Déterminants de cohomologie et lois de réciprocité : le cas des corps de nombres

M. Kapranov, A. Smirnov

Les analogies entre les corps de nombres et les corps de fonctions ont été depuis longtemps une source d'inspiration en arithmétique. Pourtant, l'un des problèmes les plus intrigants de cette approche, notamment le problème du point absolu, est toujours loin d'être compris d'une façon satisfaisante. Le schéma $\mathrm{Spec}(\mathbb{Z})$, l'objet final dans la catégorie des schémas, a pour dimension 1 par rapport à la topologie de Zariski et au moins 3 par rapport à la topologie étale. Ceci a engendré de longue date un désir d'introduire un objet plus mythique P, le "point absolu", avec un morphisme naturel $\pi_X : X \to P$ donné pour tout schéma arithmétique X de telle façon que les invariants globaux de X aient une interprétation en fonction d'une version de l'image directe en ce qui concerne π_X. Ce problème fait intervenir également la question de la compactification, puisque même un schéma propre sur $\mathbb{Z}$ est encore non-compact à l'infini arithmétique.

Une théorie qui a traité ces problèmes avec succès est la géométrie d'Arakelov [...]. Les compactifications qu'elle fournit font intervenir des métriques riemaniennes dans les ensembles des points réels des schémas arithmétiques, et les invariants cohomologiques ont la forme de volumes de domaines fondamentaux de certains réseaux (donnés par l'image directe vers $\mathrm{Spec}(\mathbb{Z})$) en ce qui concerne les formes venant des métriques. Le volume d'un corps convexe est le terme dominant de l'asymptote du nombre de points entiers de ses dilatations. Donc l'analogue des invariants de type Arakelov dans la situation plus géométrique est le terme dominant du polynôme de Hilbert d'un faisceau cohérent, qui décrit l'asymptote de la dimension de l'espace des sections d'ordre croissant des pôles à l'infini.

Par conséquent, la sortie de la théorie d'Arakelov est essentiellement archimédienne, ayant à voir avec l'asymptote de certains entiers parmi les nombres réels.

Dans le présent article, nous aimerions initier une approche différente du problème des invariants cohomologiques "absolus" qui pourrait être appelée géométrie d'Arakelov modulo n. Décrivons-en les idées principales.

D'abord, c'est une ancienne idée d'interpréter la combinatoire des ensembles finis comme la limite lorsque $q \to 1$ de l'algèbre linéaire sur les corps finis $\mathbb{F}_q$. Cela a amené à de fréquentes considérations sur l'objet folklorique $\mathbb{F}_1$, le "corps à un élément", dont les espaces vectoriels sont juste les ensembles. On peut postuler, bien sûr, que $\mathrm{Spec}(\mathbb{F}_1)$ est le point absolu, mais le problème réel est de développer les conséquences non triviales de ce point de vue.

Dans [...], la droite affine sur $\mathbb{F}_1$ a été considérée ; elle est constituée formellement de 0 et de toutes les racines de l'unité. Mis un peu différemment, cela amène à la considération des "extensions algébriques" de $\mathbb{F}_1$. Par analogie avec les corps finis authentiques, on aimerait penser qu'il y a exactement une telle extension de n'importe quel degré donné n, dénotons-la $\mathbb{F}_{1^n}$. Bien sûr, $\mathbb{F}_{1^n}$ n'existe pas dans un sens rigoureux, mais on peut penser que si un schéma X contient les racines n-ièmes de l'unité, alors il est défini sur $\mathbb{F}_{1^n}$, de telle façon qu'on a un morphisme

$$p_X : X \to \mathrm{Spec}(\mathbb{F}_{1^n}). \tag{1}$$

Le point de vue qu'adjoindre les racines de l'unité est analogue à l'extension d'un corps de base remonte au moins à Weil (Lettre à Artin, Œuvres, vol.1) et Iwasawa [...].

L'objectif de la "géométrie d'Arakelov modulo n" que nous proposons, est de donner du sens aux invariants cohomologiques obtenus via l'image directe du morphisme (1). L'un des plus intéressants parmi de tels invariants est le déterminant de la cohomologie, $\det(Rp_{X*}(\mathcal{F}))$ pour un faisceau cohérent $\mathcal{F}$ sur X. Dans le cas géométrique, le problème du calcul de ce déterminant, comme foncteur de $\mathcal{F}$, contient le problème de Riemann-Roch. Dans notre cas, les espaces vectoriels sur $\mathbb{F}_{1^n}$ sont les ensembles avec une action libre du groupe μ_n des racines n-ièmes de l'unité, et il est possible de développer le formalisme du déterminant (voir section 1 ci-dessous). Le problème correspondant de Riemann-Roch fait intervenir non pas des volumes, mais plutôt des résidus modulo n des nombres de points entiers dans certains polyèdres. Les analogues des images directes des classes de Chern (i.e. les torseurs de Deligne $\langle L, M\rangle$) font intervenir des symboles résiduels puissance n, et la bonne définition de notre formalisme de détermination entraîne une démonstration très naturelle de la loi de réciprocité pour ces symboles. En fait, certaines approches modernes de la loi de réciprocité, comme celle de Kubota [...], peuvent être vues comme traitant implicitement l'algèbre linéaire sur $\mathbb{F}_{1^n}$, en construisant des bases spéciales, etc. On utilise certaines idées de Kubota pour développer une théorie de "compactification d'Arakelov" des gerbes de vecteurs sur les courbes arithmétiques ; de façon similaire à la procédure standard, notre compactification fait intervenir certains domaines dans $M \otimes \mathbb{R}$, où M est un module sur l'anneau des entiers d'un corps de nombres, mais dans notre cas, les domaines sont de nature polyédrale et ils se comportent bien par rapport au comptage de points modulo n dans leurs dilatations.

On ne sait pas encore clairement comment formuler l'analogie correcte du théorème de Riemann-Roch ; ce qui est certain, c'est que cela devrait être une assertion reliant les résidus modulo n du nombre de points entiers dans un polyèdre avec des symboles résiduels de puissance n. Plusieurs assertions de cette sorte sont connues, à commencer par la démonstration géométrique de Gauss de la loi de réciprocité quadratique.

Détaillons maintenant le contenu de notre article plus avant. Dans la section 1 on discute avec quelques détails le formalisme des corps absolus (extensions algébriques de $\mathbb{F}_1$), algèbre linéaire sur de tels corps, théorie des déterminants et torseurs de détermination.

Dans la section 2 on développe les rudiments de l'algèbre homologique sur les corps absolus, qui nous sera nécessaire. En particulier, on étudie les analogues des séquences exactes. Tout ce formalisme est adapté pour considérer les invariants (comme la dimension) modulo n.

Dans la section 3 on définit les invariants cohomologiques des courbes arithmétiques qui sont, informellement, reliés aux faisceaux constructibles plutôt qu'aux faisceaux cohérents. Cela ne nécessite pas de compactification, mais cela nécessite de travailler avec des structures de niveau N. En particulier, on définit les "torseurs résultants" $\langle L, M\rangle$ pour les gerbes à deux droites avec structure de niveau. L'existence d'une bonne théorie de tels torseurs est équivalente à la loi de réciprocité dans la théorie des corps de classes. Nous traçons également avec quelques détails l'analogie entre la théorie des corps de classes et la théorie des nœuds et liens dans le 3-espace.

