Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.
by Serre, Jean-Pierre
in Inventiones mathematicae
volume 15; pp. 259 - 331

Göttingen State and University Library

Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Göttingen State- and University Library.
Each copy of any part of this document must contain these Terms and Conditions.With the usage of the library's online-systems to access or download a digitizied document you accept these Terms and Conditions.

Reproductions of materials on the web site may not be made for or donated to other repositories, nor may they be further reproduced without written permission from the Göttingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:
Niedersaechsische Staats- und Universitaetsbibliothek Göttingen
Digitalisierungszentrum
37070 Göttingen
Germany
E-Mail: gdz@www.sub.uni-goettingen.de

Purchase a CD-ROM

The Goettingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:

Niedersaechsische Staats- und Universitaetsbibliothek Göttingen
Digitalisierungszentrum
37070 Göttingen
Germany
E-Mail: gdz@www.sub.uni-goettingen.de

Göttingen State and University Library

Göttinger Digitalisierungs-Zentrum

Inventiones math. 15, 259 – 331 (1972)
© by Springer-Verlag 1972

Propriétés galoisiennes des points d'ordre fini des courbes elliptiques

JEAN-PIERRE SERRE (Paris)

à André Weil

Introduction

Le présent travail complète mon cours à McGill [27] (cité MG dans ce qui suit). Il s'agit de prouver que les groupes de Galois associés aux points d'ordre fini des courbes elliptiques sont «aussi gros que possible». Les méthodes de MG y parviennent, à condition de se limiter aux points d'ordre l^n, où l est un nombre premier fixé. Elles deviennent insuffisantes dès que l'on fait varier l; c'est essentiellement cette variation que nous allons étudier.

De façon plus précise, soient K un corps de nombres algébriques, $\bar{K}$ une clôture algébrique de K, et G le groupe de Galois de $\bar{K}$ sur K. Soit E une courbe elliptique sur K (par «courbe elliptique» nous entendons une variété abélienne de dimension 1, ou, ce qui revient au même, une courbe de genre 1 munie d'un point rationnel 0 pris comme origine pour la loi de groupe). Le groupe G opère de façon naturelle sur le groupe $E(\bar{K})$ des $\bar{K}$-points de E. Si n est un entier $\geqq 1$, notons E_n le groupe des éléments $x \in E(\bar{K})$ tels que $nx = 0$; c'est un $\mathbf{Z}/n\mathbf{Z}$-module libre de rang 2, et l'action de G sur E_n est donnée par un homomorphisme

$$\varphi_n \colon G \to \mathrm{Aut}(E_n) \simeq \mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z}).$$

Le groupe $\varphi_n(G)$ est le groupe de Galois de l'extension de K obtenue par adjonction des coordonnées des points de E_n.

Les propriétés des φ_n sont bien connues lorsque E a des multiplications complexes, i.e. lorsque l'anneau de ses $\bar{K}$-endomorphismes est de rang 2 sur $\mathbf{Z}$ (cf. [9], [10], [30], ainsi que le n° 4.5 du § 4). Ecartons ce cas, autrement dit supposons que E *n'a pas de multiplication complexe.* Le résultat que nous avons en vue peut alors s'énoncer de la manière suivante:

(1) *L'indice de* $\varphi_n(G)$ *dans* $\mathrm{Aut}(E_n) \simeq \mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z})$ *est borné par une constante ne dépendant que de* E *et de* K.

Il y a intérêt à reformuler (1) en «passant à la limite» sur n:

Soit E_∞ le sous-groupe de torsion de $E(\bar{K})$, i.e. la réunion des E_n. Le groupe $\mathrm{Aut}(E_\infty)$ est limite projective des groupes finis $\mathrm{Aut}(E_n)$; c'est un groupe profini, isomorphe à

$$\varprojlim \mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z}) = \mathbf{GL}_2(\hat{\mathbf{Z}}), \quad \text{où} \quad \hat{\mathbf{Z}} = \varprojlim \mathbf{Z}/n\mathbf{Z}.$$

L'action de G sur E_∞ définit un homomorphisme continu

$$\varphi_\infty : G \to \mathrm{Aut}(E_\infty).$$

L'assertion (1) équivaut à:

(2) *Le groupe $\varphi_\infty(G)$ est un sous-groupe d'indice fini de* $\mathrm{Aut}(E_\infty)$.

Comme $\varphi_\infty(G)$ et $\mathrm{Aut}(E_\infty)$ sont compacts, (2) équivaut à dire que $\varphi_\infty(G)$ est *ouvert* dans $\mathrm{Aut}(E_\infty)$, autrement dit:

(3) *Il existe un entier $m \geqq 1$ tel que $\varphi_\infty(G)$ contienne tout automorphisme de E_∞ dont la restriction à E_m est l'identité.*

Soit P l'ensemble des nombres premiers. Si $l \in P$, soit E_{l^∞} la réunion des E_{l^n}, $n \geqq 1$; c'est la composante l-primaire de E_∞; son groupe d'automorphismes est isomorphe à $\mathbf{GL}_2(\mathbf{Z}_l)$, où $\mathbf{Z}_l$ est l'anneau des entiers l-adiques. On a

$$E_\infty = \bigoplus_{l \in P} E_{l^\infty} \quad \text{et} \quad \mathrm{Aut}(E_\infty) = \prod_{l \in P} \mathrm{Aut}(E_{l^\infty}) \simeq \prod_{l \in P} \mathbf{GL}_2(\mathbf{Z}_l).$$

Notons $\varphi_{l^\infty} : G \to \mathrm{Aut}(E_{l^\infty})$ la l-ième composante de φ_∞; elle indique comment G opère sur E_{l^∞}. L'assertion (3) équivaut à la conjonction des deux suivantes:

(4) *Pour tout $l \in P$, $\varphi_{l^\infty}(G)$ est un sous-groupe ouvert de* $\mathrm{Aut}(E_{l^\infty})$.

(5) *Pour presque tout $l \in P$* (i.e. tout l sauf un nombre fini), *le groupe $\varphi_\infty(G)$ contient le l-ième facteur* $\mathrm{Aut}(E_{l^\infty})$ *de* $\mathrm{Aut}(E_\infty)$.

L'assertion (4) a déjà été démontrée: c'est le résultat principal de MG, cf. p. IV – 11. Le résultat nouveau est (5), qui entraîne:

(6) *Pour presque tout $l \in P$, on a $\varphi_{l^\infty}(G) = \mathrm{Aut}(E_{l^\infty})$.*

En particulier:

(7) *Pour presque tout $l \in P$, on a $\varphi_l(G) = \mathrm{Aut}(E_l)$.*

En fait, compte tenu de ce qui est démontré dans MG, les assertions (5), (6) et (7) sont équivalentes (MG, p. IV – 19). Tout revient donc à démontrer (7); autrement dit, si l'on identifie $\mathrm{Aut}(E_l)$ à $\mathbf{GL}_2(\mathbf{F}_l)$, il faut

prouver que l'homomorphisme

$$\varphi_l\colon G \to \mathbf{GL}_2(\mathbf{F}_l)$$

est *surjectif* pour presque tout l. Le principe de la démonstration est le suivant:

Soient v une place de K de caractéristique résiduelle l, w une place de $\bar{K}$ prolongeant v, et I_w le sous-groupe d'inertie correspondant de G. Supposons que v soit non ramifiée sur $\mathbf{Q}$, et que E ait bonne réduction en v (c'est le cas pour presque tout l). Une étude locale facile montre alors que $\varphi_l(I_w)$ est un sous-groupe de $\mathbf{GL}_2(\mathbf{F}_l)$ de l'un des types suivants:

(i) («demi-sous-groupe de Cartan déployé») Un groupe cyclique d'ordre $l-1$, représentable matriciellement par $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$.

(i') («demi-sous-groupe de Borel») Un groupe résoluble d'ordre $l(l-1)$, représentable matriciellement par $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

(ii) («sous-groupe de Cartan non déployé») Un groupe cyclique d'ordre l^2-1.

Ainsi, $\varphi_l(G)$ contient un sous-groupe de type (i), (i') ou (ii). Or, on peut faire la liste des sous-groupes de $\mathbf{GL}_2(\mathbf{F}_l)$ qui ont cette propriété. On en conclut que, si (7) est en défaut, il existe une partie infinie L de P telle que, pour tout $l \in L$, on ait l'une des situations que voici:

(a) $\varphi_l(G)$ est contenu dans un sous-groupe de Cartan, ou dans un sous-groupe de Borel, de $\mathbf{GL}_2(\mathbf{F}_l)$;

(b) $\varphi_l(G)$ est contenu dans le normalisateur N_l d'un sous-groupe de Cartan C_l de $\mathbf{GL}_2(\mathbf{F}_l)$, et n'est pas contenu dans C_l.

Dans le cas (b), le quotient N_l/C_l est d'ordre 2, et l'homomorphisme $G \to N_l/C_l$ induit par φ_l définit une extension quadratique K_l' de K; on démontre que cette extension est non ramifiée en dehors d'un ensemble fini de places de K, qui ne dépend pas de l. La composée K' des K_l' est donc finie sur K. Quitte à remplacer K par K', on est alors ramené au cas où tous les $(\varphi_l)_{l\in L}$ sont de type (a). Notons $\tilde{\varphi}_l\colon G \to \mathbf{GL}_2(\mathbf{F}_l)$ la représentation de degré 2 de G déduite de φ_l par «semi-simplification». Les groupes $\tilde{\varphi}_l(G)$, $l \in L$, sont abéliens; vu la théorie du corps de classes, on peut interpréter les $\tilde{\varphi}_l$ comme des représentations du groupe des *classes d'idèles* de K. La famille $(\tilde{\varphi}_l)_{l\in L}$ jouit de certaines propriétés globales (existence d'un conducteur – rationalité des éléments de Frobenius) et locales (caractères à exposants bornés) qui seront explicitées plus loin. Ces propriétés permettent de prouver que le système (φ_l) provient d'une représentation $\varphi_0\colon S_m \to \mathbf{GL}_2$ de l'un des groupes algébriques S_m définis dans MG, chap. II. En utilisant alors les résultats de MG, chap. IV,

on en déduit que E a des multiplications complexes, contrairement à l'hypothèse faite.

La démonstration esquissée ci-dessus fait l'objet du § 4. Les trois premiers §§ contiennent divers préliminaires. Le § 1 donne des résultats de nature locale, portant principalement sur le groupe d'inertie modérée, et son action sur les points d'ordre fini des courbes elliptiques et des groupes formels; on trouve que cette action se fait par des produits de «caractères fondamentaux» affectés d'exposants bornés par l'indice de ramification du corps local considéré; l'existence d'une telle borne joue un rôle essentiel dans la suite (tout comme l'hypothèse «localement algébrique» dans MG, chap. III – IV). Le § 2 rassemble quelques résultats élémentaires sur les sous-groupes de $\mathbf{GL}_2(\mathbf{F}_p)$, et notamment sur ceux qui contiennent un sous-groupe, ou «demi-sous-groupe», de Cartan. Le § 3 apporte un complément à MG: il donne une condition permettant d'affirmer qu'un système (ρ_l) de représentations l-adiques d'un corps de nombres provient d'une représentation d'un S_m; cette condition porte essentiellement sur la réduction (mod. l) des ρ_l, cf. n° 3.6, th. 1. Le § 5 contient des résultats spéciaux au corps $\mathbf{Q}$, et donne des exemples numériques, traités en détail; j'ai essayé de le rendre aussi indépendant que possible des §§ précédents. Un dernier § traite le cas d'un produit de deux courbes elliptiques.

Table des matières

§ 1. Inertie modérée

1.1. Notations

Dans ce §, K désigne un corps complet pour une valuation discrète v, que l'on suppose normée: on a $v(K^*)=\mathbf{Z}$. On note A (resp. $\mathfrak{m}$) l'anneau (resp. l'idéal) de v, et l'on pose $k=A/\mathfrak{m}$. *On suppose que le corps résiduel k est de caractéristique $p>0$.* Si $e=v(p)$, on a $1\leqq e\leqq\infty$. A partir du n° 1.9, on suppose que $e\neq\infty$, i.e. que la caractéristique de K est nulle.

Lorsque l'on veut préciser K, on écrit $v_K, A_K, \ldots, e_K$.

1.2. Groupes de Galois

(Les résultats rappelés dans les n^{os} 1.2 à 1.4 sont bien connus; voir par exemple [25], chap. IV, ou [5], chap. I.)

Soit K_s une clôture séparable de K. La valuation v s'étend de façon unique à K_s, et le corps résiduel correspondant est une clôture algébrique $\bar{k}$ de k. On a

$$K_s \supset K_t \supset K_{nr} \supset K,$$

où K_{nr} est la plus grande sous-extension de K_s *non ramifiée sur* K, et K_t la plus grande sous-extension de K_s *modérément ramifiée* («tamely ramified») *sur* K. Les corps résiduels de K_{nr} et K_t s'identifient à la clôture séparable k_s de k dans $\bar{k}$.

On pose

$$G = \mathrm{Gal}(K_s/K), \quad I = \mathrm{Gal}(K_s/K_{nr}) \quad \text{et} \quad I_p = \mathrm{Gal}(K_s/K_t).$$

On a $G \supset I \supset I_p$. Le groupe I (resp. I_p) est le *groupe d'inertie* (resp. le *p-groupe d'inertie*) du groupe de Galois G; c'est un sous-groupe distingué fermé de G. Le groupe $G/I = \mathrm{Gal}(K_{nr}/K)$ s'identifie à $G_k = \mathrm{Gal}(k_s/k)$.

Le groupe I_p est le plus grand pro-p-groupe contenu dans I. Le quotient $I_t = I/I_p = \mathrm{Gal}(K_t/K_{nr})$ est un groupe profini commutatif, d'ordre premier à p, appelé le *groupe d'inertie modérée* de G (ou de K); ce groupe jouera un rôle essentiel dans tout ce qui suit.

1.3. Structure du groupe d'inertie modérée

Soit d un entier $\geqq 1$, premier à p. Notons μ_d le groupe des racines d-ièmes de l'unité dans K_{nr}; ce groupe s'identifie (par réduction modulo l'idéal maximal) au groupe des racines d-ièmes de l'unité dans k_s.

Soit x une uniformisante de K_{nr}, et soit $K_d = K_{nr}(x^{1/d})$. L'extension K_d/K_{nr} est totalement ramifiée, modérée, et de degré d; son groupe de Galois est isomorphe à μ_d. Plus précisément, si $s \in \mathrm{Gal}(K_d/K_{nr})$, il existe une unique racine d-ième de l'unité $\theta_d(s)$ telle que

$$s(x^{1/d}) = \theta_d(s)\, x^{1/d},$$

et l'application θ_d: $\mathrm{Gal}(K_d/K_{nr}) \to \mu_d$ ainsi définie est un isomorphisme. De plus, K_d et θ_d ne dépendent pas du choix de x, ni de celui de sa racine d-ième.

Le corps K_t est réunion des K_d, pour $(d, p) = 1$. D'où:

$$I_t = \mathrm{Gal}(K_t/K_{nr}) = \varprojlim_d \mathrm{Gal}(K_d/K_{nr}),$$

et l'on obtient:

Proposition 1. *Les isomorphismes θ_d définissent un isomorphisme*

$$\theta\colon\ I_t \to \varprojlim \mu_d.$$

(Précisons que l'homomorphisme de transition $\mu_{dd'} \to \mu_d$ du système projectif (μ_d) est $\alpha \mapsto \alpha^{d'}$.)

Remarque. Lorsque k est algébriquement clos, le groupe $\varprojlim \mu_d$ peut s'interpréter comme le groupe fondamental $\pi_1(\mathbf{G}_m)$ du groupe multiplicatif $\mathbf{G}_m$, et l'isomorphisme $\theta\colon I_t \to \pi_1(\mathbf{G}_m)$ ainsi obtenu coïncide avec celui fourni par la théorie du corps de classes local «géométrique», cf. [24].

Revenons au cas général. Si q est une puissance de p, convenons de noter $\mathbf{F}_q$ le sous-corps à q éléments de k_s. On a $\mathbf{F}_q^* = \mu_{q-1}$. De plus, les nombres de la forme $q-1$ sont *cofinaux* dans l'ensemble des entiers premiers à p (ordonné par divisibilité); en effet, si d est un tel entier, il existe $n \geqq 1$ tel que $p^n \equiv 1 \pmod{d}$, par exemple $n = \varphi(d)$. Ainsi, le système projectif (μ_d) est *équivalent* au système projectif formé par les $\mathbf{F}_q^*$ et par les applications «norme»

$$N\colon \mathbf{F}_{q^m}^* \to \mathbf{F}_q^*, \quad \text{avec} \quad N(\alpha) = \alpha^{1+q+\cdots+q^{m-1}}.$$

La proposition 1 est donc équivalente à:

Proposition 2. *Les isomorphismes θ_{q-1} définissent un isomorphisme*

$$\theta\colon I_t \to \varprojlim \mathbf{F}_q^*,$$

où $\mathbf{F}_q$ parcourt l'ensemble des sous-corps finis de k_s.

