Groupes de Galois, courbes elliptiques, points de torsion des variétés abéliennes

Jean-Benoît Bost

Université Paris-Sud et IUF

27 octobre 2011

Des travaux de Galois ... aux représentations galoisiennes.

- Toile de fond : Gauss ; Abel, Jacobi
- Galois
- de Hermite à Kronecker
- Weil ("Coubes algébriques et variétés abéliennes")
- Conjectures de Tate sur les variétés abéliennes

Action du groupe de Galois sur les points de torsion d'une variété abéliennes

Considérons :

- k un corps, $\overline{k}$ une clôture séparable ;
- A une variété abélienne sur k de dimension g ; n un entier > 0 tel que $1/n \in k$;
- l'action du groupe $G := \mathrm{Gal}(\overline{k}/k)$ sur $A[n](\overline{k}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Lorsque le corps k est « arithmétique » (*i.e.*, de type fini sur son corps premier), G a tendance à agir « beaucoup ».

Toile de fond I
Gauss

1801 : *Disquisitiones Arithmeticae*

Sectio septima — De equationibus circuli sectiones definientibus
= étude des extensions cyclotomiques

- irréductibilité
- n premier impair ; $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^* \simeq \mathbb{Z}/(n-1)\mathbb{Z}$
- « périodes »= sommes de Gauss
  [correspondance de Galois explicite pour l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$]
- construction de polygones réguliers

Traduction française :

Paris, 1807 : *Recherches arithmétiques*, par M. C. F. Gauss, traduites par A. C. M. Poullet-Delisle.

Toile de fond II :
la théorie des fonctions elliptiques vers 1830

RECHERCHES ARITHMÉTIQUES,

Par M. Ch.-Fr. GAUSS (de Brunswick);

Traduites par A.-C.-M. POULLET-DELISLE,

Professeur de Mathématiques au Lycée d'Orléans.

A PARIS,

Chez Courcier, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, n° 57.

1807.

$\varphi(1, 1, 1, \ldots) = \varphi(a^n, b^n, c^n, \ldots) = A + A' + A'' \ldots + A^{\nu}$,

et que

$\varphi(a, b, c\ldots) + \varphi(a^2, b^2, c^2\ldots) + \varphi(a^3, b^3, c^3\ldots) + \text{etc.} + \varphi(a^n, b^n, c^n\ldots) = nA.$

Ainsi cette somme est toujours divisible par n, quand tous les coefficiens déterminés (tels que h), dans $\varphi(t, u, v\ldots)$ sont des nombres entiers.

341. THÉORÈME. *Si la fonction* X (*n°* 339) *est divisible par une fonction d'un degré inférieur*

$$P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} + \text{etc.} + Kx + L,$$

les coefficiens A, B,...L *ne peuvent pas être tous entiers ni rationnels.*

Soit $X = PQ$, (π) l'ensemble des racines de l'équation $P = 0$, (χ) l'ensemble des racines de l'équation $Q = 0$, ensorte que Ω soit composé de (π) et de (χ); soit encore (ρ) l'ensemble des racines réciproques aux racines (π), et (σ) l'ensemble des racines réciproques aux racines (χ), et supposons que les racines contenues dans (ρ) soient données par l'équation $R = 0$, qui sera évidemment

$$x^{\lambda} + \frac{K}{L}x^{\lambda-1} + \text{etc.} + \frac{A}{L}x + \frac{1}{L} = 0,$$

tandis que les racines contenues dans (σ) seront données par l'équation $S = 0$. Il est manifeste que les racines (ρ) et (σ) prises ensemble composent Ω, et qu'ainsi l'on aura $RS = X$. Cela posé, nous avons quatre cas à distinguer :

1°. Quand (π) coïncide avec (ρ) et qu'on a parconséquent $P = R$. Dans ce cas les racines (π) seront réciproques deux à deux, et parconséquent P est le produit de $\frac{1}{2}\lambda$ facteurs doubles tels que

$$x^2 - 2x\cos\omega + 1 = (x - \cos\omega)^2 + \sin^2\omega,$$

d'où il suit que quel que soit x, pourvu qu'il soit réel, P obtiendra une valeur réelle positive. Soient

$$P' = 0, \quad P'' = 0, \quad P''' = 0, \ldots . P^{\nu} = 0$$

les équations qui donnent les quarrés, cubes, biquarrés, etc.,

Rappels « modernes »

E courbe elliptique sur $\mathbb{C}$:

- surface de Riemann $E(\mathbb{C}) \simeq \mathbb{C}/\Gamma$, avec Γ réseau dans $\mathbb{C}$;
- loi d'addition $+$: $[z_1] + [z_2] := [z_1 + z_2]$.

