David A. Madore

MÉMOIRE DE MAGISTÈRE

Magistère de Mathématiques Fondamentales
et Appliquées et d'Informatique

École Normale Supérieure de Paris

Table des matières

Courbes ordinaires et logique intuitionniste

David A. Madore

3 décembre 1999

1 Avant-propos

Ce rapport de magistère se compose de deux parties. La première consiste en un rapport de mon stage de DEA, effectué avec Michel Raynaud, et aboutissant à une présentation ([8]) lors d'une rencontre à Luminy ([1]) en décembre 1998 de certains résultats obtenus par Raynaud dans [10] et [11].

La seconde partie de ce rapport présente les idées principales d'un groupe de travail sur le forcing et la logique mathématique que j'ai organisé à l'ENS pendant l'année scolaire 1998–1999.

Ce mémoire est accompagné du rapport [7] de première année de magistère ainsi que de mon rapport de DEA [8].

2 Courbes ordinaires en caractéristique p

2.1 Fibrés vectoriels sur les courbes et diviseurs θ

Soit k un corps algébriquement clos (dans un premier temps, on ne fera pas d'hypothèse sur la caractéristique de k) et X une courbe algébrique projective lisse connexe sur k de genre g. On supposera généralement que $g \geq 2$.

Si E est un fibré vectoriel sur X, on peut considérer d'une part le rang r de E (i.e. la dimension du k-espace vectoriel modèle de la fibre de E) et d'autre part son degré d (le degré est un entier relatif associé au faisceau, additif dans les suites exactes courtes, et qui coïncide avec le degré du diviseur D pour les faisceaux de la forme $\mathcal{O}(D)$). On peut alors définir la *pente* du fibré comme le rapport du degré sur le rang : $\lambda = d/r$.

On notera par exemple que les rangs et les degrés s'ajoutent dans les suites exactes courtes (en particulier, le degré (resp. le rang) de $E \oplus E'$ sont la somme du degré (resp. du rang) de E et de E'). La pente, elle, s'ajoute dans les produits tensoriels : la pente de $E \otimes E'$ est la somme des pentes de E et de E'.

Ces quantités permettent de calculer la caractéristique d'Euler-Poincaré de E, d'après la formule de Riemann-Roch :

$$\chi(X, E) = h^0(X, E) - h^1(X, E) = r(\lambda - (g - 1))$$

(ici, $h^i(X, E)$ désigne la dimension du i-ième groupe $H^i(X, E)$ de cohomologie de X à valeurs dans E). (Par exemple, si $E = \Omega^1$ est le fibré des formes différentielles, on a $r = 1$ et $\lambda = d = 2g - 2$ pour $\chi(X, \Omega^1) = g - 1$.)

En particulier, si la pente de E est $g - 1$ (la *pente critique*), on voit que $\chi(X, E) = 0$, autrement dit que $h^0(X, E) = h^1(X, E)$. On peut se demander dans ces circonstances si par hasard on aurait $h^i(X, E) = 0$.

Plus généralement, si L est un faisceau inversible de degré 0 (i.e. un faisceau de rang 1 et de pente nulle), on voit que le degré et la pente de $E \otimes L$ sont ceux de E. Si E a la pente critique, on peut se demander si $h^i(X, E \otimes L) = 0$:

Question 2.1. *Supposons que E soit un fibré vectoriel sur X de pente critique $\lambda = g - 1$. Alors pour quels faisceaux inversibles L de degré 0 a-t-on $h^0(X, E \otimes L) = 0$ (et donc aussi $h^1(X, E \otimes L) = 0$) ?*

On peut commencer par trouver une condition nécessaire : supposons que le fibré E ait un sous-fibré F tel que $\lambda(F) > \lambda(E) = g - 1$. Alors on aurait $\chi(X, F \otimes L) > 0$ (d'après la formule de Riemann-Roch) donc $h^0(X, F \otimes L) > 0$, et comme $H^0(X, F \otimes L)$ s'injecte dans $H^0(X, E \otimes L)$, cela montre $h^0(X, E \otimes L) > 0$ pour tous les L. Par contraposée, si on veut espérer que $h^0(X, E \otimes L) = 0$ pour un certain L, il faudra supposer que ce phénomène ne se produit pas. D'où la définition :

Définition 2.2. *Un fibré vectoriel E sur X est dit* semi-stable *ssi pour tout sous-fibré non nul F de E on a $\lambda(F) \leq \lambda(E)$.*

Pour répondre à question 2.1, il faudra faire varier le faisceau L. Pour cela, on introduit la *variété jacobienne* J de la courbe X : c'est la variété algébrique qui paramétrise les faisceaux inversibles de degré 0 sur X (i.e. dans un sens qu'il faudrait préciser, les points de J sont les faisceaux inversibles de degré 0 sur X). La variété J est lisse, connexe, et sa dimension est précisément le genre g de X ; de plus, si on a choisi une origine O sur X (on supposera désormais que c'est le cas), alors X s'envoie dans J par $x \mapsto \mathcal{O}(x - O)$: ce morphisme est un isomorphisme en genre 1 et est une immersion fermée en genre $g \geq 2$. Enfin, J est une variété *abélienne* : elle est munie d'une loi de groupe abélien (le produit tensoriel sur les faisceaux inversibles de degré 0) compatible avec sa structure algébrique.

Le *théorème de semicontinuité* affirme que les $h^i(X, E \otimes L)$ (comme fonctions de L) sont semi-continues supérieurement. En particulier, si $h^0(X, E \otimes L_0) = 0$ (la plus petite valeur possible) pour un certain L_0, alors c'est le cas sur tout un voisinage (ouvert) de ce L_0. Comme on a la chance de travailler en géométrie algébrique, un ouvert non vide (d'une variété irréductible telle que J) est dense, et on a $h^0(X, E \otimes L) = 0$ pour *presque tout* L. On dira que $h^0(X, E \otimes L) = 0$ pour un faisceau inversible L de degré 0 *général* et on notera $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$.

Dans ce cas (lorsque $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$, on peut s'intéresser au fermé des points L de J pour lesquels $h^0(X, E \otimes L) = 0$. On va en fait en faire un *diviseur* sur J, qu'on appellera le *diviseur thêta* de E.

On évitera de rentrer dans les détails techniques, mais pour faire varier correctement le faisceau L, il faut introduire un faisceau $\mathscr{L}$, le *faisceau de Poincaré*, sur $X \times J$, qui se restreint sur chaque $X \times \{L\}$ en le faisceau L sur X (autrement dit, on met ensemble de la manière évidente tous les faisceaux inversibles de degré 0 sur X). On cherche à calculer la cohomologie fibre à fibre de $E \otimes \mathscr{L}$ (avec l'abus de notation évident consistant à noter E pour ce qui est en réalité un fibré sur $X \times J$) : si on veut jouer avec les catégories dérivées, c'est $Rf_*(E \otimes \mathscr{L})$, où $f \colon X \times J \to J$ est la seconde projection.

Il existe un complexe $0 \to M^0 \xrightarrow{u} M^1 \to 0$ de fibrés vectoriels sur J qui calcule universellement la cohomologie (c'est-à-dire qu'elle la calcule après tout changement de base). En pratique, et pour ce qui nous intéresse, M^0 et M^1 sont deux fibrés vectoriels, et sur toute fibre L de f, le noyau et le conoyau de u sont le $h^0(X, E \otimes L)$ et le $h^1(X, E \otimes L)$. Les fibrés M^0 et M^1 ont même rang (car la caractéristique d'Euler-Poincaré de E est nulle), disons s, donc on peut considérer le déterminant

$$\mathcal{O}_J \xrightarrow{\det u} \bigwedge^s M^1 \otimes \left(\bigwedge^s M^0\right)^{\otimes -1}$$

de u.

Pour résumer toute la discussion deux cas peuvent se produire :

- *Soit* on a $h^0(X, E \otimes L) > 0$ partout (et bien sûr aussi $h^1(X, E \otimes L) > 0$), autrement dit u n'est nulle part inversible, $\det u = 0$ identiquement.

– *Soit* on a $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$. Alors u est génériquement inversible, et $\det u$ est une section non nulle du faisceau inversible $\bigwedge^s M^1 \otimes \big(\bigwedge^s M^0\big)^{\otimes -1}$. Il définit un diviseur θ_E sur J, dont le support est précisément l'ensemble des L tels que $h^0(X, E \otimes L) > 0$. En somme, θ_E marque « l'endroit sur J où E a de la cohomologie ».

On utilisera l'expression « admettre un diviseur thêta » pour signifier qu'on est dans le second cas, i.e. que $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$. Ainsi, un fibré vectoriel qui admet un diviseur thêta est semi-stable. (La réciproque n'est pas vraie comme il est montré dans [11].)

On renvoie à [9] pour le lien entre les diviseurs thêta ainsi définis et les fonctions thêta classiques.

2.2 Faisceau des différentielles localement exactes

On suppose maintenant que le corps de base k a caractéristique $p > 0$. On a alors une courbe X_1 obtenue en élevant à la puissance p les coefficients des équations projectives définissant X, et un morphisme $\pi \colon X \to X_1$, le *Frobenius relatif*, qui correspond dans l'espace projectif à élever les coordonnées à la puissance p. La courbe X_1 a le même genre g que X ; le morphisme π est plat, fini, totalement ramifié, de degré p; pour ceux qui ne sont pas très familiers avec la géométrie algébrique : π est un homéomorphisme. Le faisceau structural $\mathcal{O}_{X_1}$ (des fonctions polynômiales sur X_1), ou plutôt son image réciproque par π, apparaît comme le faisceau des puissances p-ièmes des sections de $\mathcal{O}_X$.

On considère l'application différentielle $d \colon \mathcal{O}_X \to \Omega^1_X$ (application $\mathbb{Z}$-linéaire entre faisceaux de groupes abéliens) ; son noyau est précisément $\mathcal{O}_{X_1}$ (ou, plus précisément $\pi^*\mathcal{O}_{X_1}$), le faisceau des puissances p-ièmes. On considère maintenant son image ; pour plus de commodité (i.e. pour travailler avec de vrais fibrés vectoriels) on se placera sur X_1 plutôt que sur X, et on considère donc l'image de $\pi_*(d) \colon \mathcal{O}_{X_1} \to \pi_*\mathcal{O}_X$. Appelons B_1 cette image : B_1 est un fibré vectoriel (en tant que sous-$\mathcal{O}_X$-module du fibré $\pi_*\Omega^1_X$). On l'appelle faisceau des différentielles localement exactes.

(Cela pourra naturellement surprendre si on n'est pas habitué à la caractéristique p : en caractéristique 0, naturellement, toutes les formes différentielles de degré 1 sont fermées, puisqu'on travaille en dimension 1, donc localement exactes.)

