Fonctions zêta de courbes projectives sur un corps fini et cohomologie Weil-étale

Nicolas Mascot

Mémoire de Master 2
sous la direction de

Boas Erez

École Normale Supérieure

Septembre 2010

Table des matières

Introduction

Le premier objet de ce mémoire est l'étude arithmétique des courbes algébriques planes sur un corps fini. À une telle courbe est associée une *fonction zêta*, qui encode des informations sur son arithmétique, et qui, à l'instar d'autres fonctions zêta, vérifie des propriétés telles qu'une équation fonctionnelle ou une "hypothèse de Riemann". Le fait est que, contrairement au cas des fonctions zêta de Dedekind relatives aux corps de nombres, on sait démontrer l'hypothèse de Riemann pour les fonctions zêta de courbes sur les corps finis ; ceci a de nombreuses conséquences arithmétiques, par exemple, elle permet une démonstration immédiate du théorème de Hasse pour les courbes elliptiques. Signalons qu'il est possible d'attacher une fonction zêta à une variété de dimension quelconque sur un corps fini, toutefois, par souci de simplicité, nous n'étudierons sérieusement que le cas des courbes. Notons que ceci ne nous éloigne nullement des fonctions zêta de Dedekind, puisque l'anneaux des entiers d'un corps de nombre est lui aussi de dimension un.

Afin de mieux comprendre les fonctions zêta de Dedekind en vue de l'hypothèse de Riemann, il semble profitable d'étudier davantage les fonctions zêta de variétés sur les corps finis, en raison de l'analogie qu'elles présentent avec elles. À cette fin, J.S. Milne a établi dans [Mil80] une formule reliant la valeur en zéro de la fonction zêta d'une variété sur un corps fini à une sorte de caractéristique d'Euler des espaces de cohomologie étale de ladite variété. Toutefois, cette formule ne s'applique qu'aux variétés projectives non singulières, et est de surcroît fort peu naturelle. Ces inconvénients expliquent l'intérêt des travaux de Stephen Lichtenbaum, publiés dans [Lic05], qui, grâce à l'introduction d'une *cohomologie Weil-étale*, version légèrement modifiée de la cohomologie étale, réussissent à aboutir à une formule plus naturelle, et surtout à s'affranchir du cadre projectif non singulier, et même à se généraliser au cas des schémas de type fini sur $\mathrm{Spec}(\mathbb{Z})$ tels que les anneaux d'entiers de corps de nombres, comme [Lic09] le laisse entrevoir. Aussi, après avoir présenté la cohomologie Weil-étale dans le cadre des variétés sur les corps finis, qui constitue le deuxième objet de ce mémoire, en évoquerons-nous quelques applications récentes et prometteuses.

Remerciements

Je tiens à remercier chaleureusement mon encadrant Boas Erez de m'avoir énormément soutenu et de s'être montré si disponible, et aussi de m'avoir donné goût à la géométrie arithmétique et de m'avoir initié au monde de la recherche. Je remercie également Qizheng Yin de m'avoir poussé à faire un peu de géométrie.

1 Le théorème de Riemann-Roch

L'objectif de cette première partie est l'établissement du théorème de Riemann-Roch pour les courbes projectives. Ce théorème est extrêmement performant, et nous nous en rendrons bien compte lorsque nous l'utiliserons à de multiples reprises dans la partie suivante. Nous profitons également de cette première partie pour introduire les objets géométriques sur lesquels nous travaillerons, en essayant de combiner la simplicité de [Lor96] à la puissance de [Har77].

1.1 Courbes

Les objets qui nous intéresseront par la suite, et auxquels nous appliquerons les outils liés à la cohomologie des faisceaux que nous aurons entretemps introduits, sont les *courbes*.

Fixons un corps de base k, ainsi qu'une clôture algébrique $\bar{k}$ de celui-ci. Une *courbe affine plane sur k* est le lieu Z_f des zéros d'un polynôme $f \in k[x,y]$ dans $\bar{k}^2$. On lui associe son *anneau des fonctions régulières* $C_f = k[x,y]/(f)$, qui est donc un anneau noethérien de dimension 1. À une telle courbe correspond un k-schéma affine, encore noté Z_f,

$$Z_f = \mathrm{Spec}(C_f).$$

Nous nous intéresserons plus particulièrement au cas où la courbe est *irréductible*, c'est-à-dire qu'elle n'est pas union d'autres courbes strictement incluses dans elle ; il revient au même d'exiger que f soit irréductible dans $k[x,y]$. L'anneau C_f est alors intègre, et on appelle *corps des fonctions rationnelles* son corps des fractions $k(Z_f) = \mathrm{Frac}(C_f)$.

À un point $P = (a,b) \in \bar{k}^2$ de Z_f correspond un point fermé de Z_f, c'est-à-dire un idéal premier non nul $\mathfrak{p}_P$ de C_f. On lui associe l'extension finie $k(P) = k(a,b) \simeq C_f/\mathfrak{p}_P$ de k, qui est définie comme étant l'extension engendrée par les coordonnées de P sur k.

La courbe Z_f sera dite *non singulière* si f et son gradient ne s'annulent jamais simultanément sur $\bar{k}^2$. Z_f est non singulière si et seulement si l'anneau C_f est intégralement clos, c'est donc alors un anneau de Dedekind. Il est équivalent de dire que les localisés $(C_f)_\mathfrak{p}$ de C_f en les points fermés $\mathfrak{p} \in Z_f \backslash \{0\}$ sont principaux, ce sont donc alors des anneaux de valuation discrète. On note $v_\mathfrak{p}$ la valuation normalisée associée ; c'est une valuation sur $k(Z_f)$,

triviale sur k. Si le corps de base k est fini, et il le sera dans les cas qui nous intéresseront, alors les quotients $C_f/\mathfrak{p}$, $\mathfrak{p} \in Z_f \setminus \{0\}$, sont finis ; on dit alors que C_f est *à quotients finis*, et on note

$$\|\mathfrak{p}\| = |C_f/\mathfrak{p}|$$

les cardinaux de ces quotients.

Les courbes affines sont des objets simples, mais il leur manque quelque chose : les fameux *points à l'infini*. Par exemple, le théorème de Riemann-Roch, auquel cette première partie est consacrée, s'énonce bien plus naturellement dans le cas des courbes *projectives*, que nous allons à présent introduire.

On ne présente plus le plan projectif $\mathbb{P}^2_k$ sur le corps k. Nous noterons $[c_0, c_1, c_2]$ les systèmes de coordonnées projectives. Un polynôme homogène $F \in k[x_0, x_1, x_2]$ définit une courbe projective plane X_F, représentée par le schéma $X_F = \mathrm{Proj}\left(k[x_0, x_1, x_2]/(F)\right)$.

La droite $x_2 = 0$ est la droite à l'infini, et les points de X_F sur cette droite sont ses points à l'infini. En divisant F par $x_2^{\deg F}$, on obtient un polynôme $f \in k\left[\frac{x_0}{x_2}, \frac{x_1}{x_2}\right]$, définissant une courbe affine plane Z_f qui est isomorphe à X_F privée de ses points à l'infini. Réciproquement, étant donnée une courbe affine plane Z_f d'équation $f \in k[x, y]$, on peut homogénéiser f en un polynôme homogène $F \in k[x_0, x_1, x_2]$, ce qui ajoute d'éventuels points à l'infini à Z_f.

Comme pour les courbes affines, nous ne nous intéresserons qu'aux courbes projectives *irréductibles*, c'est-à-dire que nous supposerons F irréductible. On dispose alors du corps des fractions rationnelles $k(X_F)$, qui est la tige du faisceau structural de X_F au point générique.

Comme dans le cas affine, à chaque point $P = [c_0, c_1, c_2] \in \mathbb{P}^2_{\bar{k}}$ de X_F correspond un point fermé $\mathfrak{p}_P \in X_F \setminus \{0\}$, et une extension finie $k(P)$ de k, définie par $k(P) = k(c_0/c_2, c_1/c_2)$ si par exemple $c_2 \neq 0$.

Toujours comme dans le cas affine, la courbe X_F est dite *non singulière* si F et son gradient ne s'annulent jamais simultanément sur $\mathbb{P}^2_{\bar{k}}$. Les anneaux locaux $\mathcal{O}_{X_F,\mathfrak{p}}$, $\mathfrak{p} \in X_F \setminus \{0\}$, sont alors des anneaux de valuation discrète, d'où des valuations normalisées $v_\mathfrak{p}$ sur $k(X_F)$, triviales sur k.

Dans le cas affine comme dans le cas projectif, on peut, en remplaçant le corps de base k par une extension k' d'icelui, définir de nouvelles courbes ; on dit qu'on a procédé à une *extension des scalaires*. L'ennui est que les

courbes ainsi obtenues ne sont pas forcément irréductibles, même si celle de départ l'était. On dit qu'une courbe est *géométriquement irréductible* si elle est irréductible et le reste par toute extension de scalaires. Il revient au même de dire que son équation est *absolument irréductible*, c'est-à-dire qu'elle irréductible non seulement en tant que polynôme à coefficients dans k, mais aussi en tant que polynôme à coefficients dans une clôture algébrique de k. On démontre que ceci est encore équivalent à ce que le corps de base k soit algébriquement clos dans le corps des fonctions de la courbe.

Exemple 1.1.1. Choisissons $k = \mathbb{Q}$ comme corps de base, et considérons la courbe affine Z_f définie par l'équation

$$f(x, y) = x^2 + y^2 - xy - x - y + 1 \in \mathbb{Q}[x, y].$$

En réduisant modulo y, c'est-à-dire en évaluant en $y = 0$, on vérifie facilement que f est irréductible sur $\mathbb{Q}$. Mais on a

$$f(x, y) = (x - 1)^2 - (x - 1)(y - 1) + (y - 1)^2,$$

donc après extension quadratique des scalaires, Z_f devient le réunion de deux droites, donc n'est plus irréductible. La fonction $\alpha = \frac{x-1}{y-1} \in \mathbb{Q}(Z_f)$ vérifie $\alpha^2 - \alpha + 1 = 0$, donc $\mathbb{Q}(Z_f)$ contient l'extension algébrique $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(j)$, où $j = e^{\frac{2i\pi}{3}} \in \mathbb{C}$ est une racine cubique non-triviale de l'unité, et f se factorise sur $\mathbb{Q}(j)$ en $f(x, y) = (x + jy + j^2)(x + j^2y + j) \in \mathbb{Q}(j)[x, y]$.

À chaque point d'une courbe (affine ou projective) plane non singulière, on a fait correspondre une valuation discrète normalisée sur le corps des fonctions rationnelles, triviale sur le corps de base k. Nous allons à présent pousser cette idée plus loin, en introduisant un nouveau type de courbes, dont les points sont des valuations.

Afin de poursuivre, nous aurons besoin de quelques préliminaires algébriques à propos des extensions finies d'un corps de fractions rationnelles en une indéterminée.

Pour commencer, on a le résultat de finitude suivant :

Lemme 1.1.2. *Soit k un corps, et soient K une extensions finie du corps des fractions rationnelles en une indéterminée $k(x)$ sur k. Pour tout $\alpha \in K$ transcendant sur k, l'extension $K/k(\alpha)$ est finie.*

Démonstration. Comme K est finie sur $k(x)$, $k(x,\alpha) \subseteq K$ est aussi finie sur $k(x)$. Soit donc $f \in k(x)[Y]$ le polynôme minimal de α sur $k(x)$, de sorte que $f(x,\alpha) = 0$. Comme α est transcendant sur k, $f \notin k[Y]$, donc $k(x,\alpha)$ est finie sur $k(\alpha)$. Par conséquent, K, qui est finie sur $k(x)$ donc *a fortiori* sur $k(x,\alpha)$, est finie sur $k(\alpha)$. □

La proposition suivante nous assure que certaines clôtures intégrales sont noethériennes :

Proposition 1.1.3. *Soit k un corps quelconque. Soit $k(x)$ le corps des fractions rationnelles en une indéterminée sur k, et soit K une extension finie de $k(x)$. La clôture intégrale de $k[x]$ dans K est un $k[x]$-module de type fini.*

Démonstration. Notons B la clôture intégrale de $k[x]$ dans K. Toute la difficulté réside dans le fait que K n'est pas forcément séparable sur $k(x)$; en effet, dans le cas séparable, ce résultat est bien connu et se démontre facilement grâce à la forme trace. On peut donc supposer qu'on est en caractéristique $p > 0$.

Supposons pour commencer que $K = k\big(x\big)\big(f_1^{1/p^{n_1}}, \cdots, f_s^{1/p^{n_s}}\big)$ est une extension purement inséparable de $k(x)$. Soit $n = \max n_i$, appelons k' le corps engendré sur k par les racines p^n-ièmes des coefficients des fractions rationnelles $f_1, \cdots, f_s$, et posons $K' = k'\big(x^{1/p^n}\big)$. Il est clair que $K \subseteq K'$. Soit B' la clôture intégrale de $k[x]$ dans K'. On a $B \subseteq B'$, donc, puisque $k[x]$ est principal donc noethérien, il suffit, pour montrer que B est un $k[x]$-module de type fini, de montrer que c'est le cas de B'. Or il est clair que $k'[x]$ est la clôture intégrale de $k[x]$ dans $k'(x)$, et que c'est un $k[x]$-module de type fini. Il est aussi clair que $k'\big[x^{1/p^n}\big]$ est la clôture intégrale de $k'[x]$ dans $K' = k'\big(x^{1/p^n}\big)$, et que c'est un $k'[x]$-module de type fini. Ainsi, $B' = k'\big[x^{1/p^n}\big]$ est bien un $k[x]$-module de type fini.

Revenons à présent au cas général. Soit N la clôture normale de K, et notons D la clôture intégrale de $k[x]$ dans N. On a $B \subseteq D$, donc, pour conclure, il suffit encore de montrer que D est un $k[x]$-module de type fini. Soit M la sous-extension purement inséparable maximale de $k(x)$ dans N, et soit C la clôture intégrale de $k[x]$ dans N. Il résulte du cas précédent que C est un $k[x]$-module de type fini. Mais comme l'extension N/M est séparable, D est un C-module de type fini. □

Nous aurons également besoin d'un théorème de l'élément primitif. Le lemme suivant nous permettra de surmonter les ennuis rencontrés en caractéristique positive :

Lemme 1.1.4. *Soit k un corps parfait de caractéristique $p > 0$. Donnons-nous une extension finie K du corps des fractions rationnelles $k(x)$ sur k, et soit L une extension finie purement inséparable de K, de degré p^n. Alors $K = L^{p^n}$, et en particulier, $L = K^{1/p^n}$.*

Démonstration. Étant donné un corps F de caractéristique p, nous noterons $\Phi_F : x \mapsto x^p$ son *morphisme de Frobenius*.

L'extension purement inséparable L s'obtient en ajoutant à K les racines p^{m_i}-ièmes d'un nombre fini d'éléments q_i de K. Soit $m = \max m_i$. Comme $[L : K] = p^n$, on a $m \leqslant n$. Les morphismes de Frobenius itérés définissent une tour d'isomorphismes de corps

$$\begin{array}{ccc} L & \xrightarrow{\Phi_L^m} & L^{p^m} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\Phi_K^m} & K^{p^m} \\ \uparrow & & \uparrow \\ k(x) & \xrightarrow{\Phi_{k(x)}^m} & k(x)^{p^m} \end{array}$$

et donc $[L^{p^m} : k(x)^{p^m}] = [L : k(x)]$, si bien que

$$[L : L^{p^m}] = [k(x) : k(x)^{p^m}] = [k(x) : k(x^{p^m})] = p^m$$

puisque k est parfait. Mais comme $[L : K] \leqslant [L : L^{p^m}] = p^n$, on a nécessairement $m = n$ et donc $K = L^{p^m}$. □

Lemme 1.1.5. *Soit K un corps, et soit L une extension finie de K. Le nombre d'extensions intermédiaires $K \subseteq E \subseteq L$ est fini si et seulement si L est une extension monogène de K, c'est-à-dire s'il existe un élément $y \in L$ tel que $L = K(y)$.*

Démonstration. Commençons par le sens direct.

Si K est fini, alors L aussi, donc L^* est cyclique et le résultat est évident. On peut donc supposer K infini.

Soient α et β deux éléments de L. Par hypothèse, lorsque λ décrit K, l'ensemble des $K(\alpha + \lambda\beta)$ est fini. Comme K est infini, il existe deux valeurs

distinctes $\lambda_1 \neq \lambda_2$ de λ telles que $K(\alpha + \lambda_1\beta) = K(\alpha + \lambda_2\beta) = E$. Alors $\alpha + \lambda_1\beta \in E$ et $\alpha + \lambda_2\beta \in E$, donc $(\lambda_2 - \lambda_1)\beta \in E$, donc $\beta \in E$, donc $\alpha \in E$ aussi. Comme L est finie sur K, on a $L = K(\alpha_1, \cdots, \alpha_s)$, et la méthode précédente permet de récurrer sur s pour aboutir à un élément primitif.

Réciproquement, supposons $L = K(y)$ monogène. Notons $\mu \in K[x]$ le polynôme minimal unitaire de y sur K, et, pour chaque extension intermédiaire $K \subseteq E \subseteq L$, notons $\mu_E \in E[x]$ le polynôme minimal unitaire de y sur E. Alors les μ_E divisent μ dans l'anneau factoriel $L[x]$, donc sont en nombre fini. Par ailleurs, si E' désigne le corps engendré sur K par les coefficients de μ_E, alors $E' \subseteq E$, mais μ_E est irréductible sur E' donc $[L : E] = \deg(\mu_E) = [L : E']$, donc $E = E'$; ainsi, μ_E détermine E, d'où le résultat. □

Théorème 1.1.6 (Théorème de l'élément primitif pour les extensions de degré de transcendance 1)**.** *Soit k un corps parfait, et soit K une extension finie du corps des fractions rationnelles $k(x)$ sur k. Il existe un élément $y \in K$ tel que $K = k(x)(y)$.*

Démonstration. On peut supposer qu'on est en caractéristique $p > 0$. Si un tel y n'existait pas, alors d'après le lemme 1.1.5 précédent, il existerait une famille infinie $(E_n)_{n\in\mathbb{N}}$ d'extensions intermédiaires $k(x) \subseteq E_n \subseteq K$ distinctes deux-à-deux. Notons K^s la sous-extension séparable sur $k(x)$ maximale de K, et E_n^s les sous-extensions séparables sur $k(x)$ maximales de E_n. L'extension K^s est alors séparable donc monogène sur $k(x)$, et les E_n^s en sont des extensions intermédiaires ; d'après le même lemme 1.1.5, elles sont donc en nombre fini, donc il existe un $n_0 \in \mathbb{N}$ et une partie infinie $I \subseteq \mathbb{N}$ telle que pour tout $i \in I$, $E_i \cap K^s = E_{n_0}^s$. Comme les degrés $[E_i : E_{n_0}^s]$ sont bornés par $[K : E_{n_0}^s]$, il existe deux indices distincts $i_1 \neq i_2$ tels que E_{i_1} et E_{i_2} soient de même degré d sur $E_{n_0}^s$. Or les E_i sont des extensions purement inséparables de $E_{n_0}^s$, donc le lemme 1.1.4 nous dit que $E_{i_1} = (E_{n_0}^s)^{1/d} = E_{i_2}$, ce qui est absurde puisque les E_n sont censées être toutes distinctes. □

Corollaire 1.1.7. *Soit k un corps parfait, et soit K une extension finie non-séparable du corps des fractions rationnelles $k(x)$ sur k. Il existe un élément $y \in K$, transcendant sur k, tel que $K = k(x)(y)$ et que K soit séparable sur $k(y)$.*

Démonstration. L'existence d'un $y \in K$ tel que $K = k(x)(y)$ est assurée par le théorème 1.1.6. On peut supposer sans perte de généralité que y est entier

sur $k[x]$. Soit donc $f(x,Y) \in k[x,Y]$ son polynôme minimal. Le polynôme $f(X,Y) \in k[X,Y]$ est irréductible et unitaire en Y. L'existence de f fait que $K = k(x,y)$ est algébrique sur $k(y)$; par conséquent, y ne saurait être algébrique sur k, car sinon K le serait aussi, donc $k(x)$ serait algébrique, ce qui est bien entendu absurde.

Comme K n'est pas séparable sur $k(x)$, il existe un $g \in k[X,Y]$ tel que $f(X,Y) = g(X,Y^p)$, où p désigne bien sûr la caractéristique ambiante. Si K n'était pas non plus séparable sur $k(y)$, alors il existerait un $h \in k[X,Y]$ tel que $f(X,Y) = h(X^p,Y^p)$, mais la perfection de k entraînerait que f est une puissance p-ième dans $k[X,Y]$, ce qui contredirait son irréductibilité. □

Nous pouvons alors enfin présenter le nouveau type de courbes annoncé.

Définition 1.1.8. Soit k un corps. Un *corps de fonctions* sur k est une extension K finie du corps $k(x)$ des fractions rationnelles en une indéterminée sur k, dans laquelle k est algébriquement clos.

Définition 1.1.9. Soit k un corps. Une *courbe non singulière complète* sur k est l'ensemble X des valuations discrètes normalisées d'un corps de fonctions K sur k. On pose alors $k(X) = K$, et on munit X d'une structure d'espace localement annelé comme suit :

- On munit X de la topologie des cofinis, et
- le faisceau structurel $\mathcal{O}_X$ est défini en calquant l'idée du faisceau structurel d'une courbe, c'est-à-dire en disant que $\mathcal{O}_X(U)$ est l'anneau des fonctions définies partout sur l'ouvert U. Concrètement, pour toute $v \in X$, on note
$$\mathcal{O}_v = \{\alpha \in K \mid v(\alpha) \geqslant 0\}$$
l'anneau de valuation discrète correspondant, et on pose $\mathcal{O}_\xi = K$; on définit alors, pour tout ouvert U,
$$\mathcal{O}_X(U) = \bigcap_{v \in U} \mathcal{O}_v.$$

Les éléments de $k(X)$ s'appellent les *fonctions rationnelles* sur X.

On souhaitera souvent parler de points plutôt que de valuations. Dans ce cas, on notera $\mathcal{O}_P$ l'anneau de valuation discrète, $\mathfrak{p}_P$ son idéal maximal, $k(P) = \mathcal{O}_P/\mathfrak{p}_P$ son corps résiduel, et v_P la valuation discrète normalisée associés à un point P de X. Si k' est une extension du corps de base k, on

dira que P est un point k'-*rationnel* si k' contient un sous-corps k-isomorphe à $k(P)$. L'ensemble des points k'-rationnels de X sera noté $X(k')$.

Si $\alpha \in k(X)$ est une fonction rationnelle sur X, son *domaine* est l'ensemble des points P tels que $v_P(\alpha) \geqslant 0$. Les points hors du domaine de α sont les *pôles* de α, et P est un *zéro* de α si $v_P(\alpha) > 0$. Dans chaque cas, l'ordre du zéro ou du pôle est $|v_P(\alpha)|$.

Théorème 1.1.10. *Soit X une courbe non singulière complète sur k, et soit $\alpha \in k(X)$ une fonction transcendante sur k, de sorte que $k(X)$ soit une extension finie de $k(\alpha)$. Le domaine U de α est ouvert, c'est-à-dire cofini, et $\mathcal{O}_X(U)$ est égal à la clôture intégrale de $k[\alpha]$ dans $k(X)$.*

Démonstration. Notons B la clôture intégrale de $k[\alpha)$ dans $k(X)$. Pour tout $P \in U$, on a par définition $\alpha \in \mathcal{O}_P$, donc $k[\alpha] \subseteq \mathcal{O}_P$, et même $B \subseteq \mathcal{O}_P$ puisque $\mathcal{O}_P$ est intégralement clos. Ainsi $B \subseteq \mathcal{O}_X(U)$. Réciproquement, la proposition 1.1.3 nous assure que B est un anneau de Dedekind ; on a donc une bijection entre les valuations discrètes normalisées positives sur B et ses idéaux maximaux, donc $\mathcal{O}_X(U) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(B)} B_{\mathfrak{p}} = B$. Et U est bien ouvert puisque, par un raisonnement similaire, les points de son complémentaire correspondent aux idéaux maximaux au-dessus de $(1/\alpha)$ de la clôture intégrale de $k[1/\alpha]$ dans $k(X)$, donc sont en nombre fini. □

Notons qu'on a démontré au passage que $X \sqcup \{\eta\}$, où η est un point dense (le point générique, qui correspond à la valuation triviale sur $k(X)$), pouvait être recouvert par les deux schémas affines $\mathrm{Spec}(B)$ et $\mathrm{Spec}(B')$, où B' désigne la clôture intégrale de $k[1/\alpha]$ dans $k(X)$. On peut donc voir X comme un k-schéma de dimension 1.

Exemple 1.1.11. Soit $K = k(x)$ le corps des fractions rationnelles sur k. La courbe non singulière complète sur k associée n'est autre que la droite projective $\mathbb{P}^1_k$, et le schéma associé est isomorphe au schéma $\mathbb{P}^1_k = \mathrm{Proj}\left(k[x_0, x_1]\right)$.

En effet, les valuations discrètes normalisées sur $k(x)$ qui sont triviales sur k sont les ord_f, où f parcourt l'ensemble des polynômes irréductibles unitaires de $k[x]$, plus la valuation à l'infini, définie par $v_\infty = -\deg$. On retrouve bien les points fermés du schéma $\mathbb{P}^1_k$, et cette identification est clairement compatible avec les faisceaux structurels.

Dans le cas des courbes projectives, les seules fonctions définies partout sont les constantes. Le fait qu'on ait exigé que k soit algébriquement clos dans un corps de fonctions sur k est donc justifié par la proposition suivante :

Proposition 1.1.12. *Soit k un corps, et soit K une extension finie du corps des fractions rationnelles en une indéterminée sur k. Notons k' la clôture algébrique de k dans K. Si $V(K/k)$ désigne l'ensemble des valuations discrètes normalisées sur K qui sont triviales sur k, alors on a, en notant comme d'habitude $\mathcal{O}_v \subset K$ l'anneau d'une valuation $v \in V(K/k)$,*

$$\bigcap_{v \in V(K/k)} \mathcal{O}_v = k'.$$

Démonstration. Si une valuation est triviale sur k, alors elle le reste sur tout extension algébrique de k, donc $k' \subseteq \bigcap_{v \in V(K/k)} \mathcal{O}_v$. Réciproquement, soit $\alpha \in \bigcap_{v \in V(K/k)} \mathcal{O}_v$, et supposons que $\alpha \notin k'$. Soit B la clôture intégrale de $k[1/\alpha]$ dans K. B est intégralement clos et de dimension 1, et est noethérien d'après la proposition 1.1.3 : c'est donc un anneau de Dedekind. Par conséquent, l'idéal $(1/\alpha)k[1/\alpha]$ se factorise dans B en $(1/\alpha)B = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$. Mais alors $v_{\mathfrak{p}_1}(\alpha) = -v_{\mathfrak{p}_1}(1/\alpha) < 0$, ce qui contredit le fait que $\alpha \in \mathcal{O}_{v_{\mathfrak{p}_1}}$. □

À présent que nous avons défini les objets, passons aux morphismes :

Définition 1.1.13. Soient X et Y deux courbes non singulières complètes sur un corps k. Un morphisme $\varphi : X \longrightarrow Y$ est un morphisme de k-algèbres $\varphi^* : k(Y) \longrightarrow k(X)$; il envoie le point $P \in X$ sur le point $\varphi(P) \in Y$ tel que $v_{\varphi(P)}$ est la valuation normalisée attachée à $v_P \circ \varphi$.

φ^* sera souvent injectif, auquel cas on verra $k(Y)$ comme un sous-corps de $k(X)$. Le degré $[k(X) : k(Y)]$ s'appelle alors le *degré* de φ, et est noté $\deg(\varphi)$. Il est toujours fini d'après le lemme 1.1.2. φ est dit *séparable* si $k(X)$ est séparable sur $k(Y)$.

Supposons φ séparable. Soit $P \in X$ un point de X. Notons B la clôture intégrale de $\mathcal{O}_{\varphi P}$ dans $k(X)$. B n'a qu'un nombre fini d'idéaux premiers, correspondant aux antécédents de $\varphi(P)$. En particulier, $\mathcal{O}_P$ est un localisé de B. On a donc $\mathfrak{p}_{\varphi(P)}\mathcal{O}_P = \mathfrak{p}_P^{e_P}$ pour un certain entier $e_P \in \mathbb{N}^*$, qu'on appelle l'*indice de ramification* de φ en P. Le point P (ou $\varphi(P)$) est dit *non-ramifié* si $e_P = 1$ et si l'extension de corps résiduels $k(P)/k(\varphi(P))$ est séparable ; il est dit *ramifié* dans le cas contraire. L'ensemble des points ramifiés s'appelle le *lieu de ramification*.

Exemple 1.1.14. De façon similaire au cas des courbes projectives, toute fonction rationnelle non-constante $\alpha \in k(X) \setminus k$ définit un morphisme $\varphi_\alpha : X \longrightarrow \mathbb{P}^1_k$: c'est tout simplement l'inclusion $k(\alpha) \hookrightarrow k(X)$. Son degré est $\deg(\varphi_\alpha) = [k(X)\,/k(\alpha)]$.

Proposition 1.1.15. *Soit $\varphi : X \longrightarrow Y$ un morphisme non constant séparable de degré n de courbes non singulières complètes. Alors φ est surjectif, et ses fibres sont de cardinal au plus n. De plus, le lieu de ramification de φ est fini.*

Si k est algébriquement clos, alors les fibres de φ sont de cardinal n au-dessus de tout point non-ramifié.

Démonstration. Comme φ n'est pas constant, alors φ^* est injectif puisque $k(Y)$ est un corps, donc φ est surjectif.

En plus de l'indice de ramification, on peut définir le *degré d'inertie* d'un point $P \in X$ par $f_P = \big[k(P)\,/k(\varphi(P))\big]$. On a alors

$$\sum_{\substack{P \in X \\ \varphi(P)=Q}} e_P f_P = n$$

pour tout point $Q \in Y$. En particulier, les fibres de φ sont de cardinal au plus n.

Recouvrons Y de deux ouverts affines U et U' comme dans la preuve du théorème 1.1.10. Alors U est cofini, donc, pour montrer que le lieu de ramification est fini, il suffit de montrer que son intersection avec U est finie. Or un point $Q \in U$ est ramifié si et seulement si l'idéal maximal $\mathfrak{p}_Q \cap \mathcal{O}_Y(U)$ de $\mathcal{O}_Y(U)$ contient l'idéal discriminant de l'extension $\mathcal{O}_X(\varphi^{-1}(U))/\mathcal{O}_Y(U)$; comme φ est séparable, ce discriminant est non-nul.

Enfin, si k est algébriquement clos, alors les degrés d'inertie f_P valent tous 1, d'où le résultat. □

Le fait qu'un morphisme soit soit constant, soit surjectif justifie la terminologie suivante :

Définition 1.1.16. Soit $\pi : X \longrightarrow Y$ un morphisme de courbes non singulières complètes sur un corps k. On dit que π est un *revêtement galoisien* s'il n'est pas constant et si l'extension de corps de fonctions rationnelles $k(X)/k(Y)$ est galoisienne.

Le *groupe d'automorphismes* de ce revêtement est le sous-groupe $\mathrm{Gal}\big(\mathbb{F}_q(X)/\mathbb{F}_q(Y)\big)$ de $\mathrm{Aut}(X) = \mathrm{Gal}\big(\mathbb{F}_q(X)/\mathbb{F}_q\big)$.

Exemple 1.1.17. Soit X une courbe non singulière complète sur un corps k, et soit G un sous-groupe fini de $\mathrm{Aut}(X) = \mathrm{Gal}\big(k(X)/k\big)$. Alors le sous-corps invariant $k(X)^G$ est un corps de fonctions sur k ; soit Y la courbe

non singulière complète associée, de sorte que $k(Y) = k(X)^G$. Le morphisme $\pi : X \longrightarrow Y$ associé à l'inclusion $k(Y) \hookrightarrow k(X)$ est un revêtement galoisien. En fait, Y peut être vue comme le quotient de X par G.

Dans le cas des courbes projectives, il est facile d'étendre les scalaires. Dans le cas des courbes non singulières complètes, ce n'est guère plus difficile :

Définition 1.1.18. Soit X une courbe non singulière complète sur k. Si k' est une extension de k, on démontre que l'extension composée $k' \cdot k(X)$ est un corps de fonctions sur k. On note $X_{k'}$ la courbe non singulière complète sur k' associée, de sorte que $k'(X_{k'}) = k' \cdot k(X)$.

Tout morphisme $\pi : X \longrightarrow Y$ de courbes non singulières complètes sur k s'étend naturellement en un morphisme $\pi_{k'} : X_{k'} \longrightarrow Y_{k'}$ de courbes non singulières complètes sur k' ; ainsi, l'opération d'*extension des scalaires* ainsi définie est fonctorielle.

On a ainsi défini abstraitement un nouveau type de courbes. Remarquons que, grâce à la discussion précédent l'introduction de ce nouveau type, on peut voir toute courbe projective plane non singulière géométriquement irréductible comme une courbe non singulière complète. Réciproquement, le schéma associé à une courbe non singulière complète X sur un corps k est isomorphe à une variété projective de dimension un (mais pas forcément plane) sur k. En effet, le théorème 1.1.10 montre qu'il existe un ouvert non-vide U de X isomorphe à une courbe affine irréductible $V = \mathrm{Spec}(B)$ sur k. Plongeons cette courbe dans un espace projectif $\mathbb{P}^n_k$, et soit Y sont adhérence. Nous allons prolonger l'isomorphisme $U \simeq V$ en un isomorphisme $X \simeq Y$. Il suffit de le prolonger en un morphisme de X dans $\mathbb{P}^n_k$, car alors son image sera forcément contenue dans Y. Munissons $\mathbb{P}^n_k$ de coordonnées homogènes $x_0, \cdots, x_n$. On peut supposer que V rencontre $D_+(x_0 \cdots x_n)$, car sinon V est contenue dans l'union des hyperplans $V(x_i)$, donc dans l'un d'entre eux par irréductibilité, et $V(x_i) \simeq \mathbb{P}^{n-1}_k$ donc on arrive à la situation voulue en diminuant éventuellement n. Alors les x_i/x_j sont des fonctions régulières sur V ; notons $f_{i,j} \in \mathcal{O}_X(U)$ les fonctions correspondantes sur U. Considérons un point $P \in X - U$. Posons $r_i = v_P(f_{i,0})$. On a $v_P(f_{i,j}) = r_i - r_j$, donc si i_0 est tel que r_{i_0} est minimal, alors $v_P(f_{i,i_0}) \geqslant 0$ pour tout i. Prolongeons alors l'isomorphisme $U \simeq V$ en envoyant P sur $[f_{0,i_0}(P), \cdots, f_{n,i_0}(P)]$. Ce point est dans $D_+(x_{i_0})$, car $f_{i_0,i_0}(P) = 1 \neq 0$. Or l'ouvert $D_+(x_{i_0}$ est affine, son anneau de fonctions régulières est $k[x_0/x_{i_0}, \cdots, x_n/x_{i_0}]$, ce qui correspond sur X à

$k[f_{0,i_0}, \cdots, f_{n,i_0}]$, ce qui est contenu dans $\mathcal{O}_P$ par construction ; le morphisme prolongé est donc bien un morphisme de schémas. Comme U est cofini dans X, en répétant ce procédé un nombre fini de fois, on obtient l'isomorphisme $X \simeq Y$ recherché.

Dans la suite, on ne privera donc nullement d'appliquer le théorème de Riemann-Roch qu'on aura démontré pour les courbes projectives aux courbes non singulières complètes.

1.2 Diviseurs sur une courbe

Considérons une courbe non singulière complète X sur un corps k. Le langage des diviseurs, que nous allons introduire, fournit un moyen commode pour discuter de l'existence de fonctions rationnelles sur X ayant des pôles et des zéros d'ordres prescrits en certains points de X.

Notons $\mathrm{Div}(X)$ le groupe abélien libre sur les points de X. Les éléments de $\mathrm{Div}(X)$ s'appellent les *diviseurs* sur X. Un diviseur est donc une somme formelle $D = \sum_{P \in X} n_P P$, où $(n_P)_{P \in X}$ est une famille d'entiers relatifs presque nulle. Un tel diviseur est dit *effectif* si les n_P sont tous positifs ou nuls ; on note $\mathrm{Eff}(X)$ l'ensemble des diviseurs effectifs.

Le *degré* d'un diviseur est l'entier relatif

$$\deg\left(\sum_{P \in X} n_P P\right) = \sum_{P \in X} n_P \left[k(P) \colon k\right].$$

On obtient ainsi un morphisme de $\mathrm{Div}(X)$ dans $\mathbb{Z}$.

Si $\alpha \in k(X)^*$ est une fonction rationnelle non nulle sur X, on note $\mathrm{div}(\alpha)$ le diviseur

$$\mathrm{div}(\alpha) = \sum_{P \in X} v_P(\alpha) P.$$

Un tel diviseur est dit *principal*.

Exemple 1.2.1. Soit $\alpha \in k(X)^*$. Nous lui avons associé à l'exemple 1.1.14 un morphisme φ_α de X dans $\mathbb{P}^1_k$. Notons $0 \in \mathbb{P}^1_k$ la valuation α-adique de $k[\alpha]$, et $\infty \in \mathbb{P}^1_k$ la valuation $1/\alpha$-adique de $k[1/\alpha]$. Si on pose

$$(\alpha)_0 = \sum_{P \in \varphi_\alpha^{-1}(0)} v_P(\alpha) P \quad \text{et}$$

$$(\alpha)_\infty = -\sum_{P\in\varphi_\alpha^{-1}(\infty)} v_P(\alpha)P,$$

alors $(\alpha)_0$ et $(\alpha)_\infty$ sont effectifs, et on a $\mathrm{div}(\alpha) = (\alpha)_0 - (\alpha)_\infty$. De plus, considérons la clôture intégrale B de $k[\alpha]$ dans $k(X)$; on y a la factorisation

$$(\alpha)B = \prod_{P\in\varphi_\alpha^{-1}(0)} \mathfrak{p}_P^{v_P(\alpha)},$$

d'où $[k(X) : k(\alpha)] = \sum_{P\in\varphi_\alpha^{-1}(0)} v_P(\alpha)[k(P) : k] = \deg\big((\alpha)_0\big)$; et de même $[k(X) : k(\alpha)] = \deg\big((\alpha)_\infty\big)$.

Comme div est clairement un morphisme de $k(X)^*$ dans $\mathrm{Div}(X)$, les diviseurs principaux forment un sous-groupe de $\mathrm{Div}(X)$. Le quotient de $\mathrm{Div}(X)$ par ce sous-groupe s'appelle le *groupe de Picard* de X, et est noté $\mathrm{Pic}(X)$. On note $\mathrm{cl}(D)$ la classe d'un diviseur $D \in \mathrm{Div}(X)$ dans $\mathrm{Pic}(X)$.

En résumé, on a une suite exacte

$$1 \longrightarrow k^* \longrightarrow k(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(X) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(X) \longrightarrow 0,$$

l'exactitude en $k(X)^*$ étant garantie par la proposition 1.1.12. Remarquons l'analogie avec le groupe des classes d'un corps de nombres.

À propos de corps de nombres, rappelons la formule suivante : si A est un anneau de Dedekind de corps des fractions K, si L est une extension finie de K, et si B désigne la clôture intégrale de A dans L, alors on a, pour tout $x \in L$ et pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$ non nul,

$$\mathrm{ord}_\mathfrak{p}\big(N_{L/K}(x)\big) = \sum_{\substack{\mathfrak{P}\in\mathrm{Spec}(B)\\ \mathfrak{P}|\mathfrak{p}}} f_{\mathfrak{P}/\mathfrak{p}}\,\mathrm{ord}_\mathfrak{P}(x),$$

où $f_{\mathfrak{P}/\mathfrak{p}} = [B/\mathfrak{P} : A/\mathfrak{p}]$ désigne bien sûr le degré d'inertie, et où $N_{L/K}$ est la norme de L sur K.

Si $\pi : X \longrightarrow Y$ est un morphisme de courbes non singulières complètes sur k, alors on a par définition pour tout point P de X l'identité

$$\deg(P) = f_P \deg\big(\pi(P)\big).$$

Par conséquent, si on définit (comme la formule précédente le suggère) la *norme* $N_{X/Y}$ de X sur Y par la formule

$$\begin{array}{rccc} N_{X/Y} & : & \mathrm{Div}(X) & \longrightarrow & \mathrm{Div}(Y) \\ & & \displaystyle\sum_{P\in X} n_P P & \longmapsto & \displaystyle\sum_{P\in X} n_P f_P \pi(P) \end{array},$$

on a le diagramme commutatif suivant :

$$\begin{array}{ccccc} k(X)^* & \xrightarrow{\text{div}} & \text{Div}(X) & \xrightarrow{\deg} & \mathbb{Z} \\ \Big\downarrow{\scriptstyle N_{k(X)/k(Y)}} & & \Big\downarrow{\scriptstyle N_{X/Y}} & & \Big\| \\ k(Y)^* & \xrightarrow{\text{div}} & \text{Div}(Y) & \xrightarrow{\deg} & \mathbb{Z} \end{array} \quad .$$

Si π n'est pas constant, on peut aussi tirer le diviseurs en arrière, grâce à l'application (notée π^* tout comme le morphisme de $k(Y)$ dans $k(X)$, mais le typage évite toute confusion)

$$\begin{array}{rccc} \pi^* & : & \text{Div}(Y) & \longrightarrow & \text{Div}(X) \\ & & \displaystyle\sum_{Q\in Y} n_Q Q & \longmapsto & \displaystyle\sum_{Q\in Y} n_Q \sum_{\substack{P\in X \\ \pi(P)=Q}} e_P P \ . \end{array}$$

Comme $\sum_{\pi(P)=Q} e_P f_P = \deg(\pi)$ pour tout point Q de Y, la composée $N_{X/Y} \circ \pi^*$ coïncide sur $\text{Div}(Y)$ avec la multiplication par $\deg(\pi)$.

