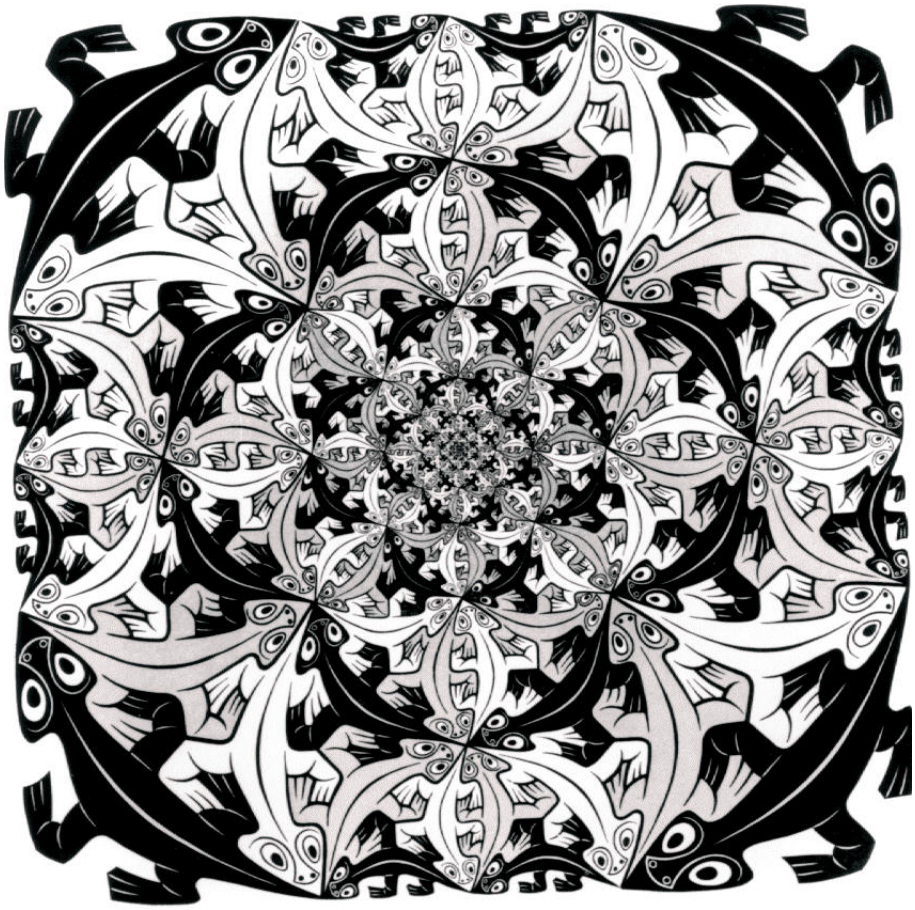
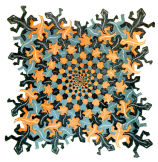
Université Bordeaux 1
351 Cours de la Libération
33400 Talence

Une variante faible de la conjecture de torsion



Mémoire écrit par : Sophie Marques
Chargée de mémoire : Anna Cadoret

Remerciements



Je tiens en premier lieu à adresser mes plus sincères remerciements à ma directrice de mémoire, Anna Cadoret, qui a su me guider de manière remarquable tout au long de ce semestre comme elle l'avait déjà fait lors de mon TER.

J'exprime toute ma gratitude à Monsieur Fresnel, une personne admirable pour sa générosité, sa grande patience et sa bienveillance tout au long des deux dernières années.
Je remercie Monsieur Matignon pour ses explications toujours pertinentes et sa disponibilité au cours de ces deux années.
Mes remerciements vont également à Monsieur Yuri Bilou pour les cours et les conseils qu'il a su prodiguer pendant cette année. Je n'oublie pas ma famille et mes amis pour leur contribution, leur soutien et leur patience.

Merci du fond du coeur à tous et à toutes.

Table des matières

Table des notations

Nous utiliserons les notations suivantes tout au long du travail :

$\bar{k} = (k^{sep})$	la cloture algébrique du corps k
$\Gamma_k = Gal(\bar{k}\|k)$	le groupe de Galois absolu du corps k
$\mathcal{O}_{X,x}$	le germe du faisceau structural de X
$\mathfrak{M}_{X,x}$	l'idéal maximal de $\mathcal{O}_{X,x}$
$k(x) := \frac{\mathcal{O}_{X,x}}{\mathfrak{M}_{X,x}}$	le corps résiduel de X
$A[n]$	les points de de n-torsion
$Tr_{K/k}(A) \to k$	la trace de chow sur K/k
$\rho_{\mathbf{A},\mathbf{n}} : \pi_1(\mathbf{X}) \to \mathrm{GL}(\mathbf{A}_\eta[\mathbf{n}])$	la représentation canonique de $\pi_1(X)$ dans le groupe $A_\eta[n]$
$X_{(n)}$	courbe modulaire abstraite définie par $U = ker(\rho_{A,n}) \lhd_{op} \pi_1(X)$
X_v	courbe modulaire abstraite définie par $U = Stab_{\pi_1(X)}(v) <_{op} \pi_1(X)$
X_n	$\bigsqcup_{\substack{\|\langle v\rangle\|=n \\ v\in A_\eta[n]}} X_v$.
$g(n)$	$\min_{v\in A_\eta[n]^\times} \{g_{X_v}\}$.
$A_\eta[n]^\times$	pour l'ensemble des points de torsion d'ordre exactement n.
G_M	l'image de $\rho_{A,M} : \pi_1(X) \to GL(M)$
K_M	le noyau de $\rho_{A,M} : \pi_1(X) \to GL(M)$
PB	place à bonne réduction
SS	place à réduction semi-stable
PSS	place à réduction potentiellement semi-stable
$\mathcal{O}_{i,n}$	$\{w \in G_\ell v \text{ tel que } \| < \gamma_{i,\ell} > w\| = n\}$
E_I	$\bigcap_{i\in I} \mathcal{O}_{i,1} = (G_\ell v)^{<\gamma_i \| i\in I>}$
Σ_i	$\sum_{I\subset\{1...,r\},\ \|I\|=i} \|E_I\|$
$\overline{\Sigma}_i$	$\|\bigcup_{I\subset\{1,...r\},\ \|I\|=i} E_I\|$
E_I^*	$E_I \setminus \bigcup_{I\subsetneq J} E_J$
Σ_i^*	$\sum_{I\subset\{1,...r\},\ \|I\|=i} \|E_I^*\|$
$\overline{\Sigma}_i^*$	$\|\bigcup_{I\subset\{1,...r\},\ \|I\|=i} E_I^*\|$
$[K(X) : K(Y)]$	degré de l'extension du corps de fonctions de X et Y.
$R := \sum_{i=1}^{n} \rho(P_i)P_i$	un diviseur de Weil
$\mathcal{L}(D)$	faisceau inversible associé au diviseur de Weil D
$CaCl(X)$	ensemble des diviseurs de Cartier de X
$Cl(X)$	ensemble des diviseurs de Weil de X
$Pic(X)$	ensemble des faisceaux inversibles de X
$long(M)$	longueur d'un module M
$\Omega_{X\|k}$	faisceau des différentielles relatives
A_K	$A \times spec(K)$
$\mathbb{G}_a$	groupe additif
$\mathbb{G}_m$	groupe multiplicatif
$G_x(i)$	$i^{\text{ème}}$ groupe de ramification
$\mathbb{T}$	tore

1. Introduction

On supposera acquis les rudiments de la géométrie algébrique ([8, chap.II-IV], [11, chap.2 et 7], [9, part A et C]) et la théorie du groupe fondamental comme exposée en [3], [22, chap.3-5].

Ce mémoire a pour objet la lecture d'une partie de l'article [4], que l'on s'est efforcé de replacer dans le contexte des travaux de ses auteurs sur les représentations du groupe fondamental des courbes.

Les résultats principaux de cet article sont :

Théorème 1.1. *Soit k un corps algébriquement clos de type fini et de caractéristique 0, K/k un corps de fonction en une variable et A une variété abélienne sur K ne contenant pas de sous variété k-isotriviale non triviale. Supposons que K est de genre $\geqslant 1$ ou que A soit à réduction semi-stable sauf éventuellement en une place. Alors il existe $N = N(A,g) \geqslant 0$ tel que toute extension finie L/K de genre $g_L \leqslant g$ on a $A(L)_{tors} \subset A[N]$.*

Corollaire 1.2. *Soit k un corps de caractéristique 0, X une courbe lisse, séparée et géométriquement connexe sur k et $A \to X$ un schéma abélien. Supposons que X est de genre supérieur ou égal à 1 ou que $A \to X$ à réduction semi-stable en tout point sauf éventuellement un point (géométrique) de $\tilde{X} \smallsetminus X$. Alors pour chaque premier ℓ il existe un entier $n(\ell) \geqslant 1$ tel que :*
(i) $n(\ell) = 1$ pour $\ell \gg 0$;
(ii) l'ensemble des $x \in X(k)$ tel que $\ell^{n(\ell)} || A_x(k)_{tors}|$ est fini pour tout premier $\ell \geqslant 0$.

Remarque 1.3.
– *On démontrera ce corollaire seulement lorsque $A_{\overline{\eta}}$ ne contient pas de sous variété abélienne $\bar{k}$-isotriviale. Sans cette hypothèse la preuve dépasse mes connaissances actuelles.*
– *Pour une reformulation plus géométrique du théorème 1.1, voir le théorème 6.1.*

La motivation de ces énoncés est la conjecture de torsion pour les variétés abéliennes.

Conjecture 1.4 (Conjecture de torsion pour les variétés abéliennes sur un corps de type fini de caractéristique 0). *Pour tout corps de type fini k de caractéristique 0 et pour tout entier $d \geqslant 1$, il existe un entier $N := N(k,d) \geqslant 1$ tel que pour tout variété abélienne $A \to k$ de dimension d, on a :*

$$A(k)_{tors} \subset A[N].$$

On peut également énoncer une variante plus faible, où l'on cherche uniquement à borner uniformément l'ordre des ℓ-Sylow :

Conjecture 1.5 (Conjecture de torsion ℓ-primaire pour les variétés abéliennes sur un corps de type fini de caractéristique 0). *Pour tout corps de type fini k de caractéristique 0, pour tout nombre premier ℓ et pour tout entier $d \geqslant 1$, il existe un entier $N := N(k,\ell,d) \geqslant 1$ tel que pour toute variété abélienne $A \to k$ de dimension d, on a :*

$$A(k)_{tors}[\ell^\infty] \subset A[\ell^N].$$

Pour les courbes elliptiques ($d = 1$), la conjecture de torsion ℓ-primaire a été montrée par Y. Manin ([12]). La preuve de la conjecture de torsion est l'aboutissement d'une série de travaux par B. Mazur (cf. [13]), D. Abramovich, L. Merel (cf. [14]).

Définissons brièvement une courbe modulaire. Soit un entier n. On considère le foncteur :

$$\begin{array}{rccl} F_1(n) : & sch^{op} & \to & Sets \\ & S & \mapsto & \left\{ (E,T) \middle| \begin{array}{l} E \to S \text{ schéma abélien dont les fibres sont des} \\ \text{courbe elliptique et } T : S \to E \text{ section de } n\text{-torsion} \end{array} \right\} / \backsim \end{array}$$

où la relation d'équivalence est définie par : $(E,T) \simeq (E,T') \Leftrightarrow \exists \alpha : E \tilde{\to} E'$ un isomorphisme de schémas elliptique tel que $\alpha \circ T = T'$. Ce foncteur n'est pas représentable c'est à dire qu'il n'existe pas un schéma $Y_1(n)$ tel que $F_1(n) = Hom_{sch}(-, Y_1(n))$. Cependant $F_1(n)$ admet des schémas de modules grossier i.e. on a le théorème :

Theorem 1.6. *Il existe une courbe $Y_1(n) \to \mathbb{Q}$ que l'on appelle **courbe modulaire** et un morphisme de foncteur $F_1(n) \xrightarrow{\theta} Hom_{sch}(-, Y_1(n))$ tel que :*

(1) Si $S = spec(\Omega)$ avec Ω corps algébriquement clos alors $Y_1(n)(\Omega) \underset{\theta(\Omega)}{\tilde{\leftarrow}} F_1(n)(spec(\Omega))$ est une bijection.

(2) Pour tout morphisme de foncteur, $F_1(n) \to Hom_{sch}(-, C)$.
On a la factorisation suivante :

$$\begin{array}{ccc} F_1(n) & \longrightarrow & Hom_{sch}(-,C)\,. \\ {\scriptstyle\theta}\downarrow & \nearrow & \\ Hom_{sch}(-, Y_1(n)) & & \end{array}$$

En outre, pour toute extension $k/\mathbb{Q}$, θ induit une bijection $F_1(n)(spec(k)) \underset{\theta(k)}{\tilde{\to}} Y_1(n)(k)$.

Les preuves de Y. Manin puis D. Abranomovich, L. Merel ont consisté à montrer que $Y_1(\ell^n)(k) = \varnothing$ pour $n \gg 0$ puis que $Y_1(\ell)(k)$ pour $\ell \gg 0$. On verra que la preuve du corollaire 1.2 à partir du théorème 6.1 reprend cette idée pour une définition ad-hoc de l'anogue des courbes modulaires $Y_1(k)$. (cf § 4.2) que nous appellerons "courbes modulaire abstraites" et dont la construction utilise la théorie du groupe fondamental.

Pour $d \geqslant 2$, les conjectures 1.5 et 1.4 sont encore complètement ouvertes. L'une des principales difficultés du cas de la dimension supérieure est que la dimension des espaces de modules de variétés abéliennes (principalement polarisées de dimension $\geqslant 2$) sont de dimension $\geqslant 2$ et que l'arithmétique des variétés de dimension supérieure est extrèmement mal comprise.

Dans leurs travaux [2, 4], A. Cadoret et A. Tamagawa proposent de considérer une situation intermédiaire entre le cas des courbes elliptiques (dont l'espace de module est $\mathbb{P}^1$) et la conjecture de torsion en dimension supérieure. Plus précisément, ils considèrent l'énoncé suivant :

Conjecture 1.7. *Pour tout corps de type fini k de caractéristique 0 et A un schéma abélien sur une courbe X sur k, il existe un entier $N := N(A) \geqslant 1$ tel que pour tout $x \in X(k)$*

$$A_x(k)_{tors} \subset A_x[N].$$

Ainsi que sa variante ℓ-primaire. Autrement dit, ils cherchent à montrer la conjecture de torsion pour les familles de variétés abéliennes *de dimension supérieure* paramétrisées par une courbe.

Dans [2], ils ont établi la conjecture de torsion ℓ-primaire pour les familles de variétés abéliennes sur les courbes (théorème 5.1). Le théorème 6.1 et le corollaire 1.2 sont des résultats partiels en direction de la conjecture de torsion pour les familles de variétés abéliennes sur les courbes.

Ce mémoire est organisé de la manière suivante. Les premières parties ont pour but de replacer le sujet dans son contexte. Pour cela nous poserons d'abord les notations et les conventions ; nous énoncerons ensuite les résultats indispensables à la suite et consacrerons une partie à la construction des courbes modulaires abstraites. Ceci étant fait pour comprendre le cheminement qui a permis d'aboutir au théorème 6.1, on expliquera d'abord la preuve du cas ℓ-primaire résolu en [2]. En combinant ce cas au théorème de Mordell-Weil et en admettant le théorème 6.1, on démontrera le corollaire 1.2, qui est déjà une avancée vers la conjecture de torsion.