On a la suite exacte :

$$0 \to \mathcal{O}_{X_1} \to \pi_* \mathcal{O}_X \to B_1 \to 0$$

On peut facilement calculer les caractéristiques numériques de B_1 : son rang est $p-1$ comme il résulte de la suite exacte ci-dessus ($\pi_*\mathcal{O}_X$ a pour rang p et $\mathcal{O}_{X_1}$ a rang 1), et sa caractéristique d'Euler-Poincaré est nulle (car $\pi_*\mathcal{O}_X$ et $\mathcal{O}_{X_1}$ ont tout deux la caractéristique d'Euler-Poincaré $1-g$), donc sa pente est $\lambda(B_1) = g-1$, la pente critique, et ce qu'on a dit dans la section précédente s'applique au fibré B_1 sur X_1.

D'après la suite exacte courte ci-dessus, on a la suite exacte longue suivante :

$$0 \to H^0(X_1, B_1) \to H^1(X_1, \mathcal{O}_{X_1}) \to H^1(X, \mathcal{O}_X) \to H^1(X_1, B_1) \to 0$$

Ainsi, la flèche du milieu est un isomorphisme si et seulement si $h^0(X_1, B_1) = 0$, ou, ce qui revient au même, $h^1(X_1, B_1) = 0$.

Définition 2.3. *Lorsque ces conditions sont réalisées, la courbe X est dite* ordinaire*.*

Ainsi, la courbe X est ordinaire ssi le faisceau B_1 admet un diviseur thêta et que ce diviseur thêta ne passe pas par l'origine (de la jacobienne de X_1).

Un des résultats centraux de [10] et pour lequel nous renvoyons à [8] pour les détails de la démonstration est que la première partie de cette condition peut être omise, car B_1 admet un diviseur thêta en toute généralité :

Théorème 2.4 (Raynaud). *Le faisceau B_1 admet un diviseur thêta. Autrement dit, pour L_{gen} faisceau inversible de degré 0 général sur X_1, on a $h^0(X_1, B_1 \otimes L_{\text{gen}}) = 0$.*

(Ainsi, une courbe est ordinaire ssi ce diviseur thêta ne passe pas par l'origine.)

Très brièvement résumé, l'argument est le suivant : on introduit J la jacobienne de X et J_1 celle de X_1. On a un morphisme $V : J_1 \to J$ (le *Verschiebung*), qui envoie $\mathcal{O}_{X_1}(\Sigma n_i x_i)$ sur $\mathcal{O}_X(\Sigma p n_i \pi^{-1}(x_i))$. On travaille au voisinage de 0 sur J_1 : soit R l'anneau local de J_1 en 0. On a un morphisme $h\colon N \to k$, où N est l'anneau local en 0 de $\ker V$, correspondant à l'évaluation en 0 : h est clairement surjectif. Or par un argument d'algèbre commutative, on montre que le dual de h, soit $h'\colon \operatorname{Ext}^g(k, R) \to \operatorname{Ext}^g(N, R)$ est un quotient de notre $\det u$ introduit dans la première section (i.e. un quotient de la multiplication par $\det u$, sur $\bigwedge^g R^g$). Mais comme h est surjective, h' est injective, donc $\det u$ ne peut pas être nulle. Ainsi, B_1 a un diviseur thêta.

Naturellement, l'argument montre aussi que $\det u$ est inversible ssi et seulement si l'anneau local N de $\ker V$ à l'origine est précisément k ; autrement dit, la courbe X est ordinaire si et seulement si le Verschiebung est étale.

Par ailleurs, dans [8] il est présenté un autre résultat de Raynaud (démontré dans [11]) : on construit un revêtement étale fini d'une courbe ordinaire qui n'est pas ordinaire. On montre même, plus précisément, qu'il existe un revêtement galoisien résoluble de la courbe générique (d'un genre donné) qui n'est pas ordinaire (la courbe générique, elle, est ordinaire, et on sait même qu'un revêtement abélien de la courbe générique est ordinaire). Nous ne présentons pas la méthode ici, qui consiste à associés des fibrés vectoriels de pente critique à des représentations finies du groupe fondamental algébrique de la courbe, et à choisir judicieusement ces représentations.

3 Logique mathématique

3.1 Forcing : présentation intuitive

Le *forcing* est une technique de démonstration inventée par Paul Cohen dans [2] et utilisée pour démontrer le résultat suivant :

Théorème 3.1. *L'hypothèse du continu n'est pas démontrable à partir des axiomes de la théorie des ensembles : autrement dit, si les axiomes de la théorie des ensembles sont non-contradictoires, ils le restent après adjonction de la négation de l'hypothèse du continu. Le même résultat est vrai avec « axiome du choix » à la place de « hypothèse du continu ».*

La manière de présenter le forcing a beaucoup évolué entre la présentation originale de Cohen et la présentation moderne développée par Scott, Solovay et Vopěnka (voir [3]). Mais le principe de base est toujours le même : on part d'un modèle de la théorie des ensembles, et on construit un nouveau modèle en étendant l'ensemble des valeurs de vérité. Dans le modèle de départ, on n'a que deux valeurs de vérité, le faux et le vrai ; dans le modèle qu'on construit, on a une algèbre de Boole complète, construite en fonction du problème à résoudre, pour ensemble de valeurs de vérité. Cette opération crée de nouveaux objets dont on peut éventuellement contrôler le comportement.

Prenons un exemple simple : choisissons comme ensemble de valeurs de vérité l'ensemble des parties de $\mathbb{N}$, qui est bien une algèbre de Boole complète. On peut alors considérer un nombre naturel x du nouveau modèle, pour lequel la valeur de vérité de $x = n$ soit égale à $\{n\}$ pour tout entier naturel (ancien) n. On a créé un nouvel entier naturel (et beaucoup d'autres, d'ailleurs), un entier « générique ». En vérité, cette construction-ci n'a rigoureusement aucun intérêt (sinon pédagogique), mais des constructions semblables, légèrement plus sophistiquées, donnent des résultats intéressants (ainsi, l'ajout d'un grand nombre de nombres réels génériques casse l'hypothèse du continu, voir [3] pour les détails ; pour casser l'axiome du choix, on fait apparaître des ensembles génériques, puis on les rend indistingables en imposant des fortes actions de groupes de permutations, qu'on ne peut casser qu'à hauteur finie, voir [3] et [4] pour les détails).

Il s'agit là du forcing « classique », qui reste entièrement dans le cadre de la logique classique. Il existe par ailleurs d'autres sortes de logique, notamment la logique intuitionniste, formée des mêmes axiomes que la logique classique mais dans laquelle on retire la loi du « tiers exclu » $A \vee \neg A$, ou la loi de Pierce $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$. Kripke a remarqué que la notion de topos, inventée par Grothendieck, permettait de définir des sémantiques (dites de Kripke-Joyal, voir [6]) pour la logique intuitionniste, qui sont des généralisations de la notion de forcing « classique » (ainsi, l'indémontrabilité de l'hypothèse du continu et de l'axiome du choix sont-elles montrées dans [6] par des méthodes purement de théorie des catégories, par opposition aux méthodes classiques qu'on trouve dans [3]) mais qui permettent, de plus, d'obtenir des résultats spécifiques à la logique intuitionniste. Le principe est toujours d'étendre l'ensemble des valeurs de vérité, mais à des choses plus générales (par exemple, l'ensemble des ouverts d'un espace topologique si on considère une sémantique de faisceaux : ils forment non pas une algèbre de Boole complète mais une algèbre de Heyting complète, voir [6]).

Un des résultats les plus spectaculaires dans ce domaine est le suivant :

Théorème 3.2 (de Brouwer). *Il est consistant, en logique intuitionniste, de supposer que toutes les fonctions $\mathbb{R} \to \mathbb{R}$ sont continues.*

(résultat à comparer avec un théorème de Solovay (voir [3]) affirmant qu'il est consistant en théorie des ensembles sans l'axiome du choix de supposer que toutes les fonctions $\mathbb{R} \to \mathbb{R}$ sont mesurables au sens de Lebesgue).

3.2 Sémantiques dans les catégories de faisceaux

La notion de topos a été inventée par Grothendieck à partir de considérations provenant de la géométrie algébrique. Il s'agit essentiellement de catégories qui ressemblent de certains points de vue à la catégorie des ensembles (mais dont la logique interne est éventuellement intuitionniste). Les logiciens ont une notion de topos (topos élémentaire) un peu plus générale (et pourtant plus simple) que les géomètres algébristes (topos de Grothendieck), mais les catégories de faisceaux, le seul exemple que nous considérerons, sont des topos[1] au sens de Grothendieck.

On considère donc une catégorie $\mathcal{C}$ de faisceaux sur un site. Si on ne sait pas ce qu'est un site, on se contentera de considérer des faisceaux sur un espace topologique.

Définition 3.3 (sémantique de Kripke-Joyal). *Soit U un ouvert, soit $\varphi(t_1, \dots, t_n)$ une formule du calcul des prédicats dans un langage dont les variables sont typées par des objets de $\mathcal{C}$ (i.e. des faisceaux), $X_1, \dots, X_n$ les types des variables $t_1, \dots, t_n$ dans cette formule (qui sont des faisceaux), et soient $x_1, \dots, x_n$ des sections de $X_1, \dots, X_n$ sur U. Alors on définit $U \Vdash \varphi(x_1, \dots, x_n)$ (lire « U "force" $\varphi(x_1, \dots, x_n)$ ») par récurrence sur la complexité de φ de la manière suivante :*

- *$U \Vdash \top$ pour tout U.*
- *$U \Vdash \varphi \wedge \psi$ ssi $U \Vdash \varphi$ et $U \Vdash \psi$.*
- *$U \Vdash \varphi \Rightarrow \psi$ ssi pour tout $V \to U$ (tout ouvert V de U) tel que $V \Vdash \varphi$ on a[2] $V \Vdash \psi$.*
- *$U \Vdash \forall t \varphi(t)$ ssi pour tout $V \to U$ et toute section x de X (le type de t) sur V on a $V \Vdash \varphi(x)$.*
- *$U \Vdash \perp$ ssi la famille vide recouvre U.*
- *$U \Vdash \varphi \vee \psi$ ss'il existe un recouvrement de U par $V \to U$ et $W \to U$ tels que $V \Vdash \varphi$ et $W \Vdash \psi$.*
- *$U \Vdash \exists t \varphi(t)$ ss'il existe un recouvrement de U par une famille $V_i \to U$ et des sections x_i de X (le type de t) sur V_i tels que $V_i \Vdash \varphi(x_i)$.*

Naturellement, il reste le problème des formules atomiques. On décrétera que $U \Vdash x = y$ ssi x et y sont égales (en tant que sections du même faisceau

[1] L'usage veut que le pluriel de « topos » soit « topoi » s'il s'agit de topoi élémentaires et « topos » s'il s'agit de topos de Grothendieck.

[2] Lorsqu'on écrit $V \Vdash \varphi$ il faut comprendre que toutes les sections sur U représentant des variables libres dans φ ont été restreintes à V (par la flèche $V \to U$ donnée si on travaille sur un site).

sur U) ; pour les autres formules atomiques, cela dépend des relations et des fonctions dont on a muni la catégorie.