Forme différentielle invariante : $\omega := dz$

Ces données sont algébrisables.

Par exemple, *à la* Weierstrass :

$$\wp_\Gamma(z) := \frac{1}{z^2} + \sum_{\gamma \in \Gamma \setminus \{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right)$$

$$\wp_\Gamma'^2 = 4\wp_\Gamma^3 - g_2\wp_\Gamma - g_3$$

Plongement projectif :

$$\begin{array}{rccl} \iota : & E(\mathbb{C}) & \xrightarrow{\sim} & C \hookrightarrow \mathbb{P}^2(\mathbb{C}) \\ & [z] & \longmapsto & (1 : \wp_\Gamma(z) : \wp_\Gamma'(z)) \\ & [0] & \longmapsto & \infty := (0:0:1). \end{array}$$

où C désigne la courbe plane d'équation affine (resp. projective) :

$$y^2 = 4x^3 - g_2 x - g_3$$

$$(X_0 X_2^2 = 4X_1^3 - g_2 X_0^2 X_1 - g_3 X_0^3).$$

Loi d'addition :

- $O = \infty$;
- $P_1 + P_2 + P_3 = O$

$$\Longleftrightarrow \exists L \text{ droite dans } \mathbb{P}^2(\mathbb{C}), L \cap C = P_1" + "P_2" + "P_3.$$

Différentielle invariante : $\omega = \frac{dx}{y}$.

En outre :

- la fonction $w = \wp_\Gamma(z)$ est "inverse" de la "fonction" définie par l'intégrale elliptique

$$\int_\infty^w \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}};$$

- la courbe elliptique E apparaît comme un "revêtement à deux feuillets"

$$x : E \longrightarrow E/\{\pm 1\} \xrightarrow{\sim} \mathbb{P}^1,$$

ramifiés en quatre points $\frac{1}{2}\Gamma/\Gamma \overset{\iota}{\simeq} \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$.

- l'invariant $j(E) := 12^3 \frac{g_2^3}{g_2^3 - 27 g_3^2}$ "classifie" les courbes elliptiques.

Notations classiques

Courbe elliptique de "module" k :

$$y^2 = (1 - x^2)(1 - k^2x^2)$$

où $k^2 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Points de ramifications : $x = \pm 1, \pm k^{-1}$.

Différentielle invariante :

$$\omega = \frac{dx}{y}.$$

Toile de fond II : la théorie des fonctions elliptiques vers 1830

Deux grandes étapes historiques :

- Fagnano, Euler, Legendre : intégrales elliptiques, *e. g.*,

$$\int \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}.$$

Formules d'addition :

$$\int_{\cdot}^{\alpha} \ldots + \int_{\cdot}^{\beta} \ldots = \int_{\cdot}^{\gamma} \ldots$$

avec γ expression rationnelle en α, β, $\sqrt{(1-\alpha^2)(1-k^2\alpha^2)}$, $\sqrt{(1-\beta^2)(1-k^2\beta^2)}$.

- Gauss ; Abel, Jacobi, à partir de 1825 :
  - fonctions elliptiques, définies par inversion de ces intégrales : ce sont des "fonctions uniformes" ! ;
  - étude algébrique des "transformations" (= isogénies) entre courbes elliptiques.

