C. R. Acad. Sci. Paris, Ser. I 335 (2002) 867–870

Théorie des nombres/*Number Theory*

La conjecture d'André–Oort pour le produit de deux courbes modulaires de Drinfeld

Florian Breuer

Institut de mathématiques de Jussieu, 175, rue Chevaleret, 75013 Paris, France

Reçu le 27 avril 2002 ; accepté après révision le 14 octobre 2002

Note présentée par Jean-Pierre Serre.

Résumé Nous démontrons un analogue de la conjecture d'André–Oort pour le produit de deux courbes modulaires de Drinfeld, suivant l'approche de S.J. Edixhoven. ***Pour citer cet article : F. Breuer, C. R. Acad. Sci. Paris, Ser. I 335 (2002) 867–870.***

The André–Oort conjecture for the product of two Drinfeld modular curves

Abstract We prove an analogue of the André–Oort conjecture for the product of two Drinfeld modular curves, following S.J. Edixhoven's approach. ***To cite this article: F. Breuer, C. R. Acad. Sci. Paris, Ser. I 335 (2002) 867–870.***

Fixons les notations suivantes. Soient q une puissance d'un nombre premier impair p, $\mathbb{F}_q$ le corps fini à q éléments, $A=\mathbb{F}_q[T]$ l'anneau des polynômes dans une variable sur $\mathbb{F}_q$, $k=\mathbb{F}_q(T)$ le corps de fonctions rationnelles sur $\mathbb{F}_q$, ∞ la place de k engendrée par $(1/T)$, $k_\infty=\mathbb{F}_q((1/T))$ le complété de k à ∞, $\mathbf{C}=\hat{\bar{k}}_\infty$ le complété de la clôture algébrique de k_∞ et $\Omega=\mathbb{P}^1(\mathbf{C})-\mathbb{P}^1(k_\infty)$ le *demi-plan de Drinfeld*. La place ∞ définit une valeur absolue sur k, k_∞ et $\mathbf{C}$, qu'on note $|\cdot|$.

Par un module de Drinfeld (voir [7] et [9] pour les notions de base) on entend toujours un A-module de Drinfeld de rang 2 défini sur $\mathbf{C}$. L'invariant-j donne une bijection entre les points (x_1,x_2) du plan affine $\mathbb{A}^2(\mathbf{C})$ et les classes d'isomorphie de couples (ϕ_1,ϕ_2) de modules de Drinfeld, où $x_1=j(\phi_1)$ et $x_2=j(\phi_2)$. On dit que (x_1,x_2) est un *point CM* si ϕ_1 et ϕ_2 sont à multiplication complexe.

Soit $N\in A$. On note par $Y_0(N)$ la courbe modulaire paramétrisant les couples (ϕ_1,ϕ_2,f) de modules de Drinfeld liés par une isogénie $f:\phi_1\to\phi_2$ *cyclique de degré N* (c'est-à-dire, $\ker(f)$ est isomorphe à A/NA comme A-module). On envoie $Y_0(N)$ dans $\mathbb{A}^2$ par l'application $(\phi_1,\phi_2,f)\mapsto(j(\phi_1),j(\phi_2))$. L'image, qu'on note $Y_0'(N)$, est une courbe algébrique absolument irréductible et définie sur k.

Dans cet article nous allons esquisser la démonstration du théorème suivant.

THÉORÈME 1. – *Soient d_1, d_2 et m des entiers positifs donnés et g un entier non-négatif donné. Alors il existe une constante effectivement calculable $B=B(d_1,d_2,m,g)$ vérifiant la propriété suivante. Soit Y une courbe algébrique absolument irréductible de bidegré (d_1,d_2) dans $\mathbb{A}^2_{\mathbf{C}}$ définie sur une extension finie F de k de degré m et de genre $g_F=g$. Alors Y est une courbe modulaire $Y_0'(N)$ pour un certain $N\in A$ si et seulement si $Y(\mathbf{C})$ contient un point CM de hauteur supérieure à B.*

On suppose $p\neq 2$ pour des raisons techniques, mais le Théorème 1 reste probablement vrai pour $p=2$.

Adresse e-mail : flo@math.jussieu.fr (F. Breuer).