Enfin, si U est l'ouvert terminal (l'espace tout entier si on travaille sur un espace topologique, ou bien l'objet terminal du site si on travaille sur un site), on note tout simplement φ (lire « φ est vraie (dans la catégorie considérée) ») au lieu de $U \Vdash \varphi$.

Donnons d'emblée un exemple frappant d'utilisation de cette sémantique de Kripke-Joyal :

Proposition 3.4. *Soit $\mathcal{C}$ la catégorie des faisceaux sur le « gros site » topologique (i.e. un objet de $\mathcal{C}$ est un foncteur contravariant qui à un espace topologique associe un ensemble, et qui est un faisceau pour la notion habituelle de recouvrement). Soit $\mathscr{R}$ l'objet de $\mathcal{C}$ qui a un espace topologique X associe l'ensemble des fonctions continues de X vers $\mathbb{R}$. Alors la formule suivante est vraie dans $\mathcal{C}$:*

$$\forall f \in \mathscr{R}^{\mathscr{R}} \ \ \forall x \in \mathscr{R} \ \ \forall \varepsilon > 0 \ \ \exists \eta > 0 \ \ \forall y \in \mathscr{R}$$
$$(x - \eta < y < x + \eta \Rightarrow f(x) - \varepsilon < f(y) < f(x) + \varepsilon)$$

(lire : toutes les fonctions de $\mathscr{R}$ vers $\mathscr{R}$ sont continues).

Démonstration. On veut montrer que $\top \Vdash \varphi$ où $\top$ est l'espace topologique terminal (à un point) et φ est la formule écrite ci-dessus. Le principal problème est de comprendre ce que signifie le type de f. Il est indiqué comme $\mathscr{R}^{\mathscr{R}}$ dans la formule. Or la définition de l'exponentielle dans une catégorie de faisceaux (expliquée dans [6]) associée au lemme de Yoneda montre que $\mathscr{R}^{\mathscr{R}}$ est le faisceau qui à un espace topologique X associe l'ensemble des fonctions continues de $X \times \mathbb{R}$ vers $\mathbb{R}$.

On déroule les trois quantificateurs universels, et on doit montrer finalement que si U est un espace topologique, $f \colon U \times \mathbb{R} \to \mathbb{R}$ continue, $x \colon U \to \mathbb{R}$ continue, et $\varepsilon \colon U \to \mathbb{R}$ continue et strictement positive, alors U force (la proposition de départ partant de $\exists \eta > 0$).

Pour chaque $u \in U$, f est continue en $(u, x(u))$, donc il existe un $\eta_u > 0$ tel que $f(u, y)$ soit à moins de $\varepsilon(u)$ de $f(u, x(u))$ si y est à moins de η_u de $x(u)$. Comme f, x et ε sont continues, ceci reste vrai pour v dans un certain voisinage V_u de u. Les V_u recouvrent U. Sur chaque V_u on prend la fonction η constante égale à η_u.

Il reste alors à montrer que V_u force (la proposition de départ partant de $\forall y \in \mathscr{R}$). Or cela est à peu près évident. $\square$

Quelques remarques cependant. D'abord, on a silencieusement interprété l'addition, la soustraction et l'inégalité sur $\mathscr{R}$ comme les relations correspondantes sur les fonctions réelles. Ensuite, on a un peu escamoté la clé de la démonstration, qui est, finalement, une application du lemme de Yoneda. Enfin, le théorème qu'on vient de démontrer n'est pas la totalité du théorème 3.2, car il manque l'explication de pourquoi $\mathscr{R}$ est bien « le corps des nombres réels » tel qu'on l'attend ; pour cela, il faut construire ce corps des réels par des coupures de Dedekind (par exemple) à partir du corps des rationnels, lui-même construit comme corps des fractions de l'anneau des entiers, lui-même construit comme symétrisé du monoïde des naturels. Cela se fait (mais c'est assez pénible). Tous les détails sont dans [6].

3.3 Relations avec la géométrie

La perspective que toutes les fonctions réelles soient continues est assurément alléchante. On peut se demander s'il y a moyen d'utiliser de tels résultats dans des « vraies » mathématiques. La réponse est **oui**. Il existe une branche de la géométrie différentielle, la « géométrie différentielle synthétique », qui utilise des axiomes, qui ne peuvent être satisfaits que dans des logiques intuitionnistes, et qui sont effectivement modélisés par des topoi élémentaires, pour faire de la géométrie en se basant sur le principe que toutes les fonctions rélles sont indéfiniment différentiables. Nous renvoyons à [5] pour plus de précisions sur cette science occulte.

Du reste, la notion de topos provient de la géométrie algébrique : il est juste qu'elle y revienne. Il devrait être possible d'utiliser des techniques semblables, ou au moins un langage semblable, en géométrie algébrique. En effet, la géométrie algébrique est, au fond, l'étude (d'une partie) du topos plat (ou étale, ou Zariski) sur les anneaux commutatifs. Cette catégorie de faisceaux possède une logique interne, sa sémantique de Kripke-Joyal, comme expliqué dans la section précédente, et celle-ci est intuitionniste. Nous menons quelques réflexions « internes » dans ce topos pour bien s'en convaincre.

Ce qui devrait représenter la « droite » est $\mathscr{R} = \operatorname{Spec} \mathbb{Z}[t]$, autrement dit le faisceau qui à un anneau commutatif A associe $\operatorname{Hom}(\mathbb{Z}[t], A)$ son ensemble sous-jacent. Cet objet $\mathscr{R}$ est muni d'une structure de groupe (interne), ce qu'en géométrie algébrique on traduit en disant que $\mathbb{G}_{\mathrm{a}} = \operatorname{Spec} \mathbb{Z}[t]$ est un schéma en groupes. En fait, $\mathscr{R}$ a même une structure d'anneau (interne), résultant des structures d'anneau sur les différents $\operatorname{Hom}(\mathbb{Z}[t], A)$. L'« ensemble des éléments non nuls » de $\mathscr{R}$, noté $\{t \in \mathscr{R} : \neg(t = 0)\}$, est le faisceau qui a un anneau A associe l'ensemble des $t \in \mathrm{Hom}(\mathbb{Z}[t], A)$ (bref, des $t \in A$) tels que $A \Vdash \neg(t = 0)$; or on voit facilement que cela signifie que t est inversible. Bref, $\{t \in \mathscr{R} : \neg(t = 0)\}$ est précisément le faisceau $\mathscr{R}^\times = \mathrm{Spec}\,\mathbb{Z}[t, t^{-1}]$ qui a un anneau A associe l'ensemble $A^\times$ des éléments inversibles de A ; c'est aussi l'« l'ensemble des éléments inversibles » de $\mathscr{R}$ pour la loi de multiplication interne, noté $\{x \in \mathscr{R} : \exists y(xy = 1)\}$. De cette dernière coïncidence on peut dire que $\mathscr{R}$ est un corps (on a $\forall x \in \mathscr{R}((\neg(x = 0)) \Leftrightarrow (\exists y(xy = 1))))$. Attention, cependant, il y a plusieurs manières de traduire « corps » en logique intuitionniste : il n'est pas vrai que $\forall x \in \mathscr{R}(x = 0 \vee \exists y(xy = 1))$.

On peut d'ailleurs donner une illustration frappante du caractère intuitionniste de la logique interne : on a vu que $\{t \in \mathscr{R} : \neg(t = 0)\}$ est $\mathrm{Spec}\,\mathbb{Z}[t, t^{-1}]$, le sous-schéma ouvert de $\mathrm{Spec}\,\mathbb{Z}[t]$ défini par l'équation $t \neq 0$; d'autre part, il est évident que $\{t \in \mathscr{R} : t = 0\}$ est tout simplement le sous-schéma fermé $\{0\}$ de $\mathrm{Spec}\,\mathbb{Z}$. Or la réunion des deux, $\{t \in \mathscr{R} : (t = 0) \vee \neg(t = 0)\}$ n'est manifestement pas $\mathscr{R} = \mathrm{Spec}\,\mathbb{Z}$ tout entier. Par exemple, les points sur $\mathbb{Z}$ de cette réunion sont $\{-1, 0, +1\}$, ce qui est loin d'être $\mathbb{Z}$ entier. Pareillement, $\{t \in \mathscr{R} : \neg\neg(t = 0)\}$ n'est pas $\{t \in \mathscr{R} : t = 0\}$: on peut montrer que c'est le faisceau qui à un anneau A associe l'ensemble des nilpotents de A (à la différence des précédents exemples, ceci n'est pas un schéma) ; et on n'a pas non plus $\forall t \in \mathscr{R}(\neg(t = 0) \vee \neg\neg(t = 0))$.

Il devrait être possible de reformuler une partie de la géométrie algébrique dans des termes purement « internes » au topos plat. (Il n'est même pas exclu que cela puisse servir, ne serait-ce que parce que cette logique interne, fût-elle intuitionniste, peut parfois se manipuler plus élégamment que des notions extrinsèques.) La question principale est alors : peut-on reformuler les principales définitions de la géométrie algébrique (ne serait-ce que « X est un schéma ») dans le langage interne, et, si oui, comment ?

C'est sur cette douloureuse question que je conclus cet exposé.

Références

[1] J.-B. Bost, F. Loeser & M. Raynaud, éd., *Courbes semi-stables et groupe fondamental en géométrie algébrique*, Birkhäuser (à paraître).

[2] P. J. Cohen, *Set Theory and the Continuum Hypothesis*, Benjamin.

[3] T. J. Jech, *Set Theory*, Academic Press (79).

[4] T. J. Jech, *The Axiom of Choice.*

[5] A. Kock, *Synthetic Differential Geometry*, Cambridge University Press (London Mathematical Society Lecture Note Series, 51).

[6] S. MacLane & I. Moerdijk, *Sheaves in Geometry and Logic*, Springer.

[7] D. Madore & J. Marot, « Le théorème de Belyĭ », rapport de première année de magistère.

[8] D. Madore, « Theta Divisors and the Frobenius Morphism », *in* [1], p. 237–246.

[9] D. Mumford, « On the Equations Defining Abelian Varieties, I », *Inventiones mathematicæ*, **1** (1966), p. 287–354.

[10] M. Raynaud, « Sections des fibrés vectoriels sur une courbe », *Bull. Soc. math. France*, **110** (1982), p. 103–125.

[11] M. Raynaud, « Revêtements des courbes en caractéristique $p > 0$ et ordinarité », à paraître.

Le Théorème de Belyĭ

(Exposé de première année de magistère,
Sujet proposé par Y. Laszlo)

David Madore (david.madore@ens.fr)
et Jean Marot (jean.marot@ens.fr)

Résumé

Un théorème dû à Riemann affirme que toute surface de Riemann compacte X est en fait une courbe algébrique (projective lisse) — c'est-à-dire peut être définie par des équations algébriques. La question se pose de savoir quand ces équations peuvent être choisies à coefficients dans $\bar{\mathbb{Q}}$, la clôture algébrique de $\mathbb{Q}$. Le théorème de Belyĭ donne une condition nécessaire et suffisante portant uniquement sur la géométrie de la surface : il faut et il suffit que celle-ci se réalise comme un revêtement holomorphe de la sphère de Riemann Σ ramifié en au plus trois points de Σ.