1.4. Fonctorialité de θ

Soit K' un sous-corps fermé non discret de K, et soit $e(K/K')$ l'indice de ramification de K sur K', autrement dit l'indice de $v_K(K'^*)$ dans $\mathbf{Z}$. Notons $I_{t,K}$ (resp. $I_{t,K'}$) le groupe d'inertie modéré de K (resp. K'). On définit de façon évidente un homomorphisme $I_{t,K} \to I_{t,K'}$, et le diagramme

$$\begin{array}{ccc} I_{t,K} & \xrightarrow{\sim} & \varprojlim \mu_d \\ \downarrow & & \downarrow{\scriptstyle e(K/K')} \\ I_{t,K'} & \xrightarrow{\sim} & \varprojlim \mu_d \end{array}$$

est *commutatif*; cela se vérifie sans difficulté, soit directement, soit en utilisant la prop. 7 ci-après.

1.5. Cas d'un corps résiduel fini

Dans ce n°, on suppose que k est un corps fini $\mathbf{F}_q$.

Soit L/K une extension *abélienne* de K, modérément ramifiée. Le groupe d'inertie $I(L/K)$ de $\mathrm{Gal}(L/K)$ est un quotient de I_t; on a donc un homomorphisme canonique

$$\alpha\colon I_t \simeq \varprojlim \mu_d \to I(L/K),$$

qui est surjectif.

D'autre part, la théorie du corps de classes local associe à L/K un homomorphisme ω: $K^* \to \mathrm{Gal}(L/K)$, l'application de réciprocité. Si U est le groupe des unités de K^*, on a $\omega(U) = I(L/K)$ et $\omega(1+\mathfrak{m}) = \{1\}$, cf. [25], chap. XV. Comme $U/(1+\mathfrak{m}) = k^*$, on voit que ω définit par passage au quotient un homomorphisme surjectif

$$\omega\colon\ k^* \to I(L/K).$$

Vu que $k^* = \mathbf{F}_q^* = \mu_{q-1}$, il s'impose de comparer α et ω:

Proposition 3. *Les homomorphismes α et ω sont opposés l'un de l'autre. Plus précisément, on a*

$$\alpha(s) = \omega \circ \theta_{q-1}(s^{-1}) \qquad \textit{pour tout } s \in I_t,$$

où θ_{q-1} désigne l'homomorphisme de I_t sur $k^* = \mu_{q-1}$ défini au n° 1.3.

Posons $d = q-1$. Soit x une uniformisante de K, et soit $K_d = K_{nr}(x^{1/d})$, cf. n° 1.3. Puisque ω: $k^* \to I(L/K)$ est surjectif, $I(L/K)$ est fini d'ordre un diviseur de d, ce qui montre que L est contenue dans K_d. Vu les propriétés fonctorielles de α et ω, on peut donc supposer que $L = K_d$.

Si $s \in I_t$, on a, par définition de θ_d,

$$s(x^{1/d}) = \theta_d(s)\, x^{1/d}.$$

D'autre part, soit $t \in k^*$, et soit $\omega(t)$ l'élément correspondant de $I(L/K)$. On a

$$\omega(t)(x^{1/d}) = (x, t)_d\, x^{1/d},$$

où $(x, t)_d \in \mu_d$ désigne le *symbole local* associé à x et t, cf. [25], chap. XIV (ici encore, on identifie l'élément t de k^* à la racine de l'unité correspondante de K^*, i.e. à son *représentant multiplicatif*). Mais, d'après une formule connue (*loc. cit.*, p. 217, cor. à la prop. 8), on a

$$(x, t)_d = t^{-v(x)} = t^{-1}.$$

Si l'on prend $t = \theta_d(s^{-1})$, on a donc $\omega(t)(x^{1/d}) = s(x^{1/d})$, et, comme s et $\omega(t)$ sont l'identité sur K_{nr}, on voit bien que s et $\omega(t)$ agissent de la même façon sur $K_d = L$, ce qui démontre la proposition.

1.6. Représentations de G en caractéristique p

Soit V un espace vectoriel de dimension finie n sur un corps k_1 de caractéristique p, et soit

$$\rho\colon\ G \to \mathbf{GL}(V)$$

une représentation linéaire continue (i.e. à noyau ouvert) de G dans V.

Proposition 4. *Si ρ est semi-simple, on a $\rho(I_p) = \{1\}$.*

(Rappelons que I_p est le p-groupe d'inertie de $G = \mathrm{Gal}(K_s/K)$, cf. n° 1.2.)

Il suffit de prouver que $\rho(I_p)=\{1\}$ lorsque ρ est *simple*. Soit alors V' l'ensemble des éléments de V invariants par $\rho(I_p)$. Comme $\rho(I_p)$ est un p-groupe fini, on a $V'\neq 0$ (cf. par exemple [25], p. 146, th. 2), et comme I_p est distingué dans G, V' est stable par $\rho(G)$, donc égal à V, d'où la proposition.

Supposons ρ semi-simple. La prop. 4 montre que I_p opère trivialement sur V, et l'action de I se factorise à travers une action du groupe d'inertie modérée $I_t=I/I_p$. L'image de I_t par ρ est un groupe cyclique d'ordre premier à p; si k_1 est assez grand (séparablement clos, par exemple), on peut mettre $\rho(I_t)$ sous forme diagonale, autrement dit la restriction $\rho|I_t$ de ρ à I_t est donnée par n *caractères* ψ_i: $I_t\to k_1^*$, $i=1,\ldots,n$. Nous verrons un peu plus loin comment on peut expliciter de tels caractères.

Exemple. Soit V_p un espace vectoriel de dimension n sur le corps p-adique $\mathbf{Q}_p$, et soit

$$\varphi\colon\ G\to \mathbf{GL}(V_p)$$

une représentation linéaire continue de G dans V_p. Choisissons un $\mathbf{Z}_p$-réseau T_p de V_p stable par G (MG, p. I – 1). Le $\mathbf{F}_p$-espace vectoriel T_p/pT_p est de dimension n; la représentation naturelle de G dans cet espace n'est pas nécessairement semi-simple; notons $\tilde{\varphi}$ sa *semi-simplifiée*, autrement dit la somme directe des représentations simples intervenant dans une suite de Jordan-Hölder de T_p/pT_p. D'après un théorème de Brauer-Nesbitt (cf. [6], §82.1), $\tilde{\varphi}$ *ne dépend pas* (à isomorphisme près) du choix de T_p. En appliquant la prop. 4 à $\tilde{\varphi}$ on obtient une représentation du groupe G/I_p, d'où des caractères $\psi_1,\ldots,\psi_n$ de I_t comme ci-dessus.

Ceci s'applique notamment à la représentation φ fournie par le module de Tate V_p d'une variété abélienne (resp. d'un groupe p-divisible) définie sur K (resp. défini sur l'anneau A), pourvu bien entendu que K soit de caractéristique zéro.

1.7. Caractères de I_t

Nous allons expliciter le groupe $X=\mathrm{Hom}(I_t,k_s^*)$ des caractères continus de I_t à valeurs dans k_s^* (ou dans la réunion des $\mathbf{F}_q^*$, cela revient au même).

Les caractères θ_d: $I_t\to \mathrm{Gal}(K_d/K_{nr})\simeq\mu_d$ du n° 1.3 appartiennent à X, et vont nous servir à «paramétrer» X. De façon plus précise, notons $(\mathbf{Q}/\mathbf{Z})'$ l'ensemble des éléments de $\mathbf{Q}/\mathbf{Z}$ d'ordre premier à p. Tout élément α de $(\mathbf{Q}/\mathbf{Z})'$ s'écrit $\alpha=a/d$, avec a, $d\in\mathbf{Z}$ et $(d,p)=1$; notons χ_α la puissance a-ième de θ_d; on vérifie aussitôt que χ_α ne dépend pas de l'écriture a/d choisie pour α. De plus:

Proposition 5. *L'application $\alpha\mapsto\chi_\alpha$ est un isomorphisme de $(\mathbf{Q}/\mathbf{Z})'$ sur le groupe X des caractères de I_t.*

Le groupe $(\mathbf{Q}/\mathbf{Z})'$ est réunion des sous-groupes $\frac{1}{d}\mathbf{Z}/\mathbf{Z}$; d'autre part I_t est limite projective des μ_d, et X est limite inductive des groupes $X_d = \mathrm{Hom}(\mu_d, k_s^*)$. La proposition résulte de là et de ce que $\alpha \mapsto \chi_\alpha$ est un isomorphisme de $\frac{1}{d}\mathbf{Z}/\mathbf{Z}$ sur X_d.

Si $\psi \in X$, l'élément α de $(\mathbf{Q}/\mathbf{Z})'$ tel que $\psi = \chi_\alpha$ est appelé *l'invariant* de ψ. Ainsi, l'invariant de θ_d est $1/d$.

Remarque. La composante p-primaire de $\mathbf{Q}/\mathbf{Z}$ est $\mathbf{Q}_p/\mathbf{Z}_p$, et l'on a les décompositions en sommes directes

$$\mathbf{Q}/\mathbf{Z} = \mathbf{Q}_p/\mathbf{Z}_p \oplus (\mathbf{Q}/\mathbf{Z})' \quad \text{et} \quad (\mathbf{Q}/\mathbf{Z})' = \bigoplus_{l \neq p} \mathbf{Q}_l/\mathbf{Z}_l.$$

On a en particulier une projection canonique $\mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to (\mathbf{Q}/\mathbf{Z})'$, dont le noyau est $\mathbf{Z}[1/p]$. Si $\alpha \in \mathbf{Q}$, on se permettra de noter χ_α le caractère $\chi_{\alpha'}$ correspondant à l'image α' de α dans $(\mathbf{Q}/\mathbf{Z})'$, et l'on dira que l'invariant de χ_α est α (mod. $\mathbf{Z}[1/p]$).

Exemples: caractères fondamentaux

Soit n un entier $\geqq 1$, et soit $q = p^n$. On appelle *caractère fondamental de niveau n* tout caractère obtenu en composant le caractère

$$\theta_{q-1} : I_t \to \mu_{q-1} = \mathbf{F}_q^*,$$

avec un automorphisme du *corps* $\mathbf{F}_q$; en d'autres termes, un tel caractère est un *conjugué* (sur $\mathbf{F}_p$) du caractère θ_{q-1}; on peut l'écrire comme

$$\chi = \theta_{q-1}^{p^i}, \qquad \text{où } i = 0, 1, \ldots, n-1.$$

Il y a donc n caractères fondamentaux de niveau n; leurs invariants sont égaux à $p^i/(q-1) = p^i/(p^n-1)$, où $i = 0, 1, \ldots, n-1$.

Plus généralement, soit k_1 un corps de caractéristique p. Un caractère χ de I_t à valeurs dans k_1^* est dit *fondamental de niveau n* si on l'obtient en composant θ_{q-1} avec un plongement du corps $\mathbf{F}_q$ dans k_1.

1.8. Représentation de G dans $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$

Prolongeons la valuation v de K au corps K_s; on obtient une valuation de K_s dont le groupe des valeurs $v(K_s^*)$ est égal à $\mathbf{Q}$. Si $\alpha \in \mathbf{Q}$, notons $\mathfrak{m}_\alpha$ (resp. $\mathfrak{m}_\alpha^+$) l'ensemble des $x \in K_s$ tels que $v(x) \geqq \alpha$ (resp. $v(x) > \alpha$); le quotient

$$V_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$$

est un espace vectoriel de dimension 1 sur le corps résiduel $\bar{k}$ de K_s. Le groupe $G = \mathrm{Gal}(K_s/K)$ opère de façon naturelle sur V_α.

Proposition 6. *Soit $s \in G$, et soit σ l'image de s dans le groupe*

$$G_k = \mathrm{Gal}(k_s/k) = \mathrm{Gal}(\bar{k}/k).$$

L'automorphisme de V_α défini par s est σ-linéaire.

En effet, l'application $(\lambda, x) \mapsto \lambda x$ de $\bar{k} \times V_\alpha$ dans V_α commute à l'action de G, et l'on a donc

$$s(\lambda x) = s(\lambda)\, s(x) = \sigma(\lambda)\, s(x),$$

ce qui signifie bien que $x \mapsto s(x)$ est σ-linéaire.

D'après la prop. 6, les éléments de I opèrent *linéairement* sur V_α; puisque V_α est de dimension 1, cela signifie que I opère sur V_α au moyen d'un *caractère* $\varphi_\alpha : I \to \bar{k}^*$; on a

$$s(x) = \varphi_\alpha(s)\, x \qquad \text{pour tout } s \in I \text{ et tout } x \in V_\alpha.$$

Comme $\bar{k}^*$ ne contient pas d'élément d'ordre p, le caractère φ_α est égal à 1 sur I_p, donc peut être considéré comme un caractère du groupe d'inertie modérée $I_t = I/I_p$.

Proposition 7. *Le caractère φ_α donnant l'action de I_t sur V_α est égal au caractère χ_α défini au* n° 1.7.

Soient $\alpha, \beta \in \mathbf{Q}$. L'application $(x, y) \mapsto xy$ de $\mathfrak{m}_\alpha \times \mathfrak{m}_\beta$ dans $\mathfrak{m}_{\alpha+\beta}$ définit par passage au quotient un isomorphisme de $V_\alpha \otimes V_\beta$ sur $V_{\alpha+\beta}$, isomorphisme qui commute à l'action de G. On en conclut que $\varphi_{\alpha+\beta} = \varphi_\alpha \varphi_\beta$, autrement dit que $\alpha \mapsto \varphi_\alpha$ est un homomorphisme.

Soient d'autre part d un entier positif premier à p, et x une racine d-ième d'une uniformisante de K. On a

$$v(x) = 1/d \quad \text{et} \quad s(x) = \theta_d(x)\, x \qquad \text{pour tout } s \in I_t, \qquad \text{cf. n° 1.3.}$$

Il en résulte que $\varphi_{1/d} = \theta_d = \chi_{1/d}$. Or, si $\alpha \in \mathbf{Q}$, il existe une puissance q de p telle que $q\alpha = a/d$, avec $a \in \mathbf{Z}$, et d positif premier à p. Vu l'additivité de $\alpha \mapsto \varphi_\alpha$ et $\alpha \mapsto \chi_\alpha$, on en conclut que

$$\varphi_\alpha^q = \varphi_{a/d} = (\varphi_{1/d})^a = (\chi_{1/d})^a = \chi_\alpha^q,$$

d'où $\varphi_\alpha = \chi_\alpha$ puisque le groupe des caractères de I_t n'a pas de p-torsion.

Application: *action de I_t sur μ_p*

Supposons K de caractéristique zéro. Soit μ_p le groupe des racines p-ièmes de l'unité dans K_s. Le groupe G opère sur μ_p, et son sous-groupe I_p opère trivialement (prop. 4). On obtient donc une action de I_t sur μ_p, d'où un caractère

$$\chi : I_t \to \mathbf{F}_p^* = \mathrm{Aut}(\mu_p).$$

Proposition 8. *Le caractère χ donnant l'action de I_t sur μ_p est la puissance e-ième du caractère fondamental θ_{p-1} de niveau* 1.

(Rappelons que $e=v(p)$ est *l'indice de ramification absolu* de K.)

Soit $\alpha=e/(p-1)$. Si $z\in\mu_p$, $z\neq 1$, on sait que $v(z-1)=\alpha$. On en conclut que l'application $z\mapsto z-1$ induit par passage au quotient un homomorphisme injectif de μ_p dans V_α; cet homomorphisme commute à l'action de G, et en particulier à celle de I_t. La proposition en résulte, puisque I_t opère sur V_α grâce au caractère $\chi_\alpha=\theta_{p-1}^e$, cf. prop. 7.

Corollaire. *Si $e=1$, on a $\chi=\theta_{p-1}$.*

1.9. Représentation de G définie par un groupe formel (cas $e=1$)

Dans ce n°, on suppose que $e=1$, i.e. que p est une *uniformisante* de K; en particulier, K est de caractéristique zéro. On note A_s l'anneau des entiers de K_s et $\mathfrak{m}_s$ l'idéal maximal de A_s.