En section 4 on construit une théorie des "compactifications modulo n " des courbes arithmétiques. En particulier, on construit la cohomologie d'un faisceau (cohérent) sur la courbe compactifiée. Ce sont, bien sûr, des espaces vectoriels sur le corps absolu. Notre approche utilise, de façon cruciale, la notion de ce qu'on appelle le "domaine cohomologique", un certain concept technique dont le rôle est de nous assurer que la cohomologie, comme nous la définissons, se comporte de la façon attendue selon l'échange avec un faisceau très ample. Ceci est fait dans la section 5 dans un autre document.

1. Corps absolus.

1.1. Le "corps" $\mathbb{F}_1$.

Rappelons brièvement l'imagerie folklorique associée à $\mathbb{F}_1$, le corps (inexistant) à un élément.

Un espace vectoriel sur $\mathbb{F}_1$ est juste un ensemble ; la dimension d'un tel espace vectoriel est le cardinal de l'ensemble. Le groupe linéaire général $\mathrm{GL}_n(\mathbb{F}_1)$ est le groupe symétrique S_n. L'analogue du déterminant $\det : \mathrm{GL}_n(F) \to F^*$ pour $F = \mathbb{F}_1$ est l'homomorphisme signe $\mathrm{sgn} : S_n \to \{\pm 1\}$. Le groupe linéaire spécial $\mathrm{SL}_n(\mathbb{F}_1)$ est juste le groupe alterné A_n.

Par conséquent, l'algèbre linéaire sur $\mathbb{F}_1$ est la même que la combinatoire des ensembles (finis). Par exemple, si X est un tel ensemble, $|X| = n$, alors on devrait penser aux sous-ensembles à k éléments dans X comme à des sous-espaces vectoriels k-dimensionnels et à X comme à un $\mathbb{F}_1$-espace vectoriel. Leur nombre, $\binom{n}{k}$ est égal à la limite pour $q \to 1$ des cardinaux des $G(k,n)(\mathbb{F}_q)$, les variétés effectives de Grassmann sur les corps effectifs $\mathbb{F}_q$.

1.2 Anneaux de polynômes sur $\mathbb{F}_1$.

En plus du "corps" $\mathbb{F}_1$, on peut souhaiter avoir l'"anneau" de polynômes $\mathbb{F}_1[t]$. Bien qu'un tel anneau n'existe pas non plus, on peut dire quelque chose à propos des objets qui lui sont reliés.

Le groupe $\mathrm{GL}_d(\mathbb{F}_1[t])$ est le groupe de tresses complet B_d sur les d chaînes. On doit penser à l'homomorphisme canonique $f : B_d \to S_d$ comme à la limite lorsque $q \to 1$ des homomorphismes d'évaluation

$$\mathrm{GL}_d(\mathbb{F}_q[t]) \to \mathrm{GL}_d(\mathbb{F}_q), \quad A(t) \mapsto A(0).$$

Le sous-groupe $P_d = \mathrm{Ker}(\epsilon)$, appelé groupe de tresses pur, est ainsi l'analogue du sous-groupe de congruence $\mathrm{GL}_d(\mathbb{F}_q[t]), t)$.

Ce point de vue peut être justifié comme suit. Le groupe B_d est le groupe fondamental de l'espace $\mathbb{C}_0^d$ des polynômes complexes $x^d + a_1 x^{d-1} + ... + a_d$ sans racine multiple, et, de façon correspondante, le sous-groupe P_n est le groupe fondamental de l'espace

$$\mathbb{C}_*^d = \mathbb{C}^d - \bigcup_{i \neq j} \{(x_1, \ldots, x_d) \ : \ x_i = x_j\}.$$

Soit maintenant F un corps algébriquement clos contenant $\mathbb{F}_q$. Le groupe $\mathrm{GL}_d(\mathbb{F}_q)$ agit sur l'espace

$$F_*^d = F^d - \bigcup_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{F}_q^d-\{0\}} \Big\{(x_1,\ldots,x_d) \ : \ \sum \alpha_i x_i = 0\Big\},$$

et le quotient est identifié à l'espace des q-polynômes

$$x^{q^d} + a_1 x^{q^{d-1}} + \ldots + a_{d-1}x^q + a_d x, \quad a_d \neq 0.$$

Pour tout $N \in \mathbb{F}_q[t], N = \sum b_i t^i$, Drinfeld a construit un recouvrement non ramifié de $F_*^d/\mathrm{GL}_d(\mathbb{F}_q)$ avec le groupe de Galois $\mathrm{GL}_d(\mathbb{F}_q[t]/N)$. C'est l'espace des modules des $\mathbb{F}_q[t]$-modules elliptiques de rang d avec une structure de niveau N, voir [...]. Donc la complétion profinie de $\mathrm{GL}_d(\mathbb{F}_q[t])$ est plongée dans le groupe fondamental de l'espace des q-polynômes.

(1.3) Extensions algébriques de $\mathbb{F}_1$. Puisqu'on pense à $\mathbb{F}_1$ comme à un "corps", on aimerait considérer ses extensions finies. Il est naturel de penser, par analogie avec les véritables corps finis, que pour tout n on a une telle extension de degré n. Dénotons-la par $\mathbb{F}_{1^n}$. On pense à $\mathbb{F}_{1^n}$ comme contenant zéro et à μ_n, comme à l'ensemble de toutes les racines de l'unité d'ordre n. On peut, si on le souhaite, dire que $\mathbb{F}_{1^n}$ est le monoïde $\{0\} \cup \mu_n$.

De façon équivalente, on introduit la droite affine sur $\mathbb{F}_1$, qui est constituée de 0 et des racines de l'unité de tous les ordres. Ainsi comme un ensemble elle est identifiée à la "clôture algébrique" de $\mathbb{F}_1$. Aussi, la droite affine devrait être regardée comme le spectre de l'anneau inexistant $\mathbb{F}_1[t]$. Pour l'analogue de l'application d'évaluation à partir du groupe de tresses correspondant à un point de la droite affine, voir le §1.4 ci-dessous.

On regarde $\mathbb{F}_1$ comme le point absolu de la catégorie des schémas, de telle façon que tout schéma est défini sur $\mathbb{F}_1$. On dit qu'un schéma X est défini sur $\mathbb{F}_{1^n}$, si l'anneau des fonctions régulières sur X contient les racines n-ièmes de 1. Ceci est en accord avec la théorie d'Iwasawa [...] dans laquelle l'addition des racines de l'unité à un nombre remplace l'extension du corps de base pour une courbe.

(1.4) Algèbre linéaire sur $\mathbb{F}_{1^n}$. Étendons le formalisme de (1.1) aux extensions algébriques de $\mathbb{F}_{1^n}$. Un espace vectoriel sur $\mathbb{F}_{1^n}$ est un ensemble pointé $(V, 0 \in V)$ avec une action du groupe μ_n libre sur $V - \{0\}$. L'élément 0 est laissé fixe par l'action. Son ajout est vraiment optionnel ; il sert à ce que les constructions standards avec les espaces vectoriels sonnent d'une façon qui soit plus familière. Également, il est toujours présent dans les exemples naturels. Pour un espace vectoriel V sur $\mathbb{F}_{1^n}$, on dénote par $\widetilde{V}$ l'ensemble $V - \{0\}$.

Une application linéaire $V \to W$ est juste une application de μ_n-ensembles.

Une *base* d'un espace vectoriel V est, par définition, un sous-ensemble $B \in \widetilde{V}$ tel que tout μ_n-orbite contient un unique élément de B. La dimension de V est la cardinalité de n'importe quelle base, i.e. la cardinalité de $\widetilde{V}/\mu_n$.