Théorème 1.2.2. *Soit X une courbe non singulière complète sur k. Le degré de tout diviseur principal sur X est nul.*

Autrement dit, une fonction rationnelle a autant de pôles que de zéros, à condition de les compter avec la bonne multiplicité.

Démonstration. Soit $x \in k(X)$ tel que $k(X)/k(x)$ soit une extension finie. L'exemple 1.1.14 lui associe un morphisme $\pi : X \longrightarrow \mathbb{P}^1_k$. D'après ce qui précède, on a, pour toute fonction rationnelle non nulle $\alpha \in k(X)^*$,

$$\deg\big(\text{div}(\alpha)\big) = \deg\big(\text{div}\big(N_{k(X)/k(x)}(\alpha)\big)\big).$$

Ainsi, on se ramène au cas où $X = \mathbb{P}^1_k$ et donc $k(X) = k(x)$ est un corps de fractions rationnelles en un indéterminée. Montrons donc que pour tout $\beta \in k(x)^*$, $\deg\big(\text{div}(\beta)\big) = 0$. Comme div est un morphisme, on peut supposer sans perte de généralité que $\beta \in k[x]$ est un polynôme irréductible. La description des points de $\mathbb{P}^1_k$ faite à l'exemple 1.1.11 montre qu'on a alors, en notant P le point associé à β,

$$\text{div}(\beta) = v_\beta(\beta)P + v_\infty(\beta)\infty = P - \deg(\beta)\infty,$$

et comme $\deg(P) = [k(P) : k] = [k[x]/(\beta) : k] = \deg(\beta)$, on a bien $\deg\big(\operatorname{div}(\beta)\big) = 0$ comme voulu. □

On déduit de ce théorème que deg se factorise en un morphisme de $\mathrm{Pic}(X)$ dans $\mathbb{Z}$. On note $\mathrm{Pic}^0(X)$ son noyau, qu'on appelle *groupe des classes* de X. Plus généralement, pour tout entier $d \in \mathbb{Z}$, on notera $\mathrm{Pic}^d(X) \subset \mathrm{Pic}(X)$ l'ensemble des éléments de $\mathrm{Pic}(X)$ de degré d, et on définit de la même manière les ensembles $\mathrm{Div}^d(X)$ et $\mathrm{Eff}^d(X)$.

Comme deg n'est clairement pas le morphisme nul, $\mathrm{Pic}(X)$ est, contrairement au groupe des classes d'un corps de nombres, toujours infini. Cependant, nous démontrerons à l'aide du théorème de Riemann-Roch que, si le corps de base k est fini, alors $\mathrm{Pic}^0(X)$ est lui aussi fini.

Le langage ainsi introduit est fort commode pour discuter de l'existence de fonctions rationnelles dont on prescrit le diviseur. Ainsi, $\mathrm{Pic}(X)$ exprime l'obstruction à la résolubilité de ce problème. Il est infini, ce qui traduit l'aspect "bête" de cette obstruction, à savoir que le diviseur prescrit doit être de degré nul pour espérer l'existence de solutions. Dans ce cas, le groupe des classes $\mathrm{Pic}^0(X)$ dit s'il existe effectivement une telle fonction. Nous pourrons bientôt, toujours grâce au théorème de Riemann-Roch, être plus précis.

Exemple 1.2.3. Le groupe des classes de la droite projective sur k est trivial. En effet, soit

$$D = \sum_f n_f f + n_\infty \infty$$

un diviseur de degré nul, où $f \in k[x]$ décrit l'ensemble des polynômes irréductibles unitaires sur k. Considérons la fraction rationnelle

$$\alpha = \prod_f f^{n_f} \in k(x).$$

Pour tout f, on a par construction $v_f(\alpha) = n_f$, et $v_\infty(\alpha) = -\sum_f n_f \deg(f) = n_\infty$ puisque $\deg(D) = 0$; par conséquent $\operatorname{div}(\alpha) = D$. Ainsi, tout diviseur de degré nul sur $\mathbb{P}^1_k$ est principal, c'est-à-dire que $\mathrm{Pic}^0(\mathbb{P}^1_k) = 0$.

1.3 Le théorème de Riemann-Roch pour les courbes

Nous allons à présent enfin nous lancer dans la démonstration du théorème de Riemann-Roch. Cette démonstration utilise des méthodes assez nettement plus complexes que ce que nous avons vu passer jusqu'à présent, telles que la cohomologie des faisceaux ; aussi avons nous choisi de reporter les définitions et les résultats relatifs à ces méthodes en annexe. Le lecteur est invité à admettre les résultats en question lors de la lecture de cette section, quitte à les étudier plus en détail ultérieurement.

Soit X une courbe non singulière complète sur un corps k.

Définition 1.3.1. Soit $D = \sum_{P \in X} n_P P \in \mathrm{Div}(X)$ un diviseur sur X. On lui associe le $\mathcal{O}_X$-module inversible

$$\mathcal{F}_D : U \longmapsto \{\alpha \in k(X) \mid \forall P \in U,\ v_P(\alpha) + n_P \geqslant 0\}.$$

Pour tout $r \in \mathbb{N}$, on pose $H^r(D) = H^r(X, \mathcal{F}_D)$. D'après le théorème 5.1.10 (a), ces k-espaces vectoriels sont de dimension finie ; on notera $h^r(D) = \dim_k H^r(X, \mathcal{F}_D)$ leur dimension.

Ceci nous permet en particulier de définir un invariant extrêmement important de la courbe X :

Définition 1.3.2. Le *genre* de X est l'entier $g = h^1(0)$.

Comme on va bientôt le voir, le genre joue un rôle fondamental dans l'énoncé du théorème de Riemann-Roch, et donc dans bien des énoncés concernant la courbe X.

Remarquons que la structure du groupe des diviseurs se reflète sur les faisceaux associés : $\mathcal{F}_0 = \mathcal{O}_X$ et $\mathcal{F}_{D+D'} \simeq \mathcal{F}_D \underset{\mathcal{O}_X}{\otimes} \mathcal{F}_{D'}$, et par conséquent, $\mathcal{F}_{-D} \simeq \mathcal{F}_D^\vee$.

Par ailleurs, tout $\mathcal{O}_X$-module inversible $\mathcal{L}$ est isomorphe à un $\mathcal{F}_D$: en effet, si on note $k(X)$ le faisceau constant égal à $k(X)$, alors sur tout ouvert sur lequel $\mathcal{L} \simeq \mathcal{O}_X$, on a $\mathcal{L} \underset{\mathcal{O}_X}{\otimes} k(X) \simeq k(X)$, si bien que $\mathcal{L} \underset{\mathcal{O}_X}{\otimes} k(X)$ est localement constant, donc constant par irréductibilité de X. L'application naturelle

$$\mathcal{L} \hookrightarrow \mathcal{L} \underset{\mathcal{O}_X}{\otimes} k(X) \simeq k(X)$$

permet alors de voir $\mathcal{L}$ comme un sous-faisceau de $k(X)$; or un tel faisceau inversible s'identifie à un $\mathcal{F}_D$ puisqu'il s'écrit localement $\alpha\mathcal{O}_X$ pour une certaine fonction rationnelle $\alpha \in k(X)$.

Avec cette dernière remarque, nous avons enfin réuni tous les ingrédients nécessaires au théorème de Riemann-Roch.

Théorème 1.3.3 (Riemann-Roch)**.** *Soit k un corps quelconque, et soit X/k une courbe non singulière complète de genre $g = h^1(0)$. Il existe un diviseur $K \in \mathrm{Div}(X)$, dit* diviseur canonique*, de degré $2g-2$, tel que, pour tout diviseur $D \in \mathrm{Div}(X)$,*

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D).$$

Démonstration. Le théorème 5.3.9, joint à l'exemple 5.2.4, nous dit que le faisceau dualisant ω_X de X est inversible, ce qui nous autorise à choisir pour diviseur canonique le diviseur K tel que $\mathcal{F}_K \simeq \omega_X$. Comme X est de dimension 1, on a par définition de ω_X un isomorphisme $H^1(D)' \simeq \mathrm{Hom}_X(\mathcal{F}_D, \omega_X)$ pour tout diviseur $D \in \mathrm{Div}(X)$. Or $\mathrm{Hom}_X(\mathcal{F}_D, \omega_X) \simeq \mathrm{Hom}_X(\mathcal{F}_D, \mathcal{F}_K) \simeq \mathrm{Hom}_X\left(\mathcal{O}_X, \mathcal{F}_D^\vee \underset{\mathcal{O}_X}{\otimes} \mathcal{F}_K\right) \simeq \Gamma\left(X, \mathcal{F}_D^\vee \underset{\mathcal{O}_X}{\otimes} \mathcal{F}_K\right) \simeq \Gamma(X, \mathcal{F}_{K-D}) = H^0(K-D)$. On a donc en particulier $h^1(D) = h^0(K-D)$ pour tout diviseur D. Pour en déduire le résultat, il suffit donc de montrer la relation

$$\forall D \in \mathrm{Div}(X), \quad \chi(D) = \deg(D) + 1 - g,$$

où $\chi(D) = h^0(D) - h^1(D)$ désigne la *caractéristique d'Euler* du diviseur D, dont nous reparlerons bien plus tard. Mais cette relation est vraie pour $D = 0$, par définition du genre et puisque $h^0(0) = k$ d'après la proposition 1.1.12 ; par conséquent, il suffit de montrer que $\chi(D) - \deg(D)$ est une constante indépendante de D, ce qui est revient encore à dire que $\chi(D+P) - \deg(D+P) = \chi(D) - \deg(D)$ pour tout diviseur D et tout point P. Or, si on voit P comme un sous-schéma fermé de X, alors son faisceau d'idéaux est formé des fonctions s'annulant en P, donc n'est autre que $\mathcal{F}_{-P}$; on a donc une suite exacte

$$0 \longrightarrow \mathcal{F}_{-P} \longrightarrow \mathcal{O}_X \longrightarrow k(P) \longrightarrow 0$$

où $k(P)$ désigne bien entendu le faisceau constant égal à $k(P)$. En tensorisant par $\mathcal{F}_{D+P}$, on obtient la suite (encore exacte puisque $\mathcal{F}_{D+P}$ est localement libre)

$$0 \longrightarrow \mathcal{F}_D \longrightarrow \mathcal{F}_{D+P} \longrightarrow k(P) \longrightarrow 0,$$

dont le début de la suite exacte longue de cohomologie est

$$0 \longrightarrow H^0(D) \longrightarrow H^0(D+P) \longrightarrow k(P) \longrightarrow H^1(D) \longrightarrow H^1(D+P) \longrightarrow 0,$$

puisque $k(P)$ est clairement acyclique. En écrivant que la somme alternée des dimensions sur k est nulle, on obtient alors exactement la relation désirée.

Enfin, en appliquant la formule ainsi obtenue à $D = K$, on vérifie que le diviseur canonique est de degré $2g - 2$. □

Puisque $h^0(D) = 0$ si $\deg(D) < 0$, on en déduit immédiatement le

Corollaire 1.3.4. *Soit $\mathcal{L} \in \mathrm{Pic}(X/k)$. Si $\deg(\mathcal{L}) \geqslant 2g - 1$, alors*

$$h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g.$$

Ainsi, en degré assez grand, la dimension de l'espace des fonctions ayant des pôles d'ordre majoré varie linéairement avec le degré. En petit degré, les choses sont perturbées, et le genre code l'étendue de la perturbation.

Le théorème de Riemann-Roch peut donc se voir comme la réponse au *problème de Riemann-Roch* :

▷ **Fixons un diviseur D. Existe-t-il des fonctions rationnelles sur X dont le diviseur est D, et si oui, combien ?** ◁

Utilisé astucieusement, il permet de montrer l'existence de fonctions intéressantes pour la résolution d'un problème donné. Illustrons ce propos par deux exemples.

Exemple 1.3.5 (Courbes rationnelles)**.** Toute courbe X de genre nul ayant un point k-rationnel est birationnelle à la droite projective $\mathbb{P}^1_k$. En effet, soit $P \in X(k)$ un tel point. On a alors par définition $\deg(P) = 1$, donc $h^0(P) = 2$ d'après le corollaire 1.3.4 au théorème de Riemann-Roch. Par conséquent, il existe une fonction rationnelle non-constante $\alpha \in k(X)$ ayant un pôle d'ordre au plus 1 en P, et aucun autre pôle. Comme α n'est pas constante, elle a en fait un pôle d'ordre exactement 1 en P d'après la proposition 1.1.12. D'après l'exemple 1.1.14, on a $[k(X) : k(\alpha)] = 1$, donc $k(X) = k(\alpha)$ est un corps de fractions rationnelles.

En fait, si on munit $\mathbb{P}^1_k$ de la coordonnée x, et si P correspond à $x = a$, la fonction α que nous avons construite est $\frac{1}{x-a}$.

Exemple 1.3.6 (Courbes elliptiques)**.** Toute courbe de genre un ayant un point k-rationnel est birationnelle à une cubique. En effet, soit $P \in X(k)$ un

tel point. Comme $\deg(nP) = n \geqslant 2g-1$ pour tout $n \in \mathbb{N}^*$, on a $h^0(nP) = n$ pour tout $n \in \mathbb{N}^*$. Par conséquent, $H^0(P)$ est donc l'espace des fonctions constantes, et $H^0(2P)$ contient une fonction $x \in k(X)$ ayant un pôle d'ordre 2 en P. De même, $H^0(3P)$ contient une fonction y ayant un pôle d'ordre 3 en P. On a $\{1, x, y, x^2\} \subset H^0(4P)$, et c'en est une base puisque ces quatre fonctions ont des pôles d'ordres distincts en P. De même, $\{1, x, y, x^2, xy\}$ est une base de $H^0(5P)$. Ensuite, on a $\{1, x, y, x^2, xy, y^2, x^3\} \subset H^0(6P)$, d'où une relation de liaison

$$b_1 + b_2x + b_3y + b_4x^2 + b_5xy + b_6y^2 + b_7x^3 = 0, \quad b_i \in k.$$

Comme y^2 et x^3 sont les seules à avoir un pôle d'ordre 6 en P, ni b_6 ni b_7 ne sauraient être nuls. On peut donc supposer que $b_7 = 1$, puisque, quitte à multiplier x et y par b_6, que $b_6 = 1$ aussi. On a donc une relation de forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k.$$

Considérons le polynôme (clairement irréductible)

$$f(X, Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in k[X, Y].$$

Soit Z_f la courbe affine associée, et soit $k(Z_f) = \mathrm{Frac}\big(k[X, Y]/(f)\big) \subset k(X)$ son corps de fonctions. On a d'une part $[k(Z_f) : k(x)] = 2$, et d'autre part $[k(X) : k(x)] = 2$ d'après l'exemple 1.1.14. Ainsi, X est birationnelle à Z_f.

Dans la même veine, notre démonstration de l'hypothèse de Riemann, et plus exactement les propositions 2.5.9 et 2.5.11, utilisent cette méthode.

Dans le cas où le corps de base k est fini, le théorème de Riemann-Roch donne des informations combinatoires qui seront utiles à l'établissement de propriétés des fonction Zêta ; rendez-vous à la deuxième partie.

On y utilisera également le corollaire suivant :

Corollaire 1.3.7. *Si $d \geqslant g$, tout élément de $\mathrm{Pic}^d(X)$ est représenté par un diviseur effectif.*

Démonstration. Soit $D \in \mathrm{Div}(X)$ un représentant de cet élément. Comme $\deg(D) \geqslant g$, on a $h^0(D) > 0$ par le théorème de Riemann-Roch 1.3.3. Soit donc $\alpha \in H^0(D) - \{0\}$ une fonction non nulle. Par définition, le diviseur $D + \mathrm{div}(\alpha)$ est effectif, et représente le même élément de $\mathrm{Pic}(X)$ que D. □

Comme promis, on déduit également du théorème de Riemann-Roch que le groupes des classes est fini si le corps de base k est lui-même fini :

Théorème 1.3.8. *Soit k un corps fini, et soit X une courbe non singulière complète sur k. Le groupe des classes* $\mathrm{Pic}^0(X)$ *est fini.*

Démonstration. Soit $e \in \mathbb{N}^*$ l'entier tel que $\deg\big(\mathrm{Div}(X)\big) = e\mathbb{Z}$. Comme $\mathrm{Pic}^0(X)$ et $\mathrm{Pic}^{de}(X)$ sont en bijection pour tout $d \in \mathbb{Z}$, il suffit de montrer que $\mathrm{Pic}^{de}(X)$ est fini pour un certain d. Or $\mathrm{Eff}^{de}(X)$ se surjecte sur $\mathrm{Pic}^{de}(X)$ d'après le corollaire 1.3.7 pour $d \gg 0$, donc il suffit de montrer que $\mathrm{Eff}^d(X)$ est fini pour $d \gg 0$. Mais il se trouve justement que $\mathrm{Eff}^d(X)$ est fini pour tout $d \in \mathbb{N}$.

En effet, d'après le corollaire 1.1.7, on peut trouver une fonction $x \in k(X)$ telle que $k(X)$ soit une extension finie séparable de $k(x)$. Soit B la clôture intégrale de $k[x]$ dans $k(X)$. D'après le théorème 1.1.10, il suffit de montrer que pour tout $\lambda \in \mathbb{R}$, que $\mathrm{Spec}(B)$ ne contient qu'un nombre fini de $\mathfrak{p}$ tels que $\|\mathfrak{p}\| < \lambda$. Or, si $P \in k[x]$ est tel que $\mathfrak{p} \cap k[x] = (P)$, alors on a

$$\|\mathfrak{p}\| = |k[x]/(P)|^{f_{\mathfrak{p}/(P)}} \geqslant |k[x]/(P)|$$

donc il suffit de montrer que pour tout $\lambda \in \mathbb{R}$, $k[x]$ ne contient qu'un nombre fini de polynômes irréductibles unitaires tels que $|k[x]/(P)| < \lambda$, ce qui est vrai puisque k est fini. □

Dans ce cas, l'ordre de $\mathrm{Pic}^0(X)$ s'appelle le nombre de classes, et sera noté h. L'hypothèse de Riemann, que l'on démontrera, implique des bornes assez pointues sur ce nombre de classes.

1.4 Calcul du genre d'une courbe plane non singulière

Lemme 1.4.1. *Soit k un corps parfait. Notons $\bar{k}$ une clôture algébrique de k, $G = \mathrm{Gal}(\bar{k}/k)$, et soit V un $\bar{k}$-espace vectoriel de dimension finie muni d'une action k-linéaire de G compatible avec son action sur $\bar{k}$. Supposons que V soit* discret, *c'est-à-dire que tout vecteur v de V soit stable par* $\mathrm{Gal}(\bar{k}/k')$ *pour une certaine extension galoisienne finie k' de k. Alors toute k-base de V^G est une $\bar{k}$-base de V.*

Démonstration. Soit $v_1, \cdots, v_s$ une famille k-libre de V^G, telle qu'on ait une relation de liaison $\sum_{i=1}^{s} \lambda_i v_i = 0$, $\lambda_i \in \bar{k}$. Notons k' l'extension générée par les d_i, et fixons-en une k-base $c_1, \cdots, c_n$, de sorte qu'on puisse écrire $\lambda_i =$

$\sum_{j=1}^{n} \mu_{i,j} c_j$, avec $\mu_{i,j} \in k$. Posons alors $w_j = \sum_{i=1}^{s} \mu_{i,j} v_i$. Par construction, les w_j sont dans V^G, et on a $\sum_{j=1}^{n} c_j w_j = 0$. On a donc aussi $\sum_{j=1}^{n} \sigma(c_j) w_j = 0$ pour tout $\sigma \in G$. Comme k' est séparable sur k par perfection de ce dernier, le discriminant de la base $c_1, \cdots, c_n$ n'est pas nul, si bien que les w_j doivent être tous nuls. Comme les v_i sont k-libres, les $\mu_{i,j}$, donc les λ_i, sont eux aussi nuls, donc v_i est $\bar{k}$-libre.

Pour conclure, il suffit de montrer que V^G engendre $\bar{k}$-linéairement V. Soit donc $v \in V$; par hypothèse, il existe une extension galoisienne finie k' de k telle que $\mathrm{Gal}(\bar{k}/k')$ stabilise v. Soit $c_1, \cdots, c_n$ une k-base de k', et soient $\sigma_1, \cdots, \sigma_n \in \mathrm{Gal}(\bar{k}/k)$ tels que $\mathrm{Gal}(k'/k) = \{\sigma_1|_{k'}, \cdots, \sigma_n|_{k'}\}$. Considérons alors les relations

$$\begin{pmatrix} \sigma_1(c_1) & \cdots & \sigma_n(c_1) \\ \vdots & & \vdots \\ \sigma_1(c_n) & \cdots & \sigma_n(c_n) \end{pmatrix} \begin{pmatrix} \sigma_1(v) \\ \vdots \\ \sigma_n(v) \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} \sigma_j(c_1 v) \\ \vdots \\ \sum_{j=1}^{n} \sigma_j(c_n v) \end{pmatrix}.$$

Comme la matrice de gauche est inversible puisque k' est séparable sur k, tous les $\sigma_i(v)$, et en particulier v, est combinaison k'-linéaire des $\sum_{j=1}^{n} \sigma_j(c_i v)$ qui sont clairement dans V^G. □

Proposition 1.4.2. *Soit X une courbe non singulière complète sur un corps parfait k, et soit $\overline{X}$ la courbe obtenue en étendant les scalaires à une clôture algébrique $\bar{k}$ de k. Les courbes X et $\overline{X}$ ont le même genre.*

Démonstration. Notons π le morphisme de $\overline{X}$ vers X correspondant à l'inclusion $k(X) \hookrightarrow \bar{k}(\overline{X}) = \bar{k} \cdot k(X)$. Le groupe $G = \mathrm{Gal}(\bar{k}/k)$ agit sur $\overline{X}$, donc sur $\mathrm{Div}(\overline{X})$. Définissons un isomorphisme $\mathrm{Div}(X) \xrightarrow{\sim} \mathrm{Div}(\overline{X})^G$ en associant à tout diviseur $D = \sum_{P \in X} n_P P \in \mathrm{Div}(X)$ le diviseur

$$\overline{D} = \sum_{P \in X} n_P \sum_{\substack{Q \in \overline{X} \\ \pi(Q) = P}} Q \in \mathrm{Div}(\overline{X})^G.$$

D'après le théorème de Riemann-Roch 1.3.3, $g_X = \deg(D) + 1 - h^0(D) + h^1(D)$ et $g_{\overline{X}} = \deg(\overline{D}) + 1 - h^0(\overline{D}) + h^1(\overline{D})$. Mais par construction, $\deg(D) = \deg(\overline{D})$, et si ce degré est suffisamment grand, alors les h^1 sont nuls. Il ne reste alors plus qu'a appliquer le lemme 1.4.1 précédent pour obtenir $h^0(D) = h^0(\overline{D})$. □

Théorème 1.4.3. *Soit k un corps parfait, et soit X_F une courbe plane projective non singulière sur k, définie par un polynôme homogène $F \in k[x_0, x_1, x_2]$ de degré d. Le genre de X_F vaut $g = (d-1)(d-2)/2$.*

Démonstration. L'idée est de calculer le h^0 d'un diviseur de degré suffisamment grand pour que le h^1 ne nous ennuie pas.

La proposition 1.4.2 nous permet de supposer sans perte de généralité que k est algébriquement clos. Alors, quitte à changer de repère, on peut supposer que X_F coupe la droite à l'infini X_{x_2} en d points simples distincts $P_1, \cdots, P_d$. Considérons le diviseur $D = \sum_{i=1}^{d} P_i$. Il est clair que pour tout entier $m \in \mathbb{N}$, $\deg(mD) = md$.

Notons V_m le sous-espace vectoriel de $k[x_0, x_1, x_2]$ formé des polynômes nuls ou homogènes de degré m. On a une application bien définie

$$\begin{array}{rccc} \varphi & : & V_m & \longrightarrow & H^0(mD) \\ & & G(x_0, x_1, x_2) & \longmapsto & \dfrac{G(x_0, x_1, x_2)}{x_2^m} \end{array},$$

qui est clairement linéaire et injective. Elle est aussi surjective car toute fonction $\alpha \in H^0(mD)$ est régulière sur la courbe affine $X_F - X_{x_2}$, donc est un polynôme $a(x_0/x_2, x_1/x_2)$ en x_0/x_2 et x_1/x_2, de surcroît de degré au plus m, donc est l'image du polynôme $G(x_0, x_1, x_2) = x_2^m a(x_0/x_2, x_1/x_2)$.

Par ailleurs, la multiplication par F est, pour $m \geqslant d$, une application linéaire injective de V_{m-d} dans V_m, dont l'image n'est autre que $\operatorname{Ker} \varphi$. On a donc une suite exacte de k-espaces vectoriels

$$0 \longrightarrow V_{m-d} \longrightarrow V_m \longrightarrow H^0(mD) \longrightarrow 0.$$

Comme $\dim_k V_m = (m+1)(m+2)/2$, on en déduit que

$$h^0(mD) = \frac{(m+1)(m+2)}{2} - \frac{(m-d+1)(m-d+2)}{2} = md+1-\frac{(d-1)(d-2)}{2}.$$

En prenant m suffisamment grand pour que $\deg(mD) = md \geqslant 2g-1$, on en déduit le résultat à l'aide du corollaire 1.3.4 au théorème de Riemann-Roch. □

2 Fonction zêta d'une courbe algébrique sur un corps fini

Nous allons à présent introduire les fameuses fonctions zêta qui font l'objet de notre propos, et en démontrer diverses propriétés, dites *conjectures de Weil*, essentiellement grâce au théorème de Riemann-Roch. Notre approche sera celle de [Lor96] ; en particulier, la preuve élémentaire de l'hypothèse de Riemann que nous donnerons est tirée de [Bom74], et constitue le point culminant de cette partie.

2.1 Action du groupe de Galois sur les points

Avant de passer aux fonctions zêta proprement dites, nous aurons besoin d'étudier l'action des groupes de Galois sur les points des plans affine et projectif, notamment l'aspect combinatoire lorsque k est un corps fini.

Fixons un corps quelconque k, et soit $\bar{k}$ une clôture algébrique de k, fixée une fois pour toutes. Le *groupe de Galois absolu* $\mathrm{Gal}(\bar{k}/k)$ agit naturellement sur l'espace affine $\mathbb{A}^2(\bar{k})$ par

$$\sigma \cdot (a,b) = \big(\sigma(a), \sigma(b)\big) \quad \big(\sigma \in \mathrm{Gal}(\bar{k}/k),\ a,b \in \bar{k}\big).$$

De plus, si Z est une courbe affine définie sur k, alors cette action stabilise $Z(\bar{k})$.

Soit $f \in k[x,y]$ un polynôme absolument irréductible. Pour $(a,b) \in Z_f(\bar{k})$, notons $\psi_{(a,b)}$ le morphisme d'évaluation

$$\begin{array}{rccc} \psi_{(a,b)} & : & k[x,y] & \longrightarrow & \bar{k} \\ & & g & \longmapsto & g(a,b) \end{array}.$$

Lemme 2.1.1. *L'application*

$$\begin{array}{rccc} I_k & : & Z_f(\bar{k})/\,\mathrm{Gal}(\bar{k}/k) & \longrightarrow & Z_f \\ & & \mathrm{Gal}(\bar{k}/k)\cdot(a,b) & \longmapsto & \mathrm{Ker}\,\psi_{(a,b)} \end{array}$$

est bien définie et est injective. On a un diagramme commutatif

$$\begin{array}{ccc} Z_f(\bar{k}) & \xrightarrow{\quad I_{\bar{k}} \quad} & Z_f \times_k \bar{k} \\ \big\downarrow & & \big\downarrow \\ Z_f(\bar{k})/Gal(\bar{k}/k) & \xrightarrow{\quad I_k \quad} & Z_f. \end{array}$$

Démonstration. Soit $(a,b) \in Z_f(\bar{k})$. Si $\sigma \in \mathrm{Gal}(\bar{k}/k)$ et si $(a',b') = \big(\sigma(a),\sigma(b)\big)$, alors $\psi_{(a',b')} = \sigma \circ \psi_{(a,b)}$, donc I_k est bien définie. Montrons que I_k est injective : soient (a,b) et (a',b') des représentants d'orbites de $Z_f(\bar{k})$ sous $\mathrm{Gal}(\bar{k}/k)$ tels que $\mathrm{Ker}\,\psi_{(a,b)} = \mathrm{Ker}\,\psi_{(a',b')}$. Alors les k-isomorphismes $C_f/\mathrm{Ker}\,\psi_{(a,b)} \simeq k(a,b)$, $C_f/\mathrm{Ker}\,\psi_{(a',b')} \simeq k(a',b')$ donnent un k-isomorphisme $k(a,b) \simeq k(a',b')$ qui se prolonge à l'extension normale $\bar{k}/k$ en un élément de $\mathrm{Gal}(\bar{k}/k)$ qui envoie (a,b) sur (a',b'). □

Lemme 2.1.2. *Supposons que k est parfait. L'orbite d'un point $P \in \mathbb{A}^2(\bar{k})$ sous l'action de $\mathrm{Gal}(\bar{k}/k)$ est de cardinal $\big[k(P) : k\big]$.*

Démonstration. Le stabilisateur de P n'est autre que $\mathrm{Gal}\big(\bar{k}/k(P)\big)$, qui est d'indice $\big[k(P) : k\big]$ dans $\mathrm{Gal}(\bar{k}/k)$ puisque k est parfait. □

Proposition 2.1.3. *Soit $f \in \mathbb{F}_q[x,y]$ un polynôme absolument irréductible, et soient $C_f = \mathbb{F}_q[x,y]/(f)$ et $Z_f = \mathrm{Spec}(C_f)$ l'anneau des fonctions régulières et la courbe affine associés. Pour tout $d \in \mathbb{N}^*$, l'ensemble des $\mathfrak{p} \in Z_f$ dont le corps résiduel est de degré d sur $\mathbb{F}_q$ est fini ; si on note b_d son cardinal, alors pour tout $n \in \mathbb{N}^*$, le nombre de points $\mathbb{F}_{q^n}$-rationnels de Z_f est*

$$N_n = |Z_f(\mathbb{F}_{q^n})| = \sum_{d|n} d\, b_d.$$

Démonstration. Montrons que l'application

$$\begin{array}{rccc} J & : & Z_f(\mathbb{F}_{q^n}) & \longrightarrow & \displaystyle\bigcup_{d|n} \{\mathfrak{p} \in Z_f \mid [C_f/\mathfrak{p} : \mathbb{F}_q] = d\} \\ & & (a,b) & \longmapsto & \mathrm{Ker}\,\psi_{(a,b)} \end{array}$$

est bien définie et est surjective. Tout d'abord, si $(a,b) \in Z_f(\mathbb{F}_{q^n})$, soit $\mathfrak{p} = \mathrm{Ker}\,\psi_{(a,b)}$ et soit $d = [C_f/\mathfrak{p} : \mathbb{F}_q]$. Alors $C_f/\mathfrak{p} \simeq \mathbb{F}_q(a,b)$ est un sous-corps de $\mathbb{F}_{q^n}$, donc $d|n$, ce qui montre que J est bien définie. Soit ensuite $\mathfrak{p} \in Z_f$ tel que $C_f/\mathfrak{p} \simeq \mathbb{F}_{q^d}$, où $d|n$. Il existe alors un plongement $\epsilon : C_f/\mathfrak{p} \hookrightarrow \mathbb{F}_{q^n}$. Soient $a = \epsilon(x)$ et $b = \epsilon(y)$. Il est alors clair que $f(a,b) = 0$, donc $(a,b) \in Z_f(\mathbb{F}_{q^n})$, et que $\mathfrak{p} = \mathrm{Ker}\,\psi_{(a,b)}$, d'où la surjectivité de J.

Soit $(a,b) \in Z_f(\mathbb{F}_{q^n})$ un point de corps résiduel $\mathbb{F}_q(a,b) \simeq \mathbb{F}_{q^d}$. Le lemme 2.1.2 nous dit que l'orbite de ce point sous $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ est de cardinal d. Comme l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est galoisienne, cette orbite est contenue dans $Z_f(\mathbb{F}_{q^n})$. D'après le lemme 2.1.1, J se factorise par l'action de $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ sur $Z_f(\mathbb{F}_{q^n})$ en une injection, donc en une bijection. Ainsi, $Z_f(\mathbb{F}_{q^n})$ contient exactement b_d orbites de cardinal d, donc $N_n = \sum_{d|n} d\, b_d$. □

Le cas du plan projectif est très similaire : on a clairement une action bien définie de $\mathrm{Gal}(\bar{k}/k)$ sur $\mathbb{P}^2(\bar{k})$, donnée par

$$\sigma \cdot [c_0, c_1, c_2] = \big[\sigma(c_0), \sigma(c_1), \sigma(c_2)\big] \quad \big(\sigma \in \mathrm{Gal}(\bar{k}/k),\ c_0, c_1, c_2 \in \bar{k}\big).$$

L'analogue du lemme 2.1.2 est alors le

Lemme 2.1.4. *Supposons que k est parfait. L'orbite d'un point $P \in \mathbb{P}^2\big(\bar{k}\big)$ sous $\mathrm{Gal}(\bar{k}/k)$ est de cardinal $[k(P) : k]$.*

Démonstration. L'idée est de se ramener au cas affine. Soient $[c_0 \colon c_1 \colon c_2] = P$. On peut supposer sans perte de généralité que $c_2 \neq 0$. Soit alors $\varphi \colon \mathbb{A}^2(\bar{k}) \longrightarrow \mathbb{P}^2\big(\bar{k}\big)$ le plongement $(a, b) \longmapsto [a, b, 1]$. On a alors $P = \varphi(c_0/c_2, c_1/c_2)$, $k(P) = k(c_0/c_2, c_1/c_2)$. Comme φ est de plus $\mathrm{Gal}(\bar{k}/k)$-invariant, on conclut à l'aide du lemme 2.1.2 analogue pour le cas affine. □

On en déduit immédiatement la

Proposition 2.1.5. *Soit $F \in \mathbb{F}_q[x_0, x_1, x_2]$ un polynôme homogène tel que la courbe projective associée X_F soit non singulière. Pour $d \in \mathbb{N}^*$, notons b_d le nombre d'orbites de cardinal d de $X_F(\overline{\mathbb{F}_q})$ sous $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, et pour $n \in \mathbb{N}^*$, soit $N_n = |X_F(\mathbb{F}_{q^n})|$ le nombre de points $\mathbb{F}_{q^n}$-rationnels de X_F. Alors on a la relation*

$$N_n = \sum_{d|n} d\, b_d.$$

2.2 Définition des fonctions zêta

Commençons par le cas affine. Considérons un polynôme absolument irréductible $f \in \mathbb{F}_q[x, y]$, définissant une courbe affine Z_f dont l'anneau des fonctions régulières est $C_f = \mathbb{F}_q[x, y]/(f)$. Supposons de plus que Z_f soit non singulière. On sait alors que C_f est un anneau de Dedekind à quotients finis. Par analogie avec les fonctions ζ de Dedekind des corps de nombres, posons (pour l'instant formellement)

$$\zeta(Z_f/\mathbb{F}_q, s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{\|\mathfrak{a}\|^s} = \prod_{\substack{\mathfrak{p} \in \mathrm{Spec}(C_f) \\ \mathfrak{p} \neq 0}} \frac{1}{1 - \frac{1}{\|\mathfrak{p}\|^s}}$$

où la somme porte bien entendu sur les idéaux non-nuls $\mathfrak{a}$ de l'anneau C_f.

Pour $d \in \mathbb{N}^*$, soit b_d le nombre d'idéaux premiers $\mathfrak{p} \in Z_f$ dont le corps résiduel est de degré exactement d sur k. Ce nombre est toujours fini d'après la proposition 2.1.3. On a alors

$$\zeta(Z_f/\mathbb{F}_q, s) = \prod_{d=1}^{+\infty} \left(1 - \frac{1}{q^{ds}}\right)^{-b_d}.$$

Par conséquent, en définissant $T = q^{-s}$, et en posant

$$Z(Z_f/\mathbb{F}_q, T) = \prod_{d=1}^{+\infty} (1 - T^d)^{-b_d},$$

le produit étant convergent dans $\mathbb{Q}[[T]]$, on a $\zeta(Z_f/\mathbb{F}_q, s) = Z(Z_f/\mathbb{F}_q, T)$.

La variable $T = q^{-s}$ se révélant à l'usage plus pratique que s, c'est elle que nous utiliserons dorénavant. Nous noterons $Z(T)$ et non pas $\zeta(T)$ les fonctions zêta, afin d'éviter toute confusion.

En passant au logarithme dans $\mathbb{Q}[[T]]$, nous obtenons

$$\log(Z(Z_f/\mathbb{F}_q, T)) = -\sum_{d=1}^{+\infty} b_d \log(1-T^d) = \sum_{d=1}^{+\infty} b_d \sum_{i=1}^{+\infty} \frac{T^{di}}{i} = \sum_{n=1}^{+\infty} \left(\sum_{d|n} d b_d\right) \frac{T^n}{n}.$$

Or la proposition 2.1.3 nous dit que $\sum_{d|n} d b_d = N_n$, où $N_n = |Z_f(\mathbb{F}_{q^n})|$ est le nombre de points $\mathbb{F}_{q^n}$-rationnels de Z_f. Nous sommes donc conduits à définir

Définition 2.2.1. La *fonction zêta* sur $\mathbb{F}_q$ de la courbe affine Z_f est la série formelle

$$Z(Z_f/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} N_n \frac{T^n}{n}\right) \in \mathbb{Q}[[T]].$$

Exemple 2.2.2. Puisque $|\mathbb{A}^1(\mathbb{F}_{q^n})| = q^n$,

$$Z(\mathbb{A}^1/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} q^n \frac{T^n}{n}\right) = \exp(-\log(1 - qT)) = \frac{1}{1 - qT}.$$

Exemple 2.2.3. Pour $p \neq 2$, soit $f(x,y) = x^2 + y^2 - 1 \in \mathbb{F}_q[x,y]$. Homogénéisons f en $F(x_0,x_1,x_2) = x_0^2 + x_1^2 - x_2^2$. Alors X_F est une conique non singulière, $X_F(\mathbb{F}_{q^n})$ n'est jamais vide puisqu'il contient au moins le point $[1:0:0]$, et par conséquent la méthode standard consistant à couper X_F par les droites passant par ce point fournit un bijection entre $X_F(\mathbb{F}_{q^n})$ et $\mathbb{P}^1(\mathbb{F}_{q^n})$; en particulier, $|X_F(\mathbb{F}_{q^n})| = q^n + 1$. Soit $i \in \bar{k}$ tel que $i^2 = -1$. Les points à l'infini de X_F sont $[1:i:0]$ et $[1:-i:0]$. Par conséquent,

- si $i \in \mathbb{F}_q$, alors $N_n = Z_f(F_{q^n}) = q^n - 1$, donc

$$Z(Z_f/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty}(q^n - 1)\frac{T^n}{n}\right) = \exp\left(\sum_{n=1}^{+\infty} q^n\frac{T^n}{n} - \sum_{n=1}^{+\infty}\frac{T^n}{n}\right) = \frac{1-T}{1-qT},$$

  tandis que

- si $i \notin \mathbb{F}_q$, alors $i \in \mathbb{F}_{q^n}$ si et seulement si n est pair, donc $N_n = q^n + (-1)^{n+1}$, si bien que

$$Z(Z_f/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} q^n\frac{T^n}{n} + \sum_{n=1}^{+\infty}(-1)^{n+1}\frac{T^n}{n}\right) = \frac{1+T}{1-qT}.$$

Passons à présent au cas projectif. Par analogie avec le cas précédent, définissons

Définition 2.2.4. Soient $F \in \mathbb{F}_q[x_0,x_1,x_2]$ un polynôme homogène, X_F la courbe projective associée, et $N_n = |X_F(\mathbb{F}_{q^n})|$. la *fonction zêta* sur $\mathbb{F}_q$ de X_F est la série formelle

$$Z(X_F/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} N_n\frac{T^n}{n}\right) \in \mathbb{Q}[[T]].$$

Exemple 2.2.5. Pour $p \neq 2$, soit $F(x_0,x_1,x_2) = x_0^2 + x_1^2 - x_2^2$. Nous avons montré plus haut que $N_n = q^n + 1$, par conséquent,

$$Z(Z_f/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty}(q^n + 1)\frac{T^n}{n}\right) = \exp\left(\sum_{n=1}^{+\infty} q^n\frac{T^n}{n} + \sum_{n=1}^{+\infty}\frac{T^n}{n}\right) = \frac{1}{(1-qT)(1-T)}.$$

Supposons X_F non singulière. Nous savons alors par le lemme 2.1.4 que le degré d'un point $P \in X_F(\overline{\mathbb{F}_q})$ est égal au cardinal de son orbite sous l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}_q}, \mathbb{F}_q)$. Soit b_d le nombre d'orbites de cardinal d sous $\mathrm{Gal}(\overline{\mathbb{F}_q}, \mathbb{F}_q)$. Puisque $N_n = \sum_{d|n} d\, b_d$ d'après la proposition 2.1.5, nous trouvons comme dans le cas affine que

Fait 2.2.6.

$$Z(X_F/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} N_n \frac{T^n}{n}\right) = \prod_{v \in X_F(\overline{\mathbb{F}_q})/\operatorname{Gal}(\overline{\mathbb{F}_q},\mathbb{F}_q)} \frac{1}{1-T^{|v|}}.$$

Corollaire 2.2.7. *Supposons que F soit l'homogénéisé de $f \in \mathbb{F}_q[x,y]$, c'est à dire que $f(x,y) = F(x,y,1)$. Soient $v_1, \cdots, v_r$ les orbites des points à l'infini de Z_f sous $\operatorname{Gal}(\overline{\mathbb{F}_q}, \mathbb{F}_q)$. Alors les fonctions zêta de Z_f et de X_F sont reliées par*

$$Z(X_F/\mathbb{F}_q, T) = Z(Z_f/\mathbb{F}_q, T) \prod_{i=1}^{r} \frac{1}{1-T^{|v_i|}}.$$

Passons enfin au cas des courbes non singulières complètes.