La suite du mémoire sera dédiée essentiellement à la preuve du théorème principal 6.1 qui ne sera pas démontré dans le cas où le genre est 1 (preuve dépassant le niveau de M2 classique). Le cas où le genre est supérieur à 2 se résout rapidement en utilisant la variante géométrique du théorème de Lang-Néron avec la formule de Riemann-Hurwitz. Le cas du genre 0 se traite à l'aide d'argument basés sur la formule de Riemann-Hurwitz, la structure spécifique du groupe fondamental $\pi_1(X)$ et le théorème de réduction semi-stable qui induisent une preuve totalement combinatoire.

2. Notations et conventions

(1) **Les corps :**

Dans tout ce qui suit, les corps considérés sont toujours de caractéristique 0. Etant donné un corps k (de caractéristique 0), on note $\bar{k} = (k^{sep})$ sa cloture algébrique et $\Gamma_k = Gal(\bar{k}|k)$ son **groupe de Galois absolu**.

(2) **Les schémas :**

Une **courbe** X sur un corps k désignera un schéma de dimension 1 et lisse, séparé, géométriquement connexe sur k. On notera η_X (ou η) son point générique et $\tilde{X}$ sa compactification lisse. On dira que X est de genre g_X avec r points à l'infini si $\tilde{X}$ est de genre g_X et $\tilde{X}\backslash X$ est de degré r. Soit $x \in X$ (pas nécessairement fermé), on note $\mathcal{O}_{X,x}$ le **germe du faisceau structural** de X, $\mathfrak{M}_{X,x}$ son idéal maximal et $k(x) := \frac{\mathcal{O}_{X,x}}{\mathfrak{M}_{X,x}}$ son **corps résiduel**. On note aussi $\bar{x} : Spec(\Omega) \to X$ **un point géométrique** où $k(x) \hookrightarrow \Omega$ est une extension algébriquement close définissant le point géométrique, on notera Ω par $\overline{k(x)}$ dans la suite.

(3) **Les variétés abéliennes $\bar{\mathbf{k}}$-isotriviales :**

Soit A_η la fibre générique de A ($A \to X \to k$ comme d'habitude) et B une sous variété abélienne de A_η alors B est $\bar{k}$-isotriviale ssi il existe une variété abélienne b sur $\bar{k}$ telle que $b \times_{\bar{k}} \bar{\eta} = B \times_\eta \bar{\eta}$. C'est la notion naturelle de sous variété abélienne constante (au sens ou elle provient - modulo une extension finie - d'une variété abélienne sur le corps de base). Etant donné un schéma abélien $A \to X$, on dira que A vérifie la condition (*) si $A_{\overline{\eta}}$ ne contient pas de sous variété abélienne k-isotriviale non triviale. Ainsi, la condition $(*)$ dit donc que la seule variété abélienne $\mathfrak{b}$ défini comme ci-dessus est la sous variété abélienne triviale, ce qui aura une conséquence pour le théorème 3.1 énoncé plus bas.

(4) **Corps de type fini, corps de fonction :**

Un **corps k est de type fini** si c'est une extension de type fini de son sous-corps premier. Ce corps premier est $\mathbb{Q}$ si k est de caractéristique 0 et $\mathbb{F}_p$ si k est de caractéristique p. Un **corps de fonctions** F sur k est un corps de type fini sur k. De façon équivalente, c'est une extension finie d'un corps de fractions rationnelles à n variables $k(t_1, \ldots, t_n)$. On dit alors que F est un corps de fonctions à n variables. C'est en particulier une extension algébrique de degré de transcendance n sur k. En particulier, le corps de fonction K à une variable est une extension de type finie sur k de degré de transcendance 1.

(5) **Lien entre courbe, corps de fonctions et courbe projective :**

Soit F/k un corps de fonctions de dimension 1.

On appelle **anneau de valuation de** F/k un anneau $\mathcal{O} \subseteq F$ tel que $k \subsetneq \mathcal{O} \subsetneq F$ et pour tout z ∈ F, z ∈ $\mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Une **place** P d'un corps de fonctions F/k est l'idéal maximal de l'anneau de valuation $\mathcal{O}$ de F/k. Tout élément $t \in P$ tel que $P = t\mathcal{O}$ est appelé **uniformisante en P** (ou encore **paramètre local en P**). On notera $\mathbb{P}_F$ l'ensemble des places de F/k. Si $\mathcal{O}$ est un anneau de valuation de F/k et P son idéal maximal, alors $\mathcal{O}$ est uniquement déterminé par P. En effet, $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. On notera donc $\mathcal{O}_P := \mathcal{O}$ **l'anneau de valuation à la place P**. A toute place $P \in \mathbb{P}_F$ on associe une valuation discrète de F/k, $\upsilon_P : F \longrightarrow \mathbb{Z} \cup \infty$ définie par : $\upsilon(0) := \infty$ et $\upsilon_P(z) := n$ pour $z = t^n u$, $u \in \mathcal{O}^*$, $n \in \mathbb{Z}$ et t un uniformisant en P.
Soit Y une k-courbe non singulière de corps de fonctions F.

Pour tout point fermé $P \in Y$, l'anneau local $\mathcal{O}_{Y,P}$ de Y en P, est un anneau local noethérien de dimension 1 et $\mathcal{O}_{Y,P}$ est un anneau de valuation (à la place P) de F/k. Ainsi les anneaux locaux de Y définissent un sous-ensemble de l'ensemble C_F des anneaux de valuations discrètes de F/k. Nous considèrerons les éléments de C_F comme des points c'est-à-dire que nous écrirons $P \in C_F$ où P est considéré comme une place de F/k d'anneau de valuation $\mathcal{O}_{Y,P}$. L'ensemble C_F est infini puisqu'il contient tous les anneaux locaux distincts de toute courbe non singulière de corps de fonctions F. Nous définissons une topologie sur C_F en prenant les ensembles fermés comme étant les sous-ensembles finis, $\varnothing$ et C_F tout entier. Si $U \subseteq C_F$ est un sous-ensemble ouvert de C_F, nous définissons **l'anneau des fonctions régulières** sur U par $\mathcal{O}(U) = \bigcap_{P \in U} \mathcal{O}_{Y,P}$.
Un élément $f \in \mathcal{O}(U)$ définit une fonction :

$$\begin{array}{rccl} f: & U & \to & k \\ & P & \to & f(P) = f \bmod P \end{array}$$

Cela munit C_F d'une structure de courbe projective non singulière.

Theorem 2.1. *Les trois catégories suivantes sont équivalentes :*

(a) les courbes projectives non singulières et les morphismes dominants ;

(b) les courbes quasi-projectives et les applications rationnelles dominantes ;

(c) les corps de fonctions de dimension 1 sur k et les k-homomorphismes.

Le foncteur définissant l'équivalence de catégorie $(b) \simeq (c)$ envoie une courbe sur son corps de fonction, le foncteur envoyant un corps de fonction F sur C_F définit l'équivalence $(c) \simeq (a)$ enfin "l'identité" définit l'équivalence $(a) \simeq (b)$. De plus, on rappelle que toute classe d'équivalence rationnelle de courbes quasi-projective contient une unique courbe projective non singulière.

(6) **Le groupe fondamental :**

On note $\pi_1(X; \bar{x})$ **le groupe fondamental** de X *i.e.* le groupe des automorphismes du foncteur fibre :

$$\begin{array}{rccl} F_{\bar{x}}: & R_X^{\acute{e}t} & \to & \pi_X(X, \bar{\eta}) - Fsets \\ & Y \to X & \mapsto & Y_{\bar{x}} = Y \times_X spec(\Omega) \end{array}$$

où $R_X^{\acute{e}t}$ est la catégorie galoisienne des revêtements étales fini de X et $\bar{x} : spec(\Omega) \to X$ un point géométrique. Lorsque X est connexe, $\pi_1(X; \bar{x})$ ne dépend pas de $\bar{x}$ et on notera souvent $\pi_1(X)$ au lieu de $\pi_1(X; \bar{x})$.

(7) $\mathbf{A[n]}$:

Théorème 2.2 (**Groupes de n-torsion en caractéristique** 0)**.** *Soit A une variété abélienne de dimension g sur un corps algébriquement clos k de caractéristique* 0*. Alors le noyau* $A[n]$ *de la multiplication par n est le schéma en groupes fini, étale sur k tel que :*

$$A[n] \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{2g}$$

Donc, en général, le schéma en groupes $A[n]$ sur k est déterminé par le Γ_k-module $A[n](\bar{k})$. On utilisera la notation $A[n]$ indifféremment pour désigner le schéma en groupes $A[n]$ ou le Γ_k-module $A[n](\bar{k})$.

3. Les théorèmes fondamentaux

Nous énonçons ici quelques théorèmes fondamentaux sur les variétés abéliennes et le groupe fondamental, qui sont des outils clefs de la preuve des résultats. Nous renvoyons aux annexes pour plus de détails.

3.1. **Sur les variétés abéliennes.**

Le théorème de Mordell-Weil - Mordell (1922) pour les courbes elliptiques sur $\mathbb{Q}$, Weil (1929) pour les jacobiennes sur les corps de nombres a été généralisé et étendu par Lang aux variétés abéliennes. Lang et Néron ont étendu aux corps de type finis de caractéristique 0 (cf. [17]). Pour énoncer leurs résultat il faut d'abord introduire la K/k-trace de Chow (cf. [10]) : si K/k est une extension régulière (i.e. $\bar{k} \cap K = k$, k est algébriquement clos dans K) et si A est une variété abélienne définie sur K, il existe une "plus grande sous-variété abélienne de A définie sur k" ; plus précisément, on considère le foncteur :

$$\begin{array}{rccl} F: & VA/k & \to & Mod(\mathbb{Z}) \\ & C & \to & Hom_{VA/K}(C_K, A) \end{array}$$

où VA/k (resp. VA/K) désigne la catégorie des variétés abéliennes sur k (resp. K) et C_K est l'extension des scalaires $C \times_k K$. Ce foncteur est représentable c'est à dire qu'il existe $Tr_{K/k}(A) \to k$ une variété abélienne définie sur k et $\tau : Tr_{K/k}(A) \times_k K \to A$ tel que

$$\begin{array}{lcl} Hom_{VA/k}(-, Tr_{K/k}(A)) & \simeq & F(-) \\ C \to Tr_{K/k}(A) & \hookrightarrow & C_K \to Tr_{K/k}(A)_K \xrightarrow{\tau} A \end{array}$$

Théorème 3.1 (Lang-Néron)**.** *(1) **(Variante géométrique)** Soit K/k un corps de fonction et A une variété abélienne sur K alors $A(K)/Tr_{K/k}(A(k))$ est de type fini.*

*(2) **(Variante arithmétique)** Soit k un corps de type fini et de caractéristique 0 et A une variété abélienne sur k alors $A(k)$ est de type fini.*

La variante arithmétique du théorème de Lang-Néron (qui est le théorème de Mordell-Weil lorsque k est un corps de nombre) implique que si A est une variété abélienne sur un corps de type fini k alors son groupe de torsion $A(k)_{tors}$ est fini, ce qui justifie l'énoncé de la conjecture de torsion. La variante géométrique du théorème de Lang-Néron sera un ingrédient essentiel dans la preuve du théorème 1.1 et justifie l'hypothèse (*) puisque sous cette hypothèse $Tr_{K/k}(A(k)) = (0)$ (cf. § 3).

3.2. **La conjecture de Mordell.**

Conjecture 3.2 (**Conjecture de Mordell ou théorème de Faltings**)**.** *Soit X une courbe propre sur un corps k de type fini et de caractéristique 0. Si X est de genre $\geqslant 2$ alors $X(k)$ est fini.*

3.3. **Le théorème de Riemann-Hurwitz.**

Soit $f : X \to Y$ un morphisme fini et séparable de courbes. On note $R_f := \sum_{x \in X} long(\Omega_{X|Y,x})x$ [1] le diviseur de ramification de $f : X \to Y$.

1. On dit qu'un module M est simple si $M \neq 0$, et si les seuls sous-modules de M sont 0 et M. On dit que M est de longueur n fini si il existe une chaîne $0 = M_0 \subset \cdots \subset M_n = M$ de sous modules de M tel que $\frac{M_{i+1}}{M_i}$ est simple pour tout $i \leqslant n-1$ (en particulier, $M_{i+1} \neq M_i$).

Théorème 3.3 (Riemann-Hurwitz)**.** *Sous les hypothèse précédente, on a :*

$$2(g_X - 1) = 2deg(f)(g_Y - 1) + deg(R_f)$$

De plus, si f est modérément ramifiée, alors

$$deg\ R_f = \sum_{x \in X}(e_x - 1)$$

3.4. **Autour du groupe fondamental.**

3.4.1. *Théorème d'existence de Riemann.* Le théorème d'existence de Riemann permet de décrire le groupe fondamental d'un schéma X localement de type fini sur $\mathbb{C}$, comme complété profini du groupe fondamental topologique de l'espace topologique $X(\mathbb{C})$ associé, ce dernier pouvant parfois se calculer explicitement par des méthodes topologiques.
Soit $(-)^{an} : Sch^{LFT} \to An_{\mathbb{C}}$ le foncteur qui a un schéma X, localement de type fini sur $\mathbb{C}$ lui associe son espace analytique (cf. [6, XII]).

Théorème 3.4 (**Théorème d'existence de Riemann**)**.** *Pour tout schéma X localement de type fini sur $\mathbb{C}$, le foncteur $(-)^{an} : Sch^{LFT} \to An_{\mathbb{C}}$ induit une équivalence de catégories entre la catégorie des revêtements étales de X et celle des revêtements analytiques étales de X^{an}.*

En particulier, comme la catégorie des revêtements analytiques étales de X^{an} est équivalent à la catégorie des revêtements topologiques finis de l'espace topologique de $X(\mathbb{C})$, pour tout $x \in X(\mathbb{C})$, on a un isomorphisme de groupe profini canonique :

$$\pi_1^{top}\widehat{(X(\mathbb{C}), x)} \simeq \pi_1(X, x).$$

(1) Lorsque X est une courbe lisse, séparée sur $\mathbb{C}$ de genre g et telle que $\tilde{X}\backslash X$ est de degré r, $X(\mathbb{C})$ est une surface de Riemann de genre g à r trous dont le groupe fondamental est le groupe libre à $2g + r$ générateurs et une relation :

$$\Gamma_{g,r} = \langle a_1, \ldots, a_g, b_1, \ldots, b_g, \gamma_1, \ldots, \gamma_r \mid [a_1, b_1] \cdots [a_g, b_g]\gamma_1 \cdots \gamma_r = 1 \rangle.$$

(2) Lorsque X est une variété abélienne de dimension g, $X(\mathbb{C})$ est un tore $\mathbb{C}^g/\Lambda$ (où $\Lambda \simeq \mathbb{Z}^{2g} \subset \mathbb{C}^g$ est un réseau). Le revêtement universel de $X(\mathbb{C})$ est le morphisme quotient :

$$\mathbb{C}^g \twoheadrightarrow \mathbb{C}^g/\Lambda$$

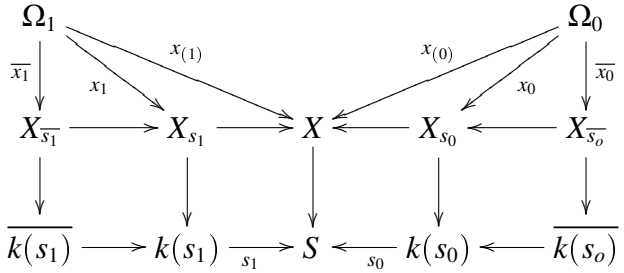
dont le groupe d'automorporhisme est Λ.
C'est ainsi que l'on obtient $\pi_1^{top}(X(\mathbb{C})) = \Lambda$, or $\pi_1(X, x) = \hat{\Lambda} = \widehat{\mathbb{Z}^{2g}} = \prod_{\ell} \mathbb{Z}_{\ell}^{2g}$, on montre ainsi que $\pi_1(X, 0) = \prod_{\ell} T_{\ell}(A)$. Notons qu'il existe une preuve purement algébrique ([16]) du fait que si X est une variété abélienne sur un corps algébriquement clos de caractéristique 0 alors :

$$\pi_1(X, 0) = \prod_{\ell} T_{\ell}(A).$$

En caractéristique 0, le groupe fondamental d'un schéma de type fini est invariant par extension de corps algébriquement clos (dans le cas des schémas propres, cela peut se voir comme un cas particulier du théorème de spécialisation, dans le cas général, voir par exemple l'argument dans [22, p 190-191]).