Soit

$$F(X,Y)=X+Y+\sum_{i,j\geq 1} c_{ij}X^iY^j, \qquad c_{ij}\in A,$$

une *loi de groupe formel* à un paramètre sur l'anneau A (cf. par exemple [12], chap. III – IV). Notons

$$[p](X)=\sum_{i=1}^{\infty} a_iX^i, \qquad a_i\in A,$$

la «multiplication par p» par rapport à la loi F; c'est une série formelle dont le premier coefficient a_1 est égal à p. Nous supposerons que F *est de hauteur finie h* ([12], chap. IV, § 2); si l'on pose $q=p^h$, cette hypothèse signifie que l'on a

$$a_i\equiv 0 \pmod{\mathfrak{m}} \quad \text{pour } i<q, \quad \text{et} \quad a_q\not\equiv 0 \pmod{\mathfrak{m}},$$

de sorte que la réduction mod. $\mathfrak{m}$ de $[p]$ commence par un terme en X^q.

Notons V le *noyau de* $[p]$, i.e. l'ensemble des $x\in\mathfrak{m}_s$ tels que $[p](x)=0$; on munit V de la loi de composition $(x,y)\mapsto F(x,y)$. On sait (cf. [14] ou [12], p. 107) que V est un $\mathbf{F}_p$-espace vectoriel de dimension h. Le groupe G opère de façon naturelle sur V, de sorte que l'on se trouve dans la situation du n° 1.6.

Proposition 9. *Il existe sur V une structure de $\mathbf{F}_q$-espace vectoriel de dimension* 1 *jouissant des propriétés suivantes*:

(i) *Soient $s\in G$, σ l'image de s dans $G_k=\mathrm{Gal}(k_s/k)$, et σ_q la restriction de σ à $\mathbf{F}_q$. L'automorphisme de V défini par s est σ_q-linéaire.*

(ii) *Le groupe I_p opère trivialement sur V, et le groupe $I_t=I/I_p$ opère par l'intermédiaire du caractère fondamental θ_{q-1}: $I_t\to\mathbf{F}_q^*$ de niveau h.*

(Rappelons que $\mathbf{F}_q$ est le sous-corps à $q=p^h$ éléments de k_s.)

La démonstration est essentiellement la même que celle de la prop. 8 (que l'on retrouve en prenant pour F la loi multiplicative $X+Y+XY$). Si x est un élément non nul de V, on a

$$p+a_2 x+\cdots+a_q x^{q-1}+\cdots=0,$$

et comme les a_i sont divisibles par p pour $i<q$, on voit, en comparant les valuations, que $v(x)=1/(q-1)$. Posons alors $\alpha=1/(q-1)$. Si $x, y\in V$, on a $x, y\in \mathfrak{m}_\alpha$ et

$$F(x, y)\equiv x+y \pmod{\mathfrak{m}_\alpha^+}.$$

On en conclut que la projection $\mathfrak{m}_\alpha \to V_\alpha=\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$ définit un homomorphisme injectif de V dans V_α; cet homomorphisme commute à l'action de G, ce qui montre déjà que I_p opère trivialement sur V. Si l'on identifie V à son image dans V_α, la prop. 7 montre que I_t opère sur V par la formule

$$s x=\theta_{q-1}(s)\, x \quad \text{si } s\in I_t,\ x\in V.$$

Comme $\theta_{q-1}\colon I_t \to \mathbf{F}_q^*$ est surjectif, ceci entraîne que V est stable par multiplication par $\mathbf{F}_q^*$, donc que c'est un sous-$\mathbf{F}_q$-espace vectoriel de V_α; comme $\mathrm{Card}(V)=q$, cet espace vectoriel est de dimension 1. L'assertion (i) résulte alors de la prop. 6, et l'assertion (ii) de la prop. 7.

Corollaire 1. *L'image de I_t dans $\mathbf{GL}(V)$ est formée des homothéties $x\mapsto \lambda x$, avec $\lambda\in\mathbf{F}_q^*$; c'est un groupe cyclique d'ordre $q-1$.*

Cela résulte de ce que $\theta_{q-1}\colon I_t \to \mathbf{F}_q^*$ est surjectif.

Corollaire 2. *Supposons que $k=\mathbf{F}_p$. L'image de G dans $\mathbf{GL}(V)$ est alors formée de tous les automorphismes semi-linéaires du $\mathbf{F}_q$-espace vectoriel V.*

(En d'autres termes, l'image de G dans $\mathbf{GL}_h(\mathbf{F}_p)$ est le normalisateur du *sous-groupe de Cartan* $\mathbf{F}_q^*$.)

En effet, l'hypothèse $k=\mathbf{F}_p$ entraîne que tout automorphisme de $\mathbf{F}_q$ est de la forme σ_q, donc est induit par un élément de G.

Remarques. 1) La structure de $\mathbf{F}_q$-espace vectoriel de V est indépendante de la coordonnée x choisie; elle ne dépend que du *groupe formel* défini par la loi F.

2) Soient k_1 une clôture algébrique de $\mathbf{F}_p$, et $V_1=k_1\otimes_{\mathbf{F}_p} V$. L'action de G sur V s'étend par linéarité en une action k_1-linéaire sur V_1; de plus, on peut mettre l'action de I_t sous forme diagonale (n° 1.6). Plus précisément:

Corollaire 3. *Les h caractères donnant l'action de I_t sur V_1 sont les h caractères fondamentaux $I_t \to k_1^*$ de niveau h.*

En effet, soit Γ l'ensemble des plongements de $\mathbf{F}_q$ dans k_1. Si $\gamma \in \Gamma$, notons $V_{(\gamma)}$ l'espace vectoriel de dimension 1 déduit du $\mathbf{F}_q$-espace vectoriel V par l'extension des scalaires γ: $\mathbf{F}_q \to k_1$. On vérifie aussitôt que V_1 est somme directe des $V_{(\gamma)}$ ($\gamma \in \Gamma$), et que I_t opère sur $V_{(\gamma)}$ au moyen du caractère $\gamma \circ \theta_{q-1}$. D'où le corollaire, puisque les $\gamma \circ \theta_{q-1}$ sont les différents caractères fondamentaux de niveau h de I_t.

1.10. Représentation de G définie par un groupe formel (cas général)

Les résultats du n° 1.9, relatifs au cas $e=1$, sont suffisants pour les applications que nous avons en vue. Aussi nous bornerons-nous à indiquer rapidement ce qui se passe lorsque e est un entier quelconque.

Soient F une loi de groupe formel à un paramètre sur A, de hauteur finie h, et $[p](X)$ la multiplication par p correspondante. On a

$$[p](X) = \sum_{i=1}^{\infty} a_i X^i,$$

avec $a_i \in A$, $a_1 = p$, $v(a_i) \geqq 1$ si $i < q = p^h$ et $v(a_q) = 0$.

Notons encore V le noyau de $[p]$ dans $\mathfrak{m}_s$; c'est un $\mathbf{F}_p$-espace vectoriel de dimension h. Les valuations des éléments de V se lisent sur le *polygone de Newton*[1] de la série formelle $[p](X)$. Comme nous n'avons affaire qu'à des éléments de valuation >0, seule la partie de ce polygone de pente <0 nous intéresse. Vu les propriétés des $v(a_i)$ données ci-dessus, cette partie est une ligne brisée dont la projection sur l'axe Ox est le segment $[1, q]$. Notons $P_i = (q_i, e_i)$ ses différents sommets, rangés de telle sorte que

$$1 = q_0 < q_1 < q_2 < \cdots < q_m = q, \qquad \text{cf. Fig. 1.}$$

On a $e_i = v(a_{q_i})$, et en particulier $e_0 = v(a_1) = v(p) = e$ et $e_m = v(a_q) = 0$; les e_i forment une suite strictement décroissante.

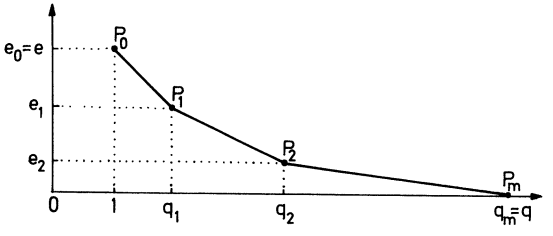

Fig. 1. Polygone de Newton de $[p](X)$

[1] Pour tout ce qui concerne les polygones de Newton des séries formelles, voir par exemple F. Bruhat, *Lectures on some aspects of p-adic analysis*, p. 111–114, Tata Institute, Bombay, 1963.

La *pente* du i-ème côté $P_{i-1}P_i$ est $-\alpha_i$, où $\alpha_i=(e_{i-1}-e_i)/(q_i-q_{i-1})$, et la longueur de la projection de $P_{i-1}P_i$ sur Ox est q_i-q_{i-1}. Il en résulte que *le nombre des éléments de V de valuation α_i est q_i-q_{i-1}*, et que *tout élément non nul de V a pour valuation l'un des α_i*. On a

$$\alpha_1>\alpha_2>\cdots>\alpha_m.$$

Soit V^i $(i=1,\ldots,m)$ le sous-ensemble de V formé des éléments x tels que $v(x)\geqq\alpha_i$; posons $V^0=0$. On vérifie sans difficulté que les V^i sont des *sous-groupes* de V; ils forment une *filtration strictement croissante*

$$0=V^0\subset V^1\subset V^2\subset\cdots\subset V^m=V.$$

Comme $\mathrm{Card}(V^i)=q_i$, on en conclut que q_i est de la forme p^{h_i}, avec $0<h_1<h_2<\cdots<h_m=h$. Posons $\mathrm{gr}^iV=V^i/V^{i-1}$, avec $i=1,\ldots,m$. Le groupe G opère sur V et conserve la filtration (V^i); il opère donc sur les gr^iV.

Proposition 10. (a) *Le groupe I_p opère trivialement sur gr^iV.*

(b) *Soit k_1 une clôture algébrique de $\mathbf{F}_p$. Les caractères donnant l'action de I_t sur $k_1\otimes_{\mathbf{F}_p}\mathrm{gr}^iV$ sont les puissances $(e_{i-1}-e_i)$-ièmes des caractères fondamentaux de niveau h_i-h_{i-1}.*

L'inclusion de V^i dans $\mathfrak{m}_{\alpha_i}$ définit par passage au quotient un homomorphisme injectif $\mathrm{gr}^iV\to V_{\alpha_i}=\mathfrak{m}_{\alpha_i}/\mathfrak{m}_{\alpha_i}^+$. Comme I_p opère trivialement sur V_{α_i}, cela démontre (a). Pour (b), on remarque d'abord que I_t opère sur V_{α_i} par le caractère χ_{α_i}; en écrivant α_i sous la forme

$$\alpha_i=(e_{i-1}-e_i)/p^{h_{i-1}}(p^{h_i-h_{i-1}}-1),$$

on voit que χ_{α_i} est la puissance $(e_{i-1}-e_i)$-ième de l'un des caractères fondamentaux de niveau h_i-h_{i-1}; l'assertion (b) s'en déduit sans grande difficulté (utiliser le fait que l'ensemble des caractères de I_t donnant l'action de ce groupe sur $k_1\otimes\mathrm{gr}^iV$ est invariant par conjugaison sur $\mathbf{F}_p$).

Remarque. On notera que les exposants $e_{i-1}-e_i$ qui interviennent dans (b) sont *compris entre* 1 *et* e; nous reviendrons au n° 1.13 sur ce fait.

1.11. Représentation de G définie par une courbe elliptique ayant bonne réduction

Dans ce n° ainsi que le suivant, on suppose K de caractéristique zéro. La lettre E désigne une courbe elliptique[2] sur K. On note E_p le noyau de la multiplication par p dans $E(K_s)$; c'est un $\mathbf{F}_p$-espace vectoriel de dimension 2. On s'intéresse à la représentation naturelle de G dans E_p.

[2] Pour les propriétés générales des courbes elliptiques, voir Cassels [4], Deuring [8], Roquette [22], ainsi que Mumford [15], p. 214–220. Pour les modèles de Néron et les propriétés de bonne ou mauvaise réduction, voir Néron [16], Ogg [19] ainsi que [30].

Comme $\wedge^2 E_p$ est canoniquement isomorphe au groupe μ_p des racines p-ièmes de l'unité ([4], th. 8.1), le *déterminant* de la représentation de G dans E_p est égal au caractère $G \to \mathbf{F}_p^*$ donnant l'action de G sur μ_p; d'après la prop. 8, la restriction de ce caractère à I_t est la *puissance e-ième du caractère fondamental* θ_{p-1} *de niveau* 1. Cela fournit un premier renseignement sur le module galoisien E_p.

Faisons maintenant l'hypothèse que E a *bonne réduction* sur A; cela signifie que l'on peut représenter E comme une cubique plane d'équation

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

à coefficients a_i appartenant à A, le discriminant $\Delta = \Delta(a_1, \ldots, a_6)$ étant *inversible* dans A (pour la formule donnant Δ, voir par exemple le n° 5.1 du § 5); le point à l'infini de l'axe $O y$ est pris comme origine. Si $\tilde{a}_i$ désigne l'image de a_i dans k, l'équation

$$y^2 + \tilde{a}_1 x y + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$$

définit une courbe elliptique $\tilde{E}$ sur k, appelée la *réduction de* E mod. $\mathfrak{m}$. Distinguons maintenant deux cas:

(1) *Bonne réduction de hauteur* 1

C'est le cas où l'invariant de Hasse de $\tilde{E}$ n'est pas nul (cf. Deuring [8]); le noyau de la multiplication par p dans $\tilde{E}(\bar{k})$ est un groupe $\tilde{E}_p$ d'ordre p. On a une suite exacte

$$0 \to X_p \to E_p \to \tilde{E}_p \to 0,$$

où $E_p \to \tilde{E}_p$ est l'homomorphisme de réduction modulo $\mathfrak{m}_s$; le noyau X_p est cyclique d'ordre p. Le groupe G laisse stable X_p. Si l'on choisit une base (e_1, e_2) de E_p telle que $X_p = \mathbf{F}_p e_1$, l'image de G dans $\mathrm{Aut}(E_p) = \mathbf{GL}_2(\mathbf{F}_p)$ est *contenue dans le sous-groupe de Borel* $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. L'image de I_p est contenue dans le sous-groupe unipotent $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$; le groupe I_t opère sur X_p (resp. sur $\tilde{E}_p$) au moyen d'un caractère χ_X (resp. χ_Y) à valeurs dans $\mathbf{F}_p^*$. En fait:

Proposition 11 (bonne réduction de hauteur 1). *On a* $\chi_X = \theta_{p-1}^e$ *et* $\chi_Y = 1$.

Le fait que $\chi_Y = 1$ résulte de ce que G opère sur $\tilde{E}_p$ par l'intermédiaire de l'homomorphisme canonique $G \to G_k$ et de l'action naturelle de G_k sur $\tilde{E}(\bar{k})$. D'autre part, le produit $\chi_X \chi_Y$ est égal au déterminant de l'action de I_t sur E_p, donc est égal à θ_{p-1}^e, d'après ce qu'on a vu plus haut.

Corollaire. *Supposons* $e=1$. *Alors*:

a) *Les deux caractères donnant l'action de* I_t *sur le semi-simplifié de* E_p *sont le caractère unité et le caractère fondamental* θ_{p-1}.

b) *Si* I_p *opère trivialement sur* E_p, *l'image de* I *dans* $\mathbf{GL}(E_p)$ *est un groupe cyclique d'ordre* $p-1$, *représentable matriciellement sous la forme* $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$, *par rapport à une base convenable* (e_1, e_2) *de* E_p, *avec* $e_1 \in X_p$.

c) *Si* I_p *n'opère pas trivialement sur* E_p, *l'image de* I *dans* $\mathbf{GL}(E_p)$ *est d'ordre* $p(p-1)$. *Elle est représentable matriciellement sous la forme* $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

L'assertion a) est évidente. Elle entraîne que χ_X: $I_t \to \mathbf{F}_p^*$ est surjectif, et l'image de I est d'ordre multiple de $p-1$; comme cette image est un sous-groupe du groupe $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$, son ordre est soit $p-1$, soit $p(p-1)$; le premier cas correspond à b) et le second cas à c).

Remarque. Je ne connais pas de critère simple permettant de reconnaître si l'on est dans le cas b) ou dans le cas c). La question est visiblement liée à celle du *relèvement canonique* de $\tilde{E}$.

Voici une question voisine: soit E_0 une courbe elliptique, sans multiplications complexes, sur un corps de nombres K_0. Notons Σ_b (resp. Σ_c) l'ensemble des places de K_0 en lesquelles E_0 a bonne réduction de hauteur 1 et de type b) (resp. de type c)) au sens ci-dessus. On sait que la *densité* de $\Sigma_b \cup \Sigma_c$ est 1 ([26], cor. 1 au th. 6 – voir aussi MG, p. IV – 13, exerc.). Que peut-on dire des densités de Σ_b et Σ_c? Est-il vrai que la densité de Σ_b est 0?