Définition 2.2.8. La *fonction zêta* d'une courbe non singulière complète $X/\mathbb{F}_q$ est la série formelle

$$Z(X/\mathbb{F}_q, T) = \prod_{P \in X} \frac{1}{1-T^{\deg(P)}} \in \mathbb{Q}[[T]].$$

Cette fois, soit b_d le nombre de points $P \in X$ dont le corps résiduel est $\mathbb{F}_{q^d}$, et soit $N_n = |X(F_{q^n})|$. On montre comme pour les deux cas précédents que $N_n = \sum_{d|n} d\, b_d$, et, comme dans les deux cas précédents, on en conclut que

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} N_n \frac{T^n}{n}\right).$$

Avant de clore cette introduction aux fonctions zêta, indiquons comment ces fonctions se comporte lorsqu'on étend le corps de base, c'est-à-dire lorsqu'on remplace $\mathbb{F}_q$ par $\mathbb{F}_{q^e}$ et qu'on voit les courbes sur $\mathbb{F}_q$ comme des courbes sur $\mathbb{F}_{q^e}$. La réponse à cette question est le lemme classique sur les séries lacunaires suivant :

Lemme 2.2.9. *Soit $f(T) = \sum_{n=0}^{+\infty} a_n T^n \in \mathbb{C}[[T]]$ une série formelle à coefficients complexes. Pour tout entier naturel non nul $e \in \mathbb{N}^*$, la* série lacunaire *$f_e(T) = \sum_{n=0}^{+\infty} a_{en} T^{en}$ obtenue en ne conservant que les termes d'indice multiple de e s'obtient par la formule*

$$f_e(T) = \frac{1}{e} \sum_{l=1}^{e} f\left(\exp\left(\frac{2l\pi i}{e}\right) T\right).$$

Démonstration. On a en effet

$$\sum_{l=1}^{e} f\left(\exp\left(\frac{2l\pi i}{e}\right)T\right) = \sum_{n=0}^{+\infty} a_n \left(\sum_{l=1}^{e} \exp\left(\frac{2nl\pi i}{e}\right)\right) T^n = \sum_{n=0}^{+\infty} a_{en} e T^{en} + 0.$$

□

On en déduit immédiatement l'application au cas qui nous intéresse, à savoir la relation

Corollaire 2.2.10.

$$Z(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e) = \prod_{l=1}^{e} Z\left(X/\mathbb{F}_q, \exp\left(\frac{2l\pi i}{e}\right)T\right).$$

Démonstration. Notons comme d'habitude $N_n = |X(F_{q^n})|$. Alors

$$Z(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T) = \exp\left(\sum_{n=1}^{+\infty} N_{en}\frac{T^n}{n}\right),$$

donc

$$\log(Z(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e)) = \sum_{n=1}^{+\infty} N_{en}\frac{T^{en}}{n} = e\sum_{n=1}^{+\infty} N_{en}\frac{T^{en}}{en} = \sum_{l=1}^{e} \log\left(Z\left(X/\mathbb{F}_q, \exp\left(\frac{2l\pi i}{e}\right)T\right)\right).$$

□

2.3 Rationalité de la fonction zêta

Le lecteur aura pu remarquer que, dans les exemples de calculs précédents, les fonctions zêta se sont toujours révélées être des fractions rationnelles en T, dont le dénominateur était un diviseur de $(1-T)(1-qT)$. Il se trouve que ce fait est général, et en fait, on peut même être beaucoup plus précis ; c'est que que nous allons voir à présent. Ceci constituera par ailleurs une première application du théorème de Riemann-Roch.

Commençons par voir ce que ce théorème peut faire pour nous. Soit $X/\mathbb{F}_q$ une courbe non singulière complète de genre g. Pour chaque classe $\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)$, notons

$$E_{\mathcal{L}} = \{D \in \mathrm{Eff}(X/\mathbb{F}_q) \mid \mathrm{cl}(D) = \mathcal{L}\} = \mathcal{L} \cap \mathrm{Eff}(X/\mathbb{F}_q).$$

Grâce à Riemann-Roch, nous pouvons calculer le cardinal de $E_{\mathcal{L}}$ si $\mathcal{L}$ est de degré assez grand :

Proposition 2.3.1. *Si* $\deg(\mathcal{L}) \geqslant g$*, alors le cardinal de* $E_{\mathcal{L}}$ *est donné par*

$$|E_{\mathcal{L}}| = \frac{q^{h^0(\mathcal{L})} - 1}{q - 1};$$

en particulier, si $\deg(\mathcal{L}) \geq 2g - 1$*, alors*

$$|E_{\mathcal{L}}| = \frac{q^{\deg(\mathcal{L})+1-g} - 1}{q - 1}.$$

Démonstration. D'après le corollaire 1.3.7 au théorème de Riemann-Roch, $E_{\mathcal{L}}$ n'est pas vide. Soit $D \in E_{\mathcal{L}}$. Par définition de $E_{\mathcal{L}}$, on a une surjection

$$\begin{array}{rcl} H^0(D) \setminus \{0\} & \longrightarrow & E_{\mathcal{L}} \\ \alpha & \longmapsto & \operatorname{div}(\alpha) + D \end{array},$$

dont il est clair qu'elle se factorise par l'action de $\mathbb{F}_q^*$ sur $H^0(D) \setminus \{0\}$ par multiplication. Montrons que l'application $(H^0(D) \setminus \{0\})/\mathbb{F}_q^* \longrightarrow E_{\mathcal{L}}$ ainsi obtenue est aussi injective : Si $\operatorname{div}(\alpha) + D = \operatorname{div}(\beta) + D$, alors $\operatorname{div}(\beta/\alpha) = 0$, donc $\beta/\alpha = c \in \mathbb{F}_q^*$ est constante d'après la proposition 1.1.12, c'est-à-dire que $\beta = c\alpha$. On en déduit que

$$|E_{\mathcal{L}}| = \frac{|H^0(D) \setminus \{0\}|}{q - 1} = \frac{q^{h^0(D)} - 1}{q - 1}.$$

Si $\deg(\mathcal{L}) \geq 2g - 1$, alors le corollaire 1.3.4 du théorème de Riemann-Roch nous dit justement que $h^0(D) = h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g$. □

Théorème 2.3.2. *Soit* $X/\mathbb{F}_q$ *une courbe non singulière complète de genre* g*. Alors sa fonction zêta est de forme*

$$Z(X/\mathbb{F}_q, T) = \frac{f(T)}{(1 - T)(1 - qT)},$$

où $f \in \mathbb{Z}_{2g}[T]$ *est un polynôme de degré au plus* $2g$ *à coefficients entiers.*
De plus, $Z(X/\mathbb{F}_q, T)$ *a un pôle simple en* $T = 1$*, de résidu*

$$\lim_{T \to 1} (T - 1) Z(X/\mathbb{F}_q, T) = \frac{h}{q - 1},$$

où $h = |\operatorname{Pic}^0(X/\mathbb{F}_q)|$ *est le nombre de classes.*

Démonstration. La clé de cette démonstration étant le théorème de Riemann-Roch, commençons par exprimer la fonction zêta en termes de diviseurs :

$$Z(X/\mathbb{F}_q, T) = \prod_{P \in X} \frac{1}{1 - T^{\deg(P)}} = \sum_{D \in \mathrm{Eff}(X/\mathbb{F}_q)} T^{\deg(D)}.$$

En regroupant les termes, nous obtenons

$$Z(X/\mathbb{F}_q, T) = \sum_{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)} \sum_{D \in E_{\mathcal{L}}} T^{\deg(\mathcal{L})} = \sum_{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})}.$$

Nous savons grâce au théorème 1.3.8 que le morphisme $\deg\colon \mathrm{Pic}(X/\mathbb{F}_q) \longrightarrow \mathbb{Z}$ a un noyau fini $\mathrm{Pic}^0(X/\mathbb{F}_q)$ d'ordre h ; par conséquent, pour tout $d \in \mathbb{N}$, la fibre

$$\mathrm{Pic}^d(X/\mathbb{F}_q) = \{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q) \mid \deg(\mathcal{L}) = d\}$$

est soit de cardinal h, soit vide selon si d est dans l'image de deg ou non. Soit donc $e \in \mathbb{N}^*$ l'unique entier tel que l'image de deg soit $e\mathbb{Z}$, de sorte que

$$\begin{aligned} Z(X/\mathbb{F}_q, T) &= \sum_{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} \\ &= \sum_{\substack{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L}) \leqslant 2g-2}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} + \sum_{\substack{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L}) \geqslant 2g-1}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} \\ &= \sum_{\substack{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L}) \leqslant 2g-2 \\ e \mid \deg(\mathcal{L})}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} + \sum_{\substack{d \\ de \geqslant 2g-1}} h \frac{q^{de+1-g} - 1}{q-1} T^{de}. \end{aligned}$$

Comme $\mathrm{Eff}^d(X)$, donc $E_{\mathcal{L}}$, sont toujours finis (voir la preuve du théorème 1.3.8), le premier terme est un polynôme en T^e, de degré au plus $2g-2$ en T, et à coefficients entiers ; quant au second, il vaut, en appelant d_0 le plus petit entier tel que $d_0 e \geqslant 2g-1$,

$$\begin{aligned} \frac{h}{q-1} \sum_{d=d_0}^{+\infty} (q^{de+1-g} - 1) T^{de} &= \frac{h}{q-1} \left(q^{d_0 e+1-g} T^{d_0 e} \sum_{d=0}^{+\infty} (qT)^{de} - T^{d_0 e} \sum_{d=0}^{+\infty} T^{de} \right) \\ &= \frac{h}{q-1} \left(\frac{q^{d_0 e+1-g} T^{d_0 e}}{1 - q^e T^e} - \frac{T^{d_0 e}}{1 - T^e} \right) \quad (\star) \\ &= h \frac{u(T^e)}{(1 - q^e T^e)(1 - T^e)} \end{aligned}$$

où u est un polynôme de degré au plus $2g$ à coefficients entiers. Ainsi,

$$Z(X/\mathbb{F}_q, T) = \frac{f(T^e)}{(1-q^eT^e)(1-T^e)},$$

où f est un polynôme de degré au plus $2g$ à coefficients entiers. De plus, $(\star)$ montre que $Z(X/\mathbb{F}_q, T)$ a un pôle simple en $T = 1$, de résidu

$$\lim_{T\to 1}(T-1)Z(X/\mathbb{F}_q, T) = \frac{h}{(q-1)e}.$$

Pour conclure, il ne reste donc plus qu'à montrer que $e = 1$, c'est-à-dire que $\deg\colon \mathrm{Pic}(X/\mathbb{F}_q) \longrightarrow \mathbb{Z}$ est surjectif. Ceci peut justement se faire en utilisant les fonctions zêta : considérons la courbe $X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}$ obtenue à partir de $X/\mathbb{F}_q$ par changement de base. D'après le corollaire 2.2.10, sa fonction zêta est

$$Z(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e) = \prod_{l=1}^{e} Z\left(X/\mathbb{F}_q, \exp\left(\frac{2l\pi i}{e}\right)T\right) = Z(X/\mathbb{F}_q, T)^e$$

puisque $Z(X/\mathbb{F}_q, T)$ est une fraction rationnelle en T^e. Or le membre de gauche a un pôle d'ordre 1 en $T = 1$ puisque $T \mapsto T^e$ est un biholomorphisme local en $T = 1$, tandis que le membre de droite y a un pôle d'ordre e. On en déduit que $e = 1$, ce qui termine la preuve. □

Puisque $Z(X/\mathbb{F}_q, 0) = 1$, on a $f(0) = 1$; par conséquent, f se factorise en

$$f(T) = \prod_{i=1}^{2g}(1-\omega_i T)$$

dans $\overline{\mathbb{Q}}[T]$, quitte à prendre certains ω_i nuls si jamais $\deg f < 2g$. Comme $f(0) = 1$, le polynôme réciproque de f, dont les ω_i non nuls sont racines, est unitaire, donc les ω_i sont des entiers algébriques. En regardant le résidu en $T = 1$, on en déduit le

Corollaire 2.3.3. $|\mathrm{Pic}^0(X/\mathbb{F}_q)| = h = f(1) = \prod_{i=1}^{2g}(1-\omega_i)$.

Cette formule explique l'intérêt des ω_i, nous en reparlerons plus tard.

Avant de clore cette section, notons pour mémoire que nous avons prouvé le

Théorème 2.3.4. *Le morphisme* $\deg\colon \mathrm{Pic}(X) \longrightarrow \mathbb{Z}$ *est surjectif.*

2.4 L'équation fonctionnelle

Dans le paragraphe précédent, nous avons démontré que la fonction zêta d'une courbe non singulière complète était une fonction rationnelle, en ne nous appuyant que sur un corollaire du théorème de Riemann-Roch. Nous allons à présent utiliser le théorème de Riemann-Roch lui-même dans toute sa puissance afin d'établir une équation fonctionnelle vérifiée par la fonction zêta, à l'instar des fonctions zêta des corps de nombres. Celles-ci vérifient en effet une célèbre équation reliant $\zeta(s)$ à $\zeta(1-s)$; puisque nous avons choisi d'utiliser la variable $T = q^{-s}$, il semble logique que l'équation fonctionnelle que nous recherchons relie $Z(T)$ à $Z(1/qT)$, et c'est effectivement ce qui se produit.

Théorème 2.4.1. *Soit $X/\mathbb{F}_q$ une courbe non singulière complète de genre g, et soit*

$$Z(X/\mathbb{F}_q, T) = \frac{f(T)}{(1-T)(1-qT)}$$

sa fonction zêta. Alors f est de degré exactement $2g$, son coefficient dominant est q^g, et l'équation fonctionnelle suivante est satisfaite :

$$Z\left(X/\mathbb{F}_q, \frac{1}{qT}\right) = (qT^2)^{1-g} Z(X/\mathbb{F}_q, T).$$

Démonstration. Exprimons la fonction zêta

$$Z(X/\mathbb{F}_q, T) = \sum_{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} = \frac{1}{q-1}(\alpha(T) + \beta(T))$$

comme combinaison linéaire des deux termes

$$\begin{aligned} \alpha(T) &= \sum_{0 \leqslant \deg(\mathcal{L}) \leqslant 2g-2} q^{h^0(\mathcal{L})} T^{\deg(\mathcal{L})}, \\ \beta(T) &= \sum_{\deg(\mathcal{L}) \geqslant 2g-1} q^{h^0(\mathcal{L})} T^{\deg(\mathcal{L})} - \sum_{\deg(\mathcal{L}) \geqslant 0} T^{\deg(\mathcal{L})}, \end{aligned}$$

et montrons que chacun de ces deux termes vérifie l'équation fonctionnelle.

D'après le corollaire 1.3.4 de Riemann-Roch et le théorème 2.3.4 sur la

surjectivité du degré, on a

$$\begin{aligned}\beta(T) &= h\sum_{d\geqslant 2g-1} q^{d+1-g}T^d - h\sum_{d\geqslant 0} T^d \\ &= hq^{1-g}(qT)^{2g-1}\sum_{d\geqslant 0}(qT)^d - \frac{h}{1-T} \\ &= h\left(\frac{q^gT^{2g-1}}{1-qT} - \frac{1}{1-T}\right),\end{aligned}$$

et il est alors facile de vérifier que $\beta(T)$ satisfait l'équation fonctionnelle.

Passons donc à $\alpha(T)$. On a une bijection

$$\begin{array}{ccc}\bigsqcup_{d=0}^{2g-2}\mathrm{Pic}^d(X/\mathbb{F}_q) & \xrightarrow{\sim} & \bigsqcup_{d=0}^{2g-2}\mathrm{Pic}^d(X/\mathbb{F}_q) \\ \mathcal{L} & \longmapsto & \mathcal{K}-\mathcal{L}\end{array},$$

où $\mathcal{K} = \mathrm{cl}(K)$ est la classe du diviseur canonique. Par conséquent,

$$\alpha(T) = \sum_{0\leqslant\deg(\mathcal{L})\leqslant 2g-2} q^{h^0(\mathcal{K}-\mathcal{L})}T^{\deg(\mathcal{K}-\mathcal{L})}.$$

Or le théorème de Riemann-Roch 1.3.3 nous dit que $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g + h^0(\mathcal{K}-\mathcal{L})$, et donc

$$\begin{aligned}\alpha(T) &= \sum_{0\leqslant\deg(\mathcal{L})\leqslant 2g-2} q^{h^0(\mathcal{L})-\deg(\mathcal{L})-1+g}\; T^{\deg(\mathcal{K})-\deg(\mathcal{L})} \\ &= \sum_{0\leqslant\deg(\mathcal{L})\leqslant 2g-2} q^{g-1}\,T^{\deg(\mathcal{K})}\,q^{h^0(\mathcal{L})}\,(qT)^{-\deg(\mathcal{L})} \\ &= q^{g-1}\,T^{2g-2}\,\alpha\left(\frac{1}{qT}\right).\end{aligned}$$

L'équation fonctionnelle étant ainsi prouvée, on vérifie, en comparant les équivalents lorsque $T\to+\infty$, que f est de degré exactement $2g$, le coefficient dominant valant $\prod_{i=1}^{2g}\omega_i = q^g$. □

2.5 L'hypothèse de Riemann

Considérons une courbe non singulière complète $X/\mathbb{F}_q$ de genre g, de fonction zêta

$$Z(X/\mathbb{F}_q,T) = \frac{\prod_{i=1}^{2g}(1-\omega_iT)}{(1-T)(1-qT)}.$$

Nous avons déjà établi la formule

$$h = \prod_{i=1}^{2g}(1-\omega_i)$$

donnant le nombre de classes $h = |\operatorname{Pic}^0(X/\mathbb{F}_q)|$ en fonction des ω_i. Voici une autre formule formule faisant intervenir les ω_i :

Proposition 2.5.1. *Les nombres $N_n = |X(\mathbb{F}_{q^n})|$ sont donnés par*

$$N_n = q^n + 1 - \sum_{i=1}^{2g}\omega_i^n.$$

Démonstration. Par définition, on a

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} N_n \frac{T^n}{n}\right),$$

mais d'autre part

$$\begin{aligned}
\log\left(Z(X/\mathbb{F}_q, T)\right) &= \log\left(\frac{\prod_{i=1}^{2g}(1-\omega_i T)}{(1-T)(1-qT)}\right) \\
&= \sum_{i=1}^{2g}\log(1-\omega_i T) - \log(1-T) - \log(1-qT) \\
&= \sum_{n=1}^{+\infty}\left(-\sum_{i=1}^{2g}\omega_i^n + 1 + q^n\right)\frac{T^n}{n}.
\end{aligned}$$

□

Il serait donc particulièrement intéressant de disposer d'informations sur les ω_i. Ces nombres étant les inverses des zéros de la fonction $Z(X/\mathbb{F}_q, T)$, on pense bien évidemment à un analogue de l'hypothèse de Riemann pour les fonctions ζ de Dedekind, qui prédit que les zéros non-triviaux desdites fonctions sont de partie réelle $1/2$. Dans notre cas, en termes de $T = q^{-s}$, ceci se traduit par la version suivante de l'hypothèse de Riemann :

Théorème 2.5.2 (Hypothèse de Riemann pour les courbes sur les corps finis)**.** *Soit $X/\mathbb{F}_q$ une courbe non singulière complète de genre g, et soit*

$$Z(X/\mathbb{F}_q, T) = \frac{\prod_{i=1}^{2g}(1-\omega_i T)}{(1-T)(1-qT)}$$

sa fonction zêta. Alors

$$\forall 1 \leqslant i \leqslant n, \quad |\omega_i|_{\mathbb{C}} = \sqrt{q}.$$

Remarquons que ceci est compatible avec le théorème 2.4.1, qui affirme (entre autres) que le produit des ω_i vaut q^g.

Il se trouve que, contrairement au cas des corps de nombres, on sait démontrer l'hypothèse de Riemann pour les courbes sur les corps finis ; c'est ce à quoi nous allons à présent nous attacher, après avoir donné quelques exemples d'applications de l'hypothèse de Riemann au préalable.

Corollaire 2.5.3. *Pour le nombres de classes $h = |\operatorname{Pic}^0(X/\mathbb{F}_q)|$, on a l'estimation*

$$(\sqrt{q}-1)^{2g} \leqslant h \leqslant (\sqrt{q}+1)^{2g}.$$

Démonstration. En effet, $h = \prod_{i=1}^{2g}(1-\omega_i) = \left|\prod_{i=1}^{2g}(1-\omega_i)\right|$. □

On retrouve ainsi le fait que la droite projective $\mathbb{P}^1_k$ n'a qu'une seule classe.

Corollaire 2.5.4. *Pour tout $n \in \mathbb{N}^*$, le nombre de points $\mathbb{F}_{q^n}$-rationnels $N_n = |X(\mathbb{F}_{q^n})|$ vérifie*

$$|N_n - (q^n+1)| \leqslant 2g\sqrt{q^n}.$$

Démonstration. Ceci provient directement de la proposition 2.5.1. □

Exemple 2.5.5. Soit $F \in \mathbb{F}_q[x_0, x_1, x_2]$ un polynôme homogène de degré 3, et soit X_F la courbe associée. Supposons que X_F soit non singulière, et soit $N_1 = |X_F(\mathbb{F}_q)|$. D'après le théorème 1.4.3, le genre de X_F est $g = \frac{(3-1)(3-2)}{2} = 1$, et comme $\omega_1 + \omega_2 = N_1 - q - 1$, la fonction zêta de X_F est

$$Z(X_F/\mathbb{F}_q, T) = \frac{1 + (N_1 - q - 1)T + qT^2}{(1-T)(1-qT)}.$$

On vérifie alors que l'équation fonctionnelle $Z(X_F/\mathbb{F}_q, T) = Z(X_F/\mathbb{F}_q, 1/qT)$ est satisfaite.

D'après le corollaire 2.5.4, le nombre de points $\mathbb{F}_q$-rationnels de X_F vérifie $|N_1 - (q+1)| \leqslant 2\sqrt{q}$, résultat connu sous le nom de théorème de Hasse. En particulier, une cubique non singulière sur un corps fini a toujours au moins un point rationnel, car sinon on aurait $q + 1 \leqslant 2\sqrt{q}$, d'où $(\sqrt{q} - 1)^2 \leqslant 0$, ce qui est impossible puisque $q \geqslant 2$.

Si $N_1 = q + 1$, milieu de la fourchette du théorème de Hasse qui est par exemple réalisé pour $p = q = 2$ et $F(x_0, x_1, x_2) = x_0^3 + x_1^3 + x_2^3$, alors $\omega_1 + \omega_2 = 0$, donc $\omega_1 = \sqrt{q}$ et $\omega_2 = -\sqrt{q}$, et par conséquent $N_{2m} = |X_F(\mathbb{F}_{q^{2m}})| = q^{2m} + 1 + \omega_1^m + \omega_2^m = (q^m + 1)^2$, et $N_{2m+1} = |X_F(\mathbb{F}_{q^{2m+1}})| = q^{2m+1} + 1$. On constate ainsi que la borne supérieure $N_n - (q^n + 1) \leqslant 2\sqrt{q^n}$ prédite par l'hypothèse de Riemann est atteinte pour tous les valeurs paires de n dans ce cas.

Enfin, dans le cas particulier $p = q = 2$, le corollaire 2.5.3 nous dit que le nombre de classes h vaut au plus 5.

Exemple 2.5.6. Soit $F(x_0, x_1, x_2) = x_0^4 + x_1^4 + x_2^4 \in \mathbb{F}_3[x_0, x_1, x_2]$. La courbe projective X_F est non singulière de genre 3, et l'hypothèse de Riemann affirme que le nombre de points $\mathbb{F}_9$-rationnels de X_F est au plus 28. On peut facilement vérifier qu'il est en fait exactement égal à 28.

Après cet aperçu de la puissance de l'hypothèse de Riemann, tâchons de la prouver. La démonstration que nous donnerons est celle, assez élémentaire, exposée par Bombieri en 1972 dans [Bom74]. Pour commencer, remarquons qu'il suffit de prouver la version plus faible suivante :

Lemme 2.5.7. *S'il existe un entier $e \in \mathbb{N}^*$ tel que, lorsque $n \to +\infty$,*

$$|N_{en} - (q^{en+1} + 1)| = \left| \sum_{i=1}^{2g} \omega_i^{en} \right| = \mathcal{O}\left(\sqrt{q^{en}}\right),$$

alors l'hypothèse de Riemann 2.5.2 est vérifiée.

Pour ce faire, nous aurons besoin du petit lemme élémentaire suivant :

Lemme 2.5.8. *Notons $\mathbb{S}^1$ le cercle unité*

$$\mathbb{S}^1 = \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\}$$

du plan complexe. Soient $\lambda_1, \cdots, \lambda_s \in \mathbb{S}^1$ des nombres complexes de module 1. Pour tout $\varepsilon > 0$, il existe des entiers arbitrairement grands $n \in \mathbb{N}$ tels que

$$\left| \sum_{i=1}^{s} \lambda_i^n \right| > s - \varepsilon.$$

Démonstration. Pour tout entier $n \in \mathbb{N}$, posons $\Lambda_n = (\lambda_1^n, \cdots, \lambda_s^n) \in (\mathbb{S}^1)^n$. Comme $(\mathbb{S}^1)^n$ est un espace métrique compact, on peut extraire de la suite $(\Lambda_n)_{n\in\mathbb{N}}$ une sous-suite convergente $(\Lambda_{n_k})_{k\in\mathbb{N}}$. Quitte à ré-extraire, on peut supposer que lorsque $k \to +\infty$, $n_{k+1} - n_k$ croit vers $+\infty$. Alors $\Lambda_{n_{k+1}-n_k}$ converge vers $(1, \cdots, 1)$, d'où le résultat. □

Démonstration du lemme 2.5.7. On peut supposer les ω_i rangés par ordre de module croissant. Soit $s < 2g$ l'entier tel que

$$|\omega_{2g}| = \cdots = |\omega_{s+1}| > |\omega_s|.$$

D'après le lemme élémentaire 2.5.8, pour tout $\varepsilon > 0$, il existe des entiers $n \in \mathbb{N}$ arbitrairement grands tels que

$$\left| \sum_{i=1}^{2g} \omega_i^{en} \right| \geqslant \left| \sum_{i=s+1}^{2g} \omega_i^{en} \right| - \left| \sum_{i=1}^{s} \omega_i^{en} \right| \geqslant (2g - s - \varepsilon)|\omega_{2g}|^{en} - s|\omega_s|^{en} \geqslant (1 - 2\varepsilon)|\omega_{2g}|^{en},$$

puisque $s|\omega_s|^{en} \leqslant \varepsilon s|\omega_{2g}|^{en}$ pour n assez grand. Par conséquent, l'hypothèse implique l'existence d'une constante $C > 0$ telle que, pour des valeurs arbitrairement grandes de n, $|\omega_{2g}|^{dn} \leqslant C\sqrt{q^{en}}$, donc on a $|\omega_{2g}| \leqslant \sqrt{q}$. Mais comme le produit des ω_i vaut q^g d'après le théorème 2.4.1, ceci conclut. □

Nous devons donc nous assurer que les hypothèses du lemme 2.5.7 sont vérifiées. Il nous faut donc borner $N_{en} - (q^{en+1} + 1)$. La proposition suivante fournit la majoration :

Proposition 2.5.9 (Borne supérieure)**.** *Soit X une courbe non singulière complète de genre g sur $\mathbb{F}_q$. Si $q = p^\alpha$ avec α pair, et si $q > (g+1)^4$, alors*

$$N_1 < q + 1 + (2g + 1)\sqrt{q}.$$

Démonstration. Soit P un point de X tel que $\mathbb{F}_q(P) = \mathbb{F}_q$ (si un tel point n'existe pas, alors la proposition est vraie !). Pour tout $m \in \mathbb{N}$, notons $H_m = H^0(mP) \subseteq \mathbb{F}_q(X)$ l'espace des fonctions rationnelles définies partout

sauf peut-être en P, et ayant un pôle d'ordre au plus m en P, et notons $h_m = h^0(mP)$ sa dimension sur $\mathbb{F}_q$. Les H_m forment une filtration de $\mathbb{F}_q(X)$, compatibles avec la multiplication au sens où $H_m H_n \subseteq H_{m+n}$.

Considérons un élément $f = \sum_{i=1}^r \nu_i s_i^q$ de $H_l^{p^\mu} H_m^q$, avec $\nu_i \in H_l^{p^\mu}$ et $s_i \in H_m$. Supposons qu'on puisse trouver une telle fonction f qui soit non-nulle, mais telle que la fonction $\delta(f) = \sum_{i=1}^r \nu_i s_i = 0$ soit nulle. Alors, pour tout point $\mathbb{F}_q$-rationnel Q distinct de P, comme $\mathbb{F}_q(Q) = \mathcal{O}_Q/\mathfrak{p}_Q = \mathbb{F}_q$, et comme les ν_i et les s_i sont dans $\mathcal{O}_Q$, on a

$$f = \sum_{i=1}^r \nu_i s_i^q \equiv \sum_{i=1}^r \nu_i s_i = 0 \mod \mathfrak{p}_Q,$$

c'est-à-dire que f s'annule en tous les points $\mathbb{F}_q$-rationnels de X distincts de P. Si de plus $p^\mu < q$, alors f est, comme tout élément de $H_l^{p^\mu} H_m^q$, une puissance p^μ-ième, donc f a au moins $p^\mu(N_1 - 1)$ zéros, comptés avec multiplicité. Mais comme toute fonction a autant de zéros que de pôles d'après le théorème 1.2.2, et comme f au plus $lp^\mu + mq$ pôles (toujours comptés avec multiplicité), on a nécessairement

$$N_1 \leqslant l + mq/p^\mu + 1.$$

Voyons donc comment construire une telle fonction f, puis choisissons soigneusement la valeur des paramètres l, m et μ.

Comme le degré de P vaut 1, on a $h_{m+1} \leqslant h_m + 1$ pour tout m ; par conséquent, on peut trouver une base $(s_i)_{1 \leqslant i \leqslant h_m}$ de H_m adaptée à la filtration, c'est-à-dire telle que pour tout i, $\mathrm{ord}_P(s_i) \geqslant \mathrm{ord}_p(s_{i-1}) + 1$. Comme $p^\mu < q$, $H_m^{p^\mu}$ est un $\mathbb{F}_q$-espace vectoriel, dont il est clair que les $(s_i^{p^\mu})_{1 \leqslant i \leqslant h_m}$ forment une base. Montrons que si $lp^\mu < q$, alors tout élément de $H_l^{p^\mu} H_m^q$ s'écrit d'une unique façon sous la forme $\sum_{i=1}^r \nu_i s_i^q$: s'il existait $\rho \leqslant r$ tel que $\nu_\rho \neq 0$ alors que $\sum_{i=\rho}^r \nu_i s_i^q = 0$, alors on aurait

$$\mathrm{ord}_P(\nu_\rho s_\rho^q) = \mathrm{ord}_P\left(-\sum_{i=\rho+1}^r \nu_i s_i^q\right) \geqslant \min_{i>\rho} \mathrm{ord}_P(\nu_i s_i^q) \geqslant -lp^\mu + q\,\mathrm{ord}_P(s_{\rho+1}),$$

donc $\mathrm{ord}_P(\nu_\rho) \geqslant lp^\mu + q\big(\mathrm{ord}_P(s_{\rho+1}) - \mathrm{ord}_P(s_\rho)\big) \geqslant -lp^\mu + q > 0$, donc ν_ρ serait définie partout, donc constante, et aurait un zéro en P, donc serait nulle, contradiction. Par conséquent, l'application $\mathbb{F}_q$-linéaire

$$\begin{array}{rccc} \delta & : & H_l^{p^\mu} H_m^q & \longrightarrow & H_l^{p^\mu} H_m \\ & & \displaystyle\sum_{i=1}^r \nu_i s_i^q & \longmapsto & \displaystyle\sum_{i=1}^r \nu_i s_i \end{array}$$

est bien définie. De plus, l'unicité de l'écriture $\sum_{i=1}^{r} \nu_i s_i^q$ montre que

$$\dim_{\mathbb{F}_q}(H_l^{p^\mu} H_m^q) = \dim_{\mathbb{F}_q}(H_l^{p^\mu}) \dim_{\mathbb{F}_q}(H_m^q).$$

Comme $H_l^{p^\mu} H_m \subseteq H_{lp^\mu+m}$, on a donc

$$\dim_{\mathbb{F}_q}(\operatorname{Ker}\delta) \geqslant \dim_{\mathbb{F}_q}(H_l^{p^\mu}) \dim(H_m^q) - \dim_{\mathbb{F}_q}(H_{lp^\mu+m}).$$

Or le théorème de Riemann-Roch 1.3.3 nous dit que $\dim_{\mathbb{F}_q}(H_l^{p^\mu}) = \dim_{\mathbb{F}_q}(H_l) = h_l \geqslant l+1-g$, et de même que $\dim(H_m^q) \geqslant m+1-g$, tandis que si $l, m \geqslant g$, on a $lp^\mu + m \geqslant 2g-1$ donc le corollaire 1.3.4 du théorème de Riemann-Roch nous dit que $\dim_{\mathbb{F}_q}(H_{lp^\mu+m}) = h_{lp^\mu+m} = lp^\mu + m + 1 - g$, si bien qu'on finalement

$$\dim_{\mathbb{F}_q}(\operatorname{Ker}\delta) \geqslant (l+1-g)(m+1-g) - (lp^\mu + m + 1 - g)$$

dans ce cas-là.

Prenons alors $\mu = \alpha/2$ et $m = \sqrt{q} + 2g$ (rappelons que α est pair par hypothèse). On a alors bien $p^\mu < q$ et $m \geqslant g$, et on aura $\operatorname{Ker}\delta \neq 0$ si $l > g + g\sqrt{q}/(g+1)$. Pour un tel l, on aura bien $l \geqslant g$. Mais on veut aussi $lp^\mu < q$, c'est-à-dire $l < \sqrt{q}$. On cherche donc un *entier* l tel que $g + g\sqrt{q}/(g+1) < l < \sqrt{q}$. Il en existe si et seulement si $g + g\sqrt{q}/(g+1) + 1 < \sqrt{q}$, c'est-à-dire si $(g+1)^2 < \sqrt{q}$, ce qui est bien le cas par hypothèse. La fonction f recherchée existe donc, et on en déduit que

$$N_1 \leqslant l + mq/p^\mu + 1 < \sqrt{q} + (\sqrt{q} + 2g)\sqrt{q} + 1,$$

ce qui conclut. □

La minoration va, quant à elle, réclamer un peu plus de travail.

Considérons un revêtement galoisien $\pi : X \longrightarrow Y$ de courbes non singulières complètes sur le corps $\mathbb{F}_q$. Notons $G = \operatorname{Gal}\big(\mathbb{F}_q(X)/\mathbb{F}_q(Y)\big)$ le groupe d'automorphismes de ce revêtement. D'un point de vue géométrique, les points au-dessus de $Q \in Y$ correspondent aux idéaux maximaux au-dessus de $\mathfrak{p}_Q$ dans la clôture intégrale de $\mathcal{O}_Q$ dans $\mathbb{F}_q(X)$, et le groupe G permute transitivement ces points ; plus précisément, pour si P est un point de X tel que $\pi(P) = Q$, un automorphisme $\sigma \in G$ envoie les fonctions rationnelles sur X définies en $\sigma(P)$ sur celles définies en P par

$$\sigma^* = \sigma^{-1} : \mathcal{O}_{\sigma(P)} = \sigma(\mathcal{O}_P) \longrightarrow \mathcal{O}_P,$$

le $^{-1}$ assurant que G agit à droite sur $\mathbb{F}_q(X)$. Notons D_P le *sous-groupe de décomposition*, c'est-à-dire le stabilisateur de P sous G, qui est d'ordre $e_P f_P$. Notons aussi G_P le groupe de Galois $G_P = \mathrm{Gal}\left(\mathbb{F}_q(P)/\mathbb{F}_q(Q)\right)$, qui est cyclique d'ordre f_P, engendré par l'*automorphisme de Frobenius* $x \mapsto x^{q\deg(Q)}$. L'automorphisme σ induit aussi un morphisme $\mathbb{F}_q(\sigma(P)) \longrightarrow \mathbb{F}_q(P)$ entre les corps résiduels, d'où un antimorphisme de groupes de D_P dans G_P. Son noyau, le *sous-groupe d'inertie* I_P, est donc d'ordre e_P ; on peut donc définir l'*élément de Frobenius* d'un point non-ramifié $P \in X$ comme l'unique élément de D_P correspondant à l'automorphisme de Frobenius de G_P.

Étendons chaque automorphisme $\sigma \in G$ en un automorphisme $\bar{\sigma}$ de $\overline{X} = X_{\overline{\mathbb{F}_q}}$. Pour tout point $\overline{P} \in \overline{X}$, notons $P \in X$ son image par le quotient par $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Si $\overline{P}$ n'est pas ramifié, on définit l'*élément de Frobenius* en $\overline{P}$ comme étant l'automorphisme $\bar{\sigma}$ tel que σ soit l'élément de Frobenius de P. Étendons aussi π en $\overline{\pi} : \overline{X} \longrightarrow \overline{Y} = Y_{\overline{\mathbb{F}_q}}$, fixons un $\sigma \in G$, et posons

$$\mathcal{N}_1(X/Y, \sigma) = \left\{ \overline{P} \in \overline{X} \;\middle|\; \begin{array}{c} \overline{\pi}(\overline{P}) \in Y(\mathbb{F}_q),\ \overline{P} \text{ est non-ramifié et} \\ \bar{\sigma} \text{ est l'élément de Frobenius en } \overline{P} \end{array} \right\}.$$

Comme les fibres de $\overline{\pi}$ sont finies et que $Y(\mathbb{F}_q)$ est aussi fini, cet ensemble doit lui-même être fini. Nous noterons $N_1(X/Y, \sigma)$ son cardinal. On a alors le

Lemme 2.5.10. *Soit $\pi : X \longrightarrow Y$ un revêtement galoisien de groupes d'automorphismes G de courbes non singulières complètes sur $\mathbb{F}_q$. Pour tout $n \in \mathbb{N}^*$, étendons π en un revêtement galoisien de $X_{\mathbb{F}_{q^n}}$ sur $X_{\mathbb{F}_{q^n}}$. La suite*

$$\left(\sum_{\sigma \in G} N_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}}, \sigma) - |G||Y(\mathbb{F}_{q^n})| \right)_{n \in \mathbb{N}^*}$$

est bornée.

Démonstration. Comme l'élément de Frobenius d'un point non ramifié est unique, on a

$$\sum_{\sigma \in G} N_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}}, \sigma) = |G||U_n|,$$

où $U_n \subseteq Y(\mathbb{F}_{q^n})$ désigne l'ensemble des points $\mathbb{F}_{q^n}$-rationnels non-ramifiés de Y. Mais comme $\overline{\pi}$ est séparable, son lieu de ramification est fini d'après la proposition 1.1.15 ; et le cardinal de celui-ci borne la suite en question. □

L'élévation à la puissance q-ième définit un $\mathbb{F}_q$-endomorphisme de corps Fr^* de $\mathbb{F}_q(X)$. On appelle *endomorphisme de Frobenius* de X est l'endomorphisme Fr de X associé. Cet endomorphisme s'étend en un endomorphisme $\overline{\mathrm{Fr}}$ de $\overline{X}$, $\overline{\mathrm{Fr}}^*$ étant par définition l'endomorphisme de $\overline{\mathbb{F}_q}(\overline{X})$ envoyant $\frac{\sum_i \lambda_i \alpha_i}{\sum_j \lambda_j \alpha_j}$ sur $\frac{\sum_i \lambda_i \alpha_i^q}{\sum_j \lambda_j \alpha_j^q}$, où α_i, $\alpha_j \in \mathbb{F}_q(X)$ et λ_i, $\lambda_j \in \overline{\mathbb{F}_q}$. Si $\overline{P}$ est un point de $\overline{X}$, d'élément de Frobenius $\overline{\sigma}$, il est clair que $\overline{\mathrm{Fr}}(\overline{P}) = \overline{\sigma}(\overline{P})$.

On peut alors énoncer le résultat de borne supérieure suivant :

Proposition 2.5.11. *Soit $\pi : X \longrightarrow Y$ un revêtement galoisien de courbes non singulières complètes sur $\mathbb{F}_q$, et soit $G = \mathrm{Gal}\left(\mathbb{F}_q(X)/\mathbb{F}_q(Y)\right) \subseteq \mathrm{Aut}(X/\mathbb{F}_q)$ le groupe d'automorphismes de ce revêtement. Notons g le genre de X. Si $q = p^\alpha$ avec α pair, et si $q > (g+1)^4$, alors pour tout $\sigma \in G$,*

$$N_1(X/Y, \sigma) \leqslant q + 1 + (2g+1)\sqrt{q}.$$

Démonstration. La démonstration étant très similaire à celle de la borne inférieure 2.5.9, nous serons assez elliptiques et ne détaillerons que les différences entre ces deux preuves.