Le groupe général linéaire $\mathrm{GL}_d(\mathbb{F}_{1^n})$ est le groupe des automorphismes d'un espace vectoriel de dimension d ; c'est juste le produit en couronne de S_d et $(\mu_n)^d$. On peut le voir comme le groupe

de matrices de taille d sur d qui contient exactement un élément non nul dans chaque ligne et dans chaque colonne, et cet élément est une racine de l'unité de μ_n. Étant donnée une racine de l'unité $\epsilon \in \mu_n$, on a l'"application d'évaluation"

$$f_\epsilon : B_d = \mathrm{GL}_d(\mathbb{F}_1[t]) \to \mathrm{GL}_d(\mathbb{F}_{1^n})$$

décrite comme suit. Rappelons que B_d est engendré par les éléments $\sigma_i, i = 1, \ldots, d-1$ avec les relations

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \quad \sigma_i\sigma_j = \sigma_j\sigma_i, \quad |i-j| \geq 2.$$

L'application f_ϵ est définie par la condition

$$f_\epsilon(\sigma_i) = 1_{i-1} \oplus 1_{n-i-1},$$

où l'on dénote par 1_i la matrice unité de taille i par i, et où $\oplus$ représente la somme directe de matrices (diagonales par blocs).

La catégorie des $\mathbb{F}_{1^n}$-espaces vectoriels est équipée des opérations de somme directe $V \vee W$ et de smash produit $V \wedge W$. Par définition, $V \vee W$ est obtenu à partir de l'union disjointe $V \amalg W$ en identifiant les éléments nuls, et $V \wedge W$ est obtenu à partir du produit cartésien $V \times W$ en identifiant $(V \times 0) \cup (0 \times W)$ avec 0. Ainsi, après avoir ignoré les éléments nuls, les opérations $\vee, \wedge$ correspondent à l'union disjointe et au produit cartésien de μ_n-ensembles libres.

On introduit également le produit tensoriel $V \otimes W$ comme le quotient de $V \wedge W$ par l'action antidiagonale de μ_n, i.e. par l'identification $x \wedge y = \epsilon x \wedge \epsilon^{-1} y$. Dénotons par $x \otimes y$ l'image de $x \wedge y$ dans $V \otimes W$ et équipons $V \otimes W$ avec la μ_n-action par la règle $\epsilon(x \otimes y) = (\epsilon x) \otimes y = x \otimes (\epsilon y)$. Il est clair que

$$\dim(V \vee W) = \dim(V) + \dim(W), \quad \dim(V \otimes W) = \dim(V) \times \dim(W).$$

(1.5) Déterminants. Soit V un espace vectoriel sur $\mathbb{Z}_1$, et $A : V \to V$ son automorphisme. Son déterminant $\det(A)$ est défini comme suit. Choisissons n'importe quelle base $e_1, ..., e_d$ de V, de telle façon que $A(e_i) = \alpha_i e_{\sigma(i)}$ pour une certaine permutation $\sigma \in S_d$ et certaines racines de l'unité $\alpha_i \in \mu_n$. Alors, par définition, $\det(A) = \prod \alpha_i$. On vérifie aisément l'égalité $\det(AB) = \det(A)\det(B)$ qui implique que $\det(A)$ est indépendante du choix de la base.

Notons l'absence de signe moins dans notre définition du déterminant. Nous donnerons une explication de cela ultérieurement. Maintenant fournissons deux exemples justifiant notre choix.

1.2.1. Proposition. *Proposition (1.6). Soit $n = 2$ et soit V un $\mathbb{F}_{1^2}$-espace vectoriel, alors V est un ensemble avec involution libre. Soit $d = \dim(V)$ et $A : V \to V$ un automorphisme. Alors $\det(A) \in \mu_2 = \{\pm 1\}$ coïncide avec le signe de la permutation $\widetilde{V} \to \widetilde{V}$ des $2d$ éléments de $\widetilde{V}$ donnés par A.*

(1.7) Symbole des résidus de puissance comme déterminant. Soit q une puissance de nombre premier et $\mathbb{F}_q$, un corps fini à q éléments. Supposons que $q \cong 1 \pmod{n}$. Alors $\mathbb{F}_q$ contient

les racines n-ièmes de 1, et on identifie μ_n avec le sous-groupe dans $\mathbb{F}_q^*$. Alors pour tout $a \in \mathbb{F}_q^*$ on a le symbole des résidus de puissance

$$\left(\frac{a}{\mathbb{F}_q}\right)_n = a^{\frac{q-1}{n}} \in \mu_n.$$

D'un autre côté, le plongement $\mu_n 1 \mathbb{F}_q^*$ fait de $\mathbb{F}_q$ un espace vectoriel sur $\mathbb{F}_{1^n}$ au sens défini ci-dessus. La multiplication par a est un automorphisme de cet espace. Le fait suivant est une version d'un lemme classique de Gauss.

1.2.2. Proposition. *Proposition (1.8). Le symbole résiduel de n-ième puissance* $\left(\frac{a}{\mathbb{F}_q}\right)_n$ *est égal au déterminant de la multiplication par a.*

On laisse la preuve au lecteur.

(1.9) Espaces de détermination et puissances extérieures. Soit A n'importe quel groupe abélien, avc une opération écrite multiplicativement. La catégorie des torseurs (espaces principaux homogènes) sur A a une structure naturelle de monoïde que l'on dénote $\otimes$. Explicitement, si T, S sont des A-torseurs, alors $T \otimes S$ est engendré par les symboles $t \otimes s$ avec $t \in T, s \in S$ vérifiant les relations $(at) \otimes s = t \otimes (as)$. L'opération $\otimes$ est trivialement commutative et associative au sens où nous avons des isomorphismes naturels. Quand A est le groupe multiplicatif d'un corps F, alors l'opération correspond au produit tensoriel de F-espaces vectoriels de dimension 1.

Soit maintenant V un espace vectoriel de dimension d sur $\mathbb{F}_{1^n}$. Alors $\widetilde{V}$ est l'union des μ_n-orbites, chacune étant un μ_n-torseur. On définit l'espace déterminant $\det(V)$ comme l'union de zéro et du $\otimes$-produit de tous ces torseurs:

$$\det(V) = \{0\} \cup \bigotimes_{T \in \widetilde{V}/\mu_n} T.$$

Il est clair que pour un automorphisme $f : V \to V$, son déterminant $\det(f)$ est juste l'application induite $\det(V) \to \det(V)$.

Notons, en particulier, que pour tout $\epsilon \in \mu_n$, la multiplication par ϵ définit un isomorphisme de $V \to V$, et son déterminant, qui est une application de $\det(V) \to \det(V)$, est la multiplication par $\epsilon^{\dim}(V)$. Ainsi det en tant que foncteur retrouve les dimensions des $\mathbb{F}_{1^n}$-espaces vectoriels pris modulo n. Ultérieurement, on considérera la dimension modulo n comme l'invariant de base d'un espace vectoriel (voir §2).