(2) *Bonne réduction de hauteur* 2

C'est le cas où l'invariant de Hasse de $\tilde{E}$ est nul; la courbe $\tilde{E}$ n'a pas de point d'ordre p, et tous les éléments de E_p se réduisent en l'élément neutre de $\tilde{E}$.

Ecrivons comme ci-dessus l'équation de E sous la forme

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

avec $a_i \in A$ et Δ inversible. Si $(x, y) \in E(K_s)$ se réduit suivant l'élément neutre de $\tilde{E}$, on voit facilement que $t = x/y$ appartient à $\mathfrak{m}_s$, et tout élément de $\mathfrak{m}_s$ est obtenu ainsi, de manière unique. De plus, la loi de composition de la courbe E se traduit en une *loi de groupe formel*

$$F(t, t') = t + t' + a_1 t t' - a_2(t^2 t' + t t'^2) + \cdots$$

à coefficient dans A. (Le groupe formel associé à F est le *complété formel* du modèle de Néron de E sur A.)

Soit $[p](t)=pt+a_1\binom{p}{2}t^2+\cdots$ la série formelle donnant la multiplication par p relativement à F (cf. n° 1.9). D'après ce qui précède, le groupe E_p s'identifie par $(x,y)\mapsto t=x/y$ au *noyau* de $[p]$. Comme $\mathrm{Card}(E_p)=p^2$, il en résulte que la *hauteur h de F est égale à* 2, résultat d'ailleurs facile à retrouver directement. On peut donc appliquer la prop. 9 et ses corollaires. D'où:

Proposition 12 (bonne réduction de hauteur 2). *Supposons que* $e=1$. *Alors*:

a) *L'action de* I_p *sur* E_p *est triviale.*

b) *Il existe sur* E_p *une structure de* $\mathbf{F}_{p^2}$*-espace vectoriel de dimension* 1 *telle que l'action de* I_t *soit donnée par le caractère fondamental* θ_{p^2-1} *de niveau* 2.

c) *L'image de I dans* $\mathbf{GL}(E_p)$ *est un groupe cyclique C d'ordre* p^2-1 («sous-groupe de Cartan non déployé», cf. n° 2.1).

d) *L'image de G dans* $\mathbf{GL}(E_p)$ *est égale à C ou au normalisateur N de C suivant que k contient ou ne contient pas* $\mathbf{F}_{p^2}$.

En particulier:

Corollaire. *Soit* k_1 *une clôture algébrique de* $\mathbf{F}_p$. *L'action de* I_t *sur* $k_1\otimes E_p$ *est donnée par les deux caractères fondamentaux* $I_t\to k_1^*$ *de niveau* 2.

Remarque. Lorsque $e>1$, la prop. 10 fournit des renseignements sur le module galoisien E_p, à condition que l'on connaisse le polygone de Newton de la série formelle $[p](t)$. Vu ce qui a été démontré au n° 1.10, il suffit de connaître la *valuation* du p-ième coefficient de cette série formelle. En voici un exemple simple:

Prenons $p=5$, et supposons E donnée sous la forme

$$y^2=x^3+a_4x+a_6,\quad \text{avec } v(a_4)>0 \text{ et } v(a_6)=0.$$

On a

$$[5](t)=5t-1248a_4t^5+\cdots.$$

Posons $f=v(a_4)$, $P_0=(1,e)$, $P_1=(5,f)$, $P_2=(25,0)$. Il y a deux cas à distinguer:

On a $f\geqq 5e/6$, i.e. le point P_1 est au-dessus du segment P_0P_2. Le polygone de Newton de la série $[5](t)$ est P_0P_2. Les caractères de I_t qui interviennent sont les puissances e-ièmes des caractères fondamentaux de niveau 2.

On a $f<5e/6$, i.e. P_1 est strictement au-dessous de P_0P_2. Le polygone de Newton est la ligne brisée $P_0P_1P_2$; les caractères de I_t qui interviennent sont les puissances f-ièmes et $(e-f)$-ièmes du caractère fondamental de niveau 1.

[Pour des valeurs plus grandes de p, il n'est pas nécessaire de calculer exactement le p-ième coefficient de $[p](t)$, il suffit de connaître sa valeur modulo p; or on peut vérifier que cette valeur est égale à *l'invariant de Hasse* de la réduction mod. p (et pas seulement mod. m!) de E; elle s'exprime donc en fonction des covariants c_4 et c_6 par des formules connues (cf. [8], par exemple).]

1.12. Représentation de G définie par une courbe elliptique ayant mauvaise réduction de type multiplicatif

On suppose maintenant que la courbe elliptique E peut être écrite comme une cubique plane dont la réduction $\tilde{E}$ est une cubique irréductible de genre 0 ayant un seul point double à tangentes distinctes. Le modèle de Néron de E est de type (b_m), cf. [16], p. 124; la composante neutre de sa fibre spéciale est une «forme» du groupe multiplicatif.

Pour étudier le module galoisien E_p, le plus simple est d'utiliser la théorie de Tate (cf. [19], [22], ainsi que MG, p. IV−29 à IV−37). L'invariant modulaire j de E a une valuation <0, égale à $-m$. Il lui correspond un unique élément q de m tel que:

$$j=\frac{(1+240\sum n^3 q^n/(1-q^n))^3}{q\prod(1-q^n)^{24}}=\frac{1}{q}+744+196884q+\cdots.$$

A l'élément q est attachée une *courbe de Tate* $E(q)=\mathbf{G}_m/q^{\mathbf{Z}}$, cf. [22] ou MG, *loc. cit.* Les courbes E et $E(q)$ ont même invariant modulaire; il existe une plus petite extension K' de K sur laquelle elles deviennent isomorphes, et l'on a $[K':K]\leqq 2^3$. De plus, en utilisant le fait que le modèle de Néron de E est de type (b_m), on montre (cf. Ogg [19], § II) que K' est une extension *non ramifiée* de K; l'extension résiduelle correspondante est la plus petite extension sur laquelle les tangentes au point double de $\tilde{E}$ sont rationnelles. On en déduit (MG, p. IV−31) une suite exacte (valable sur K')

$$0\to\mu_p\to E_p\to\mathbf{Z}/p\mathbf{Z}\to 0.$$

D'où, comme dans le cas de la bonne réduction de hauteur 1:

Proposition 13 (mauvaise réduction de type multiplicatif). *L'image de I dans $\mathbf{GL}(E_p)$ est contenue dans un sous-groupe de type* $\begin{pmatrix}*&*\\0&1\end{pmatrix}$. *Les*

---

[3] De façon plus précise, on a $K'=K(\sqrt{-c_6})$, avec les notations usuelles (n° 5.1); cela résulte des deux faits suivants:

a) Pour la courbe de Tate $E(q)$, sous forme standard ([22], p. 29), on a

$$-c_6=1-504\sum_{n=1}^{\infty}n^5 q^n/(1-q^n),$$

qui est un carré puisque 504 est divisible par 8.

b) Si E' se déduit de E par «torsion» relativement à une extension quadratique K'/K, on a $K'=K(\sqrt{\alpha})$, avec $\alpha=c_6(E')/c_6(E)$.

deux caractères de I_t qui interviennent dans cette représentation sont le caractère unité et le caractère θ_{p-1}^e.

On en déduit, comme au n° précédent:

Corollaire. *Supposons que $e=1$. Alors:*

a) *Les deux caractères donnant l'action de I_t sur le semi-simplifié de E_p sont le caractère 1 et le caractère θ_{p-1}.*

b) *Si I_p opère trivialement sur E_p, l'image de I dans $\mathbf{GL}(E_p)$ est un groupe cyclique d'ordre $p-1$, représentable matriciellement par $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$.*

c) *Si I_p n'opère pas trivialement sur E_p, l'image de I est représentable matriciellement par $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.*

Ici, il est facile de donner un critère pour que l'on soit dans le cas b): il faut et il suffit que q ait une racine p-ième dans K_{nr}. Noter que cette condition entraîne

$$v(j) = -v(q) \equiv 0 \pmod{p}.$$

On en conclut que, si $v(j) \not\equiv 0 \pmod{p}$, on est nécessairement dans le cas c), cf. MG, p. IV – 37.

Remarque. A la place de la théorie de Tate, on pourrait utiliser le fait que le groupe formel $\hat{E}$ complété de E est isomorphe au *groupe formel multiplicatif* sur l'anneau des entiers de K'; en particulier, c'est un groupe de hauteur 1.

1.13. Compléments

Dans tous les exemples traités ci-dessus, on remarque que les caractères de I_t qui interviennent s'expriment en fonction des caractères fondamentaux *avec des exposants compris entre* 0 *et* e (donc égaux à 0 ou 1 lorsque $e=1$). On peut se demander si c'est là un fait général, lié à la bonne réduction (ou, plus généralement, à la réduction «semi-stable»). La réponse est affirmative. De façon précise, Raynaud vient de démontrer le résultat suivant (cf. [21] pour plus de détails):

Soit E un schéma en groupes commutatif, fini et plat sur A; on suppose que E est annulé par p; son rang est une puissance p^h de p. Soit $E_p = E(K_s)$ le groupe des points de E à valeurs dans K_s; c'est un $\mathbf{F}_p$-espace vectoriel de dimension h sur lequel opère G, et en particulier I. Soit V l'un des quotients de Jordan-Hölder du I-module E_p, et soit n sa dimension sur $\mathbf{F}_p$; posons $q=p^n$. Il existe alors sur V une structure de $\mathbf{F}_q$-espace vectoriel de dimension 1 telle que l'action de I_t sur V soit donnée par un caractère $\psi: I_t \to \mathbf{F}_q^*$ de la forme

$$\psi = \psi_1^{e(1)} \dots \psi_n^{e(n)},$$

où les ψ_i sont les différents caractères fondamentaux de I_t de niveau n, et les $e(i)$ des entiers *compris entre* 0 *et* e.

Ce résultat s'applique notamment au schéma en groupes E_p noyau de la multiplication par p dans un groupe p-divisible, ou dans une variété abélienne ayant bonne réduction.

On peut aussi se demander s'il existe des résultats analogues pour *l'homologie* (ou la cohomologie) *étale* de dimension d quelconque (le cas traité par Raynaud étant essentiellement le cas $d=1$). Plus précisément, soit X un schéma projectif lisse sur A, et soit H le d-ième groupe d'homologie étale de $X \times_A K_s$, à coefficients dans $\mathbf{Z}/p\mathbf{Z}$. Soit V un quotient de Jordan-Hölder du I-module H; posons $n=\dim. V$ et $q=p^n$. L'action de I sur V est donnée par un caractère $\psi: I_t \to \mathbf{F}_q^*$. *Est-il vrai que l'on peut écrire* ψ *sous la forme* $\psi_1^{e(1)} \ldots \psi_n^{e(n)}$ *comme ci-dessus, avec des exposants* $e(i)$ *entiers compris entre* 0 *et* e ?

On peut se poser des questions analogues pour d'autres représentations modulo p, par exemple pour celle liée à la fonction τ de Ramanujan (cf. [7], [28]): est-il vrai que les exposants $e(i)$ correspondants sont compris entre 0 et 11? Si oui, cela permettrait d'appliquer à cette représentation les arguments du § 4.

§ 2. Sous-groupes de $\mathbf{GL}_2(\mathbf{F}_p)$

Dans ce §, V désigne un espace vectoriel de dimension 2 sur le corps $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$. Le groupe $\mathbf{GL}(V)$ des automorphismes de V est isomorphe à $\mathbf{GL}_2(\mathbf{F}_p)$; on s'intéresse à ses sous-groupes.

2.1. Sous-groupes de Cartan

Il y en a de deux sortes: déployés et non déployés.

a) *Cas déployé*

Soient D_1 et D_2 deux droites distinctes de V; on a $V=D_1 \oplus D_2$. Soit C le sous-groupe de $\mathbf{GL}(V)$ formé des éléments s tels que $sD_1=D_1$ et $sD_2=D_2$. On dit que C est le *sous-groupe de Cartan* (déployé) défini par $\{D_1, D_2\}$; si l'on choisit une base de V formée d'un vecteur de D_1 et d'un vecteur de D_2, C est représentable matriciellement sous la forme $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$. Le groupe C est abélien de type $(p-1, p-1)$; si $p \neq 2$, la donnée de C détermine $\{D_1, D_2\}$ sans ambiguïté.

Soit C_1 le sous-groupe de C formé des éléments qui opèrent trivialement sur D_1. C'est un groupe cyclique d'ordre $p-1$, représentable matriciellement sous la forme $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$ (ou sous la forme $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$, cela

revient au même). Un tel sous-groupe est appelé un *demi-sous-groupe de Cartan déployé.*

Soit C' un demi-sous-groupe de Cartan déployé, et soit $C = C' \cdot \mathbf{F}_p^*$ le groupe engendré par C' et par les homothéties. Le groupe C est l'unique sous-groupe de Cartan déployé contenant C'. L'image de C dans le groupe projectif $\mathbf{PGL}(V) = \mathbf{GL}(V)/\mathbf{F}_p^*$ est égale à celle de C'; c'est un groupe cyclique d'ordre $p-1$, appelé *sous-groupe de Cartan déployé de* $\mathbf{PGL}(V)$.

b) *Cas non déployé*

Soit k une sous-algèbre de $\mathrm{End}(V)$ qui soit un corps à p^2 éléments. Le sous-groupe k^* de $\mathbf{GL}(V)$ est cyclique d'ordre p^2-1. Son image dans $\mathbf{PGL}(V)$ est cyclique d'ordre $p+1$. Un tel sous-groupe de $\mathbf{GL}(V)$ (resp. de $\mathbf{PGL}(V)$) est appelé un *sous-groupe de Cartan non déployé.*

L'intersection des sous-groupes de Cartan est le groupe $\mathbf{F}_p^*$ des homothéties. Leur réunion est l'ensemble des éléments semi-simples (i.e. d'ordre premier à p) de $\mathbf{GL}(V)$. Si $p \neq 2$, et si $s \in \mathbf{GL}(V)$ est tel que $\mathrm{Tr}(s)^2 - 4\det(s) \neq 0$, l'élément s appartient à un sous-groupe de Cartan et un seul; ce groupe est déployé si et seulement si $\mathrm{Tr}(s)^2 - 4\det(s)$ est un carré dans $\mathbf{F}_p$.

2.2. Normalisateurs des sous-groupes de Cartan

Soit C un sous-groupe de Cartan de $\mathbf{GL}(V)$; on suppose $p \neq 2$ si C est déployé. La sous-algèbre $k = \mathbf{F}_p C$ de $\mathrm{End}(V)$ engendrée par C est alors une algèbre commutative semi-simple de rang 2, et C est égal au groupe multiplicatif de k. Soit N le *normalisateur* de C dans $\mathbf{GL}(V)$. Si $s \in N$, l'application $x \mapsto sxs^{-1}$ est un automorphisme de k; si cet automorphisme est l'identité, s commute à k, donc appartient à k, et par suite à C. On en conclut que $(N:C) = 2$. Lorsque C est déployé, et correspond à $\{D_1, D_2\}$ comme ci-dessus, les éléments de $N - C$ sont les éléments $s \in \mathbf{GL}(V)$ tels que $sD_1 = D_2$ et $sD_2 = D_1$; lorsque C est non déployé, les éléments de $N - C$ sont les éléments $s \in \mathbf{GL}(V)$ tels que $s(ax) = a^p s(x)$ pour $a \in k$, $x \in V$ (i.e. ceux qui sont *semi-linéaires* pour la structure de k-espace vectoriel de V).

Soient C_1 et N_1 les images de C et N dans $\mathbf{PGL}(V)$. Le groupe N_1 est le normalisateur de C_1 dans $\mathbf{PGL}(V)$. C'est un groupe *diédral*, produit semi-direct d'un groupe $\{1, \sigma\}$ d'ordre 2 par le groupe cyclique C_1; on a $\sigma x \sigma = x^{-1}$ pour tout $x \in C_1$; tout élément de $N_1 - C_1$ est d'ordre 2.

Proposition 14. *Soient C un sous-groupe de Cartan de $\mathbf{GL}(V)$ et N son normalisateur. Soit C' un sous-groupe de Cartan* (resp. *un demi-sous-groupe de Cartan déployé*) *de $\mathbf{GL}(V)$ contenu dans N. Supposons $p \geqq 5$ si C' est déployé, et $p \geqq 3$ sinon. On a alors $C' = C$* (resp. $C' \subset C$).