Cette caractérisation étant obtenue, on en déduit une action fidèle du groupe de Galois "absolu" de $\bar{\mathbb{Q}}/\mathbb{Q}$ sur le groupe profini libre à deux générateurs.

1 Préliminaires sur les surfaces de Riemann

Une <u>surface de Riemann</u> est une variété différentiable de dimension 1 complexe (2 réelle) munie d'un atlas dont les changements de cartes sont holomorphes. Une application entre surfaces de Riemann qui, dans les systèmes de coordonnées donnés par un tel atlas, se représente par des fonctions holomorphes, est dite holomorphe. Les morphismes entre surfaces de Riemann sont les applications holomorphes. Les isomorphismes entre surfaces de Riemann sont les applications holomorphes bijectives (la réciproque en est alors nécessairement holomorphe).

Exemples : Le plan complexe $\mathbb{C}$, la sphère de Riemann notée $\bar{\mathbb{C}}$, $\mathbb{P}^1(\mathbb{C})$ ou Σ, et le demi-plan de Poincaré

$$\mathcal{H} := \{z \in \mathbb{C}\colon\ \operatorname{Im} z > 0\}$$

sont des surfaces de Riemann — ce sont d'ailleurs les seules simplement connexes.

On rappelle qu'un point critique d'une fonction différentiable f (entre variétés différentiables) est un point où f n'est pas submersive. Et une valeur critique est l'image d'un point critique. Un point de la variété d'arrivée qui n'est pas une valeur critique (y compris s'il n'est pas atteint du tout) est appelé valeur régulière.

Une application continue surjective $p\colon X \to Y$ entre espaces topologiques non vides est appelée un revêtement [topologique] ssi pour tout point $y \in Y$ il existe un voisinage ouvert V de y dans Y tel que $p^{-1}(V)$ soit une union disjointe d'ouverts U_i avec $p|_{U_i}\colon U_i \to V$ un homéomorphisme pour tout i. Le nombre de préimages d'un point $y \in Y$ est alors localement constant, donc constant si Y est connexe. Dans ce dernier cas, et s'il est fini, on l'appelle le degré du revêtement. Il est clair que le degré d'une composée est le produit des degrés.

On appellera revêtement [holomorphe] ramifié une application $f\colon X \to Y$ holomorphe non constante *propre* entre surfaces de Riemann. Si de plus f est sans valeur critique, alors f est un revêtement au sens topologique ([3]). Quitte à restreindre le domaine, on peut toujours se ramener à ce cas, et ainsi définir le degré $\deg f$ de f même dans le cas ramifié. On utilise ici implicitement le fait que l'ensemble des valeurs régulières est non vide — en fait l'ensemble des valeurs critiques d'une application C^∞ entre variétés différentielles est de mesure nulle, c'est le théorème de Morse-Sard, cf. [8] — mais puisqu'ici on ne se servira du degré que pour des revêtements entre surfaces de Riemann compactes, ce résultat n'est pas nécessaire. On a encore la propriété de multiplicativité des degrés $\deg(fg) = (\deg f)(\deg g)$. On remarquera que toute application holomorphe non constante entre surfaces de Riemann *compactes* est un revêtement ramifié (en effet, elle est trivialement propre).

Il est bien connu que toute application holomorphe non constante est localement, et à changement de variable près, l'application $z \mapsto z^n$ avec $n > 0$; n est alors appelé l'indice de ramification au point considéré. On montre ([3], [7], [5]) que le degré d'un revêtement ramifié est égal à la somme des indices de ramification des préimages d'un point quelconque.

Soient $f_1, \ldots, f_m$ des polynômes à coefficients complexes homogènes en les $n+1$ variables $z_0, \ldots, z_n$, et supposons de plus que la matrice jacobienne $(\frac{\partial f_i}{\partial z_j})$ soit de rang $n-1$ en tout point de $\mathbb{C}^{n+1} \setminus \{0\}$ où tous les f_i s'annulent. Alors l'ensemble

$$X = \{(z_0 \colon z_1 \colon \cdots \colon z_n) \colon f_1(z_0, \ldots, z_n) = \cdots = f_m(z_0, \ldots, z_n)\}$$

des zéros communs aux f_i dans l'espace projectif $\mathbb{P}^n(\mathbb{C})$ est une sous-variété différentiable de celui-ci, de dimension 2 réelle. On le munit d'une structure de surface de Riemann en décrétant que les projections $(z_0 \colon \cdots \colon z_n) \mapsto z_i/z_j$ sont toutes holomorphes (là où elles sont définies). Une telle surface de Riemann est appelée une <u>courbe algébrique</u> projective lisse, définie par les équations $f_1 = \cdots = f_m = 0$.

Lorsque X est une courbe algébrique projective lisse, définie par les équations $f_1 = \cdots = f_m = 0$, on appelle <u>fonction rationnelle</u> sur X un élément *de degré zéro* du corps des fractions du quotient de $\mathbb{C}[X_0, \ldots, X_n]$ par l'idéal engendré par $f_1, \ldots, f_m$, c'est-à-dire le rapport de deux classes de polynômes homogènes de même degré. Les fonctions rationnelles définissent des fonctions holomorphes de X privé d'un nombre fini de points (les zéros communs au numérateur et au dénominateur) vers la sphère de Riemann Σ. En regardant dans des cartes, on voit aisément que ces points manquants ne sont pas des singularités essentielles, et qu'il est donc possible d'étendre les fonctions rationnelles en des fonctions holomorphes sur X tout entier.

On a le théorème fondamental suivant :

Théorème 1.1 (de Riemann). *Toute surface de Riemann compacte est (isomorphe à) une courbe algébrique projective lisse. De plus, toute fonction méromorphe dessus est rationnelle.*

Démonstration. [3], [5] ou [7]. □

Classification des surfaces de Riemann compactes : On rappelle ([8]) qu'une surface différentiable compacte orientable est classifiée par un unique invariant : son genre. Par conséquent, le genre constitue également un invariant des surfaces de Riemann compactes. Ainsi, la sphère de Riemann est la seule surface de Riemann compacte de genre 0. En revanche, pour tout genre $g \geq 1$, l'ensemble des classes d'isomorphismes de surfaces de Riemann compactes de genre g est indénombrable — dans un sens que nous ne préciserons pas, elles sont classifiées par $3g-3$ paramètres complexes pour $g \geq 2$, et par un seul paramètre pour $g = 1$ (voir plus loin).

2 Théorème de Belyĭ

On appelle <u>fonction de Belyĭ</u> sur une surface de Riemann X un revêtement ramifié $\beta\colon X \to \Sigma$ (où Σ est la sphère de Riemann) dont l'ensemble des valeurs critiques est contenu dans $\{0, 1, \infty\}$.

Exemple fondamental : Pour $m, n \in \mathbb{Z}$, avec $m, n, m+n \neq 0$, posons

$$\begin{aligned} \beta_{m,n}\colon \quad & \Sigma \to \Sigma \\ & z \mapsto \tfrac{(m+n)^{m+n}}{m^m n^n} z^m (1-z)^n \end{aligned}$$

On a alors, en dehors de ∞ et des pôles éventuels,

$$\beta'_{m,n}(z) = \frac{(m+n)^{m+n}}{m^m n^n} z^{m-1}(1-z)^{n-1}(m - (m+n)z)$$

et par conséquent $\beta'_{m,n}(z)$ ne s'annule pas en-dehors de 0, 1 et $\frac{m}{m+n}$. L'ensemble des points critiques est donc inclus dans $\{0, 1, \frac{m}{m+n}, \infty\}$, et l'ensemble des valeurs critiques, dans $\{0, 1, \infty\}$. Il s'ensuit que $\beta_{m,n}$ est une fonction de Belyĭ.

Théorème 2.1 (de Belyĭ). *Soit X une courbe algébrique projective lisse définie par des équations à coefficients dans $\bar{\mathbb{Q}}$. Alors il existe une fonction de Belyĭ $\beta\colon X \to \Sigma$.*

On aura pour cela besoin du résultat suivant, qui découle immédiatement de la formule de composition des différentielles :

Lemme 2.2. *Soit $f_i\colon X_i \to X_{i+1}$ une application C^∞ pour tout $1 \leq i \leq r-1$ avec X_i des variétés différentiables. Alors les valeurs critiques de $f_{r-1} \circ \cdots \circ f_1$ sont exactement les $y \in X_r$ qui sont image par $f_{r-1} \circ \cdots \circ f_{i+1}$ d'une valeur critique de f_i, pour un certain i.*

Démonstration. (du théorème) Supposons X définie par des équations polynômiales dans $\mathbb{P}^n(\mathbb{C})$. On peut clairement supposer que X n'est pas entièrement contenue dans un hyperplan. La fonction rationnelle $(z_0\colon \cdots : z_n) \mapsto z_1/z_0$ restreinte à X définit une fonction méromorphe non constante sur X, c'est-à-dire un revêtement ramifié $\pi\colon X \to \Sigma$. Les équations définissant X étant à coefficients algébriques, les valeurs critiques de π sont clairement dans $\bar{\mathbb{Q}} \cup \{\infty\}$.

Soit f_1 le polynôme minimal sur $\mathbb{Q}$ de l'ensemble des valeurs critiques finies de π, c'est-à-dire le polynôme (unitaire) à coefficients rationnels de plus petit degré s'annulant sur toutes les valeurs critiques finies de π — un tel polynôme existe puisque les valeurs critiques en question sont algébriques. Par récurrence, soit f_{i+1} le polynôme minimal sur $\mathbb{Q}$ de l'ensemble des valeurs critiques finies de f_i. Or tout conjugué algébrique d'un zéro de f_i' est un zéro de f_i' (car $f_i' \in \mathbb{Q}[X]$), donc tout conjugué algébrique d'une valeur critique de f_i est une valeur critique de f_i. Comme celles-ci sont en nombre au plus $\deg f_i - 1$, il s'ensuit que $\deg f_{i+1} \leq \deg f_i - 1$, et les f_i forment une suite de polynômes dont les degrés décroissent strictement. Ainsi, il existe k tel que les valeurs critiques finies de f_k soient rationnelles. Considérons l'application composée

$$\rho = f_k \circ \cdots \circ f_1 \circ \pi \colon X \to \Sigma$$

les valeurs critiques finies de π sont envoyées dans $\mathbb{Q}$ par f_1 et y restent par l'action de $f_k \circ \cdots \circ f_2$; de même, les valeurs critiques finies de f_i sont envoyées dans $\mathbb{Q}$ par f_{i+1} et y restent par l'action de $f_k \circ \cdots \circ f_{i+2}$. En appliquant le lemme, on dispose maintenant d'une application $\rho \colon X \to \Sigma$ dont toutes les valeurs critiques finies sont rationnelles.

