JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

E.-U. GEKELER

Sur la géométrie de certaines algèbres de quaternions

Journal de Théorie des Nombres de Bordeaux, tome 2, n° 1 (1990), p. 143-153

<http://www.numdam.org/item?id=JTNB_1990__2_1_143_0>

Séminaire de Théorie des Nombres,
Bordeaux **2** *(1990), 143-153*

Sur la géométrie de certaines algèbres de quaternions.

par E.-U. GEKELER

1 - Introduction. Soit K un corps global (i.e. un corps de nombres ou un corps de fonctions d'une variable sur un corps fini), et S un ensemble non vide de places de K contenant les places archimédiennes. $A = A_S$ désignera toujours l'anneau des S-entiers de K. Soit D une algèbre de quaternions sur K [9]. Nous appellerons brèvement *ordre* dans D tout A-ordre maximal B dans D. Les faits suivants sont bien connus :

(1.1) Le nombre de classes d'idéaux à gauche de B est fini et ne dépend que de D et S, mais non du choix de B ; S étant fixé, on l'appelle $h(D)$.

(1.2) Soit $\mathfrak{b}$ un idéal à gauche de B et $B_d(\mathfrak{b}) = \{f \in D | \mathfrak{b}f \subset \mathfrak{b}\}$. Alors, $B_d(\mathfrak{b})$ est un ordre (*l'ordre à droite de* $\mathfrak{b}$), i.e. maximal. A conjugaison près, chaque ordre intervient de telle manière.

(1.3) Le nombre $t(D)$ de *types* de D (=classes de conjugaison d'ordres) est fini et inférieur ou égal à $h(D)$.

Le problème fondamental de l'arithmétique de D est donc de décrire les ensembles finis de classes d'idéaux de B et de types de D.

Dans un cas assez spécial (voir sect. 2), on a une belle interprétation de ces ensembles, reliant l'arithmétique dans D à la théorie des courbes elliptiques [4]. Nous donnerons une interprétation similaire de certaines algèbres sur les corps de fonctions, où les modules de Drinfeld remplacent les courbes elliptiques.

Supposons maintenant que K soit un corps global de fonctions sur le corps de constantes $\mathbf{F}_q$ à q éléments, et que S consiste en une seule place "∞" de degré d_∞ sur $\mathbf{F}_q$. Soit $\mathfrak{p}$ une place de K différente de ∞, de degré d, et $D = D(\mathfrak{p})$ l'algèbre de quaternions sur K qui se ramifie en $\mathfrak{p}$ et ∞. Ecrivons la fonction zêta de K dans la forme

$$\zeta_K(S) = \frac{P(q^{-s})}{(1-q^s)(1-q^{1-s})} \tag{1.4}$$

avec un polynôme à coefficients entiers. On sait que le cardinal $h = \#(\mathrm{Pic}\ A)$ du groupe de classes $\mathrm{Pic}\ A$ de A est donné par

$$h = d_\infty . P(1) . \tag{1.5}$$

Notre interprétation de D impliquera le

Manuscrit reçu le 23 novembre 1989

THÉORÈME 1. *Soit B un ordre dans D.*

(i) Pour chaque idéal à gauche $\mathfrak{b}$ de B, l'ordre $B_d(\mathfrak{b})$ a un groupe d'unités isomorphe au groupe multiplicatif de $\mathbf{F}_q$ ou de son extension quadratique $\mathbf{F}_{q^2}$. Soient $h_1(D)$, $h_2(D)$ les nombres de classes correspondants de B (qui ne dépendent pas du choix de B).

(ii) Si d ou d_∞ est pair, on a

$$h_1(D) = d_\infty.P(1).P(q).Q \quad \text{et} \quad h_2(D) = 0.$$

Si d et d_∞ sont impairs, on a

$$h_1(D) = d_\infty.P(1)\,[P(q).Q - P(-1)/(q+1)] \text{ et } h_2(D) = d_\infty.P(1).P(-1).$$

Ici, on a posé

$$Q = \frac{(q^d-1)(q^{d_\infty}-1)}{(q-1)(q^2-1)}.$$

(iii) Dans chaque cas, on a la formule de masse

$$\sum w(\mathfrak{b})^{-1} = d_\infty.P(1).P(q).Q,$$

où la somme porte sur un système de représentants des classes d'idéaux à gauche de B, et $w(\mathfrak{b}) = \#(B_d^*(\mathfrak{b}) : A^*)$.