Soient C_1, N_1 et C_1' les images de C, N et C' dans $\mathbf{PGL}(V)$. Vu les hypothèses faites, C_1' est cyclique d'ordre $p \pm 1 > 2$. Si s est un générateur de C_1', on a donc $s \in C_1$ (sinon s appartiendrait à $N_1 - C_1$ et serait d'ordre 2). Mais deux sous-groupes de Cartan de $\mathbf{PGL}(V)$ qui sont distincts ont pour intersection $\{1\}$. Puisque $s \in C_1 \cap C_1'$, on a donc $C_1 = C_1'$, d'où $C' \mathbf{F}_p^* = C$ et la proposition en résulte.

Remarque. La prop. 14 ne s'étend pas au cas $p=3$. En effet, dans ce cas, V possède 4 droites D_1, D_2, D_3, D_4 et les sous-groupes de Cartan déployés définis par $\{D_1, D_2\}$ et $\{D_3, D_4\}$ ont même normalisateur; en outre, ce dernier est strictement contenu dans le normalisateur d'un sous-groupe de Cartan non déployé.

2.3. Sous-groupes de Borel

Soit D une droite de V. Le sous-groupe B de $\mathbf{GL}(V)$ formé des éléments s tels que $sD = D$ est d'ordre $p(p-1)^2$; il est représentable matriciellement par $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. Un tel sous-groupe est appelé un *sous-groupe de Borel* de $\mathbf{GL}(V)$; la droite D correspondante est l'unique droite de V stable par B.

Si un sous-groupe de Cartan, ou un demi-sous-groupe de Cartan déployé, est contenu dans B, ce sous-groupe est déployé et (si $p \geqq 3$) D est l'une des deux droites qui lui sont associées.

2.4. Sous-groupes d'ordre divisible par p

Proposition 15. *Soit G un sous-groupe de $\mathbf{GL}(V)$ d'ordre divisible par p. Alors, ou bien G contient $\mathbf{SL}(V)$, ou bien G est contenu dans un sous-groupe de Borel de $\mathbf{GL}(V)$.*

(Rappelons que $\mathbf{SL}(V)$ désigne le noyau de det: $\mathbf{GL}(V) \to \mathbf{F}_p^*$.)

Tout élément x d'ordre p de $\mathbf{GL}(V)$ est représentable matriciellement sous la forme $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, donc laisse fixe une droite D_x et une seule. Si toutes les droites D_x correspondant aux éléments d'ordre p de G sont égales à une même droite D, le groupe G laisse stable D, donc est contenu dans le groupe de Borel défini par D. S'il y a au moins deux droites D_x différentes, on peut les prendre pour axes de coordonnées, et G contient des éléments x et y représentables matriciellement par:

$$x = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, \quad \text{avec } a, b \neq 0.$$

La proposition résulte alors de ce que $\mathbf{SL}_2(\mathbf{F}_p)$ est engendré par ses sous-groupes $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$, cf. par exemple Bourbaki, A, III, p. 104, prop. 17.

2.5. Sous-groupes finis exceptionnels de $\mathbf{PGL}_2(k)$

Dans ce n°, k désigne un corps commutatif; on note $\mathbf{PGL}_2(k)$ le groupe projectif $\mathbf{GL}_2(k)/k^*$.

Proposition 16. *Soit H un sous-groupe fini de $\mathbf{PGL}_2(k)$ d'ordre premier à la caractéristique car.k de k. On suppose que H n'est ni cyclique ni diédral. Alors H est isomorphe à l'un des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$. En particulier, l'ordre de H est* 12, 24 *ou* 60; *les éléments de H sont d'ordre* 1, 2, 3, 4 *ou* 5.

(Rappelons que $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$) désigne le *groupe symétrique* (resp. *alterné*) de n lettres.)

Ce résultat est bien connu lorsque k est le corps $\mathbf{C}$ des nombres complexes, cf. par exemple Weber [36], §68. On peut le déduire du fait que $\mathbf{PGL}_2(\mathbf{C})$ a pour sous-groupe compact maximal $\mathbf{SO}_3(\mathbf{R})$, de sorte que H est isomorphe à un groupe fini de rotations de $\mathbf{R}^3$ et correspond à un «polyèdre régulier» ($\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ correspondent ainsi au tétraèdre, au cube, et à l'icosaèdre).

Dans le cas général, on peut procéder de plusieurs façons. Par exemple:

1) On reprend les raisonnements donnés dans Weber, *loc. cit.*, et l'on constate qu'ils restent valables dans le cas général, du fait que l'ordre de H est premier à car. k.

2) On peut aussi, si car.$k=0$, appliquer le *principe de Lefschetz* pour se ramener à $k=\mathbf{C}$. Si car.$k=p\neq 0$, on écrit k comme corps résiduel d'un anneau de valuation discrète complet A dont le corps des fractions K est de caractéristique zéro. Du fait que l'ordre de H est premier à p, un argument standard montre que l'on peut relever H en un sous-groupe de $\mathbf{PGL}_2(A)$, donc aussi de $\mathbf{PGL}_2(K)$, et l'on est ramené au cas de caractéristique zéro.

Corollaire. *Si* car.$k=2$ *ou* 3, *tout sous-groupe fini de $\mathbf{PGL}_2(k)$ d'ordre premier à* car.k *est cyclique ou diédral.*

C'est clair.

Remarque. On peut se demander à quelle condition $\mathbf{PGL}_2(k)$ contient un sous-groupe isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$. La réponse est la suivante:

a) $\mathbf{PGL}_2(k)$ *contient* $\mathfrak{A}_4$ *si et seulement si*:
il existe $x\in k$ tel que $x^2+x=1$ (si car.$k=2$)
il existe $y, z\in k$ tels que $y^2+z^2=-1$ (si car.$k\neq 2$).

b) $\mathbf{PGL}_2(k)$ *contient* $\mathfrak{S}_4$ *si et seulement si*:
car.$k\neq 2$ et il existe $y, z\in k$ tels que $y^2+z^2=-1$.

c) $\mathbf{PGL}_2(k)$ *contient* $\mathfrak{A}_5$ *si et seulement si*:
il existe $x, y, z\in k$ tels que $x^2+x=1$ et $y^2+z^2=-1$.

(Noter que la condition portant sur (y, z) est vérifiée si car.$k\neq 0$; si car.$k=0$, elle signifie que k neutralise le corps des quaternions. Quant à la condition portant sur x, elle signifie que k contient $\sqrt{5}$ si car.$k\neq 2$, et contient $\sqrt[3]{1}$ si car.$k=2$.)

2.6. Sous-groupes d'ordre premier à p

Soit G un sous-groupe de $\mathbf{GL}(V)$ d'ordre premier à p, et soit H son image dans $\mathbf{PGL}(V)$. La prop. 16, appliquée au corps $k=\mathbf{F}_p$, montre que l'on a les possibilités suivantes:

i) H est *cyclique*, donc contenu dans un sous-groupe de Cartan de $\mathbf{PGL}(V)$, unique si $H \neq \{1\}$; on en conclut que *G est contenu dans un sous-groupe de Cartan de* $\mathbf{GL}(V)$.

ii) H est *diédral*, donc contient un sous-groupe cyclique C' non trivial d'indice 2. Le groupe C' est contenu dans un unique sous-groupe de Cartan C de $\mathbf{PGL}(V)$; comme H normalise C', il normalise aussi C. Revenant à $\mathbf{GL}(V)$, on en conclut que *G est contenu dans le normalisateur d'un sous-groupe de Cartan de* $\mathbf{GL}(V)$.

iii) H est *isomorphe à* $\mathfrak{A}_4$, $\mathfrak{S}_4$ *ou* $\mathfrak{A}_5$, ce dernier cas n'étant d'ailleurs possible que si $p \equiv \pm 1 \pmod 5$. Les éléments de H sont alors d'ordre 1, 2, 3, 4 ou 5. On en déduit facilement que, si $s \in G$, l'élément $u=\mathrm{Tr}(s)^2/\det(s)$ est égal à 4, 0, 1, 2 ou vérifie l'équation $u^2-3u+1=0$.

2.7. Sous-groupes contenant un sous-groupe de Cartan

Le résultat suivant jouera un rôle essentiel au §4:

Proposition 17. *Soit G un sous-groupe de $\mathbf{GL}(V)$ contenant un sous-groupe de Cartan C* (resp. *un demi-sous-groupe de Cartan déployé C*). *On suppose $p \neq 5$ si C est déployé. Alors*:

ou bien $G=\mathbf{GL}(V)$,
ou bien G est contenu dans un sous-groupe de Borel,
ou bien G est contenu dans le normalisateur d'un sous-groupe de Cartan.

Distinguons deux cas:

a) L'ordre de G est divisible par p

La prop. 15 du n° 2.4 montre que G est contenu dans un sous-groupe de Borel, ou contient $\mathbf{SL}(V)$. Mais, puisque G contient C, son image par det: $\mathbf{GL}(V) \to \mathbf{F}_p^*$ est égale à $\mathbf{F}_p^*$ tout entier. On en conclut que, si G contient $\mathbf{SL}(V)$, il est nécessairement égal à $\mathbf{GL}(V)$.

b) L'ordre de G n'est pas divisible par p

Soit H l'image de G dans $\mathbf{PGL}(V)$. D'après le n° 2.6, tout revient à montrer que H est cyclique ou diédral, i.e. n'est pas isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$. C'est clair si $p=2$ ou 3. Supposons donc $p \geqq 5$. L'image C_1 de C dans $\mathbf{PGL}(V)$ est cyclique d'ordre $p \pm 1 \geqq 6$ (grâce au fait que l'on suppose $p \geqq 7$ lorsque C est déployé). Comme $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ ne contiennent pas

d'élément d'ordre $\geqq 6$, on voit bien que H ne peut être isomorphe à aucun de ces groupes.

Remarque. Lorsque $p=5$ et que C est déployé, il y a une quatrième possibilité: l'image de G dans $\mathbf{PGL}(V)$ peut être isomorphe à $\mathfrak{S}_4$. Ce cas est caractérisé par le fait que la fonction $s \mapsto \mathrm{Tr}(s)^2/\det(s)$ prend sur G la valeur 1 et ne prend pas la valeur 3.

Le cas où G est *distingué* est beaucoup plus simple:

Proposition 18. *Soit G un sous-groupe de $\mathbf{GL}(V)$ contenant un sous-groupe de Cartan C* (resp. *un demi-sous-groupe de Cartan déployé C*). *On suppose $p \neq 2$ et G distingué dans $\mathbf{GL}(V)$. Alors $G = \mathbf{GL}(V)$.*

Supposons $p \geqq 5$. D'après un résultat connu (cf. par exemple Artin [1], chap. IV, th. 4.9), le fait que G soit distingué dans $\mathbf{GL}(V)$ entraîne, soit que G est contenu dans le centre de $\mathbf{GL}(V)$, soit que G contient $\mathbf{SL}(V)$. Le premier cas est exclu puisque G contient C; le second entraîne $G = \mathbf{GL}(V)$ du fait que $\det(C) = \mathbf{F}_p^*$.

Si $p=3$, on peut identifier $\mathbf{PGL}(V)$ au groupe $\mathfrak{S}_4$ et l'image H de G dans $\mathbf{PGL}(V)$ devient un sous-groupe distingué de $\mathfrak{S}_4$. Si C est déployé (resp. non déployé), H contient une transposition (resp. un cycle d'ordre 4); il en résulte facilement que $H = \mathfrak{S}_4$, donc que l'ordre de G est divisible par 3. Comme G n'est pas contenu dans un sous-groupe de Borel, la prop. 15 montre que G contient $\mathbf{SL}(V)$, et l'on conclut comme ci-dessus.

2.8. Un critère pour que $G = \mathbf{GL}(V)$

Soit G un sous-groupe de $\mathbf{GL}(V)$. La prop. 17 fournit un critère pour que $G = \mathbf{GL}(V)$: pour $p \geqq 7$, il suffit que G contienne un sous-groupe de Cartan, et ne soit contenu, ni dans un sous-groupe de Borel, ni dans le normalisateur d'un sous-groupe de Cartan. Voici un critère un peu différent:

Proposition 19. *Supposons $p \geqq 5$ et faisons les hypothèses suivantes:*

i) *G contient un élément s tel que $\mathrm{Tr}(s)^2 - 4\det(s)$ soit un carré $\neq 0$ dans $\mathbf{F}_p$, et que $\mathrm{Tr}(s) \neq 0$.*

ii) *G contient un élément s' tel que $\mathrm{Tr}(s')^2 - 4\det(s')$ ne soit pas un carré dans $\mathbf{F}_p$, et que $\mathrm{Tr}(s') \neq 0$.*

iii) *G contient un élément s'' tel que $u = \mathrm{Tr}(s'')^2/\det(s'')$ soit distinct de 0, 1, 2 et 4 et soit tel que $u^2 - 3u + 1 \neq 0$.*

Alors G contient $\mathbf{SL}(V)$. En particulier, si det: $G \to \mathbf{F}_p^*$ *est surjectif, on a $G = \mathbf{GL}(V)$.*

Distinguons encore deux cas:

a) L'ordre de G est divisible par p

Si G ne contenait pas $\mathbf{SL}(V)$, G serait contenu dans un sous-groupe de Borel (prop. 15), et les valeurs propres des éléments de G appartiendraient toutes à $\mathbf{F}_p$, ce qui contredirait ii).

b) L'ordre de G n'est pas divisible par p

Soit H l'image de G dans $\mathbf{PGL}(V)$. La condition iii) montre que H ne peut pas être isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$, cf. n° 2.6.

Ainsi, H est cyclique ou diédral, et G est contenu dans le normalisateur N d'un sous-groupe de Cartan C. Si C est déployé, l'élément s' ne peut appartenir, ni à C (car $\mathrm{Tr}(s')^2-4\det(s')$ serait un carré), ni à $N-C$ (car $\mathrm{Tr}(s')$ serait 0). Si C n'est pas déployé, le même argument montre que s ne peut appartenir, ni à C, ni à $N-C$. Le cas b) est donc impossible.

Corollaire ([32], lemme 4). *Faisons l'hypothèse suivante*:

(*) *Quels que soient* $t\in\mathbf{F}_p$, $d\in\mathbf{F}_p^*$, *il existe* $s\in G$ *tel que* $\mathrm{Tr}(s)=t$ *et* $\det(s)=d$.

Alors, si $p\geqq 5$, *on a* $G=\mathbf{GL}(V)$.

En effet, les conditions (i) à (iii) sont satisfaites, et l'homomorphisme det: $G\to\mathbf{F}_p^*$ est surjectif.

Remarque. Lorsque $p=2$ (resp. $p=3$), l'hypothèse (*) n'entraîne pas que $G=\mathbf{GL}(V)$. Elle entraîne seulement que G contient le 3-groupe de Sylow (resp. un 2-groupe de Sylow) de $\mathbf{GL}(V)$. Plus précisément:

si $p=2$, on a $\mathbf{GL}(V)\simeq\mathfrak{S}_3$, et, pour que G contienne le sous-groupe d'ordre 3 de $\mathbf{GL}(V)$, il faut et il suffit qu'il existe $s\in G$ tel que $\mathrm{Tr}(s)=1$;

si $p=3$, on a $\mathbf{PGL}(V)\simeq\mathfrak{S}_4$, et, pour que G contienne un 2-groupe de Sylow de $\mathbf{GL}(V)$ (i.e. un normalisateur de sous-groupe de Cartan non déployé), il faut et il suffit qu'il existe $s, s'\in G$ tels que

$$\det(s)=\det(s')=-1 \quad \text{et} \quad \mathrm{Tr}(s)=0,\ \mathrm{Tr}(s')=\pm 1.$$

§ 3. Systèmes de représentations abéliennes modulo l

3.1. Notations

Ce sont celles de MG, chap. II. Rappelons-les brièvement:

K est un corps de nombres algébriques (i.e. une extension finie de $\mathbf{Q}$), de clôture algébrique $\overline{K}$;

O_K est l'anneau des entiers de K, et $E=O_K^*$ est le groupe des unités de K;

Σ est l'ensemble des places ultramétriques de K, et Σ^∞ l'ensemble des places archimédiennes; on pose $\overline{\Sigma}=\Sigma\cup\Sigma^\infty$.

K_v est le complété de K en v ($v \in \bar{\Sigma}$);

U_v, k_v, Nv, p_v sont respectivement le groupe des unités, le corps résiduel, le nombre d'éléments du corps résiduel et la caractéristique résiduelle du corps local K_v ($v \in \Sigma$).

I est le groupe des idèles de K; si $a \in I$ et $v \in \bar{\Sigma}$, on note a_v la composante de a en v; on a $a_v \in K_v^*$ pour tout $v \in \bar{\Sigma}$, et $a_v \in U_v$ pour presque tout v;

$C = I/K^*$ est le groupe des classes d'idèles de K.