On utilisera ici le fait que le théorème d'existence de Riemann implique en particulier que le groupe profini $G := \pi_1(X, x)$ est de type fini. On peut alors montrer que $\forall n \in \mathbb{N}^*$, l'ensemble $S(G,\ n) := \{U < G$ sous groupe ouvert tel que $[G : U] \leqslant n\}$ est fini.

3.4.2. *Théorème de spécialisation.* Soit S un schéma connexe et localement nothérien et $f : X \to S$ un morphisme propre tel que $f_*\mathcal{O}_X = \mathcal{O}_S$ (Ainsi, en particulier, $f : X \to S$ est surjective géométriquement connexe et X est connexe). Le théorème de spécialisation ou semi-continuité du groupe fondamental permet de comparer les groupes fondamentaux des fibres de $X \to S$.
Fixons deux points $s_0,\ s_1 \in S$ avec $s_0 \in \overline{\{s_1\}}$ et considérons les notations suivantes :



Théorème 3.5 (**Semi-continuité du groupe fondamental**). *Il existe un morphisme de groupes profinis :*

$$sp : \pi_1(X_{\overline{s_1}},\ \bar{x_1}) \to \pi_1(X_{\overline{s_0}},\ \overline{x_0})$$

défini canoniquement à automorphisme intérieur prés. De plus,

(1) si $f : X \to S$ est séparable alors $sp : \pi_1(X_{\overline{s_1}},\ \overline{x_1}) \twoheadrightarrow \pi_1(X_{\overline{s_0}},\ \overline{x_0})$ est un épimorphisme ;

(2) si $f : X \to S$ est lisse alors $sp : \pi_1(X_{\overline{s_1}},\ \overline{x_1}) \xrightarrow{\sim} \pi_1(X_{\overline{s_0}},\ \overline{x_0})$ est un isomorphisme.

Le morphisme $sp : \pi_1(X_{\overline{s_1}}, \overline{x_1}) \to \pi_1(X_{\overline{s_0}},\ \overline{x_0})$ est appelé le **morphisme de spécialisation** de s_1 vers s_0.

On appliquera ce théorème lorsque $X \to S$ est un schéma abélien et S une courbe sur un corps k (de caractéristique 0), $s_1 = \eta$ est le point générique de S et $s_0 = s$ est un point fermé de S. s induit alors une section $\sigma_s : \Gamma_{k(s)} \to \pi_1(S)$ bien définie à conjugaison intérieure près par les éléments de $\pi_1(S_{\overline{k}})$ identifiant le groupe de décomposition de s à $\Gamma_{k(s)}$. Le morphisme de spécialisation :

$$sp : \pi_1(X_{\overline{\eta}}, \overline{0}) \xrightarrow{\sim} \pi_1(X_{\overline{s}},\ \overline{0})$$

est alors Galois-équivariant au sens où :

$$sp(\sigma_s(\tau)\gamma) = \tau sp(\gamma),\ \gamma \in \pi_1(X_{\overline{\eta}}, \overline{0}),\ \tau \in \Gamma_{k(s)}.$$

Comme $sp : \pi_1(X_{\overline{\eta}}, \overline{0}) \xrightarrow{\sim} \pi_1(X_{\overline{s}},\ \overline{0})$ est un isomorphisme de groupes profinis, il préserve les ℓ-Sylow donc induit :

$$sp : T_\ell(X_{\overline{\eta}}) \xrightarrow{\sim} T_\ell(X_{\overline{s}})$$

Il envoie également $\ell^n T_\ell(X_{\overline{\eta}})$ sur $\ell^n T_\ell(X_{\overline{s}})$ donc induit :

$$sp : X_{\overline{\eta}}[\ell^n] \xrightarrow{\sim} X_{\overline{s}}[\ell^n]$$

et donc, pour tout entier $n \geqslant 1$:

$$sp : X_{\overline{\eta}}[n] \xrightarrow{\sim} X_{\overline{s}}[n]$$

4. Construction des courbes modulaires abstraites

Soit un entier $n \geqslant 0$

4.1. **La représentation $\rho_{\mathbf{A,n}} : \pi_1(\mathbf{X}) \to \mathrm{GL}(\mathbf{A}_\eta[\mathbf{n}])$ et son image $\mathbf{G_n}$.** On va construire des représentations canoniques de $\pi_1(X)$ dans le groupe des points (génériques) de n-torsion.

On rappelle que pour tout schéma V sur k, on définit une action naturelle de Γ_k sur les points $\bar{k}$-rationnels de V comme suit. Pour tout $u \in V(\bar{k})$ et $\sigma \in \Gamma_k$ induisant un morphisme $\tilde{\sigma} : spec(\bar{k}) \to spec(\bar{k})$.

$$\begin{array}{ccc} \Gamma_k \times V(\bar{k}) & \to & V(\bar{k}) \\ (\sigma, u) & \mapsto & \sigma.u := u \circ \tilde{\sigma} \end{array}$$

En particulier, on a l'action :

$$(\triangle) \quad \Gamma_{k(\eta)} \times A_\eta[n] \to A_\eta[n]$$

Comme la structure du groupe algébrique de A_η est définie sur $k(\eta)$, cette action est en fait une action par automorphisme de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$-module. Soit $\bar{\eta} : \overline{k(\eta)} \to X$ le point générique géométrique associé à X. Comme X est un schéma connexe normal, on a une surjection $s : \Gamma_{k(\eta)} \twoheadrightarrow \pi_1(X, \bar{\eta})$ (cf. [3, cor.6.2.4]). L'action $(\triangle)$ se factorise via s et induit une action par le critère de bonne réduction (cf. [20, thm 5 p 183]) : $\pi_1(X) \times A_\eta[n] \to A_\eta[n]$ par automorphisme de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$- module i.e. un morphisme de groupes $\rho_{A,n} : \pi_1(X) \to Aut_{\frac{\mathbb{Z}}{n\mathbb{Z}}}(A_\eta[n]) \simeq GL_{2g}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ ($A_\eta[n] \simeq (\frac{\mathbb{Z}}{n\mathbb{Z}})^{2d}$ par le théorème 2.2).

L'action $\pi_1(X) \times A_\eta[n] \to A_\eta[n]$ peut se définir d'une autre manière, on obtient alors la représentation sans utiliser l'hypothèse "X normal". Soit $A \to X$ un schéma abélien, $A[n] \to X$ est un schéma fini étale (revêtement étale) donc en particulier, l'équivalence de catégorie :

$$\begin{array}{rccc} F_{\bar{\eta}} : & R_X^{\acute{e}t} & \tilde{\to} & \pi_1(X, \bar{\eta})\text{-}Fsets \\ & Y \to X & \mapsto & Y_{\bar{\eta}} \end{array}$$

induit automatiquement donc une action de $\pi_1(X, \bar{\eta})$ sur $Y_{\bar{\eta}}$. Donc $A[n]_{\bar{\eta}} = A_{\bar{\eta}}[n]$ (la multiplication commute au changement de base) est un $\pi_1(X, \bar{\eta})$-ensemble fini. Quand X est normal, les deux actions coïncident.

4.2. **Utilisation du dictionnaire pour la construction des courbes.** On rappelle que $\pi_1(X)$ est muni d'une structure de groupe profini. Ainsi, un groupe ouvert $U \subset_{op} \pi_1(X)$ est un sous groupe fermé d'indice fini. En particulier, $\frac{\pi_1(X)}{U}$ est un ensemble fini sur lequel $\pi_1(X)$ agit continuement par translation à gauche. Par la théorie de Galois, il correspond donc à un revêtement fini étale de X, que l'on notera $X_U \to X$ (et $U = \pi_1(X_U)$). Comme X est géométriquement connexe, on a la suite exacte courte :

$$1 \to \pi_1(X_{\bar{k}}) \to \pi_1(X) \xrightarrow{p} \Gamma_k \to 1 \text{ (cf. [3, Prop.7.0.6])}$$

avec $p(U) = \Gamma_{k_U} \subset \Gamma_k$, k_U est le corps de définition de X_U.

Lorsque X est normal (ce qui est notre cas), on peut décrire $X_U \to X$ plus concrètement comme suit. Considérons de nouveau la surjection $s : \Gamma_{k(\eta)} \twoheadrightarrow \pi_1(X)$. Pour tout U sous-groupe ouvert de $\pi_1(X)$, $s^{-1}(U)$ est un sous groupe ouvert de $\Gamma_{k(\eta)}$ donc par la théorie de Galois "usuelle", il correspond à une extension fini $K_U/k(\eta)$. X_U est la normalisation de X dans $K_U/k(\eta)$ et $k_U = K_U \cap \bar{k}$.

♣ Les courbes $\mathbf{X_v}$, $\mathbf{X_n}$ et $\mathbf{X_{n^n}}$

On notera :
- $X_U = X_{(n)}$ pour $U = ker(\rho_{A,n}) \lhd_{op} \pi_1(X)$;
- $X_U = X_v$ pour $U = Stab_{\pi_1(X)}(v) <_{op} \pi_1(X)$, $v \in A_\eta[n]$.

Notons que, comme $ker(\rho_{A,n})$ est distingué dans $\pi_1(X)$, $X_{(n)} \to X$ est un revêtement galoisien de groupe de Galois $Im(\rho_{A,n}) = G_n$.
Enfin on notera

$$X_n = \bigsqcup_{\substack{|\langle v \rangle|=n \\ v \in A_\eta[n]}} X_v$$

♣ **La notation g_n**

On pose :

$$g_n := \min_{v \in A_\eta[n]^\times} \{g_{X_v}\}.$$

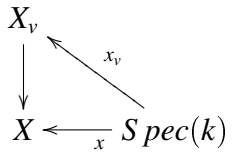
où $A_\eta[n]^\times$ pour l'ensemble des points de torsion d'ordre exactement n.

♣ **L'image G_M et le noyau K_M de $\rho_{A,M}$**

Pour chaque premier n on note G_n l'image de $\rho_{A,n} : \pi_1(X) \to GL(A_\eta[n])$. Plus généralement, si on se donne M un $\pi_1(X)$-sous module de $A_\eta[n]$ on note $\rho_{A,M} : \pi_1(X) \to GL(M)$ la représentation, G_M son image et K_M son noyau.

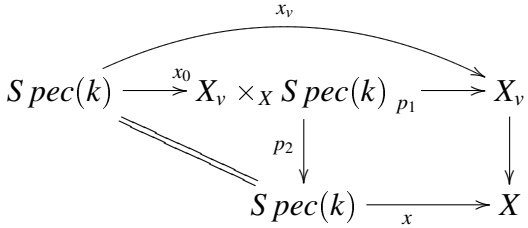
4.3. **Un lemme pour une reformulation du problème.** Pour tout point k-rationnel $x : Spec(k) \to X$, on considère l'isomorphisme (cf. § 3.4.2) de $\pi_1(X)$-module $sp : A_\eta[m] \xrightarrow{\sim} A_x[m]$. Soit $v \in A_\eta[m]^\times$.

Lemme 4.1. *Sous les hypothèses précédentes, on a l'équivalence $sp(v) \in A_x(k)_{tors}[m]$ si et seulement si $x : Spec(k) \to X$ se révèle en un point k-rationnel :*



Démonstration. On note encore par x la section $\Gamma_k \hookrightarrow \pi_1(X)$ de $\pi_1(X) \to \Gamma_k$ induite (à conjugaison près) par $x : Spec(k) \to X$, alors l'existence d'un relèvement $x_v : Spec(k) \to X_v$ de $x : \Gamma_k \hookrightarrow \pi_1(X)$ est équivalente à l'inclusion de $x(\Gamma_k) \subset \pi_1(X_v)$; ceci est à nouveau une conséquence de la théorie de Galois.

En effet, au morphisme $x : \Gamma \to \pi_1(X)$ correspond le foncteur fondamental $H : R_X^{et} \to R_k^{et}$ de changement de base. Et d'après [3, lemme 4.2.1], l'inclusion $Im(x) \subset \pi_1(X_v) = stab_{\pi_1(X)}(v)$ est équivalente à l'existence d'un homomorphisme de revêtement étale fini x_0 qui rend le diagramme suivant commutatif.



Enfin, la donnée de x_0 est équivalente à celle de x_v (si on se donne x_0, on prend $x_v = p_1 \circ x_0$ et réciproquement, si on se donne x_v, x_0 est donnée par la propriété universelle du produit fibré).
Il reste à voir que $x(\Gamma_k) \subset \pi_1(X_v) = stab_{\pi_1(X)}(v)$ est équivalent à $v \in A_x(k)_{tors}[m]$.

D'une part, on a les applications et les actions suivantes

$$\begin{array}{ccc} A_\eta[m] & \underset{sp}{\xrightarrow{\sim}} & A_x[m] \\ \circlearrowleft & & \circlearrowleft \\ \pi_1(X) & \underset{x}{\leftarrow} & \Gamma_k \end{array}$$

Ainsi, pour tout $\tau \in \Gamma_k$ et $v \in A_\eta[m]$, $\tau.sp(v) = sp(\sigma_x(\tau).v)$ $(\triangle)$.

D'autre part, en réécrivant l'inclusion $x(\Gamma_k) \subset Stab_{\pi_1(X)}(v)$, on obtient $\forall \tau \in \Gamma_k,\ x(\tau).v = v$ et en appliquant le morphisme de spécialisation qui est un isomorphisme, l'égalité précédente est équivalent à : $\forall \tau \in \Gamma_k,\ sp(x(\tau).v) = sp(v)$ Par $(\triangle)$, on a $\forall \tau \in \Gamma_k,\ \tau.sp(v) = sp(v)$ c'est à dire $sp(v_m) \subset A_x(k)_{tors}[m]$. CQFD □

5. Cas ℓ-primaire versus cas général

Dans la suite, ℓ désigne un premier et n un entier.