(1.6) *Remarque.* Evidemment, (iii) est une conséquence triviale de (i) et (ii). Le point essentiel c'est que le terme à droite de (iii) a une signification universelle. Il est égal à $h(A).\zeta_{S^*}(-1)$, où ζ_{S^*} est la fonction zêta de K, privée des facteurs d'Euler qui correspondent aux places dans $S^* = \{\mathfrak{p}, \infty\}$.

2. Courbes elliptiques supersingulières.

Pour motiver ce qui suit, nous rappelons la relation (aujourd'hui bien connue) entre algèbres de quaternions sur $\mathbf{Q}$ et courbes elliptiques en caractéristique positive.

Soit E une courbe elliptique (= variété abélienne de dimension un) définie sur la clôture algébrique $\overline{\mathbf{F}}_p$ du corps fini $\mathbf{F}_p$, où p est un nombre premier. Nous supposons E supersingulière, i.e. elle ne possède aucun point de p-torsion non nul. D'ailleurs, soit $D = D(p)$ l'algèbre de quaternions qui se ramifie à p et à la place archimédienne. D'après Deuring et Eichler [4], on sait que

(2.1) L'anneau $B = \mathrm{End}(E)$ des endomorphismes de E est (isomorphe à) un $\mathbf{Z}$-ordre maximal dans D (i.e. un "ordre", si l'on pose $S = \{\infty\}, A = \mathbf{Z}$).

(2.2) Soit $\mathfrak{b}$ un idéal à gauche de B et $H(\mathfrak{b}) \subset E$ le schéma en groupes fini $\cap \operatorname{Ker}(b)$, où b parcourt $\mathfrak{b}$. Le quotient $E(\mathfrak{b}) = E/H(\mathfrak{b})$ est une courbe elliptique supersingulière et $\mathfrak{b} \mapsto E(\mathfrak{b})$ définit une bijection entre l'ensemble des classes d'idéaux à gauche de B et l'ensemble $\sum(p)$ des classes d'isomorphisme de courbes elliptiques supersingulières sur $\overline{\mathbf{F}}_p$.

(2.3) $B_d(\mathfrak{b})$ est isomorphe à $\operatorname{End}(E(\mathfrak{b}))$.

(2.4) $B_d(\mathfrak{b})$ et $B_d(\mathfrak{b}')$ sont isomorphes si et seulement si $E(\mathfrak{b})$ $E(\mathfrak{b}')$ définissent des classes dans $\sum(p)$ qui sont conjuguées sous le groupe de Galois $Gal(\overline{\mathbf{F}}_p : \mathbf{F}_p)$.

(2.5) *Remarque.* D'après le théorème de Skolem-Noether, deux ordres isomorphes sont en fait conjugués dans D. De plus, les éléments de $\sum(p)$ sont définis sur l'extension quadratique $\mathbf{F}_q$ de $\mathbf{F}_p, q = p^2$. Donc (2.4) dit que les types de D correspondent aux orbites de $\sum(p)$ sous l'action de $Gal(\mathbf{F}_q : \mathbf{F}_p)$.

Considérons maintenant le schéma modulaire "de Hecke" $M_0(p)$ [3]. C'est un schéma normal sur $\mathbf{Z}$ qui paramétrise les courbes elliptiques munies d'un sous-schéma en groupes fini de degré p. On a $M_0(p)(\mathbf{C}) = \Gamma_0(p)\backslash H$ avec le demi-plan H de Poincaré et le groupe $\Gamma_0(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbf{Z}) | c \equiv 0(p)\}$, qui opère sur H. La fibre spéciale $M_0(p) \times \overline{\mathbf{F}}_p$ a une jolie description : c'est une courbe avec deux composantes irréductibles, toutes deux isomorphes à la j-droite affine (j = l'invariant modulaire des coubes elliptiques), et qui se coupent transversalement aux points supersinguliers. En particulier, le genre arithmétique p_a de $\overline{M}_0(p) \times \overline{\mathbf{F}}_p$ (où $\overline{M}_0(p)$ est la compactification naturelle de $M_0(p)$) se calcule comme

$$p_a = \#(\text{points doubles}) - 1 = h(D) - 1. \tag{2.6}$$

De l'autre côté, p_a est égale au genre de la surface de Riemann $\overline{M}_0(p)(\mathbf{C})$, qui est facilement calculé à l'aide de la formule de Hurwitz. Il en résulte des formules explicites pour $h(D(p)) = \#(\Sigma(p))$ et pour $t(D(p))$, voir e.g. [1]. De plus, on a la formule de masse