S1631-073X(02)02589-X/FLA

Comme les structures de niveau ne jouent aucun rôle, on peut remplacer $\mathbb{A}^2$ par un produit $X_1 \times X_2$, où X_i est une *courbe modulaire de Drinfeld*, c'est-à-dire le quotient de Ω par un sous-groupe d'indice fini de $\mathrm{GL}_2(A)$. Les courbes modulaires $Y_0'(N)$ seront alors remplacées par les correspondances de Hecke T_N. On remarque que, comme dans [2], on peut facilement étendre le Théorème 1 au cas des courbes dans $\mathbb{A}^n$.

C'est une version pour la caractéristique p d'un cas spécial de la conjecture d'André–Oort. Ce cas a été démontré, en caractéristique 0, par André [1]. Avant, Edixhoven [4] avait trouvé une autre démonstration, sous l'hypothèse de Riemann généralisée, qui permet de traiter des cas plus généraux (voir par exemple [5]), et qui est effective. Nous tâchons essentiellement de traduire son approche en caractéristique p. Notons que l'hypothèse de Riemann généralisée est vraie dans ce cas.

1. Partie arithmétique : démonstration du Théorème 1

Soit $x \in \mathbf{C}$. Alors x correspond à un module de Drinfeld ϕ avec $x = j(\phi)$. Dans la suite, on parlera souvent de x au lieu de ϕ (e.g. on parlera des isogénies entre points de $\mathbf{C}$). Tout comme dans [2] on définit la *hauteur CM* de x par $H_{CM}(x) := |\operatorname{Discr}(\operatorname{End}(x))|$, c'est donc la valeur absolue du discriminant de l'anneau d'endomorphismes du module de Drinfeld ϕ correspondant à x. Pour $(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbf{C})$ on définit $H_{CM}(x_1, \ldots, x_n) = \max_{1 \leqslant i \leqslant n} H_{CM}(x_i)$. La hauteur CM définit bien une fonction de comptage sur les points CM dans $\mathbb{A}^2(\mathbf{C})$, en fait on a $\#\{x \in \mathbf{C} \mid x \text{ est CM et } H_{CM}(x) \leqslant B\} = \mathrm{O}(B^{3/2+\varepsilon})$ pour tout $\varepsilon > 0$. Utilisant une majoration de la fonction j des points CM en termes du discriminant de l'anneau d'endomorphismes [3] on peut comparer, comme dans [2], la hauteur CM et la hauteur arithmétique usuelle. On obtient ainsi $h(x) \leqslant H_{CM}(x)^{1/2} + \sqrt{q}(q+1)/2$. Il suffit donc de montrer le Théorème 1 pour la hauteur CM.

Soit $n \in A$ sans facteurs carrés. On définit *la correspondance de Hecke* T_n sur $\mathbb{A}^2$ comme l'image de l'application $Y_0'(n) \times Y_0'(n) \to \mathbb{A}^2 \times \mathbb{A}^2$, $((x_1, x_2), (y_1, y_2)) \mapsto ((x_1, y_1), (x_2, y_2))$. On peut aussi voir T_n comme une application des sous-ensembles de $\mathbb{A}^2$ vers les sous-ensembles de $\mathbb{A}^2$ engendrée par $T_n\{(x_1, x_2)\} = \{(y_1, y_2) \mid \text{il existe des isogénies cycliques } x_1 \to y_1 \text{ et } x_2 \to y_2 \text{ de degré } n\}$.

Notre résultat repose sur la caractérisation suivante des courbes $Y_0'(N)$, qu'on démontrera plus bas.

THÉORÈME 2. – *Soit Y une courbe algébrique absolument irréductible de bidegré (d_1, d_2) dans $\mathbb{A}^2_{\mathbf{C}}$, avec $d_1 d_2 \neq 0$. Soit $n \in A$ un produit des polynômes irréductibles distincts $\mathfrak{p} \in A$ avec $|\mathfrak{p}| \geqslant \max(d_1, 13)$ et $\deg(\mathfrak{p})$ pair. Si $Y \subset T_n(Y)$, alors Y est une courbe modulaire $Y_0'(N)$ pour un certain $N \in A$.*

Supposons d'abord que l'extension F/k soit galoisienne. Soit maintenant $(x_1, x_2) \in Y(\mathbf{C})$ un point CM. Alors $\mathcal{O}_i = \operatorname{End}(x_i)$ est un ordre de conducteur $f_i \in A$ dans une extension quadratique « imaginaire » K_i de k (i.e. telle que K_i ne se plonge pas dans k_∞) pour $i = 1, 2$. Notons $K = K_1 K_2$ et $M = K(x_1, x_2)$. Soit $\mathfrak{p}$ un premier de degré pair dans k qui se décompose totalement dans FK et ne divise pas $f_1 f_2$. Soit $\mathfrak{P}$ un premier de FM au-dessus de $\mathfrak{p}$, et notons par $\mathfrak{P}_i$ ses restrictions aux corps $K_i(x_i)$.