5.1. **Schéma de la preuve de la conjecture 1.5 ([2, thm. 1.1, cor. 1.2]).** Ce qui différencie fondamentalement le cas ℓ-primaire du cas général est que, dans le cas ℓ-primaire, on dispose d'une structure de système projectif naturelle donnée par la multiplication par ℓ :

$$A[\ell^{n+1}] \to A[\ell^n],\ n \geqslant 0$$

qui, à son tour, induit une structure de système projectif :

$$X_{\ell^{n+1}} \to X_{\ell^n},\ n \geqslant 0.$$

Alors que cet aspect disparait complètement lorsqu'on s'intéresse au cas général.
Il est question plus exactement dans l'article [2] de démontrer le théorème suivant qui est une version plus faible de la conjecture 1.5 :

Théorème 5.1. *Soit X une courbe lisse, séparée et géométriquement connexe sur k. On considère une variété abélienne A sur k et $A \to X$ un schéma abélien de fibre générique $A_\eta \to Spec(k(s))$ de dimension d. Si on suppose que k est de type fini sur $\mathbb{Q}$. Alors il existe un entier $N := N(A, X, k, \ell)$ tel que $\forall x \in X(k)$, le Γ_k-module $A_x(k)_{tors}[\ell^\infty]$ est contenu dans $A_x[\ell^N]$.*

La preuve se décompose en trois étapes :

(1) On reformule le résultat que l'on veut établir en $X_{\ell^n}(k) = \varnothing,\ n \gg 0$, (application directe du lemme 4.1 pour $m = \ell^n$).

(2) Par le théorème de Lang-Néron (variante arithmétique) on a :

$$\varprojlim X_{\ell^n}(k) = \varnothing$$

En effet, dans le cas contraire, considérons $a \in \varprojlim X_{\ell^n}(k)$, par définition pour tout $n \in \mathbb{N}$, si on note $x_n : X_{\ell^{n+1}}(k) \to X_{\ell^n}(k)$ les applications de transitions du sytème projectif et $\pi_n : \varprojlim X_{\ell^n}(k) \to X_{\ell^n}(k)$ les projections, on a $x_n(\pi_{n+1}(a)) = \pi_n(a)$. Or par le lemme 4.1, à tout $\pi_n(a) \in X_{\ell^n}(k)$ correspond un élément $v_n \in A_\eta[\ell^n]^\times$ tel que $sp(v_n) \in A_{\pi_n(a)}(k)_{tors}[\ell^n]$ et nous avons donc une infinité d'éléments dans $A_{\pi_n(a)}(k)_{tors}$, ce qui est en contradiction avec le théorème 3.1.

(3) Le point crucial et difficile est l'énoncé géométrique suivant :

Théorème 5.2. *Si $A_{\overline{\eta}}$ vérifie (*) alors :*

$$\lim_{n \to \infty} g_{\ell^n} = +\infty.$$

(4) Supposons que $A_{\overline{\eta}}$ vérifie (*) alors, d'après (2) et la conjecture de Mordell, $X_{\ell^n}(k)$ est fini pour $\ell \gg 0$. Comme la limite projective d'un système projectif d'ensembles finis non vides est non vide, on déduit de (1) que $X_{\ell^n}(k) = \varnothing,\ n \gg 0$. Dans le cas où $A_{\overline{\eta}}$ ne vérifie pas (*), il faut raffiner un peu la preuve.

Notons également que la preuve du théorème 5.2 exploite elle-aussi les structures de système projectif ci-dessus de façon cruciale.

5.2. **Une première étape vers le cas général.** La conjecture 1.7 est donc la généralisation naturelle du théorème 5.1 et le théorème 1.1 (sans l'hypothèse de semi-stabilité) est l'analogue du théorème 5.2. Il n'est cependant pas suffisant pour établir que $X_n(k) = \varnothing,\ n \gg 0$ car l'argument de système projectif de l'étape (3) dans le cas ℓ-primaire, permettant de passer de "fini à vide" ne s'applique plus. Cependant, en combinant le cas ℓ-primaire, le théorème 1.1 et la conjecture de Mordell, on obtient le corollaire 1.2 comme suit.

Supposons que A vérifie la condition (*) alors, d'après le théorème 1.1 on a :

$$\lim_{\substack{\ell\to\infty \\ \ell \text{ premier}}} g_\ell = \infty.$$

En particulier, il existe $N \geqslant 0$ tel que $g_\ell \geqslant 2$, $\ell \geqslant N$ donc, par la conjecture de Mordell, $X_\ell(k)$ est fini pour $\ell \geqslant N$.

Soit ℓ un nombre premier. On distinguera deux cas :

(1) $\ell \geqslant N$: Notons F_ℓ l'image de $X_\ell(k) \to X(k)$. On vient de voir que F_ℓ est fini. Mais par définition, F_ℓ est l'ensemble des $x \in X(k)$ tels qu'il existe $v \in A_\eta[\ell]^\times$ et $x_v \in X_v(k)$ d'image x par $X_\ell(k) \to X(k)$. Par le lemme 4.1, c'est également l'ensemble des $x \in X(k)$ tels qu'il existe $v \in A_\eta[\ell]^\times$ tel que $sp_x(v) \in A_x[\ell](k)$ autrement dit, c'est l'ensemble des $x \in X(k)$ tels que $sp_x^{-1}(A_x[\ell]^\times(k)) \neq \varnothing$ ou encore, puisque $sp_x : A_\eta[\ell] \tilde{\to} A_x[\ell]$ est un isomorphisme, l'ensemble des $x \in X(k)$ tels que $A_x[\ell]^\times(k) \neq \varnothing$ *i.e.* $\ell \,||A_x(k)_{tors}|$. D'où l'assertion (i).

(2) $\ell < N$: D'après la conjecture 1.5 dans le cas ℓ-primaire, il existe $n(\ell) \geqslant 1$ tel que $X_{\ell^{n(\ell)}}(k) = \varnothing$, $n > n(\ell)$ et donc, par le même argument que ci-dessus, on obtient que l'ensemble des $x \in X(k)$ tels que $\ell^{n(\ell)} \,||A_x(k)_{tors}|$ est vide (donc, à fortiori, fini). D'où l'assertion (ii).

Comme nous l'avons déjà indiqué, il faut raffiner un peu la preuve pour traiter le cas où A_η ne vérifie pas la condition (*).

Le dernier chapitre de ce mémoire est consacré à la preuve du théorème 6.1 dans le cas où X est soit de genre $\geqslant 2$, soit de genre 0. Le cas du genre 1 repose sur des arguments dépassant le niveau d'un mémoire de M2 classique et ne sera pas du tout abordé ici.

6. La preuve du théorème 6.1

Avec les notations précédentes le théorème 1.1 devient :

Théorème 6.1. *Soit F un corps de caractéristique 0, X une courbe lisse, séparée et géométriquement connexe sur F et $A \to X$ un schéma abélien tel que A_η qui ne contient pas de sous variété k-isotriviale abelienne non triviale. Supposons que soit $g_X \geqslant 1$ soit $A \to X$ admet une réduction semi-stable sur tous les points sauf pour au plus un point de $\tilde{X}\backslash X$. Alors*

$$\lim_{\substack{\ell\to\infty \\ \ell \text{ premier}}} g_\ell = \infty$$

6.1. **Quelques lemmes.** On reprend les notations du début pour démontrer deux lemmes utiles pour la suite. Le premier lemme est une conséquence du théorème 3.1 :

Lemme 6.2. *(1)* $A_\eta[\ell]^{G_\ell} = 0$ pour $\ell \gg 0$.

(2) $\lim_{\ell\mapsto\infty} \min_{v\in A_\eta[\ell]^\times} \{|G_\ell v|\} = +\infty$.

En particulier, $\lim_{\ell\mapsto\infty} \min_{0\neq M\subset A_\eta[\ell]} \{|G_M|\} = +\infty$.

Démonstration. (1) On a : $A_\eta[\ell]^{G_\ell} = A_\eta[\ell]^{\pi_1(X)} = A_\eta[\ell]^{\Gamma_{k(\eta)}} = A_\eta(k(\eta))[\ell] \subset A_\eta(k(\eta))_{tors}$, qui est fini, par le théorème de Lang-Néron variante géométrique et l'hypothèse (*).
(2) Raisonnons par l'absurde et supposons qu'il existe un entier $B \geqslant 1$ tel que pour une infinité de premiers ℓ il existe $v_\ell \in A_\eta[\ell]^\times$ tel que $|G_\ell v_\ell| = deg(X_{v_\ell} \to X) = [\pi_1(X) : \pi_1(X_{v_\ell})] \leqslant B$.
Par le théorème d'existence de Riemann, $\pi_1(X)$ est topologiquement de type fini donc il n'y a qu'un nombre fini de revêtements étales finis de X de degré $\leqslant B$.
Ainsi, quitte à remplacer X par un de ces revêtements, on peut supposer que pour une infinité de premiers ℓ il existe $v_\ell \in A_\eta[\ell]^\times$ tel que $|G_\ell v_\ell| = 1$, ce qui contredit (1).
La deuxième assertion de (2) provient du fait que : $|G_M| \geqslant |G_\ell v| \ \forall v \in M\backslash\{0\}$. En effet, $G_M.v = G_\ell.v$ (cf § 4.2). Ainsi, $|G_M| \geqslant \frac{|G_M|}{|Stab_{G_\ell}(v)|} = |G_M.v| = |G_\ell.v|$. □

Le deuxième lemme est une réécriture de la formule de Riemann-Hurwitz (cf. annexes thm 3.3). Pour chaque $P \in \tilde{X}\backslash X$, on note $I_{P,\ell} \subset G_\ell$ l'image du groupe d'inertie I_P au point P dans G_ℓ (bien défini à conjugaison près).

Lemme 6.3. *Soit $v \in A_\eta[\ell]$. Pour chaque $Q \in \tilde{X}_v \smallsetminus X_v$, soit $e(Q) \geqslant 1$ l'indice de ramification en Q du revêtement $\pi_v : \tilde{X}_v \to \tilde{X}$.*
Alors on a :

$$\begin{aligned} 2g_{X_v} - 2 &= |G_\ell v|(2g_X - 2) + \sum_{P \in \tilde{X}\backslash X} \sum_{Q \in \pi_v^{-1}(P)} (e(Q) - 1) \\ &= |G_\ell v|(2g_X - 2) + \sum_{P \in \tilde{X}\backslash X} (|G_\ell v| - |I_{P,\ell}\backslash G_\ell v|) \end{aligned}$$

Démonstration. La première égalité est la formule de Riemann-Hurwitz pour le revêtement (ramifié) $\pi_v : \tilde{X}_v \to \tilde{X}$. Comme π_v est de degré $|G_l v|$, on a également :

$$\sum_{Q \in \pi_v^{-1}(P)} e(Q) = \deg(\pi_v) = |G_\ell v|.$$

Enfin, $\sum_{Q \in \pi_v^{-1}(P)} 1 = |\pi_v^{-1}(P)|$. Il reste donc à voir que $\pi_v^{-1}(P) \simeq I_{P,\ell}\backslash G_\ell v$. Pour cela, considérons le diagramme de revêtements :

$$\begin{array}{ccc} X_\ell & \xrightarrow{\pi_{\ell,v}} & X_v \\ & \searrow^{\pi_\ell} & \downarrow{\scriptstyle \pi_v} \\ & & X \end{array}$$

$\pi_\ell : X_\ell \to X$ est galoisien de groupe G_ℓ donc $\pi_\ell^{-1}(P)$ est en bijection avec $I_{P,\ell}\backslash G_\ell$ (notons que comme k est algébriquement clos, groupes de décomposition et groupes d'inertie coincident). Et $\pi_{\ell,v} : X_\ell \to X$ est le quotient de X_ℓ par le sous-groupe d'automorphismes Stab $_{G_\ell}(v) \subset G_\ell$ donc :

$$\pi_v^{-1}(P) \simeq \pi_{\ell,v}(\pi_\ell^{-1}(P)) \simeq (I_{P,\ell}\backslash G_\ell)/\mathrm{Stab}_{G_\ell}(v).$$

On vérifie immédiatement que :

$$(I_{P,\ell}\backslash G_\ell)/\mathrm{Stab}_{G_\ell}(v) \simeq I_{P,\ell}\backslash(G_\ell/\mathrm{Stab}_{G_\ell}(v)) \simeq I_{P,\ell}\backslash G_\ell v.$$

□

6.2. **La preuve dans le cas où $g_X \geqslant 2$.** Par le lemme 6.3, on a : $2g_{X_v} - 2 \geqslant |G_\ell v|(2g_X - 2)$. Ainsi, $g_{X_v} \geqslant |G_\ell v|(g_X - 1) + 1$. Le théorème 6.1 découle alors du lemme 6.2 (2).

6.3. **La preuve dans le cas où $g_X = 1$.** Omis.

6.4. **La preuve dans le cas où $g_X = 0$.**

6.4.1. *Le théorème de Réduction semi stable (cf. Annexes).* On notera $PB,\ SS,\ PSS \subset \tilde{X} \smallsetminus X$ pour les sous-ensembles correspondant aux places qui ont une réduction :
- **PB** : potentiellement bonne (mais pas bonne)
- **SS** : semi-stable (mais pas bonne)
- **PSS** : potentiellement semi-stable (mais ni semi-stable ni bonne)

Pour chaque place $P \in \tilde{X} \smallsetminus X$ et pour tout premier ℓ, nous noterons $I_{P,\ell}$ l'image du groupe d'inertie I_P en P dans G_ℓ, qui est un groupe cyclique (k est de caractéristique 0).

Par le théorème de réduction semistable [7, Exp. IX] on a le résultat suivant :
- si $P \in$ **PB** alors il existe un entier $N_P \geqslant 2$ tel que $I_{P,\ell}^{N_P} = 1$ pour tout ℓ et que $I_{P,\ell}^{N} \neq 1$ pour $N < N_P$ et $\ell \gg 0$.
- Si $P \in$ **SS** alors $I_{P,\ell}$ est unipotent [2] d'échelon 2 .
- Si $P \in$ **PSS** alors il existe un entier $N_P \geqslant 2$ tel que $I_{P,\ell}^{N_P}$ est unipotent d'échelon 2 pour tout ℓ et que $I_{P,\ell}^{N}$ n'est pas unipotent pour $N < N_P$ et $\ell \gg 0$.

Nous dirons que $A \to X$ admet une réduction du type $(n_P)_{P\in\tilde{X}\smallsetminus X}$, où

$$n_P := \begin{array}{ll} N_P, & P \in PB\,; \\ \infty, & P \in SS\,; \\ N_P\infty, & P \in PSS\,. \end{array}$$

Avant de poursuivre la preuve du théorème 6.1, nous allons décrire brièvement la stratégie.

6.4.2. *Réduction à un problème combinatoire.* Pour tout ℓ, soit $v_\ell \in A_\eta[\ell]^\times$ tel que $g_\ell = g_{X_{v_\ell}}$.
Par le lemme 6.3, on a

$$\begin{aligned} 2g_{X_{v_\ell}} - 2 &= |G_\ell v_\ell|(2g_X - 2) + \sum_{P\in\tilde{X}\smallsetminus X} |G_\ell v_\ell| - |I_{P,\ell}\backslash G_\ell v_\ell| \\ &= -2|G_\ell v_\ell| + \sum_{P\in\tilde{X}\smallsetminus X} |G_\ell v_\ell|(1 - \varepsilon_P(v_\ell)) \end{aligned}$$

avec

$$\varepsilon_P(v_\ell) = \frac{|I_{P,\ell}\backslash G_\ell v_\ell|}{|G_\ell v_\ell|},\ P \in \tilde{X} \smallsetminus X.$$

Posons

$$\lambda_{v_\ell} := \frac{2g_{X_{v_\ell}} - 2}{|G_\ell v_\ell|} = r - 2 - \sum_{P\in\tilde{X}\smallsetminus X} \varepsilon_P(v_\ell) \quad \text{où } r := |\tilde{X} \smallsetminus X|.$$

Alors $g_\ell \geqslant 2$ pour $\ell \gg 0$ si et seulement si $\lambda_{v_\ell} > 0$ pour $\ell \gg 0$ (ou, de manière équivalente $\sum_{P\in\tilde{X}\smallsetminus X} \varepsilon_P(v_\ell) < r - 2$ pour $\ell \gg 0$). Et, par le lemme 6.2 (2), on a : $\lim\limits_{\ell\mapsto\infty} \min\limits_{v\in A_\eta[\ell]^\times} \{|G_\ell v|\} = +\infty$. Or par hypothèse on a $g_\ell = g_{X_{v_\ell}}$. Donc, on a $\lim\limits_{\ell\mapsto\infty} g_\ell = +\infty$ si il existe $\varepsilon > 0$ tel que $\lambda_{v_\ell} > \varepsilon$ (ou, de manière équivalente, $\sum_{P\in\tilde{X}\smallsetminus X} \varepsilon_P(v_\ell) < r - 2 - \varepsilon$), pour $\ell \gg 0$.