Soit A_1 l'ensemble des valeurs critiques finies de ρ autres que 0 et 1. Cet ensemble est bien entendu fini. S'il est vide, le théorème est démontré. Sinon, il contient un rationnel, qui peut s'écrire sous la forme $\frac{m}{m+n}$ avec $m, n, m+n \neq 0$. Posons $g_1 = \beta_{m,n}$. Par récurrence, on définit A_{i+1} comme l'ensemble des valeurs critiques finies de $g_i \circ \cdots \circ g_1 \circ \rho$ autres que 0 et 1, et, s'il contient un rationnel $\frac{m}{m+n}$, on pose $g_{i+1} = \beta_{m,n}$. D'après le lemme, et puisque les valeurs critiques de chaque g_i sont contenues dans $\{0, 1, \infty\}$, chaque A_{i+1} est contenu dans $g_i(A_{i+1})$. Comme de plus $\beta_{m,n}$ envoie $\frac{m}{m+n}$ sur 1, on a $\mathrm{card} A_{i+1} < \mathrm{card} A_i$ pour tout i, et par conséquent il existe i tel que $A_i = \emptyset$. Alors la fonction

$$\beta = g_{i-1} \circ \cdots \circ g_1 \circ \rho$$

est la fonction de Belyĭ recherchée. $\square$

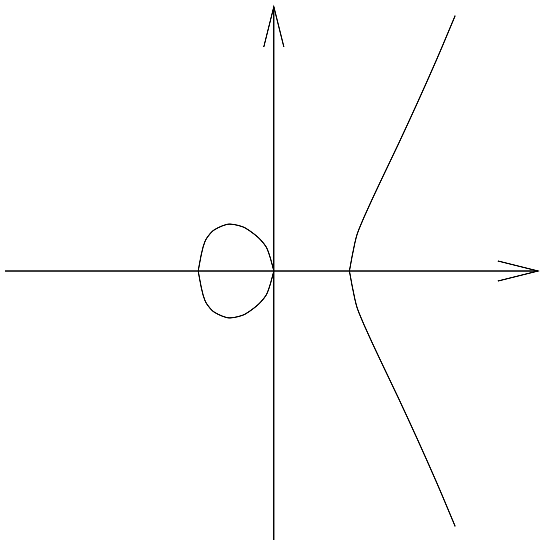
Remarque : La réciproque de ce théorème est vraie en toute généralité — une surface de Riemann compacte sur laquelle il existe une fonction de Belyĭ peut être définie par des équations à coefficients algébriques. Ce résultat sera démontré plus bas dans le cas particulier des courbes elliptiques.

3 Courbes elliptiques (tores complexes)

On appelle courbe elliptique une surface de Riemann compacte de genre 1 ; on montre [11] qu'elle est isomorphe à une courbe algébrique dans $\mathbb{P}^2(\mathbb{C})$ d'équation

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$$

où g_2, g_3 sont des coefficients complexes vérifiant $\Delta := g_2^3 - 27g_3^2 \neq 0$. Ce Δ s'appelle alors le discriminant de la courbe elliptique — ce n'est autre que le discriminant du polynôme $4x^3 - g_2x - g^3$, à un facteur près. Réciproquement, toute équation de cette forme est une courbe elliptique. On définit de plus l'invariant j de la courbe comme $1728g_2^3/\Delta$.



La courbe elliptique d'invariant 1728

Théorème 3.1. *Deux courbes elliptiques sont isomorphes (en tant que surfaces de Riemann) ssi elles ont le même invariant j. De plus, pour tout $j \in \mathbb{C}$ il existe une courbe elliptique d'invariant j.*

Démonstration. On trouvera dans [11] une démonstration du fait que deux courbes elliptiques sont isomorphes en tant que courbes algébriques ssi elles ont le même invariant j, et dans [3], [5] ou [7] une démonstration que deux surfaces de Riemann compactes sont isomorphes en tant que surfaces de Riemann ssi elles le sont en tant que courbes algébriques. Posons enfin $J = j/1728$ et $g_2 = g_3 = \frac{27J}{J-1}$ (si $J \neq 0, 1$; si $J = 0$, on prend $g_2 = 0$ et $g_3 = 1$; si $J = 1$, on prend $g_2 = 1$ et $g_3 = 0$). La courbe d'équation $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ est alors une courbe elliptique d'invariant j. $\square$

Proposition 3.2. *Une courbe elliptique X peut être définie par des équations algébriques à coefficients dans un sous-corps K de $\mathbb{C}$ ssi son invariant j appartient à K.*

Démonstration. Si X est définie par des équations à coefficients dans K, alors on peut ramener par des transformations rationnelles sur K ces équations à une équation sous forme de Weierstraß, $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, avec $g_2, g_3 \in K$ (voir [11] pour les détails). On a alors évidemment $j \in K$. Réciproquement, si $j \in K$, la courbe définie dans la démonstration du théorème précédent est à coefficients dans K, et puisqu'elle a le même invariant j que X, elle lui est isomorphe. Autrement dit, X peut être définie par une équation à coefficients dans K. $\square$

On peut alors démontrer la réciproque du théorème de Belyĭ pour les courbes elliptiques ; on a tout d'abord besoin du

Lemme 3.3. *Soit G un groupe finiment engendré. Alors pour tout n, G n'a qu'un nombre fini de sous-groupes d'indice n.*

Démonstration. Soit G un groupe engendré par $g_1, \dots, g_k$. Si H est un sous-groupe de G d'indice n, identifions les classes à gauches de H à $\{1, \dots, n\}$ où 1 représente H lui-même. L'action de G par multiplication à gauche définit alors un morphisme $G \to \mathfrak{S}_n$. Ces morphismes sont en nombre fini puisqu'il suffit pour en définir un de fixer les images de $g_1, \dots, g_k$. Et de plus, H est alors le stabilisateur de 1 pour cette action. $\square$

Théorème 3.4. *Soit X une courbe elliptique. On suppose qu'il existe une fonction de Belyĭ $\beta\colon X \to \Sigma$. Alors X peut être définie par des équations à coefficients algébriques.*

Démonstration. Soit $\Sigma_0 = \Sigma \backslash \{0, 1, \infty\}$, et $X_0 = \beta^{-1}(\Sigma_0)$. Ainsi, la restriction $\beta\colon X_0 \to \Sigma_0$ est un revêtement (au sens topologique). Il en va de même de $\beta^\sigma\colon X_0^\sigma \to \Sigma_0$ pour tout automorphisme σ de $\mathbb{C}$ (β^σ s'obtient en appliquant σ à tous les coefficients de β, et de même pour X^σ). D'après la théorie générale des revêtements ([4], [6]), il lui correspond un sous-groupe H d'indice $\deg \beta$ de $\pi_1(\Sigma_0)$, lequel n'est autre que le groupe libre $\mathfrak{F}$ sur deux générateurs (précisément, H est le sous-groupe constitué des lacets dans Σ_0 qui se relèvent en un lacet dans X_0). De plus, deux revêtements correspondant au même sous-groupe (ou même à des sous-groupes conjugués) sont isomorphes. Or $\mathfrak{F}$ n'a qu'un nombre fini de sous-groupes d'indice fini donné, donc il n'existe qu'un nombre fini de revêtements $\beta^\sigma\colon X_0^\sigma \to \Sigma_0$ deux-à-deux non isomorphes.

La théorie des revêtements des surfaces de Riemann (cf. [3]) assure alors que d'une part les isomorphismes obtenus sont holomorphes, et d'autre part qu'ils se prolongent en des isomorphismes $X^\sigma \to X^\tau$. Ainsi, il n'y a qu'un nombre fini de X^σ deux à deux non isomorphes, et donc qu'un nombre fini de j^σ distincts (puisque $j(X^\sigma) = j^\sigma$). Ceci implique que j est algébrique, et donc que X peut être définie par des équations à coefficients algébriques. $\square$

4 Groupes de Galois

Si $\beta\colon X \to \Sigma$ est une fonction de Belyĭ, où X est une surface de Riemann compacte, alors la composition par β induit un morphisme $\beta^*\colon \bar{\mathbb{Q}}(t) \hookrightarrow \bar{\mathbb{Q}}(X)$, où $\bar{\mathbb{Q}}(X)$ désigne le corps des fonctions rationnelles sur X à coefficients dans $\bar{\mathbb{Q}}$ (des équations algébriques de X à coefficients dans $\bar{\mathbb{Q}}$ étant choisies). De plus ([3], [11]), si l'extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ est galoisienne (on dit que β est galoisien), le groupe de Galois de $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ est le groupe $\mathrm{Aut}(\beta)$ des automorphismes de β (automorphismes de X au-dessus de Σ) — et celui-ci est le quotient de $\pi_1(\Sigma_0)$ par un sous-groupe distingué d'indice $\deg \beta$, soit $\mathfrak{F}/H$ avec $\mathfrak{F}$ le groupe libre sur deux générateurs et H un sous-groupe distingué d'indice fini de $\mathfrak{F}$.

Si $\beta_1\colon X_1 \to \Sigma$ et $\beta_2\colon X_2 \to \Sigma$ sont deux fonctions de Belyĭ, il existe $\beta\colon X \to \Sigma$ une fonction de Belyĭ réalisant un revêtement galoisien, et se factorisant à la fois par β_1 et β_2 ; par conséquent, $\bar{\mathbb{Q}}(X_1)$ et $\bar{\mathbb{Q}}(X_2)$ se plongent tous deux dans le corps $\bar{\mathbb{Q}}(X)$. On peut donc considérer l'union (ou plus précisément la limite inductive, cf. [2]) des corps $\mathbb{Q}(X)$ avec $\beta\colon X \to \Sigma$ fonction de Belyĭ réalisant un revêtement galoisien. Soit $\mathbf{F}$ le groupe de Galois de $M/\bar{\mathbb{Q}}(t)$. On peut vérifier que $\mathbf{F}$ est la limite projective des $\mathfrak{F}/H$ avec H distingué d'indice fini dans $\mathfrak{F}$: cela signifie qu'un élément de $\mathbf{F}$ est une famille $(x_H)_H$ avec $x_H \in \mathfrak{F}/H$ pour tout H, vérifiant de plus $\varpi(x_H) = x_{H'}$ si $H \leq H'$, avec $\varpi\colon \mathfrak{F}/H \to \mathfrak{F}/H'$ la surjection canonique. On dit que $\mathbf{F}$ est le complété profini de $\mathfrak{F}$.

La tour de corps $\mathbb{Q}(t) \subseteq \bar{\mathbb{Q}}(t) \subseteq M$ donne lieu à la suite exacte de groupes de Galois

$$1 \to \mathbf{F} \to \mathrm{Gal}(M/\mathbb{Q}(t)) \to \mathbf{G} \to 1$$

où $\mathbf{G}$ est le groupe de Galois de $\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)$, autrement dit celui de $\bar{\mathbb{Q}}/\mathbb{Q}$. La conjugaison par un élément de $\mathbf{G}$ définit alors un morphisme $\mathbf{G} \to \mathrm{Aut}\mathbf{F}/\mathrm{Int}\mathbf{F}$. En fait, on peut dire plus : il est prouvé dans [1] que cette suite exacte se scinde, autrement dit que $\mathrm{Gal}(M/\mathbb{Q}(t))$ est un produit semi-direct de $\mathbf{F}$ par $\mathbf{G}$, et donc que l'on a un morphisme $\mathbf{G} \to \mathrm{Aut}\mathbf{F}$.