Plus généralement, pour tout $k \leq d$, on définit la k-ième puissance extérieure $\bigwedge^k V$ comme suit :

$$\bigwedge^k V = \{0\} \cup \amalg_{I 1 \widetilde{V}/\mu_n,\, |I|=k} \bigotimes_{T \in I} T.$$

Il est pratique de faire l'algèbre tensorielle d'une façon un peu plus systématique. Fixons l'action suivante du groupe symétrique S_k sur $V^{\otimes k}$:

$$\sigma(x_1 \otimes \ldots \otimes x_k) = x_{\sigma(1)} \otimes ... \otimes x_{\sigma(k)}$$

Alors $\bigwedge^k V$ s'obtient à partir du quotient $V^{\otimes k}/S_k$ en identifiant à 0 tout élément $x_1 \otimes ... \otimes x_k$ dans lequel certains des x_i, x_j sont proportionnels (avec un coefficient de proportionnalité étant dans μ_n). On dénote par $x_1 \wedge ... \wedge x_k$ l'image de $x_1 \otimes ... \otimes x_k$ dans $\bigwedge^k V$.

Une autre justification encore pour l'absence de signes dans notre théorie déterminante est donnée par le fait suivant :

1.2.3. Proposition. *Proposition (1.10). Soit q une puissance de nombre premier, $\mathbb{F}_q$ un corps à q éléments et $n = q - 1$. Identifions μ_n à $\mathbb{F}_q^*$. Soit V un espace $\mathbb{F}_q$-vectoriel quelconque. Alors le déterminant de V regardé comme un espace $\mathbb{F}_{1^n}$-vectoriel est identifié à la puissance extérieure supérieure standard de V regardé comme un espace $\mathbb{F}_q$-vectoriel (l'identification étant équivariante par rapport au groupe* $\mathrm{Aut}_{\mathbb{F}_q}(V)$*).*

En particulier, pour tout automorphisme $\mathbb{F}_q$-linéaire $f : V \to V$, les deux définitions possibles du déterminant de f coïncident.

Preuve. Au vu de notre définition du déterminant sur $\mathbb{F}_{1^n}$, notre assertion revient à une assertion d'algèbre $\mathbb{F}_q$-linéaire pure qui peut être énoncée comme l'existence d'un isomorphisme naturel

$$\det_{\mathbb{F}_q}(V) \to \bigotimes_{L \in P(V)} L, \tag{1.11}$$

où l'on a du côté droit le produit tensoriel (ordinaire) de tous les sous-espaces 1-dimensionnels $\mathbb{F}_q$-vectoriels dans V. $P(V)$ dénote la projectivisation de V.

Par définition, le côté droit de (1.11) est engendré par les éléments $x_\phi = \bigotimes_{L \in P(V)} \phi(L)$ pour toutes les sections ϕ de la projection naturelle $V - \{0\} \to P(V)$. Si ϕ, ψ sont deux tels éléments, alors on a

$$x_\psi = \left(\prod_{L \in P(V)} \frac{\psi(L)}{\phi(L)} \right) x_\phi.$$

D'un autre côté, l'espace $\det_{\mathbb{F}_q}(V)$ est étendu par les symboles $v_1 \wedge ... \wedge v_d$, pour toutes les bases $v_1, \ldots, v_d$ de V avec les relations standards d'antisymétrie et de multi-linéarité. On définit maintenant une application $\det_{\mathbb{F}_q}(V) \to det_{\mathbb{F}_{1^n}(V)}$ comme suit :

Soit $v_1, \ldots, v_d$ une base de V. Considérons le système suivant de représentants de la $\mathbb{F}_q^*$-action sur $V - \{0\}$: en d'autres termes, ceci est l'élévation naturelle vers $V - \{0\}$ de la décomposition cellulaire de $P(V)$ associée à la base $v_1, \ldots, v_d$.

1.2.4. Lemme. *Lemme (1.12). L'élément $x(v_1, \ldots, v_d) \in \otimes_{L \in P(V)} L$ donné par le produit tensoriel de l'ensemble des représentants qui vient d'être construit dépend de $v_1, \ldots, v_d$ d'une façon anti-symétrique et multilinéaire.*

Preuve. (a) Antisymétrie : Supposons qu'on échange v_i et v_{i+1}. Considérons d'abord pour simplifier le cas $i = 1$. Dénotons par P^l la projectivisation du $\mathbb{F}_q$-sous-espace dans V étendu par v_1, v_2. Les éléments $x(v_{,1} v_1, \ldots, v_d)$ et $x(v_2, v_1, \ldots, v_d)$ diffèrent d'un facteur qui est le produit sur tous les

$L \in P^1$ des ratios des représentants de la première et de la seconde famille vivant dans L. Si $L = \mathbb{F}_q v_1$ ou $\mathbb{F}_q v_2$, alors les représentants correspondant sont les mêmes. Si L est étendu par $v_1 + av_2$ avec $a \in \mathbb{F}_q^*$, alors le ratio des deux représentants est égal à a^{-1}. Par conséquent

$$\frac{x(v_1, v_2, \ldots, v_d)}{x(v_2, v_1, \ldots, v_d)} = \prod_{a \in \mathbb{F}_q^*} a^{-1} = -1.$$

Dans le cas où on échange v_i et v_{i+1}, avec $i > 1$, on a essentiellement le même dessin mais directement multiplié par $(\mathbb{F}_q)^{i-1}$. Donc, le ratio des deux éléments de det sera $(-1)^{q^{i-1}}$. Cette quantité est toujours égale à 1 dans le corps $\mathbb{F}_q$: si q est impair, alors on élève (-1) à une puissance impaire et on obtient (-1), alors que si q est pair, alors $(-1)^q = 1$.

(b) Multilinéarité : il suffit de démontrer que, premièrement, $x(v_1, ..., v_d)$ est inchangé par les transformations élémentaires, i.e. le remplacement de v_i par $v_i + \lambda v_j$ et, deuxièmement, la multiplication d'un des v_i par $\lambda \in \mathbb{F}_q$ multiplie $x(v_1, \ldots, v_d)$ par λ. Pour prouver la première assertion, il suffit, par anti-symétrie, de considérer le cas $i = 2, j = 1$. Mais pour deux bases différant par une telle transformation, les ensembles correspondant de représentants sont les mêmes. Pour démontrer la seconde assertion, il suffit de multiplier v_1 par λ. Mais $x(\lambda v_1, v_2, \ldots, v_d) = \lambda x(v_1, v_2, \ldots, v_d)$ par définition. Le lemme 1.12 et la proposition 1.10 sont démontrés.

2 Algèbre homologique sur les corps absolus.

Dans cette section, on fixe un entier n, on dénote μ_n, le groupe des racines n-ièmes de 1, simplement par μ et on écrit simplement F plutôt que $\mathbb{F}_{1^n}$.

La catégorie des F-espaces de dimension finie sera dénotée par $\mathcal{M}$. Cette catégorie est non-linéaire, de telle façon que le remplacement naturel de l'algèbre homologique devrait être la théorie des catégories de modèles fermés de Quillen [...]. Pourtant, il semble que $\mathcal{M}$ ne permet pas une structure de modèle fermé, et on définit seulement certains rudiments d'une telle structure.

(2.1) Cofibrations. Le rôle des cofibrations sera joué par les plongements des F-espaces. Si $f : V \hookrightarrow W$ est un tel plongement, on dénote par V/W le résultat de la contraction de W en 0. Occasionnellement, on traitera également les quotients des groupes abéliens (qui peuvent aussi être des F-espaces). Pour éviter la confusion, le quotient en théorie des groupes sera toujours dénoté par $\frac{W}{V}$.