Par la théorie de la multiplication complexe pour les modules de Drinfeld (qui est similaire à celle des courbes elliptiques, voir par exemple [6]), on sait que ces extensions de corps sont galoisiennes, que $\operatorname{Gal}(K_i(x_i)/K_i) \cong \operatorname{Pic}(\mathcal{O}_i)$ et que $\mathfrak{P}/\mathfrak{p}$ est non-ramifié. Soit $\sigma = (\mathfrak{P}, FM/k)$ le Frobenius, et $\sigma_i = (\mathfrak{P}_i, K_i(x_i)/k) = \sigma|_{K_i(x_i)}$. Puisque $\mathfrak{p}$ est décomposé dans K_i, on a en fait $\sigma_i = (\mathfrak{P}_i, K_i(x_i)/K_i)$. Donc, il y a des isogénies cycliques $x_i \to \sigma_i(x_i)$ de degré $\mathfrak{p}$, d'où $(x_1, x_2)^\sigma \in Y^\sigma \cap T_\mathfrak{p}(Y) = Y \cap T_\mathfrak{p}(Y)$, car σ agit trivialement sur F.

L'indice de l'intersection est $Y \cdot T_\mathfrak{p}(Y) = 2 d_1 d_2 (|\mathfrak{p}| + 1)^2$. Or, toute la $\operatorname{Gal}(FM/F)$-orbite du point (x_1, x_2) est dans cette intersection, donc si $\#\operatorname{Pic}(\mathcal{O}_i) > 2 m d_1 d_2 (|\mathfrak{p}| + 1)^2$, alors l'intersection est impropre et il en résulte que $Y \subset T_\mathfrak{p}(Y)$, donc Y est modulaire d'après le Théorème 2.

Le genre g_i de K_i est donné par $g_i = (\deg(D_i) - 2)/2$ si $\deg(D_i)$ est pair et par $g_i = (\deg(D_i) - 1)/2$ si $\deg(D_i)$ est impair, où on écrit $K_i = k(\sqrt{D_i})$, avec $D_i \in A$ sans facteurs carrés. On a d'ailleurs $H_{CM}(x_i) = |D_i f_i^2|$. En utilisant le théorème de Hasse–Weil, on peut minorer le nombre de classes du corps K_i par $h_{K_i} \geqslant (q-1)(q^{2g_i} - 2g_i q^{g_i} + 1)/2g_i(q^{g_i+1} - 1)$.

Il existe une constante (effectivement calculable) C_1 tel qu'on ait $\#\operatorname{Pic}(\mathcal{O}_i) \geqslant C_1 h_{K_i} |f_i| / \log |f_i|$.

Il reste à trouver des premiers $\mathfrak{p}$ assez petits qui se décomposent dans FK. Soit

$$\pi_{FK}(t) = \#\big\{\mathfrak{p} \in A \mid \text{premier, décomposé dans } FK/k \text{ et } \deg(\mathfrak{p}) = t\big\}.$$

Supposons que $K_1 \neq K_2$ (le cas $K_1 = K_2$ étant similaire). Soit L la clôture algébrique de $\mathbb{F}_q$ dans FK, et notons $n_c = [L : \mathbb{F}_q]$ et $n_g = [FK : Lk]$. Alors le théorème de Čebotarev [8] nous dit que si $n_c|t$, alors $|\pi_{FK}(t) - q^t/n_g t| < 4(g_{FK} + 3)q^{t/2}$. Ici g_{FK} dénote le genre du corps FK, qu'on peut majorer grâce à l'inégalité de Castelnuovo : $g_{FK} \leqslant 2m(g_1 + g_2) + 4g + 4m - 3$. On veut $\pi_{FK}(t) > \log|f_1 f_2|$ (pour trouver un $\mathfrak{p}$ qui ne divise pas $f_1 f_2$) et aussi $\#\operatorname{Pic}(\mathcal{O}_i) > 2md_1d_2(|\mathfrak{p}| + 1)^2$. Il nous faut alors une solution $t \in 2\mathbb{N}$ pour les inégalités :