On se donne une partie finie S de Σ ainsi qu'un *module* $\mathfrak{m} = (m_v)_{v \in S}$ de support S, les m_v étant des entiers $\geqq 1$. On définit $U_{v,\mathfrak{m}}$ comme la composante neutre de K_v^* si $v \in \Sigma^\infty$, le groupe U_v si $v \in \Sigma - S$, et le sous-groupe de U_v formé des éléments x tels que $v(1-x) \geqq m_v$ si $v \in S$. Le groupe $U_{\mathfrak{m}} = \prod_v U_{v,\mathfrak{m}}$ est un sous-groupe ouvert de I. On pose $E_{\mathfrak{m}} = E \cap U_{\mathfrak{m}}$ et $C_{\mathfrak{m}} = I/K^* U_{\mathfrak{m}}$, de sorte que l'on a la suite exacte

$$0 \to K^*/E_{\mathfrak{m}} \to I/U_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 0.$$

Le groupe $C_{\mathfrak{m}}$ peut aussi s'interpréter comme le groupe des classes (mod. $\mathfrak{m}$) d'idéaux premiers à S; c'est un groupe fini; son ordre est noté $h_{\mathfrak{m}}$.

La limite projective des $C_{\mathfrak{m}}$ (pour $\mathfrak{m}$ variable) est égale au quotient de C par sa composante neutre; d'après la théorie du corps de classes ([5], [42]), ce quotient s'identifie à $\mathrm{Gal}(K^{ab}/K)$ où K^{ab} est la clôture abélienne de K dans $\bar{K}$. En particulier, on a, pour tout $\mathfrak{m}$, un homomorphisme canonique

$$\mathrm{Gal}(K^{ab}/K) \to C_{\mathfrak{m}}$$

qui est surjectif; le groupe $C_{\mathfrak{m}}$ s'identifie ainsi au groupe de Galois de la plus grande extension abélienne de K de conducteur $\leqq \mathfrak{m}$.

3.2. Les groupes algébriques T, $T_{\mathfrak{m}}$ et $S_{\mathfrak{m}}$

Ce sont des groupes algébriques affines sur $\mathbf{Q}$, définis dans MG, chap. II, n^{os} 1.1 et 2.2:

Le groupe T est le tore qui «représente le groupe multiplicatif de K»; de façon plus précise, pour toute $\mathbf{Q}$-algèbre commutative A, le groupe $T(A)$ des points de T à valeurs dans A est égal au groupe $(K \otimes_{\mathbf{Q}} A)^*$ des éléments inversibles de $K \otimes_{\mathbf{Q}} A$; en particulier, on a $T(\mathbf{Q}) = K^*$.

Le groupe $T_{\mathfrak{m}}$ est le tore quotient de T par l'adhérence de $E_{\mathfrak{m}}$ pour la topologie de Zariski (cela a un sens, puisque $E_{\mathfrak{m}}$ est contenu dans $K^* = T(\mathbf{Q})$).

Le groupe $S_{\mathfrak{m}}$ est extension du groupe fini $C_{\mathfrak{m}}$ (considéré comme groupe algébrique «constant», de dimension 0) par le tore $T_{\mathfrak{m}}$. Il est muni

d'un homomorphisme $I/U_m \to S_m(\mathbf{Q})$ rendant commutatif le diagramme:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^*/E_m & \longrightarrow & I/U_m & \longrightarrow & C_m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id.}} & & \\ 0 & \longrightarrow & T_m(\mathbf{Q}) & \longrightarrow & S_m(\mathbf{Q}) & \longrightarrow & C_m & \longrightarrow & 0. \end{array}$$

3.3. Caractères de T, T_m et S_m

Soit $\bar{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$. Si G est un groupe algébrique sur $\mathbf{Q}$, nous appellerons *groupe des caractères de* G, et nous noterons $X(G)$, le groupe des $\bar{\mathbf{Q}}$-homomorphismes de $G_{/\bar{\mathbf{Q}}}$ dans le groupe multiplicatif $\mathbf{G}_{m/\bar{\mathbf{Q}}}$. Ceci s'applique notamment aux groupes T, T_m et S_m; nous allons expliciter les groupes de caractères correspondants.

Soit Γ l'ensemble des plongements de K dans $\bar{\mathbf{Q}}$. A tout élément σ de Γ est attaché un caractère $[\sigma]$ de T (MG, chap. II, n° 1.1), et l'on a

$$[\sigma](x)=\sigma(x) \quad \text{si } x\in T(\mathbf{Q})=K^*.$$

Les caractères $[\sigma]$ forment une base du groupe $X(T)$. Tout élément φ de $X(T)$ s'écrit donc de façon unique (en notation multiplicative):

$$\varphi=\prod_{\sigma\in\Gamma}[\sigma]^{n(\sigma)}, \quad \text{avec } n(\sigma)\in\mathbf{Z}.$$

Nous dirons que les $n(\sigma)$ sont les *exposants* de φ.

Comme $T_m=T/\bar{E}_m$, le groupe $X(T_m)$ s'identifie au sous-groupe de $X(T)$ formé des caractères φ du type ci-dessus tels que l'on ait

$$\varphi(x)=\prod_{\sigma\in\Gamma}\sigma(x)^{n(\sigma)}=1 \quad \text{pour tout } x\in E_m.$$

Enfin, la construction de S_m donnée dans MG, chap. II, n° 2.2 montre qu'un élément de $X(S_m)$ est un couple (φ, f), où $\varphi\in X(T)$, et $f\in\mathrm{Hom}(I, \bar{\mathbf{Q}}^*)$, avec:

i) $f(x)=1$ pour tout $x\in U_m$,

ii) $f(x)=\varphi(x)$ pour tout $x\in K^*$.

Ces deux propriétés entraînent que $\varphi(x)=1$ pour tout $x\in E_m$, i.e. on a $\varphi\in X(T_m)$. D'autre part, la propriété ii) montre que la connaissance de f détermine celle de φ.

La suite exacte $0\to T_m\to S_m\to C_m\to 0$ donne par transposition la suite exacte:

$$0\to X(C_m)\to X(S_m)\to X(T_m)\to 0,$$

où $X(C_m)=\mathrm{Hom}(C_m, \bar{\mathbf{Q}}^*)$ est le dual du groupe fini C_m. En particulier, tout caractère φ de T_m peut être prolongé en un caractère (φ, f) de S_m, et les divers prolongement possibles sont en nombre égal à $h_m=\mathrm{Card}(C_m)$.

Remarques. 1) Le groupe $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ opère de façon évidente sur $X(T)$, $X(T_{\mathfrak{m}})$ et $X(S_{\mathfrak{m}})$ qui se trouvent ainsi munis de structures de *modules galoisiens*; ces modules permettent d'ailleurs de reconstituer T, $T_{\mathfrak{m}}$ et $S_{\mathfrak{m}}$ puisque ces groupes sont des groupes algébriques «de type multiplicatif».

2) Les caractères de $S_{\mathfrak{m}}$ sont substantiellement identiques aux caractères de C de conducteur $\leqq \mathfrak{m}$ et «de type (A_0)» au sens de Weil [39]. Comme Weil lui-même l'a montré, ces caractères jouent un rôle essentiel aussi bien dans la multiplication complexe (cf. [40], ainsi que [30], § 7) que dans l'arithmétique (et l'homologie) des variétés d'équations

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0 \qquad \text{(cf. [37], [38])}.$$

3.4. Représentations de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ définies par un caractère de $S_{\mathfrak{m}}$

Introduisons d'abord quelques notations:

Soit l un nombre premier. On dit que $v \in \Sigma$ *divise* l si $p_v = l$, et l'on écrit alors $v|l$. On pose:

$$K_l = \prod_{v|l} K_v = K \otimes \mathbf{Q}_l.$$

Le groupe multiplicatif $K_l^* = \prod_{v|l} K_v^*$ s'identifie de façon naturelle à un facteur direct du groupe I des idèles de K. Si $a \in I$, on note a_l la composante de a dans K_l^*; on a $a_l = (a_v)_{v|l}$. On pose également:

$$U_l = \prod_{v|l} U_v \quad \text{et} \quad U_{l,\mathfrak{m}} = \prod_{v|l} U_{v,\mathfrak{m}}.$$

D'autre part, on *choisit* une valuation v_l de $\bar{\mathbf{Q}}$ prolongeant la valuation l-adique de $\mathbf{Q}$. Le complété $\bar{\mathbf{Q}}_l$ de $\bar{\mathbf{Q}}$ pour v_l est une clôture algébrique de $\mathbf{Q}_l$. On note O_l (resp. $\mathfrak{p}_l$, resp. k_l) l'anneau (resp. l'idéal, resp. le corps résiduel) de v_l étendue à $\bar{\mathbf{Q}}_l$; le corps k_l est une clôture algébrique du corps premier $\mathbf{F}_l$.

Tout plongement σ de K dans $\bar{\mathbf{Q}}$ s'étend par linéarité en un homomorphisme de $\mathbf{Q}_l$-algèbres σ_l: $K_l \to \bar{\mathbf{Q}}_l$; cet homomorphisme est trivial sur toutes les composantes K_v de K_l sauf une (celle correspondant à l'unique v qui soit équivalente à $v_l \circ \sigma$). Inversement, tout $\mathbf{Q}_l$-homomorphisme de K_l dans $\bar{\mathbf{Q}}_l$ est de la forme σ_l, pour un élément $\sigma \in \Gamma$ bien déterminé. Enfin, si $\varphi = \prod_{\sigma \in \Gamma} [\sigma]^{n(\sigma)}$ est un caractère du tore T, on note φ_l l'homomorphisme de $K_l^* = T(\mathbf{Q}_l)$ dans $\bar{\mathbf{Q}}_l^*$ défini par la formule

$$\varphi_l(x) = \prod_{\sigma \in \Gamma} \sigma_l(x)^{n(\sigma)}.$$

Nous pouvons maintenant définir le *caractère l-adique* de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ attaché à un caractère de $S_{\mathfrak{m}}$:

Soit $\psi=(\varphi, f)$ un élément de $X(S_{\mathfrak{m}})$, cf. n° 3.3. Si a est un idèle de K, posons

$$\psi_l(a)=f(a)\,\varphi_l(a_l^{-1}). \tag{1}$$

On obtient ainsi un homomorphisme $\psi_l\colon I\to\overline{\mathbf{Q}}_l^*$ dont on vérifie tout de suite (cf. MG, chap. II, § 2) qu'il est continu, et égal à 1 sur K^*; par passage au quotient, il définit un homomorphisme continu de $C=I/K^*$ dans $\overline{\mathbf{Q}}_l^*$, homomorphisme qui est trivial sur la composante neutre de C, puisque $\overline{\mathbf{Q}}_l^*$ est totalement discontinu. Vu la théorie du corps de classes, on obtient finalement un *homomorphisme continu*

$$\psi_l\colon \mathrm{Gal}(K^{\mathrm{ab}}/K)\to\overline{\mathbf{Q}}_l^*,$$

i.e. un «caractère l-adique» du groupe de Galois $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

[On peut aussi définir ψ_l comme le composé de l'homomorphisme

$$\varepsilon_l\colon \mathrm{Gal}(K^{\mathrm{ab}}/K)\to S_{\mathfrak{m}}(\mathbf{Q}_l) \qquad \text{(cf. MG, p. II}-11),$$

avec l'homomorphisme de $S_{\mathfrak{m}}(\mathbf{Q}_l)$ dans $\overline{\mathbf{Q}}_l^*$ défini par le caractère ψ.]

Du fait que $f=1$ sur $U_{\mathfrak{m}}$, on a:

$$\psi_l(a)=\varphi_l(a_l^{-1})=\prod_{\sigma\in\Gamma}\sigma_l(a_l^{-1})^{n(\sigma)} \qquad \text{pour tout } a\in U_{\mathfrak{m}}, \tag{2}$$

où les entiers $n(\sigma)$ sont les *exposants* de φ.

L'image de ψ_l est compacte, donc contenue dans le groupe des unités de $\overline{\mathbf{Q}}_l$. Par réduction (mod. $\mathfrak{p}_l$) on déduit donc de ψ_l un «caractère modulo l»

$$\tilde{\psi}_l\colon \mathrm{Gal}(K^{\mathrm{ab}}/K)\to k_l^*.$$

L'image de $\tilde{\psi}_l$ est un sous-groupe *fini* (car discret et compact) de k_l^*. La formule (2) donne:

$$\tilde{\psi}_l(a)\equiv\prod_{\sigma\in\Gamma}\sigma_l(a_l^{-1})^{n(\sigma)} \quad (\mathrm{mod.}\,\mathfrak{p}_l) \qquad \text{pour tout } a\in U_{\mathfrak{m}}. \tag{3}$$

Il y a intérêt pour la suite à récrire (3) comme conjonction des deux propriétés suivantes:

(3_1) On a $\tilde{\psi}_l(a)=1$ pour tout $a\in U_{v,\mathfrak{m}}$ si v ne divise pas l.

(3_2) Si v divise l, notons $\Gamma(v)$ la partie de Γ formée des plongements $\sigma\colon K\to\mathbf{Q}_l$ tels que $v_l\circ\sigma$ soit équivalente à v. Si $\sigma\in\Gamma(v)$, σ se prolonge en un plongement de K_v dans $\overline{\mathbf{Q}}_l$, et définit par passage aux corps résiduels un plongement $\tilde{\sigma}_l$ de k_v dans k_l. On a alors

$$\tilde{\psi}_l(a)=\prod_{\sigma\in\Gamma(v)}\tilde{\sigma}_l(\tilde{a}^{-1})^{n(\sigma)} \qquad \text{pour tout } a\in U_{v,\mathfrak{m}},$$

où $\tilde{a}$ désigne l'image de a dans k_v^*.

Remarque. Si $v \notin S = \mathrm{Supp}(\mathfrak{m})$, les propriétés (3_1) et (3_2) donnent $\tilde{\psi}_l$ sur U_v tout entier; vu la théorie du corps de classes, on connaît la restriction de $\tilde{\psi}_l$ au *sous-groupe d'inertie* I_v de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ relatif à v:

a) si v ne divise pas l, on a $\tilde{\psi}_l(I_v) = \{1\}$, i.e. $\tilde{\psi}_l$ est *non ramifiée en* v;

b) si v divise l, la restriction de $\tilde{\psi}_l$ à I_v est le produit des caractères $\alpha \mapsto \tilde{\sigma}_l(\alpha^{-1})$ $(\sigma \in \Gamma(v))$ affectés des exposants $n(\sigma)$. (Noter que, d'après la prop. 3 du n° 1.5, chacun des caractères $\alpha \mapsto \tilde{\sigma}_l(\alpha^{-1})$ est un *caractère fondamental* du groupe d'inertie modérée en v.)

3.5. Réciproque: passage d'un système de caractères (mod. l) à un élément de $X(S_{\mathfrak{m}})$

Dans l'énoncé qui suit, L désigne un ensemble *infini* de nombres premiers. Pour tout $l \in L$, on se donne un homomorphisme continu

$$\theta_l : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to k_l^*;$$

on identifie θ_l, *via* la théorie du corps de classes, à un homomorphisme de I dans k_l^*.

Proposition 20. *Supposons qu'il existe une famille d'entiers $n(\sigma, l)$, où σ parcourt Γ et l parcourt L, telle que:*

i) *les valeurs absolues des $n(\sigma, l)$ sont bornées par un entier N indépendant de σ, l;*

ii) *pour tout $l \in L$ et tout $a \in U_{\mathfrak{m}}$, on a*

$$\theta_l(a) \equiv \prod_{\sigma \in \Gamma} \sigma_l(a_l^{-1})^{n(\sigma, l)} \pmod{\mathfrak{p}_l}. \tag{4}$$

Il existe alors $\psi \in X(S_{\mathfrak{m}})$ tel que $\tilde{\psi}_l = \theta_l$ pour une infinité de valeurs de l.

Comme les $n(\sigma, l)$ ne peuvent prendre qu'un nombre fini de valeurs, et que L est infini, il existe une partie infinie L' de L telle que $n(\sigma, l)$ soit indépendant de l pour $l \in L'$; notons $n(\sigma)$ la valeur commune des $n(\sigma, l)_{l \in L'}$ et soit φ le caractère de T ayant pour exposants les $n(\sigma)$. Nous allons voir que φ *est un caractère de* $T_{\mathfrak{m}}$, i.e. que $x \in E_{\mathfrak{m}}$ entraîne $\varphi(x) = 1$. Considérons x comme un idèle (principal) du corps K. On a $\theta_l(x) = 1$ pour tout $l \in L$. D'autre part, puisque x appartient à $U_{\mathfrak{m}}$, l'hypothèse ii) montre que l'on a

$$\theta_l(x) \equiv \prod_{\sigma \in \Gamma} \sigma(x^{-1})^{n(\sigma)} \equiv \varphi(x^{-1}) \pmod{\mathfrak{p}_l} \qquad \text{pour tout } l \in L'.$$

On a donc $\varphi(x) \equiv 1 \pmod{\mathfrak{p}_l}$ pour une infinité de valeurs de l, ce qui entraîne bien $\varphi(x) = 1$ (en effet, un élément non nul de $\overline{\mathbf{Q}}$ n'appartient qu'à un nombre *fini* des $\mathfrak{p}_l$).