$$\sum w(\mathfrak{b})^{-1} = (p - 1/12 = \zeta_{S^*}(-1), \tag{2.7}$$

où $\mathfrak{b}$ parcourt l'ensemble des classes d'idéaux à gauche de

$$B = \operatorname{End}(E),\ w(\mathfrak{b}) = \#(B_d(\mathfrak{b})^* : \mathbf{Z}^*) = \#(\operatorname{Aut}(E(\mathfrak{b})) : \{\pm 1\})$$

et $S^* = \{p, \infty\}$.

3. Modules de Drinfeld.

Nous allons donner une interprétation géométrique analogue pour certaines algèbres de quaternions sur les corps de fonctions. A partir de maintenant, nous supposons que K soit un corps global de fonctions avec comme corps de constantes le corps F_q (q puissance d'un nombre premier p), et que S consiste d'une seule place "∞" de K. Soit $|?| = |?|_\infty$ la valeur absolue normalisée correspondante, donnée sur un élément non nul de A par $|a| = \#(A/a)$. Dans ce contexte, Drinfeld [5] a introduit la notion des modules elliptiques, que nous appellerons des modules de Drinfeld. Ceux-ci sont des objets diophantiens qui ressemblent beaucoup aux courbes elliptiques. Soit L un corps muni d'une structure $\gamma : A \to L$ de A-algèbre, et τ l'endomorphisme $x \mapsto x^q$ du schéma en groupes additif $G_a|L$. Rappelons que l'anneau des endomorphismes $\mathrm{End}_L(G_a)$ de $G_a|L$ est l'anneau des polynômes additifs $\sum a_i X^{p^i}$ à coefficients dans L, où la "multiplication" est définie par insertion des polynômes. Soit $L\{\tau\} \subset \mathrm{End}_L(G_a)$ la sous-algèbre engendrée par τ. C'est un "anneau de polynômes non-commutatif" avec la règle de commutation $\tau a = a^q \tau$ si $a \in L$. Au "polynôme" $\sum a_i \tau^i$ correspond l'opérateur $x \mapsto \sum a_i x^{q^i}$ sur $G_a|L$. Un *A-module de Drinfeld* de rang r sur L est une structure de A-module sur $G_a|L$, donnée par un homomorphisme d'anneaux

$$\begin{aligned} \Phi : A &\to L\{\tau\}, \\ a &\mapsto \Phi_a = \sum a_i \tau^i \end{aligned}$$

tel que pour chaque a non nul, les deux conditions sont satisfaites ;

(3.1) (i) $a_0 = \gamma(a)$, (ii) le degré du polynôme additif correspondant $\sum a_i X^{q^i}$ est égal à $|a|^r$.

(3.2)*Exemple.* Si $K = \mathbf{F}_q(T)$ et ∞ est la place à l'infini usuelle, A est l'anneau $\mathbf{F}_q[T]$ des polynômes en T. Un module de Drinfeld de rang r est donné par $\Phi_T = \sum a_i \tau^i$, où $a_0 = \gamma(T)$ et $a_r \neq 0$.

Un *morphisme* $u : \Phi \to \Psi$ de modules de Drinfeld (défini sur L) est un élément u de $\mathrm{End}_L(G_a)$ tel que $u \circ \Phi_a = \Psi_a \circ u, a \in A$. Donc l'anneau $\mathrm{End}(\Phi) = \mathrm{End}_L(\Phi)$ des L-endomorphismes de Φ est le centralisateur de $\Phi(A)$ dans $\mathrm{End}_L(G_a)$ (en fait, dans $L\{\tau\}$). Pour a non nul, le sous-schéma en A-modules ${}_a\Phi = \mathrm{Ker}(\Phi_a)$ de $G_a|L$ est fini de degré $|a|^r$. C'est le schéma des *points de a-torsion* de Φ. Ecrivons $\mathrm{car}_A(L) = \infty$, si γ est injectif, et $\mathrm{Ker}(\gamma)$ dans le cas contraire. Si de plus, a est premier à $\mathrm{car}_A(L)$, ${}_a\Phi$

est réduit, et ses points ${}_a\Phi(\overline{L})$ sur la clôture algébrique de L forment un A-module abstrait qui est libre de dimension r sur A/a. Tout ce qu'on vient d'expliquer se généralise au schéma ${}_a\Phi$ des *points de* $\mathfrak{a}$*-torsion* de Φ, où $\mathfrak{a}$ est un idéal non nécessairement principal de A. On utilise ces faits à définir des structures de niveau sur les modules de Drinfeld, puis à construire des schémas de modules, ce qui est tout à fait analogue aux constructions similaires dans la théorie des courbes elliptiques. (Voir [5] et [2] pour les détails).