$$\frac{1}{4m}q^t/t - 8\big(m(g_1 + g_2 + 2) + 2g\big)q^{t/2} > \log|f_1 f_2|, \tag{1}$$

$$\frac{C_1(q-1)(q^{2g_i} - 2g_i q^{g_i} + 1)|f_i|}{g_i(q^{g_i+1} - 1)\log|f_i|} > 4d_1d_2\big(q^t + 1\big)^2 \tag{2}$$

pour $i = 1$ ou $i = 2$, et $n_c|t$. De telles solutions existent si $H_{CM}(x_i) = |D_i f_i^2|$ est suffisamment grand.

Supposons maintenant que F/k ne soit pas galoisienne. Soit F_s la clôture séparable de k dans F, et soit F_s' la clôture de Galois de F_s. Le degré et le genre de F_s' sont encore majorés en termes de m et de g. Alors on définit $\sigma = (\mathfrak{P}, F_s'M/k) \in \operatorname{Gal}(F_s'M/k)$, et son extension $\sigma \in \operatorname{Aut}(FF_s'M/k)$ a les propriétés requises.

2. Partie topologique : esquisse de la démonstration du Théorème 2

Supposons maintenant que $Y \subset T_n(Y)$ pour $n \in A$ produit de premiers distincts de degrés pair. Alors l'intersection de $Y \times Y$ avec la correspondance T_n dans $\mathbb{A}^2 \times \mathbb{A}^2$, moins les composantes de dimension 0, est une courbe notée $T_{Y,n}$. Par abus de notation, on note aussi T_n la correspondance sur $\mathbb{A}^1$ donnée simplement par $Y_0'(n) \subset \mathbb{A}^2$.

Soit $Y \times_{\mathbb{A}^1} T_n$ le produit fibré des deux projections sur la première coordonnée, $pr_1 : Y \to \mathbb{A}^1$ et $pr_1 : Y_0'(n) \to \mathbb{A}^1$. Alors on a un morphisme naturel $T_{Y,n} \to Y \times_{\mathbb{A}^1} T_n$ envoyant $((x_1, y_1), (x_2, y_2))$ sur $((x_1, y_1), (x_1, x_2))$. Puisque c'est un morphisme de type fini des courbes algébriques, il est surjectif si $Y \times_{\mathbb{A}^1} T_n$ est irréductible. Notons par $\mathbf{C}(Z)$ le corps de fonctions d'une courbe Z sur $\mathbf{C}$. Alors $Y \times_{\mathbb{A}^1} T_n$ est irréductible si et seulement si les corps $\mathbf{C}(Y)$ et $\mathbf{C}(Y_0(n))$ sont linéairement disjoints. Soit $Y(n)$ la courbe modulaire de Drinfeld définie par $Y(n) = \Gamma(n)\diagdown\Omega$, où $\Gamma(n)$ est le groupe des matrices dans $\mathrm{GL}_2(A)$ dont la réduction modulo n sont des matrices scalaires. Alors, $\mathbf{C}(Y(n))$ contient $\mathbf{C}(Y_0(n))$, et $\operatorname{Gal}(\mathbf{C}(Y(n))/\mathbf{C}) \cong \prod_{\mathfrak{p}_i|n} \mathrm{PSL}_2(A/\mathfrak{p}_i)$. Or, si $|\mathfrak{p}| \geqslant 13$, alors $\mathrm{PSL}_2(A/\mathfrak{p})$ n'a pas de sous-groupe propre d'indice inférieur à $|\mathfrak{p}| + 1$, donc $\mathbf{C}(Y(n))$ ne contient pas $\mathbf{C}(Y)$. On a donc montré

LEMME 3. – *La projection $pr_1 : T_{Y,n}(Y) \to T_n(\mathbb{A}^1)$ est surjective.*

Tout comme le cas de caractéristique 0, le groupe $\mathrm{PGL}_2(k_\infty)$ agit sur Ω par transformations de Möbius. Par contre, cette action n'est pas transitive, puisque $\mathbf{C}$ est de dimension infinie sur k_∞. En particulier, les stabilisateurs des points $z \in \Omega$ ne sont pas tous conjugués. On distingue deux cas. Si z est quadratique sur k_∞, alors $\operatorname{Stab}(z)$ est un groupe de Lie compact de dimension 1 sur k_∞, sinon $\operatorname{Stab}(z) = \{1\}$.

