathbb{Q}(\sqrt{-21})^1 \cdot K_6^1 \cdot K_{18}^1 \cdot K_{18}'^3$	2, 3, 7, 11
$\frac{283}{256}$	$\mathbb{Q}(\sqrt{-14})^1\cdot {{K_{18}^{\prime\prime}}^3}\cdot K_{24}^1$	2, 3, 7, 11
$\infty$	$\mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12}$	2,3

Special fibre at  $t = \infty$  of minimal regular model of base change of  $\mathcal{H}$  to  $\mathbb{Q}(t^{1/2})$  in characteristic  $\neq 2$ :



This model is no longer regular in characteristic 2.

# Thank you!