4. Relation avec les ordres.

Dans ce qui suit, on écrit "module de Drinfeld", ou "module de D." pour "module de Drinfeld de rang deux". Nous fixons un idéal maximal $\mathfrak{p}$ de A, de degré d et d'ordre m dans le groupe de classes Pic A de A. Nous écrivons $\mathbf{F}_\mathfrak{p} = A/\mathfrak{p}$, et plus généralement $\mathbf{F}_\mathfrak{p}^{(i)}$ pour l'extension de degré i de $\mathbf{F}_\mathfrak{p}$. Un module de D. Φ sur une extension L de $\mathbf{F}_\mathfrak{p}$ est dit *supersingulier* si le schéma des points de $\mathfrak{p}$-torsion ${}_\mathfrak{p}\Phi$ est local, ou ce qui est équivalent, si ${}_f\Phi(\overline{L}) = 0$ pour un f dont le diviseur est une puissance de $\mathfrak{p}$.

(4.1) *Remarque.* D'après [8], Cor. 5.2, $\mathbf{F}_\mathfrak{p}^{(m)}$ est l'extension minimale de $\mathbf{F}_\mathfrak{p}$ sur laquelle existent des modules de D. Chaque module supersingulier peut être défini sur $\mathbf{F}_\mathfrak{p}^{(2m)}$ (loc. cit. Prop. 4.2).

Soit $D = D(\mathfrak{p})$ l'algèbre de quaternions sur K qui se ramifie à $\mathfrak{p}$ et ∞. Le théorème suivant (comparer aux assertions (2.1) - (2.4) !) est un cas spécial du Thm. 4.3 de [8].

THÉORÈME 2. *Soit Φ un module de Drinfeld supersingulier (de rang 2) sur la clôture algébrique $\overline{\mathbf{F}}_\mathfrak{p}$ de $\mathbf{F}_\mathfrak{p}$.*

(i) L'anneau des endomorphismes $B = End(\Phi)$ est isomorphe à un A-ordre maximal dans $D(\mathfrak{p})$.

(ii) Il existe une bijection canonique $(\mathfrak{b}) \mapsto (\Phi^\mathfrak{b})$ de l'ensemble des classes d'idéaux à gauche de B sur l'ensemble $\sum(\mathfrak{p})$ des classes d'isomorphisme des modules de D. supersinguliers sur $\overline{\mathbf{F}}_\mathfrak{p}$.

(iii) L'ordre à droite $B_d(\mathfrak{b})$ de $\mathfrak{b}$ dans $B \otimes K = D$ est isomorphe à $End(\Phi^\mathfrak{b})$.

(iv) Supposons que Pic A soit engendré par la classe de $\mathfrak{p}$. Alors, $B_d(\mathfrak{b})$ et $B_d(\mathfrak{b}')$ sont isomorphes si et seulement si $\Phi^\mathfrak{b}$ et $\Phi^{\mathfrak{b}'}$ définissent des classes dans $\sum(\mathfrak{p})$ qui sont conjuguées sous $Gal(\overline{F}_\mathfrak{p} : \mathbf{F}_\mathfrak{p})$.

Donc il nous reste à décrire l'ensemble $\sum(\mathfrak{p})$ sur un schéma de modules convenable.

5. Schémas de modules.

Considérons le schéma grossier de modules "de type Hecke" $M_0(\mathfrak{p})$. Il paramétrise les classes d'isomorphisme des paires (Φ, U), où Φ est un module de $D.$ de rang 2, et U un sous-schéma en A-modules de ${}_{\mathfrak{p}}\Phi$ qui est fini de degré q^d. (Dans la terminologie de [7], I, §3, $M_0(\mathfrak{p})$ est le schéma $M^2_{\mathfrak{K}}$, où $\mathfrak{K}$ est le sous-groupe de congruence de Hecke $\mathfrak{K} = \mathfrak{K}_0(\mathfrak{p}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \hat{A}) | c \equiv 0(\mathfrak{p})\}$.) D'ailleurs, soit $M(1)$ le schéma grossier pour les modules de rang 2 sans structure de niveau, et $\overline{M}_0(\mathfrak{p}), M(1)$ les compactifications canoniques ([5], sect. 9). Ce sont des schémas projectifs sur Spec A, obtenus en compactifiant $M_0(\mathfrak{p}), M(1)$ fibre par fibre sur Spec A. Alors,