On considère maintenant l'espace Ω^2, sur lequel $G = \mathrm{PGL}_2(k_\infty)^2$ agit. On note aussi $S = \mathrm{PSL}_2(k_\infty)^2$ et $\Gamma = \mathrm{PGL}_2(A)^2$. L'application $\pi = (j \times j) : \Omega^2 \to \mathbb{A}^2$ est une application analytique rigide, c'est le quotient par l'action du groupe discret Γ. Soit X une composante irréductible de la variété analytique rigide $\pi^{-1}(Y)$. Soit G_X le stabilisateur de X sous l'action de G, et notons $S_X = G_X \cap S$ et $\Gamma_X = G_X \cap \Gamma$.

On va étudier la structure de S_X pour en déduire que Y doit être une courbe modulaire. Comme dans [4] on peut montrer

LEMME 4. –

(1) *Les deux projections $pr_i : G_X \to \mathrm{PGL}_2(k_\infty)$ sont injectives.*
(2) *$pr_i(\Gamma_X)$ est d'indice au plus d_i dans $\mathrm{PGL}_2(A)$.*

Notons Δ_n^* l'ensemble des matrices $\alpha \in M_2(A)$ avec $\det(\alpha) = \mu n$ pour un $\mu \in \mathbb{F}_q^*$ et dont les quatre éléments n'ont pas de facteur en commun. Choisissons des représentants $t_i, i \in I = \{1, \ldots, \psi(n)\}$, des classes $\Delta_n^*/\mathrm{GL}_2(A)$ et notons $t_{ij} = (t_i, t_j)$. Définissons $J = \{(i, j) \in I \times I \mid t_{ij}(X) \subset \pi^{-1}(Y)\}$. Donc pour chaque $(i, j) \in J$ on a $\gamma_{ij} t_{ij} \in G_X$ pour un $\gamma_{ij} \in \mathrm{PGL}_2(A)^2$. Or, $T_n(Y) = \bigcup_{i,j \in I} \pi(t_{ij}(X))$ et $T_{Y,n}(Y) = \bigcup_{(i,j)\in J} \pi(t_{ij}(X))$, donc le Lemme 3 implique que pour chaque $i \in I$, $\exists \gamma_i \in \mathrm{PGL}_2(A)$ tel que $\gamma_i t_i \in H_1 := pr_1(G_X)$. Donc on a trouvé plusieurs éléments non-triviaux dans H_1.

Maintenant des calculs explicites (qui remplacent la théorie de Lie utilisée par Edixhoven) montrent que $H_1 \cap \mathrm{PSL}_2(A[1/n])$ est d'indice fini dans $\mathrm{PSL}_2(A[1/n])$, donc G_X n'est pas discret et H_1 est fermé. Il en résulte, tenant compte que $\mathrm{PSL}_2(k_\infty)$ est simple, que H_1 contient $\mathrm{PSL}_2(k_\infty)$. De même, on a $\mathrm{PSL}_2(k_\infty) \subset pr_2(G_X)$. Par le lemme de Goursat, on obtient $S_X = \{(g, \rho(g)) \mid g \in \mathrm{PSL}_2(k_\infty)\}$ où $\rho \in \mathrm{Aut}(\mathrm{PSL}_2(k_\infty))$. Or, tout automorphisme de $\mathrm{PSL}_2(k_\infty)$ est de la forme $g \mapsto h g^\sigma h^{-1}$ avec $h \in \mathrm{PGL}_2(k_\infty)$ et $\sigma \in \mathrm{Aut}(k_\infty)$ (voir [10]). On a donc montré

LEMME 5. – *$S_X = \{(g, h g^\sigma h^{-1}) \mid g \in \mathrm{PSL}_2(k_\infty)\}$ où $h \in \mathrm{PGL}_2(k_\infty)$ et $\sigma \in \mathrm{Aut}(k_\infty)$.*

Comme $pr_1(\Gamma_X) \cap \mathrm{PSL}_2(A)$ est d'indice fini dans $\mathrm{PSL}_2(A)$ on peut montrer que $h \in \mathrm{PGL}_2(k)$ et qu'il existe un entier t tel que $\sigma(\alpha) = \alpha^{p^t}$ pour tout $\alpha \in \mathbb{F}_q$ et $\sigma(T) = uT + v$ avec $u \in \mathbb{F}_q^*$ et $v \in \mathbb{F}_q$.