Puisque φ est un caractère de $T_{\mathfrak{m}}$, il se prolonge (cf. n° 3.3) en un caractère $\chi = (\varphi, f)$ de $S_{\mathfrak{m}}$. Soit $\tilde{\chi}_l$ le caractère (mod. l) associé à χ, et

posons

$$\theta'_l = \tilde{\chi}_l \theta_l^{-1} \quad \text{pour tout } l \in L'.$$

Comme $\tilde{\chi}_l$ et θ_l satisfont à (4) avec les mêmes exposants $n(\sigma)$, on a $\theta'_l(a)=1$ pour tout $a \in U_{\mathfrak{m}}$, autrement dit θ'_l s'identifie à un *homomorphisme de* $C_{\mathfrak{m}}$ *dans* k_l^*; ses valeurs appartiennent au groupe $H_{\mathfrak{m},l}$ des racines $h_{\mathfrak{m}}$-ièmes de l'unité de k_l, avec $h_{\mathfrak{m}} = \mathrm{Card}(C_{\mathfrak{m}})$. Quitte à diminuer un peu L', on peut supposer qu'aucun élément l de L' ne divise $h_{\mathfrak{m}}$. Si $H_{\mathfrak{m}}$ désigne le groupe des racines $h_{\mathfrak{m}}$-ièmes de l'unité de $\bar{\mathbf{Q}}$, la réduction modulo $\mathfrak{p}_l$ définit alors un isomorphisme de $H_{\mathfrak{m}}$ sur $H_{\mathfrak{m},l}$ et θ'_l se relève en un homomorphisme θ''_l: $C_{\mathfrak{m}} \to H_{\mathfrak{m}}$. Comme $C_{\mathfrak{m}}$ et $H_{\mathfrak{m}}$ sont finis, il existe une partie infinie L'' de L' telle que θ''_l soit égal à un même homomorphisme θ'' pour tout $l \in L''$. On a $\theta'' \in X(C_{\mathfrak{m}})$, d'où $\theta'' \in X(S_{\mathfrak{m}})$ et le caractère $\psi = \theta''^{-1}\chi$ est tel que $\tilde{\psi}_l = \theta_l'^{-1}\tilde{\chi}_l = \theta_l$ pour tout $l \in L''$, ce qui démontre la proposition.

Remarque. La prop. 20 porte sur un *ensemble infini* de nombres premiers, et c'est sous cette forme que nous l'utiliserons. Il est toutefois possible de la reformuler «en termes finis»; voici l'énoncé auquel on arrive:

Proposition 20′. *Pour* $\mathfrak{m}$ *et* $n(\sigma)_{\sigma \in \Gamma}$ *donnés, il existe une constante* l_0 *telle que, si* $l \geqq l_0$, *et si* θ: $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to k_l^*$ *est un homomorphisme tel que*

$$\theta(a) \equiv \prod_{\sigma \in \Gamma} \sigma_l(a_l^{-1})^{n(\sigma)} \quad (\mathrm{mod.}\, \mathfrak{p}_l) \qquad \textit{pour tout } a \in U_{\mathfrak{m}},$$

il existe un caractère $\psi = (\varphi, f)$ *de* $S_{\mathfrak{m}}$ *et un seul tel que* $\tilde{\psi}_l = \theta$ *et que les exposants de* φ *soient égaux aux* $n(\sigma)$.

De plus, la constante l_0 est *effectivement calculable* à partir de K, $\mathfrak{m}$ et des $n(\sigma)$.

3.6. Application à certains systèmes de représentations l-adiques

Soit P l'ensemble des nombres premiers. Dans ce qui suit, $(\rho_l)_{l \in P}$ désigne un *système de représentations l-adiques de* K: pour tout $l \in P$, on se donne un espace vectoriel V_l de dimension finie sur $\mathbf{Q}_l$, et un homomorphisme continu

$$\rho_l\colon \mathrm{Gal}(\bar{K}/K) \to \mathbf{GL}(V_l).$$

On suppose en outre que les ρ_l sont *semi-simples, rationnelles* (MG, p. I−9) et forment un système *strictement compatible* (MG, p. I−11). Rappelons que les deux dernières propriétés équivalent à l'existence d'une partie finie S_ρ de Σ jouissant des propriétés (i) et (ii) que voici:

(i) *Si* $v \in \Sigma - S_\rho$, *et si* $l \neq p_v$, *la représentation* ρ_l *est* non ramifiée *en* v.

On peut alors parler de *l'élément de Frobenius* F_{w,ρ_l} de $\mathrm{Im}(\rho_l)$ attaché à un prolongement w de v à $\bar{K}$ (MG, p. I−7). Sa classe de conjugaison

ne dépend que de v; en particulier, si t est une indéterminée, le polynôme

$$P_{v,\rho_l}(t)=\det(1-tF_{w,\rho_l})$$

ne dépend que de v et l.

(ii) *Pour tout* $v\in\Sigma-S_\rho$, *il existe un polynôme* $P_v(t)$ *à coefficients dans* $\mathbf{Q}$ *tel que* $P_v(t)=P_{v,\rho_l}(t)$ *pour tout* $l\neq p_v$.

Voici deux conséquences de (i) et (ii):

(iii) Les V_l ont *même dimension*; on la notera d.

(iv) Pour tout $l\in P$, $\mathrm{Im}(\rho_l)$ est compact, donc laisse stable un $\mathbf{Z}_l$-*réseau* T_l de V_l (MG, p. I−1); il en résulte que, pour tout $\alpha\in\mathrm{Im}(\rho_l)$ les coefficients de $\det(1-t\alpha)$ appartiennent à $\mathbf{Z}_l$. Vu (ii), les coefficients de $P_v(t)$ appartiennent donc à $\mathbf{Z}_l$ pour tout $l\neq p_v$, i.e. *ce sont des éléments de* $\mathbf{Z}[1/p_v]$.

Exemples de systèmes (ρ_l) vérifiant les conditions ci-dessus:

(1) le système défini par une *courbe elliptique* (cf. §4 ainsi que MG, chap. IV);

(2) le système (φ_l) attaché à une représentation linéaire

$$\varphi_0\colon S_m\to\mathbf{GL}_d$$

du groupe algébrique S_m (MG, p. II−19); noter que ce système est *abélien*, i.e. que, pour tout l, $\mathrm{Im}(\varphi_l)$ est abélien, de sorte que φ_l s'identifie à un homomorphisme continu de $\mathrm{Gal}(K^{ab}/K)$ dans $\mathbf{GL}(V_l)$.

Revenons au cas général. Soit $l\in P$, et soit T_l comme ci-dessus un $\mathbf{Z}_l$-réseau de V_l stable par $\mathrm{Im}(\rho_l)$. Le groupe $\mathrm{Gal}(\overline{K}/K)$ opère sur T_l/lT_l; nous noterons $\tilde{V}_l$ le *semi-simplifié* de T_l/lT_l pour l'action en question, et nous noterons $\tilde{\rho}_l$ l'homomorphisme correspondant de $\mathrm{Gal}(\overline{K}/K)$ dans $\mathbf{GL}(\tilde{V}_l)$; c'est une représentation linéaire de degré d de $\mathrm{Gal}(\overline{K}/K)$ sur le corps $\mathbf{F}_l$. D'après Brauer-Nesbitt (cf. [6], §82.1), $\tilde{\rho}_l$ ne dépend pas (à isomorphisme près) du choix de T_l; nous dirons, par abus de langage, que c'est la *réduction* (mod. l) de ρ_l.

Si $\tilde{\rho}_l$ est *abélienne* (i.e. a pour image un groupe abélien), on peut la mettre *sous forme diagonale* après extension des scalaires de $\mathbf{F}_l$ à sa clôture algébrique k_l (cf. n° 3.4); on obtient d caractères

$$\theta_l^{(i)}\colon \mathrm{Gal}(K^{ab}/K)\to k_l^*,\qquad i=1,\ldots,d.$$

Nous les identifierons, comme d'habitude, à des homomorphismes de I dans k_l^*.

Venons-en maintenant au principal résultat de ce §:

Théorème 1. *Soit* (ρ_l) *un système de représentations l-adiques semi-simples de K ayant les propriétés* (i) *et* (ii) *ci-dessus. Supposons qu'il existe un entier N et une partie infinie L de P jouissant de la propriété suivante*:

(*) *Pour tout* $l \in L$, *la réduction* $\tilde{\rho}_l$ *de* ρ_l (mod. l) *est abélienne, et, si* $\theta_l^{(i)}$: $I \to k_l^*$ *est un caractère intervenant dans* $\tilde{\rho}_l$, *il existe des entiers* $n(\sigma, l, i)_{\sigma \in \Gamma}$, *inférieurs à* N *en valeur absolue, tels que*

$$\theta_l^{(i)}(a) \equiv \prod_{\sigma \in \Gamma} \sigma_l(a_l^{-1})^{n(\sigma, l, i)} \quad \text{(mod. } \mathfrak{p}_l) \qquad \text{pour tout } a \in U_{\mathfrak{m}}.$$

Le système (ρ_l) *est alors isomorphe au système* (φ_l) *associé à une représentation* φ_0: $S_{\mathfrak{m}} \to \mathbf{GL}_d$ *définie sur* $\mathbf{Q}$ (cf. exemple 2 ci-dessus).

En particulier:

Corollaire. *Pour tout* $l \in P$, ρ_l *est abélienne.*

Vu (*), les $(\theta_l^{(1)})_{l \in L}$ satisfont aux hypothèses de la prop. 20. Il existe donc une partie infinie L_1 de L et un caractère $\psi^{(1)}$ de $S_{\mathfrak{m}}$ tels que $\tilde{\psi}_l^{(1)} = \theta_l^{(1)}$ pour tout $l \in L_1$. De même, en appliquant la prop. 20 aux $(\theta_l^{(2)})_{l \in L_1}$ on obtient une partie infinie L_2 de L_1 et un caractère $\psi^{(2)}$ de $S_{\mathfrak{m}}$ tels que $\tilde{\psi}_l^{(2)} = \theta_l^{(2)}$ pour tout $l \in L_2$. En répétant cet argument, on obtient finalement une partie infinie L' de L et des caractères $\psi^{(i)}$, $i = 1, \ldots, d$, de $S_{\mathfrak{m}}$ tels que $\tilde{\psi}_l^{(i)} = \theta_l^{(i)}$ pour tout $l \in L'$.

Soit φ la représentation de $S_{\mathfrak{m}/\bar{\mathbf{Q}}}$ dans $\mathbf{GL}_{d/\bar{\mathbf{Q}}}$ somme directe des d représentations de degré 1 fournies par les caractères $\psi^{(i)}$. Si $v \in \Sigma - S$, soit f_v un idèle dont la v-ième composante est une uniformisante de K_v et dont les autres composantes sont égales à 1, et soit $F_v \in S_{\mathfrak{m}}(\mathbf{Q})$ l'image de f_v par l'homomorphisme canonique ε: $I \to S_{\mathfrak{m}}(\mathbf{Q})$, cf. MG, p. II – 11; on a $\varphi(F_v) \in \mathbf{GL}_d(\bar{\mathbf{Q}})$.

Lemme 1. *Si* $v \in \Sigma - (S_\rho \cup S)$, *on a* $\det(1 - t\varphi(F_v)) = P_v(t)$.

Posons

$$P_v'(t) = \det(1 - t\varphi(F_v)) = \prod_{i=1}^{d} (1 - t\psi^{(i)}(F_v)).$$

Si $l \neq p_v$, on a $\psi^{(i)}(F_v) = \psi_l^{(i)}(f_v)$ d'après la formule (1) du n° 3.4; si en outre l appartient à L', on en déduit que

$$\psi^{(i)}(F_v) \equiv \psi_l^{(i)}(f_v) \equiv \theta_l^{(i)}(f_v) \quad \text{(mod. } \mathfrak{p}_l),$$

d'où

$$P_v'(t) \equiv \prod (1 - t\,\theta_l^{(i)}(f_v)) \quad \text{(mod. } \mathfrak{p}_l).$$

Mais les $\theta_l^{(i)}(f_v)$ sont les valeurs propres de l'élément de Frobenius attaché à v dans la représentation $\tilde{\rho}_l$. On a donc

$$\prod (1 - t\,\theta_l^{(i)}(f_v)) \equiv P_v(t) \quad \text{(mod. } l),$$

d'où

$$P_v'(t) \equiv P_v(t) \quad \text{(mod. } \mathfrak{p}_l), \quad \text{si } l \in L',\ l \neq p_v.$$

Comme cette congruence a lieu pour une infinité de valeurs de l, on en déduit bien que $P_v'(t) = P_v(t)$.

Le lemme 1 montre en particulier que *la trace de la matrice* $\varphi(F_v)$ *appartient à* $\mathbf{Q}$ pour tout $v \in \Sigma - (S_\rho \cup S)$. Comme les F_v sont denses dans S_m pour la topologie de Zariski, il en résulte que φ *est définissable sur* $\mathbf{Q}$ (MG, p. II – 16, prop. 2). En d'autres termes, il existe une représentation linéaire

$$\varphi_0 \colon S_m \to \mathbf{GL}_d$$

de S_m, définie sur $\mathbf{Q}$, telle que φ et φ_0 deviennent isomorphes après extension des scalaires à $\bar{\mathbf{Q}}$. Si $l \in P$, notons φ_l la représentation l-adique attachée à φ_0. Si $v \in \Sigma - (S_\rho \cup S)$ ne divise pas l, on a

$$\begin{aligned} P_{v,\varphi_l}(t) &= \det(1 - t\,\varphi_0(F_v)) && \text{(MG, p. II – 20)} \\ &= \det(1 - t\,\varphi(F_v)) = P_v(t) && \text{(lemme 1)} \\ &= P_{v,\rho_l}(t). \end{aligned}$$

Les deux représentations φ_l et ρ_l sont donc *compatibles* au sens de MG, p. I – 10. Comme elles sont en outre semi-simples, il en résulte qu'elles sont isomorphes (*loc. cit.*), ce qui achève la démonstration du théorème.

§ 4. Courbes elliptiques (résultats généraux)

4.1. Notations; rappels

Dans ce §, K est un corps de nombres algébriques, et E une courbe elliptique sur K, munie d'un point rationnel, pris comme origine; on note j l'invariant modulaire de E. Pour tout ce qui est relatif à K (resp. à E), on conserve les notations du § 3 (resp. celles de l'*Introduction*). En particulier, si n est un entier $\geqq 1$, E_n désigne le noyau de la multiplication par n dans $E(\bar{K})$, et on note

$$\varphi_n \colon G \to \mathrm{Aut}(E_n)$$

l'homomorphisme qui donne l'action de $G = \mathrm{Gal}(\bar{K}/K)$ sur E_n.