(5.1) - $\overline{M}_0(\mathfrak{p}), \overline{M}(1)$ sont des schémas normaux, irréductibles, de type fini sur Spec A, et $M_0(\mathfrak{p}) \subset \overline{M}_0(\mathfrak{p}), M(1) \subset \overline{M}(1)$ sont partout denses ;

- le morphisme canonique $\overline{M}_0(\mathfrak{p}) \to \overline{M}(1)$ est plat et fini de degré $q^d + 1$;

- le morphisme structural $\overline{M}(1) \to$ Spec A est lisse de dimension un (voir [5], 5.4 et 9.3).

En comparant notre situation avec celle de la section 2, il y a une importante différence, qui résulte de l'existence d'idéaux non-principaux dans A. Soit $h = \#(\text{Pic } A)$ le nombre de classes de A, et posons H pour le *corps de classes de Hilbert* de (K, ∞), c'est-à-dire l'extension maximale abélienne non-ramifiée de K qui se décompose complètement à l'infini. L'application d'Artin identifie Pic A à Gal$(H : K)$, et l'idéal $\mathfrak{p}$ se décompose dans l'anneau A_H des A-entiers de H en s idéaux différents, où $s = h/m$. Contrairement à la section 2, $K = \text{Fract}(A)$ n'est pas algébriquement clos dans le corps de fonctions de $\overline{M}(1)$ (resp. $\overline{M}_0(\mathfrak{p})$.) Plus précisément, il résulte de [7], II, §4 que :

(5.2) Le normalisé de Spec A dans ces deux schémas est isomorphe à Spec(A_H).

Dans le langage traditionnel des variétés, on dirait que "la courbe algébrique $\overline{M}(1)$ est définie sur H", de même pour $\overline{M}_0(\mathfrak{p})$.

6. La fibre spéciale.

Les arguments de cette section sont essentiellement ceux de [6], eux mêmes inspirés par [3], où on peut trouver plus de détails.

Notons $X(1), \overline{X}(1), X_0(\mathfrak{p}), \overline{X}_0(\mathfrak{p})$ les produits fibrés sur A avec $\overline{\mathbf{F}}_{\mathfrak{p}}$ de

$M(1), \overline{M}(1), M_0(\mathfrak{p}), \overline{M}_0(\mathfrak{p})$; $X(1)$ et $X_0(\mathfrak{p})$ paramétrisent les modules de Drinfeld Φ, (muni d'un sous-A-module U de degré q^d de ${}_{\mathfrak{p}}\Phi$ dans le dernier cas) sur $\overline{\mathbf{F}}_{\mathfrak{p}}$.

Soit $F = \tau^d$ le morphisme de Frobenius qui correspond à $\mathbf{F}_{\mathfrak{p}}$. Avoir donné Φ, on a $F : \Phi \to \Phi^F$ où Φ^F est le module Φ tordu par F (i.e., le module obtenu en appliquant l'élément correspondant de $\mathrm{Gal}(\overline{\mathbf{F}}_{\mathfrak{p}} : \mathbf{F}_{\mathfrak{p}})$ aux coefficients de Φ). Le noyau $\mathrm{Ker}(F)$ de F, qui est strictement local, est contenu dans ${}_{\mathfrak{p}}\Phi$, donc il existe une section canonique (en fait, une immersion fermée)

$$i : X(1) \to X_0(\mathfrak{p}) \tag{6.1}$$

de la projection

$$\pi : X_0(\mathfrak{p}) \to X(1),$$

qui sur les objets des problèmes de modules est donnée par $\Phi \mapsto (\Phi, \mathrm{Ker}(F))$. Cette application est bijective sur les objets supersinguliers, car pour de tels Φ, il n'existe qu'un seul sous-A-module