Soit $\overline{P} \in \overline{X}$ un point dans $\mathcal{N}_1(X/Y, \sigma)$. Rappelons que $\bar{\sigma}(\overline{P}) = \overline{\mathrm{Fr}}(\overline{P})$. Considérons l'endomorphisme $\psi = \sigma^{-1} \circ \mathrm{Fr}$ de X, et étendons le à $\overline{X}$ en $\overline{\psi}$. Il est clair que $\mathcal{N}_1(X/Y, \sigma)$ est contenus dans l'ensemble des points de $\overline{X}$ fixes par $\overline{\psi}$.

Pour tout entier $m \in \mathbb{N}$, posons $H_m = H^0(m\overline{P})$. On a $\overline{\psi}^*(H_m) \subseteq H_{qm}$, donc toute fonction non constante de $\psi^*(H_m)$ a un pôle en $\overline{P}$ et est régulière ailleurs.

Comme $\deg(\overline{P}) = 1$, H_m admet une base $(s_i)_{1 \leqslant i \leqslant r}$ telle que $v_{\overline{P}}(s_{i+1}) \geqslant v_{\overline{P}}(s_i) + 1$ pour tout $i < r$. Comme $\overline{\psi}^*$ est injective, $\left(\overline{\psi}^*(s_i)\right)_{1 \leqslant i \leqslant r}$ est une base de $\overline{\psi}^*(H_m)$. On en déduit que l'application linéaire

$$\begin{array}{rccc} \delta_\sigma & : & \underset{r}{H_l^{p^\mu}} \overline{\psi}^*(H_m) & \longrightarrow & \underset{r}{H_l^{p^\mu}} H_m \\ & & \displaystyle\sum_{i=1} \nu_i \overline{\psi}^*(s_i) & \longmapsto & \displaystyle\sum_{i=1} \nu_i s_i \end{array}$$

est bien définie. Or un élément non nul f de $\mathrm{Ker}\,\delta_\sigma$ s'annule en tous les points $\overline{Q} \in \mathcal{N}_1(X/Y, \sigma) - \{\overline{P}\}$; en effet, les ν_i et les $\overline{\psi}^*(s_i)$ sont dans $\mathcal{O}_{\overline{Q}}$, et $\overline{\psi}^*(s_i) \equiv s_i \mod \mathfrak{p}_{\overline{Q}}$ par définition de l'élément de Frobenius. On vérifie qu'on peut choisir l, m et μ pour que $\mathrm{Ker}\,\delta_\sigma$ ne soit pas réduit à 0, et on conclut comme en 2.5.9. □

Voyons à présent comment utiliser ces deux bornes. Quitte à étendre les scalaires de $\mathbb{F}_q$ à $\mathbb{F}_{q^e}$, nous supposerons dorénavant que $q > (g+1)^4$. Soit X la courbe sur laquelle nous travaillons. Le corollaire 1.1.7 nous assure l'existence d'un morphisme séparable ν de X vers la droite projective $\mathbb{P}^1_{\mathbb{F}_q}$. Si ν était un revêtement galoisien, on pourrait lui appliquer ce qui précède ; comme il n'y a aucune raison pour que ce soit les cas, introduisons la courbe non singulière complète $\widetilde{X}$ sur $\mathbb{F}_q$ telle que $\mathbb{F}_q(\widetilde{X})$ soit la clôture normale de $\mathbb{F}_q(X)$ dans $\mathbb{F}_q(\mathbb{P}^1_{\mathbb{F}_q})$, ce qui peut également nécessiter une extension de scalaires, pour que $\mathbb{F}_q$ demeure algébriquement clos dans $\mathbb{F}_q(\widetilde{X})$. Cette courbe s'accompagne naturellement d'un revêtement galoisien $\pi : \widetilde{X} \longrightarrow X$ de X tel que $\nu \circ \pi$ soit un revêtement galoisien de $\mathbb{P}^1_{\mathbb{F}_q}$. Notons $H = \mathrm{Aut}(\widetilde{X}/X) \subset G = \mathrm{Aut}(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q})$. On a l'inclusion suivante :

Lemme 2.5.12. *Pour tout $\sigma \in H$, on a $\mathcal{N}_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma) \subseteq \mathcal{N}_1(\widetilde{X}/X, \sigma)$.*

Démonstration. Soit $\overline{P} \in \mathcal{N}_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma)$, et notons $P \in \widetilde{X}$ le point correspondant. Par définition, P n'est pas ramifié sur $\mathbb{P}^1_{\mathbb{F}_q}$; il n'est donc pas ramifié sur X non plus. Le sous-groupe de décomposition $D(P)$ associé au revêtement $\nu \circ \pi : \widetilde{X} \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ est le groupe cyclique engendré par σ, donc est inclus dans H ; c'est donc aussi le sous-groupe de décomposition du revêtement $\pi : \widetilde{X} \longrightarrow X$. Par construction, on a

$$\mathbb{F}_q(\mathbb{P}^1_{\mathbb{F}_q}) \subset \mathbb{F}_q(\widetilde{X})^H = \mathbb{F}_q(X) \subset \mathbb{F}_q(\widetilde{X})^{D(P)} \subset \mathbb{F}_q(\widetilde{X}).$$

Notons $Q = \pi(P) \in X$ et $R = \nu(Q) \in \mathbb{P}^1_{\mathbb{F}_q}$. Comme $\mathbb{F}_q(X) \subset \mathbb{F}_q(\widetilde{X})^{D(P)}$, on a $e_{Q/R} = f_{Q/R} = 1$, et comme R est $\mathbb{F}_q$-rationnel par hypothèse, le fait que $f_{Q/R} = 1$ entraîne que Q est aussi $\mathbb{F}_q$-rationnel, d'où le résultat. □

En appliquant le lemme 2.5.10 au revêtement galoisien $\widetilde{X} \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$, on obtient une constante C_1, indépendante du corps de base, telle que

$$\left| \sum_{\sigma \in G} N_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma) - |G|(q+1) \right| \leqslant C_1,$$

d'où l'inégalité

$$N_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma) - (q+1) + \sum_{\substack{\tau \in G \\ \tau \neq \sigma}} \big(N_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \tau) - (q+1) \big) \geqslant -C_1.$$

Or la proposition 2.5.11 appliquée au même revêtement nous dit que

$$N_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma) \leqslant q + 1 + (2g_{\widetilde{X}} + 1)\sqrt{q}\,;$$

par conséquent, on a l'inégalité

$$N_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma) - (q+1) \geqslant -C_1 - (|G| - 1)(2g_{\widetilde{X}} + 1)\sqrt{q} = C_2 + C_3\sqrt{q},$$

où C_2 et C_3 sont indépendantes du corps de base puisque le genre est invariant par extension algébrique des scalaires d'après le théorème 1.4.3.

Le lemme 2.5.10 appliqué cette fois au revêtement galoisien $\pi : \widetilde{X} \longrightarrow X$ nous fournit une constante C_4 indépendante du corps de base telle que

$$\left| \sum_{\sigma \in H} N_1(\widetilde{X}/X, \sigma) - |H||X(\mathbb{F}_q)| \right| \leqslant C_4,$$

d'où la minoration

$$|X(\mathbb{F}_q)| \geqslant -\frac{C_4}{|H|} + \frac{1}{|H|} \sum_{\sigma \in H} N_1(\widetilde{X}/X, \sigma).$$

Mais grâce au lemme 2.5.12, on a, pour tout $\sigma \in H$,

$$N_1(\widetilde{X}/X, \sigma) \geqslant N_1(\widetilde{X}/\mathbb{P}^1_{\mathbb{F}_q}, \sigma) \geqslant q + 1 + C_2 + C_3\sqrt{q},$$

d'où la borne inférieure

$$N_1(X) = |X(\mathbb{F}_q)| \geqslant -\frac{C_4}{|H|} + q + 1 + C_2 + C_3\sqrt{q}$$

ce qui s'écrit encore

$$N_1(X) - (q+1) \geqslant C_5 + C_6\sqrt{q},$$

avec des constantes C_5 et C_6 indépendantes du corps de base. Par ailleurs, la proposition 2.5.9 fournit la borne supérieure analogue

$$N_1(X) - (q+1) \leqslant C_7\sqrt{q}.$$

Comme $N_n(X) = N_1(X_{\mathbb{F}_{q^n}})$, ceci implique que les conditions du lemme 2.5.7 sont vérifiées, ce qui achève la preuve de l'hypothèse de Riemann 2.5.2.

3 La cohomologie Weil-étale

À présent que nous avons planté le décor, nous allons nous attaquer à notre sujet central : la topologie Weil-étale. Cette topologie de Grothendieck, introduite par Lichtenbaum dans [Lic05], est une version modifiée de la célèbre cohomologie étale qui, comme on le verra, est bien plus adaptée qu'elle à l'étude des fonctions zêta de courbes sur les corps finis ; mais elle a également d'autres applications récentes et prometteuses, que nous présenterons succinctement dans la prochaine et dernière partie. En attendant, avant d'entrer dans le vif du sujet, il nous faut encore quelques préliminaires théoriques.

3.1 Cohomologie des groupes

Soit G un groupe. On appelle *G-ensemble* tout ensemble X sur lequel G agit, et on appelle *G-module* tout groupe abélien X sur lequel G agit $\mathbb{Z}$-linéairement (dans les deux cas, ceci signifie qu'on s'est donné un morphisme de G dans le groupe des automorphismes de X).

Notons $g \cdot x$ l'action d'un élément de G sur un élément de X. On dispose alors du foncteur *points fixes*

$$X \longmapsto X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\},$$

qui à X associe le plus grand sous-objet de X sur lequel G agit trivialement, et du foncteur *points cofixes*

$$X \longmapsto X_G = X/(g \cdot x \sim x), \quad g \in G,\ x \in X,$$

qui à X associe le plus grand quotient de X sur lequel G agit trivialement.

Dorénavant, nous ne nous intéresserons plus qu'aux G-modules. La catégorie des G-modules est celle des $\mathbb{Z}G$-modules, où

$$\mathbb{Z}G = \bigoplus_{g \in G} \mathbb{Z}g$$

est l'algèbre du groupe G, dont le produit est défini en étendant linéairement la loi de G ; cette catégorie est donc abélienne.

Soit $\mathbb{Z}$ le G-module avec action triviale de G. On remarque que

Fait 3.1.1. *On a les isomorphismes de foncteurs* $\cdot^G \simeq \mathrm{Hom}_G(\mathbb{Z}, \cdot)$ *et* $\cdot_G \simeq \cdot \underset{\mathbb{Z}G}{\otimes} \mathbb{Z}$*; en particulier, le premier est exact à gauche, et le second, exact à droite.*

Cependant, ces foncteurs ne sont en général pas exacts. On définit donc

Définition 3.1.2. Soit M un G-module. La cohomologie de G à valeurs dans M est donnée par les foncteurs dérivés à droite du foncteur points fixes $\cdot^G$, et l'homologie de G à valeurs dans M est celle des foncteurs dérivés à gauche du foncteur points cofixes $\cdot_G$. Les groupes de cohomologie de G à valeurs dans M sont notés $H^r(G, M)$, et ceux d'homologie, $H_r(G, M)$, $r \in \mathbb{N}$.

Dans la suite, nous ne intéresserons qu'à la cohomologie ; le lecteur déçu par ce choix pourra se référer à [HS71] ou [Bro82] pour de plus amples renseignements sur l'homologie des groupes.

Pour calculer la cohomologie de G à valeurs dans M, la première idée est de prendre une résolution $\mathbb{Z}G$-injective de M, de lui appliquer le foncteur points fixes, et enfin de prendre la cohomologie du complexe obtenu. Toutefois, puisque $\cdot^G \simeq \mathrm{Hom}_G(\mathbb{Z}, \cdot)$, il est plus intelligent de choisir une bonne fois pour toutes une résolution $\mathbb{Z}G$-projective de $\mathbb{Z}$, à laquelle on appliquera $\mathrm{Hom}_G(\cdot, M)$ avant de prendre la cohomologie.

Une première telle résolution est

$$\cdots \longrightarrow P_r \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

où P_r est le $\mathbb{Z}$-module libre sur les $(r+1)$-uples $(g_0, \cdots, g_r)$ d'éléments de G, sur lequel G agit diagonalement par multiplication à gauche :

$$g \cdot (g_0, \cdots, g_r) = (gg_0, \cdots, gg_r),$$

$\varepsilon \colon \mathbb{P}_0 \longrightarrow \mathbb{Z}$ est le *morphisme d'augmentation* défini par

$$\begin{array}{rccc} \varepsilon & : & \mathbb{Z}G & \longrightarrow & \mathbb{Z} \\ & & \displaystyle\sum_{g \in G} n_g g & \longmapsto & \displaystyle\sum_{g \in G} n_g \end{array},$$

et où les autres cobords sont définis par la formule familière

$$\begin{array}{rccc} d_r & : & P_r & \longrightarrow & P_{r-1} \\ & & (g_0, \cdots, g_r) & \longmapsto & \displaystyle\sum_{i=0}^{r} (-1)^i (g_0, \cdots, \hat{g_i}, \cdots, g_r) \end{array},$$

le chapeau signifiant comme d'habitude que le terme a été omis. Il est bien connu que cette formule définit un complexe ; de plus, si définit $k_r : P_r \longrightarrow P_{r+1}$ comme l'application envoyant $(g_0, \cdots, g_r)$ sur $(1, g_0, \cdots, g_r)$, alors on a $d_{r+1} \circ k_r + k_{r-1} \circ d_r = \mathrm{Id}_{P_r}$, donc si $d_r(x) = 0$ alors $x = d_{r+1}\big(k_r(x)\big)$, donc ce complexe est bien exact. Enfin, il est clair que les P_r sont $\mathbb{Z}G$-projectifs car $\mathbb{Z}G$-libres. On en déduit donc :

Proposition 3.1.3 (Calcul de la cohomologie des groupes au moyen du complexe de cochaînes homogènes)**.** *Soit G un groupe, et soit M un G-module. Le* complexe de cochaînes homogènes *de M est le complexe*

$$0 \longrightarrow \widetilde{C}^0 \xrightarrow{d^0} \widetilde{C}^1 \xrightarrow{d^1} \cdots \xrightarrow{d^{r-1}} \widetilde{C}^r \xrightarrow{d^r} \widetilde{C}^{r+1} \xrightarrow{d^{r+1}} \cdots$$

où $\widetilde{C}^r$ est l'ensemble des applications f de G^{r+1} dans M telles que pour tout $g \in G$, on ait $g \cdot f(g_0, \cdots, g_r) = f(gg_0, \cdots, gg_r)$, et où le cobord est donné par la formule

$$\begin{array}{ccccc} d^r & : & \widetilde{C}^r & \longrightarrow & \widetilde{C}^{r+1} \\ (f : G^{r+1} \to M) & \longmapsto & \left(\begin{array}{ccc} G^{r+2} & \longrightarrow & M \\ (g_0, \cdots, g_{r+1}) & \longmapsto & \displaystyle\sum_{i=0}^{r+1} (-1)^i f(g_0, \cdots, \hat{g_i}, \cdots, g_{r+1}) \end{array} \right). \end{array}$$

La cohomologie de ce complexe est la cohomologie de G à valeurs dans M.

Démonstration. En effet, un élément de $\mathrm{Hom}_G(P_r, M)$ s'identifie par restriction à une application f de G^{r+1} dans M astreinte à ce que pour tout $g \in G$, on ait $g \cdot f(g_0, \cdots, g_r) = f(gg_0, \cdots, gg_r)$. Le résultat découle donc de la discussion précédente. □

Cette première résolution est assez maniable pour les calculs pratiques, mais nous allons faire encore mieux. Nous venons de voir qu'un élément de $\mathrm{Hom}_G(P_r, M)$ était déterminé par sa restriction à G^{r+1}, mais une réflexion à peine plus poussée montre qu'il est encore entièrement déterminé par sa valeur sur les éléments de forme $(1, g_1, g_1g_2, \cdots, g_1 \cdots g_r)$ de G^{r+1}, ce qui permet d'identifier $\mathrm{Hom}_G(P_r, M)$ à l'ensemble des applications quelconques de G^r dans M.

On est donc amené à réaliser la construction suivante :

Théorème 3.1.4 (Calcul de la cohomologie des groupes au moyen du complexe de cochaînes inhomogènes)**.** *Soit G un groupe, et soit M un G-module. Le* complexe de cochaînes inhomogènes *de M est le complexe*

$$0 \longrightarrow C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} \cdots \xrightarrow{d^{r-1}} C^r \xrightarrow{d^r} C^{r+1} \xrightarrow{d^{r+1}} \cdots$$

où C^r est l'ensemble des applications de G^r dans M (donc en particulier $C^0 \simeq M$), et où le cobord est donné par la formule

$$\begin{array}{rcccl} d^r & : & C^r & \longrightarrow & C^{r+1} \\ & & & & \\ (f : G^r \to M) & \longmapsto & \left(\begin{array}{ccc} G^{r+1} & \longrightarrow & M \\ (g_1, \cdots, g_{r+1}) & \longmapsto & g_1 \cdot f(g_2, \cdots, g_{r+1}) \\ & & + \ \displaystyle\sum_{i=1}^{r} (-1)^i f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{r+1}) \\ & & + \ (-1)^{r+1} f(g_1, \cdots, g_r) \end{array} \right) \end{array}$$

La cohomologie de ce complexe est la cohomologie de G à valeurs dans M.

L'intérêt du complexe de cochaînes inhomogènes est qu'il se prête assez bien aux calculs explicites.

Exemple 3.1.5. On a bien $H^0(G, M) = \operatorname{Ker} d^0 = M^G$, comme voulu.

Les 1-cocycles sont les *morphismes croisés*, c'est-à-dire les applications $f : G \longrightarrow M$ telles que

$$\forall g_1, g_2 \in G, \quad f(g_1 g_2) = g_1 \cdot f(g_2) + f(g_1),$$

tandis que les 1-cobords sont les *morphismes croisés principaux*, c'est-à-dire les applications $f : G \longrightarrow M$ de forme $g \mapsto g \cdot m - m$, où $m \in M$.

Exemple 3.1.6. Si G agit trivialement sur M, alors les morphismes croisés sont les morphismes, et les morphismes croisés principaux sont nuls, donc

$$H^1(G, M) = \operatorname{Hom}_{\mathfrak{Gr}}(G, M) = \operatorname{Hom}_{\mathbb{Z}}(G^{\mathrm{ab}}, M),$$

où G^{ab} désigne l'abélianisé de G.

Exemple 3.1.7. Si $G = < g_0 > \simeq \mathbb{Z}/n\mathbb{Z}$ est cyclique, alors un morphisme croisé f est entièrement déterminé par sa valeur $m_0 = f(g_0)$ en le générateur g_0, par la formule

$$f(g_0^i) = \sum_{j=0}^{i-1} g_0^j \cdot m_0 \quad (i \in \mathbb{N}).$$

En particulier, m_0 est astreint à vérifier $\sum_{g\in G} g\cdot m_0 = 0$, et f est principal si et seulement si il existe $m \in M$ tel que $m_0 = g_0 \cdot m - m$.

Ainsi, si on définit les applications

$$\begin{array}{rccc} \mathrm{Nm}_G & : & M & \longrightarrow & M \\ & & m & \longmapsto & \displaystyle\sum_{g\in G} g\cdot m \end{array} \quad \text{et}$$

$$\begin{array}{rccc} g_0 - 1 & : & M & \longrightarrow & M \\ & & m & \longmapsto & g_0\cdot m - m \end{array},$$

alors on a

$$H^1(G,M) = \mathrm{Ker}(\mathrm{Nm}_G)/\,\mathrm{Im}(g_0 - 1).$$

Par exemple, si K est un corps et L une extension galoisienne de K, alors le groupe multiplicatif L^* est naturellement un $\mathrm{Gal}(L/K)$-module ; si l'extension L/K est cyclique, alors le théorème 90 de Hilbert exprime très exactement l'annulation du premier groupe de cohomologie $H^1\big(\mathrm{Gal}(L/K), L^*\big)$.

Exemple 3.1.8. [Théorème de Schreier] Un 2-cocycle est ce qu'on appelle un *système de facteurs*, c'est-à-dire une application $f : G^2 \longrightarrow M$ telle que

$$\forall g_1, g_2, g_3 \in G, \quad f(g_1g_2, g_3) + f(g_1, g_2) = f(g_1, g_2g_3) + g_1 \cdot f(g_2, g_3).$$

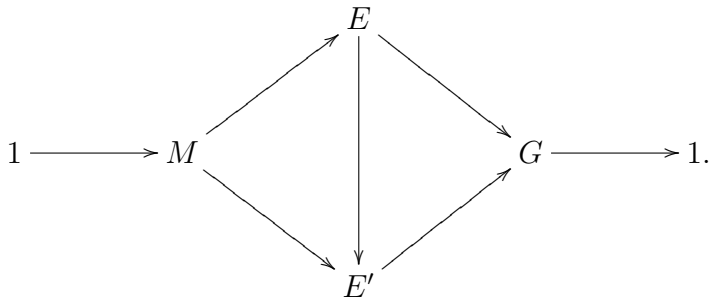
C'est un 2-cobord s'il existe une application $\phi : G \longrightarrow M$ telle que

$$\forall g_1, g_2 \in G, \quad f(g_1, g_2) = \phi(g_1) - \phi(g_1g_2) + g_1 \cdot \phi(g_2).$$

Nous allons voir que $H^2(G,M)$ classifie les *extensions de M par G*, c'est-à-dire les groupes E tels qu'on ait une suite exacte courte de groupes

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1,$$

deux telles extensions E et E' étant identifiées si et seulement si il existe un morphisme $E \longrightarrow E'$ faisant commuter le diagramme



Un tel morphisme est alors un isomorphisme par le lemme des cinq, donc ceci définit bien une relation d'équivalence.

Soient donc M un groupe abélien, $1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$ une extension de M par G, et choisissons une section ensembliste quelconque $s : G \longrightarrow E$. Si g_1 et g_2 sont deux éléments de G, alors $s(g_1)s(g_2)$ et $s(g_1g_2)$ s'envoient tous les deux sur g_1g_2 dans G, donc il existe une application $f : G^2 \longrightarrow M$ définie par

$$\forall g_1, g_2 \in G, \quad s(g_1)s(g_2) = f(g_1, g_2)s(g_1g_2).$$

Intuitivement, f mesure combien s n'est pas un morphisme de groupes, ou encore à quel point E n'est pas un produit semi-direct.

En particulier, puisque M est abélien, on munit M d'une structure de G-module en posant

$$g \cdot m = s(g)ms(g)^{-1}.$$

En écrivant que E est associatif,

$$\begin{array}{rll} \big(s(g_1)s(g_2)\big)s(g_3) = f(g_1,g_2)s(g_1g_2)s(g_3) & = f(g_1,g_2)f(g_1g_2,g_3)s(g_1g_2g_3) \\ = \quad s(g_1)\big(s(g_2)s(g_3)\big) = s(g_1)f(g_2,g_3)s(g_2g_3) & = \big(s(g_1)\cdot f(g_2,g_3)\big)s(g_1)s(g_2g_3) \\ & = \big(s(g_1)\cdot f(g_2,g_3)\big)f(g_1,g_2g_3)s(g_1g_2g_3), \end{array}$$

on se rend compte que f est un système de facteurs.

Si $s' : G \longrightarrow E$ est une autre section, alors il existe une application $\phi : G \longrightarrow M$ telle que $s'(g) = \phi(g)s(g)$, donc l'action induite sur M est la même, ainsi qu'une application $f' : G^2 \longrightarrow M$ définie comme précédemment par $s'(g_1)s'(g_2) = f'(g_1, g_2)s'(g_1g_2)$, mais alors

$$\begin{aligned} s'(g_1)s'(g_2) &= f'(g_1,g_2)\phi(g_1g_2)s(g_1g_2) = f'(g_1,g_2)\phi(g_1g_2)f(g_1,g_2)^{-1}s(g_1)s(g_2) \\ &= f'(g_1,g_2)f(g_1,g_2)^{-1}\phi(g_1g_2)\phi(g_1)^{-1}s'(g_1)\phi(g_2)^{-1}s'(g_2) \\ &= f'(g_1,g_2)f(g_1,g_2)^{-1}\phi(g_1g_2)\phi(g_1)^{-1}\big(g_1\cdot\phi(g_2)^{-1}\big)s'(g_1)s'(g_2), \end{aligned}$$

donc dans M, où la loi est cette fois notée additivement,

$$f(g_1, g_2) = f'(g_1, g_2) + \phi(g_1g_2) - \phi(g_1) - g_1 \cdot \phi(g_2).$$

Ainsi, la classe de f dans $H^2(G, M)$ ne dépend pas du choix de la section s.

Cette classe ne dépend pas non plus du choix de l'extension E, car si $\varphi : E \xrightarrow{\sim} E'$ est un isomorphisme d'extensions au sens expliqué plus haut,

$$\varphi\big(s(g_1)\big)\varphi\big(s(g_2)\big) = \varphi\big(s(g_1)s(g_2)\big) = \varphi\big(f(g_1,g_2)s(g_1g_2)\big) = f(g_1,g_2)\varphi\big(s(g_1g_2)\big).$$

On obtient ainsi une application des classes d'extensions de M par G induisant une action donnée de G sur M vers $H^2(G,M)$. De manière semblable, on peut construire une application de $H^2(G,M)$ vers les classes d'extensions de M par G induisant l'action de G sur M, et on vérifie alors que ces deux applications sont inverses l'une de l'autre.

Étant donné un G-module M, on a donc établi une correspondance entre $H^2(G,M)$ et les classes d'extension de M par G telle que l'action par conjugaison (après relèvement) de G sur M coïncide avec la structure de G-module sur M. Notons que l'élément nul de $H^2(G,M)$ correspond au produit semi-direct $M \rtimes G$.

Grâce aux cochaînes inhomogènes, on peut aussi démontrer la propriété suivante, qui n'avait rien d'évident jusqu'ici :

Proposition 3.1.9. *Soit G un groupe fini. Pour tout G-module M, les groupes de cohomologie $H^r(G,M)$ sont de torsion pour tout $r > 0$; plus précisément, ils sont de $|G|$-torsion.*

Démonstration. J'emprunte cette démonstration à Boas Erez.

Fixons $r > 0$, et soit $f : G^r \longrightarrow M$ un r-cocycle. Il nous faut montrer que $|G|f$ est un r-cobord. Considérons l'application

$$\begin{array}{rccc} \varphi & : & G^{r-1} & \longrightarrow & M \\ & & (g_2, \cdots, g_r) & \longmapsto & \displaystyle\sum_{g_{r+1} \in G} f(g_2, \cdots, g_{r+1}) \ . \end{array}$$

Puisque f est un cocycle, on a par définition

$$g_1 f(g_2, \cdots, g_{r+1}) + \sum_{i=1}^{r} (-1)^i f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{r+1}) + (-1)^{r+1} f(g_1, \cdots, g_r) = 0$$

pour tous $g_1, \cdots, g_{r+1} \in G$, ce qui s'écrit encore

$$f(g_1, \cdots, g_r) = (-1)^r \left(g_1 f(g_2, \cdots, g_{r+1}) + \sum_{i=1}^{r} (-1)^i f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{r+1}) \right).$$

En sommant ceci sur $g_{r+1} \in G$, on obtient

$$\begin{aligned}
& |G| f(g_1, \cdots, g_r) \\
= \; & (-1)^r \left(\sum_{g_{r+1} \in G} g_1 f(g_2, \cdots, g_{r+1}) + \sum_{i=1}^{r} (-1)^i \sum_{g_{r+1} \in G} f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{r+1}) \right) \\
= \; & (-1)^r \Bigg(g_1 \varphi(g_2, \cdots, g_r) + \sum_{i=1}^{r-1} (-1)^i \varphi(g_1, \cdots, g_i g_{i+1}, \cdots, g_r) \\
& \qquad + (-1)^r \sum_{g_{r+1} \in G} f(g_1, \cdots, g_{r-1}, g_r g_{r+1}) \Bigg) \\
= \; & (-1)^r \left(g_1 \varphi(g_2, \cdots, g_r) + \sum_{i=1}^{r-1} (-1)^i \varphi(g_1, \cdots, g_i g_{i+1}, \cdots, g_r) + (-1)^r \varphi(g_1, \cdots, g_{r-1}) \right) \\
= \; & (-1)^r \, d\varphi(g_1, \cdots, g_r).
\end{aligned}$$

□

Nos $H^r(G, M)$ ne sont pour l'instant munis que d'une structure de groupes abéliens ; nous allons à présent étoffer cela. Étant donnés deux G-modules M et N, leur produit tensoriel $M \underset{\mathbb{Z}}{\otimes} N$ est naturellement muni d'une structure de G-module, définie par l'action diagonale de G :

$$g \cdot (m \otimes n) = (g \cdot m) \otimes (g \cdot n) \qquad (g \in G,\ m \in M,\ n \in N).$$

Il est clair que $(M \underset{\mathbb{Z}}{\otimes} N)^G \supseteq M^G \underset{\mathbb{Z}}{\otimes} N^G$; par conséquent, on a une application naturelle

$$H^0(G, M) \underset{\mathbb{Z}}{\otimes} H^0(G, N) \longrightarrow H^0(G, M \underset{\mathbb{Z}}{\otimes} N).$$

Cette construction se généralise en posant

$$\begin{aligned}
H^r(G, M) \underset{\mathbb{Z}}{\otimes} H^s(G, N) & \longrightarrow H^{r+s}(G, M \underset{\mathbb{Z}}{\otimes} N) \\
f \otimes f' & \longmapsto \Big((g_1, \cdots, g_{r+s}) \mapsto f(g_1, \cdots, g_r) \otimes (g_1 \cdots g_r) \cdot f'(g_{r+1}, \cdots, g_{r+s}) \Big).
\end{aligned}$$

Les applications obtenues, dont on laisse au lecteur le soin de vérifier qu'elles sont bien définies, forment ce que l'on appelle le *cup-produit* ; le cup-produit de $f \in H^r(G, M)$ et de $f' \in H^s(G, N)$ est noté $f \cup f' \in H^{r+s}(G, M \underset{\mathbb{Z}}{\otimes} N)$. Des calculs quelque peu fastidieux montrent que le cup-produit est associatif et anticommutatif gradué, c'est-à-dire que $f' \cup f = (-1)^{rs} f \cup f'$ si $f \in H^r(G, M)$ et $f' \in H^s(G, N)$, après l'identification $M \underset{\mathbb{Z}}{\otimes} N \simeq N \underset{\mathbb{Z}}{\otimes} M$.

Exemple 3.1.10. Posons pour tout G-module M

$$H(G,M) = \bigoplus_{r\in\mathbb{N}} H^r(G,M);$$

grâce aux identifications de G-modules $\mathbb{Z}\underset{\mathbb{Z}}{\otimes}\mathbb{Z} \simeq \mathbb{Z}$ puis $\mathbb{Z}\underset{\mathbb{Z}}{\otimes} M \simeq M$, le cup-produit munit $H(G,\mathbb{Z})$ d'une structure d'anneau anticommutatif gradué, sur lequel les $H(G,M)$ sont des modules gradués.

Nous ne ferons qu'une utilisation extrêmement basique du cup-produit, aussi nous contenterons-nous de mentionner qu'il possède de très nombreuses propriétés, consultables par exemple dans [Bro82], chapitre V.

Intéressons-nous à présent au cas où le groupe G et le module M sont munis d'une topologie. On supposera dans toute la suite que ces topologies sont compatibles, c'est-à-dire que l'action de G sur M

$$\begin{array}{ccc} G\times M & \longrightarrow & M \\ (g,m) & \longmapsto & g\cdot m \end{array}$$

est continue. On s'intéressera plus particulièrement au cas où le groupe G est profini et où le module M est discret, ce qui revient à dire que le stabilisateur de chaque élément $m \in M$ est un sous-groupe fermé, donc ouvert, de G.

On redéfinit alors les groupes de cohomologie $H^\cdot(G,M)$ comme étant les groupes de cohomologie du complexe de cochaînes (homogènes ou inhomogènes) *continues*.

Le théorème suivant relie cette nouvelle cohomologie à l'ancienne.

Théorème 3.1.11. *Soit G un groupe profini, et soit M un G-module discret. Pour tout $r \in \mathbb{N}$, on a*

$$H^r(G,M) \simeq \varinjlim_{U} H^r(G/U, M^U),$$

où U parcourt les sous-groupes distingués ouverts de G.

Démonstration. Nous allons bien sûr utiliser le complexe $C^\cdot_{ct}$ des cochaînes inhomogènes continues pour calculer la cohomologie de G à valeurs dans M.

Si $V \subseteq U$ sont deux sous-groupes distingués ouverts de G, les projections

$$G^r \longrightarrow (G/V)^r \longrightarrow (G/U)^r$$

induisent des morphismes

$$C^r_{ct}(G/U, M^U) \longrightarrow C^r_{ct}(G/V, M^V) \longrightarrow C^r_{ct}(G, M)$$

qui commutent clairement au cobord, d'où des morphismes

$$H^r(G/U, M^U) \longrightarrow H^r(G/V, M^V) \longrightarrow H^r(G, M).$$

Les $H^r(G/U, M^U)$ forment donc un système inductif filtrant, d'où un morphisme

$$\varinjlim_U H^r(G/U, M^U) \longrightarrow H^r(G, M)$$

dont il s'agit de montrer que c'est un isomorphisme. Pour ce faire, montrons que le morphisme

$$\varinjlim_U C^r_{ct}(G/U, M^U) \longrightarrow C^r_{ct}(G, M)$$

est lui-même un isomorphisme. Il est clair qu'il est injectif puisque les morphismes $C^r_{ct}(G/U, M^U) \longrightarrow C^r_{ct}(G, M)$ le sont. De plus, toute r-cochaîne inhomogène continue $f : G^r \longrightarrow M$ est d'image compacte puisque G^r est compact, donc finie puisque M est discret, donc contenue dans M^U pour un certain sous-groupe distingué ouvert U de G. Par ailleurs, la préimage de tout point m de M par f est ouverte, donc contient un translaté de V^r_m, où V_m est un certain sous-groupe distingué ouvert de G. Par conséquent, si on pose

$$V = \bigcap_{m \in f(G^r)} V_m,$$

alors V est un sous-groupe distingué ouvert de G tel que f se factorise par $(G/V)^r$, donc, si on pose $W = U \cap V$, alors f provient d'un élément de $C^r_{ct}(G/W, M^W)$, d'où la surjectivité.

On a donc un isomorphisme

$$\varinjlim_U C^r_{ct}(G/U, M^U) \simeq C^r_{ct}(G, M),$$

et comme les limites inductives en jeu sont filtrantes donc exactes, on en déduit que

$$\varinjlim_U H^r(G/U, M^U) \simeq H^r\big(\varinjlim_U C^\cdot_{ct}(G/U, M^U)\big) \simeq H^r\big(C^\cdot_{ct}(G, M)\big) = H^r(G, M).$$

□

Par exemple, la cohomologie d'un groupe fini étant de torsion d'après la proposition 3.1.9, on en déduit immédiatement le corollaire

Corollaire 3.1.12. *La cohomologie d'un groupe profini à valeurs dans un module discret est de torsion en degré $r > 0$.* $\square$

En guise d'application, montrons quelques résultats de comparaison cohomologique entre $\mathbb{Z}$ et $\widehat{\mathbb{Z}}$ qui nous seront utiles plus tard, lors de l'étude de la cohomologie Weil-étale.

Lemme 3.1.13. *Soit M un $\widehat{\mathbb{Z}}$-module discret de torsion. Pour tout $r \in \mathbb{N}$, l'application naturelle de $H^r(\widehat{\mathbb{Z}}, M)$ dans $H^r(\mathbb{Z}, M)$ est un isomorphisme.*

Démonstration. On a $M^{\widehat{\mathbb{Z}}} = M^{\mathbb{Z}}$ par densité de $\mathbb{Z}$ dans $\widehat{\mathbb{Z}}$, d'où le résultat pour $r = 0$.

Notons g un générateur de $\mathbb{Z}$. Par un raisonnement identique à celui mené dans l'exemple 3.1.7, on a $H^1(\mathbb{Z}, M) \simeq M/(g-1)M$, tandis que le même exemple 3.1.7 combiné au théorème 3.1.11 montre que

$$H^1(\widehat{\mathbb{Z}}, M) \simeq \varinjlim_{n \in \mathbb{N}^*} N_n^{<g^n>}/(g-1)M^{<g^n>},$$

où N_n désigne le noyau dans M de l'action de $\gamma_n = 1 + g + \cdots + g^{n-1}$. Soit $m \in M$. Comme M est de torsion, il existe un $\lambda \in \mathbb{Z}$ tel que $\lambda m = 0$, et comme m est discret, il existe un $n \in \mathbb{N}^*$ tel que $g^n \cdot m = 0$. On a alors $\gamma_{\lambda n} \cdot m = \lambda(\gamma_n \cdot m) = 0$, ce qui montre que

$$M = \bigcup_{n \in \mathbb{N}^*} N_n^{<g^n>},$$

d'où le résultat pour $r = 1$.

Pour terminer, montrons que $H^r(\widehat{\mathbb{Z}}, M) = H^r(\mathbb{Z}, M) = 0$ pour $r \geqslant 2$. La nature même de $\mathbb{Z}$ fait que toute extension

$$1 \longrightarrow M \longrightarrow E \longrightarrow \mathbb{Z} \longrightarrow 1$$

est scindée ; de même, comme M est de torsion, toute extension

$$1 \longrightarrow M \longrightarrow E \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 1$$

est scindée, car l'adhérence du sous-groupe de E engendré par une image réciproque d'un générateur topologique de $\widehat{\mathbb{Z}}$ est envoyé isomorphiquement

sur $\widehat{\mathbb{Z}}$. Ainsi, $H^2(\widehat{\mathbb{Z}}, M) = H^2(\mathbb{Z}, M) = 0$ d'après le théorème de Schreier qui a fait l'objet de l'exemple 3.1.8. Notons $G = \mathbb{Z}$ ou $\widehat{\mathbb{Z}}$, et considérons la suite exacte courte de G-modules

$$0 \longrightarrow M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)/M \longrightarrow 0,$$

où $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)$ est muni de l'action définie par $(g \cdot \varphi)(\cdot) = g \cdot \varphi(g^{-1}\cdot)$, M étant vu comme le sous-module des fonctions constantes. Soit

$$\cdots \longrightarrow P_r \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

une résolution $\mathbb{Z}G$-libre de $\mathbb{Z}$, par exemple celle décrite au début de cette section. On a $\mathrm{Hom}_G\big(P_r, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)\big) \simeq \mathrm{Hom}_{\mathbb{Z}}(P_r, M)$; comme les P_r sont $\mathbb{Z}$-libres, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)$ est donc acyclique. La suite exacte longue de cohomologie associée à la suite exacte courte précédente révèle alors que pour tout $r \in \mathbb{N}$, on a $H^{r+1}(G, M) = H^r\big(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)/M\big)$. Puisque $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)$ est de torsion dès que M l'est, on en déduit par récurrence que $H^r(\widehat{\mathbb{Z}}, M) = H^r(\mathbb{Z}, M) = 0$ pour tout $r \geqslant 2$, ce qu'il fallait démontrer. □

Signalons au passage que la méthode utilisée à la fin de la démonstration est un avatar d'une méthode générale en cohomologie des groupes, le *dimension shifting*, qui permet comme son nom l'indique de ramener le calcul de la cohomologie en degré $r+1$ à celui de la cohomologie en degré r, au prix d'une complexification du module.

Lemme 3.1.14. *Soit M un $\widehat{\mathbb{Z}}$-module discret. On a les isomorphismes fonctoriels en M suivants :*

(a) $H^0(\widehat{\mathbb{Z}}, M) \simeq H^0(\mathbb{Z}, M)$,

(b) $H^1(\widehat{\mathbb{Z}}, M) \simeq H^1(\mathbb{Z}, M)_{\mathrm{tor}}$,

(c) $H^2(\widehat{\mathbb{Z}}, M) \simeq H^1(\mathbb{Z}, M) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}/\mathbb{Z}$.

Démonstration. Le (a) est évident. Pour montrer (b) et (c), supposons tout d'abord M sans torsion. Pour tout $n \in \mathbb{N}^*$, on a un diagramme commutatif

$$\begin{array}{ccccccccc}
H^1(\mathbb{Z}, M) & \xrightarrow{n} & H^1(\mathbb{Z}, M) & \longrightarrow & H^1(\mathbb{Z}, M/nM) & \longrightarrow & 0 & & \\
\uparrow & & \uparrow & & \uparrow\wr & & \uparrow & & \\
H^1(\widehat{\mathbb{Z}}, M) & \xrightarrow{n} & H^1(\widehat{\mathbb{Z}}, M) & \longrightarrow & H^1(\widehat{\mathbb{Z}}, M/nM) & \longrightarrow & H^2(\widehat{\mathbb{Z}}, M)_n & \longrightarrow & 0,
\end{array}$$

où l'indice n dénote la composante de n-torsion. Les lignes sont exactes car — rappelons que $H^2(\mathbb{Z}, M) = 0$ pour tout M d'après le théorème de Schreier 3.1.8 — ce sont des extraits des suites exactes longues de cohomologie associées à

$$0 \longrightarrow M \xrightarrow{n} M \longrightarrow M/nM \longrightarrow 0,$$

et la troisième flèche verticale est un isomorphisme d'après le lemme 3.1.13 précédent. Après tensorisation par $\mathbb{Z}/n\mathbb{Z}$ au-dessus de $\mathbb{Z}$, une petite chasse au diagramme montre que

$$H^2(\widehat{\mathbb{Z}}, M)_n \simeq \big(H^1(\mathbb{Z}, M) \underset{\mathbb{Z}}{\otimes} (\mathbb{Z}/n\mathbb{Z})\big) \big/ \big(H^1(\widehat{\mathbb{Z}}, M) \underset{\mathbb{Z}}{\otimes} (\mathbb{Z}/n\mathbb{Z})\big).$$

En passant à la limite inductive sur $n \in \mathbb{N}^*$, on en déduit que

$$H^2(\widehat{\mathbb{Z}}, M)_{\mathrm{tor}} \simeq \big(H^1(\mathbb{Z}, M) \underset{\mathbb{Z}}{\otimes} (\mathbb{Q}/\mathbb{Z})\big) \big/ \big(H^1(\widehat{\mathbb{Z}}, M) \underset{\mathbb{Z}}{\otimes} (\mathbb{Q}/\mathbb{Z})\big).$$

Or $H^1(\widehat{\mathbb{Z}}, M)$ et $H^2(\widehat{\mathbb{Z}}, M)$ sont de torsion d'après le corollaire 3.1.12, donc $H^2(\widehat{\mathbb{Z}}, M)_{\mathrm{tor}} = H^2(\widehat{\mathbb{Z}}, M)$ et $H^1(\widehat{\mathbb{Z}}, M) \underset{\mathbb{Z}}{\otimes} (\mathbb{Q}/\mathbb{Z}) = 0$, ce qui montre (c).