Il est clair qu'on a un isomorphisme canonique

$$\det(V) \otimes \det(W/V) \to \det(W).$$

(2.2) Fibrations et équivalences. Soit $f : V \to W$ un morphisme d'espaces F-vectoriels. On dit que f est une fibration si pour chaque $w_1, w_2 \in W$ on a la congruence $|f^{-1}(w_1)| \equiv |f^{-1}(w_2)| \pmod{n}$.

On dit que f est une équivalence si $f^{-1}(0) = 0$ et pour tout $w \in W$ non nul, la cardinalité de $f^{-1}(w)$ est congrue à 1 modulo n. Par conséquent toute équivalence à notre sens est une fibration.

Clairement, si f est une équivalence, alors $\dim(V) \cong \dim(W) \pmod n$.

On dénote par $\mathcal{M}^*$ la sous-catégorie de $\mathcal{M}$ avec les mêmes objets que $\mathcal{M}$ et des morphismes qui sont des équivalences.

2.0.5. Proposition. *Proposition (2.3). Soit $f : V \to W$ une équivalence et $B = \{w_1, \ldots, w_d\}$ une base de W. Alors $f^{-1}(B)$ est une base de V. De plus, la règle*

$$w_1 \wedge ... \wedge w_d \mapsto \bigwedge_{v \in f^{-1}(B)} v$$

définit un isomorphisme de $\det(W) \to \det(V)$. *Cet isomorphisme est indépendant du choix d'une base B.*

On dénote par $\det(f) : \det(V) \to \det(W)$ l'isomorphisme inverse de celui construit dans la proposition 2.3.

Soit $\mathcal{P}$ la catégorie des espaces F-vectoriels 1-dimensionnels. Alors det est étendu vers un facteur covariant $\mathcal{M}^* \to \mathcal{P}$. Puisque tout morphisme dans $\mathcal{P}$ est un isomorphisme, cela montre que la catégorie obtenue à partir de $\mathcal{M}^*$ en inversant formellement tous les morphismes est non triviale.

2.0.6. Définition. *Définition (2.4). Une séquence d'espaces F-vectoriels et de leurs morphismes*

(2.4.1) $$S = \left\{0 \to V' \xrightarrow{\alpha} V \xrightarrow{\beta} V'' \to 0\right\}$$

est dite exacte, si α est une injection en théorie des ensembles, la composition $\beta\alpha$ est égale à 0, et l'application de $V/\alpha(V')$ vers V'' induite par β, est une équivalence.

Il est clair que pour toute séquence exacte, on a

$$\dim(V) \equiv \dim(V') + \dim(V'') \pmod n.$$

(2.5) Exemples. (a) Pour tout V, l'application $(V \times F)/(0 \times F) \to V$ est une équivalence.

(b) Soit q une puissance de nombre premier, et n un diviseur de $q-1$. Identifions $\mu = \mu_n$, avec le groupe des racines n-ièmes de l'unité à l'intérieur du corps fini $\mathbb{F}_q$. Alors tout espace $\mathbb{F}_q$-vectoriel devient un espace F-vectoriel, et toute séquence exacte courte d'espaces $\mathbb{F}_q$-vectoriels et d'opérateurs $\mathbb{F}_q$-linéaires est exacte au sens de la définition 2.3.

(2.6) Déterminants et séquences exactes. La catégorie $\mathcal{P}$ des espaces vectoriels 1-dimensionnels et de leurs isomorphismes est naturellement une catégorie de Picard, i.e. une catégorie monoïdale symétrique avec tout objet fonctoriellement inversible. L'opération sur $\mathcal{P}$ est donnée par le produit tensoriel $\otimes$ (qui correspond au produit $\odot$ sur les μ-torseurs).

Étant donnée une séquence exacte S comme dans (2.3.1), la fonctorialité de det sur les équivalences donne un isomorphisme

$$\lambda_S : \det(V') \otimes \det(V'') \to \det(V)$$

qui est naturel selon les équivalences des séquences exactes courtes.

(2.7) Complexes exacts. Soit

$$0 \to V^0 \stackrel{d_0}{\to} V^1 \stackrel{d_1}{\to} V^2 \stackrel{d_2}{\to} \dots \stackrel{d_{n-1}}{\to} V^n \to 0$$

une séquence d'espaces F-vectoriels et de leurs morphismes. Une telle séquence est appelée un complexe, si la composition $d_i \circ d_{i-1}$ est l'application zéro pour tout i. Une séquence est dite exacte si c'est un complexe et si pour tout i, la séquence

$$0 \to \mathrm{Im}(d_{i-1}) \hookrightarrow V^i \stackrel{d_i}{\to} \mathrm{Im}(d_i) \to 0$$

est exacte.

Pour tout F-espace valué $V^\bullet = (V^i, i \in \mathbb{Z})$, on définit

$$\det(V^\bullet) = \bigotimes \det(V^i)^{(-1)^i}.$$

En particulier, tout complexe donne un F-espace valué.

2.0.7. Proposition. *Proposition (2.8). Si $V^\bullet = (V^i, d_i)$ est un complexe exact, alors il y a une identification naturelle*

$$\mathrm{Eu} : \det(V^\bullet) \to \mu.$$

Cet isomorphisme dépend des applications dans le complexe. On dénote par $\langle V^\bullet \rangle \in \det(V^\bullet)$ l'image inverse de $1 \in \mu$ par l'isomorphisme Eu.

3. Théorie des corps de classes et structures de niveaux.

(3.1) Un point de vue 3-dimensionnels sur $\mathrm{Spec}(\mathbb{Z})$**.** Une partie considérable de la théorie des corps de classes peut être vue comme un analogue de la théorie des nœuds et des liens dans les 3-variétés.

Plus précisément, le spectre d'un corps fini $\mathbb{F}_q$ peut naturellement être visualisé comme un cercle, parce que, similairement au cercle, il a une couverture non ramifiée connectée $\mathrm{Spec}(\mathbb{F}_{q^m})$ pour tout $m \geq 1$. L'élément de Frobenius, générant $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ est représenté par la monodromie le long du cercle.

Soit maintenant K un corps de nombres, A son anneau d'entiers et $X = \mathrm{Spec}(A)$. Alors il est naturel de voir X comme une variété 3-dimensionnelle. Les spectres des corps résiduels premiers de A peuvent ainsi être vus comme des cercles à l'intérieur de cette 3-variété qui peut être nouée, reliée, etc. Ce point de vue a été défendu par Y. Manin et B. Mazur. Il est en accord avec le fait que la dimension cohomologique étale de X est égale à 3, voir [...].

(3.2) Symboles de Legendre et nombres de liaison. Rappelons une des définitions du nombre de liaison. Soit M une 3-variété compacte et C, D deux cercles plongés dans M et ne s'intersectant pas. Supposons que C est homologue à 0. Alors il existe un recouvrement de Galois connecté

$\widetilde{M} \to M$, de groupe de Galois $\mathbb{Z}$ ramifié le long de C. La monodromie le long de D dans ce recouvrement est par conséquent un entier (C, D) appelé nombre de liaison de C et D. Dans le cas où D est également homologue à 0, le nombre (D, C) est défini et on a

(3.2.1) $$(D, C) = (C, D)$$

Si C est homologue à 0 modulo n, on peut, en utilisant des $\mathbb{Z}/n$-recouvrements, définir l'indice d'intersection modulo n.

Une autre définition, plus standard de (C, D) est le nombre d'intersections $(\sigma \cdot D)$ où σ est une 2-chaîne bornant C.