U d'ordre q^d dans ${}_{\mathfrak{p}}\Phi$. Nous avons encore besoin de l'application

$$w : X_0(\mathfrak{p}) \to X_0(\mathfrak{p})$$

définie par $(\Phi, U) \mapsto (\Phi/U, {}_{\mathfrak{p}}\Phi/U)$. Ici, Φ/U est le module Ψ, but d'un morphisme $u : \Phi \to \Psi$ à noyau U, qui est déterminé à isomorphisme près, et ${}_{\mathfrak{p}}\Phi/U$ l'image de ${}_{\mathfrak{p}}\Phi$ sous u. (En général, w n'est pas une involution, mais on a toujours $w^{2m} = id.$). Finalement, nous écrivons

$$F_{X(1)} : X(1) \to X(1)$$

pour l'endomorphisme donné par $\Phi \mapsto \Phi^F$. On a

$$\pi \circ i = id_{X(1)} \text{ et } \pi \circ w \circ i = F_{X(1)}. \tag{6.2}$$

Si Φ n'est pas supersingulier, U est soit réduit, soit local, donc $\mathrm{im}(i) \cup \mathrm{im}(w \circ i) = X_0(\mathfrak{p})$ et $\mathrm{im}(i) \cap \mathrm{im}(w \circ i)$ consiste en des modules supersinguliers. Cela entraîne (comparer avec [3], V, §1 et VI, §6) :

(6.3) $X_0(\mathfrak{p})$ est l'union de deux copies de $X(1)$, qui se coupent transversalement aux points supersinguliers.

(La transversalité vient du fait évident que $F_{X(1)}$ est purement inséparable.) On recolle le point supersingulier Φ de la deuxième copie au point Φ^F de la première.

Parce que $\overline{M}(1) \times_A \mathbf{F}_\mathfrak{p} = \amalg \overline{M}(1) \times_{A_H} \mathbf{F}_{\mathfrak{q}_i}$ est lisse sur $\mathbf{F}_\mathfrak{p}$, $\overline{X}(1) = \overline{M}(1) \times \overline{\mathbf{F}}_\mathfrak{p}$ est l'union disjointe de $h = s.m$ courbes algébriques, lisses, connexes et projectives. Vu que les composantes sont permutées par
Pic $A = \mathrm{Gal}(H : K)$, il est évident que chacune contient des points supersinguliers. Le genre commun de ces courbes est

$$g(1) = \mathrm{genre}(\overline{M}(1) \times_{A_H} H). \tag{6.4}$$

Il existe des extensions uniques $\overline{\pi}, \overline{i}, \overline{w}, F_{\overline{X}(1)}$ aux compactifications $\overline{X}(1), \overline{X}_0(\mathfrak{p})$ des morphismes $\pi, i, w, F_{X(1)}$, et les relations (6.2) restent valables. Donc $\overline{X}_0(\mathfrak{p})$ est l'union de deux copies de $\overline{X}(1)$. On dérive de la propriété modulaire de $\overline{M}_0(\mathfrak{p})$ ([5], sect. 9) que $\overline{i}(\overline{X}(1) \setminus X(1))$ et $\overline{w} \circ \overline{i}(\overline{X}(1) \setminus X(1))$ sont disjoints. Cela entraîne que les composantes connexes de $\overline{X}_0(\mathfrak{p})$ sont de la forme $X \cup Y$, où $X = F_{\overline{X}(1)}(Y)$ et Y sont des composantes de $\overline{X}(1)$ recollées en les points supersinguliers comme cela est décrit plus haut. Le genre arithmétique se calcule par

$$p_a(\overline{X}_0(\mathfrak{p})) = \sum_Y (2g(1) + \sigma_Y - 1) = h(2g(1) - 1) + \sigma, \tag{6.5}$$

où la somme porte sur les composantes Y de $\overline{X}(1)$, σ_Y est le nombre de points supersinguliers sur Y (en fait, tous les σ_Y sont égaux), et $\sigma = \sum \sigma_Y = h(D(\mathfrak{p}))$. En tenant compte du fait

$$p_a\overline{X}_0(\mathfrak{p})) = h.g_0(\mathfrak{p}) = h.\mathrm{genre}(\overline{M}_0(\mathfrak{p}) \times_{A_H} H), \tag{6.6}$$

on obtient

$$h(D(\mathfrak{p})) = h(g_0(\mathfrak{p})) - 2g(1) + 1) \tag{6.7}$$

Les nombres $g(1)$ et $g_0(\mathfrak{p})$ sont calculés dans [7], VI 5.8 et VII 5.13 à l'aide des formes modulaires. Nous renonçons à écrire les formules compliquées ; ils fournissent le résultat

$$h(D(\mathfrak{p})) = d_\infty.P(1)[Q.P(q) + \eta] \tag{6.8}$$

avec $\eta = 0$ si d ou d_∞ est pair, $\eta = (q/(q+1))\,P(-1)$ si d et d_∞ sont impairs, et Q comme dans l'énoncé du théorème 1.