Puisque $H^0(\mathbb{Z}, M) \simeq H^0(\widehat{\mathbb{Z}}, M)$ et $H^0(\mathbb{Z}, M) \simeq H^0(\widehat{\mathbb{Z}}, M)$, on a $H^1(\mathbb{Z}, M)_n \simeq H^1(\widehat{\mathbb{Z}}, M)_n$ d'après le lemme des cinq, donc le (b) en passant à la limite inductive.

On en déduit facilement le résultat dans le cas général en appliquant aux deux suites exactes longues de cohomologie associées à la suite exacte courte

$$0 \longrightarrow M_{\mathrm{tor}} \longrightarrow M \longrightarrow M/M_{\mathrm{tor}} \longrightarrow 0$$

le lemme des cinq, ce qui est loisible par le lemme 3.1.13. □

3.2 Topologies de Grothendieck

Nous allons à présent introduire, à l'aide du langage des catégories, une généralisation de la notion de faisceau sur un espace topologique. Pour ce faire, commençons par examiner cette notion sous un angle catégorique.

Étant donné un espace topologique X, on définit la catégorie $\mathfrak{Op}(X)$ des ouverts de X comme suit : ses objets sont les ouverts de X, et on pose, pour $U, V \subseteq X$,

$$\mathrm{Hom}_{\mathfrak{Op}(X)}(U, V) = \begin{cases} \{\mathrm{pt}\} & \text{si } U \subseteq V \\ \emptyset & \text{sinon} \end{cases},$$

où $\{\mathrm{pt}\}$ dénote un singleton ; l'idée étant que les morphismes sont les inclusions. Avec cette définition, un préfaisceau sur X à valeurs dans un catégorie $\mathfrak{C}$ n'est rien d'autre qu'un foncteur contravariant de $\mathfrak{Op}(X)$ dans $\mathfrak{C}$.

Remarquons que la catégorie $\mathfrak{Op}(X)$ admet des produits et des coproduits, et que ces notions coïncident avec celles d'intersection et d'union, respectivement :

$$\prod_{i\in I} U_i = \bigcap_{i\in I} U_i, \quad \coprod_{i\in I} U_i = \bigcup_{i\in I} U_i.$$

De plus, puisque X est un objet terminal dans $\mathfrak{Op}(X)$, l'intersection de deux ouverts U et V coïncide aussi avec leur produit fibré au-dessus de X :

$$U \cap V = U \times V = U \times_X V.$$

Ainsi, un faisceau d'objets de $\mathfrak{C}$ sur X, c'est-à-dire un préfaisceau respectant le principe du "local-global", est un foncteur contravariant $\mathcal{F}\colon \mathfrak{Op}(X) \longrightarrow \mathfrak{C}$, tel que pour tout ouvert U de X, et pour tout recouvrement $(U_i)_{i\in I}$ de U, on ait le diagramme d'égalisateur

$$\mathcal{F}(U) \longrightarrow \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j\in I} \mathcal{F}(U_i \times_U U_j)\,.$$

Ici, dire que $(U_i)_{i\in I}$ est un recouvrement de U signifie bien sûr que $U = \bigcup_{i\in I} U_i$; mais il sera utile de généraliser cette idée. À cette fin, examinons quelques propriétés des recouvrements au sens usuel du terme :

Soit $U = \bigcup_{i\in I} U_i$ un recouvrement. Alors

- Pour tout ouvert V, $V = \bigcup_{i\in I}(U_i \cap V)$ est un recouvrement de V, et
- Si on se donne des recouvrements $U_i = \bigcup_j U_{ij}$ des U_i, alors $U = \bigcup_{i,j} U_{ij}$ est un recouvrement de U.

Après traduction de ces idées en langage catégorique, on obtient la généralisation de la notion de faisceau suivante :

Définition 3.2.1. Une topologie de Grothendieck T consiste en la donnée d'une catégorie $\mathrm{cat}(T)$, dont les objets s'appellent *ouverts* (*cf* la catégorie des ouverts d'un espace topologique), et d'un ensemble $\mathrm{cov}(T)$ de familles de morphismes $(\varphi_i\colon U_i \longrightarrow U)_{i\in I}$ (servant à définir la notion de recouvrement), tels que

(T1) Pour tout recouvrement $(U_i \longrightarrow U)_{i\in I} \in \mathrm{cov}(T)$, et pour tout morphisme $V \longrightarrow U$ dans $\mathrm{cat}(T)$, les produits fibrés $U_i \times_U V$ existent et $(U_i \times_U V \longrightarrow V)_{i\in I}$ est un recouvrement de V,

(T2) Pour tout recouvrement $(U_i \longrightarrow U)_{i\in I} \in \mathrm{cov}(T)$, pour toute famille de recouvrements $(U_{ij} \longrightarrow U_i)_{j\in J_i} \in \mathrm{cov}(T)$, la famille des morphismes composés $(U_{ij} \longrightarrow U)_{i\in I, j\in J_i}$ est un recouvrement,

(T3) Pour tout isomorphisme $\varphi\colon U' \xrightarrow{\sim} U$, $(\varphi\colon U' \xrightarrow{\sim} U)$ est un recouvrement.

Soit $\mathfrak{C}$ une catégorie admettant des produits et des noyaux. On appelle *préfaisceau* de T dans $\mathfrak{C}$ tout foncteur contravariant $\mathcal{F}\colon \mathrm{cat}(T) \longrightarrow \mathfrak{C}$. Un préfaisceau $\mathcal{F}$ est un *faisceau* si pour tout ouvert $U \in \mathrm{cat}(T)$ et pour tout recouvrement $(U_i \longrightarrow U)_{i\in I} \in \mathrm{cov}(T)$, on a le diagramme d'égalisateur

$$\mathcal{F}(U) \longrightarrow \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j\in I} \mathcal{F}(U_i \times_U U_j)\ .$$

Exemple 3.2.2. Toute topologie (au sens usuel du terme) est une topologie de Grothendieck ; ceci résulte directement de la discussion ci-dessus.

Exemple 3.2.3. Si X est un espace topologique, en prenant pour catégorie des ouverts $\mathrm{cat}(T)$ la catégorie $\mathfrak{Op}(X)$ des ouverts de X, comme précédemment, mais en définissant $\mathrm{cov}(T)$ comme les recouvrements usuels *finis*, c'est-à-dire

$$\mathrm{cov}(T) = \left\{ (U_i \longrightarrow U)_{i\in I} \mid U = \bigcup_{i\in I} U_i \text{ et } I \text{ fini} \right\},$$

la topologie de Grothendieck obtenue est différente ; par exemple, si $X = \mathbb{R}$, alors le préfaisceau des fonctions continues bornées est un faisceau pour T, alors que ce n'est qu'un préfaisceau pour la topologie usuelle.

Exemple 3.2.4. Soit G un groupe. On définit une topologie de Grothendieck T_G en prenant pour $\mathrm{cat}(T_G)$ la catégorie des G-ensembles, et en posant

$$\mathrm{cov}(T_G) = \left\{ (U_i \longrightarrow U)_{i\in I} \mid U = \bigcup_{i\in I} U_i \right\}.$$

On peut alors démontrer que tout faisceau d'ensembles sur T_G est *représentable*, c'est-à-dire isomorphe à un faisceau de la forme $\mathrm{Hom}_G(\cdot, X)$, où X est un G-ensemble.

Si G est un groupe profini, on obtient le même résultat avec la catégorie des G-ensembles discrets.

Une application continue $f : X \longrightarrow Y$ entre deux espaces topologiques X et Y détermine un foncteur $f^{-1} : \mathfrak{Op}_Y \longrightarrow \mathfrak{Op}_X$, qui commute aux intersections, et qui préserve les recouvrements. En se basant sur ce modèle, on est donc amené à définir

Définition 3.2.5. Soient T et T' deux topologies de Grothendieck. Un *morphisme* de T vers T' est un foncteur de $\mathrm{cat}(T)$ vers $\mathrm{cat}(T')$ qui commute aux produits fibrés et qui préserve la notion de recouvrement.

Si f est un tel morphisme, on définit comme dans le cas des topologies usuelles les foncteurs f_*, f^*, $f_!$, $\cdots$ sur les faisceaux. Ceci nécessite de définir la notion de faisceau associé à un préfaisceau, ce que nous ne ferons pas ici.

On démontre, et nous l'admettrons, que pour toute topologie de Grothendieck T, la catégorie des faisceaux de groupes abéliens sur T est abélienne et admet assez d'injectifs. Étant donné un ouvert $U \in \mathrm{cat}(T)$, on dispose du foncteur section $\Gamma(U, \cdot)$, qui à un faisceau de groupes abéliens $\mathcal{F}$ sur T associe le groupe abélien $\mathcal{F}(U)$. Comme pour les faisceaux usuels, ce foncteur est exact à gauche, mais pas à droite en général ; on définit donc les groupes de cohomologie

$$H^r(U, \cdot) = R^r\Gamma(U, \cdot) \quad (r \in \mathbb{N})$$

comme les foncteurs dérivés à droite de $\Gamma(U, \cdot)$.

Auparavant, nous nous étions intéressés au cas des sections *globales*. Puisque dans un espace topologique X, l'ouvert X est terminal dans la catégorie des ouverts $\mathfrak{Op}(X)$, il est naturel de s'intéresser plus particulièrement au cas où $U \in \mathrm{cat}(T)$ est un objet terminal, s'il en existe. Comme les objets terminaux sont uniques à isomorphisme près, on peut définir

Définition 3.2.6. Soit T une topologie de Grothendieck telle que $\mathrm{cat}(T)$ admette un objet terminal X. On pose

$$H^r(T, \cdot) = R^r\Gamma(X, \cdot) \quad (r \in \mathbb{N}).$$

Exemple 3.2.7. Dans le cas de l'exemple 3.2.2 de la topologie de Grothendieck T_X associée à un espace topologique X, la catégorie $\mathrm{cat}(T_X) = \mathfrak{Op}(X)$ admet, comme on vient de le voir, un unique objet terminal, à savoir X lui-même ;. Pour tout faisceau de groupes abéliens $\mathcal{F}$ sur X, les groupes $H^r(T_X, \mathcal{F})$ coïncident donc avec les groupes de cohomologie des faisceaux usuelle.

Exemple 3.2.8. Dans le cas de l'exemple 3.2.4 de la topologie de Grothendieck T_G sur les G-ensembles, la catégorie $\mathrm{cat}(T_G)$ des G-ensembles admet pour objet terminal le singleton $\{\mathrm{pt}\}$ avec action triviale de G. En admettant comme en 3.2.4 que tout faisceau est représentable, on voit que tout faisceau de groupes abéliens sur T_G est de forme $\mathcal{F} \simeq \mathrm{Hom}_G(\cdot, M)$, où M est un G-module. On a alors $\Gamma(\{\mathrm{pt}\}, \mathcal{F}) \simeq \mathrm{Hom}_G(\{\mathrm{pt}\}, M) \simeq M^G$; on retrouve donc ainsi la cohomologie des groupes.

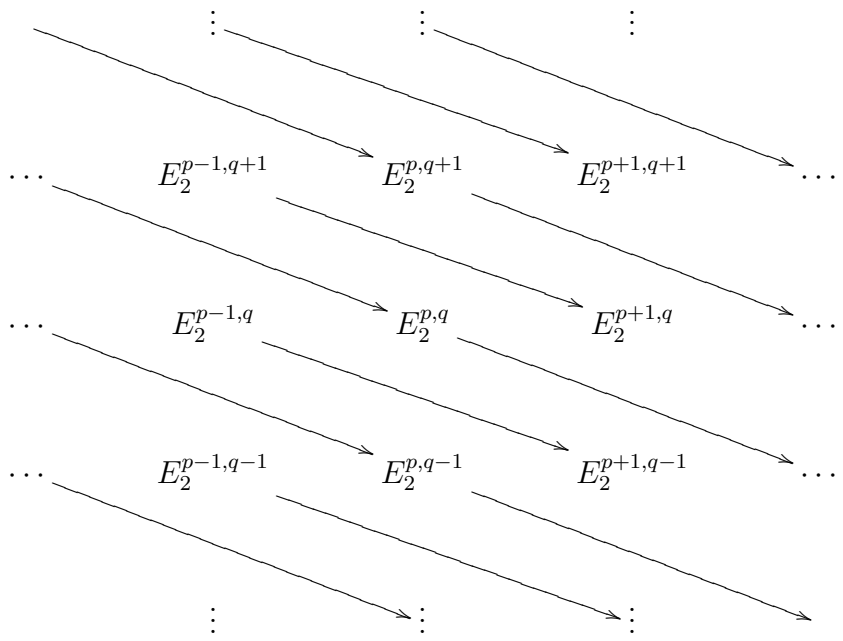
3.3 Suites spectrales

Définition 3.3.1. Soit $\mathfrak{C}$ une catégorie abélienne. Une *suite spectrale* débutant à la *page* $r_0 \in \mathbb{Z}$ dans $\mathfrak{C}$ est la donnée d'objets $(E_r^{p,q})_{p,q\in\mathbb{Z},r\geqslant r_0}$ de $\mathfrak{C}$, de morphismes $d_r^{p,q} : E_r^{p,q} \longrightarrow E_r^{p+r,q-r+1}$ vérifiant la condition de complexe $d_r^{p+r,q-r+1} \circ d_r^{p,q} = 0$, tels qu'on ait des isomorphismes $E_{r+1}^{p,q} \simeq \mathrm{Ker}\, d_r^{p,q} / \mathrm{Im}\, d_r^{p-r,q+r-1}$, et d'une suite d'objets filtrés $\cdots \supseteq F^pE^n \supseteq F^{p+1}E^n \supseteq \cdots$ de $\mathfrak{C}$. Posons $\mathrm{gr}_p E^n = F^pE^n \supseteq F^{p+1}E^n$. On suppose que pour tout p et pour tout q, $d_r^{p,q} = 0$ pour r assez grand ; c'est par exemple le cas si $E_{r_0}^{p,q} = 0$ dès que $p < 0$ ou $q < 0$ — on parle alors de suite spectrale *cohomologique* — car pour r grand, les flèches sont si longues qu'elle démarrent ou aboutissent nécessairement sur un 0. Notons alors $E_\infty^{p,q}$ la valeur sur laquelle stationne $E_r^{p,q}$; on exige des isomorphismes $E_\infty^{p,q} \simeq \mathrm{gr}_p E^{p+q}$. On résume tout ceci par la notation

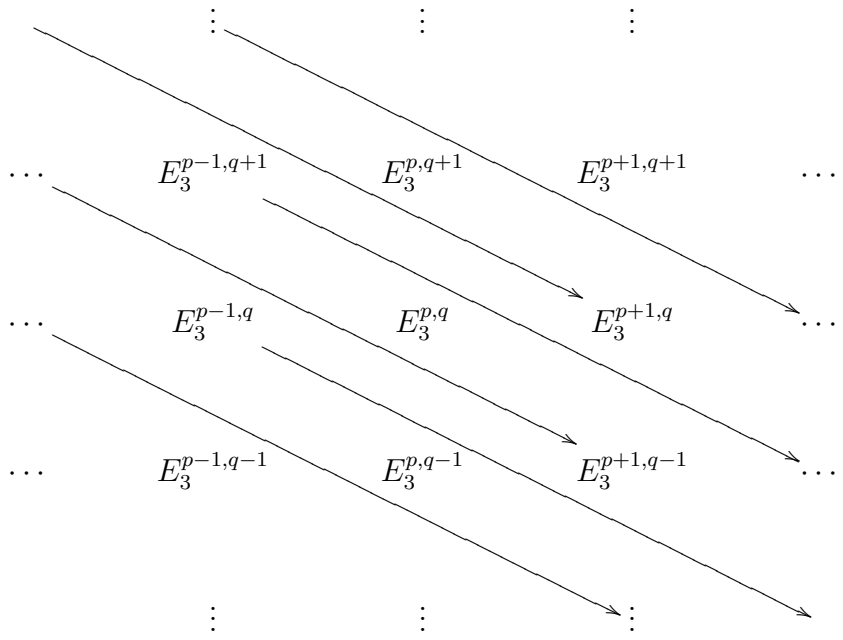
$$E_{r_0}^{p,q} \Longrightarrow E^{p+q}.$$

En pratique, on prend souvent $r_0 = 2$. Il est naturel de représenter la suite spectrale comme une suite de *pages* indexées par $r \geqslant r_0$, avec sur chaque page un réseau d'objets $E_r^{p,q}$ indexés par p et q, et munis des différentielles d. Si on dit que le degré de $E_r^{p,q}$ est $p+q$, alors ces différentielles augmentent le degré de 1, ; on pourrait aussi bien définir des suites spectrales "homologiques" dont les différentielles diminueraient le degré de 1. Pour passer de la page r à la page $r+1$ de la suite spectrale, on prend la cohomologie des complexes de la page r.

Ainsi, la page $r = 2$ ressemble à ceci :



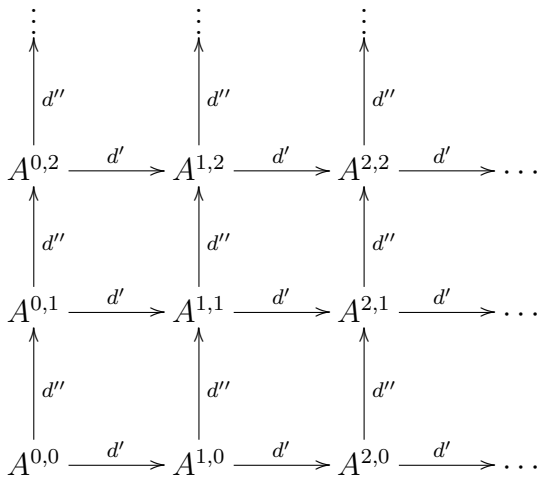
En prenant la cohomologie, on arrive à la page $r = 3$:



et cætera. Par définition, $E_{r+1}^{p,q}$ est un sous-quotient de $E_r^{p,q}$.

Dans toutes la suite, nous ne nous intéresserons qu'aux suites spectrales *cohomologiques*, pour lesquelles $E_r^{p,q} = 0$ si $p < 0$ ou $q < 0$.

Les suites spectrales sont un puissant outil d'algèbre homologique. Étant donné un *complexe double*



où $d' \circ d'' = -d'' \circ d'$, on peut définir le *complexe total*

$$A^{0,0} \xrightarrow{d} A^{1,0} \oplus A^{0,1} \xrightarrow{d} \cdots \xrightarrow{d} \bigoplus_{p+q=n} A^{p,q} \xrightarrow{d} \cdots ,$$

dont la différentielle est la somme $d = d' + d'' : A^{p,q} \longrightarrow A^{p+1,q} \oplus A^{p,q+1}$.

Voyons comment les suites spectrales permettent de calculer la cohomologie de ce complexe total en termes de cohomologie du complexe double. Notons $A^n = \bigoplus_{p+q=n} A^{p,q}$ les termes du complexe total, et soit $E^n = H^n(A^\cdot)$ leur cohomologie, que l'on souhaite calculer. Les A^n sont munis d'une filtration naturelle, à savoir

$$F^p A^n = \bigoplus_{i \geqslant p} A^{i,n-i}.$$

Notons $E^n = H^n(A^\cdot)$ les groupes de cohomologie à calculer, et soit $F^p E^n$ la filtration induite sur ceux-ci. Définissons la page $r_0 = 2$ d'une suite spectrale en prenant la cohomologie du complexe double, d'abord verticalement, puis horizontalement :

$$E_2^{p,q} = H^p(H^q(A^{\cdot,\cdot})).$$

Remarquons que ceci revient à choisir le complexe double lui-même comme page $r = 0$, puis à passer à la page 2. On démontre qu'il est possible d'itérer canoniquement ce procédé, ce qui fournit une suite spectrale $E_r^{p,q} \Longrightarrow E^n$ aboutissant à la cohomologie du complexe total. Pour plus de détails, le lecteur est invité à consulter [Neu99].

Les suites spectrales sont donc un outil intéressant pour réaliser certaines calculs en algèbre homologique. Nous utiliserons essentiellement le cas particulier suivant :

Théorème 3.3.2 (Grothendieck)**.** *Soient $\mathfrak{C}$, $\mathfrak{C}'$ et $\mathfrak{C}''$ des catégories abéliennes, les deux premières ayant assez d'injectifs, et soient $F : \mathfrak{C} \longrightarrow \mathfrak{C}'$ et $G : \mathfrak{C}' \longrightarrow \mathfrak{C}''$ deux foncteurs. On suppose que G est exact à gauche, et que F envoie les objets injectifs de $\mathfrak{C}$ sur des objets G-acycliques que $\mathfrak{C}'$. Alors il existe une foncteur spectral cohomologique $E_2^{p,q} \Longrightarrow E^n$ de termes initiaux $E_2^{p,q} = R^pG\big(R^qF(\cdot)\big)$ formés sur les foncteurs dérivés de F et G et qui aboutit aux foncteurs dérivés $R^{p+q}(G \circ F)(\cdot)$ du foncteur composé, pour une filtration convenable.*

Ici, le terme "foncteur spectral" dénote simplement une suite spectrale dépendant fonctoriellement de l'objet de $\mathfrak{C}$. L'idée de la démonstration de ce théorème est de prendre une résolution injective de l'objet de $\mathfrak{C}$, de lui appliquer F, puis de prendre une résolution injective de chaque objet du complexe obtenu, et enfin d'appliquer G. Les foncteurs dérivés du composé $G \circ F$ s'obtiennent alors en calculant la cohomologie du complexe double ainsi obtenu, calcul réalisé par une suite spectrale comme expliqué précédemment.

3.4 La cohomologie étale

Nous allons bientôt définir une topologie de Grothendieck, dite topologie Weil-étale, donc nous étudierons ensuite quelques propriétés. Cette topologie est très proche de la topologie étale, donc nous commençons par rappeler la définition. Fixons un corps k.

Définition 3.4.1. Soient X et Y deux k-schémas. Un k-morphisme $f : X \longrightarrow Y$ est dit *étale* s'il est plat et non ramifié, ou, de manière équivalente, si pour tout $y \in Y$, la fibre $X \times_Y k(y)$ est isomorphe au spectre d'une k-algèbre étale, c'est-à-dire à une somme finie de spectres d'extensions séparables finies de k. On dit alors que X est *étale* sur Y, f étant sous-entendu.

De manière informelle, cette condition revient à dire que les fibres de f sont des ensembles finis de points ; la notion de morphisme étale est donc la traduction algébrique de la notion de *revêtement* en topologie. Il est alors plausible, et on le vérifie effectivement, que la catégorie des schémas étales sur un k-schéma admette des produits fibrés.

Définition 3.4.2. Soit X un k-schéma. On définit une topologie de Grothendieck ét_X, dite *topologie étale sur* X, en prenant pour $\text{cat}(\text{ét}_X)$ la catégorie des k-schémas étales sur X, et en posant

$$\text{cov}(\text{ét}_X) = \left\{ (f_i : U_i \longrightarrow U)_{i\in I} \;\middle|\; U = \bigcup_{i\in I} U_i \right\}.$$

Bien que X ne soit pas terminal dans la catégorie $\text{cat}(\text{ét}_X)$, il est naturel de définir les groupes de *cohomologie étale* $H^r_{\text{ét}}(X, \cdot)$ à partir des foncteurs dérivés à droite du foncteur $\Gamma(X, \cdot)$.

Exemple 3.4.3. Soit $\bar{k}$ un corps algébriquement clos, et considérons le cas du point $X = \text{Spec}\,(\bar{k})$. Par définition, les schémas étales sur X sont les $\text{Spec}(A)$, où A est une $\bar{k}$-algèbre étale, donc isomorphe à $\bar{k}^n$ pour un certain $n \in \mathbb{N}$; géométriquement, ce sont des ensembles finis de n points qui se projettent sur le point X, et les X-morphismes entre deux tels objets correspondent aux applications quelconques entre ces points. Le foncteur envoyant un ensemble fini I sur $\text{Spec}\,(\bar{k}^I)$ est donc une équivalence de catégories entre la catégorie des ensembles finis et la catégorie $\text{cat}(\text{ét}_{\text{Spec}(\bar{k})})$, à travers laquelle les produits fibrés correspondent aux intersections, et la notion de recouvrement $\text{cov}(\text{ét}_{\text{Spec}(\bar{k})})$, à la notion de recouvrement usuelle.

Soit $\mathcal{F}$ un faisceau étale de groupes abéliens sur $\text{Spec}(\bar{k})$. En écrivant la condition de faisceau associée au recouvrement vide de l'ensemble vide $\text{Spec}(\bar{k}^0)$, on trouve que $\mathcal{F}\big(\text{Spec}(\bar{k}^0)\big) = 0$; ensuite, pour tout $n \in \mathbb{N}^*$, la condition de faisceau appliquée au recouvrement de $\text{Spec}\,(\bar{k}^n)$ par des $\text{Spec}\,(\bar{k})$ disjoints montre que $\mathcal{F}\big(\text{Spec}(\bar{k}^n)\big) \simeq \mathcal{F}\big(\text{Spec}(\bar{k})\big)^n$. Par conséquent $\mathcal{F}$ est entièrement déterminé par ses sections sur le point $\text{Spec}\,(\bar{k})$, et ce foncteur de sections est une équivalence entre la catégorie des faisceaux étales de groupes abéliens sur $\text{Spec}\,(\bar{k})$ et la catégorie des groupes abéliens.

On peut généraliser la notion de fonction zêta d'une courbe en attachant

à toute variété projective X sur un corps fini $\mathbb{F}_q$ la série formelle

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{+\infty} \frac{|X(\mathbb{F}_{q^n})|}{n} T^n\right) \in \mathbb{Q}[[T]].$$

En 1949, Weil [Wei49] émit les célèbres conjectures suivantes :

Théorème 3.4.4 (Conjectures de Weil)**.** *Soit X une variété projective non singulière de dimension N sur $\mathbb{F}_q$.*

(Rationalité) La fonction zêta de X est une fraction rationnelle :

$$Z(X/\mathbb{F}_q, T) \in \mathbb{Q}(T).$$

(Équation fonctionnelle) Il existe un entier ϵ, appelé caractéristique d'Euler *de X, tel que*

$$Z(X/\mathbb{F}_q, 1/q^N T) = \pm q^{N\epsilon/2} T^\epsilon Z(X/\mathbb{F}_q, T).$$

(Hypothèse de Riemann) La fonction zêta de X se factorise en

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(T) \cdots P_{2N-1}(T)}{P_0(T) P_2(T) \cdots P_{2N}(T)},$$

où les P_i sont des polynômes en T à coefficients entiers, avec

$$P_0(T) = 1 - T, \qquad P_{2N}(T) = 1 - q^N T,$$

et pour $0 < i < 2N$, P_i se factorise dans $\overline{\mathbb{Q}}[T]$ en

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \omega_{i,j} T),$$

les $\omega_{i,j}$ étant des entiers algébriques de module $|\omega_{i,j}| = \sqrt{q}$.

La rationalité fut prouvée en 1960 par Dwork [Dwo60] grâce à des méthodes d'analyse fonctionnelle p-adique ; une version claire et détaillée de cette démonstration occupe le dernier chapitre de [Kob84]. Peu après, la cohomologie étale introduite entre autres par Artin et Grothendieck permit de démontrer l'équation fonctionnelle, tout en fournissant une nouvelle preuve de la rationalité. Enfin, Deligne [Del74] démontra l'hypothèse de Riemann en 1973 ; un survol de sa démonstration fait l'objet de [Kat76].

L'objet de la seconde partie de ce mémoire n'était donc autre que la démonstration de ces conjectures en dimension $N = 1$.

On montre que les facteurs $P_i(T)$ de la fonction zêta s'interprètent comme les réciproques des polynômes caractéristiques de l'action du Frobenius de $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ sur les espaces de cohomologie étale de la variété ; il apparaît donc que la cohomologie étale est intimement liée à la fonction zêta. Cette cohomologie donne toutefois des résultats apparemment imparfaits, ce qui suggère la possibilité d'une amélioration. Dans son article [Mil86], J.S. Milne démontre en effet les résultats suivants, que nous admettrons : si X est une variété projective non singulière sur un corps fini $\mathbb{F}_q$, alors, en notant $\mathbb{Z}$ le faisceau constant $\mathbb{Z}$ sur ét_X, $H^1_{\text{ét}}(X, \mathbb{Z}) = 0$, $H^2_{\text{ét}}(X, \mathbb{Z})$ est le $\mathbb{Q}/\mathbb{Z}$-dual d'un groupe abélien de type fini de rang 1, donc est isomorphe à $\mathbb{Q}/\mathbb{Z} \oplus A$ où A est un groupe abélien fini, et les $H^r_{\text{ét}}(X, \mathbb{Z})$ sont finis pour $r \geqslant 3$ et nuls pour $r \gg 0$; de plus, la *valeur essentielle*

$$Z^*(X/\mathbb{F}_q, 1) = \lim_{T \to 1} (T-1)^{-\operatorname{ord}_{T=1} Z(X/\mathbb{F}_q, T)} Z(X/\mathbb{F}_q, T)$$

de la fonction zêta de X en $s = 0$, c'est-à-dire en $T = 1$, est donnée par la formule

$$Z^*(X/\mathbb{F}_q, 1) = \frac{1}{\text{dét}(\delta)} \, |A| \prod_{r=3}^{+\infty} |H^r_{\text{ét}}(X, \mathbb{Z})|^{(-1)^r},$$

où δ est une application linéaire que nous définirons plus tard, et où A est le groupe abélien tel que $H^2_{\text{ét}}(X, \mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z} \oplus A$; par ce qui précède, le produit est en fait fini.

Notons que l'établissement de cette dernière formule utilise rien de moins que l'interprétation de la fonction zêta en termes de cohomologie étale, un théorème de Gabber extrait de [Gab83], la démonstration [Del80] de l'hypothèse de Riemann sur les variétés sur les corps finis par Deligne, et des calculs p-adiques effectués par Milne lui-même.

Il faut bien le reconnaître, cette formule de Milne que nous venons de donner est fort peu élégante : on aimerait que le produit, sorte de "caractéristique d'Euler multiplicative", commençât à $r = 0$ au lieu de $r = 3$, et qu'il ne soit pas nécessaire de bricoler ainsi le terme $r = 2$; de plus, le déterminant qui traîne n'arrange rien. Bien entendu, ce bricolage du $H^2_{\text{ét}}(X, \mathbb{Z})$ est inévitable du fait de son infinitude, pire, il n'est en fait même pas de type fini ; on peut donc soupçonner que la cohomologie étale n'est pas la plus adaptée à notre propos, ce qui motive la définition d'une nouvelle topologie de Grothendieck,

dont les groupes de cohomologie jouiront, on l'espère, de meilleures propriétés de finitude.

3.5 La cohomologie Weil-étale

Nous allons donc tenter de définir une nouvelle topologie de Grothendieck, la topologie Weil-étale, en modifiant légèrement la définition de la topologie étale.

Soit X un $\mathbb{F}_q$-schéma. Notons comme d'habitude $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, et soient $\pi_1 : \overline{X} \longrightarrow X$ et $\pi_2 : \overline{X} \longrightarrow \overline{\mathbb{F}_q}$ les projections associées. Le groupe de Galois absolu $G = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ est isomorphe au complété profini $\widehat{\mathbb{Z}}$ de $\mathbb{Z}$, et est topologiquement engendré par l'*automorphisme de Frobenius* $\Phi : x \mapsto x^q$. Le *groupe de Weil* est le sous-groupe $G_0 \simeq \mathbb{Z}$ de G engendré (non topologiquement) par Φ.

Si U et V sont deux $\mathbb{F}_q$-schémas, U étant de plus supposé connexe, un morphisme de $\mathbb{F}_q$-schémas de $\overline{U}$ vers $\overline{V}$ induit par π_2 un élément de G sur $\overline{\mathbb{F}_q}$.

Si X est un $\mathbb{F}_q$-schéma, on définit donc une nouvelle topologie de Grothendieck, la *topologie Weil-étale* $\mathcal{W}_X$, qui est à la topologie étale ce que le groupe de Weil est au groupe de Galois, comme suit : les objets de $\mathrm{cat}(\mathcal{W}_X)$ sont les schémas étales de type fini sur $\overline{X}$, et les morphismes entre deux tels objets $U \xrightarrow{f} \overline{X}$ et $V \xrightarrow{g} \overline{X}$, avec U connexe, sont les morphismes φ de $\mathbb{F}_q$-schémas de U dans V

- qui sont en fait des morphismes de X-schémas, et
- qui induisent un élément du groupe de Weil sur $\overline{\mathbb{F}_q}$,

c'est-à-dire que φ est un morphisme dans $\mathrm{cat}(\mathcal{W}_X)$ si et seulement si les deux conditions suivantes sont vérifiées :

- $\pi_1 \circ g \circ \varphi = \pi_1 \circ f$,
- $\pi_2 \circ g \circ \varphi = \pi_2 \circ f \circ \Phi^n$ pour un certain $n \in \mathbb{Z}$, et non $\widehat{\mathbb{Z}}$.

Si U n'est pas connexe, un morphisme est une collection de tels morphismes sur les composantes connexes de U. Autrement dit, le n de Φ^n a le droit de dépendre de la composante connexe ; tout ce qui importe, c'est qu'il reste dans $\mathbb{Z}$.

Quant aux recouvrements, ils sont définis comme pour la topologie étale :

$$\mathrm{cov}(\mathcal{W}_X) = \left\{ (f_i : U_i \longrightarrow U)_{i \in I} \;\middle|\; U = \bigcup_{i \in I} U_i \right\}.$$

Tout ceci est loisible, car on vérifie facilement l'existence des produits fibrés nécessaires.

Définition 3.5.1. La *cohomologie Weil-étale* $H^{\cdot}_{\mathcal{W}}(X, \cdot)$ est donnée par les foncteurs dérivés à droite de $\Gamma\big(\overline{X}, \cdot\big)^{G_0}$.

Nous allons à présent comparer les cohomologies étale et Weil-étale, et voir quels sont les avantages de la seconde sur la première.

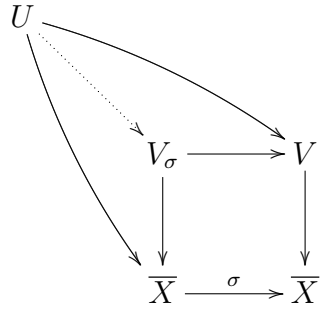
Définition 3.5.2. Soient X un schéma, H un sous-groupe du groupe des automorphismes de X, et $\mathcal{F}$ un faisceau sur X. On dit que H *agit sur* $\mathcal{F}$ si on s'est donné une famille de morphismes $\psi_\sigma : \mathcal{F} \longrightarrow \sigma_*\mathcal{F}$, $\sigma \in H$ *compatible*, c'est-à-dire que $\psi_\sigma \circ \psi_\tau = \psi_{\sigma\circ\tau}$, σ, $\tau \in H$.

Étant donnés un $\mathbb{F}_q$-schéma X et un faisceau Weil-étale $\mathcal{F}$ sur X, nous noterons $\rho(\mathcal{F})$ le faisceau étale sur $\overline{X}$ sous-jacent.

Proposition 3.5.3. *Soit X un $\mathbb{F}_q$-schéma. Le foncteur ρ est une équivalence entre la catégorie des faisceaux Weil-étales sur X et la catégorie des faisceaux étales sur $\overline{X}$ munis d'une action du groupe de Weil G_0.*

Démonstration. Pour tout schéma étale U sur $\overline{X}$ et pour tout $\sigma \in G_0$, notons $U_\sigma = U \times_{\overline{X}} \overline{X}$, où l'application de $\overline{X}$ dans $\overline{X}$ est donnée par σ. Comme $\sigma \in G_0$, la projection $U_\sigma \longrightarrow U$ est un morphisme dans la catégorie Weil-étale $\mathrm{cat}(\mathcal{W}_X)$, donc induit un morphisme (clairement fonctoriel en U) de $\mathcal{F}(U)$ dans $\mathcal{F}(U_\sigma)$, c'est-à-dire un morphisme $\psi_\sigma : \rho(\mathcal{F}) \longrightarrow \sigma_*\rho(\mathcal{F})$; il est clair que la famille ainsi obtenue est compatible.

Réciproquement, soit $\mathcal{F}$ est un faisceau étale sur $\overline{X}$ muni d'une action de G_0. Un morphisme $U \longrightarrow V$ dans $\mathrm{cat}(\mathcal{W}_X)$ donne par définition lieu à un diagramme commutatif de la forme



où σ est un élément du groupe de Weil G_0, d'où le $\overline{X}$-morphisme de U dans V_σ, qui induit à son tour le morphisme

$$\mathcal{F}(V) \xrightarrow{(\psi_\sigma)^*} \mathcal{F}(V_\sigma) \longrightarrow \mathcal{F}(U).$$

On peut donc voir $\mathcal{F}$ comme un faisceau Weil-étale sur X. □

En combinant ceci aux résultats établis par l'exemple 3.4.3, on obtient immédiatement le

Corollaire 3.5.4. *La catégorie des faisceaux de groupes abéliens Weil-étales sur $X = \mathrm{Spec}(\mathbb{F}_q)$ est équivalente à la catégorie des G_0-modules. Par cette équivalence, la cohomologie Weil-étale $H^r_{\mathcal{W}}\big(\mathrm{Spec}(\mathbb{F}_q), \mathcal{F}\big)$ est canoniquement isomorphe à la cohomologie des groupes $H^r\big(G_0, \mathcal{F}(\overline{\mathbb{F}_q})\big)$.*

On en déduit un point d'appui pour comparer les cohomologies étale et Weil-étale :

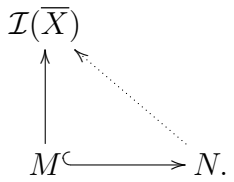
Lemme 3.5.5. *Soit X un $\mathbb{F}_q$-schéma, et soit $\mathcal{F}$ un faisceau Weil-étale sur X. Il existe une suite spectrale de termes initiaux*

$$E_2^{p,q} = H^p\big(G_0, H^q_{\text{ét}}(\overline{X}, \rho(\mathcal{F}))\big)$$

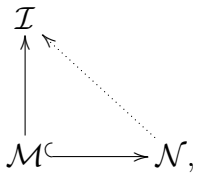
aboutissant aux groupes de cohomologie Weil-étale $H^{p+q}_{\mathcal{W}}(X, \mathcal{F})$.

Démonstration. Ceci résulte directement du théorème 3.3.2. En effet, la cohomologie étale se calcule par définition en dérivant le composé du foncteur sections globales $\Gamma(\overline{X}, \cdot)$ et du foncteur points fixes $\cdot^{G_0}$. Le second est bien évidemment exact à gauche ; pour conclure, il suffit donc de montrer que si $\mathcal{I}$ est un faisceau Weil-étale sur X, alors $\mathcal{I}(\overline{X})$ est un G_0-module cohomologiquement trivial. Nous allons en fait montrer que c'est un G_0-module *injectif*.

Considérons en effet un diagramme de G_0-modules de la forme



On cherche un morphisme de G_0-modules faisant commuter ce diagramme. Mais par définition de la catégorie Weil-étale, notre diagramme donne lieu au diagramme de faisceaux Weil-étales suivant :



où $\mathcal{M}$ et $\mathcal{N}$ désignent les faisceaux constants égaux respectivement à M et N. Par injectivité du faisceau $\mathcal{I}$, on trouve un morphisme faisant commuter ce diagramme, morphisme qu'il n'y a plus qu'à évaluer en $\overline{X}$. □

On peut donc associer fonctoriellement à tout faisceau étale $\mathcal{F}$ sur X une suite spectrale

$$H^p\big(G_0, H^q_{\text{ét}}(\overline{X}, \rho\pi_1^*\mathcal{F})\big) \Longrightarrow H^{p+q}_{\mathcal{W}}(X, \pi_1^*\mathcal{F})$$

(Rappelons que π_1 est la projection de $\overline{X}$ sur X). De même, à ce faisceau étale sur X, on associe fonctoriellement une suite spectrale

$$H^p\big(G, H^q_{\text{ét}}(\overline{X}, \pi_1^*\mathcal{F})\big) \Longrightarrow H^{p+q}_{\text{ét}}(X, \mathcal{F}).$$

Il en résulte que, comme espéré, les groupes de cohomologie Weil-étale sont plus sympathiques que les groupes de cohomologie étale :

Théorème 3.5.6. *Soit X une variété projective non singulière sur $\mathbb{F}_q$. Les groupes de cohomologie Weil-étale $H^r_{\mathcal{W}}(X, \mathbb{Z})$ sont tous de type fini, finis si $r \geqslant 2$, et nuls pour $r \gg 0$.*

Démonstration. D'après ce qu'on vient de voir, on a les deux suites spectrales

$$H^p\big(G_0, H^q_{\text{ét}}(\overline{X}, \mathbb{Z})\big) \Longrightarrow H^{p+q}_{\mathcal{W}}(X, \mathbb{Z})$$

et

$$H^p\big(G, H^q_{\text{ét}}(\overline{X}, \mathbb{Z})\big) \Longrightarrow H^{p+q}_{\text{ét}}(X, \mathbb{Z}).$$

Rappelons que d'après [Mil86], on a $H^1_{\text{ét}}(X, \mathbb{Z}) = 0$, $H^2_{\text{ét}}(X, \mathbb{Z}) = \mathbb{Q}/\mathbb{Z} \oplus A$, où A est fini, et les $H^r_{\text{ét}}(X, \mathbb{Z})$ pour $r \geqslant 3$ sont finis et nuls pour $r \gg 0$. En comparant nos deux suites spectrales grâce au lemme 3.1.14, on trouve alors que $H^1_{\mathcal{W}}(X, \mathbb{Z}) = \mathbb{Z}$, que $H^2_{\mathcal{W}}(X, \mathbb{Z}) = A$ est fini, et que $H^r_{\mathcal{W}}(X, \mathbb{Z}) \simeq H^r_{\text{ét}}(X, \mathbb{Z})$ pour $r \geqslant 3$, d'où le résultat. □

Essayons à présent de généraliser ceci à des variétés pas forcément projectives et éventuellement singulières.