Du point de vue $\mathbb{C}$-analytique :

$$\begin{array}{rccc} \phi : & \mathbb{C}/\Gamma & \longrightarrow & \mathbb{C}/\Gamma' \\ & [0] & \longmapsto & [0] \end{array}$$

$$\phi^* \omega' = \lambda . \omega$$

$$\phi([z]) = [\lambda z]$$

$$\lambda \Gamma \subset \Gamma'.$$

Du point de vue classique, on se donne :

$$E \text{ courbe elliptique } y^2 = (1 - x^2)(1 - k^2 x^2),$$

$$E' \text{ courbe elliptique } y'^2 = (1 - x'^2)(1 - k'^2 x'^2),$$

et on cherche (x', y') comme expressions rationnelles en (x, y) ...

$$\frac{dx'}{\sqrt{(1 - x'^2)(1 - k'^2 x'^2)}} = \lambda \frac{dx}{\sqrt{(1 - x^2)(1 - k^2 x^2)}}.$$

Abel et Jacobi étudient notamment :

- $E[N] := \ker([N] : E \to E) \simeq (\mathbb{Z}/N\mathbb{Z})^2$.
- (Abel) les courbes elliptiques admettant des endomorphismes non-triviaux : multiplication complexe.
  [Cas "lemmiscatique" : $y^2 = 1 - x^4$.]
- (Jacobi) l'existence de p-isogénies, pour tout premier p.
  (p= 2, Landen, ... ; p=3, Legendre)

N.B. :

- méthodes essentiellement algébriques ;
- merveilleuses formules, mais, bien sûr, un certain flou sur les corps sur lesquels on travaille...

Equation modulaire

En 1829, Jacobi publie *Fundamenta Nova Theoriae Functionum Ellipticarum*

Première partie : *De Transformatione Functionum Ellipticarum* = Sur les isogénies des courbes elliptiques.

Point culminant : sections 29 –34, *De aequatione modularium affectibus*.

Jacobi se donne p premier et considère le "diagramme"

$$\{\text{espaces des "modules" des } p\text{-isogénies}\}$$

$$\Downarrow\Downarrow$$

$$\{\text{espaces des "modules" des courbes elliptiques}\}$$

défini par les "fléches"

$$[E \to E'] \longmapsto [E] \text{ et } [E \to E'] \longmapsto [E'].$$

C'est une correspondance symétrique, de degré $(p+1, p+1)$(en effet $\#\mathbb{P}^1(\mathbb{F}_p) = p+1$).

Son équation (en (j, j'), ou (k, k'), ou $(k^{1/4}, k'^{1/4})$, etc...) est l'équation modulaire.

Variante : division complète par p

$\{$espaces des "modules" des (E, P), P point d'ordre exactement $p\}$

$\downarrow$

$\{$espaces des "modules" des courbes elliptiques$\}$

$$[(E, P)] \longmapsto E.$$

Revêtement de degré $\frac{1}{2}(p^2 - 1)$.

Lettre de Jacobi à Legendre, 14 mars 1829

$$n = p$$

Ma formule qui donne l'expression algébrique de sin am *u au moyen de* sin am *nu suppose connue la section de la fonction entière. C'est ainsi qu'on savait résoudre algébriquement depuis plus d'un siècle les équations qui se rapportent à la division d'un arc de cercle, toutefois en supposant connue celle de la circonférence entière, cette dernière n'étant donnée généralement que dans les derniers temps par les travaux de Gauss.*

J'ai été convaincu, et M. Abel l'a confirmé, qu'il n'est pas possible de résoudre algébriquement ces équations de degré $n+1$; aussi, comme M. Abel sait établir des critères nécessaires et suffisants pour qu'une équation algébrique puisse être résolue, il pourra sans doute prouver cela avec toute la rigueur analytique. Quant aux cas spéciaux, comme M. Abel a promis en plusieurs lieu d'en traiter, je ne me suis pas beaucoup occupé de cet objet, sans doute très-intéressant. (...)
Le module transformé ou, ce qui revient au même, le régulateur qui y répond étant supposé connu, il faut encore résoudre une équation de de degré $\frac{n-1}{2}$ pour parvenir (...) à la section de la fonction entière.(...) M. Abel a prouvé que la méthode M. Gauss s'applique presque mot à mot à la résolution de ces équations, de sorte que ce ne sont que les équations aux modules qu'on ne sait pas résoudre algébriquement.