Maintenant le symbole de Legendre de la réciprocité quadratique est l'analogue arithmétique du nombre de liaison mod 2. Notamment, prenons $X = \mathrm{Spec}(\mathbb{Z})$ et soit $p \in \mathbb{Z}$ un nombre premier de la forme $4k + 1$. Alors le schéma $\widetilde{X}$, le spectre de l'anneau des entiers de $\mathbb{Q}[\sqrt{p}]$, est un double recouvrement de X ramifié seulement en p. Si q est un autre nombre premier, alors le symbole de Legendre $\left(\frac{p}{q}\right)$ est l'élément de $\mathrm{Gal}(X/X) = \{\pm 1\}$ correspondant au Frobenius en q, i.e. correspondant dans notre visualisation à la monodromie le long du cercle $\mathrm{Spec}(\mathbb{F}_q)1X$. Ainsi $\left(\frac{p}{q}\right)$ peut être vu comme le nombre de liaison des "cercles" $\mathrm{Spec}(\mathbb{F}_p)$ et $\mathrm{Spec}(\mathbb{F}_q)$ dans la "3-variété" $\mathrm{Spec}(\mathbb{Z})$. Si à la fois p, q sont de la forme $4k + 1$, alors la loi de réciprocité de Gauss montre que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ qui est l'analogue de (3.2.1).

Si, cependant, $p = 4k + 3$, alors il n'y a pas de recouvrement de X ramifié seulement en p (en prenant $\sqrt{p}$ on obtient une ramification en p et en 2, alors qu'en prenant $\sqrt{-p}$ on obtient une ramification en p et en l'∞). Cela signifie que dans ce cas, $\mathrm{Spec}(\mathbb{F}_p)1\mathrm{Spec}(\mathbb{Z})$ devrait être regardé comme un cercle non homologue à 0. Donc avant d'aller plus loin, discutons de la manière dont la notion de nombre de liaison se généralise à de tels cercles.

(3.3) Torseurs de liaison. Soit M n'importe quelle 3-variété. Il est possible d'associer à n'importe quelles deux classes d'homologie $c, d \in H_1(M, \mathbb{Z})$ un certain $\mathbb{Z}$-torseur $\langle c, d\rangle$ ayant les propriétés suivantes :

1. Il y a des isomorphismes naturels

$$\langle c + c', d\rangle \simeq \langle c, d\rangle \otimes \langle c', d\rangle, \quad \langle c, d + d'\rangle \simeq \langle c, d\rangle \otimes \langle c, d'\rangle, \quad \langle d, c\rangle = \langle c, d\rangle.$$

   où $\otimes$ est la structure monoïdale naturelle sur la catégorie des $\mathbb{Z}$-torseurs.

2. Si $c = 0$, alors $\langle c, d\rangle$ est identifié canoniquement à $\mathbb{Z}$.

3. Pour n'importe quelles sous-variétés 1-dimensionnelles orientées ne s'intersectant pas $C, D1M$ de classes d'homologie c et d, il y a un élément défini naturellement $(C, D) \in \langle c, d\rangle$, et ces éléments satisfont les propriétés :

$$(C + C', D) = (C, D) + (C', D), \quad (C, D + D') = (C, D) + (C, D'), \quad (C, D) = -(D.C).$$

4. Si C, C' sont deux cercles de la même classe d'homologie c, et si D est un cercle de classe d'homologie d, alors on a égalité entre les entiers

$$(C, D) - (C', D) = (\sigma \cdot D),$$

où l'entier sur la gauche est la différence de deux éléments du $\mathbb{Z}$-torseur $\langle c, d\rangle$ et où σ est une 2-chaîne telle que $\partial\sigma = C - C'$.

En fait, on peut définir $\langle c, d\rangle$ comme étant engendrés par les symboles (C, D) avec $C \in c, D \in d$ qui vérifient les relations de (4).

(3.4) Théorie des corps de classes. Soit K un corps de nombres contenant μ_n, le groupe des racines n-ièmes de l'unité, A son anneau d'entiers, $X = \mathrm{Spec}(A)$. Ainsi, on peut voir X comme un schéma sur le corps absolu $\mathbb{F}_{1^n}$, voir §1.

La partie de la théorie des corps de classes pour F reliée aux extensions cycliques de degré n de F peut être reformulée d'une façon très similaire à (3.3).

Si N est un idéal de A, et L est un faisceau de droites sur X, on appelle structure de niveau N sur L une trivialisation de L modulo N plus le choix d'une direction (dite positive) dans la complétion L_v pour toute valuation réelle archimédienne v de K. (Puisqu'on suppose que K contient μ_n, les valuations réelles ne seront pas présentes si $n > 2$). Si f est une section rationnelle de L, on dit que $f \equiv 1 \pmod N$, si le diviseur de f est premier à N, l'image de f par l'application composée $L \to L/NL \to A/N$ est égale à 1, et l'image de f dans chaque L_v, où v est une valuation réelle, est positive (elle est dans la demi-droite distinguée).

3.0.8. Théorème. *Théorème (3.5). Il existe :*

1. *un idéal $N\mathtt{1}A$ s'étendant au-dessus de n.*
2. *une règle qui associe à deux fibrés en droites L, M sur X à structure de niveau N un torseur $\langle L, M\rangle$.*
3. *une règle qui associe à toutes les sections $l \in L, m \in M$ qui sont premières à 1 et congrues à 1 modulo N un élément $(l, m)_n \in \mu_n$ avec les propriétés suivantes :*
4. *Il y a des isomorphismes naturels*

$$\langle L \otimes L', M \simeq \langle L, M\rangle \otimes \langle L', M\rangle, \quad \langle L, M \otimes M'\rangle \simeq \langle L, M\rangle \otimes \langle L, M'\rangle, \quad \langle M, L\rangle = \langle L, M\rangle,$$

5. *Si $L = \mathcal{O}_X$ de structure de niveau N triviale, alors $\langle L, M\rangle$ est identifié canoniquement à μ_n.*
6. *On a les égalités $(l \otimes l', m)_n = (l, m)_n(l', m)_n$, and $(L, m \otimes m')_n = (l, m)_n(l, m')_n$.*
7. *(loi de réciprocité) : on a $(l, m)_n = (m, l)_n$.*

8. *Si f est un élément de A congru à 1 modulo N, alors pour tout M et toute section $m \in M, m \equiv 1 \pmod{N}$ première à f, alors l'élément $(f, m) \in (\mathcal{O}_X, M) \simeq \mu_n$ est égal au produit de symboles résiduels de puissances*

$$\prod_{v \in X} \left(\frac{f}{\mathbb{F}_v}\right)_n^{\mathrm{ord}_v(m)},$$

3.0.9. Corollaire. *Corollaire (3.6). Si $f, g \in A$ sont deux éléments premiers l'un à l'autre congrus à 1 modulo N, alors*

$$\prod_v \left(\frac{f}{\mathbb{F}_v}\right)_n^{\mathrm{ord}_v(g)} = \prod_v \left(\frac{g}{\mathbb{F}_v}\right)_n^{\mathrm{ord}_v(g)}$$

Ceci est la loi de réciprocité dans sa forme classique. Elle peut être utilisée pour retrouver la structure complète donnée par le théorème 3.5.