Il s'agit alors d'estimer la taille du " terme local" $\sum_{P\in\tilde{X}\smallsetminus X} \varepsilon_P(v_\ell)$. Sous la condition de semistabilité du théorème 1.1, la preuve réside en des manipulations combinatoires basées sur la structure spécifique de $\pi_1(X)$ lorsque $g_X = 0$.

2. On rappelle qu'un groupe G unipotent d'échelon 2 est un groupe dont tous les élément sont unipotents d'échelon 2 (i.e. $\forall\gamma \in G \smallsetminus \{1\}$, $(\gamma - 1)^2 = 0$).

6.4.3. *La preuve (combinatoire).* Dans la suite, on écrira $\tilde{X} \smallsetminus X = \{P_1, \dots, P_r\}$ Rappelons que $\pi_1(X)$ est la complétion profini du groupe $\Gamma_{0,r}$ engendré par les $\gamma_1, \dots, \gamma_r$ et la relation $\gamma_1 \cdots \gamma_r = 1$, où γ_i est un générateur de I_{P_i}. On notera $\gamma_{i,\ell}$ l'image de γ_i dans G_ℓ (donc $I_{P_i,\ell} = \langle \gamma_{i,\ell} \rangle$).
Pour finir, introduisons :

$$\mathcal{O}_{i,n} = \{\omega \in G_\ell v \text{ tel que } |\langle \gamma_{i,\ell} \rangle \omega| = n\}$$

Donc, en faisant agir $I_{P_i,\ell}$ sur $\mathcal{O}_{i,n}$, on a en particulier, $\begin{cases} \mathcal{O}_{i,1} &= (G_\ell v)^{I_{P_i,\ell}} \\ \mathcal{O}_{i,n} &= \varnothing \text{ sauf si } n \mid |I_{P_i,\ell}| \end{cases}$

6.4.3.1. Un calcul général. Pour tout sous ensemble $I \subset \{1, \dots, r\}$, posons :

$$E_I := \bigcap_{i \in I} \mathcal{O}_{i,1} = (G_\ell v)^{\langle \gamma_i | i \in I \rangle}$$

(Ainsi, en particulier, $E_\varnothing = G_\ell v$).
Et, pour chaque $0 \leqslant i \leqslant r$, posons :

$$\Sigma_i := \sum_{I \subset \{1,\dots r\},\ |I|=i} |E_I|,$$

$$\overline{\Sigma}_i := |\bigcup_{I \subset \{1,\dots r\},\ |I|=i} E_I|.$$

De la même manière, définissons les variantes $*$, pour tout sous ensemble $I \subset \{1, \dots, r\}$,

$$E_I^* := E_I \smallsetminus \bigcup_{I \subsetneq J} E_J$$

et, pour tout $1 \leqslant i \leqslant r$,

$$\Sigma_i^* := \sum_{I \subset \{1,\dots r\},\ |I|=i} |E_I^*|,$$

$$\overline{\Sigma}_i^* := |\bigcup_{I \subset \{1,\dots r\},\ |I|=i} E_I^*|.$$

Remarquons que, en fait, $\overline{\Sigma}_i^* = \Sigma_i^*$, $i = 0, \dots, r$, puisque les E_I^* sont disjoints.

Considérons dès à présent l'application :

$$\begin{array}{rccl} \nu : & G_\ell v & \to & \{0, \dots, r\} \\ & \omega & \mapsto & \nu(\omega) := |\{1 \leqslant i \leqslant r \mid \omega \in E_{\{i\}}\}|. \end{array}$$

On rapelle que $E_i = {G_\ell v}^{\gamma_i}$. Alors,

$$\Sigma_1 = \sum_{1 \leqslant i \leqslant r} |E_{\{i\}}| = \sum_{\omega \in G_\ell v} \nu(\omega) = \sum_{0 \leqslant i \leqslant r} i |\nu^{-1}(i)| = \sum_{0 \leqslant i \leqslant r} i \overline{\Sigma}_i^* = \sum_{0 \leqslant i \leqslant r} i \Sigma_i^*.^3$$

D'autre part, on a : $\overline{\Sigma}_i = \sum_{i \leqslant j \leqslant r} \Sigma_j^*$, $i = 1, \dots, r$. En effet, $\bigcup_{I \subset \{1,\dots r\},\ |I|=i} E_I = \coprod_{i \leqslant j \leqslant r} \bigcup_{I \subset \{1,\dots r\},\ |I|=j} E_I^*$ et, on trouve finalement que :

$$\Sigma_1 = \sum_{0 \leqslant i \leqslant r} i \Sigma_i^* = \sum_{1 \leqslant i \leqslant r} \sum_{i \leqslant j \leqslant r} \Sigma_j^* = \sum_{1 \leqslant i \leqslant r} \overline{\Sigma}_i.$$

De plus, par le lemme 3.1 (1), pour tout $\ell \gg 0$ et tout $I \subset \{1, \dots, r\}$ avec $|I| = r$, *ou* $r - 1$, on a $A_\eta[\ell]^{\langle \gamma_{i,\ell} | i \in I \rangle} = A_\eta[\ell]^{G_\ell} = 0$ par la structure du groupe fondamental.

3. Plus généralemant, on a $\Sigma_i = \sum_{i \leqslant j \leqslant r} C_j^i \Sigma_j^*$

Donc, en particulier, $E_I = \varnothing$. Il résulte que :

$$\begin{array}{l}\overline{\Sigma}_r = \Sigma_r = 0\,;\\ \overline{\Sigma}_{r-1} = \Sigma_{r-1} = 0\,;\\ \overline{\Sigma}_{r-2} = \Sigma^*_{r-2} = \Sigma_{r-2}\end{array}$$

et

$$\overline{\Sigma}_i \leqslant |G_\ell v|,\ i = 1, \ldots, r-3.$$

D'où :

$$\Sigma_1 \leqslant (r-3)|G_\ell v| + \Sigma_{r-2}.$$

6.4.3.2. Estimation de Σ_{r-2}. C'est ici que nous utilisons le théorème de réduction semistable [7, Exp. IX] énoncé plus haut. On a pour tout $1 \leqslant i \leqslant r$ avec $P_i \in SS$ et tout $\ell \gg 0$, l'élément $\gamma_{i,\ell}$ est unipotent d'échellon exactement 2, c'est-à-dire, $\gamma_{i,\ell} = Id + \nu_{i,\ell}$ avec $\nu^2_{i,\ell} = 0$ et $\nu_{i,\ell} \neq 0$. En particulier, $\gamma_{i,\ell}$ est d'ordre exactement ℓ.

(1) *Réduction semistable :*

Fixons un ensemble $I \subset \{1, \ldots, r\}$ tel que $|I| = r-2$. Considérons $\omega \neq \omega' \in E_I$. Alors, pour tout $j \in \{1, \ldots, r\} \setminus I$ on a $\langle \gamma_{j,\ell} \rangle \omega \cap \langle \gamma_{j,\ell} \rangle \omega' = \varnothing$. Sinon, en effet, il existerait un entier $1 \leqslant k \leqslant \ell - 1$ tel que $\gamma^k_{j,\ell}\omega = \omega'$. Donc, comme $\gamma^k_{j,\ell}\omega = \omega + k\nu_{j,\ell}(\omega)$, (binôme de Newton), i.e. : $0 \neq \omega' - \omega = k\nu_{j,\ell}(\omega) \in \ker(\nu_{j,\ell})$.
Mais, par hypothèse, $\omega, \omega' \in \ker(\nu_{i,\ell}),\ i \in I$. Donc :

$$0 \neq \omega' - \omega \in \bigcap_{i \in I \cup \{j\}} \ker(\nu_{i,\ell})$$

Ce qui contredit le lemme 6.2 (1) i.e :

$$A_\eta[\ell]^{\langle \gamma_{i,\ell} | i \in I \cup \{j\} \rangle} = A_\eta[\ell]^{G_\ell} = 0.$$

Et comme, pour tout $\omega \in E_I$ et tout $j \in \{1, \ldots, r\} \setminus I$ on a $|\langle \gamma_{j,\ell} \rangle \omega| = \ell$, on déduit de l'injection

$$\begin{array}{rcl} E_I & \hookrightarrow & < \gamma_{j,\ell} > \backslash (G_{\ell_v} \setminus E_{\{j\}}) \\ \omega & \mapsto & < \gamma_{i\ell} > .\omega \end{array}$$

que l'on a :

$$|E_I| \leqslant | < \gamma_{i\ell} > \backslash (G_\ell v \setminus E_{\{j\}})| = \frac{|G_\ell v \setminus E_{\{i\}}|}{\ell}$$

Ainsi,

$$\ell |E_I| \leqslant |G_\ell v| - |E_{\{j\}}|.$$

De même,

$$\ell |E_I| \leqslant |G_\ell v| - |E_{\{j'\}}|.$$

Avec $\{1, \ldots, r\} \setminus I = \{j, j'\}$, on a :

$$|E_I| \leqslant \frac{|G_\ell v|}{\ell} - \frac{|E_{\{j\}}| + |E_{\{j'\}}|}{2\ell}$$

et en sommant sur tous les $I \subset \{1, \ldots, r\}$ avec $|I| = r-2$, on obtient :

$$\begin{array}{rcl} \Sigma_{r-2} & \leqslant & \frac{C^{r-2}_r}{\ell}|G_\ell v| - \frac{1}{2} \times \frac{1}{2\ell} \sum_{j=1}^{r} \sum_{i \neq j} |(E_{\{i\}}| + |E_{\{j\}}|) \\ & \leqslant & \frac{C^{r-2}_r}{\ell}|G_\ell v| - \frac{r-1}{2\ell}\Sigma_1 \\ & \leqslant & \frac{r(r-1)}{2\ell}|G_\ell v|. \end{array}$$

(2) *Réduction semi-stable sauf pour un point :*

Supposons que $A \to X$ a réduction semi-stable en $P_1, \ldots, P_{r-1}$. Soit $I \subset \{1,\ldots,r\}$ tel que $|I| = r-2$.
Alors, si $r \in I$ on a, encore, avec $\{1,\ldots,r\} \smallsetminus I = \{j, j'\}$:

$$|E_I| \leqslant \frac{|G_\ell v|}{\ell} - \frac{|E_{\{j\}}| + |E_{\{j'\}}|}{2\ell} \leqslant \frac{|G_\ell v|}{\ell}.$$

Si $r \notin I$ alors, avec $\{1,\ldots,r\} \smallsetminus I = \{j, r\}$, on a seulement :

$$|E_I| \leqslant \frac{|G_\ell v|}{\ell} - \frac{|E_{\{j\}}|}{\ell} \leqslant \frac{|G_\ell v|}{\ell}.$$

Donc, en sommant les égalité ci dessus $I \subset \{1,\ldots,r\}$ avec $|I| = r-2$, on obtient, encore,

$$\Sigma_{r-2} \leqslant \frac{r(r-1)}{2\ell}|G_\ell v|.$$

6.4.3.3. Conclusion.

(1) *Réduction semi-stable :*
Dans un premier temps, observons que $G_\ell v$ peut s'écrire comme l'union disjointe $G_\ell v = \mathcal{O}_{i,1} \sqcup \mathcal{O}_{i,\ell}$ de $\mathcal{O}_{i,1}$ et de $G_\ell v \smallsetminus \mathcal{O}_{i,1} = \mathcal{O}_{i,\ell}$.
Ainsi, on obtient :

$$\begin{aligned} \varepsilon_{P_i}(v) &= \tfrac{|<\gamma_{i,\ell}>\backslash G_\ell v|}{|G_\ell v|} \\ &= \tfrac{|\mathcal{O}_{i,1}|}{|G_\ell v|} - \tfrac{|\mathcal{O}_{i,\ell}|}{\ell|G_\ell|} \\ &= \tfrac{|\mathcal{O}_{i,1}|}{|G_\ell v|} + \tfrac{1}{\ell}(1 - \tfrac{|\mathcal{O}_{i,1}|}{|G_\ell v|}). \end{aligned}$$

Donc, on a :

$$\lambda_v = r(1-\frac{1}{\ell}) - 2 - \frac{1}{|G_\ell v|}(1-\frac{1}{\ell})\Sigma_1.$$

Par conséquent, (*) est équivalent à :

$$(**) \quad \Sigma_1 < (r - (2+\varepsilon)\frac{\ell}{\ell-1})|G_\ell v| \text{ pour } v = v_\ell,\ \ell \gg 0.$$

Mais, par les calculs précédents, on a :

$$\begin{aligned} \Sigma_1 &\leqslant (r-3)|G_\ell v| + \Sigma_{r-2} \\ &\leqslant (r-3+\varepsilon(\ell))|G_\ell v| \end{aligned}$$

où

$$\varepsilon(\ell) = \frac{r(r-1)}{2\ell} = O(\frac{1}{\ell}).$$

Donc, il suffit de montrer que :

$$r - 3 + \varepsilon(\ell) < r - (2+\varepsilon)\frac{\ell}{\ell-1} \text{ pour } \ell \gg 0.$$

Mais ceci est toujours valable pour $0 < \varepsilon < 1$ puisque le terme de gauche tend vers $r-3$ tandis que le terme de droite $r-2-\varepsilon$.