En résumé, deux situations très différentes, pour E courbe elliptique sur k :

- Si les points de $E[N](\overline{k})$ sont k rationnels ("*la division de la section entière est connue*"),la division par n des points de $E(k)$ conduit à des extensions abéliennes.
  Si $P \in E(k)$ *et si* $P' \in E(\overline{k})$ *satisfait* $[n].P' = P$, *alors le corps* $k(P')$ *est une extension abélienne de* k.
  En fait on a :

$$\begin{array}{rcl} \mathrm{Gal}(k(P')/k) & \hookrightarrow & E[n] \\ \sigma & \mapsto & \sigma(P') - P'. \end{array}$$

- En revanche (k corps de fonctions de l'espace des modules), les groupes de Galois de l'équation modulaire et de la "division complète par n" ne sont pas résolubles.

Galois : lettre à Auguste Chevalier, 29 mai 1832

La dernière application de la théorie des équations est relative aux équations modulaires des fonctions elliptiques. (...) par conséquent l'équation modulaire correspondante aura pour groupe

$$x_{\frac{k}{l}} \quad x_{\frac{ak+bl}{ck+dk}},$$

dans lequel $\frac{k}{l}$ *peut avoir les* $p+1$ *valeurs* ∞, 0, 1, 2,..., $p-1$. *(...)*
En donnant à a, b, c, d *toutes les valeurs, on obtient* $(p+1)p(p-1)$ *permutations. Or ce groupe se décompose proprement en deux groupes, dont les substitutions sont*

$$x_k \quad x_{\frac{ak+b}{ck+d}}$$

$ad - bc$ *étant un résidu quadratique de* p. *(...)*

Il n'est plus décomposable proprement, à moins que $p = 2$, *ou* $p = 3$. *Ainsi de quelque manière que l'on transforme l'équation, son groupe aura toujours le même nombre de permutations. Mais il est curieux de savoir si le degré peut s'abaisser. (...) Pour les cas de* $p = 5, 7, 11$ *l'équation modulaire s'abaisse au degré* p.
En toute rigueur, cette réduction n'est pas possible dans les cas plus élevés.

- le groupe de Galois de l'équation modulaire est $PGL_2(\mathbb{F}_p)$ ou $PSL_2(\mathbb{F}_p)$ [? ?] agissant par permutation sur $\mathbb{P}^1(\mathbb{F}_p)$.

  [Choix du corps de constantes $\mathbb{Q}$, ou $\overline{\mathbb{Q}}$ ou $\mathbb{C}$? ?]

- $PSL_2(\mathbb{F}_p)$ est simple si $p \geq 5$.

- pour $p \geq 5$, $PSL_2(\mathbb{F}_p)$ admet un sous-groupe d'indice p si et seulement si $p \in \{5, 7, 11\}$.

La mise au point de ces résultats a suscité une littérature considérable au XIX-ème siécle, notamment par :

- Betti
- Hermite
- Brioschi
- Kronecker
- Jordan
- Klein

Hermite

- Fasciné depuis ses débuts par l'étude systématique et la classification des nombres algébriques — $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ — par des méthodes algébriques *et* analytiques, et tout particulièrement par la construction d'extensions non résolubles de $\mathbb{Q}$ au moyen de la théorie des espaces de modules de courbes elliptiques.

Darboux (1907) :

> *Si quelque jeune géomètre venait lui demander une direction, il lui assignait comme but de devenir un* vir ellipticus*...*
> *Ce qui l'attirait par dessus tout, ce sont les relations que Jacobi avait commencé à mettre en évidence entre les transcendantes elliptiques et l'Arithmétique supérieure.*

Hermite

- Fasciné depuis ses débuts par l'étude systématique et la classification des nombres algébriques — $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ — par de méthodes algébriques *et* analytiques, et tout particulièrement par la construction d'extensions non résolubles de $\mathbb{Q}$ au moyen de la théorie des espaces de modules de courbes elliptiques.

- Étude des cas $p = 5, 7, 11$, non seulement du point de vue des "groupes", mais aussi des "équations" concrètes.
  Sur la théorie des équations modulaires, CRAS 1859.

  A prolongé l'étude du cas $p = 5$ par son étude des équations du cinquième degré, qui se développera dans les travaux de Klein sur les extensions icosaédriques.
  [cf. J-P. Serre, *Extensions icosaédriques*, STN de Bordeaux 1979/1980 ; N. Sepherd-Barron, R. Taylor, *Mod 2 and mod 5 icosahedral representations*, JAMS 10 (1997).]