Lemme 3.5.7. *Soit U une courbe sur $\mathbb{F}_q$. Soit $j : U \longrightarrow X$ une complétion projective de U, c'est-à-dire que j est une immersion ouverte de U dans une courbe projective X dans laquelle U est dense. Soit $\mathcal{F}$ un faisceau de groupes abéliens Weil-étale sur U.*

(a) Les groupes de cohomologie Weil-étale $H^r_{\mathcal{W}}(X, j_!\mathcal{F})$ sont indépendants du choix de la complétion projective (X, j), et

(b) si $\mathcal{F}$ est le faisceau constant $\mathbb{Z}$, ils sont de type fini.

Démonstration. Pour montrer (a), considérons deux complétions $j : U \longrightarrow X$ et $j' : U \longrightarrow X'$. Quitte à remplacer X' par l'adhérence de l'image de U dans $X \times X'$, on peut supposer qu'il existe un morphisme $\Pi : X' \longrightarrow X$ tel que $\Pi \circ j' = j$. Il est clair que Π est fini, donc $\overline{\Pi}$ aussi, et on montre alors que $\overline{\Pi}_*$ est exact en topologie étale. Par conséquent, pour tout faisceau Weil-étale $\mathcal{G}$ sur X', les groupes de cohomologie étale $H^{\cdot}_{\text{ét}}\big(\overline{X'}, \rho(\mathcal{G})\big)$ et $H^{\cdot}_{\text{ét}}\big(\overline{X}, \overline{\Pi}_*\rho(\mathcal{G})\big)$ sont isomorphes. Grâce à la suite spectrale du lemme 3.5.5, on en déduit que les groupes de cohomologie Weil-étale $H^{\cdot}_{\mathcal{W}}\big(X', \mathcal{G}\big)$ et $H^{\cdot}_{\mathcal{W}}\big(X, \overline{\Pi}_*\mathcal{G}\big)$ sont eux aussi isomorphes. Comme $j'_!\mathcal{F} \simeq \overline{\Pi}_* j_!\mathcal{F}$, il suffit de prendre $\mathcal{G} = j_!\mathcal{F}$ pour conclure.

Passons à (b). Supposons qu'on ait un sous-schéma U qui est un ouvert dense d'un sous-schéma V lui-même ouvert dense de la courbe projective non singulière X. Notons $i : U \longrightarrow X$ et $j : V \longrightarrow X$ les immersions ouvertes, et soit $\iota : V - U \longrightarrow X$ l'immersion fermée. On a alors la suite exacte

$$0 \longrightarrow i_!\mathbb{Z} \longrightarrow j_!\mathbb{Z} \longrightarrow \iota_*\mathbb{Z} \longrightarrow 0.$$

Nous allons utiliser la suite exacte longue de cohomologie Weil-étale associée pour montrer le résultat pour les courbes non singulières projectives, puis pour les courbes non singulières, et enfin pour les courbes quelconques. Dans le premier cas, c'est une application immédiate du théorème 3.5.6. Ensuite, si U est une courbe non-singulière, plongeons-la dans une courbe projective non singulière X, et prenons $V = X$. Alors $V - U$ est de dimension 0, donc les groupes de cohomologie Weil-étale de V et de $V - U$ pour les faisceaux considérés sont de type fini d'après le théorème 3.5.6 ; la suite exacte longue montre alors qu'il en est de même pour la cohomologie de U, d'où le résultat pour les courbes non singulières. Enfin, prenons V une courbe quelconque,

et soit U l'ensemble des ses points non singuliers. Alors les cohomologies de U et de $V - U$ sont de type fini, donc celle de V aussi. □

Théorème 3.5.8. *Soit U une courbe ou une surface sur $\mathbb{F}_q$. On suppose que U est non singulière et quasi projective. En résolvant les singularités, on trouve une immersion ouverte $j : U \longrightarrow X$ de U dans une variété projective non singulière X dans laquelle U est dense. Alors les groupes de cohomologie Weil-étale $H^r_{\mathcal{W}}(X, j_!\mathbb{Z})$ sont indépendants du choix de la complétion projective (X, j), tous de type fini, et nuls pour $r \gg 0$.*

Démonstration. Posons $Z = X - U$, et notons $\iota : Z \longrightarrow X$ l'immersion fermée correspondante. Comme ι_* est exact puisque Z est fermé, on a $H^r_{\mathcal{W}}(X, \iota_*\mathbb{Z}) \simeq H^r_{\mathcal{W}}(Z, \mathbb{Z})$ pour tout $r \in \mathbb{N}$, et comme Z est projectif non singulier, ces groupes de cohomologie sont de type fini et nuls pour $r \gg 0$. D'après le théorème 3.5.6, c'est également le cas des $H^r_{\mathcal{W}}(X, \mathbb{Z})$. En considérant la suite exacte longue de cohomologie associée à la suite exacte

$$0 \longrightarrow j_!\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \iota_*\mathbb{Z} \longrightarrow 0,$$

on en déduit qu'il en va de même pour les $H^r_{\mathcal{W}}(X, j_!\mathbb{Z})$.

Nous nous contenterons d'esquisser la preuve de l'indépendance. Soient $j : U \longrightarrow X$ et $j' : U \longrightarrow X'$ deux immersions comme ci-dessus. Posons $Y = X \times X'$. U se plonge dans Y par j et j' ; notons Z son adhérence. En résolvant les singularités, on peut trouver une $\Pi : Z' \longrightarrow Z$, où Z' est projective et non singulière ; alors, quitte à remplacer X' par Z', on peut, comme dans la démonstration précédente, supposer qu'il existe un morphisme $\Pi : X' \longrightarrow X$ tel que $\Pi \circ j' = j$. On a alors $\Pi_* j'_!\mathbb{Z} = j_!\mathbb{Z}$, donc Π fournit un morphisme entre $H^{\cdot}_{\mathcal{W}}(X, j_!\mathbb{Z})$ et $H^{\cdot}_{\mathcal{W}}(X', j'_!\mathbb{Z})$, dont il s'agit de montrer que s'est un isomorphisme. Pour ce faire, on remarque que c'est bien un isomorphisme pour $r \gg 0$ puisque les deux membres sont alors nuls, et on procède ensuite à une récurrence descendante sur r. □

La cohomologie Weil-étale semble donc se comporter aussi bien qu'on pourrait le souhaiter ; lançons nous donc dans l'amélioration de la formule de Milne.

3.6 La conjecture de Lichtenbaum

Avant d'attaquer le vif du sujet, préparons le terrain en nous intéressant aux caractéristiques d'Euler.

Le cadre est le suivant. Dans une catégorie abélienne $\mathfrak{C}$, on se donne un δ-foncteur $H^{\cdot}$ de $\mathfrak{C}$ dans la catégorie des groupes abéliens, H^r étant nul pour $r < 0$, et une transformation naturelle $\theta : H^r \longrightarrow H^{r+1}$ définie pour tout $r \in \mathbb{Z}$ et de carré nul. Pour tout objet $C \in \mathfrak{C}$, on a donc un complexe

$$\cdots \xrightarrow{\theta} H^{r-1}(C) \xrightarrow{\theta} H^r(C) \xrightarrow{\theta} H^{r+1}(C) \xrightarrow{\theta} \cdots,$$

dont on note $h^{\cdot}(C)$ la cohomologie. On dira que l'objet $C \in \mathfrak{C}$ est *θ-fini*, ou que les $H^r(C)$ sont *θ-finis*, si les $h^r(C)$ sont tous finis et si $H^r(C)$ est nul pour $r \gg 0$, auquel cas on définit la *caractéristique d'Euler*

$$\chi(C) = \prod_{r=0}^{+\infty} |h^r(C)|^{(-1)^r}.$$

C'est donc une caractéristique d'Euler multiplicative, au lieu de la version additive usuelle ; ce choix s'explique par le fait que la version additive est inefficace pour notre propos, comme on s'en apercevra bientôt (cf. conjecture 3.6.2(b)).

Les résultats dont nous aurons besoin sont les suivants :

Proposition 3.6.1. *Soit* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *une suite exacte courte dans* $\mathfrak{C}$.

(a) [Multiplicativité] Si A, B et C sont tous les trois θ-finis, alors $\chi(B) = \chi(A)\chi(C)$.

(b) Si B et C sont θ-finis, et si les $H^r(B)$ sont tous finis dès que $r \geqslant 2$, alors A est θ-fini.

Démonstration. Tout cela est très élémentaire, et un peu fastidieux ; aussi nous contenterons-nous de montrer (a). Nommons les morphismes de la suite exacte longue de cohomologie comme suit :

$$\cdots \xrightarrow{\gamma^{r-1}} H^r(A) \xrightarrow{\alpha^r} H^r(B) \xrightarrow{\beta^r} H^r(C) \xrightarrow{\gamma^r} H^{r+1}(A) \xrightarrow{\alpha^{r+1}} \cdots.$$

Posons $D^r = \operatorname{Im}\alpha^r$, $E^r = \operatorname{Im}\beta^r$, et $F^r = \operatorname{Im}\gamma^r$. Notons l'action de θ sur $H^r(A)$ par f^r, sur $H^r(B)$, par g^r, et sur $H^r(C)$, par h^r. Enfin, notons δ^r, ε^r et φ^r l'action induite par θ sur D^r, E^r et F^r. On a alors trois diagrammes

commutatifs du style

$$\begin{array}{ccccccccc}
0 & \longrightarrow & D^0 & \longrightarrow & H^0(B) & \xrightarrow{\beta^0} & E^0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta^0} & & \downarrow{\scriptstyle g^0} & & \downarrow{\scriptstyle \varepsilon^0} & & \\
0 & \longrightarrow & D^1 & \longrightarrow & H^1(B) & \xrightarrow{\beta^1} & E^1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta^1} & & \downarrow{\scriptstyle g^1} & & \downarrow{\scriptstyle \varepsilon^1} & & \\
0 & \longrightarrow & D^2 & \longrightarrow & H^2(B) & \xrightarrow{\beta^2} & E^2 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta^2} & & \downarrow{\scriptstyle g^2} & & \downarrow{\scriptstyle \varepsilon^2} & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array},$$

d'où par le lemme du serpent autant de suites exactes longues

$$0 \longrightarrow H^0(\delta) \longrightarrow H^0(g) \longrightarrow H^0(\varepsilon) \longrightarrow H^1(\delta) \longrightarrow H^1(g) \longrightarrow H^1(\varepsilon) \longrightarrow \cdots,$$

$$0 \longrightarrow H^0(\varepsilon) \longrightarrow H^0(h) \longrightarrow H^0(\varphi) \longrightarrow H^1(\varepsilon) \longrightarrow H^1(h) \longrightarrow H^1(\varphi) \longrightarrow \cdots,$$

$$0 \longrightarrow H^0(f) \longrightarrow H^0(\delta) \longrightarrow H^0(\varphi) \longrightarrow H^1(f) \longrightarrow H^1(\delta) \longrightarrow H^1(\varphi) \longrightarrow \cdots,$$

où bien entendu $H^r(\delta)$ signifie $\operatorname{Ker}(\delta^r)/\operatorname{Im}(\delta^{r-1})$, *etc.*

Par hypothèse, les $H^r(f)$, $H^r(g)$ et $H^r(h)$ sont finis ; une récurrence immédiate montre alors qu'il en est de même des $H^r(\delta)$, $H^r(\varepsilon)$ et $H^r(\varphi)$. De plus, $H^r(A)$, $H^r(B)$ et $H^r(C)$ sont nuls pour $r \gg 0$, donc D^r, E^r et F^r aussi. Par conséquent toutes les caractéristiques d'Euler sont bien définies, et, avec les notations naturelles, on a les relations

$$\chi(D)\chi(E) = \chi(B), \quad \chi(E)\chi(F) = \chi(C), \text{ et } \chi(A)\chi(F) = \chi(D),$$

d'où $\chi(A)\chi(C) = \chi(B)$ comme voulu. □

Voyons comment incarner ce qui précède. Le corollaire 3.5.4 nous dit que

$$H^1_{\mathcal{W}}\big(\operatorname{Spec}(\mathbb{F}_q), \mathbb{Z}\big) \simeq H^1(G_0, \mathbb{Z}) \simeq \operatorname{Hom}_{\mathbb{Z}}(G_0, \mathbb{Z}),$$

le second isomorphisme provenant du fait que G_0 agit trivialement sur le faisceau constant $\mathbb{Z}$. Le fait que $G_0 \simeq \mathbb{Z}$ nous invite alors à considérer l'élément "identité" de $\mathrm{Hom}_{\mathbb{Z}}(G_0, \mathbb{Z})$, c'est-à-dire celui qui envoie le Frobenius sur 1 ; soit $\theta \in H^1_{\mathcal{W}}\big(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}\big)$ l'élément correspondant. Plus généralement, si X est un $\mathbb{F}_q$-schéma, on peut tirer θ en arrière le long du morphisme structural $X \longrightarrow \mathrm{Spec}(\mathbb{F}_q)$; l'élément de $H^1_{\mathcal{W}}(X, \mathbb{Z})$ ainsi obtenu sera encore noté θ. Pour tout faisceau Weil-étale $\mathcal{F}$ sur X, on a l'application naturelle $\mathcal{F} \underset{\mathbb{Z}}{\otimes} \mathbb{Z} \longrightarrow \mathbb{Z}$ induite par $x \otimes n \mapsto nx$; ainsi le cup-produit avec θ induit-il des morphismes de $H^r_{\mathcal{W}}(X, \mathcal{F})$ vers $H^{r+1}_{\mathcal{W}}(X, \mathcal{F})$. Or $\theta \in H^1(G_0, \mathbb{Z})$, donc $\theta \cup \theta$ habite dans $H^2(G_0, \mathbb{Z})$, qui est nul d'après le théorème de Schreier 3.1.8 ; ainsi, le cup-produit par θ nous permet de munir les groupes de cohomologie Weil-étale d'une structure de complexe, et d'appliquer ce qui précède. On notera alors pour alléger $\chi(X, \mathcal{F})$ plutôt que $\chi\big(H^{\cdot}_{\mathcal{W}}(X, \mathcal{F})\big)$.

Nous disposons à présent du matériel nécessaire pour étayer la conjecture suivante.

Conjecture 3.6.2 (Lichtenbaum, 2003)**.** Soit U une variété quasi-projective sur $\mathbb{F}_q$, et soit $j : U \longrightarrow X$ une complétion projective de U. Supposons que U est non singulière, ou que U est une courbe. Alors

(a) Les groupes de cohomologie Weil-étale $H^r_{\mathcal{W}}(X, j_!\mathbb{Z})$ sont indépendants du choix de j, de type fini, et nuls pour $r \gg 0$.

(b) La "première caractéristique d'Euler additive" est nulle :

$$\sum_{r=0}^{+\infty} (-1)^r \ \mathrm{rg}_{\mathbb{Z}} \left(H^r_{\mathcal{W}}(X, j_!\mathbb{Z}) \right) = 0.$$

(c) L'ordre d'annulation de la fonction zêta de U en $T = 1$ (c'est-à-dire en $s = 0$) est égal à la "seconde caractéristique d'Euler additive" :

$$\mathrm{ord}_{T=1} \, Z(U/\mathbb{F}_q, T) = \sum_{r=0}^{+\infty} (-1)^r r \ \mathrm{rg}_{\mathbb{Z}} \left(H^r_{\mathcal{W}}(X, j_!\mathbb{Z}) \right).$$

(d) Les groupes de cohomologie Weil-étale $H^r_{\mathcal{W}}(X, j_!\mathbb{Z})$ sont θ-finis,

(e) La valeur essentielle $Z^*(U/\mathbb{F}_q, 1) = \lim_{T \to 1} (T-1)^{-\mathrm{ord}_{T=1} Z(U/\mathbb{F}_q, T)} Z(U/\mathbb{F}_q, T)$ de la fonction zêta de U en $T = 1$ (ou $s = 0$) est égale, au signe près, à la caractéristique d'Euler multiplicative :

$$Z^*(U/\mathbb{F}_q, 1) = \pm \chi(X, j_!\mathbb{Z}).$$

Afin de justifier cette conjecture, nous allons la démontrer dans le cas d'une variété projective non singulière, dans le cas d'une surface non singulière se plongeant dans une surface projective elle aussi non singulière, et enfin dans le cas d'une courbe.

Au préalable, donnons enfin la définition du δ apparaissant dans la formule de Milne : il s'agit du cup-produit avec l'analogue étale de θ dans $H^1\big(G,\widehat{\mathbb{Z}}\big) \simeq Hom_{\mathbb{Z}}\big(G,\widehat{\mathbb{Z}}\big) \ni \mathrm{Id}$, de $H^0_{\text{ét}}\big(X,\widehat{\mathbb{Z}}\big)$ vers $H^1_{\text{ét}}\big(X,\widehat{\mathbb{Z}}\big)$. Comme on a les identifications $H^r_{\text{ét}}\big(X,\widehat{\mathbb{Z}}\big) \simeq H^r_{\mathcal{W}}(X,\mathbb{Z}) \underset{\mathbb{Z}}{\otimes} \widehat{\mathbb{Z}}$, on en déduit que

$$\text{dét}(\delta) = \pm \left| \text{Coker}\left(H^0_{\mathcal{W}}(X,\mathbb{Z}) \xrightarrow{\cup\theta} H^1_{\mathcal{W}}(X,\mathbb{Z})\right)\right|.$$

Démonstration. Commençons par le cas où $U = X$ est projective non singulière ; on ne peut alors prendre que $j = \mathrm{Id}_X$. Tout d'abord, le (a) a fait l'objet du théorème 3.5.6. Plus précisément, au cours de la démonstration de ce théorème, on a en fait calculé que $H^0_{\mathcal{W}}(X,\mathbb{Z}) = H^1_{\mathcal{W}}(X,\mathbb{Z}) = \mathbb{Z}$, et que les $H^r_{\mathcal{W}}(X,\mathbb{Z})$ sont finis pour $r \geqslant 2$; il en résulte que

$$\sum_{r=0}^{+\infty} (-1)^r \ \mathrm{rg}_{\mathbb{Z}}\left(H^r_{\mathcal{W}}(X, j_!\mathbb{Z})\right) = 0,$$

ce qui prouve (b), et que

$$\sum_{r=0}^{+\infty} (-1)^r r \ \mathrm{rg}_{\mathbb{Z}}\left(H^r_{\mathcal{W}}(X, j_!\mathbb{Z})\right) = -1;$$

or Deligne, en démontrant l'hypothèse de Riemann, a prouvé que parmi les facteurs

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)}$$

de la fonction zêta de X, seul $P_0(T) = 1 - T$ s'annule en $T = 1$; $Z(X/\mathbb{F}_q, T)$ y a donc un pôle simple et (c) est donc vérifié.

Compte tenu des calculs précédents, le complexe de cohomologie Weil-étale s'écrit

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cup\theta} \mathbb{Z} \xrightarrow{\cup\theta=0} A \xrightarrow{\cup\theta} H^3_{\mathcal{W}}(X,\mathbb{Z}) \xrightarrow{\cup\theta} \cdots,$$

il est donc clairement θ-fini donc (d) est satisfait ; de plus on a

$$h^0\big(H^{\cdot}_{\mathcal{W}}(X,\mathbb{Z})\big) = 0,$$

$$h^1\big(H^{\cdot}_{\mathcal{W}}(X,\mathbb{Z})\big) = \mathrm{Coker}(\mathbb{Z} \xrightarrow{\cup\theta} \mathbb{Z}) = |\,\mathrm{dét}(\delta)|,$$
$$h^2\big(H^{\cdot}_{\mathcal{W}}(X,\mathbb{Z})\big) = \mathrm{Ker}\,\big(A \xrightarrow{\cup\theta} H^3_{\mathcal{W}}(X,\mathbb{Z})\big)$$

et, pour $r \geqslant 3$, puisque $H^{r-1}_{\mathcal{W}}(X,\mathbb{Z})$, $H^r_{\mathcal{W}}(X,\mathbb{Z})$ et $H^{r+1}_{\mathcal{W}}(X,\mathbb{Z})$ sont finis, on a, en notant pour alléger

$$\begin{array}{l} z^r = \mathrm{Ker}\,\big(H^r_{\mathcal{W}}(X,\mathbb{Z}) \xrightarrow{\cup\theta} H^{r+1}_{\mathcal{W}}(X,\mathbb{Z})\big), \\ b^r = \mathrm{Im}\,\big(H^{r-1}_{\mathcal{W}}(X,\mathbb{Z}) \xrightarrow{\cup\theta} H^r_{\mathcal{W}}(X,\mathbb{Z})\big) \qquad \text{et} \\ h^r = h^r\big(H^{\cdot}_{\mathcal{W}}(X,\mathbb{Z})\big) = z^r/b^r, \end{array}$$

$$|h^r| = \frac{|z^r|}{|b^r|} = \frac{|z^r|}{|H^{r-1}_{\mathcal{W}}(X,\mathbb{Z})|/|z^{r-1}|},$$

d'où le calcul télescopique de la caractéristique d'Euler :

$$\begin{aligned} \chi(X,\mathbb{Z}) = \prod_{r=0}^{+\infty} |h^r|^{(-1)^r} &= \frac{1}{|\,\mathrm{dét}(\delta)|}|z^2| \prod_{r\geqslant 3} \left(\frac{|z^r|}{|H^{r-1}_{\mathcal{W}}(X,\mathbb{Z})|/|z^{r-1}|}\right)^{(-1)^r} \\ &= \pm\frac{1}{\mathrm{dét}(\delta)} \prod_{r\geqslant 2} |H^r_{\mathcal{W}}(X,\mathbb{Z})|^{(-1)^r} \\ &= \pm\frac{1}{\mathrm{dét}(\delta)}|A| \prod_{r\geqslant 3} |H^r_{\text{ét}}(X,\mathbb{Z})|^{(-1)^r} \\ &= \pm Z^*(X/\mathbb{F}_q,1) \end{aligned}$$

d'après la formule de Milne, ce qui démontre (e).

Nous avons donc démontré la conjecture pour les variétés projectives non-singulières. Dans les autres cas, soit $Z = X - U$, et notons $\iota : Z \longrightarrow X$ l'immersion fermée correspondante, de sorte qu'on ait une suite exacte courte

$$0 \longrightarrow j_!\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow i_*\mathbb{Z} \longrightarrow 0.$$

Le (a) a fait l'objet du lemme 3.5.7 pour les courbes, et du théorème 3.5.8 pour les surfaces. Par ailleurs, sur la formule

$$\exp\left(\sum_{n=1}^{+\infty} N_n \frac{T^n}{n}\right)$$

de la fonction zêta d'une variété sur $\mathbb{F}_q$, on voit clairement que $Z(X/\mathbb{F}_q,T) = Z(U/\mathbb{F}_q,T)Z(Z/\mathbb{F}_q,T)$, d'où en particulier $Z^*(X/\mathbb{F}_q,1) = Z^*(U/\mathbb{F}_q,1)Z^*(Z/\mathbb{F}_q,1)$.

Or la proposition 3.6.1 nous dit que la caractéristique d'Euler est multiplicative ; ainsi, si la conjecture est vraie par Z, alors (d) et (e) sont vérifiés par U. De même, en considérant la suite exacte longue de cohomologie associée à la suite exacte courte évoquée ci-dessus, on trouve que

$$\mathrm{rg}_{\mathbb{Z}}\, H^1_{\mathcal{W}}(X, j_!\mathbb{Z}) = \mathrm{rg}_{\mathbb{Z}}\, H^0_{\mathcal{W}}(X, i_*\mathbb{Z}) - 1,$$

$$\mathrm{rg}_{\mathbb{Z}}\, H^2_{\mathcal{W}}(X, j_!\mathbb{Z}) = \mathrm{rg}_{\mathbb{Z}}\, H^1_{\mathcal{W}}(X, i_*\mathbb{Z}) - 1,$$

$$\text{et} \quad \mathrm{rg}_{\mathbb{Z}}\, H^r_{\mathcal{W}}(X, j_!\mathbb{Z}) = \mathrm{rg}_{\mathbb{Z}}\, H^{r-1}_{\mathcal{W}}(X, i_*\mathbb{Z}) \text{ pour } r \geqslant 3,$$

ce qui montre que si Z vérifie la conjecture, alors U vérifie (b) et (c) puisque $\mathrm{ord}_{T=1}\, Z(U/\mathbb{F}_q, T) = \mathrm{ord}_{T=1}\, Z(X/\mathbb{F}_q, T) - \mathrm{ord}_{T=1}\, Z(Z/\mathbb{F}_q, T)$.

Ceci démontre immédiatement la conjecture pour les courbes. Enfin, pour les surfaces, il suffit de remarquer que $Z = X - U$ est une courbe, donc vérifie la conjecture.

□

Notons que la validité de cette conjecture pour les variétés de toutes dimensions impliquerait la possibilité d'utiliser la cohomologie Weil-étale pour étudier le comportement des fonctions zêta des variétés sur les corps finis non plus seulement en $s = 0$, mais en toutes valeurs entières relatives de s. En effet, la relation $\zeta(X \times \mathbb{A}^m_{\mathbb{F}_q} / \mathbb{F}_q, s) = \zeta(X/\mathbb{F}_q, s - m)$, qui est évidente sur la formule

$$\zeta(X/\mathbb{F}_q, s) = \exp\left(\sum_{n=1}^{+\infty} \frac{N_n}{n} q^{-ns}\right),$$

permet de ramener l'étude de la fonction zêta d'une variété en $s = -m \in \mathbb{Z}_-$ à l'application de la conjecture de Lichtenbaum à $X \times \mathbb{A}^m$; et pour effectuer cette étude en $s = m \in \mathbb{N}$, l'équation fonctionnelle nous ramène au cas précédent.

4 Perspectives

En guise de conclusion, évoquons quelques applications ou extensions récentes de la cohomologie Weil-étale.

4.1 La cohomologie étale pour les corps de nombres

Dans l'article [Lic05] que nous avons étudié, Lichtenbaum introduisait la cohomologie Weil-étale pour les variétés algébriques sur un corps fini, autrement dit, pour les schémas de type fini sur $\mathbb{F}_q$. Dans un nouvel article [Lic09] paru en 2009, il explique chercher à définir une cohomologie Weil-étale pour les schémas de type fini sur $\mathbb{Z}$, le but étant encore d'obtenir des groupes de cohomologie de type fini et en nombre fini, et de relier les valeurs de fonctions zêta à certaines caractéristiques d'Euler multiplicatives. Il ne propose toutefois pour l'instant que des résultats portant sur l'anneau des entiers d'un corps global, ce qui est déjà très intéressant, en vue de l'hypothèse de Riemann par exemple. Examinons donc ces résultats.

Commençons par définir la caractéristique d'Euler multiplicative, comme nous l'avions fait dans le cadre des variétés sur un corps fini. Lichtenbaum définit tout d'abord le *déterminant* d'une suite exacte de $\mathbb{R}$-espaces vectoriels de dimensions finies

$$0 \longrightarrow V_0 \xrightarrow{T_0} V_1 \xrightarrow{T_1} \cdots \xrightarrow{T_{n-1}} V_n \longrightarrow 0$$

munis de bases $(e_j^i)_{1 \leqslant j \leqslant \dim V_i}$, en procédant inductivement sur la longueur n de la suite en question :

- si $n = 1$, le déterminant de la suite est celui de la matrice représentant l'application linéaire $V_0 \xrightarrow{T_0} V_1$ sur les bases (e_j^0) et (e_j^1) ;
- si $n = 2$, soient $v_j^1 = T_0(e_j^0)$, $1 \leqslant j \leqslant \dim V_0$, et choisissons w_j^1, $1 \leqslant j \leqslant \dim V_2$, tels que $T_1(w_j^1) = e_j^2$; alors la puissance extérieure maximale $\bigwedge^{\dim V_1} V_1$ est un espace de dimension 1 généré par

  $$v_1^1 \wedge \cdots \wedge v_{\dim V_0}^1 \wedge w_1^1 \wedge \cdots \wedge w_{\dim V_2}^1,$$

  qui est clairement indépendant du choix des w_j^1, et on définit le déterminant de la suite exacte comme étant le $\delta \in \mathbb{R}$ tel que

  $$v_1^1 \wedge \cdots \wedge v_{\dim V_0}^1 \wedge w_1^1 \wedge \cdots \wedge w_{\dim V_2}^1 = \delta\, e_1^1 \wedge \cdots \wedge e_{\dim V_1}^1;$$

- enfin, si $n > 2$, notons $I \subseteq V_{n-1}$ l'image de l'avant-dernière application T_{n-2}, de sorte que la suite exacte se casse en deux morceaux

$$0 \longrightarrow V_0 \xrightarrow{T_0} V_1 \xrightarrow{T_1} \cdots \xrightarrow{T_{n-2}} I \longrightarrow 0 \qquad (1) \qquad \text{et}$$

$$0 \longrightarrow I \longrightarrow V_{n-1} \xrightarrow{T_{n-1}} V_n \longrightarrow 0 \qquad (2)\ ;$$

on munit alors I d'une base quelconque, et on définit le déterminant de la grande suite exacte comme valant $\delta_1(\delta_2)^{(-1)^{n-1}}$, où δ_1 est le déterminant de (1), et δ_2, celui de (2), ce qui ne dépend pas du choix d'une base pour I, comme on le vérifie facilement.

Ensuite, si $A_0, \cdots, A_n$ sont des groupes abéliens de type fini (en pratique, ce seront les groupes de cohomologie Weil-étale) tels qu'il existe une suite exacte

$$0 \longrightarrow V_0 \xrightarrow{T_0} V_1 \xrightarrow{T_1} \cdots \xrightarrow{T_{n-1}} V_n \longrightarrow 0,$$

où $V_i = A_i \underset{\mathbb{Z}}{\otimes} \mathbb{R}$, on définit leur caractéristique d'Euler par la formule

$$\chi(A_0, \cdots, A_n, T_0, \cdots, T_{n-1}) = \frac{1}{\delta} \prod_{i=0}^{n} |(A_i)_{\text{tor}}|^{(-1)^i},$$

où δ est le déterminant de la suite exacte des V_i munis de $\mathbb{R}$-bases provenant de $\mathbb{Z}$-bases des groupes abéliens libres $A_i/(A_i)_{\text{tor}}$. De telles bases ne sont certes pas uniques ; il est cependant clair que changer ces bases multiplie la caractéristique d'Euler par ± 1, ainsi cette dernière est-elle bien définie au signe près.

Ensuite, il nous faut définir le *groupe de Weil* d'un corps global, qui est un sous-groupe du groupe de Galois. Nous rappellerons ici succinctement sa définition dans le cas d'un corps de nombres, le cas des corps de fonctions étant très similaire, et nous renvoyons le lecteur à [AT09] pour de plus amples et plus précises références. Soit donc K un corps de nombres, dont on supposera fixée une clôture algébrique $\overline{K}$. Notons $C_{\overline{K}}$ le groupe des classes idéliques de $\overline{K}$, qui est naturellement muni d'une structure de $\text{Gal}(\overline{K}/K)$-module. Pour toute extension galoisienne M/L d'extensions finies de K et pour tout $r \in \mathbb{N}$, posons $H^r(M/L) = H^r\big(\text{Gal}(M/L), C_{\overline{K}}^{\text{Gal}(\bar{K}/L)}\big)$. D'après le théorème 90 de Hilbert, les $H^1(M/L)$ sont nuls ; de plus, on démontre que les $H^2(M/L)$ sont cycliques d'ordres $[M : L]$, et qu'il est possible d'en trouver

des générateurs, dits *classes fondamentales*[1], de manière compatible (en un certain sens) entre les extensions M/L. On définit alors le *groupe de Weil* $W_{M/L}$ d'une extension M/L comme l'extension

$$1 \longrightarrow C_{\overline{K}}^{\mathrm{Gal}(\bar{K}/L)} \longrightarrow W_{M/L} \longrightarrow \mathrm{Gal}(M/L) \longrightarrow 1$$

correspondant, en vue du théorème de Schreier 3.1.8, à la classe fondamentale de $H^2(M/L)$. Enfin, le *groupe de Weil* du corps de nombres K est la limite projective des $W_{M/L}$ de toutes les extensions galoisiennes d'extensions finies M/L de K.

On définit de même — c'est en fait beaucoup plus facile dans ce cas — le groupe de Weil d'un corps local, en remplaçant le groupe de classes idéliques $C_{\overline{K}}$ par la clôture algébrique du corps.

Lichtenbaum construit la *cohomologie Weil-étale* comme suit. Soit K un corps global. Notons Y_K l'ensemble des places de K, en incluant la valuation triviale v_0 sur K, que l'on peut voir comme point générique ; Y_K est donc formé de l'ouvert affine $\mathrm{Spec}(\mathcal{O}_K)$ et des places à l'infini de K. Notons K_v le complété de K en $v \in S_K$, et W_v son groupe de Weil, avec la convention $W_{v_0} = W_K$, et posons $W_{\kappa(v)} = \mathbb{Z}$ si v est ultramétrique (ce qui, notons-le, est cohérent avec la partie précédente, où on avait $G_0 \simeq \mathbb{Z}$), $W_{\kappa(v)} = \mathbb{R}$ si v est archimédienne, et $W_{\kappa(v_0)} = W_K$. On montre qu'on a dans chaque cas un morphisme naturel $\pi_v \colon W_v \longrightarrow W_{\kappa(v)}$; par exemple, si v est ultramétrique, il s'écrit

$$W_v \longrightarrow W_v^{\mathrm{ab}} \simeq K_v \xrightarrow{v} \mathbb{Z} = W_{\kappa(v)},$$

où ab dénote l'abélianisation. On montre aussi l'existence de de morphismes continus $\theta_v : W_v \longrightarrow W_K$, dits *morphismes de Weil*, vérifiant certaines propriétés et uniques à conjugaison par W_k près.

Soit L un extension galoisienne finie de K, et soit S un ensemble fini de places (non-triviales) de K, contenant toute les places se ramifiant dans L. Définissons une topologie de Grothendieck $\mathcal{W}_{L/K,S}$:

Les objets de $\mathrm{cat}(\mathcal{W}_{L/K,S})$ sont les collections $(X_v)_{v\in Y_K}, (f_v)_{v\neq v_0}$, où X_v est un $W_{\kappa(v)}$-espace, et où pour toute $v \neq v_0$, $f_v \colon X_v \longrightarrow X_{v_0}$ est un W_v-morphisme, X_v étant un W_v-espace par π_v, et W_{v_0}, par θ_v ; pour v_0, on demande que l'action de W_K sur X_{v_0} de factorise par $W_{L/K}$. Un morphisme

1. Notons au passage que ces classes fondamentales jouent un grand rôle dans la formulation cohomologique de la théorie du corps de classes.

dans cette catégorie est une collection

$$(X_v \longrightarrow X'_v)_{v \in Y_k}$$

de W_v-morphismes commutant avec les $f_{w,v}$, et les recouvrements sont les $(X_{i,v} \longrightarrow X_v)$ tels que chaque $X_{i,v} \longrightarrow X_v$ admette des sections locales. Les produits fibrés existent et sont définis de manière naturelle.

La catégorie $\mathrm{cat}(\mathcal{W}_{L/K,S})$ admet clairement un objet terminal, dont les composantes sont toutes réduites à un singleton. Par conséquent, nous pouvons définir les groupes de cohomologie $H^r(\mathcal{W}_{L/K,S}, \mathcal{F})$ de tout faisceau de groupes abéliens $\mathcal{F}$ sur $\mathcal{W}_{L/K,S}$.

On pose alors enfin, pour tous r et $\mathcal{F}$,

$$H^r(\mathcal{W}_K, \mathcal{F}) = \varinjlim_{L,S} H^r(\mathcal{W}_{L/K,S}, \mathcal{F}).$$

Lichtenbaum explique alors comment construire le faisceau $\varphi_!\mathbb{Z}$, où φ est l'inclusion de $\mathrm{Spec}(\mathcal{O}_K)$ dans Y_K, lui associe une caractéristique d'Euler au sens de la définition ci-dessus, et démontre le résultat suivant :

Théorème 4.1.1 (Lichtenbaum, 2009)**.** *Soit K un corps global, et soit ζ_K sa fonction zêta de Dedekind. Supposons que les groupes de cohomologie Weil-étale $H^r(\mathcal{W}_K, \varphi_!\mathbb{Z})$ sont nuls pour $r > 3$. Alors la caractéristique d'Euler est bien définie au signe près, et est égale à $\pm\zeta_K^*(0)$, où nous avons posé comme d'habitude*

$$\zeta_K^*(0) = \lim_{s \to 0} s^{-\operatorname{ord}_{s=0} \zeta_K(s)} \zeta_K(s).$$

Signalons que Lichtenbaum obtient ce résultat en reliant les groupes de cohomologie Weil-étale aux invariants arithmétiques du corps K que sont le nombre w de racines de l'unité contenues dans K, le nombre de classes h et le régulateur R, à partir desquels $\zeta_K^*(0)$ peut lui-même s'exprimer selon la célèbre formule

$$\zeta_K^*(0) = -\frac{hR}{w}.$$

4.2 Valeur des fonctions zêta en $s = 1/2$

Dans son article [Ram05], Niranjan Ramachandran tente d'examiner les valeurs prises par la fonction zêta d'une variété sur un corps fini en des valeurs de s non entières, et plus particulièrement en $s = 1/2$, valeur effectivement critique en vue de l'hypothèse de Riemann ; d'autre part, Ramachandran explique que si le 2 au dénominateur est surmontable, il semble beaucoup plus difficile de gérer d'autres dénominateurs tels que $s = 1/3,\ 1/4,\ \cdots$.

En fait, Ramachandran est à la recherche d'interprétations *motiviques* (entre autres) des valeurs prises par les fonctions zêta, sujet sur lequel nous ne nous étendrons pas, car les connaissances de l'auteur ne le permettent tout simplement pas. Citons toutefois, sans définitions, cet exemple : pour $X = \mathrm{Spec}(\mathbb{F}_q)$, les valeurs de la fonction zêta aux entiers strictement négatifs vérifient

$$-\frac{1}{\zeta(X,-n)} = q^n - 1 = |K_{2n-1}(\mathbb{F}_q)| = \left|\mathrm{Ext}^1_{\mathcal{A}}\left(\mathbb{Z},\mathbb{Z}(n)\right)\right| = |\mathbb{G}_m(\mathbb{F}_{q^n})| = |T_n(\mathbb{F}_q)|,$$

où $K_{2n-1}(\mathbb{F}_q)$ est la version proposée par Quillen du $(2n-1)^{\text{ème}}$ groupe de K-théorie, $\mathcal{A}$ est la catégorie des motifs effectifs entiers, $\mathbb{Z}(n)$ est le motif de Tate, et T_n est le tore sur $\mathbb{F}_q$ obtenu par Weil-restriction des scalaires à partir du groupe multiplicatif $\mathbb{G}_m$ défini sur $\mathbb{F}_{q^n}$. Ramachandran affirme qu'une interprétation motivique des valeurs prises par les fonctions zêta en $s = 1/2$ est conditionnée à l'existence d'un mystérieux motif $\mathbb{Z}(1/2)$, racine carrée du motif de Tate $\mathbb{Z}(1)$, qu'il tente de construire dans cet article. Selon lui, .l'existence de $\mathbb{Z}(1/2)$ est plausible, contrairement à celles de $Z(1/3)$, $\mathbb{Z}(1/4)$, $\cdots$, d'où la difficulté à étudier les valeurs en $s = 1/3,\ 1/4,\ \cdots$.

Revenons à la cohomologie Weil-étale. Remarquons que la rationalité des fonctions zêta $Z(X/\mathbb{F}_q, T)$ montre que le calcul de la valeur d'une fonction zêta en $s = 1/2$ conduit à évaluer une fraction rationnelle en $T = 1/\sqrt{q}$, ce qui risque fort de donner un résultat irrationnel, donc difficilement reliable à une caractéristique d'Euler, dès que $\sqrt{q}$ est irrationnel. C'est pourquoi Ramachandran restreint ses investigations au cas où $q = p^{2f}$ est une puissance *paire* d'un nombre premier p, ce qui revient encore à dire que le corps de base $\mathbb{F}_q$ contient $\mathbb{F}_{p^2}$.