Théorème 4.1 ([1], [9]). *Cette action de* $\mathbf{G}$ *sur* $\mathbf{F}$ *est fidèle.*

Démonstration. Soit $\sigma \in \mathbf{G}$ différent de l'identité. Alors il existe $j \in \bar{\mathbb{Q}}$ tel que $j^\sigma \neq j$. Considérons la courbe elliptique X d'invariant j. D'après le théorème de Belyĭ, il existe une fonction de Belyĭ $\beta \colon X \to \Sigma$. Puisque les courbes elliptiques X et X^σ ne sont pas isomorphes (elles n'ont pas le même invariant), les revêtements β et β^σ ne le sont pas non plus, donc les sous-groupes de $\mathfrak{F}$ qui leur sont associés, disons H et H^σ, ne sont pas égaux dans $\mathfrak{F}$. Or H et H^σ sont d'indice fini, donc correspondent à des sous-groupes, également notés H et H^σ, de $\mathbf{F}$, qui ne sont toujours pas conjugués (vérification aisée). Mais l'action de σ sur $\mathbf{F}$ envoie H sur H^σ, donc n'est pas l'identité. □

On en déduit que $\mathbf{G}$ peut se voir comme un sous-groupe de $\mathrm{Aut}\mathbf{F}$. On peut alors chercher à caractériser plus précisément ce sous-groupe. Il est montré ([10]) qu'il est contenu dans le groupe dit “de Grothendieck-Teichmüller”. Par ailleurs, on peut utiliser des arguments similaires à ceux présentés ici pour étudier le problème de Galois inverse (à savoir celui de construire une extension galoisienne de $\mathbb{Q}$ ayant pour groupe de Galois un groupe fini donné).

Références

[1] G. V. Belyĭ, “О расширениях Галуа максимального кругового поля” (“On Galois extensions of a maximal cyclotomic field”), *Известия Академии Наук СССР* 43 (1979) 269–276 (en russe), *Math. USSR-Izvestija* 14 (1980) 247–256 (traduction anglaise).

[2] N. Bourbaki, *Théorie des ensembles*.

[3] P. Dolbeault, *Analyse complexe*, Maîtrise de mathématiques pures, Masson.

[4] R. Douady & A. Douady, *Algèbre et théories galoisiennes, tome 2*, Nathan.

[5] H. Farkas & I. Kra, *Riemann Surfaces, 2nd ed.*, Graduate Texts in Mathematics (71), Springer-Verlag.

[6] C. Godbillon, *Éléments de topologie algébrique*, Hermann.

[7] R. C. Gunning, *Lectures on Riemann Surfaces*, Princeton Mathematical Notes.

[8] Morris W. Hirsch, *Differential Topology*, Graduate Texts in Mathematics (33), Springer-Verlag.

[9] Gareth Jones & David Singerman, "Belyĭ functions, hypermaps and Galois groups", *Bulletin of the London Mathematical Society*, 28 (1996) 561–590.

[10] L. Schneps, *The Grothendieck Theory of Dessins d'Enfants*, London Mathematical Society Lecture Notes (200).

[11] Joseph Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics (106), Springer-Verlag.

Theta divisors and the Frobenius morphism

David A. Madore

Abstract

We introduce theta divisors for vector bundles and relate them to the ordinariness of curves in characteristic $p > 0$. We prove, following M. Raynaud, that the sheaf of locally exact differentials in characteristic $p > 0$ has a theta divisor, and that the generic curve in (any) genus $g \geq 2$ and (any) characteristic $p > 0$ has a cover that is not ordinary (and which we explicitely construct).

1 Theta divisors for vector bundles

Let k be an algebraically closed field and X a smooth proper connected curve over $\operatorname{Spec} k$ having genus g. We assume throughout that $g \geq 2$.

If E is a vector bundle (i.e. a locally free invertible sheaf) of rank r and degree d over X, we define its *slope* to be $\lambda = d/r$. The Riemann-Roch formula gives the Euler-Poincaré characteristic of E:

$$\chi(X, E) = h^0(X, E) - h^1(X, E) = r(\lambda - (g - 1))$$

In particular for $\lambda = g - 1$ (the *critical slope*) we have $\chi(X, E) = 0$; moreover, it is still true for any invertible sheaf L of degree 0 over X that $\chi(X, E \otimes L) = 0$, in other words, $h^0(X, E \otimes L) = h^1(X, E \otimes L)$. Under those circumstances, it is natural to ask the following question:

Question 1.1. *Suppose E has critical slope. Then for which invertible sheaves L of degree 0 (if any) is it true that $h^0(X, E \otimes L) = 0$ (and consequently also $h^1(X, E \otimes L) = 0$)? Is this true for some L, for many L, or for none?*

We start with a necessary condition. Suppose there were some subbundle $F \rightarrowtail E$ having slope $\lambda(F) > \lambda(E) = g - 1$. Then we would have

$\chi(X, F \otimes L) > 0$, hence $h^0(X, F \otimes L) > 0$. Now $H^0(X, F \otimes L) \rightarrowtail H^0(X, E \otimes L)$, so this implies $h^0(X, E \otimes L) > 0$. So if we are to have $h^0(X, E \otimes L) > 0$ for some L, this must not happen, and we say that E is *semi-stable*:

Definition 1.2. *A vector bundle E over X is said to be* stable *(resp.* semi-stable*) iff for every sub-vector-bundle F of E (other than 0 and E) we have $\lambda(F) < \lambda(E)$ (resp. $\lambda(F) \leq \lambda(E)$).*

Another remark we can make bearing some relation with question (1.1) is that, by the semicontinuity theorem, if we let L vary on the jacobian of X, the functions $h^0(X, E \otimes L)$ and $h^1(X, E \otimes L)$ are upper semicontinuous. This means that they increase on closed sets. In particular, if $h^0(X, E \otimes L) = 0$ (the smallest possible value) for some L, then this is true in a whole neighborhood of L, that is, for almost all L. We then say that this holds for a *general* invertible sheaf of degree 0 and we write $h^0(X, E \otimes L_{\text{gen}}) = 0$.

Now introduce the jacobian variety J of X and let $\mathscr{L}$ be the (some) Poincaré sheaf (universal invertible sheaf of degree 0) on $X \times_{\operatorname{Spec} k} J$. We aim to use $\mathscr{L}$ to let L vary and provide universal analogues for our formulæ. Let

$$\begin{array}{c} X \times_{\operatorname{Spec} k} J \\ \big\downarrow{\scriptstyle f} \\ J \end{array}$$

be the second projection.

Consider the sheaf $E \otimes \mathscr{L}$ (by this we mean the twist by $\mathscr{L}$ of the pullback of E to $X \times_{\operatorname{Spec} k} J$). Our interest is mainly in the higher direct image $Rf_*(E \otimes \mathscr{L})$, which incorporates information about $H^i(X, E \otimes L)$ (and much more).

To be precise, we know that there exists a complex $0 \to M^0 \xrightarrow{u} M^1 \to 0$ of vector bundles on J that universally computes the $R^i f_*(E \otimes \mathscr{L})$, in the sense that the i-th cohomology group ($i = 0, 1$) of the complex is $R^i f_*(E \otimes \mathscr{L})$ and that this remains true after any base change $J' \to J$. (One particularly important such base change, of course, is the embedding of a closed point $\{L\}$ in J.)

Now M^0 and M^1 have the same rank, say s (because the Euler-Poincaré characteristic of E is 0). So we can consider the determinant of u, $\bigwedge^s M^0 \xrightarrow{\det u} \bigwedge^s M^1$, or rather

$$\mathcal{O}_J \xrightarrow{\det u} \textstyle\bigwedge^s M^1 \otimes \left(\bigwedge^s M^0\right)^{\otimes -1}$$

Exactly one of the following two things happens:

- *Either* the determinant $\det u$ is zero (identically). In this case, u is nowhere (i.e. on no fiber) invertible, it always has a kernel and a cokernel: we have $h^0(X, E \otimes L) > 0$ (and of course $h^1(X, E \otimes L) > 0$) for all L.

- *Or* $\det u$ is a nonzero section of the invertible sheaf $\bigwedge^s M^1 \otimes \left(\bigwedge^s M^0\right)^{\otimes -1}$ on J and it defines a positive divisor θ_E on J, whose support is precisely the locus of L such that $h^0(X, E \otimes L) > 0$. We then have $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$.

In other words, precisely in the case where $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$ we can define a positive divisor θ_E on J which tells us "where the bundle E has cohomology". We call this divisor the *theta divisor* of the vector bundle E. And we will use the expression "to admit a theta divisor" as synonymous for $h^0(X, E \otimes L_{\mathrm{gen}}) = 0$. For example, a vector bundle that admits a theta divisor is semi-stable (but the converse is not true, cf. [1]).

2 Enters the Frobenius morphism

We now assume that the base field k has characteristic $p > 0$. We then have a relative Frobenius morphism

$$\begin{tikzcd} X \arrow[rr, "\pi"] \arrow[dr] & & X_1 \arrow[dl] \\ & \operatorname{Spec} k & \end{tikzcd}$$

which is obtained by factoring the absolute Frobenius morphism through the pullback to X of the Frobenius on k (more descriptively, π has the effect, in projective space, of raising the coordinates to the p-th power, while X_1 is the curve obtained by raising to the p-th powers the coefficients in the equations defining X).

The curve X_1 has the same genus g as X. The morphism π is flat, finite and purely inseparable of degree p. From it we deduce a morphism $\mathcal{O}_{X_1} \to \pi_* \mathcal{O}_X$ (of $\mathcal{O}_{X_1}$-modules), which is mono because π is surjective. Call B_1 the cokernel, so that we have the following short exact sequence:

$$0 \to \mathcal{O}_{X_1} \to \pi_* \mathcal{O}_X \to B_1 \to 0 \qquad (1)$$

Now the sheaf B_1 can be viewed in a different way: if we call d the differential $\mathcal{O}_X \to \Omega^1_X$ (between sheaves of $\mathbb{Z}$-modules) then $\pi_*(d)$ is $\mathcal{O}_{X_1}$-linear and has $\mathcal{O}_{X_1}$ as kernel. Consequently, B_1 can also be seen as the image of $\pi_*(d)$, hence its name of *sheaf of locally exact differentials*. As a subsheaf of the locally free sheaf $\pi_*\Omega^1_X$, it is itself a vector bundle.

In the short exact sequence (1) above, the vector bundles $\mathcal{O}_{X_1}$ and $\pi_*\mathcal{O}_X$ have rank 1 and p respectively, so that B_1 has rank $p-1$. On the other hand, since $\mathcal{O}_{X_1}$ and $\pi_*\mathcal{O}_X$ each have Euler-Poincaré characteristic $g-1$, we have $\chi(X_1, B_1) = 0$, or in other words, $\lambda(B_1) = g-1$ (the critical slope), and what we have said in the previous section applies to the sheaf B_1.