(2) *Reduction semi-stable sauf en un point* :

Supposons encore que $A \to X$ a une réduction semistable en $P_1, \ldots, P_{r-1}$ et une réduction potentiellement semistable mais pas semistable en P_r.
On a :

$$G_\ell v = \bigsqcup_{n\geqslant 1} O_{i,n} = O_{i,1} \bigsqcup_{n\geqslant 2} O_{i,n}.$$

Le nombre d'orbites de longueur n est égal à $\frac{|O_{i,n}|}{n}$. En effet, $I_{P_i,\ell} =< \gamma_{i,\ell} >$ agit *via* :

$$\begin{array}{ccc} I_{P_i,\ell} \times O_{i,n} & \to & O_{i,n} \\ (\gamma, \omega) & \hookrightarrow & \gamma.\omega \end{array}$$

qui permet d'écrire :

$$O_{i,n} = \bigsqcup_{\omega \in I_{P_i,\ell}\backslash O_{i,n}} I_{P_i,\ell}.\omega \text{ où } |I_{P_i,\ell}.\omega| = n.$$

Ainsi

$$|O_{i,n}| = |I_{P_i,\ell}\backslash O_{i,n}|.n$$

Par suite :

$$\varepsilon_{P_r}(v) = \frac{1}{|G_\ell v|}(|O_{r,1}| + \sum_{n\geqslant 2} \frac{1}{n}|O_{r,n}|)$$

Donc, on a :

$$\begin{array}{rcl} \lambda_v & = & r(1-\frac{1}{\ell}) - 2 + \frac{1}{\ell} - \frac{1}{|G_\ell v|}(1-\frac{1}{\ell})\Sigma_1 \ldots \\ & & \cdots - \frac{1}{\ell}\frac{|O_{r,1}|}{|G_\ell v|} - \frac{1}{|G_\ell v|}\sum_{n\geqslant 2}\frac{1}{n}|O_{r,n}|. \end{array}$$

Ainsi, (*) est équivalent à :

$$(***) \quad \Sigma_1 + \frac{|O_{r,1}|}{\ell-1} + \frac{\ell}{\ell-1}\sum_{n\geqslant 2}\frac{1}{n}|O_{r,n}| < (r - \frac{\ell-1}{\ell}(2+\varepsilon-\frac{1}{\ell}))|G_\ell v|$$
$$\text{pour } v = v_\ell,\ \ell \gg 0.$$

Soit q le diviseur premier minimal N_{P_r}. On peut supposer que $q < \ell$ pour $\ell \gg 0$. Observons maintenant que :

$$\begin{array}{l} \Sigma_1 + \frac{|O_{r,1}|}{\ell-1} + \frac{\ell}{\ell-1}\sum_{n\geqslant 2}\frac{1}{n}|O_{r,n}| \\ \leqslant \Sigma_1 + \frac{|O_{r,1}|}{\ell-1} + \frac{\ell}{\ell-1}\frac{1}{q}\sum_{n\geqslant 2}|O_{r,n}| \\ \leqslant \Sigma_1 + \frac{|O_{r,1}|}{\ell-1} + \frac{\ell}{\ell-1}\frac{1}{q}(|G_\ell v| - |O_{r,1}|) \\ \leqslant \Sigma_1 + (\frac{1}{q} + \frac{1}{\ell-1})|G_\ell v|. \end{array}$$

Ainsi, il suffit de prouver que :

$$\Sigma_1 + (\frac{1}{q} + \frac{1}{\ell-1})|G_\ell v| \leqslant (r - \frac{\ell-1}{\ell}(2+\varepsilon-\frac{1}{\ell}))|G_\ell v|$$

Mais, par les calculs précédents on a toujours :

$$\Sigma_1 \leqslant (r-3)|G_\ell v| + \Sigma_{r-2} \leqslant (r-3+\varepsilon(\ell))|G_\ell v|,$$

où

$$\varepsilon(\ell) = \frac{r(r-1)}{2\ell} = O(\frac{1}{\ell}).$$

Donc, il suffit de montrer que :

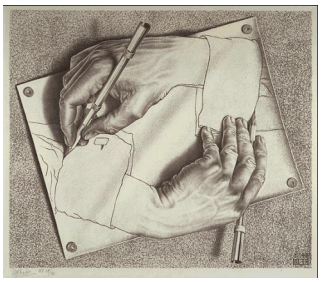
$$r - 3 + \varepsilon(\ell) + (\frac{1}{q} + \frac{1}{\ell - 1}) < r - \frac{\ell - 1}{\ell}(2 + \varepsilon - \frac{1}{\ell}) \text{ pour } \ell \gg 0.$$

Mais, ceci est toujours vrai $0 < \varepsilon < 1 - \frac{1}{q}$ puisque le terme de gauche tend vers $r - 3 + \frac{1}{q}$ tandis que le terme de droite tend vers $r - 2 - \varepsilon$.

7. Conclusion

Dans ce mémoire nous avons cherché à présenter la conjecture de torsion dans son contexte et à comprendre les étapes qui ont mené à l'énoncé de la conjecture 1.7 et à la preuve du théorème 5.1 et de la conjecture 1.5. Il ne s'agissait pas ici de tout comprendre en détail (au delàs du niveau d'un master) mais plutôt en admettant certains résultats profonds (théorème d'existence de Riemann, théorème de réduction semi-stable ...), de mettre en évidence les idées importantes et les techniques utilisées. Il semble clair que l'une des théories essentielles pour traiter ce problème est la théorie du groupe fondamental. Le dictionnaire donné par cette théorie nous a permis de construire les courbes modulaires abstraites qui ont permis à leur tour, de reformuler le problème et de ramener la preuve à une étude du genre. Le théorème fondamental ici est la formule théorème de Riemann Hurwitz qui relie le genre de deux courbes et l'indice de ramification (cf. annexe). Elle a permis de ramener le problème à un problème totalement combinatoire que l'on résout en combinant le théorème de Lang-Néron, la structure du groupe fondamental donné par le théorème d'existence de Riemann et le théorème de réduction semi-stable.

L'une des lacunes actuelles est que tous les résultats ont été démontrés en caractéristique 0. Dès lors, l'une des questions qui peut naturellement se poser est : **Que deviennent le corollaire 1.2 et le théorème 6.1 en caractéristique** p **?** Ce cas est à priori plus difficile. Par exemple, en observant la formule de Riemann Hurwitz en carctéristique p lorsque la ramification est sauvage, on observe qu'elle est plus complexe ce qui rend les choses plus difficiles. Ce sont ces motivations qui nous ont poussé à étudier ce cas en annexe. Cependant, dans le cas ℓ-primaire, le résultat est déjà démontré (cf. [1]). Enfin, supprimer l'hypothèse de semi-stabilité serait une nouvelle avancée vers la conjecture..



8. Annexes

8.1. Schéma abélien et variété abélienne (cf. [5, 20, 9, 16, 18]).

Soit S un schéma.

(1) **Foncteur représentable**

On rappelle aussi qu'un foncteur $F : C \to Sets$ est dit représentable si il existe un élément G de C tel qu'on a un isomorphisme de foncteur $F(-) \simeq Hom_C(G, -)$ i.e, pour tout $f : X \to Y$, on a le diagramme commutatif suivant : $\forall Y,\ Z \in C$

$$\begin{array}{ccc} F(Y) & \xrightarrow{\theta(Y)} & Hom_C(G,Y) \\ {\scriptstyle F(f)}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \circ f} \\ F(Z) & \xrightarrow[\theta(Z)]{} & Hom_C(G,Z) \end{array}$$

Il suit du lemme de Yoneda que l'isomorphisme $F(-) \simeq Hom_C(G, -)$ détermine X à isomorphisme prés.

(2) **Schéma en groupe**

Soit G un schéma sur S, on peut lui associer le foncteur de points

$$\begin{array}{rccl} F_G : & sch/S & \to & Ens \\ & X \to S & \to & Hom_{sch/S}(X, G) \end{array}$$

et on dit que G est un schéma en groupe si F_G est à valeur dans la catégories des groupes. Le lemme de Yoneda permet d'obtenir les diagrammes suivant qui donnent à G une structure de groupe.

(a) Il existe un $S-$morphisme $m : G \times_S G \to G$, m est appelé la multiplication en groupe. Le diagramme suivant commute :

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{Id \times m} & G \times_S G \\ {\scriptstyle m \times Id}\downarrow & \circlearrowleft & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow[m]{} & G \end{array}$$

Ce diagramme traduit l'associativité de la loi pour m.

(b) Il une section $\varepsilon : S \to G$ pour le morphisme structurel $\pi : G \to S$ tel que les diagrammes suivants sont commutatifs :

$$(E) \qquad \begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle (Id,\ \varepsilon)}\uparrow & \nearrow_{1} & \\ G \times_S S & & \end{array} \qquad \text{et} \qquad \begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle (\varepsilon,\ Id)}\uparrow & \nearrow_{1} & \\ G \times_S S & & \end{array}$$

Ceci signifie que ε joue le rôle de l'identité.

(c) Il existe un $S-$morphisme $inv : G \to G$ tel que les diagrammes suivant commutent :

$$\begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times_S G & \xrightarrow{1 \times inv} & G \times_S G \\ {\scriptstyle \pi}\downarrow & & & & \downarrow{\scriptstyle m} \\ G & & \xrightarrow[\varepsilon]{} & & G \end{array}$$

et

$$\begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times_S G & \xrightarrow{inv\times 1} & G \times_S G \\ {\scriptstyle\pi}\downarrow & & & & \downarrow{\scriptstyle m} \\ G & & \xrightarrow[\varepsilon]{} & & G \end{array}$$

où $\Delta : G \to G \times_S G$ est la diagonale.

La commutativité de ces diagrammes traduisent le fait que *inv* est l'application inverse.

Les notions d'homomorphismes de schéma en groupe ou de sous schéma en groupe sont définies naturellement. Nous pouvons supposer que tous les schémas sont séparés. Ainsi Δ est une immersion fermée et (E) montre que ε est une immersion fermée et un homomorphisme. S est le shéma en groupe sur S trivial. Notons aussi que un changement de base de schéma en groupe G sur S vers une nouvelle base T, nous donne un nouveau schéma en groupe $G_T = G \times_S T$ sur T. La manière correcte de penser à un schéma en groupe sur S est de le penser en tant que famille de schéma en groupe, $\{G_s,\ s \in S\}$ où $G_s = G \times_S spec(k(s))$ avec $k(s)$ corps résiduel en s. On parle aussi de schéma en groupe sur A lorsque il s'agit d'un schéma en groupe sur $S\,pec(A)$ où A est un anneau commutatif. Nous voyons que chaque G_s est un schéma de groupe sur un corps (le corps $k(s)$).

(3) **Variété abélienne**

Une variété abélienne sur un corps k est un groupe algébrique A sur k, dont le schéma sous-jacent est projectif, connexe et géométriquement réduit. La loi de groupe d'une variété A est commutative (rigidité). Si k est de caractéristique nulle, la condition "géométriquement réduit" est automatiquement satisfaite pour tout groupe algébrique sur k (Théorème de Cartier).

(4) **Schéma abélien**

Si le schéma de base S n'est pas un corps, on peut définir la notion de schéma abélien sur S. Un schéma $\mathcal{A}$ sur S est un schéma abélien sur S si et seulement si :

(a) $\mathcal{A}$ est un schéma en groupe

(b) $\mathcal{A}$ est propre sur S

(c) $\mathcal{A}$ est lisse sur S

(d) tous les $\mathcal{A}_s$ sont des variétés abéliennes sur les corps résiduels respectifs $k(s)$.

C'est la bonne notion de familles de variétés abéliennes paramétrisées par S.

8.2. **Exemples classiques de schéma en groupe (cf [15]) :**

– **Le groupe additif :**

Soit $\mathbb{G}_a$ le foncteur envoyant une k-algèbre R sur R considérée comme groupe additif, i.e. $\mathbb{G}_a(R) = (R, +)$. Alors

$$\mathbb{G}_a(R) \simeq Hom_{k-alg}(k[X], R),$$

et donc $\mathbb{G}_a$ est un schéma en groupe, appelé le **groupe additif**.

– **Le groupe multiplicatif :**

Soit $\mathbb{G}_m(R) = (R^\times, \times)$. Soit $k(X)$ le corps des fractions de $k[X]$, et soit $k[X, X^{-1}]$ le sous anneau de $k(X)$ des polynômes en X et X^{-1}. Alors

$$\mathbb{G}_m(R) \simeq Hom_{k-alg}(k[X, X^{-1}], R),$$

et donc $\mathbb{G}_m$ est un schéma en groupe appelé le **groupe multiplicatif**.

– **Le groupe μ_n :**

Soit μ_n le foncteur $\mu_n(R) = \{r \in R | r^n = 1\}$. Alors

$$\mu_n(R) \simeq Hom_{k-alg}\left(\frac{k[X]}{(X^n-1)}, R\right),$$

et donc μ_n est un schéma en groupe tel que $k[\mu_n] = \frac{k[X]}{(X^n-1)}$.

– **Les tores :**

Un **tore** $\mathbb{T}$ sur K est un schéma en groupe, isomorphe à un produit de G_m sur la clôture algébrique de K. On dit que $\mathbb{T}$ est **déployé** si l'isomorphisme est défini sur K.

8.3. Les réductions d'une variété abélienne :

8.3.1. *Le théorème de Chevalley (cf. [20]) :* On connait la structure des groupes algébriques. C'est le théorème de Chevalley.

Théorème 8.1. *Soit k un corps de caractéristique 0 et G un groupe algébrique lisse, connexe sur k. Alors*

(1) ***Théorème de Chevalley***
Il existe un plus petit sous-groupe algébrique H affine connexe, normal (automatiquement lisse) de G tel que G/H soit une variété algébrique sur k.

(2) Si, de plus H est commutatif alors H contient un unique sous-groupe unipotent, normal, connexe maximal et G/H est un tore.
Donc tout groupe algébrique g lisse connexe commutatif sur k s'écrit comme une extension

$$0 \to \mathbb{T} \times U \to G \to B \to 0$$

où B est une variété abélienne, U est un groupe algébrique unipotent commutatif et $\mathbb{T}$ est un tore.

8.3.2. *Le modèle de Néron (cf. [9, 20]).* Soit S un schéma de Dédekind (i.e. schéma noethérien régulier de dimension 1) et K son corps de fonction. Considérons un K-schéma X_K de type fini, on cherche à construire un S-modèle X de X_K qui est lisse, séparé et de type fini sur S. De plus, on veut que ce soit un modèle minimal parmi tous les modèles de ce type, i.e. un S-modèle X tel que pour tout autre S-modèle Y de ce type, il existe un unique morphisme $Y \to X$ dont la restriction à la fibre générique soit l'identité. Ceci introduit la notion de modèle de Néron.

Définition 8.2. *Soit X_K un K-schéma de type fini lisse et séparé. Un* ***modèle de Néron*** *de X_K est un S-modèle X qui est lisse, séparé et de type fini, et qui satisfait la propriété universelle suivante :*
Pour chaque S-schéma Y et chaque K-morphisme $u_K : Y_K \to X_K$, il existe un unique S-morphisme $u : Y \to X$ prolongeant u_K.

On va lister quelques propriétés élémentaires du modèle de Néron qui découle directement de la définition.

Proposition 8.3. *Soit X un S-schéma lisse et séparé qui est le modèle de Néron de sa fibre générique X_K.*

(1) X est déterminé de manière unique par X_K, à isomorphisme près.

(2) La formation de modèles de Néron commutent avec les changements de base étale ; i.e. si $S' \to S$ est un morphisme étale et si K' est le corps des fonctions de S', alors $X_{S'} = X \times_S S'$ est un modèle de Néron sur S' du K-schéma $X_{K'} = X_K \times_K K'$.

Remarque 8.4. *(2) est faux si le changement de base n'est pas étale.*

Un théorème difficile montre l'existence d'un modèle de Néron pour les variétés abéliennes :

Théorème 8.5. *Soit S un schéma de Dédekind connexe, K son corps de fonction et soit A_K une variété abélienne sur K. Alors A_K admet un modèle de Néron A sur S.*

8.3.3. *Types de réduction.* Soit X un schéma de Dédekind, K son corps de fonction, A une variété abélienne sur K et $\mathcal{A}$ son modèle de Néron sur X. Pour tout $P \in X$, on note $\mathcal{A}_P$ la fibre de $\mathcal{A}$ en P. D'aprés le théorème de Chevalley $\mathcal{A}_P$ s'écrit :

$$0 \to \mathbb{T} \times U \to \mathcal{A}_P \to B \to 0$$

On dit que :

(1) A a une **bonne réduction** si $\mathcal{A}_P$ est une variété abélienne.