- Semble le premier a avoir compris explicitement le lien entre théorie de Galois et monodromie.

  Point de départ : article de Puiseux au Journal de Liouville 15 (1850).
  Puiseux établit « GAGA pour π_0 » :
  Une courbe algébrique plane complexe définie par un polynôme irréductible

  $$P(x, y) = 0$$

  est connexe.
  Une fonction algébrique "uniforme" est rationnelle.

  Hermite en déduit (*Sur les fonctions algébriques*, CRAS 1851) :
  Le groupe de Galois de l'équation $P(x, y)$ sur le corps $\mathbb{C}(x)$ coïncide avec la monodromie de la "fonction" $y(x)$ implicitement définie par cette équation.

Ce type d'argument permet de calculer topologiquement le groupe de Galois de l'équation modulaire.
Il semble vraisemblable qu'Abel, Jacobi et Galois avaient songé à ce type d'argument lorsqu'ils se sont « convaincus »de sa nature non-résoluble. L'inclusion

$$\{\text{groupe de monodromie}\} \subset \{\text{groupe de Galois}\}$$

peut en fait s'établir indépendamment du résultat de Puiseux.

Complété par Jordan qui montre (CRAS 1868) que, comme annoncé par Galois, *si* $p > 11$, *alors* $PSL_2(\mathbb{F}_p)$ *n'a pas de sous-groupe d'indice* p.

Jordan donne un exposé d'ensemble de ces questions en 1870, dans son *Traité des substitutions et des équations algébriques.*

Klein

- *Über die Erniedrigung der Modular Gleichungen*, Math. Annal. 14, 1878–1879
- *Über die Transformationen siebenter Ordnung der elliptsichen Funktionen*, ibid.
  $p = 7$

Am wichtigsten ist aber unsere Kurve wohl dadurch geworden (...) das erste konkrete Beispiel für die Uniformisierung der algebraischen Kurven höheren Geschlechtes war...

Kronecker

- points fixes des correspondances modulaires et nombre de classes des corps quadratiques imaginaires
- géométrie algébrique « sur les entiers » ;
  « schéma des modules des courbes elliptiques ».

C. Jordan : *Traité des substitutions et des équations algébriques*, Paris, 1870.

Dans l'Introduction, avançant les raisons pour lesquelles il n'a pas inclus les résultats de Kronecker :

> *... la nature arithmétique de ses méthodes, si différentes de la nôtre ; la difficulté de reconstituer intégralement une suite de démonstrations le plus souvent à peine indiquées ; enfin l'espérance de voir grouper un jour en un corps de doctrine suivi et complet ces beaux théorèmes qui font maintenant l'envie et le désespoir des géométres.*

Kronecker

Etude des schémas intègres $\mathcal{X}$ de type fini sur $\mathbb{Z}$

- $\dim \mathcal{X} = 0$: $\mathcal{X} = \operatorname{Spec} \mathbb{F}_q$; corps de Galois !
- $\dim \mathcal{X} = 1$:
  - $\mathcal{X} = \operatorname{Spec} R$, R (ordre dans l'anneau des S-)entiers d'un corps de nombres ;
  - $\mathcal{X}$ courbe géométriquement intègre sur un corps fini $\mathbb{F}_q$.

Théorie analytique sur les corps de fonctions d'une variable à corps de constantes finis

Kornblum, Artin, Hasse, F.K. Schmidt

C courbe projective lisse géométriquement intègre, de genre g sur un corps fini $\mathbb{F}_q$.