(3.7) Fibrés en droites avec structure de niveau. On conserve la notation de §3.4. On dénote par $\widetilde{\mathrm{Pic}}(X)$ le groupe de fibrés en droites L sur X avec structure de niveau N. On dénote par $K^*(N)$ les groupes multiplicatifs de $f \in K$ qui sont totalement positifs, premiers à N et congrus à 1 modulo N. Dans le théorème 3.5, on est libre de faire grandir N. Dans la suite, on fera toujours les suppositions suivantes sur N :

3.0.10. Remarque. *Supposition (3.8). Pour tout $f \in K^*(N)$ on a la congruence*

$$\mathrm{Norm}_{K/\mathbb{Q}}(f) \equiv 1 \pmod{n^2}.$$

Cela sera vrai, par exemple, si N est divisible par (la remontée dans A de) n^2.

Soit $\mathrm{Div}(X, N)$ le groupe des diviseurs sur X premiers à N. Alors, clairement,

$$\widetilde{\mathrm{Pic}}(X) = \mathrm{Div}(X, N)/\{\mathrm{div}(f), f \in K^*(N)\}$$

Aussi loin que modulo n les phénomènes soient concernés, les fibrés en droites (et en vecteurs) sur X à structure de niveau N se comportent comme des fibrés sur une courbe compacte, même si X lui-même n'est en aucun sens compactifié. Par exemple, le μ_n-torseur $\langle L, M \rangle$ a la signification de l'image directe

$$\int_{X/\mathrm{Spec}(\mathbb{F}_{1^n})} c_1(L) c_1(M),$$

cf. [Deligne].

De plus, de tels fibrés en droites ont une notion de degré qui prend des valeurs dans $\mathbb{Z}/n$. Il est défini comme suit. Utilisons le langage des sections 1 et 2, en particulier, utilisons l'algèbre linéaire sur le corps absolu $F = \mathbb{F}_{1^n}$. Pour un idéal $D1A$ premier à N on pose

$$\deg_n(D) = \dim_F(A/D) \pmod{n}.$$

3.0.11. Proposition. *Proposition (3.9). (a) Pour deux idéaux $D_1, D_2 1A$ premiers à N on a* $\deg_{\mathrm{n}}(\mathrm{D_1 D_2}) \equiv \deg_{\mathrm{n}}(\mathrm{D_1}) + \deg_{\mathrm{n}}(\mathrm{D_2}) \pmod{\mathrm{n}}$.

(b) Si $f \in A \cap K^*(N)$*, alors* $\deg_n(\mathrm{div}(f)) \equiv 0 \pmod n$.

Preuve. (a) Soit $\Delta_i = \mathrm{Norm}_{K/\mathbb{Q}}(D_i)$. Alors Δ_i est un idéal dans $\mathbb{Z}$; soit d_i son générateur positif. Clairement $|A/D_i| = |\mathbb{Z}/\Delta_i| = d_i$. Donc $\deg_n(D_i) \equiv (d_i - 1)/n \pmod n$, et $\deg_n(D_1 + D_2) \equiv (d_1 d_2 - 1)/n \pmod n$. Notre assertion revient à la congruence

$$\frac{d_1 d_2 - 1}{n} \equiv \frac{d_1 - 1}{n} + \frac{d_2 - 1}{n} \pmod n.$$

On peut réécrire cela en

$$(d_1 - 1)(d_2 - 1) \equiv 1 \pmod{n^2},$$

qui est vrai du fait de la supposition 3.8.

(b) Appelons, comme précédemment, d le générateur positif de $\mathrm{Norm}_{K/\mathbb{Q}}(f)$. Alors $d \equiv 1 \pmod{n^2}$ par la supposition 3.8 et, d'un autre côté, $\deg_n(\mathrm{div}(f)) \equiv (d-1)/n \pmod n$.

3.0.12. Corollaire. *Corollaire (3.10). L'application* $\deg_n$ *s'étend à un homomorphisme bien défini*

$$\deg_n \ : \ \widetilde{Pic}(X) \to \mathbb{Z}/n.$$

Preuve. Tout élément de $K^*(N)$ est le ratio de deux éléments de $A \cap K^*(N)$.

4. Courbes arithmétiques compactifiées.

Comme dans les sections précédentes, dénotons par K un corps de nombres contenant le groupe $\mu = \mu_n$ des racines n-ièmes de l'unité, par A son anneau d'entiers et par X le spectre de A. On choisit également un idéal N dans A comme dans la section 3.

Bien que les fibrés en droites sur X avec structure de niveau N aient un degré modulo n et aient également les torseurs $\langle L, M\rangle$, ils n'ont pas d'espaces de dimension finie de sections globales ou bien de cohomologie. Dans la situation géométrique, pourtant, une étape importante est la comparaison de $\langle L, M\rangle$ avec le déterminant de la cohomologie. De ce fait, on introduit des objets pour lesquels de tels déterminants ont du sens.

(4.1) Domaines fondamentaux. Nous allons faire quelques constructions polyédrales dans l'espace vectoriel réel $K_{\mathbb{R}} = K \otimes \mathbb{R}$. En fait, tensoriser par $\mathbb{R}$ n'est pas vraiment nécessaire, mais cela aide à la visualisation.

Fixons quelques éléments de terminologie reliés aux sous-ensembles de tout espace vectoriel réel V. On appellera polytope (convexe) toute fermeture convexe d'un ensemble fini de points (donc, en particulier, c'est un sous-ensemble fermé de V). Un polytope P a des *faces*, qui sont des sous-polytopes (fermés) dans P. Par *domaine polyédral* on désigne un sous-ensemble dans V de la forme $P - Q$ où P est un polytope et où Q est l'union des intérieurs de certaines faces de P.

L'anneau A est un réseau dans $K_{\mathbb{R}}$, comme l'est également tout A-sous-module projectif de rang 1 dans K, par exemple, tout idéal fractionnaire.

Si Λ est un tel sous-module, on appellera *polytope fondamental* pour Λ un polytope convexe $P \in K_{\mathbb{R}}$ avec la propriété suivante : pour n'importe quels deux $\alpha, \beta \in \Lambda$, leur intersection translatée $(P+\alpha) \cap (P+\beta)$ est une face qui leur est commune. Bien sûr, un choix évident d'un polytope fondamental pourrait être le "cube" du réseau, mais on aura besoin d'autres choix (voir ci-dessous).

Un *ensemble de représentants* pour Λ est un domaine polyédral $B \in K_{\mathbb{R}}$ tel que la projection composée $B \hookrightarrow K_{\mathbb{R}} \to K_{\mathbb{R}}/\Lambda$ est une bijection.

Par exemple, quand $K = \mathbb{Q}$, alors $[0,1]$ est un polytope fondamental pour $\Lambda = \mathbb{Z}$, alors que $[0,1)$ est un ensemble de représentants.

(4.2) Définition. Soit $B \mathtt{1} K_{\mathbb{R}}$ un sous-ensemble μ-invariant contenant 0. On dit que B est un domaine contrôlé, s'il existe des sous-ensembles $B_f, B_c \mathtt{1} B$ et un idéal fractionnaire $\Lambda \mathtt{1} K$ avec les propriétés suivantes :

1. On a $B = B_f \cup B_c$ et $B_f \cap B_c = \varnothing$.
2. L'ensemble B_f est un ensemble de représentants pour Λ.
3. Pour tout $x \in B_c \cap K$ l'idéal $(x : \Lambda) = \{\alpha \in A | \alpha x \in \Lambda\}$ est divisible par tout idéal premier dans A qui divise n.