(2) A a une **réduction semi-stable** en P si on a la suite exacte $0 \to \mathbb{T} \to \mathcal{A}_P \to B \to 0$ où $\mathbb{T}$ est un tore et B une variété abélienne.

(3) une **réduction potentiellement bonne** (resp. **potentiellement réduction semi-stable**) en P s'il existe un revêtement fini étale $Y \to X$ et un point $Q \in \tilde{Y}$ au dessus de P tel que $A \times_X Y$ a une bonne réduction (resp. a une réduction **semi-stable**) en $Q \in \tilde{Y}/Y$.

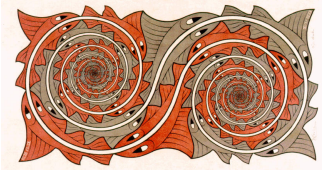
Le théorème de réduction semi-stable dit que se sont les seules possibilités (i.e. la partie unipotente est toujours tuée par un changement de base fini).

Théorème 8.6 (Théorème de réduction semi-stable). *$\mathbb{T}$ est un schéma abélien sur X à réduction semi-stable*

De plus, on peut lire le type de réduction sur la représentation $\rho_{A,\ell} : \pi_1(X) \to GL(A_\eta[\ell])$.

Théorème 8.7. *(cf. [7, exp IX]) Avec les notations ci-dessus.*

- *si $P \in$ **PB** alors il existe un entier $N_P \geqslant 2$ tel que $I_{P,\ell}^{N_P} = 1$ pour tout ℓ et que $I_{P,\ell}^{N} \neq 1$ pour $N < N_P$ et $\ell \gg 0$.*
- *Si $P \in$ **SS** alors $I_{P,\ell}$ est unipotent[4] d'échelon 2 .*
- *Si $P \in$ **PSS** alors il existe un entier $N_P \geqslant 2$ tel que $I_{P,\ell}^{N_P}$ est unipotent d'échelon 2 pour tout ℓ et que $I_{P,\ell}^{N}$ n'est pas unipotent pour $N < N_P$ et $\ell \gg 0$.*



4. On rappelle qu'un groupe G unipotent d'échelon 2 est un groupe dont tous les élément sont unipotents d'échelon 2 (i.e. $\forall \gamma \in G \setminus \{1\}$, $(\gamma - 1)^2 = 0$).

8.4. **Théorème de Riemann-Hurwitz.** Soit k un corps algébriquement clos. On considère un morphisme fini de courbe $f : X \to Y$ et on étudie la relation entre les diviseurs canoniques. La formule résultante de cette étude liant le genre de X, le genre de Y et le nombre de points ramifiés est appelée théorème d'Hurwitz. On appelle le degré d'un morphisme fini $f : X \to Y$ de courbes, le degré $[K(X) : K(Y)]$ de l'extension du corps de fonction.

8.4.1. *Diviseurs sur les courbes - Rappels.* Comme les courbes sont des schémas noethériens, intègres, séparés et localement factoriels, les trois notions classiques de diviseurs sont équivalentes. Soit X une courbe et $Pic(X)$ le groupe des faisceaux inversibles à isomorphisme prés. On rappelle rapidement la définition d'un diviseur de Weil et celle de diviseur de Cartier.

8.4.1.1. Diviseur de Weil : On note $Div(X)$ le groupe abélien libre engendré par les points fermés X^f de X. Donc un élément de $Div(X)$ est une application $\rho : X^f \to \mathbb{Z}$ telle que $\rho(P) = 0$, pour tout P sauf un nombre fini. On note ρ par $\sum_P \rho(P)P$. On dit que la somme formelle $R = \sum_{i=1}^{n} \rho(P_i)P_i$ est un **diviseur de Weil** de X. Le **degré du diviseur** est $\sum ni$ où on a noté $n_i = \rho(P_i)$. Si $n_i \geqslant 0$, on dit que le **diviseur est effectif**. On donne à un diviseur effectif R une structure de schéma fermé, en définissant son faisceau d'idéaux $\mathcal{J} \subset \mathcal{O}_R$ de la façon suivante. Pour tout $P \notin \{P_i\} \forall i \in \{1, \ldots, n\}$, $\mathcal{J}_P = \mathcal{O}_{X,\,P}$. Pour tout P_i, pour tout $i \in \{1, \ldots, n\}$, $\mathcal{J}_{P_i} = \frac{\mathcal{O}_{X,P_i}}{\mathfrak{M}_{P,P_i}^{n_i}}$.

Deux diviseurs sont **linéairement équivalents** si leur différence est un **diviseur principal** i.e le diviseur d'une fonction rationnelle. On note $\mathbf{Cl}(\mathbf{X})$ le groupe des diviseurs de Weil modulo la relation d'équivalence. Le degré d'un diviseur ne dépend que de la classe d'équivalence linéaire.

8.4.1.2. Diviseur de Cartier : Soit U un ouvert affine $U = spec(A)$. On note $\mathcal{K}$ le corps de fonctions de X i.e. $\mathcal{K} = \mathcal{O}_{U,\eta} = Frac(A)$. On note aussi $\mathcal{K}^*$ le faisceau (de groupe multiplicatifs) des éléments inversibles du faisceau d'anneau $\mathcal{K}$. De même, on note $\mathcal{O}^*$ le faisceau des inversibles de $\mathcal{O}_X$ (c'est un faisceau constant sous nos hypothèses). Un **diviseur de Cartier** est une section globale du faisceau $\frac{\mathcal{K}^*}{\mathcal{O}^*}$, en d'autres termes, un diviseur de Cartier est la donnée des couples $\{(U_i, f_i)\}_{i\in\{1,\ldots,n\}}$ où $\{U_i\}_{i\in\{1,\ldots,n\}}$ est un recouvrement de X par des ouverts et $f_i \in \mathcal{K}^*(U_i)$ tel que $\forall i, j$, $\frac{f_i}{f_j} \in \mathcal{O}^*(U_i \cap U_j)$. Un **diviseur de cartier est principal** s'il est dans l'image de l'application naturelle $\mathcal{K}^*(X) \to \frac{\mathcal{K}^*}{\mathcal{O}^*}(X)$. Deux **diviseurs de Cartier sont équivalents** si leur différence est principale.
A partir d'un diviseur de Cartier, on définit $\mathcal{L}(D)$ comme la classe d'isomorphismes du sous-faisceau inversible de $\mathcal{K}$ défini par $\mathcal{L}(D)|_{U_i} = f_i^{-1}\mathcal{O}_{U_i}$, $i \in I$ et $\mathcal{W}(D)$ est la classe d'équivalence du diviseur de Weil :

$$\sum_{x\in X} v_x(f_{i_x})x,$$

où $i_x \in I$ est n'importe quel indice vérifiant $x \in U_{i_x}$. Notons $CaCl(X)$ le groupe des diviseurs de Cartier.

Lemme 8.8. *La correspondance $D \to \mathcal{L}(D)$ induit une application $CaCl(X) \to Pic(X)$ qui est un morphisme de groupe.*

On a de plus les isomorphismes :

Théorème 8.9. *Soit X une courbe. Alors les morphismes de groupes canoniques :*

$$\begin{array}{rccc} \mathcal{L} : & CaCl(X) & \xrightarrow{\sim} & Pic(X) \\ & D & \mapsto & \mathcal{L}(D) \end{array} \quad et \quad \begin{array}{rccc} \mathcal{W} : & CaCl(X) & \xrightarrow{\sim} & Cl(X) \\ & D & \mapsto & \mathcal{W}(D) \end{array}$$

sont des isomorphismes.

Sous les hypothèses du théorème 8.9, tout faisceau inversible est un sous-$\mathcal{O}_X$-module du faisceau contenant $\mathcal{K}_X = k(\eta_X)$ (cf. [8]). Ce théorème permet de définir concrètement un isomorphisme de $Pic(X)$ sur $Cl(x)$. En effet, comme $\mathcal{O}_{X,x}$ est un anneau de valuation discrète, on peut fixer une uniformisante u_x de $\mathcal{O}_{X,x}$ et on a, pour $\mathscr{L}$ faisceau inversible de X que $\mathscr{L}_x = \mathcal{O}_{X,x} u_x^{v_x(\mathscr{L})}$. L'image de $\mathscr{L}$ par $\mathcal{W} \circ \mathcal{L}^{-1}$ est la classe d'équivalence linéaire du diviseur de Weil :

$$\sum_{x \in X} v_x(\mathscr{L}) x$$

Si $v_x(\mathscr{L}) \geqslant 0$ alors on a aussi $v_x(\mathscr{L}) = long(\frac{\mathcal{O}_{X,x}}{\mathscr{L}_x})$.
Si D est un diviseur effectif, le sous-schéma fermé associé à D est le sous-schéma fermé - encore noté D - défini par le sous-faisceau d'idéaux $\mathcal{L}(-D) \subset \mathcal{O}_X$. Autrement dit, on a une suite exacte courte de $\mathcal{O}_X$-modules :

$$0 \to \mathcal{L}(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$$

8.4.1.3. Diviseurs canoniques : On note $\Omega_{X|k}$ ou simplement Ω_X le faisceau des différentielles relatives de X sur k. Comme X est de dimension 1, Ω_X est un faisceau inversible sur X et donc est égal à son faisceau canonique ω_X de X. On appelle tout diviseur dans la classe d'équivalence linéaire correspondante un diviseur canonique et on le note $\mathcal{K}_X$.

8.4.2. *L'indice de ramification, rappels.* Pour un point $P \in X$ nous définissons l'indice de ramification e_p comme suit. Soit $Q = f(P)$, $t \in \mathcal{O}_{X,Q}$ un paramètre local de Q i.e. un générateur de l'idéal maximal. On considère t comme un élément de $\mathcal{O}_{X,P}$ via l'application naturelle $f^\sharp : \mathcal{O}_{X,Q} \to \mathcal{O}_{X,P}$ et on définit $e_P = v_P(t)$ où v_P est la valuation associée à l'anneau de valuation $\mathcal{O}_{X,P}$.

. Si $e_P > 1$ on dit que f ramifié de P et que Q est un point de branchement de f.

. Si $e_P = 1$ on dit que f est non ramifié.

Si $car(k) = 0$ ou si $car(k) = p > 0$, si $p \nmid e_P$ on dit que la ramification est modérée. Si $car(k) = p > 0$ et $p | e_P$, on dit que la ramification est sauvage.
On définit l'homophisme $f^* : Div\ Y \to Div\ X$ en posant pour tout $Q \in Y$:

$$f^*(Q) = \sum_{P \to Q} e_P P,$$

où la somme est sur les P tels que $f(P) = Q$ et en étendant cette définition par linéarité. (Comme f est un morphisme fini, on a ici une somme finie donc on est en présence d'un diviseur sur X).

Lemme 8.10. *On vérifie que f^* préserve l'équivalence linéaire donc induit un morphisme de groupe $f^* : Cl(Y) \to Cl(X)$. Si D est un diviseur sur Y alors $f^*(\mathcal{L}(D)) \cong \mathcal{L}(f^*(D))$ donc l'application f^* induit un homomorphisme $f^* : Pic(Y) \to Pic(X)$.*

On dit qu'un morphisme $f : X \to Y$ est **séparable** si $K(X)$ est une extension séparable du corps $K(Y)$.

8.4.3. *L'énoncé.* On note $\sim$ l'équivalence linéaire sur les diviseurs. La formule de Riemann-Hurwitz est un corollaire du théorème de Riemann-Roch et de la proposition suivante.

Proposition 8.11. *Soit $f : X \to Y$ un morphisme fini et séparable de courbes. On note $\mathcal{K}_X$ et $\mathcal{K}_Y$ les diviseurs canoniques de X et Y respectivement et :*

$$R_f := \sum_{x \in X} long(\Omega_{X|Y,x}) x$$

le diviseur de ramification de $f : X \to Y$. Alors :

$$\mathcal{K}_X \sim f^* \mathcal{K}_Y + R_f$$

Si on note $g_X := dim(H^0(X,\Omega_X)) = dim(H^1(H,\mathcal{O}_X)_1)$ le genre géométrique de X, il en résulte du théorème de Riemann-Roch :

Corollaire 8.12.

$$deg(K_X) = 2g_X - 2$$

Donc, en prenant les degrés, on déduit de la proposition 8.11 et du fait que $deg(f^*(-)) = deg(f)deg(-)$ que :

Corollaire 8.13 (Formule de Riemann-Hurwitz)**.** *Soit $f : X \to Y$ un morphisme fini et séparable de courbes. On a :*

$$2(g_X - 1) = 2deg(f)(g_Y - 1) + deg(R_f)$$

De plus, si f est modérément ramifiée, alors

$$deg\ R_f = \sum_{x\in X}(e_x - 1)$$

8.5. **Preuve de la proposition 8.11.**

Démonstration. D'après le théorème 8.9, $\mathcal{K}_X \sim f^*\mathcal{K}_Y + R_f$ équivaut à $\Omega_X = f^*\Omega_Y \otimes_{\mathcal{O}_Y} \mathcal{L}(-R_f)$ ou encore à $\Omega_X \otimes_{\mathcal{O}_X} (f^*\Omega_Y)^{-1} = \mathcal{L}(-R_f)$. Notons η_X, η_Y les points génériques de X et Y respectivement.

(1) **Fait 1 :** $(\Omega_{X|Y})_{\eta_X} = 0$.
En effet, $(\Omega_{X|Y})_{\eta_X} = \Omega_{\mathcal{O}_{X,\eta_X}|\mathcal{O}_{Y,\eta_Y}} = \Omega_{k(\eta_X)|k(\eta_Y)} = 0$, la dernière égalité résultant du fait que $f : X \to Y$ est séparable.

(2) **Fait 2 :** On a une suite exacte courte $0 \to f^*\Omega_Y \to \Omega_X \to \Omega_{X|Y} \to 0$.
On a toujours la suite exacte courte $f^*\Omega_Y \xrightarrow{\alpha} \Omega_X \to \Omega_{X|Y} \to 0$ donc le seul point à vérifier est l'exactitude à gauche. D'après le fait 1, en localisant en η_X, on obtient : $\alpha_{\eta_X} : (f^*\Omega_Y)_{\eta_X} \tilde{\to} \Omega_{X,\eta_X}$. Notons $\mathcal{N}$ le noyau de α. Pour tout $x \in X$, $\mathcal{N}_x$ est un sous-$\mathcal{O}_{X,x}$-module de $(f^*\Omega_Y)_x$, qui est libre de rang 1. Comme $\mathcal{O}_{X,x}$ est principal, $\mathcal{N}_x$ est soit 0 soit $\mathcal{O}_{X,x}$-module de rang 1 i.e on a un isomorphisme de $\mathcal{O}_{X,x}$-modules $\mathcal{O}_{X,x} \tilde{\to} \mathcal{N}_x$. En localisant en $\mathcal{O}_{X,x}\backslash\{0\}$, on obtient : $k(\eta_X) \tilde{\to} \mathcal{N}_{\eta_X}$, ce qui contredit $\mathcal{N}_{\eta_X} = 0$. Donc $\mathcal{N}_x = 0$ et ceci pour tout $x \in X$. Comme $\mathcal{N}$ est quasi-cohérent, on en déduit $\mathcal{N} = 0$.