Pour parvenir à son résultat, Ramachandran construit un faisceau Weil-étale sur une courbe elliptique supersingulière E. Pour comprendre, notons

que pour tout corps k, si on voit E comme un schéma, les k-points de E sont donnés par la formule

$$E(k) = \mathrm{Hom}\big(\mathrm{Spec}(k), E\big).$$

La fonctorialité en k de la loi de groupe sur E se traduit par le fait que cette loi de groupe peut se définir intrinsèquement, c'est-à-dire qu'elle est donnée par un morphisme de schémas $E \times E \longrightarrow E$ satisfaisant les axiomes qu'une loi de groupe se doit de vérifier. On peut donc définir un faisceau Weil-étale de groupes abéliens sur une variété algébrique X sur $\mathbb{F}_q$ en posant, pour tout $\overline{X}$-schéma étale U,

$$\mathcal{E}(U) = \mathrm{Hom}(U, E);$$

il suffit juste de vérifier la condition de faisceau.

En substituant ce faisceau $\mathcal{E}$ au faisceau constant $\mathbb{Z}$ utilisé par Lichtenbaum dans [Lic05], Ramachandran obtient le résultat suivant :

Théorème 4.2.1 (Ramachandran, 2005)**.** *Soit X une variété projective non singulière sur $\mathbb{F}_q$, où $q = p^{2f}$ est une puissance* paire *d'un nombre premier p, et soit $\zeta(X/\mathbb{F}_q, s)$ sa fonction zêta.*

(a) Les groupes de cohomologie Weil-étale $H^r_{\mathcal{W}}(X, \mathcal{E})$ sont tous de type fini.

(b) Ils sont nuls pour $r > 2\dim(X) + 1$.

(c) La première caractéristique d'Euler additive associée est nulle :

$$\sum_{r=0}^{+\infty} (-1)^r \,\mathrm{rg}_{\mathbb{Z}}\, H^r_{\mathcal{W}}(X, \mathcal{E}) = 0.$$

(d) L'ordre d'annulation de $\zeta(X/\mathbb{F}_q, s)$ en $s = 1/2$ est donné par la seconde caractéristique d'Euler additive associée :

$$\sum_{r=0}^{+\infty} (-1)^r r \,\mathrm{rg}_{\mathbb{Z}}\, H^r_{\mathcal{W}}(X, \mathcal{E}) = -2\,\mathrm{ord}_{s=1/2}\,\zeta(X/\mathbb{F}_q, s).$$

(e) Munissons comme nous l'avions fait pour $s = 0$ les groupes de cohomologie Weil-étale de la structure de complexe donnée par le cup-produit avec θ, et soit $\chi(X, \mathcal{E})$ la caractéristique d'Euler multiplicative associée. Notons de plus

$$\chi(X, \mathcal{O}_X) = \prod_{r=0}^{+\infty} |H^r(X, \mathcal{O}_X)|^{(-1)^r}$$

la caractéristique d'Euler multiplicative *de la cohomologie* usuelle *de* X*. La valeur essentielle*

$$Z^*(X/\mathbb{F}_q, 1/\sqrt{q}) = \lim_{T \to 1/\sqrt{q}} (1 - \sqrt{q}T)^{-\operatorname{ord}_{T=1/\sqrt{q}} Z(X/\mathbb{F}_q, T)} Z(X/\mathbb{F}_q, T)$$

est donnée par

$$Z^*(X/\mathbb{F}_q, 1/\sqrt{q}) = \frac{\chi(X, \mathcal{O}_X)}{\chi(X, \mathcal{E})}.$$

On peut se demander si, comme la conjecture de Lichtenbaum 3.6.2, ce résultat ne se généralise pas aux variétés quasi-projectives potentiellement singulières, au moins en petite dimension.

4.3 Valeurs de fonctions L associées à un revêtement

Dans son article [Bur04] paru en 2004, David Burns émet — et étaie très sérieusement — une conjecture reliant la cohomologie Weil-étale d'une courbe sur un corps fini aux valeurs de fonctions L relatives aux représentations du groupe d'automorphismes d'un revêtement d'une autre courbe par cette courbe. Bien que quelque peu sibylline car s'exprimant dans un espace assez abstrait, la validité de cette conjecture aurait des conséquences très importantes.

La conjecture de Burns implique en effet par exemple les conjectures dites Ω de Chinburg, ainsi qu'une conjecture de Gross, et, à sous quelques conditions, un conjecture de Tate, version raffinée de celle de Gross. Ces conjectures étant bien au-delà de notre propos, nous ne expliciterons pas ; le lecteur désireux de connaître les références afférentes pourra consulter l'article de Burns.

Considérons donc une extension galoisienne finie E/K de corps globaux de caractéristique $p > 0$. Du point de vue des courbes non singulières complètes, cette extension peut s'interpréter comme un revêtement galoisien de courbes, dont le groupe d'automorphismes est $G = \mathrm{Gal}(E/K)$.

Intéressons-nous aux représentations complexes de dimensions finies de G. Les briques sont contenues dans $Irr_{\mathbb{C}}(G)$, l'ensemble des caractères de représentations complexes de dimensions finies de G *irréductibles*. Pour $\chi \in$

$Irr_{\mathbb{C}}(G)$, notons V_χ l'espace vectoriel complexe sur lequel G agit par l'intermédiaire du morphisme

$$\rho_\chi : G \longrightarrow Gl(V_\chi).$$

Fixons un ensemble fini S de places de K contenant toutes les places se ramifiant dans E. Soit v une place de K qui n'est pas dans S, et soit w une place de E au-dessus de v. Comme w n'est pas ramifiée, on peut définir son *élément de Frobenius* $\left(\frac{E/K}{w}\right) \in G$, qui est caractérisé par la relation

$$\forall \alpha \in E,\ \text{si}\ \ \mathrm{ord}_w(\alpha) \geqslant 0, \qquad \mathrm{ord}_w\left(\left(\frac{E/K}{w}\right)(\alpha) - \alpha^{|\kappa(v)|}\right) > 0,$$

où ord_w désigne la valuation sur E normalisée associée à w, et où $\kappa(v)$ est le corps résiduel de v. Les w au-dessus d'une même v sont permutés transitivement par G, donc les éléments de Frobenius $\left(\frac{E/K}{w}\right)$ correspondants forment une classe de conjugaison dans G, notée $\left(\frac{E/K}{v}\right)$.

On définit alors la *fonction L* d'une représentation irréductible $\chi \in Irr_{\mathbb{C}}(G)$ par la formule

$$L_S(\chi, s) = \prod_{v \notin S} \text{dét}\left(I - |\kappa(v)|^{-s}\rho_\chi\left(\frac{E/K}{v}\right)\right)^{-1},$$

ce qui est bien défini puisque le fait que $\left(\frac{E/K}{v}\right)$ ne soit défini qu'à conjugaison près n'empêche pas l'évaluation du déterminant. Le produit converge pour $\Re s > 1$, et se prolonge méromorphiquement à $\mathbb{C}$; nous noterons donc comme d'habitude

$$L_S^*(\chi, 0) = \lim_{s \to 0}\ s^{-\mathrm{ord}_{s=0} L_S(\chi,s)} L_S(\chi, s).$$

Un calcul similaire à celui menant à la formule $\text{dét}(e^A) = e^{\mathrm{Tr}\, A}$ permet d'exprimer les fonctions L directement à partir de χ :

$$L_S(\chi, s) = \prod_{v \notin S} \exp\left(\sum_{n=1}^{+\infty} \frac{1}{n}|\kappa(v)|^{-ns}\chi\left(\frac{E/K}{v}\right)\right),$$

ce qui montre au passage comment se construit la fonction L d'une représentation réductible :

$$L_S(\chi \oplus \chi', s) = L_S(\chi, s) \times L_S(\chi', s).$$

Notons enfin que la fonction L associée au caractère trivial est, à un nombre fini de facteurs eulériens près, égale à la fonction zêta de K.

Ces fonctions L encodent toute l'information relative à la représentation χ puisque, d'après le théorème de Chebotarev, tout $\sigma \in G$ est de la forme $\left(\frac{E/K}{v}\right)$ pour certaines v. Ce sont elles qui font l'objet de l'article [Bur04] de David Burns que nous allons à présent étudier. Afin de les étudier toutes simultanément, posons

$$\Theta_{E/K,S}(s) = \big(L_S(\chi, s)\big)_{\chi \in Irr_{\mathbb{C}}(G)} : \mathbb{C} \longrightarrow \mathbb{C}^{Irr_{\mathbb{C}}(G)}.$$

L'identification naturelle

$$\mathbb{C}^{Irr_{\mathbb{C}}(G)} \simeq C_{\mathbb{C}G},$$

où C dénote le centre, permet de voir $\Theta_{E/K,S}$ comme une fonction à valeurs dans $C_{\mathbb{C}G}$; notons que $\Theta^*_{E/K,S}(0)$ habite même dans $C_{\mathbb{R}G}$.

Pour tout anneau R, définissons l'antiautomorphisme involutif de RG envoyant $g \in G$ sur g^{-1} et prolongé R-linéairement par $x \longmapsto x^\sharp$. Nous utiliserons plus tard la valeur $\Theta^*_{E/K,S}(0)^\sharp \in C_{\mathbb{R}G}$.

Pour comprendre le cadre dans lequel s'énonce la conjecture émise par Burns dans son article, il nous faut toutefois au préalable rappeler quelques définitions de K-théorie.

Nous ne ferons ici qu'un rapide rappel des définitions de K-théorie algébrique dont nous aurons besoin par la suite, aussi renvoyons-nous le lecteur à [Ros94] pour un traitement plus complet du sujet.

Soit R un anneau unitaire, mais pas forcément commutatif. Convenons que dans la suite, tous les modules seront des modules à gauche. Considérons le monoïde des classes d'isomorphisme des R-modules projectifs de type fini, muni de la loi $\oplus$. On appelle *groupe de Grothendieck* de R, et on note $K_0(R)$, le groupe formé [2] sur ce monoïde, c'est-à-dire qu'on ajoute tout d'abord des inverses formels à tous les éléments, puis qu'on quotiente par la relation

$$\exists Q : P \oplus Q \simeq P' \oplus Q \implies P \sim P'.$$

Exemple 4.3.1. Si R est un corps, les projectifs de type fini sont les espaces vectoriels de dimension finie, le monoïde qu'ils forment est isomorphe à $(\mathbb{N}, +)$, donc $K_0(R) \simeq \mathbb{Z}$.

2. un instant de réflexion montre que ce procédé n'est autre que l'adjoint à gauche du foncteur d'oubli des groupes vers les monoïdes.

Exemple 4.3.2. Si R est un anneau de Dedekind, on montre, en s'appuyant sur la relation

$$I \oplus J \simeq R \oplus IJ$$

pour I, J idéaux de R, que $K_0(R) \simeq \mathbb{Z} \times Cl(R)$, où $Cl(R)$ est le groupe des classes de R.

Passons au K_1. Le groupe linéaire $Gl_n(R)$ des matrices inversibles $n \times n$ à coefficients dans R se plonge dans $Gl_{n+1}(R)$, suivant la formule

$$A \longmapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix};$$

ceci nous permet de former le groupe

$$Gl(R) = \bigcup_{n=1}^{+\infty} Gl_n(R).$$

Notons $E_n(R) \subset Gl_n(R)$ le sous-groupe engendré par les transvections, et posons de même

$$E(R) = \bigcup_{n=1}^{+\infty} E_n(R).$$

Un théorème de Whitehead nous dit alors que $E(R)$ coïncide avec le sous-groupe dérivé de $Gl(R)$, quel que soit l'anneau R. On note alors $K_1(R)$ l'abélianisé de $Gl(R)$:

$$K_1(R) = Gl(R)^{\mathrm{ab}} = Gl(R)/E(R).$$

Exemple 4.3.3. Si R est un corps, il est bien connu que le groupe dérivé de $Gl(R)$ est le groupe spécial linéaire $Sl(R)$; aussi $K_1(R) \simeq R^*$.

Exemple 4.3.4. Si R est un anneau euclidien, la division euclidienne permet de réduire toute matrice de $Gl(R)$ sous la forme

$$\begin{pmatrix} \lambda & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & \ddots \end{pmatrix}, \quad \lambda \in R^*,$$

uniquement par des opérations élémentaires sur les lignes et les colonnes ; ainsi là encore $K_1(R) \simeq R^*$.

Par contre, il existe des anneaux principaux non euclidiens pour lesquels $K_1(R) \not\simeq R^*$.

Le K_0 et le K_1 sont tous les deux clairement fonctoriels.

De la même manière qu'une paire d'espaces topologiques (X, A) donne lieu à des groupes d'*homologie relative* qui prennent place dans une suite exacte longue

$$\cdots \longrightarrow H_r(A) \longrightarrow H_r(X) \longrightarrow H_r(X, A) \longrightarrow H_{r-1}(A) \longrightarrow \cdots ,$$

il est possible, étant donné un morphisme d'anneaux $f : R \longrightarrow R'$, de définir un K_0 relatif $K_0(R, f)$ de sorte qu'on ait une suite exacte

$$K_1(R) \longrightarrow K_1(R') \xrightarrow{\partial} K_0(R, f) \longrightarrow K_0(R) \longrightarrow K_0(R').$$

Plus précisément, considérons la catégorie dont les objets sont les triplets (X, ϕ, Y), où X et Y sont des R-modules projectifs de type fini, et ϕ, un isomorphisme de R'-modules

$$\phi : R' \underset{R}{\otimes} X \longrightarrow R' \underset{R}{\otimes} X,$$

R' étant vu comme un module-R à *droite* par f, et dont les morphismes entre deux objets (X, ϕ, Y) et (X', ϕ', Y') sont les couples de morphismes $(\xi : X \longrightarrow X',\ \eta : Y \longrightarrow Y')$ tels que

$$\begin{array}{ccc} R' \underset{R}{\otimes} X & \xrightarrow{Id\otimes\xi} & R' \underset{R}{\otimes} X' \\ \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle \phi'} \\ R' \underset{R}{\otimes} Y & \xrightarrow[Id\otimes\eta]{} & R' \underset{R}{\otimes} Y' \end{array}$$

commute. Disons que

$$0 \longrightarrow (X', \phi', Y') \longrightarrow (X, \phi, Y) \longrightarrow (X'', \phi'', Y'') \longrightarrow 0$$

est une suite exacte si les suites de R-modules associées

$$0 \longrightarrow X' \longrightarrow X \longrightarrow X'' \longrightarrow 0$$

et

$$0 \longrightarrow Y' \longrightarrow Y \longrightarrow Y'' \longrightarrow 0$$

sont exactes.

Définissons alors $K_0(R, f)$ comme le groupe abélien généré par ces triplets (X, ϕ, Y), et avec les relations

- Pour tout suite exacte

$$0 \longrightarrow (X', \phi', Y') \longrightarrow (X, \phi, Y) \longrightarrow (X'', \phi'', Y'') \longrightarrow 0,$$

$$(X, \phi, Y) = (X', \phi', Y') + (X', \phi', Y'),$$

- $(X, \psi \circ \phi, Z) = (X, \phi, Y)(Y, \psi, Z)$.

Les applications insérant $K_0(R, f)$ dans la suite exacte évoquée ci-dessus sont

$$\begin{array}{rcl} K_1(R') & \longrightarrow & K_0(R, f) \\ A \in Gl_n(R') & \longmapsto & (R^n, A, R^n) \end{array}$$

et

$$\begin{array}{rcl} K_0(R, f) & \longrightarrow & K_0(R) \\ (X, \phi, Y) & \longmapsto & X - Y \end{array},$$

dont on vérifie assez facilement qu'elles sont bien définies.

Pour en revenir à notre propos, pour tout anneau intègre R, et pour toute extension E du corps des fractions de R, on a donc une suite exacte

$$K_1(RG) \longrightarrow K_1(EG) \xrightarrow{\partial} K_0(RG, E) \longrightarrow K_0(RG) \longrightarrow K_0(EG),$$

où on a encore noté E la tensorisation par E au-dessus de R.

La tensorisation par $\mathbb{Z}_\ell$ induit quant à elle un morphisme

$$\rho_\ell : K_0(\mathbb{Z}G, \mathbb{Q}) \longrightarrow K_0(\mathbb{Z}_\ell G, \mathbb{Q}_\ell),$$

et on peut montrer que le produit de ces ρ_ℓ pour ℓ premier induit un isomorphisme

$$\prod_\ell \rho_\ell : K_0(\mathbb{Z}G, \mathbb{Q}) \xrightarrow{\sim} \bigoplus_\ell K_0(\mathbb{Z}_\ell G, \mathbb{Q}_\ell).$$

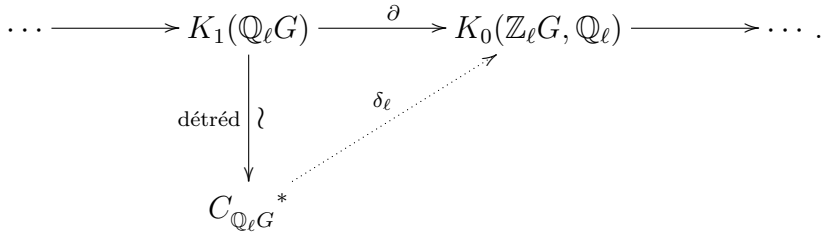
Voyons comment relier tout cela à nos fonctions L. Soit A une F-algèbre semi-simple, soit F' une extension de F telle que $A' = A \underset{F}{\otimes} F'$ soit déployée, et choisissons un idempotent indécomposable e de A'. Pour tout A-module de type fini V, on définit le *déterminant réduit* détréd(f) d'un endomorphisme $f \in End_A(V)$ par

$$\text{détréd}(f) = \text{dét}_{F'}\left((f \otimes Id)|_{e(V \otimes_F F')}\right),$$

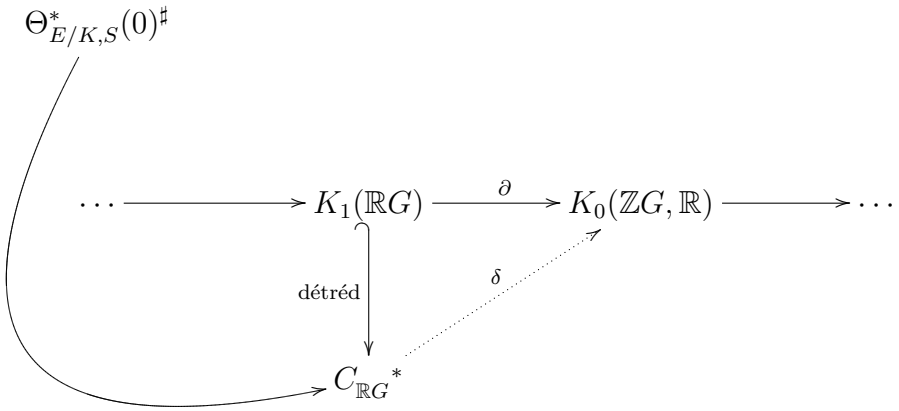
ce qui est un élément de F qui ne dépend pas des choix de F' et de e. Appliquons ceci à $A = FG$, où F est une extension du corps des fractions de R, ce qui est loisible puisque F étant de caractéristique nulle, FG est semi-simple. À un élément x de $K_1(FG)$, représenté par une matrice $M \in Gl(FG)$, on peut donc associer l'élément détréd$(M) \in F^*$, puisque les éléments de $E(FG)$ sont de déterminant réduit 1. Comme F^* se plonge dans ${C_{FG}}^*$, on obtient ainsi une application

$$\text{détréd} : K_1(FG) \longrightarrow {C_{FG}}^*.$$

Dans le cas où $R = \mathbb{Z}_\ell$, $F = \mathbb{Q}_\ell$, cette application se trouve être bijective, donc il existe une unique application δ_ℓ faisant commuter le diagramme



Dans le cas $R = \mathbb{Z}$, $E = \mathbb{R}$, l'application détréd n'est qu'injective, mais on démontre qu'il est néanmoins possible de construire une application faisant commuter le diagramme, similaire au diagramme précédent, sur lequel vient se greffer la valeur $\Theta^*_{E/K,S}(0)^\sharp$ définie plus haut :



Soit S_E l'ensemble des places de E au-dessus des places de K contenues dans S. Soit $Y_S = \mathbb{Z}S_E$ le groupe abélien libre sur S_E, et soit $X_S \subset Y_S$

le noyau du morphisme de Y_S dans $\mathbb{Z}$ envoyant tous les éléments de S_E sur 1. Notons aussi $\mathcal{O}_{E,S}$ l'anneau des S_E-entiers de E, $\mathcal{O}_{E,S}^*$ le groupe des S_E-unités, et $U_{E,S} = \mathrm{Spec}(\mathcal{O}_{E,S})$. $U_{E,S}$ est une courbe, que l'on peut voir comme la courbe non singulière complète associée à E et privée des points correspondant aux éléments de S_E ; on peut donc parler de ses groupes de cohomologie Weil-étale $H^i_{\mathcal{W}}(U_{E,S}, \mathbb{G}_m)$, où $\mathbb{G}_m$ désigne le groupe multiplicatif. Considérons par ailleurs le morphisme

$$\begin{array}{rccl} R_{E,S} : & \mathcal{O}_{E,S}^* & \longrightarrow & X_S \underset{\mathbb{Z}}{\otimes} \mathbb{R} \\ & u & \longmapsto & -\displaystyle\sum_{w \in S_E} w \otimes \log |u|_w, \end{array}$$

où $|\cdot|_w$ désigne la valeur absolue normalisée associée à w ; d'après la formule du produit, l'image de ce morphisme atterrit bien dans $X_S \underset{\mathbb{Z}}{\otimes} \mathbb{R} \subset Y_S \underset{\mathbb{Z}}{\otimes} \mathbb{R}$.

Burns explique comment utiliser $R_{E,S}$ pour construire une *caractéristique d'Euler* $\chi\big(H^i_{\mathcal{W}}(U_{E,S}, \mathbb{G}_m), R_{E,S}\big)$, qui est à valeurs dans $K_0(\mathbb{Z}G, \mathbb{R})$. Sa conjecture s'énonce alors ainsi :

Conjecture 4.3.5 (Burns, 2004)**.**

$$\delta\big(\Theta^*_{E/K,S}(0)^\sharp\big) = \chi\big(H_{\mathcal{W}}(U_{E,S}, \mathbb{G}_m), R_{E,S}\big) \in K_0(\mathbb{Z}G, \mathbb{R}).$$

Remarquons que le changement de variable permet, comme on a souvent eu l'occasion de le constater, d'éliminer la transcendance et d'aboutir à une version "rationnelle" de cette conjecture : en effet, si on pose

$$\Delta_{E/K,S}(T) = \Theta_{E/K,S}(s),$$

et si on remplace le morphisme $R_{E,S}$ par

$$\begin{array}{rccl} D_{E,S} : & \mathcal{O}_{E,S}^* & \longrightarrow & X_S \\ & u & \longmapsto & \displaystyle\sum_{w \in S_E} \mathrm{ord}_w(u)\,[\kappa(w) : \mathbb{F}_p]\,w, \end{array}$$

alors on a $\Delta^*_{E/K,S}(1) \in {C_{\mathbb{Q}G}}^*$, et la conjecture de Burns est équivalente à l'identité

$$\delta\big(\Delta^*_{E/K,S}(1)^\sharp\big) = \chi\big(H_{\mathcal{W}}(U_{E,S}, \mathbb{G}_m), D_{E,S}\big),$$

qui a le bon goût de s'exprimer dans $K_0(\mathbb{Z}G, \mathbb{Q})$ au lieu de $K_0(\mathbb{Z}G, \mathbb{R})$.

Dans son article, Burns apporte un soutien certain à sa conjecture, en prouvant qu'elle est vraie localement, ou presque. Plus précisément, il démontre que l'image par $\rho_\ell : K_0(\mathbb{Z}G, Q) \longrightarrow K_0(\mathbb{Z}_\ell G, \mathbb{Q}_\ell)$ de sa conjecture version rationnelle est vraie lorsque $\ell \neq p$, et est vraie modulo la torsion pour $\ell = p$. Puisque

$$\prod_\ell \rho_\ell : K_0(\mathbb{Z}G, \mathbb{Q}) \xrightarrow{\sim} \bigoplus_\ell K_0(\mathbb{Z}_\ell G, \mathbb{Q}_\ell)$$

est un isomorphisme, ceci l'étaie considérablement.

Par exemple, on peut montrer que si p ne divise pas l'ordre de G, alors $K_0(\mathbb{Z}_p G, \mathbb{Q}_p)$ est sans torsion, si bien que la conjecture de Burns est alors vraie.

5 Annexe

5.1 Cohomologie des faisceaux

Soit X un espace topologique. Notons $\mathfrak{Sh}_X$ la catégorie des faisceaux de groupes abéliens sur X, et $\mathfrak{Ab}$ la catégorie des groupes abéliens. Pour tout faisceau de groupes abéliens $\mathcal{F}$ sur X, posons $\Gamma(X, \mathcal{F}) = \mathcal{F}(X)$. Le foncteur *sections globales*

$$\Gamma(X, .) : \mathfrak{Sh}_X \longrightarrow \mathfrak{Ab}$$

ainsi défini est exact à gauche, mais pas à droite en général. La *cohomologie des faisceaux* sert à mesurer ce défaut d'exactitude, que l'on peut voir comme l'obstruction à un passage du local au global.

Définition 5.1.1. Notons, pour $r \in \mathbb{N}$, $H^r(X, \cdot) = R^r\Gamma(X, .)$ le r-ième foncteur dérivé à droite de $\Gamma(X, .)$. La *cohomologie d'un faisceau de groupes abéliens* $\mathcal{F}$ sur X est la donnée des groupes abéliens $H^r(X, \mathcal{F})$, $i \geqslant 0$.

Cette définition est justifiée par le fait (que nous ne démontrerons pas) que la catégorie abélienne $\mathfrak{Sh}_X$ admet assez d'injectifs. Notons qu'on a en particulier $H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F})$.

Le cas qui nous intéresse est celui où X est une variété projective sur un corps k. Dans ce cadre, rappelons le résultat suivant, dû à Serre, et dont le corollaire nous sera d'une grande utilité à plusieurs reprises :

Théorème 5.1.2. *Soit X une variété projective sur un anneau noethérien R. Pour tout faisceau cohérent $\mathcal{F}$ sur X, il existe un entier $n_0 \in \mathbb{N}$ tel que pour tout entier $n \geqslant n_0$, le faisceau décalé $\mathcal{F}(n)$ soit généré par un nombre fini de ses sections globales.*

Ce résultat étant très classique, nous ne le redémontrerons pas ici. Le lecteur souhaitant en voir une démonstration pourra consulter [Har77], théorème III.4.5.

Corollaire 5.1.3. *Soit X une variété projective sur un anneau noethérien R. Tout faisceau cohérent $\mathcal{F}$ sur X est un quotient d'un faisceau de forme $\bigoplus_{i=1}^{r} \mathcal{O}_X(n_i)$, et on peut prendre les $n_i \in \mathbb{Z}$ arbitrairement proches de $-\infty$.*

Démonstration. Soit $n \in \mathbb{N}$ tel que $\mathcal{F}(n)$ soit généré par un nombre fini de sections globales, de sorte qu'on ait une surjection

$$\bigoplus_{i=1}^{r} \mathcal{O}_X \longrightarrow \mathcal{F}(n) \longrightarrow 0.$$

En tensorisant par $\mathcal{O}_X(-n)$, on obtient comme voulu une surjection

$$\bigoplus_{i=1}^{r} \mathcal{O}_X(-n) \longrightarrow \mathcal{F} \longrightarrow 0,$$

et on peut prendre $n \geqslant n_0$ aussi grand qu'on veut. □

Nous admettrons également le théorème suivant, dû à Grothendieck :

Théorème 5.1.4 (Bornitude de la cohomologie)**.** *Sur un espace topologique de dimension n, la cohomologie de tout faisceau de groupes abéliens est nulle en degré strictement supérieur à n.*

Une démonstration (assez technique) de ce résultat est disponible dans [Har77], théorème III.2.7.

Pour le moment, la seule méthode à notre disposition pour calculer la cohomologie d'un faisceau $\mathcal{F}$ consiste à prendre une résolution injective de $\mathcal{F}$, puis à calculer la cohomologie du complexe des sections globales. Il faut bien reconnaître que cette méthode est fort peu pratique. Heureusement, il existe une autre méthode, beaucoup plus simple à utiliser : la cohomologie de Čech.

Définition 5.1.5. Soit X un espace topologique, et soit $\mathcal{U} = (U_i)_{i \in I}$ un recouvrement ouvert de X. Munissons une bonne fois pour toutes l'ensemble d'indices I d'un ordre total $\prec$. Soit $\mathcal{F}$ un faisceau de groupes abéliens sur X. Le *complexe de Čech* de $\mathcal{F}$ relatif à $\mathcal{U}$ est défini ainsi : c'est un complexe de groupes abéliens, nul en degré strictement négatif, et dont les objets sont, pour $r \in \mathbb{N}$,

$$\check{C}^r(\mathcal{U}, \mathcal{F}) = \prod_{i_0 \prec \cdots \prec i_r} \mathcal{F}(U_{i_0, \cdots, i_r}),$$

où l'on a noté $U_{i_0,\cdots,i_r}$ pour $U_{i_0} \cap \cdots \cap U_{i_r}$, le cobord étant défini en posant, pour $\alpha \in \check{C}^r(\mathcal{U}, \mathcal{F})$,

$$(d\alpha)_{i_0,\cdots,i_{r+1}} = \sum_{j=0}^{r+1} (-1)^j \alpha_{i_0,\cdots,\hat{i_j},\cdots,i_{r+1}}|_{U_{i_0,\cdots,i_{r+1}}},$$

où $\hat{i_j}$ signifie que i_j a été omis. On vérifie facilement que $d \circ d = 0$, donc ceci définit bien un complexe. On définit alors la *cohomologie de Čech* de $\mathcal{F}$ relativement à $\mathcal{U}$ comme la cohomologie du complexe de Čech $\check{C}^{\cdot}(\mathcal{U}, \mathcal{F})$, et on la note $\check{H}^{\cdot}(\mathcal{U}, \mathcal{F})$

Remarquons qu'on a $\check{H}^0(\mathcal{U}, \mathcal{F}) \simeq \Gamma(X, \mathcal{F})$ pour tous $\mathcal{U}$, $\mathcal{F}$.

Nous aurons également besoin d'une version "faisceau" de la construction précédente :

Définition 5.1.6. On définit un complexe de faisceaux nul en degré strictement négatif en posant, pour $r \in \mathbb{N}$,

$$\check{\mathcal{C}}^r(\mathcal{U}, \mathcal{F}) = \prod_{i_0 \prec \cdots \prec i_r} \iota_{U_{i_0,\cdots,i_r}*}(\mathcal{F}|_{U_{i_0,\cdots,i_r}}) = \left(V \mapsto \prod_{i_0 \prec \cdots \prec i_r} \mathcal{F}(U_{i_0,\cdots,i_r} \cap V) \right),$$

où $\iota_U : U \hookrightarrow X$ est l'inclusion, et en définissant le cobord comme précédemment.

Notons que dans ce cas, on a $\Gamma\big(X, \check{\mathcal{C}}^r(\mathcal{U}, \mathcal{F})\big) = \check{C}^r(\mathcal{U}, \mathcal{F})$ pour tout $r \in \mathbb{N}$.

L'intérêt de la cohomologie de Čech réside dans le fait qu'elle constitue un moyen plus pratique de calcul de la cohomologie des faisceaux. C'est ce que nous dit le résultat suivant :

Théorème 5.1.7. *Soit X un schéma noethérien séparé, et soit $\mathcal{U}$ un recouvrement de X par des ouverts affines. Pour tout faisceau de groupes abéliens $\mathcal{F}$ sur X, on a, pour tout $r \in \mathbb{N}$,*

$$\check{H}^r(\mathcal{U}, \mathcal{F}) \simeq H^r(X, \mathcal{F}).$$

Démonstration. Une preuve complète serait fastidieusement technique et nous entraînerait trop loin de notre propos ; aussi ne donnerons-nous qu'une ébauche de la démonstration. Le lecteur trouvera la démonstration complète dans [Har77].

Soit $\mathcal{I}^{\cdot}$ une résolution injective de $\mathcal{F}$. Par injectivité des objets de $\mathcal{I}^{\cdot}$, l'identité de $\Gamma(X, \mathcal{F})$ se prolonge en un morphisme de $\check{C}^{\cdot}(\mathcal{U}, \mathcal{F})$ dans $\mathcal{I}^{\cdot}$, d'où, en passant à la cohomologie, un morphisme $\check{H}^{\cdot}(\mathcal{U}, \mathcal{F}) \longrightarrow H^{\cdot}(X, \mathcal{F})$ dont il s'agit de montrer que c'est un isomorphisme. Ceci a déjà été vérifié en degré 0.

On démontre qu'on peut plonger $\mathcal{F}$ dans un faisceau flasque et quasi-cohérent $\mathcal{G}$, d'où une suite exacte

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{G}/\mathcal{F} \longrightarrow 0.$$

Puisque X est séparé, l'intersection de deux ouverts affines est affine, donc les $U_{i_0,\cdots,i_r}$ sont affines. Or on démontre tout faisceau quasi-cohérent est acyclique sur un schéma affine noethérien, donc la suite

$$0 \longrightarrow \mathcal{F}(U_{i_0,\cdots,i_r}) \longrightarrow \mathcal{G}(U_{i_0,\cdots,i_r}) \longrightarrow (\mathcal{G}/\mathcal{F})(U_{i_0,\cdots,i_r}) \longrightarrow 0$$

est exacte ; en prenant les produits idoines, on en déduit que la suite des complexes de Čech

$$0 \longrightarrow \check{C}^{\cdot}(\mathcal{U},\mathcal{F}) \longrightarrow \check{C}^{\cdot}(\mathcal{U},\mathcal{G}) \longrightarrow \check{C}^{\cdot}(\mathcal{U},\mathcal{G}/\mathcal{F}) \longrightarrow 0$$

est elle-même exacte.

On démontre que tout faisceau flasque est acyclique sur tout espace topologique X. Comme $\mathcal{G}$ est flasque, les faisceaux de Čech $\check{\mathcal{C}}^r(\mathcal{U},\mathcal{G})$ sont eux aussi flasques, donc on peut utiliser la résolution $0 \longrightarrow \mathcal{G} \longrightarrow \check{\mathcal{C}}^{\cdot}(\mathcal{U},\mathcal{G})$ pour calculer la cohomologie de $\mathcal{G}$, qui est nulle en degré non nul puisque $\mathcal{G}$ est flasque donc acyclique. Ainsi $\check{\mathcal{H}}^r(\mathcal{U},\mathcal{G}) = 0$ pour tout $r \geqslant 1$, donc la suite exacte longue de cohomologie de la suite exacte courte de complexes de Čech obtenue précédemment donne une suite exacte

$$0 \longrightarrow \check{H}^0(\mathcal{U},\mathcal{F}) \longrightarrow \check{H}^0(\mathcal{U},\mathcal{G}) \longrightarrow \check{H}^0(\mathcal{U},\mathcal{G}/\mathcal{F}) \longrightarrow \check{H}^1(\mathcal{U},\mathcal{F}) \longrightarrow 0$$

ainsi que des isomorphismes

$$\check{H}^r(\mathcal{U},\mathcal{G}/\mathcal{F}) \simeq \check{H}^{r+1}(\mathcal{U},\mathcal{F})$$

pour $r \geqslant 1$. En comparant cette dernière suite exacte avec celle obtenue à partir de la suite exacte longue de cohomologie des faisceaux, on obtient que l'application

$$\check{H}^1(\mathcal{U},\mathcal{F}) \longrightarrow H^1(X,\mathcal{F})$$

est un isomorphisme. Mais comme $\mathcal{G}/\mathcal{F}$ est aussi quasi-cohérent, on en déduit le résultat par récurrence sur $r \geqslant 1$. □

À titre d'exemple, calculons la cohomologie de l'espace projectif, résultat qui nous servira plus tard.

Le petit lemme suivant nous sera utile :

Lemme 5.1.8. *Soit X un espace topologique, et soit $Z \subseteq X$ un fermé de X. Pour tout faisceau de groupes abéliens $\mathcal{F}$ sur Z, on a*

$$\forall r \in \mathbb{N}, \quad H^r(Z, \mathcal{F}) = H^r(X, \iota_* \mathcal{F}),$$

où $\iota : Z \hookrightarrow X$ est l'inclusion.

On pourra donc se permettre l'abus de notation consistant à écrire $\mathcal{F}$ pour $\iota_* \mathcal{F}$.

Démonstration. Rappelons que tout faisceau flasque étant acyclique, on peut calculer la cohomologie d'un faisceau avec une résolution flasque de celui-ci.

Soit donc $\mathcal{I}^\cdot$ une résolution flasque de $\mathcal{F}$ sur Z. Alors $\iota_* \mathcal{I}^\cdot$ est une résolution flasque de $\iota_* \mathcal{F}$ sur X, et $\Gamma(Z, \mathcal{I}^\cdot) = \Gamma(X, \iota_* \mathcal{I}^\cdot)$, d'où le résultat. □

Théorème 5.1.9 (Cohomologie de l'espace projectif)**.** *Soit $S = k[x_0, \cdots, x_n]$, et soit $X = \mathbb{P}^n_k = \mathrm{Proj}(S)$ l'espace projectif de dimension n sur k. Alors*

(a) L'application naturelle $S \longrightarrow \bigoplus_{m \in \mathbb{Z}} H^0\big(X, \mathcal{O}_X(m)\big)$ est un isomorphisme de S-modules gradués,

(b) Pour tout $m \in \mathbb{Z}$, on a $H^r\big(X, \mathcal{O}_X(m)\big) = 0$ pour $0 < r < n$,

(c) $H^n\big(X, \mathcal{O}_X(-n-1)\big) \simeq k$,

(d) Pour tout $m \in \mathbb{Z}$, on a un accouplement parfait

$$H^0\big(X, \mathcal{O}_X(m)\big) \underset{k}{\otimes} H^n\big(X, \mathcal{O}_X(-m-n-1)\big) \longrightarrow H^n\big(X, \mathcal{O}_X(-n-1)\big) \simeq k.$$

Démonstration. Soit $\mathcal{F}$ le faisceau quasi-cohérent $\bigoplus_{m \in \mathbb{Z}} \mathcal{O}_X(m)$. Comme la cohomologie commute aux sommes directes sur un espace topologique noethérien, la cohomologie de $\mathcal{F}$ sera la somme directe de la cohomologie des $\mathcal{O}_X(m)$. Nous allons donc calculer la cohomologie de $\mathcal{F}$, en prenant garde à la graduation.

Nous choisissons bien évidemment de prendre comme recouvrement affine la famille $\big(U_i = D_+(x_i)\big)_{0 \leqslant i \leqslant n}$. On a alors $U_{i_1, \cdots, i_r} = D_+(x_{i_1} \cdots x_{i_r})$, donc $\mathcal{F}(U_{i_1, \cdots, i_r}) = S[x_{i_1}^{-1}, \cdots, x_{i_r}^{-1}]$. Ainsi, le complexe de Čech s'écrit

$$\prod_{0 \leqslant i_0 \leqslant n} S[x_{i_0}^{-1}] \longrightarrow \prod_{0 \leqslant i_0 < i_1 \leqslant n} S[x_{i_0}^{-1}, x_{i_1}^{-1}] \longrightarrow \cdots \longrightarrow S[x_0^{-1}, \cdots, x_n^{-1}].$$

$H^0(X,\mathcal{F})$ est le noyau de la première flèche, c'est-à-dire S, comme prévu. Ceci prouve (a).

Ensuite, $H^n(X,\mathcal{F})$ est le conoyau de la dernière flèche

$$d^{n-1} \,:\, \prod_{0\leqslant i\leqslant n} S[x_0^{-1},\cdots,\widehat{x_i^{-1}},\cdots,x_n^{-1}] \longrightarrow S[x_0^{-1},\cdots,x_n^{-1}].$$

$S[x_0^{-1},\cdots,x_n^{-1}]$ est un k-espace vectoriel dont une base est formée par les monômes $x_0^{l_0}\cdots x_n^{l_n}$, avec $l_i\in\mathbb{Z}$, et il est clair que l'image de d^{n-1} est le sous-espace engendré par les monômes tels que au moins un des l_i est positif ou nul. Par conséquent, $H^n(X,\mathcal{F})$ est le k-espace vectoriel dont une base est formée par les $x_0^{l_0}\cdots x_n^{l_n}$ avec les l_i strictement négatifs, et la graduation est donnée par le degré $\sum_{i=0}^n l_i$. Il n'existe qu'un seul tel monôme de degré $-n-1$, à savoir $x_0^{-1}\cdots x_n^{-1}$, ce qui prouve (c).

Passons à (d). Le résultat est trivialement vérifié pour $m<0$, puisque les deux membres sont alors nuls d'après (a) et (c). Si maintenant $m\geqslant 0$, $H^0\big(X,\mathcal{O}_X(m)\big)$ admet pour base les monômes $x_0^{l_0}\cdots x_n^{l_n}$ tels que les l_i sont positifs ou nuls et de somme m. L'accouplement avec $H^n\big(X,\mathcal{O}_X(-m-n-1)\big)$ vers $H^n\big(X,\mathcal{O}_X(-n-1)\big)$ est donné par

$$x_0^{l_0}\cdots x_n^{l_n}\otimes x_0^{l'_0}\cdots x_n^{l'_n}\longmapsto x_0^{l_0+l'_0}\cdots x_n^{l_n+l'_n},$$

où $\sum_{i=0}^n l'_i=-m-n-1$ et où le monôme à droite est considéré comme nul dès que l'un des $l_i+l'_i$ est positif ou nul. Ceci est donc bien un accouplement parfait, la base duale des $x_0^{l_0}\cdots x_n^{l_n}$ étant formée des $x_0^{-l_0-1}\cdots x_n^{-l_n-1}$.