More precisely, we have the following long exact sequence in cohomology, derived from (1):

$$\begin{array}{ccccccccc} & & k & \xrightarrow{\sim} & k & & & & \\ & & \| & & \| & & & & \\ 0 & \to & H^0(X_1, \mathcal{O}_{X_1}) & \to & H^0(X, \mathcal{O}_X) & \to & H^0(X_1, B_1) & \to & \\ & \to & H^1(X_1, \mathcal{O}_{X_1}) & \to & H^1(X, \mathcal{O}_X) & \to & H^1(X_1, B_1) & \to & 0 \end{array}$$

Here the first arrow is an isomorphism as shown. Consequently, the arrow $H^1(X_1, \mathcal{O}_{X_1}) \to H^1(X, \mathcal{O}_X)$ is also an isomorphism if and only if $h^0(X_1, B_1) = 0$, or, what amounts to the same, $h^1(X_1, B_1) = 0$. This is again the same as saying that B_1 has a theta divisor (something which we will see is always true) and that it does not go through the origin.

Definition 2.1. *When the equivalent conditions mentioned in the previous paragraph are satisfied, we say that the curve X is* ordinary.

3 The sheaf of locally exact differentials has a theta divisor

In this section we prove the following result due to M. Raynaud ([1]):

Theorem 3.1. *If X is a smooth projective connected curve over an algebraically closed field k of characteristic $p > 0$ and B_1 is the sheaf of locally exact differentials on X_1, as introduced above, then we have $h^0(X_1, B_1 \otimes L_{\text{gen}}) = 0$, i.e. the vector bundle B_1 admits a theta divisor (in particular, it is semi-stable).*

Thus we can state the fact that a curve is ordinary simply by saying that the theta divisor of B_1 does not go through the origin.

To start with, introduce the jacobians J and J_1 of X and X_1 respectively. Then J_1 is the Frobenius image of J, and we have a relative Frobenius morphism $F\colon J \to J_1$ that is purely inseparable of degree p^g; it corresponds to taking the norm on invertible sheaves of degree 0 — or, if we prefer using points, it takes $\mathcal{O}_X(\Sigma n_i x_i)$ to $\mathcal{O}_{X_1}(\Sigma n_i \pi(x_i))$. On the other hand, we also have the *Verschiebung* morphism in the other direction $V\colon J_1 \to J$, which corresponds to pulling back by π — or again, it takes $\mathcal{O}_{X_1}(\Sigma n_i x_i)$ to $\mathcal{O}_X(\Sigma p n_i \pi^{-1}(x_i))$. The Verschiebung map also has degree p^g. The composite of the Verschiebung and Frobenius morphisms, in any direction, is the raising to the p-th power.

We will show something more precise than just saying that B_1 has a theta divisor: we will actually show that this theta divisor does not contain all of $\ker V$ in the neighborhood of 0. However, we will see from actual equations that it "almost" does.

If L_1 is an invertible sheaf of degree 0 on X_1 (that is, a k-point of J_1), the short exact sequence (1) becomes, after tensoring by L_1:

$$0 \to L_1 \to \pi_* \pi^* L_1 \to B_1 \otimes L_1 \to 0 \tag{2}$$

Now let $\mathscr{L}_1$ be the Poincaré bundle on $X_1 \times_{\operatorname{Spec} k} J_1$. The universal analogue of (2) above is

$$0 \to \mathscr{L}_1 \to (\pi \times 1_{J_1})_* (\pi \times 1_{J_1})^* \mathscr{L}_1 \to B_1 \otimes \mathscr{L}_1 \to 0$$

But by the definition of the Verschiebung, the sheaf $(\pi \times 1_{J_1})^* \mathscr{L}_1$ is also $(1_X \times V)^* \mathscr{L}$ so that the exact sequence can be written as

$$0 \to \mathscr{L}_1 \to (\pi \times 1_{J_1})_* (1_X \times V)^* \mathscr{L} \to B_1 \otimes \mathscr{L}_1 \to 0$$

We now introduce projections as designated on the following diagram:

$$\begin{tikzcd} X \times J \arrow[d, "f"'] & X \times J_1 \arrow[l, "1_X \times V"'] \arrow[r, "\pi \times 1_{J_1}"] \arrow[d, "g"'] \arrow[dl, phantom, "\square"] & X_1 \times J_1 \arrow[dl, "f_1"] \\ J & J_1 \arrow[l, "V"'] & \end{tikzcd} \tag{3}$$

Now we want to calculate the $R(f_1)_*$ of this. For one thing, looking at the diagram (3) above, we see that $R(f_1)_*(\pi \times 1_{J_1})_*(1_X \times V)^* \mathscr{L}$ is $Rg_*(1_X \times V)^* \mathscr{L}$, and by base change (note that the morphism V is flat), this is $V^*Rf_*\mathscr{L}$. Thus we have the following distinguished triangle, in the derived category of the category of sheaves on J_1:

$$\begin{tikzcd} & R(f_1)_*(B_1 \otimes \mathscr{L}_1) \arrow[dl, "+1"'] & \\ R(f_1)_*\mathscr{L}_1 \arrow[rr, "a"] & & V^*Rf_*\mathscr{L} \arrow[ul] \end{tikzcd} \tag{4}$$

And the corresponding long exact sequence of cohomology is

$$0 \to (f_1)_*(B_1 \otimes \mathscr{L}_1) \to R^1(f_1)_*\mathscr{L}_1 \overset{a}{\to} V^*R^1f_*\mathscr{L} \to R^1(f_1)_*(B_1 \otimes \mathscr{L}_1) \to 0$$

(the two first terms cancel). We want to show that a is generically invertible.

To start with, consider a minimal resolution of $Rf_*\mathscr{L}$ in the neighborhood of the origin. It has the form

$$\mathcal{O}_{J,0} \overset{u'}{\to} \mathcal{O}_{J,0}^g$$

where $u'(1) = (x_1, \ldots, x_g)$ is a system of parameters around 0. Indeed, this last statement is the same as saying, if u is the transpose of u', that the image of u is the maximal ideal of the regular local ring $\mathcal{O}_{J,0}$, and this is easy because $\{0\}$ is the largest closed subscheme of $\operatorname{Spec}\mathcal{O}_{J,0}$ on which $\mathscr{L}$ is trivial.

Now apply what we have just proven to J_1 on the one hand, and to J on the other, but pulling back by V, we find the following resolution for the arrow a in triangle (4):

$$\begin{tikzcd} R \arrow[r, "a_0"] \arrow[d, "u'"'] & R \arrow[d, "v'"] \\ R^g \arrow[r, "a_1"] & R^g \end{tikzcd} \tag{5}$$

where we have written $R = \mathcal{O}_{J_1,0}$, and where $u'(1) = (x_1, \ldots, x_g)$ is a system of parameters of J_1 around 0 and $v'(1) = (y_1, \ldots, y_g)$ is a regular sequence that gives an equation of $\ker V$ around 0. Now of course a_0 is just an element of R, and it is invertible because modulo the maximal ideal of R (that is, *at* the origin) the arrow a is just the identity on k. So we can assume that a_0 is the identity. What we want to prove is that $\det a_1$ is not zero (of course, it is invertible precisely when the curve is ordinary).

Consider the diagram (5) and its transpose (i.e. its image by the functor $\mathrm{Hom}_R(\cdot, R)$), and complete them both by adding the Koszul complex on either column. That is, consider the diagrams:

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
R \arrow[r, "1"] \arrow[d, "u'"'] & R \arrow[d, "v'"] \\
R^g \arrow[r, "a_1"] \arrow[d, dotted, no head] & R^g \arrow[d, dotted, no head] \\
\wedge^g R^g \arrow[r, "\det a_1"] \arrow[d] & \wedge^g R^g \arrow[d] \\
M' \arrow[r, "h'"] \arrow[d] & N' \arrow[d] \\
0 & 0
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
\wedge^g R^g \arrow[r, "\det a_1"] \arrow[d, dotted, no head] & \wedge^g R^g \arrow[d, dotted, no head] \\
R^g \arrow[r, "a_1^\vee"] \arrow[d, "v"'] & R^g \arrow[d, "u"] \\
R \arrow[r, "1"] \arrow[d] & R \arrow[d] \\
N \arrow[r, "h"] \arrow[d] & M \arrow[d] \\
0 & 0
\end{tikzcd}$$

in which we have written u, v and $a_1^\vee$ for the transposes of u', v' and a_1 respectively and M and N for the cokernels of u and v respectively. Since $u'(1)$ and $v'(1)$ are regular sequences, M and N are modules of finite length, and the Koszul complex is a resolution of them: the columns of both diagram are exact. We have $M' = \mathrm{Ext}^g_R(M, R)$ and $N' = \mathrm{Ext}^g_R(N, R)$ (since we have taken a resolution, transposed it, and shifted in g degrees). But since the Koszul complex is autodual (that is, the left column of the right diagram is the same as the right column of the left diagram, and *vice versa*), M and M' are the same and so are N and N'. Finally, it is known that (R being a regular local ring) the functor $\mathrm{Ext}^g_R(\cdot, R)$ is dualizing on modules of finite length. Now h is surjective as is seen on the diagram on the right, so that its image h' by the functor in question is injective. Hence $\det a_1$ is nonzero, what we wanted.

We can be more precise than this. As we have seen, M is isomorphic to k, and N to the local ring of $\ker V$ at 0: the support of θ_{B_1} swallows everything in $\ker V$ around the origin but just one k. (Incidentally, X is ordinary if and only if the support of θ_{B_1} does not contain the origin, so we recover the known fact that X is ordinary if and only if the local ring of $\ker V$ at the origin is k, i.e. V is étale.)

4 Constructing a non ordinary cover

We now present another result of M. Raynaud's ([2]), namely the fact that a finite étale cover of an ordinary curve is not necessarily ordinary, even when the base curve is generic. In fact, we obtain a cover $Y \twoheadrightarrow X$ such that the image of the map $J(X_1) \rightarrowtail J(Y_1)$ on the jacobians is completely contained in the support of the theta divisor of B_1 on Y_1 — and in particular 0 is, so that Y is not ordinary. The construction is sufficiently general to apply to the generic curve (for a given genus $g \geq 2$ and characteristic p). We also get estimations on the Galois group of Y over X; a theorem of Nakajima states that an abelian cover of the generic curve is ordinary, so we have to work with non abelian groups if we want a non ordinary cover — however, we will see that a nilpotent group can suffice.