(3) Comme $(\Omega_X)^{-1}$ est un faisceau inversible, le foncteur $- \otimes_{\mathcal{O}_X} (\Omega_X)^{-1}$ est exact. Par ailleurs, d'après le fait 1, $\Omega_{X|Y} \otimes_{\mathcal{O}_X} (\Omega_X)^{-1} \simeq \Omega_{X|Y}$ donc, en tensorisant $0 \to f^*\Omega_Y \to \Omega_X \to \Omega_{X|Y} \to 0$ par $- \otimes_{\mathcal{O}_X} (\Omega_X)^{-1}$, on obtient :

$$0 \to f^*\Omega_Y \otimes_{\mathcal{O}_X} (\Omega_X)^{-1} \to \mathcal{O}_X \to \Omega_{X|Y} \to 0$$

Pour tout $x \in X$, l'anneau $\mathcal{O}_{X,x}$ est un anneau de valuation discrète. En particulier, le morphisme de k-modules canonique $\frac{\mathfrak{M}_{X,x}}{\mathfrak{M}_{X,x}^2} \tilde{\to} \Omega_{X,x}$ est un isomorphisme. Donc si $u_x \in \mathfrak{M}_{X,x}$ est une uniformisant de $\mathcal{O}_{X,x}$, $\Omega_{X,x} = \mathcal{O}_{X,x}d_x(u_x)$. De même, si $u_{f(x)} \in \mathfrak{M}_{Y,f(x)}$ est une uniformisant de $\mathcal{O}_{Y,f(x)}$, $\Omega_{Y,f(x)} = \mathcal{O}_{Y,f(x)}d_{f(x)}(u_{f(x)})$. En écrivant $f_x^\sharp(u_{f(x)}) = au_x^{e_x}$ avec $a \in \mathcal{O}_{X,x}^*$, le morphisme $\phi_x : \Omega_{Y,f(x)} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{O}_{X,x} \to \Omega_{X,x}$ est entièrement déterminé par :

$$\phi_x(d_{f(x)}(u_{f(x)})) = d_x f_x^\sharp(u_{f(x)}) = d_x(au_x^{e_x}) = e_x a u_x^{e_x-1} d_x(u_x) + u_x^{e_x} d_x(a) =: \frac{d_x(f_x^\sharp(u_{f(x)})}{d_x(u_x)}.$$

La suite exacte courte $0 \to f^*\Omega_Y \otimes_{\mathcal{O}_X} (\Omega_X)^{-1} \to \mathcal{O}_X \to \Omega_{X|Y} \to 0$ localisée en $x \in X$ devient donc

$$0 \to \frac{d_x(f_x^\sharp(u_{f(x)}))}{d_x(u_x)}\mathcal{O}_{X,x} \to \mathcal{O}_{X,x} \to \Omega_{X|Y,x} \to 0.$$

On en déduit, d'une part que le diviseur de Weil associé à $f^*\Omega_Y \otimes_{O_X} (\Omega_X)^{-1}$ est :

$$\begin{aligned}\sum_{x\in X} v_x\Big(\tfrac{d_x(f_x^\sharp(u_{f(x)}))}{d_x(u_x)}\Big)x &= \sum_{x\in X} long\left(\frac{O_{X,x}}{\Big(\tfrac{d_x(f_x^\sharp(u_{f(x)}))}{d_x(u_x)}\Big)}\right)x \\ &= \sum_{x\in X} long(\Omega_{X|Y,x})x \\ &= R_f\end{aligned}$$

D'autre part, que $\Omega_{X|Y}$ est de longueur $v_x\Big(\tfrac{d_x(f_x^\sharp(u))}{d_x(u_x)}\Big) = e_x - 1$, si la ramification est modérée et $v_x\Big(\tfrac{d_x(f_x^\sharp(u))}{d_x(u_x)}\Big) \geqslant e_x - 1$, sinon.

□

8.6. **Cas où la ramification est sauvage (cf. [21, p 124] [19, chap. IV]).** Si la ramification est sauvage, l'étude est beaucoup plus complexe. Mais, dans le cas où le revêtement est Galoisien de groupe $G := Gal(K(X)/K(Y))$, on obtient la formule de Riemann-Hurwitz qui s'exprime à l'aide des groupes de ramification que nous allons définir. Donnons nous un $P \in X$, posons $Q := f(P) \in Y$. Etant donné que nous sommes en présence d'un revêtement galoisien, il existe un élément $x \in O_{X,P}$, qui engendre $O_{X,P}$ considéré comme $O_{X,Q}$-algèbre. Sous ces conditions, le lemme suivant est vérifié :

Lemme 8.14. *Soit $s \in G$, et soit i un entier $\geqslant -1$. Les trois conditions suivantes sont équivalentes :*
- *s opère trivialement sur l'anneau quotient $\frac{O_{X,P}}{\mathcal{M}_{X,P}^{i+1}}$*
- *$v_P(s(a) - a) \geqslant i + 1$ pour tout $a \in O_{X,P}$.*
- *$v_P(s(x) - x) \geqslant i + 1$.*

Pour tout entier $i \geqslant -1$, soit $G_x(i)$ l'ensemble des $s \in G$ qui vérifient les conditions (a), (b), (c) du lemme. Les $G_x(i)$ forment une suite décroissante de sous-groupes distingués de G. On a $G_x(1) = \{Id\}$ pour i assez grand, $G_x(0)$ est le sous groupe d'inertie de G et $G_x(-1) = G$. Le groupe $G_x(i)$ s'appelle le $i^{\text{ème}}$ groupe de ramification de G (ou de L/K).

Théorème 8.15 (Formule de Riemann-Hurwitz-Cas général (admis)). *Soit $f : X \to Y$ un revêtement galoisien de groupe G, séparable de degré n de courbes.*

$$2(g(X) - 1) = 2|G|(g(Y) - 1) + \sum_{x\in X}\sum_{i\in N}(|G_x(i)| - 1)deg(x)$$

où x parcourt les points fermés de X, $deg(x) = [k(x) : k(f(x))]$, $G_x(i)$ désigne le $i^{ième}$ groupe de ramification en x dans l'extension $K(X)/K(Y)$.
Lorsque k est de caractéristique 0, $deg(x) = 1$.

On remarque que avec cette formule est plus complexe ce qui rend difficile l'obtention d'un analogue de la preuve du théorème 6.1 en caractéristique p.

Références

[1] Cadoret and A. Tamagawa. *Torsion of abelian schemes and rational points on moduli spaces*. 2009.

[2] Cadoret and A. Tamagawa. *Uniform boundedness of p-primary torsion on abelian schemes*. Preprint 2008.

[3] Anna Cadoret. *Galois Categories*. The G.A.M.S.C summer school, June 9th-June 20th 2008.

[4] Anna Cadoret and Akio Tamagawa. *On a weak variant of the geometry torsion conjecture*. 2010.

[5] Gary Cornell and Joseph H. Silverman. *Arithmetic geometry*. Springer-Verlag, New York Berlin Heidelberg London Paris Tokyo, 1998.

[6] Grothendieck. *Revêtements étales et groupe fondamental (SGA1)*. Lecture Notes in Mathematics **224**, Springer-Verlag, 1971.

[7] Grothendieck. *Groupe de Monodromie en Géométrie Algébrique, I (SGA7I)*. Lecture Notes in Mathematics **288**, Springer-Verlag, 1972.

[8] Robin Hartshorne. *Algebraic Geometry*, volume 52. Springer-Verlag, New York-Heidelberg, 1977.

[9] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry : An Introduction*. Springer, 2000.

[10] Lang-Néron. *Abelian varieties*. Interscience réédité par Springer-Verlag, 198, New York 1959.

[11] Quing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics, 2009.

[12] I. Manin. *The $p-$torsion of elliptic curves uniformly bounded(Russian)*. Akad. Nauk SSSR. Ser. Mat. **3**, 1969.

[13] B. Mazur. *Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S.*, volume 47. 1977.

[14] L. Merel. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. nvent. Math. **124**.

[15] Milne. *Algebraic Groups and Arithmetic Groups*. 2006.

[16] David Mumford. *Abelian Varieties*. Oxford University Press, 1970.

[17] Amer. J.(avec A. Néron). *Rational points of abelian varieties over function fields*. Math. 81, 1959.

[18] Pierre Schapira. *Categoties and homological algebra*, 2009.

[19] Jean Pierre Serre. *Corps Locaux*. Hermann, 1968.

[20] Michel Raynaud Siegfried Bosch, Werner Lütkebohmert. *Néron models A Series of Modern Surveys in Mathematics Series*. Éditeur Springer, 1990.

[21] Henning Stichtenoth. *Algebraic function fields and codes*. Éditeur Springer, 2000.

[22] Tamás Szamuely. *Galois groups and fundamental groups*. Cambridge University Press, 2009.

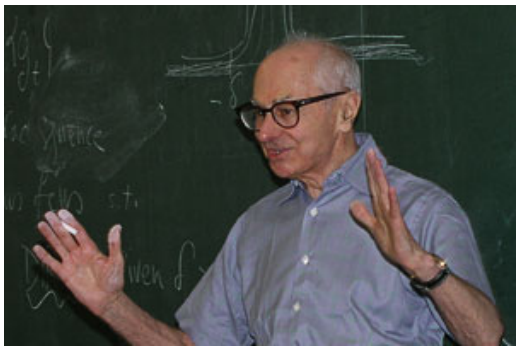
Évariste Galois (Bourg-la-Reine, 25 octobre 1811 - Paris, 31 mai 1832) est un mathématicien français. Il a entre autres laissé son nom à la théorie de Galois, qui étudie la résolubilité des équations algébriques à partir des groupes de permutations de leurs racines et qui est considérée comme un ingrédient important dans le point de vue structural des mathématiques modernes. Il a aussi contribué à l'élaboration des corps de Galois, autre nom des corps finis, qui jouent par exemple un rôle essentiel en cryptographie. Les démêlés de Galois avec les autorités, tant scientifiques que politiques, les zones d'ombre entourant sa mort prématurée, contrastant avec l'importance reconnue maintenant à ses travaux, ont contribué à en faire l'incarnation même du génie malheureux.

Adolf Hurwitz (26 mars 1859- 18 novembre 1919) était un mathématicien allemand, l'une des figures importantes des mathématiques de la seconde moitié du XIXe siècle. Il est né à Hildesheim et mort à Zurich en Suisse. Il fut un des premiers à maîtriser la théorie des surfaces de Riemann. Il s'en servit pour montrer des résultats fondamentaux sur les courbes algébriques, dont le théorème des automorphismes de Hurwitz. Ce travail anticipe des théories postérieures, dont la théorie des correspondances algébriques, les opérateurs de Hecke et le théorème des points fixes de Lefschetz. Il s'intéressait aussi à la théorie des nombres. Il a étudié les ordres maximaux dans les quaternions, introduisant ce qui s'appelle aujourd'hui les quaternions d'Hurwitz.

Alexandre Grothendieck est un mathématicien apatride, ayant passé la majorité de sa vie en France, né le 28 mars 1928 à Berlin (Allemagne). Lauréat de la médaille Fields en 1966, refondateur de la géométrie algébrique, il est considéré comme l'un des plus grands mathématiciens du XXe siècle.

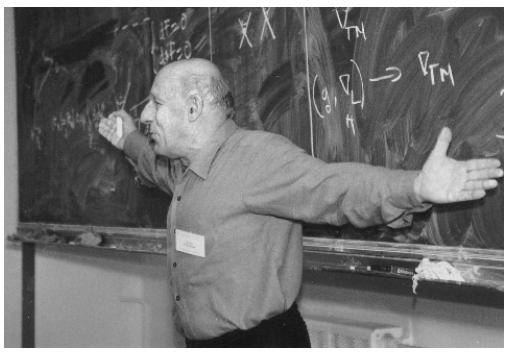
David Bryant Mumford (né le 11 juin 1937) est un mathématicien américain connu pour son travail en géométrie algébrique puis pour sa recherche en théorie de la vision. Il est actuellement professeur dans la division de mathématiques appliquées de l'Université Brown, après une longue carrière académique à Harvard.

Jean-Pierre Serre est un mathématicien français né le 15 septembre 1926 à Bages (Pyrénées-Orientales). Il est considéré comme l'un des plus grands mathématiciens du XXe siècle. Il a reçu de nombreuses récompenses pour ses recherches dont la médaille Fields en 1954, faisant de lui le plus jeune récompensé. Il est aussi le premier lauréat du Prix Abel, créé en 2003.

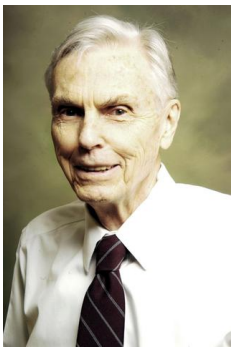


Serge Lang (19 mai 1927 - 12 septembre 2005) est un mathématicien américain né en France. Il est connu pour ses travaux en théorie des nombres et pour ses manuels scolaires, dont l'influent Algebra. Il fut membre de la National Academy of Sciences et du groupe Bourbaki.

Georg Friedrich Bernhard Riemann, né le 17 septembre 1826 à Breselenz, État de Hanovre, mort le 20 juillet 1866 à Selasca, hameau de la commune de Verbania, Italie, est un mathématicien allemand. Influent sur le plan théorique, il a apporté une contribution importante à l'analyse et à la géométrie différentielle.



Pierre Cartier, est un ancien élève de l'Ecole Normale Supérieure, il est docteur en mathématiques (1958), directeur de recherche au CNRS, professeur de mathématiques à l'Ecole normale supérieure. Il a été membre du groupe Bourbaki.



John Torrence Tate Jr. (13 mars 1925 à Minneapolis) est un mathématicien américain. En 2010, il a reçu le prix Abel pour ses travaux en théorie des nombres. John Tate est décrit par William Beckner, directeur du département de mathématiques de l'université du Texas, comme un des mathématiciens marquants de ces cinquante dernières années la théorie des nombres.

André Weil, né le 6 mai 1906 à Paris et mort à Princeton (New Jersey, États-Unis) le 6 août 1998, est une des grandes figures parmi les mathématiciens du XXe siècle. Connu pour son travail fondamental en théorie des nombres et en géométrie algébrique, il fut un des membres fondateurs du groupe Bourbaki. Il est le frère de la philosophe Simone Weil.

André Néron (30 Novembre 1922 - 6 avril 1985) était un mathématicien français de l' Université de Poitiers qui a travaillé sur les courbes elliptiques et variétés abéliennes. Il a découvert le modèle de Néron minimal d'une courbe elliptique ou de la variété abélienne, le groupe de Néron-Severi, la hauteur de Néron-Tate des points rationnels sur une variété abélienne, et classé les fibres éventuelle d'une fibration elliptique.

Michel Raynaud (né le 16 juin 1938) est un mathématicien français qui a travaillé en géométrie algébrique. Depuis 1967, il est professeur à l'université de Paris-Sud 11. Avec Alexandre Grothendick et d'autres mathématiciens, il a travaillé sur plusieurs volumes du Séminaire de géométrie algébrique. En 1938, il écrivit une preuve de la conjecture de Manin-Mumford. En 1987, l'académie des Sciences lui décerna le prix Ampère. En 1995, il reçut avec David Harbater, le prix Cole pour ses solutions de la conjecture Abhynkar.

Les Contemplations, I, 13 : A propos d'Horace (extrait)

. . .

J'étais alors en proie à la mathématique.
Temps sombre ! enfant ému du frisson poétique
On me livrait tout vif aux chiffres, noirs bourreaux
On me faisait de force ingurgiter l'algèbre
On me tordait depuis les ailes jusqu'au bec
Sur l'affreux chevalet des *x* et des *y*
Hélas, on me fourrait sous les os maxillaires
Le théorème orné de tous ses corollaires.
Pourtant, on peut être poète et mathématicien.

. . .

Victor Hugo