Soit maintenant $f = (T^q - T)^{q-1}$, alors $F = \mathbb{F}_p((1/f))$ est un sous-corps complet de k_∞ sur lequel σ agit trivialement. Fixons un $\alpha \in \mathbb{F}_q^*$ non carré, et notons $P = \{z \in \Omega \mid z^2 = \alpha e,\ e \in F\}$. Remarquons que $\sigma(\alpha e) = \beta^2 \alpha e$, avec $\beta = \alpha^{(p^t-1)/2} \in \mathbb{F}_q^*$.

Soit $z_1 \in P$, alors $S_1 = \mathrm{Stab}_{\mathrm{PSL}_2(F)}(z_1)$ est un groupe de Lie compact de dimension 1 sur F. Soit $z_2 \in \Omega$ tel que $(z_1, z_2) \in X$, et considérons la $(S_1, h S_1^\sigma h^{-1})$-orbite de (z_1, z_2) :

$$\left\{\left(g(z_1), h g^\sigma h^{-1}(z_2)\right) \mid g \in S_1\right\} \subset X \cap \left(\{z_1\} \times \Omega\right). \tag{3}$$

Cet ensemble est discret, mais S_1 ne l'est pas, donc il existe $g \in S_1$ non trivial tel que $h g^\sigma h^{-1}$ fixe z_2. Mais $h g^\sigma h^{-1}$ fixe $h(\beta z_1)$, aussi, et tout $g \in \mathrm{PGL}_2(k_\infty)$ a au plus deux points fixes. Donc, soit $z_2 = h(\beta z_1)$, soit $z_2 = h(-\beta z_1)$, le conjugué. Puisque pour chaque $z_1 \in P$ on a $j(z_1) = j(-z_1)$, on voit que la courbe Y contient une infinité de points de la forme $(j(z_1), j(h'(z_1)))$ ou $(j(-z_1), j(h'(-z_1)))$, où on a noté $h' = h \circ \beta \in \mathrm{PGL}_2(k)$. Soit $a \in k^*$ tel que les quatre éléments de ah' soient des éléments de A sans facteur en commun, et posons $N = \det(ah')$. Alors la courbe $\{(j(z), j(h'(z))) \mid z \in \Omega\}$ dans $\mathbb{A}^2$ n'est autre que la courbe modulaire $Y_0'(N)$, donc on a montré que $Y = Y_0'(N)$.

Remerciements. L'auteur tient à remercier Marc Hindry pour son soutien constant, Bas Edixhoven pour son aide, et aussi Gerhard Frey, Hans-Georg Rück et Henning Stichtenoth pour des discussions stimulantes. Une partie de ce travail a été effectuée à l'Institut für Experimentelle Mathematik, Universität Essen, et l'auteur voudrais remercier l'Institut pour l'agréable ambiance de travail.

Références bibliographiques

[1] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, J. Reine Angew. Math. 505 (1998) 203–208.
[2] F. Breuer, Heights of CM points on complex affine curves, Ramanujan J. 5 (2001) 311–317.
[3] M.L. Brown, Singular moduli and supersingular moduli of Drinfeld modules, Invent. Math. 110 (1992) 419–439.
[4] S.J. Edixhoven, Special points on the product of two modular curves, Compositio Math. 114 (1998) 315–328.
[5] S.J. Edixhoven, A. Yafaev, Subvarieties of Shimura varieties, Ann. of Math., à paraître.
[6] E.-U. Gekeler, Zur Arithmetik von Drinfeld–Moduln, Math. Ann. 256 (1982) 549–560.
[7] E.-U. Gekeler, et al. (Eds.), Drinfeld Modules, Modular Schemes and Applications, World Sci. Publishing, River Edge, NJ, 1997.
[8] M. Fried, M. Jarden, Field Arithmetic, Springer-Verlag, 1986.
[9] D. Hayes, A brief introduction to Drinfeld modules, in: D. Goss, et al. (Eds.), The Arithmetic of Function Fields, de Gruyter, New York, 1992.
[10] L.K. Hua, appendice de : J. Dieudonné, On the automorphisms of the classical groups, Mem. Amer. Math. Soc. 2 (1951) 1–95.