We start with a few generalities on representations of the fundamental group of curves. We refer to [2] for details. If $\rho\colon \pi_1(X) \to GL(r,k)$ is a representation of the fundamental group of X in k-vector spaces of rank r, and ρ has open kernel (or, which amounts to the same, ρ is continuous and has finite image), then ρ defines a locally constant étale sheaf in k-vector spaces of rank r on X, written $\mathbb{V}_\rho$ (very succintly, $\mathbb{V}_\rho$ can be obtained as follows: find a Galois cover $Y \twoheadrightarrow X$ whose Galois group factors through the kernel of ρ, then make $\pi_1(X)/\ker\rho$ act on $Y \times k^r$ componentwise, and take the fixed points of that action). Tensoring $\mathbb{V}_\rho$ by $\mathcal{O}_X$ gives a Zarisky sheaf V_ρ which is locally free of rank r and has degree 0, i.e. a vector bundle of rank r and slope 0 on X. Among the functoriality properties of V_ρ cited in [2], we will need the fact that if $Y \overset{a}{\twoheadrightarrow} X$ is finite étale and ρ is a representation of $\pi_1(Y)$ as above then $a_* V_\rho$ is precisely $V_{\rho'}$, where ρ' is the representation of $\pi_1(X)$ induced by ρ.

We say that a representation ρ as above has a theta divisor (respectively, is ordinary) if and only if the sheaf $V_{1,\rho} \otimes B_1$ on X_1 has a theta divisor (respectively, has a theta divisor that does not go through the origin), $V_{1,\rho}$ being the bundle V_ρ as above constructed on X_1. Thus, we have seen that the trivial representation has a theta divisor, and it is ordinary precisely when the curve X is ordinary. The existence of a theta divisor for B shows that if L is a general invertible sheaf of finite order n prime to p then the representation ρ of rank 1 associated to it is ordinary.

Theorem 4.1. *Let k be an algebraically closed field of characteristic $p > 0$, and let X be the generic curve of any genus $g \geq 2$ over* $\operatorname{Spec} k$*. Then there exists a Galois cover of X with solvable Galois group of order prime to p that is not ordinary.*

Let X be as stated, and let J be its jacobian. If we choose a base point on X then we get a map $S^{g-1}X \to J$ from the $(g-1)$-th symmetric power of X, whose image defines a positive divisor on J, called the *classical theta divisor*, and written Θ. Let $N = \mathcal{O}_J(\Theta)$ be the invertible sheaf defined by Θ. We can assume that N is symmetric (i.e. that if $\iota\colon J \to J$ is the inverse map then $\iota^* N = N$) and we will do so.

Let n be a positive integer that is prime to p, and denote by α the multiplication by n map on J, which is étale of degree n^{2g}. Call A the kernel of α, the (étale) set of points of J whose order divides n. Because we have chosen N symmetric, we have $\alpha^* N = N^{\otimes n^2}$.

We recall (cf. [3]) that the kernel $H(N^{\otimes n})$ is the subgroup of closed x in J such that $T_x^* N^{\otimes n} \cong N^{\otimes n}$ (where T_x denotes translation by x). This kernel is obviously A. Now in [3], D. Mumford defines another, more interesting, group associated to an invertible sheaf on an abelian variety. In our case, it is the group

$$\mathscr{G}(N^{\otimes n}) = \{(x, \varphi) \mid \varphi\colon N^{\otimes n} \tilde{\to} T_x^* N^{\otimes n}\}$$

with multiplication defined in the obvious way. There is a short exact sequence

$$1 \to k^\times \to \mathscr{G}(N^{\otimes n}) \to H(N^{\otimes n}) \to 1$$

and in fact $k^\times$ is precisely the center of $\mathscr{G}(N^{\otimes n})$. The commutator of two elements of $\mathscr{G}(N^{\otimes n})$ is an element of $k^\times$ and it depends only on the class in $H(N^{\otimes n})$ of the two elements. Thus, the commutator defines a skew-symmetric biadditive form $\langle \cdot, \cdot \rangle\colon A \times A \to k^\times$. It is moreover shown in [3] that this form is non degenerate.

Let B a maximal totally isotropic subgroup of A for the form we have just defined. So B has order n^g, and $C = A/B$ has order n^g. We factor α as follows

$$
\begin{tikzcd}
J \arrow[dd, "\alpha"'] \arrow[dr, "\beta"] & \\
& J' = J/B \arrow[dl, "\gamma"] \\
J &
\end{tikzcd}
$$

where β has kernel B and γ has kernel (identified with) C.

Because B is isotropic, by a result in [3], the sheaf $N^{\otimes n}$ descends to an invertible sheaf M on J', i.e. a sheaf such that $N^{\otimes n} = \beta^* M$. And M is a principal polarization on J'. Now note that $\gamma^* N$ and $M^{\otimes n}$ have the same pullback (namely $N^{\otimes n^2}$) by β; if n is odd we can choose M to be symmetric, so that $\gamma^* N$ and $M^{\otimes n}$ coincide. We will now suppose this to be the case.

If L is an invertible sheaf on J that is algebraically equivalent to 0 (that is, a closed point of $J^\vee$) then we have $\gamma_*(M \otimes \gamma^* L) \cong (\gamma_* M) \otimes L$, so that $h^0(J', M \otimes \gamma^* L) = h^0(J, (\gamma_* M) \otimes L)$. Now the point is that $M \otimes \gamma^* L$ is a principal polarization on J, so this number is 1. In particular $h^0(J, (\gamma_* M) \otimes L) > 0$, and this implies that for any invertible sheaf L of degree 0 on X we have $h^0(X, F \otimes L) > 0$, where F is the restriction of $\gamma_* M$ to X. This is a good first step, but we need to twist F by an invertible sheaf having the right degree to compensate for the slope of F (since the sheaves V_ρ have slope zero).

We now calculate the slope of F. Its rank is n^g. Introduce the curves Y and Z that are inverse image of X by γ and α respectively, thus:

$$
\begin{tikzcd}
Z \arrow[dd, "\alpha"'] \arrow[dr, "\beta"] & \\
& Y \arrow[dl, "\gamma"] \\
X &
\end{tikzcd}
$$

The degree of N restricted to X is well-known: it is g. Pulling this back by α, we see that the degree of $N^{\otimes n^2}$ restricted to Z is gn^{2g}, and that of $N^{\otimes n}|Z$ is gn^{2g-1}. Descending to Y, we see that the degree of $M|Y$ is gn^{g-1}. So the slope of F is finally g/n.

Now assume that g divides n, i.e. that $g/n = d$, the slope of F, is an integer. The degree of $N|X$ is $g = nd$, so there exists an invertible sheaf P

of degree d on X such that $N|X = P^{\otimes n}$. Let $L' = (M|Y) \otimes \gamma^* P^{\otimes -1}$, which is an invertible sheaf of degree zero. Its inverse image $L'' = \beta^* L'$ is such that $L''^{\otimes n}$ is trivial on Z, so that the order of L'' divides n (in fact, it is exactly n, but we won't need this). If $E = \gamma_* L'$ then $E = F \otimes P^{\otimes -1}$, which is an invertible sheaf of degree 0 on X and satisfies $h^0(X, E \otimes L_{d,\mathrm{gen}}) > 0$ for a general invertible sheaf $L_{d,\mathrm{gen}}$ of degree d on X.

Now L'' is of order dividing n, so there is a cyclic covering of degree n $Z'' \twoheadrightarrow Z$ which trivializes it. It is Z'' that we will prove not to be ordinary (under certain numerical conditions at least). The invertible sheaf L' of degree 0 corresponds to an abelian representation of $\pi_1(Y)$ that factors trough $\pi_1(Z'')$, and when we induce that representation to $\pi_1(X)$ we see that $E = \gamma_* L'$ is of the form V_ρ for some representation ρ of $\pi_1(X)$ that factors through $\pi_1(Z'')$ (and which can actually be described: see [2]).

All these constructions were performed on X and J. They could equally well have been performed on X_1 and J_1. We now consider E as a sheaf of X_1. We have seen $h^0(X, E \otimes L_{d,\mathrm{gen}}) > 0$ and we wish to have $h^0(X, E \otimes B_1 \otimes L_{\mathrm{gen}}) > 0$. We are therefore done if we can show that B_1 contains an invertible subsheaf of degree d.

But A. Hirschowitz claims in [4] and proves in [5] that a general bundle of rank r_0 and slope λ_0 contains a subbundle of rank r' and slope λ' (the quotient having rank $r'' = r_0 - r'$ and slope λ'') if $\lambda'' - \lambda' \geq g - 1$. If we are looking for $r' = 1$ and $\lambda' = d$, with $r_0 = p - 1$ and $\lambda_0 = g - 1$ (the numerical values of B_1), so $r'' = p - 2$ and $\lambda'' = [(g-1)(p-1) - d]/(p-2)$, this condition is satisfied iff $(g - 1 - d)(p-1)/(p-2) \geq g - 1$, that is iff $d \leq \frac{g-1}{p-1}$. By deforming and specializing to B_1, we see that if this inequality is satisfied then B_1 contains an invertible sheaf of degree d.

Finally, we have shown that if p and g are such that there exists a positive odd integer n, prime to p, dividing g, and satisfying $\frac{g}{n} \leq \frac{g-1}{p-1}$ then the generic curve X of genus g in characteristic p has a covering that is not ordinary. This is not always the case, but we can always reduce to that case by first taking a cyclic cover X' of degree m prime to p of X (X' then has genus $g' = 1 + m(g-1)$), and apply the result to X'. Here are the details:

- If p is odd, take m even, not multiple of p and large enough so that $g' = 1 + m(g-1) \geq p$.
  - If p does not divide g', then $n = g'$ works (it is odd because m is even, it is prime to p, and $\frac{g'}{n} = 1 \leq \frac{g'-1}{p-1}$ because $g' \geq p$).

  - If p does divide g' then we double m and this is no longer the case, so we are reduced to the previous point.

- If $p = 2$, write $g = 2^r s$ with s odd.
  - If $s \geq 3$, take $m = 1$, $n = s$. (Then n is odd, and $\frac{g}{n} = 2^r \leq g - 1$.)
  - If $s = 1$ then $g = 2^r$.
    - If $r \geq 2$, take $m = 3$, $n = g'/2 = 3 \times 2^{r-1} - 1$. (Then n is odd, and $\frac{g'}{n} = 2 \leq g' - 1$.)
    - If $r = 1$ so $g = 2$ and we take $m = 5$, $g' = 6$, $n = 3$.

Finally, we note that our final covering was constructed as a composite $Z'' \twoheadrightarrow Y \twoheadrightarrow X' \twoheadrightarrow X$ of coverings all of which are abelian: it is therefore solvable.

References

[1] M. Raynaud, "Sections des fibrés vectoriels sur une courbe", *Bull. Soc. math. France*, **110** (1982), p. 103–125.

[2] M. Raynaud, "Revêtements des courbes en caractéristique $p > 0$ et ordinarité", forthcoming.

[3] D. Mumford, "On the Equations Defining Abelian Varieties, I", *Inventiones mathematicæ*, **1** (1966), p. 287–354.

[4] A. Hirschowitz, "Problèmes de Brill-Noether en rang supérieur", *C. R. Acad. Sci*, **307** (1988), p. 153–156.

[5] A. Hirschowitz, "Problèmes de Brill-Noether en rang supérieur", `http://math.unice.fr/~ah/Brill/`, on the World Wide Web.

David Madore
c/o École Normale Supérieure de Paris
45 rue d'Ulm
75 230 PARIS CEDEX 05
FRANCE
david.madore@ens.fr