7. Points elliptiques.

Un point géométrique de $M(1)$ est dit *elliptique* s'il correspond à un module de Drinfeld Φ ayant un groupe d'automorphismes strictement plus grand que $\mathbf{F}_q^*$. Dans ce cas, $\mathrm{Aut}(\Phi)$ est le groupe multiplicatif de l'extension quadratique de $\mathbf{F}_q$. Cette remarque triviale, combinée avec le théorème 2 (iii) montre déjà (i) du théorème 1.

Posons $A' = A \otimes \mathbf{F}_{q^2}$ et $K' = \mathrm{Fract}(A')$, et supposons d'abord que d_∞ soit *pair* . Si le module de $D.\Phi : A \to L\{\tau\}$ satisferait à $\mathrm{Aut}(\Phi) \cong \mathbf{F}_{q^2}^*$, l'homomorphisme Φ aurait une extension à A'. Mais ceci est absurde parce que, grâce à l'hypothèse, A' a un groupe d'unités infini. Donc, si d_∞ est pair, il n'existe aucun point elliptique, et nous pouvons supposer dans tout ce qui suit que d_∞ soit *impair*. Alors, la place ∞ est inerte dans K', et l'on peut regarder les A- modules de Drinfeld de rang 2 avec $\mathrm{Aut}(\Phi) \simeq \mathbf{F}_{q^2}^*$ comme des A'-modules de rang 1 et vice-versa. Ceci définit un morphisme

$$\varepsilon : M^1_{A'}(1) \to M^2(1) = M(1)$$

dont l'image consiste en des points elliptiques. Ici, $M^1_{A'}(1)$ est le schéma de modules des A'-modules de $D.$ de rang 1 "sans niveau". Grâce à [5], Thm. 1, il est égal au spectre de $A'_{H'} = A'$-entiers dans le corps de classes de Hilbert H' de K'. La conjugaison de $\mathbf{F}_{q^2}$ sur $\mathbf{F}_q$ induit une involution β de $M^1_{A'}(1)$, vu comme A-schéma. Soit $\pi : M^1_{A'}(1) \to \mathrm{Spec}(A_\beta)$ le morphisme quotient, où $A_\beta \subset A'_{H'}$ est le sous-anneau des β- invariants. Alors ε se factorise en $\varepsilon = \tilde{\varepsilon} \circ \pi$, et $\tilde{\varepsilon} : \mathrm{Spec}(A_\beta) \to M^2(1)$ est une immersion fermée ([7], VII, §2). Vu que A_β est fini, plat et non ramifié sur A, l'image de $\tilde{\varepsilon}$ contient

$$h' = [A_\beta : A] = [A'_{H'} : A'] = \#(\mathrm{Pic}A')$$

points géométriques au-dessus de chaque $\mathfrak{p} \in \mathrm{Spec}\ A$ (i.e. points elliptiques sur $\overline{\mathbf{F}}_\mathfrak{p}$). Il est facile de voir que h' est donné par $d_\infty.P(1).P(-1)$, donc :

(7.1) PROPOSITION : *Si d_∞ est impair (pair), il existe $d_\infty.P(1).P(-1)$ (resp. nuls) points elliptiques dans $M(1) \times \overline{\mathbf{F}}_\mathfrak{p}$.*

Il reste à voir combien de points elliptiques sont supersinguliers. La réponse est

(7.2) LEMME : *Supposons d_∞ impair. Un point elliptique de $M(1) \times \overline{\mathbf{F}}_\mathfrak{p}$ est supersingulier si et seulement si $d = deg\ \mathfrak{p}$ est impair.*

DÉMONTRATION : Soient $\mathfrak{q}$ (*resp.*$\mathfrak{q}_1, \mathfrak{q}_2$) les diviseurs dans A' de $\mathfrak{p}$, si d est impair (resp. pair). Si $\mathrm{Aut}(\Phi) \cong \mathbf{F}_{q^2}^*$, Φ se prolonge en $\Phi' : A' \to$