Si P est un point fermé de C, on pose

$$N_P := |\kappa(P)| = q^{[\kappa(P):\mathbb{F}_q]}.$$

$$\zeta_C(s) := \prod_{P \in C} (1 - N_P^{-s})^{-1}$$

Au moyen de la géométrie algébrique sur la courbe C (Riemann-Roch), on établit :

Théorème

La fonction zeta de C peut s'écrire

$$\zeta_C(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

où P est un polynôme de degré $2g$ dans $\mathbb{Z}[X]$, tel que $P(0) = 1$ et

$$P(X) = q^g X^{2g} P(1/qX).$$

Analogue de

$$\zeta(s) := \prod_p (1-p^{-s})^{-1},$$

ou plutôt de : $\xi(s) := \zeta(s)\pi^{-s/2}\Gamma(s/2)$,
et de l'équation fonctionnelle de Riemann :

$$\xi(1-s) = \xi(s).$$

Hypothèse de Riemann pour les corps de fonctions d'une variable

Théorème (Hasse (g=1, 1936) ; Weil (1940–1948))

Pour toute courbe projective lisse C, géométriquement irréductible, de genre g sur le corps fini $\mathbb{F}_q$, on a :

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g.q^{1/2}.$$

$$|\#C(\mathbb{F}_{q^n}) - (q^n+1)| \leq 2g.q^{n/2}.$$

Weil

- *Sur les fonctions algébriques à corps de constantes finies*, CRAS, 1940.
- *On the Riemann hypothesis in function-fields*, Proc. Nat. Acad. Sci., 1941.
- Lettre à Artin, 1942.
- (*Foundations of algebraic geometry*, New York, 1946)
- *Sur les courbes algébriques et les variétés qui s'en déduisent* et *Variétés abéliennes et courbes algébriques*, Paris, 1948.

Weil, 1940 :

> *... la théorie des correspondances donne la clé de ces problèmes ; mais la théorie algébrique des correspondances, qui est due à Severi, n'y suffit point, et il faut étendre à ces fonctions la théorie transcendante de Hurwitz.*

Weil à Artin, 1942.

> *(...Weil esquisse sa preuve de l'hypothèse de Riemann, faisant appel à la théorie de l'intersection.)*
> *We now leave the "elementary" part altogether.*
> *The "transcendental" method depends upon the use of the divisors (or, properly speaking, of the classes of divisors) of finite order.*

A. Hurwitz *Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip*, Math. Ann. 28 (1887).

C surface de Riemann compacte connexe de genre g ;

Σ correspondance algébrique sur C, de bidegré (a, b) ;

$$\begin{array}{rrcl} \phi_\sigma : & \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ \mathrm{Lie}\,\phi_\sigma : & \mathrm{Lie\ Jac}(C) & \longrightarrow & \mathrm{Lie\ Jac}(C) \\ \tilde{\phi}_\Sigma : & H_1(C, \mathbb{Z}) & \longrightarrow & H_1(C, \mathbb{Z}). \end{array}$$

Le nombre de points fixes de Σ vaut :

$$\Sigma.\Delta_C = a + b - \mathrm{Tr}_{H_1} \tilde{\phi}_\Sigma.$$

A variété abélienne sur k, l premier tel que $l^{-1} \in k$

$$A[l^n](\overline{k}) \simeq (\mathbb{Z}/l^n\mathbb{Z})^{2g}$$

$$\bigcup_n A[l^n](\overline{k}) \simeq (\mathbb{Z}[l^{-1}]/\mathbb{Z})^{2g}$$

$$\mathrm{End}_{\mathbb{Z}}\mathbb{Z}[l^{-1}]/\mathbb{Z} \simeq \varprojlim \mathbb{Z}/l^n\mathbb{Z} \simeq \mathbb{Z}_l$$

$$T_l(A) := \varprojlim A[l^n](\overline{k}) \simeq \varprojlim (\mathbb{Z}/l^n\mathbb{Z})^{2g} \simeq \mathbb{Z}_l^{2g}$$

$$\rho_l : \mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{Aut} \bigcup_n A[l^n](\overline{k}) \simeq \mathrm{Aut}_{\mathbb{Z}_l} T_l(A) \simeq GL_{2g}(\mathbb{Z}_l)$$

- $k = \mathbb{F}_q$, $A = \mathrm{Jac}(C) = \mathrm{Pic}\,(C)$, $l \neq p$

$$P(X) = \det(Id - \rho_l(F_q))$$

- k corps de nombres
  Y. Taniyama, *L-functions of number fields and zeta functions of abelian varieties*, J. Math. Soc. Japan 9 (1957).

  exemple de système compatible de représentations l-adiques.