Pour terminer, montrons (b) par récurrence sur n. Pour $n=1$ il n'y a rien à prouver, supposons donc $n>1$. En localisant notre complexe de Čech de S-modules gradués par rapport à x_n, on obtient le complexe de Čech de $\mathcal{F}|_{U_n}$ par rapport au recouvrement affine $(U_i\cap U_n)_{0\leqslant i\leqslant n}$ de U_n. Sa cohomologie est donc nulle en degré non nul puisque U_n est affine. Comme la localisation est exacte, on en déduit que pour tout $r>0$, $H^r(X,\mathcal{F})_{x_n}=0$, c'est-à-dire que que tout élément de $H^r(X,\mathcal{F})$, $r>0$, est tué par une puissance de x_n suffisamment grande. Pour conclure, il suffit de montrer que pour $0<r<n$, la multiplication par x_n est une bijection de $H^r(X,\mathcal{F})$ dans lui-même. De la suite exacte de S-modules gradués

$$0\longrightarrow S(-1)\xrightarrow{x_n} S\longrightarrow S/x_nS,$$

on déduit une suit exacte de faisceaux

$$0\longrightarrow\mathcal{O}_X(-1)\longrightarrow\mathcal{O}_X\longrightarrow\mathcal{O}_H\longrightarrow 0,$$

où H est l'hyperplan $x_n = 0$. En faisant la somme directe des suites tordues par $\mathcal{O}_X(n)$ pour tout $n \in \mathbb{Z}$, on obtient

$$0 \longrightarrow \mathcal{F}(-1) \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}_H \longrightarrow 0,$$

où $\mathcal{F} = \bigoplus_{n\in\mathbb{Z}} \mathcal{O}_H(n)$. Il en résulte la suite exacte longue de cohomologie

$$\cdots \longrightarrow H^r\big(X, \mathcal{F}(-1)\big) \longrightarrow H^r\big(X, \mathcal{F}\big) \longrightarrow H^r\big(X, \mathcal{F}_H\big) \longrightarrow H^{r+1}\big(X, \mathcal{F}(-1)\big) \longrightarrow \cdots .$$

En tant que S-modules gradués, on a $H^r\big(X, \mathcal{F}(-1)\big) \simeq H^r\big(X, \mathcal{F}\big)(-1)$, et l'application $H^i\big(X, \mathcal{F}(-1)\big) \longrightarrow H^r\big(X, \mathcal{F}\big)$ est la multiplication par x_n. Or $H \simeq \mathbb{P}_k^{n-1}$; par hypothèse de récurrence, on a donc $H^r(H, \mathcal{F}_H) = 0$ pour $0 < r < n-1$, donc $H^r(X, \mathcal{F}_H) = 0$ pour $0 < r < n-1$ d'après le lemme 5.1.8. De plus, la suite

$$0 \longrightarrow H^0\big(X, \mathcal{F}(-1)\big) \longrightarrow H^0\big(X, \mathcal{F}\big) \longrightarrow H^0\big(X, \mathcal{F}_H\big) \longrightarrow 0$$

est exacte, tout simplement parce que $H^0(X, \mathcal{F}_H) = S/x_nS$, et à l'autre extrémité, la suite

$$0 \longrightarrow H^{n-1}\big(X, \mathcal{F}_H\big) \longrightarrow H^n\big(X, \mathcal{F}(-1)\big) \longrightarrow H^n\big(X, \mathcal{F}\big) \longrightarrow 0$$

est aussi exacte, comme on le vérifie facilement à partir de la description donnée en (a) et en (c). Ainsi, la suite exacte longue de cohomologie nous dit que la multiplication par x_n est un isomorphisme de $H^r\big(X, \mathcal{F}(-1)\big)$ dans $H^r\big(X, \mathcal{F}\big)$, ce qui achève de prouver (b). □

On peut en déduire le résultat de finitude suivant :

Théorème 5.1.10. *Soit X une variété projective sur un corps k, et soit $\mathcal{F}$ un faisceau cohérent sur X.*

(a) Les espaces de cohomologie $H^r(X, \mathcal{F})$ sont tous de dimension finie sur k.

(b) Il existe un entier $n_0 \in \mathbb{N}$ (dépendant de $\mathcal{F}$) tel que pour tout entier $n \geqslant n_0$ et pour tout $r > 0$, $H^r\big(X, \mathcal{F}(n)\big) = 0$.

Démonstration. Considérons un plongement $\iota : X \hookrightarrow \mathbb{P}_k^n$. Comme $\iota_*\mathcal{F}$ est aussi cohérent et a les mêmes espaces de cohomologie que $\mathcal{F}$ d'après le lemme 5.1.8, on peut supposer sans perte de généralité que $X = \mathbb{P}_k^n$.

D'après les formules explicites données par le théorème 5.1.9, le résultat est vrai pour tout faisceau de forme $\mathcal{O}_X(m)$, $m \in \mathbb{Z}$, donc pour toute somme

directe finie de tels faisceaux. Écrivons donc $\mathcal{F}$ comme quotient d'une somme directe finie (puisque $\mathcal{F}$ est cohérent) $\mathcal{G}$ de tels faisceaux, ce qui est loisible grâce au corollaire 5.1.3, et soit $\mathcal{R}$ le noyau, de sorte que la suite

$$0 \longrightarrow \mathcal{R} \longrightarrow \mathcal{G} \longrightarrow \mathcal{F} \longrightarrow 0$$

est exacte.

Montrons que la dimension de $H^r(X, \mathcal{F})$ est finie par récurrence descendante sur r. On a déjà $H^r(X, \mathcal{F}) = 0$ pour $r > n$, car le complexe de Čech est trop court pour permettre le contraire. Mais si $r \leqslant n$, alors la suite exacte longue de cohomologie

$$\cdots \longrightarrow H^r(X, \mathcal{G}) \longrightarrow H^r(X, \mathcal{F}) \longrightarrow H^{r+1}(X, \mathcal{R}) \longrightarrow \cdots$$

permet de récurrer, prouvant ainsi (a).

Pour (b), tensorisons par $\mathcal{O}_X(n)$, et considérons à nouveau la suite exacte longue de cohomologie

$$\cdots \longrightarrow H^r\big(X, \mathcal{G}(n)\big) \longrightarrow H^r\big(X, \mathcal{F}(n)\big) \longrightarrow H^{r+1}\big(X, \mathcal{R}(n)\big) \longrightarrow \cdots .$$

Récurrons à nouveau sur $r \leqslant n$. Pour $n \gg 0$, d'après le théorème 5.1.9, l'espace de gauche est nul, et celui de droite est nul aussi par hypothèse de récurrence ; c'est donc aussi le cas de celui du milieu. Comme il n'y a qu'un nombre fini de valeurs de r en jeu, on peut trouver un n_0 convenable pour toute valeur de r. □

5.2 Faisceaux de différentielles

Nous allons à présent définir un faisceau particulier qui jouera un rôle essentiel lors de la démonstration du théorème de Riemann-Roch. Toutefois, avant définir ce *faisceau de différentielles*, nous avons besoin d'un préliminaire d'algèbre commutative à propos des dérivations.

Soient R un anneau commutatif unitaire, A une R-algèbre, et M un A-module.

Définition 5.2.1. Une *R-dérivation de A à valeurs dans M* est une application $d : A \longrightarrow M$ telle que

- $d(a + a') = d(a) + d(a') \quad (a, a' \in A)$
- $d(aa') = ad(a') + a'd(a) \quad (a, a' \in A)$

- $\forall r \in R$, $d(r) = 0$.

Définition 5.2.2. Un *module de dérivations universel* est un A-module $\Omega_{A/R}$ muni d'une dérivation $\partial : A \to \Omega_{A/R}$ vérifiant la propriété universelle suivante : pour tout A-module M et pour toute dérivation $d : A \to M$, il existe une unique application A-linéaire $f : \Omega_{A/R} \to M$ telle que $d = f \circ \partial$.

Exemple 5.2.3. Soit $A = R[x_1, \cdots, x_n]$ une algèbre de polynômes. Alors A admet un module de dérivations universel, à savoir

$$\Omega_{A/R} = \bigoplus_{i=1}^{n} A\,\partial x_i;$$

en effet les axiomes de dérivations font qu'on dérivation de A dans un A-module M est entièrement déterminée par sa valeur en les x_i, $1 \leqslant i \leqslant n$, et que ces valeurs peuvent être arbitrairement choisies.

Exemple 5.2.4. Si $A = R[x_1, \cdots, x_n]/(f_1, \cdots, f_r)$ est une R-algèbre de type fini, alors on voit de même que A admet le module de dérivations universel

$$\Omega_{A/R} = \left(\bigoplus_{i=1}^{n} A\,\partial x_i\right) \Big/ \left(\sum_{i=1}^{n} \frac{\partial f_1}{\partial x_i}\partial x_i, \cdots, \sum_{i=1}^{n} \frac{\partial f_r}{\partial x_i}\partial x_i\right),$$

où $\frac{\partial f}{\partial x_i}$ désigne bien entendu la dérivée partielle usuelle.

Il est clair que le couple $(\Omega_{A/R}, \partial)$, s'il existe, est unique à isomorphisme près. Le résultat suivant nous explique comment le construire.

Théorème 5.2.5. *Soit $B = A \underset{R}{\otimes} A$, muni de la structure de A-module définie par $a \cdot (x \otimes y) = ax \otimes y$, et soient $\mu : B \to A$, $x \otimes y \mapsto xy$ la multiplication de A, et $I = \operatorname{Ker} \mu \subset B$ son noyau. Alors $\Omega_{A/R} = I/I^2$, muni de*

$$\begin{array}{rccc} \partial & : & A & \longrightarrow & I/I^2 \\ & & a & \longmapsto & (1 \otimes a - a \otimes 1) \bmod I^2 \end{array},$$

est un module de dérivations universelles.

Démonstration. Tout d'abord, il est facile de vérifier que ∂ est bien une dérivation : si $a, a' \in A$, alors on a dans B

$$1 \otimes aa' = (1 \otimes a)(1 \otimes a') = (a \otimes 1 + \partial(a))(a' \otimes 1 + \partial(a')) \equiv aa' \otimes 1 + a\partial(a') + a'\partial(a) \bmod I^2,$$

et il est clair que ∂ envoie R sur 0. Étudions à présent le problème universel. On remarque que dans B,

$$x \otimes y = xy \otimes 1 + x(1 \otimes y - y \otimes 1) = \mu(x \otimes y) + x\partial(y).$$

Par conséquent, si $\sum_i x_i \otimes y_i \in I = \operatorname{Ker} \mu$, alors $\sum_i x_i \otimes y_i = \sum_i x_i \partial y_i$, ce qui montre que $\Omega_{A/R}$ est engendré par les $\partial(a)$ en tant que A-module. Ainsi, l'application f, si elle existe, est unique. Pour montrer l'existence, munissons le A-module $C = A \times M$ d'une structure de A-algèbre en posant

$$(a, m)(a', m') = (aa', am' + a'm).$$

Pour ce produit, $M \subset C$ est un idéal de carré nul, et l'application

$$\begin{array}{rccc} \phi & : & B & \longrightarrow & C \\ & & x \otimes y & \longmapsto & (xy, xd(y)) \end{array}$$

est un morphisme de A-algèbres. De plus, comme $\phi(I) \subset M$, $\phi(I^2) = 0$, donc $\phi|_I$ se factorise en une application A-linéaire $f : \Omega_{A/R} \longrightarrow M$ qui répond au problème puisque $(f \circ \partial)(a) = \phi(1 \otimes a - a \otimes 1) = 1d(a) - ad(1) = d(a)$ car $d(1) = 0$. □

Corollaire 5.2.6. *Pour toute partie multiplicative S de A, $\Omega_{S^{-1}A/R} = S^{-1}\Omega_{A/R}$.*

Ce corollaire permet la définition suivante :

Définition 5.2.7. Soit X un R-schéma. Le *faisceau des différentielles* de X est le faisceau quasi-cohérent Ω_X obtenu par recollement des faisceaux $\widetilde{\Omega_{A/R}}$ définis sur les ouverts affines $U = \operatorname{Spec}(A)$ de X.

Les dérivations universelles $\partial : A \longrightarrow \Omega_{A/R}$ se recollent en un morphisme de faisceaux de groupes abéliens $\partial : \mathcal{O}_X \longrightarrow \Omega_X$ qui induit des R-dérivations universelles sur les anneaux locaux.

Exemple 5.2.8. Le raisonnement mené à l'exemple 5.2.3 montre que pour $X = \mathbb{A}^n_R$, le faisceau Ω_X est un $\mathcal{O}_X$-module libre de rang n, généré par les sections globales $\partial x_1, \cdots, \partial x_n$, où $x_1, \cdots, x_n$ sont des coordonnées affines sur X.

Il est égalent possible d'expliciter le faisceau de différentielles d'un espace projectif, c'est ce que nous ferons pour conclure cette section.

Proposition 5.2.9. *Soit $X = \mathbb{P}^n_R$ l'espace projectif de dimension $n \in \mathbb{N}$ sur R. On a une suite exacte*

$$0 \longrightarrow \Omega_X \longrightarrow \mathcal{O}_X(-1)^{n+1} \longrightarrow \mathcal{O}_X \longrightarrow 0.$$

Démonstration. Soit $S = R[x_0, \cdots, x_n]$ l'anneau de coordonnées homogènes de X, et soit E le S-module gradué $S(-1)^{n+1}$, de base formée par les éléments $e_0, \cdots, e_n$ de degré 1. Considérons le morphisme de S-modules gradués de E dans S envoyant e_i sur x_i, et soit $M \subset E$ son noyau. Bien que ce morphisme ne soit pas surjectif, il l'est en degré non nul, donc la suite exacte de S-modules gradués

$$0 \longrightarrow M \longrightarrow E \longrightarrow S \longrightarrow 0$$

donne lieu à une suite exacte courte de faisceaux

$$0 \longrightarrow \widetilde{M} \longrightarrow \mathcal{O}_X(-1)^{n+1} \longrightarrow \mathcal{O}_X \longrightarrow 0.$$

Pour conclure, construisons un isomorphisme $\varphi : \Omega_X \xrightarrow{\sim} \widetilde{M}$. On remarque qu'en localisant en x_i, on obtient un morphisme surjectif $E_{x_i} \longrightarrow S_{x_i}$ de S_{x_i}-modules, de noyau M_{x_i} libre de rang n puisque admettant pour base $\left(e_j - \frac{x_j}{x_i} e_i\right)_{j \neq i}$. Par conséquent, en notant comme d'habitude $U_i = D_+(x_i)$, $\widetilde{M}|_{U_i}$ est le $\mathcal{O}_{U_i}$-module libre de rang n généré par les sections globales $\left(\frac{1}{x_i} e_j - \frac{x_j}{x_i^2} e_i\right)_{j \neq i}$. Or $U_i \simeq \operatorname{Spec}\left(R\left[\frac{x_0}{x_i}, \cdots, \frac{x_0}{x_i}\right]\right) \simeq \mathbb{A}^n_R$, donc d'après l'exemple 5.2.8, Ω_{U_i}, qui n'est d'ailleurs rien d'autre que $\Omega_X|_{U_i}$, est le $\mathcal{O}_{U_i}$-module libre de rang n généré par $\left(\partial\left(\frac{x_j}{x_i}\right)\right)_{j \neq i}$. On peut donc définir un isomorphisme

$$\begin{array}{rccc} \varphi_i & : & \Omega_{U_i} & \longrightarrow & \widetilde{M}|_{U_i} \\ & & \partial\left(\frac{x_j}{x_i}\right) & \longmapsto & \frac{1}{x_i} e_j - \frac{x_j}{x_i^2} e_i. \end{array}$$

Ces isomorphismes $(\varphi_i)_{0 \leqslant i \leqslant n}$ se recollent en un isomorphisme $\varphi : \Omega_X \xrightarrow{\sim} \widetilde{M}$; en effet, sur $U_i \cap U_j$, on a $\dfrac{x_k}{x_i} = \dfrac{x_k}{x_j} \dfrac{x_j}{x_i}$, donc

$$\partial\left(\frac{x_k}{x_i}\right) - \frac{x_k}{x_j}\, \partial\left(\frac{x_j}{x_i}\right) = \frac{x_j}{x_i}\, \partial\left(\frac{x_k}{x_j}\right),$$

et, en appliquant φ_i au membre de gauche et φ_j au membre de droite, on obtient la même chose, à savoir $\dfrac{x_j e_k - x_k e_j}{x_i x_j}$. □

5.3 Dualité de Serre

Dans cette section, nous présentons la *dualité de Serre*, qui relie les groupes de cohomologie des faisceaux H^r et H^{n-r} sur une variété de dimension n. Nous l'appliquerons plus tard en dimension $n = 1$, ce qui nous permettra de démontrer le théorème de Riemann-Roch par les courbes.

Définition 5.3.1. Si $\mathcal{F}$ et $\mathcal{G}$ sont deux $\mathcal{O}_X$-modules sur un schéma X, nous noterons $\mathrm{Hom}_X(\mathcal{F}, \mathcal{G})$ le *groupe abélien* des morphismes de $\mathcal{O}_X$-modules de $\mathcal{F}$ dans $\mathcal{G}$, et $\mathcal{H}om_X(\mathcal{F}, \mathcal{G})$ le *faisceau de groupes abéliens* de morphismes de $\mathcal{O}_X$-modules de $\mathcal{F}$ dans $\mathcal{G}$. En posant $\mathcal{F}^\vee = \mathcal{H}om_X(\mathcal{F}, \mathcal{O}_X)$, on a alors, pour tout $\mathcal{O}_X$-module $\mathcal{L}$ localement libre de rang fini,

$$\mathcal{H}om_X(\mathcal{L}, \mathcal{F}) \simeq \mathcal{L}^\vee \underset{\mathcal{O}_X}{\otimes} \mathcal{F},$$

$$\mathrm{Hom}_X\left(\mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{F}, \mathcal{G}\right) \simeq \mathrm{Hom}_X\left(\mathcal{F}, \mathcal{H}om_X(\mathcal{L}, \mathcal{G})\right),$$

et donc $\mathrm{Hom}_X\left(\mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{F}, \mathcal{G}\right) \simeq \mathrm{Hom}_X\left(\mathcal{F}, \mathcal{L}^\vee \underset{\mathcal{O}_X}{\otimes} \mathcal{G}\right)$.

On définit les foncteurs Ext^r_X et $\mathcal{E}xt^r_X$ comme les foncteurs dérivés à droite par rapport à la seconde variable de Hom_X et $\mathcal{H}om_X$, respectivement (on ne pourrait pas dériver par rapport à la première variable car les catégorie des $\mathcal{O}_X$-modules n'a pas toujours assez de projectifs).

Commençons par établir une dualité pour l'espace projectif :

Théorème 5.3.2 (Dualité pour l'espace projectif)**.** *Soient k un corps, $X = \mathbb{P}^n_k$ l'espace projectif de dimension n sur k, Ω_X son faisceau de différentielles, et $\omega_X = \bigwedge^n \Omega_X$.*

(a) $H^n(X, \omega_X) \simeq k$. Un tel isomorphisme étant fixé,

(b) Pour tout faisceau cohérent $\mathcal{F}$ sur X, l'application naturelle

$$\mathrm{Hom}_X(\mathcal{F}, \omega_X) \underset{k}{\otimes} H^n(X, \mathcal{F}) \longrightarrow H^n(X, \omega_X) \xrightarrow{\sim} k$$

est un accouplement parfait de k-espaces vectoriels de dimension finie,

(c) Pour tout $r \geqslant 0$, on a un isomorphisme $\mathrm{Ext}^r_X(\mathcal{F}, \omega_X) \simeq H^{n-r}(X, \mathcal{F})'$, fonctoriel en $\mathcal{F}$.

Démonstration. D'après la proposition 5.2.9, on a une suite exacte

$$0 \longrightarrow \Omega_X \longrightarrow \mathcal{O}_X(-1)^{n+1} \longrightarrow \mathcal{O}_X \longrightarrow 0.$$

En prenant les puissances extérieures n-ièmes, on en déduit que

$$\omega_X = \bigwedge^n \Omega_X \simeq \mathcal{O}_X(-n-1).$$

Le (a) découle donc du théorème 5.1.9 (a).

Passons donc à (b). D'après le théorème 5.1.10 (a), les espaces en jeu sont bien de dimension finie sur k. L'accouplement est défini comme suit : le morphisme de $\mathcal{F}$ dans ω_X définit par fonctorialité un morphisme de $H^n(X, \mathcal{F})$ dans $H^n(X, \omega_X)$, que l'on évalue sur l'élément de $H^n(X, \mathcal{F})$ pour arriver dans $H^n(X, \omega_X)$.

Si $\mathcal{F}$ est un $\mathcal{O}(m)$ pour un certain $m \in \mathbb{Z}$, alors $\mathrm{Hom}(\mathcal{F}, \omega_X) \simeq H^0\big(X, \omega_X(-m)\big)$, et le résultat s'ensuit par le théorème 5.1.9 (d). Dans le cas général, on écrit $\mathcal{F}$ comme le conoyau

$$\mathcal{R} \longrightarrow \mathcal{G} \longrightarrow \mathcal{F} \longrightarrow 0,$$

où $\mathcal{R}$ et $\mathcal{G}$ sont des sommes directes de $\mathcal{O}(m_i)$, $m_i \in \mathbb{Z}$. Comme $\mathrm{Hom}(\cdot, \omega_X)$ et $H^n(X, \cdot)'$ sont tous les deux des foncteurs contravariants exacts à gauche, le lemme des cinq permet de conclure.

Montrons (c) pour terminer. Les deux membres sont des δ-foncteurs en $\mathcal{F}$, indexés par $r \geqslant 0$. Pour $r = 0$, on a bien un isomorphisme par (b). Pour conclure, il suffit donc de montrer que ces δ-foncteurs sont universels. Or, comme $\mathcal{F}$ est cohérent, c'est d'après le corollaire 5.1.3 le quotient d'un faisceau $\mathcal{E} = \bigoplus_{i=1}^s \mathcal{O}_X(-m_i)$ avec $m_i \gg 0$. On alors d'une part $\mathrm{Ext}^r_X(\mathcal{E}, \omega_X) \simeq \bigoplus_{i=1}^s H^r\big(X, \omega_X(m_i)\big)$, qui est nul pour $r > 0$ et $m_i \gg 0$ d'après le théorème 5.1.9, et d'autre part $H^{n-r}(X, \mathcal{E})' \simeq \bigoplus_{i=1}^s H^{n-r}\big(X, \mathcal{O}_X(-m_i)\big)'$, qui est lui aussi nul pour $r > 0$ et $m_i \gg 0$ d'après le théorème 5.1.9. Par conséquent, ces δ-foncteurs sont coeffaçables, donc universels. □

Ceci motive la définition suivante :

Définition 5.3.3. Soit X une variété projective de dimension n sur un corps k. Un *faisceau dualisant* pour X consiste en la donnée d'un faisceau cohérent ω_X sur X et d'une forme k-linéaire t, dite *forme trace*, sur $H^n(X, \omega_X)$, tels que pour tout faisceau cohérent $\mathcal{F}$ sur X, l'application naturelle

$$\mathrm{Hom}(\mathcal{F}, \omega_X) \underset{k}{\otimes} H^n(X, \mathcal{F}) \longrightarrow H^n(X, \omega_X) \xrightarrow{t} k$$

soit un accouplement parfait, donnant ainsi un isomorphisme

$$\mathrm{Hom}(\mathcal{F}, \omega_X) \simeq H^n(X, \mathcal{F})'.$$

Remarquons qu'un faisceau dualisant, s'il existe, est unique. En effet, l'isomorphisme ci-dessus étant clairement fonctoriel en $\mathcal{F}$, on peut reformuler la définition en disant que ω_X représente $H^n(X, \cdot)'$; il est donc unique d'après le lemme de Yoneda.

Nous allons à présent montrer que toute variété projective admet un faisceau dualisant, et le calculer. Pour ce faire, nous verrons la variété en question comme plongée dans un espace projectif, et, grâce au lemme 5.1.8, on ne se privera pas de voir les faisceaux définis sur la variété comme des faisceaux sur l'espace projectif tout entier.

Commençons par montrer l'existence. Comme nous utiliserons les Ext, nous démarrons par quelques lemmes à leur sujet.

Lemme 5.3.4. *Soit X un schéma, et soit $\mathcal{L}$ un $\mathcal{O}_X$-module localement libre de rang fini.*

(a) Pour tout $\mathcal{O}_X$-module injectif $\mathcal{I}$, $\mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{I}$ est aussi injectif.

(b) Pour tous $\mathcal{O}_X$-modules $\mathcal{F}$ et $\mathcal{G}$, on a pour tout $r \in \mathbb{N}$

$$\mathrm{Ext}^r_X\left(\mathcal{F} \underset{\mathcal{O}_X}{\otimes} \mathcal{L}, \mathcal{G}\right) \simeq \mathrm{Ext}^r_X\left(\mathcal{F}, \mathcal{L}^\vee \underset{\mathcal{O}_X}{\otimes} \mathcal{G}\right) \quad \textit{et}$$

$$\mathcal{E}xt^r_X\big(\mathcal{F} \underset{\mathcal{O}_X}{\otimes} \mathcal{L}, \mathcal{G}\big) \simeq \mathcal{E}xt^r_X\big(\mathcal{F}, \mathcal{L}^\vee \underset{\mathcal{O}_X}{\otimes} \mathcal{G}\big) \simeq \mathcal{E}xt^r_X\big(\mathcal{F}, \mathcal{G}\big) \underset{\mathcal{O}_X}{\otimes} \mathcal{L}^\vee.$$

Démonstration. Le (a) résulte de ce que le foncteur $\mathrm{Hom}_X\left(\cdot, \mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{I}\right) \simeq \mathrm{Hom}_X\left(\cdot \underset{\mathcal{O}_X}{\otimes} \mathcal{L}^\vee, \mathcal{I}\right)$ est exact, puisque composé du foncteur $\cdot \underset{\mathcal{O}_X}{\otimes} \mathcal{L}^\vee$, qui est exact puisque $\mathcal{L}^\vee$ est localement libre, et de $\mathrm{Hom}_X(\cdot, \mathcal{I})$, qui est exact puisque $\mathcal{I}$ est injectif.

Il est clair que (b) est vrai pour $r = 0$. Mais les cinq membres sont des δ-foncteurs indexés par r puisque $\cdot \underset{\mathcal{O}_X}{\otimes} \mathcal{L}^\vee$ est exact, et (a) nous dit qu'ils s'annulent si $\mathcal{G}$ est injectif ; ils sont donc effaçables, donc universels, donc l'isomorphisme pour $r = 0$ se propage à tous les r. □

Lemme 5.3.5. *Soit X une variété projective sur un corps k, et soient $\mathcal{F}$ et $\mathcal{G}$ deux faisceaux cohérents sur X. Pour tout $r \in \mathbb{N}$, il existe un $n_0 \in \mathbb{N}$ tel que pour tout $n \geqslant n_0$, on ait* $\mathrm{Ext}^r_X\left(\mathcal{F}, \mathcal{G}(n)\right) \simeq \Gamma\big(X, \mathcal{E}xt^r_X\big(\mathcal{F}, \mathcal{G}(n)\big)\big)$.

Démonstration. Comme Hom $= \Gamma(X, \mathcal{H}om)$, ceci est vrai pour $r = 0$. De plus, si $\mathcal{F} = \mathcal{O}_X$, comme $\mathcal{H}om_X(\mathcal{O}_X, \cdot)$ est le foncteur identité, d'une part il n'a pas de cohomologie donc le membre de droite est nul pour $r > 0$, et d'autre part le membre de gauche vaut $H^r\big(X, \mathcal{G}(n)\big)$, donc est nul pour $r > 0$ et $n \gg 0$ d'après le corollaire 5.1.10 (b), d'où le résultat pour $\mathcal{F} = \mathcal{O}_X$.

Si $\mathcal{F}$ est localement libre (donc forcément de rang fini), on se ramène au cas précédent grâce au lemme 5.3.4 (b) précédent.

En fin, dans le cas général, écrivons $\mathcal{F}$ comme quotient d'un faisceau localement libre de rang fini, ce qui est loisible d'après le corollaire 5.1.3, et notons $\mathcal{R}$ le quotient, de sorte que

$$0 \longrightarrow \mathcal{R} \longrightarrow \mathcal{E} \longrightarrow \mathcal{F} \longrightarrow 0$$

soit exacte. Alors pour tout $\mathcal{O}_X$-module injectif $\mathcal{I}$, la suite

$$0 \longrightarrow \mathrm{Hom}_X(\mathcal{F}, \mathcal{I}) \longrightarrow \mathrm{Hom}_X(\mathcal{E}, \mathcal{I}) \longrightarrow \mathrm{Hom}_X(\mathcal{R}, \mathcal{I}) \longrightarrow 0$$

est encore exacte ; par conséquent, si on prend une résolution injective $0 \longrightarrow \mathcal{G}(n) \longrightarrow \mathcal{I}^{\cdot}$ de $\mathcal{G}(n)$, on obtient la suite exacte de complexes

$$0 \longrightarrow \mathrm{Hom}_X(\mathcal{F}, \mathcal{I}^{\cdot}) \longrightarrow \mathrm{Hom}_X(\mathcal{E}, \mathcal{I}^{\cdot}) \longrightarrow \mathrm{Hom}_X(\mathcal{R}, \mathcal{I}^{\cdot}) \longrightarrow 0.$$

Le cas précédent nous dit alors que la suite exacte longue associée se scinde en une suite exacte

$$0 \to \mathrm{Hom}_X\left(\mathcal{F}, \mathcal{G}(n)\right) \to \mathrm{Hom}_X\left(\mathcal{E}, \mathcal{G}(n)\right) \to \mathrm{Hom}_X\left(\mathcal{R}, \mathcal{G}(n)\right) \to \mathrm{Ext}^1_X\left(\mathcal{F}, \mathcal{G}(n)\right) \to 0$$

et en des isomorphismes $\mathrm{Ext}^r\left(\mathcal{R}, \mathcal{G}(n)\right) \simeq \mathrm{Ext}^{r+1}\left(\mathcal{F}, \mathcal{G}(n)\right)$ pour $r > 0$, et on obtient un résultat similaire pour $\mathcal{H}om$ et $\mathcal{E}xt$. D'après le théorème 5.1.2, si $n \gg 0$, alors les faisceaux de la suite à quatre termes sont engendrés par leurs sections globales, donc les suites de sections globales sont exactes, d'où le résultat pour $r = 1$ par le lemme des cinq. Et comme $\mathcal{R}$ est lui-même cohérent, les isomorphismes permettent d'en déduire le résultat général par récurrence. □

Nous pouvons alors débuter la construction d'un faisceau dualisant :

Lemme 5.3.6. *Soit X un sous-schéma fermé de codimension $d = N - \dim(X)$ de l'espace projectif $P = \mathbb{P}^N_k$. Pour tout $r < d$, on a $\mathcal{E}xt^r_P(\mathcal{O}_X, \omega_P) = 0$.*

Démonstration. Pour tout r, le faisceau $\mathcal{E}xt^r_P(\mathcal{O}_X, \omega_P)$ est cohérent sur P, donc, après décalage par un entier m suffisamment grand, est généré par ses sections globales d'après le théorème 5.1.2. Par conséquent, pour montrer qu'il est nul, il suffit de montrer que $\Gamma\big(P, \mathcal{E}xt^r_P(\mathcal{O}_X, \omega_P)(m)\big) = 0$ pour $m \gg 0$. Or les lemmes 5.3.4 et 5.3.5 précédents nous disent que $\Gamma\big(P, \mathcal{E}xt^r_P(\mathcal{O}_X, \omega_P)(m)\big) \simeq \Gamma\big(P, \mathcal{E}xt^r_P\big(\mathcal{O}_X, \omega_P(m)\big)\big) \simeq \mathrm{Ext}^r_P\big(\mathcal{O}_X, \omega_P(m)\big)$ si $m \gg 0$, et le membre de droite est le dual de $H^{N-r}\big(P, \mathcal{O}_X(-m)\big) \simeq H^{N-r}\big(X, \mathcal{O}_X(-m)\big)$ d'après le théorème 5.3.2 (c). Comme $N - r > \dim(X)$ pour $r < d$, ce groupe de cohomologie est nul d'après le théorème 5.1.4, ce qui conclut. □

Lemme 5.3.7. *Soit X un sous-schéma fermé de codimension d de l'espace projectif $P = \mathbb{P}^N_k$. Pour tout $\mathcal{O}_X$-module $\mathcal{F}$, on a un isomorphisme*

$$\mathrm{Hom}_X\big(\mathcal{F}, \mathcal{E}xt^d_P(\mathcal{O}_X, \omega_P)\big) \simeq \mathrm{Ext}^d_P(\mathcal{F}, \omega_P),$$

fonctoriel en $\mathcal{F}$.

Démonstration. Soit $0 \longrightarrow \omega_P \longrightarrow \mathcal{I}^{\cdot}$ une résolution de ω_P par des $\mathcal{O}_P$-modules injectifs, de sorte que les $\mathrm{Ext}^r_P(\mathcal{F}, \omega_P)$ sont les groupes de cohomologie du complexe $\mathrm{Hom}_P(\mathcal{F}, \mathcal{I}^{\cdot})$. Comme $\mathcal{F}$ est un $\mathcal{O}_X$-module, on a $\mathcal{F} \simeq \mathcal{H}om_P(\mathcal{O}_X, \mathcal{F})$ car $\mathcal{H}om_P(\mathcal{O}_X, \cdot) = \mathcal{H}om_X(\mathcal{O}_X, \cdot)$ est le morphisme identité sur les $\mathcal{O}_X$-modules ; par conséquent tout morphisme de $\mathcal{F}$ vers un $\mathcal{I}^r$ se factorise par $\mathcal{J}^r = \mathcal{H}om_P(\mathcal{O}_X, \mathcal{I}^r)$, si bien que les $\mathrm{Ext}^r_P(\mathcal{F}, \omega_P)$ sont les groupes de cohomologie du complexe $\mathrm{Hom}_X(\mathcal{F}, \mathcal{J}^{\cdot})$.

Comme $\mathrm{Hom}_X(\cdot, \mathcal{J}^r) \simeq \mathrm{Hom}_P(\cdot, \mathcal{I}^r)$ est exact sur les $\mathcal{O}_X$-modules, les $\mathcal{J}^r$ sont des $\mathcal{O}_X$-modules injectifs. De plus, les groupes de cohomologie de $\mathcal{J}^{\cdot}$ étant les $\mathcal{E}xt^{\cdot}_P(\mathcal{O}_X, \omega_P)$, le lemme 5.3.7 précédent nous dit que le complexe $\mathcal{J}^{\cdot}$ est exact en degré $r < d$, donc scindé en degré $r \leqslant d$ puisque ses objets sont injectifs. Par conséquent, il s'écrit comme somme directe $\mathcal{J}^{\cdot} = \mathcal{J}^{\cdot}_1 \oplus \mathcal{J}^{\cdot}_2$ d'un complexe exact $\mathcal{J}^{\cdot}_1$ concentré entre les degrés 0 et d et d'un complexe $\mathcal{J}^{\cdot}_2$ démarrant en degré d. On a donc $\mathcal{E}xt^d_P(\mathcal{O}_X, \omega_P) = \mathrm{Ker}(d^d_2 : \mathcal{J}^d_2 \to \mathcal{J}^{d+1}_2)$, d'où $\mathrm{Hom}_X\big(\mathcal{F}, \mathcal{E}xt^d_P(\mathcal{O}_X, \omega_P)\big) \simeq \mathrm{Ext}^d_P(\mathcal{F}, \omega_P)$ fonctoriellement en les $\mathcal{O}_X$-modules $\mathcal{F}$ comme voulu. □

Théorème 5.3.8. *Soit X une variété projective sur un corps k. Voyons X comme un sous-schéma fermé de l'espace projectif $P = \mathbb{P}^N_k$. Alors X admet le faisceau dualisant $\omega_X = \mathcal{E}xt^d_P(\mathcal{O}_X, \omega_P)$, où $d = N - \dim(X)$ est la codimension de X.*

Démonstration. Soit d la codimension de X dans P. Posons $\omega_X = \mathcal{E}xt^d_P(\mathcal{O}_X, \omega_P)$, et montrons que c'est bien un faisceau dualisant pour X.

D'après le lemme 5.3.7 précédent, on a $\mathrm{Hom}_X(\mathcal{F}, \omega_X) \simeq \mathrm{Ext}^d_P(\mathcal{F}, \omega_P)$ pour tout $\mathcal{O}_X$-module $\mathcal{F}$. Or, si $\mathcal{F}$ est cohérent, le théorème 5.3.2 (c) nous dit que $\mathrm{Ext}^d_P(\mathcal{F}, \omega_P) \simeq H^{N-d}(P, \mathcal{F})'$. Comme $\mathcal{F}$ est un faisceau sur X, on obtient bien un isomorphisme $\mathrm{Hom}_X(\mathcal{F}, \omega_X) \simeq H^{\dim(X)}(X, \mathcal{F})'$ fonctoriel en $\mathcal{F}$. En particulier, en prenant $\mathcal{F}\omega_X$, l'élément $Id \in \mathrm{Hom}_X(\omega_X, \omega_X)$ fournit la forme trace $t \in H^{\dim(X)}(X, \mathcal{F})'$. On vérifie alors facilement par fonctorialité que (ω_X, t) est bien dualisant pour X. □

Nous avons donc prouvé l'existence d'un faisceau dualisant sur toute variété projective, mais force est de reconnaître que la forme que nous en avons donnée n'est guère explicite. Le théorème suivante corrige ce problème de manière satisfaisante.

Théorème 5.3.9. *Soit X une variété projective sur un corps k, et soit Ω_X son faisceau de différentielles. Le faisceau dualisant de X vaut $\omega_X \simeq \bigwedge^{\dim(X)} \Omega_X$.*

Ce résultat généralise donc le cas de l'espace projectif 5.3.2. Nous n'en donnerons pas la démonstration, car celle-ci nous emmènerait trop loin ; le lecteur pourra la trouver dans [Har77], théorème III.7.11.

Références

[AT09] Artin, Emil ; Tate, John, **Class field theory**. Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009. viii+194 pp. ISBN : 978-0-8218-4426-7.

[Bom74] Bombieri, Enrico, **Counting points on curves over finite fields** (d'après S. A. Stepanov). Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, pp. 234–241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974.

[Bro82] Brown, Kenneth S., **Cohomology of groups**. Graduate Texts in Mathematics, 87. Springer-Verlag, New York-Berlin, 1982. x+306 pp. ISBN : 0-387-90688-6.

[Bur04] Burns, David, **On the values of equivariant zeta functions of curves over finite fields**. Doc. Math. 9 (2004), 357–399.

[Del74] Deligne, Pierre, **La conjecture de Weil I**. Inst. Hautes Études Sci. Publ. Math. No. 43 (1974), 273–307.

[Del80] Deligne, Pierre, **La conjecture de Weil II**. Inst. Hautes Études Sci. Publ. Math. No. 52 (1980), 137–252.

[Dwo60] Dwork, Bernard, **On the rationality of the zeta function of an algebraic variety**. Amer. J. Math. 82 1960 631–648.

[Gab83] Gabber, Ofer, **Sur la torsion dans la cohomologie l-adique d'une variété**. C. R. Acad. Sci. Paris Sér. I Math. 297 (1983), no. 3, 179–182.

[Har77] Hartshorne, Robin, **Algebraic geometry**. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. ISBN : 0-387-90244-9.

[HS71] Hilton, Peter John ; Stammbach, Urs, **A course in homological algebra**. Graduate Texts in Mathematics, Vol. 4. Springer-Verlag, New York-Berlin, 1971. ix+338 pp.

[Kat76] Katz, Nicholas M., **An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields**. Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), pp. 275–305. Amer. Math. Soc., Providence, R.I., 1976.

[Kob84] Koblitz, Neal, **p-adic numbers, p-adic analysis, and zeta-functions**. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984. xii+150 pp. ISBN : 0-387-96017-1.

[Lic05] Lichtenbaum, Stephen, **The Weil-étale topology on schemes over finite fields**. Compos. Math. 141 (2005), no. 3, 689–702.

[Lic09] Lichtenbaum, Stephen, **The Weil-étale topology for number rings**. Ann. of Math. (2) 170 (2009), no. 2, 657–683.

[Lor96] Lorenzini, Dino, **An invitation to arithmetic geometry**. Graduate Studies in Mathematics, 9. American Mathematical Society, Providence, RI, 1996. xvi+397 pp. ISBN : 0-8218-0267-4.

[Mil80] Milne, James S., **Étale cohomology**. Princeton Mathematical Series, 33. Princeton University Press, Princeton, N.J., 1980. xiii+323 pp. ISBN : 0-691-08238-3.

[Mil86] Milne, James S., **Values of zeta functions of varieties over finite fields**. Amer. J. Math. 108 (1986), no. 2, 297–360.

[Neu99] Neukirch, Jürgen ; Schmidt, Alexander ; Wingberg, Kay, **Cohomology of number fields**. Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2000. xvi+699 pp. ISBN : 3-540-66671-0.

[Ram05] Ramachandran, Niranjan, **Values of zeta functions at $\mathbf{s = 1/2}$**. Int. Math. Res. Not. 2005, no. 25, 1519–1541.

[Ros94] Rosenberg, Jonathan, **Algebraic K-theory and its applications**. Graduate Texts in Mathematics, 147. Springer-Verlag, New York, 1994. x+392 pp. ISBN : 0-387-94248-3.

[Wei49] Weil, André, **Numbers of solutions of equations in finite fields**. Bull. Amer. Math. Soc. 55, (1949). 497–508.