$\overline{\mathbf{F}}_q\{\tau\}$ (resp. en $\Phi' : A' \to \overline{\mathbf{F}}_{q_1}\{\tau\} = \overline{\mathbf{F}}_p\{\tau\}$). En tous cas, Φ' est un A'-module de D. de rang 1. Si d est impair, ${}_p\Phi = {}_q\Phi'$ est local, donc Φ est supersingulier. Si d est pair, on a pour les centralisateurs dans $\overline{\mathbf{F}}_p\{\tau\}$:

$$\mathrm{Cent}(\Phi(A)) = \mathrm{Cent}(\Phi'(A')) = \Phi'(A') \cong A',$$

ce qui est un A-module projectif de rang deux, et Φ n'est pas supersingulier.

En combinant (7.1), (7.2) avec le théorème 2 et (6.8), on arrive à (ii) du théorème 1.

8. Exemples.

(8.1) Considérons le cas de l'exemple 3.2 où $K = \mathbf{F}_q(T)$ et $A = \mathbf{F}_q[T]$. Alors $P(X) = 1$. On a

$$h_1 = (q^d - 1)/(q^2 - 1) \quad \text{et } h_2 = 0, \text{ si } d \text{ est pair, et}$$
$$h_1 = (q^d - q)/(q^2 - 1) \quad \text{et } h_2 = 1, \text{ si } d \text{ est impair.}$$

Le nombre $t(D(\mathfrak{p}))$ de types de $D(\mathfrak{p})$ peut aussi être calculé à l'aide des nombres de classes des extensions quadratiques de K ([8] 4.7).

(8.2) Soit encore K un corps de fonctions rationnelles, mais "∞" de degré 2, e.g. le corps de fonctions de la courbe

$$Y^2 = aX^2 + bX + c,$$

où $p > 2$, a n'est pas carré dans $\mathbf{F}_q$, et $b^2 - 4ac \neq 0$. Alors $h_1(D(\mathfrak{p})) = 2(q^d - 1)/(q - 1)$ et $h_2(D(\mathfrak{p})) = 0$. Si $d = 1$, les deux classes de modules supersinguliers sur $\overline{\mathbf{F}}_p$ sont définies sur l'extension quadratique $\mathbf{F}_p^{(2)}$ de $\mathbf{F}_p$ et conjuguées, ce qui résulte de (4.1). Donc par le théorème 2, $t(D(\mathfrak{p})) = 1$.

(8.3) Soit K de genre 1 et "∞" une place de degré 1. Le polynôme $P(X)$ prend la forme $qX^2 - tX + 1$ avec $|t| \leq 2q^{1/2}$. On a

$h_1 = P(1)\ P(q)\ q^d - 1)/(q^2 - 1)$ et $h_2 = 0$, si d est pair, et

$h_1 = P(1)\ P(q)\ (q^d - 1)/(q^2 - 1) - P(1)\ P(-1)/(q+1)$ et $h_2 = (q+1)^2 - t^2$, si d est impair.

Le nombre h_1 se simplifie à $(q - t + 1)(q^2 - q - t)$ pour $d = 1$.

BIBLIOGRAPHIE

[1] A. BRUMER, *Courbes modulaires.* Grenoble, (1975).

[2] P. DELIGNE, D. HUSEMÖLLER, *Survey of Drinfeld modules*, Contemp. Mat. **67** (1987), 25–91.

[3] P. DELIGNE, M. RAPOPORT, *Les schémas de modules de courbes elliptiques*, Lecture Notes in Mathematics **349**. Springer-Verlag, (1973).

[4] M. DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Hamb. **14** (1941), 197–272.

[5] V.G. DRINFELD, *Elliptic modules*, Math. USSR-Sbornik **23** (1976), 561–592.

[6] E.-U. GEKELER, *Über Drinfeld'sche Modulkurven vom Hecke-Typ*, Comp. Math. **57** (1986), 219–236.

[7] E.-U. GEKELER, *Drinfeld modular curves*, Lecture Notes in Mathematics **1231**. Springer-Verlag, (1986).

[8] E.-U. GEKELER, *On finite Drinfeld modules*, J. Algebra. à paraître.

[9] M.-F. VIGNÉRAS, *Arithmétique des Algèbres de Quaternions*, Lecture notes in Mathematics **800**. Springer-Verlag, (1980).

Institut des Hautes Etudes Scientifiques
35, route de Chartres
91440 - Bures-sur-Yvette (FRANCE)