(4.3) Exemple. Dans le cas où $K = \mathbb{Q}$ l'intervalle $[-1,1]$ est un domaine contrôlé. En effet, on peut prendre $B_f = [-1,1)$ le demi-intervalle ouvert, $B_c = \{1\}$ et $\Lambda = 2\mathbb{Z}$.

En général, un domaine contrôlé peut être vu comme un remplacement de cet intervalle. Le fait suivant sera prouvé dans la prochaine section.

4.0.13. Théorème. *Théorème (4.4). Si n est une puissance de nombre premier, $n = p^t$ et K est un corps de nombres contenant μ_n, alors il existe un domaine contrôlé dans $K_{\mathbb{R}}$.*

4.0.14. Définition. *Définition (4.5). Une courbe compacte sur $\mathbb{F}_{1^n}$ est une paire $\overline{X} = (X, B)$, où $X = \mathrm{Spec} A$ avec A l'anneau des entiers d'un corps de nombres K contenant μ_n et $B \mathtt{1} K_{\mathbb{R}}$ est un domaine contrôlé tel que $\mu_n \mathtt{1} B$.*

Dans la suite de cette section, on suppose que X et B sont choisis.

4.0.15. Définition. *Définition (4.6). Un fibré en droites sur $\overline{X}$ est une paire $L = (M_L, B_L)$ où M_L est un A-module projectif de rang 1 et $B_L \mathtt{1} M_L \otimes \mathbb{R}$ est un sous-ensemble qui est K-linéairement isomorphe à $B \mathtt{1} K_{\mathbb{R}}$.*

On dénote par $H^0(\overline{X}, L) = M_L \cap B_L$. C'est un espace vectoriel sur $F = \mathbb{F}_{1^n}$. Pour tout diviseur D sur X, on dénote par $\mathcal{O}(D) \mathtt{1} K$ l'idéal fractionnaire correspondant et on dénote par $L(D)$ la paire formée par $M_L(D) = M_L \otimes \mathcal{O}(D)$ et le même ensemble B_L. On dénotera par $\mathcal{O}_{\overline{X}}$ ou simplement $\mathcal{O}$ la paire (A, B).

Supposons que D est positif, i.e. $\mathcal{O}(D)$ est un idéal dans A. Alors $M_L\mathtt{1}M_L(D)$ et le quotient peuvent être vu comme un faisceau gratte-ciel sur X avec support sur le support de D. On dénote ce faisceau par $L(D)|_D$, et on pense au groupe quotient $M_L(D)/M_L$ comme à l'espace des sections globales (sur X ou $\overline{X}$) de ce faisceau. Ainsi on a une séquence

$$0 \to H^0(\overline{X}, L) \to H^0(\overline{X}, L(D)) \to H^0(X, L(D)|_D) \to 0 \tag{4.7}$$

Quand D est premier à n, les ensembles dans cette séquence sont des espaces F-vectoriels où $F = \mathbb{F}_{1^n}$.

4.0.16. Définition. *Définition (4.8). Un fibré en droites L sur $\overline{X}$ est dit acyclique (ou est dit ne pas avoir de cohomologie plus haute) si pour tout diviseur positif D dans A, la séquence (4.7) est exacte au sens de la section 2.*

4.0.17. Théorème. *Théorème (4.9). Pour tout fibré en droites L sur $\overline{X}$, il y a un diviseur positif D premier à n tel que pour tout diviseur $D' \geq D$ premier à n, le fibré en droites $L(D)$ est acyclique.*

Preuve.

4.0.18. Corollaire. *Corollaire (4.10). (Riemann-Roch modulo n). Il existe un nombre $g = g(\overline{X}) \in \mathbb{Z}/n$ tel que pour $D \gg 0$ on ait*

$$\dim H^0(\overline{X}, \mathcal{O}(D)) = \deg_n(D) + 1 - g \pmod{n}.$$

Ici le nombre $\deg_n(D)$ a été défini dans la section 3.

(2.7) Colimites d'homotopie. Puisqu'on a défini seulement les rudiments d'une structure de modèle fermé, on peut définir les limites et les colimites seulement dans des cas particuliers. Voici la situation que nous utiliserons.

Soit I une catégorie finie et $\Phi : I \to \mathcal{M}$ un foncteur, i.e. un diagramme de F-espaces de type I. Supposons que tous les morphismes $\Phi(\alpha), \alpha \in \mathrm{Mor}(I)$ soient des plongements. Un système constitué d'un objet $C \in M$ et de morphismes $\beta_i : \Phi(i) \to C$ est appelé une colimite d'homotopie de Φ, si :

1. $\beta(i)\Phi(\alpha) = \beta_j$ pour tout $\alpha : j \to i$ dans I.
2. Le morphisme naturel $\mathrm{colim}_I \Phi \to C$ existant par la propriété (1) est une équivalence.

(2.8) Exemples. (a) Une séquence (2.4.1) est exacte si et seulement si V'' est une colimite homotopique du diagramme ;

(b) Carrés exacts (cocartésiens homotopiques). Un carré commutatif sera dit exact, ou cocartésien homotopique, si les applications dans le diagramme sont des plongements et si V_{11} est une limite homotopique de ce diagramme.

De façon similaire, on définit les cubes exacts de dimension arbitraire d. Par définition, un tel foncteur est un diagramme commutatif constitué de f-espaces V_S où S parcourt les sous-ensembles

dans $\{1,...,d\}$, et il y a une application $V_S \to V_T$ quand $S1T$. Un cube est dit exact si dans le sous-diagramme formé par les $V_S, S \neq \{1,...,d\}$ toutes les applications sont des plongements et si $V_{\{1,...,d\}}$ est une limite homotopique de ce diagramme.

4.0.19. Proposition. *Proposition (2.9). Si (V_s) est un cube d-dimensionnel exact, alors on a l'isomorphisme naturel*

$$\bigotimes \det(V_S)^{(-1)^{|S|}} \simeq \mu.$$

(4.2) Exemple : le corps cyclotomique. Soit $n = p^t$ où p est un nombre premier, et soit $K = \mathbb{Q}(\sqrt[n]{1})$ le n-ième corps cyclotomique. Soit $A = \mathbb{Z}[\sqrt[n]{1}]$ son anneau d'entiers. Le seul idéal dans A étendu sous p est $\Lambda = (1-\zeta)$ où ζ est n'importe quelle racine primitive de 1. Considérons l'ensemble

$$P = \left\{ \sum_{\epsilon \in \mu_n} a_\epsilon \epsilon \right\}, \quad a_\epsilon \in [0,1].$$

Ceci est clairement un polytope, puisque c'est l'image du cube $[0,1]^{\mu_n}$ sous la projection naturelle sur $K_{\mathbb{R}}$.

4.0.20. Proposition. *Proposition (4.2.1). P est un polytope fondamental pour Λ.*

Preuve. Fixons une racine primitive $\zeta \in \mu_n$. Une $\mathbb{R}$-base de $K_{\mathbb{R}}$ et une $\mathbb{Z}$-base de A est fournie par les puissances ζ^i, où $1 \leq i \leq n$ et $(i,n) = 1$. Par conséquent le cube

$$Q = \left\{ \sum_{(i,n)=1} a_i \zeta^i \right\}, \quad a_i \in [0,1]$$

est un polytope fondamental pour A. Maintenant P est l'union de n cubes ayant subi une rotation de $\zeta^j Q$ où $0 \leq j \leq n-1$, et l'intersection de n'importe quelle paire de deux tels cubes est leur face commune. Cela peut être vérifié d'une façon triviale.