A côté des E_n, il est commode d'utiliser les *modules de Tate* T_l et V_l de la courbe E (MG, p. I – 3). Rappelons que, si $l \in P$, on pose

$$T_l = \varprojlim E_{l^n} \quad \text{et} \quad V_l = T_l\left[\frac{1}{l}\right] = T_l \otimes_{\mathbf{Z}_l} \mathbf{Q}_l,$$

et que T_l (resp. V_l) est un $\mathbf{Z}_l$-module libre (resp. un $\mathbf{Q}_l$-espace vectoriel) de rang 2. Le groupe $\mathbf{GL}(T_l)$ est isomorphe à $\mathbf{GL}_2(\mathbf{Z}_l)$; c'est un sous-groupe ouvert compact du groupe $\mathbf{GL}(V_l)$, lui-même isomorphe à $\mathbf{GL}_2(\mathbf{Q}_l)$. Les φ_{l^n} définissent un homomorphisme continu

$$\rho_l \colon G \to \mathbf{GL}(T_l) \subset \mathbf{GL}(V_l).$$

Remarques. 1) On a

$$V_l/T_l = \bigcup_n l^{-n} T_l/T_l = \bigcup_n E_{l^n} = E_{l^\infty}.$$

On déduit de là un homomorphisme $\mathbf{GL}(T_l) \to \mathrm{Aut}(E_{l^\infty})$, qui est en fait un *isomorphisme*, comme on le vérifie aussitôt; cela permet d'identifier ρ_l à l'homomorphisme φ_{l^∞} défini dans l'*Introduction.*

2) On sait (MG, p. I – 11, IV – 5) que les représentations l-adiques ρ_l sont *rationnelles* et forment un système *strictement compatible*; l'ensemble exceptionnel correspondant est l'ensemble S_E des places de K où E a *mauvaise réduction* (cf. [30], ainsi que MG, p. IV – 5). Plus précisément, si $v \in \Sigma - S_E$, et si $l \neq p_v$, la représentation ρ_l est non ramifiée en v, et le polynôme $P_{v,\rho_l}(T)$ correspondant est donné par

$$P_{v,\rho_l}(T) = 1 - \mathrm{Tr}(F_v)\, T + Nv\, T^2;$$

dans cette formule, F_v désigne *l'endomorphisme de Frobenius* de la courbe elliptique $\tilde{E}_v$ déduite de E par réduction en v, et $\mathrm{Tr}(F_v)$ est la *trace* de F_v. Le nombre de points de $\tilde{E}_v$ sur le corps fini k_v est lié à $\mathrm{Tr}(F_v)$ par la formule:

$$\mathrm{Card}\, \tilde{E}_v(k_v) = 1 + Nv - \mathrm{Tr}(F_v).$$

4.2. Surjectivité des φ_l

Nous allons maintenant démontrer l'un des principaux résultats annoncés dans l'*Introduction*:

Théorème 2. *Supposons que la courbe elliptique E n'ait pas de multiplication complexe sur $\overline{K}$. Alors, pour presque tout nombre premier l, l'homomorphisme φ_l: $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E_l)$ est surjectif.*

(En d'autres termes, le groupe de Galois des «points de division par l» est presque toujours isomorphe à $\mathbf{GL}_2(\mathbf{F}_l)$.)

La démonstration comporte plusieurs étapes:

a) *Réduction au cas semi-stable*[4]

Quitte à remplacer K par une extension finie, on peut supposer (et nous le ferons dans ce qui suit) que la courbe elliptique E a *bonne réduction* en toute place $v \in \Sigma$ telle que $v(j) \geqq 0$, et *mauvaise réduction de type multiplicatif* en toute place v telle que $v(j) < 0$ (il suffit, par exemple, d'adjoindre à K les coordonnées des points de E d'ordre 12). Le modèle

[4] Cette réduction n'est pas indispensable; elle ne sert qu'à alléger un peu les énoncés, et les démonstrations, des lemmes 2 et 4 ci-après.

de Néron de E sur O_K a alors pour fibres, soit des courbes elliptiques, soit des groupes dont la composante neutre est de type multiplicatif; il est *semi-stable* au sens de Grothendieck et Mumford.

b) *Structure des groupes* $\varphi_l(G)$

Dans ce qui suit, nous supposons qu'il existe une *partie infinie* L *de* P *telle que* $\varphi_l(G) \neq \mathrm{Aut}(E_l)$ *pour tout* $l \in L$, et il nous faut prouver que E admet des multiplications complexes. Quitte à retrancher de L un ensemble fini, nous pouvons supposer que tout élément de L est $\geqq 7$, et est non ramifié dans K.

Soit $l \in L$, soit v une place de K divisant l, et choisissons une place w de $\overline{K}$ prolongeant v; soit I_w le sous-groupe d'inertie de G relatif à w. L'étude locale du §1, appliquée au corps K_v, donne la structure du sous-groupe $\varphi_l(I_w)$ de $\varphi_l(G)$:

si, en v, E a bonne réduction de hauteur 1, ou mauvaise réduction de type multiplicatif, $\varphi_l(I_w)$ est soit d'ordre $l-1$ soit d'ordre $l(l-1)$, et on peut le représenter matriciellement par $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$, cf. n° 1.11, cor. à la prop. 11 ainsi que n° 1.12, cor. à la prop. 13;

si, en v, E a bonne réduction de hauteur 2, $\varphi_l(I_w)$ est cyclique d'ordre l^2-1, cf. n° 1.12, prop. 12.

Dans le premier cas, $\varphi_l(G)$ contient un demi-sous-groupe de Cartan déployé, et dans le second cas il contient un sous-groupe de Cartan non déployé. De plus, on a $\varphi_l(G) \neq \mathrm{Aut}(E_l)$ par hypothèse. La prop. 17 du n° 2.7 ne laisse alors que les deux possibilités suivantes:

i) $\varphi_l(G)$ *est contenu dans un sous-groupe de Borel, ou dans un sous-groupe de Cartan*;

ii) $\varphi_l(G)$ *est contenu dans le normalisateur* N_l *d'un sous-groupe de Cartan* C_l, *et n'est pas contenu dans* C_l.

Nous allons maintenant montrer que ii) ne se produit que pour un nombre fini de valeurs de l (si E n'a pas de multiplication complexe):

c) *Elimination du cas* ii)

Soit $l \in L$ de type ii) ci-dessus, avec $\varphi_l(G) \subset N_l$ et $\varphi_l(G) \not\subset C_l$. Identifions N_l/C_l au groupe $\{\pm 1\}$, et notons ε_l le composé:

$$G \to N_l \to N_l/C_l \simeq \{\pm 1\}.$$

C'est un caractère d'ordre 2 de G; il correspond à une extension quadratique K_l' de K.

Lemme 2. *L'extension* K_l'/K *est non ramifiée.*

Soit $v \in \Sigma$, soit w un prolongement de v à $\overline{K}$, et soit I_w le sous-groupe d'inertie correspondant. Il nous faut montrer que $\varepsilon_l(I_w) = \{1\}$. Distinguons trois cas:

v_1) *On a* $p_v = l$. On a vu ci-dessus la structure de $\varphi_l(I_w)$; c'est, soit un demi-sous-groupe de Cartan déployé, soit un sous-groupe de Cartan non déployé (le cas où $\varphi_l(I_w)$ serait d'ordre $l(l-1)$ est écarté, puisque $\varphi_l(I_w)$ est contenu dans N_l, dont l'ordre est premier à l). La prop. 14 du n° 2.2 montre alors que $\varphi_l(I_w)$ est contenu dans C_l, i.e. que $\varepsilon_l(I_w) = \{1\}$.

v_2) *On a* $p_v \neq l$ *et* E *a bonne réduction en* v. On a alors $\varphi_l(I_w) = \{1\}$, d'où *a fortiori* $\varepsilon_l(I_w) = \{1\}$.

v_3) *On a* $p_v \neq l$ *et* E *a mauvaise réduction en* v. Vu a), cette mauvaise réduction est de type multiplicatif. D'après la théorie de Tate (MG, p. IV – 31), on a une suite exacte

$$0 \to \mu_l \to E_l \to \mathbf{Z}/l\mathbf{Z} \to 0,$$

qui est compatible avec l'action de I_w. Il en résulte que $\varphi_l(I_w)$ est, soit réduit à $\{1\}$, soit cyclique d'ordre l. Le second cas est impossible du fait que l'ordre de N_l est premier à l. On a donc $\varphi_l(I_w) = \{1\}$, d'où $\varepsilon_l(I_w) = \{1\}$, ce qui achève la démonstration du lemme.

Supposons maintenant qu'il existe une partie infinie L' de L telle que, pour tout $l \in L'$, $\varphi_l(G)$ soit de type ii). Comme les extensions quadratiques non ramifiées de K sont en nombre fini, il existe une telle extension K' qui est égale à K'_l pour une infinité de valeurs de $l \in L'$.

Lemme 3. *Si* $v \in \Sigma$ *est inerte* (i.e. non décomposée) *dans* K', *et si* E *a bonne réduction en* v, *on a* $\mathrm{Tr}(F_v) = 0$ *et la courbe* $\tilde{E}_v$ *est de hauteur* 2.

(Rappelons que F_v désigne l'endomorphisme de Frobenius de $\tilde{E}_v$ sur le corps fini k_v.)

Si $l \neq p_v$, φ_l est non ramifiée en v; si π_w désigne l'élément de Frobenius de $\varphi_l(G)$ associé à un prolongement w de v, on a $\mathrm{Tr}(F_v) \equiv \mathrm{Tr}(\pi_w) \pmod{l}$. Supposons en outre que l appartienne à L' et que $K'_l = K'$; on a $\pi_w \in N_l$, et, du fait que v est inerte dans K', on a $\varepsilon_l(\pi_w) = -1$, i.e. $\pi_w \in N_l - C_l$. Mais les éléments de $N_l - C_l$ ont une trace nulle. On en déduit:

$$\mathrm{Tr}(F_v) \equiv \mathrm{Tr}(\pi_w) \equiv 0 \pmod{l}.$$

Comme cette congruence est réalisée pour une infinité de valeurs de l, on a $\mathrm{Tr}(F_v) = 0$, et l'on sait que cela entraîne que $\tilde{E}_v$ est de hauteur 2.

Soit Σ' l'ensemble des places v qui satisfont aux hypothèses du lemme 3. D'après le théorème de densité de Čebotarev, la densité de Σ est égale à 1/2. D'autre part, on sait (cf. [26], cor. 1 au th. 6, ainsi que MG, p. IV – 13, exerc.) que, si E n'a pas de multiplication complexe, l'ensemble des places v pour lesquelles $\tilde{E}_v$ est de hauteur 2 est de densité 0.

Le lemme 3 entraîne donc que E a des multiplications complexes dans le cas considéré.

Variante. Au lieu d'utiliser la nullité des $\mathrm{Tr}(F_v)$, et l'argument de densité ci-dessus, on peut aussi remarquer que, si l'on étend le corps de base à K', les groupes $\varphi_l(G)_{l\in L'}$ deviennent de type i), ce qui permet d'appliquer les arguments de d) et e) ci-dessous.

d) *Le cas* i)

Soit $l\in L$ tel que $\varphi_l(G)$ soit de type i). Notons

$$\tilde{\varphi}_l\colon\ G\to \mathbf{GL}_2(\mathbf{F}_l)$$

la représentation de G déduite de φ_l par *semi-simplification.* Du fait que $\varphi_l(G)$ est de type i), la représentation $\tilde{\varphi}_l$ est *abélienne.* Par extension des scalaires de $\mathbf{F}_l$ à sa clôture algébrique k_l (cf. n° 3.4), on peut mettre $\tilde{\varphi}_l$ sous forme diagonale, et elle est donnée par deux caractères

$$\theta_l^{(i)}\colon\ \mathrm{Gal}(K^{\mathrm{ab}}/K)\to k_l^*,\qquad i=1,2;$$

comme d'habitude, nous identifierons les $\theta_l^{(i)}$ à des homomorphismes de I dans k_l^*, où I est le groupe des idèles de K.

Lemme 4. *Soit* $\mathfrak{m}$ *le module de* K *de support* $S=\emptyset$. *Il existe une famille d'entiers* $n(\sigma, l, i)$ $(i\in\{1,2\}, \sigma\in\Gamma)$, *égaux à* 0 *ou* 1, *telle que*

$$\theta_l^{(i)}(a)\equiv\prod_{\sigma\in\Gamma}\sigma_l(a_l^{-1})^{n(\sigma,l,i)}\qquad(\mathrm{mod.}\ \mathfrak{p}_l)$$

quels que soient $i\in\{1,2\}$ *et* $a\in U_{\mathfrak{m}}$.

(Les notations sont celles du § 3; en particulier, Γ désigne l'ensemble des plongements de K dans $\bar{\mathbf{Q}}$.)

Vérifions d'abord que $\tilde{\varphi}_l$ est *non ramifié en toute place* $v\in\Sigma$ *ne divisant pas* l. C'est clair si E a bonne réduction en v. Dans le cas contraire, E a mauvaise réduction de type multiplicatif en v; l'argument utilisé dans la démonstration du lemme 2 montre que le groupe d'inertie $\varphi_l(I_w)$ correspondant à v est, soit réduit à $\{1\}$, soit cyclique d'ordre l; par semi-simplification, un tel groupe devient trivial, ce qui montre bien que $\tilde{\varphi}_l(I_w)=\{1\}$.

Ainsi, les caractères $\theta_l^{(i)}$ sont non ramifiés en dehors des places divisant l. D'après la théorie du corps de classes, cela équivaut à dire que $\theta_l^{(i)}(a)=1$ si $a\in U_{v,\mathfrak{m}}$, et $p_v\neq l$. Pour prouver (*), il suffit donc de trouver des exposants $n(\sigma, i, l)$, égaux à 0 ou 1, tels que l'on ait

$$(*')\qquad \theta_l^{(i)}(a)\equiv\prod_{\sigma\in\Gamma}\sigma_l(a^{-1})^{n(\sigma,l,i)}\qquad(\mathrm{mod.}\ \mathfrak{p}_l)\qquad\text{pour tout } a\in U_l.$$

Utilisons la décomposition $U_l=\prod_{v|l}U_v$, et notons $\Gamma(v)$ l'ensemble des plongements $\sigma\colon K\to\bar{\mathbf{Q}}$ tels que $v_l\circ\sigma$ soit équivalente à v. Les $\Gamma(v)$,

pour $v|l$, forment une *partition* de Γ, cf. n° 3.4, et la formule (∗′) équivaut à:

$$(**) \qquad \theta_l^{(i)}(a) \equiv \prod_{\sigma \in \Gamma(v)} \sigma_l(a^{-1})^{n(\sigma, l, i)} \pmod{\mathfrak{p}_l} \qquad \text{pour tout } a \in U_v.$$

La question est maintenant locale en v. Du fait que v est non ramifié sur $\mathbf{Q}$, $[K_v:\mathbf{Q}_l]$ est égal au degré résiduel $f_v=[k_v:\mathbf{F}_l]$ de v, et $\Gamma(v)$ a f_v éléments. De plus, les homomorphismes

$$\tilde{\sigma}_l\colon\ k_v \to k_l \qquad (\sigma \in \Gamma(v)),$$

déduits des σ_l par réduction mod. $\mathfrak{p}_l$, ne sont autres que les *différents plongements* de k_v dans le corps algébriquement clos k_l. Il en résulte, d'après la théorie du corps de classes local (cf. n° 1.5, prop. 3) que les homomorphismes

$$a \mapsto \sigma_l(a^{-1}) \pmod{\mathfrak{p}_v}$$

constituent, lorsque σ parcourt $\Gamma(v)$, les différents *caractères fondamentaux de niveau* f_v du groupe d'inertie modérée de K_v. La formule (∗∗) équivaut donc à dire que *la restriction de* $\theta_l^{(i)}$ *au groupe d'inertie* I_v *relatif à* v *est produit des caractères fondamentaux de niveau* f_v *affectés d'exposants égaux à* 0 *ou* 1. Or cette assertion résulte des déterminations explicites du § 1, n^{os} 1.11 et 1.12. De façon plus précise, il y a trois cas à considérer:

d_1) *E a bonne réduction de hauteur* 1 *en* v. D'après le cor. à la prop. 11, les restrictions des $\theta_l^{(i)}$ à I_v sont, d'une part le caractère unité, d'autre part le caractère fondamental $I_v \to \mathbf{F}_l^*$ de niveau 1. Dans le premier cas, on prend tous les exposants $n(\sigma, l, i)$ égaux à 0, et dans le second tous égaux à 1.

d_2) *E a bonne réduction de hauteur* 2 *en* v. D'après la prop. 12(b), les restrictions des $\theta_l^{(i)}$ à I_v sont les deux caractères fondamentaux $\chi^{(1)}$ et $\chi^{(2)}$ de niveau 2; de plus, la prop. 12(d) montre que k_v contient $\mathbf{F}_{l^2}$, de sorte que $\chi^{(1)}$ et $\chi^{(2)}$ s'obtiennent en composant le caractère fondamental

$$\theta_{l^2-1}\colon\ I_v \to \mathbf{F}_{l^2}^*$$

avec les deux plongements possibles $\tau^{(1)}$ et $\tau^{(2)}$ de $\mathbf{F}_{l^2}$ dans k_l. On prend alors

$$n(\sigma, l, i) = \begin{cases} 1 & \text{si } \tilde{\sigma}_l \text{ prolonge } \tau^{(i)} \\ 0 & \text{sinon,} \end{cases}$$

ce qui prouve notre assertion dans ce cas.

d_3) *E a mauvaise réduction de type multiplicatif en* v. D'après le cor. à la prop. 13, la situation est la même que dans le cas d_1).

Cela achève la vérification du lemme 4.

e) *Fin de la démonstration du théorème* 2

Vu b) et c), on peut supposer que $\varphi_l(G)$ est de type i) pour tout $l \in L$. Le système de représentations l-adiques

$$\rho_l\colon\ G \to \mathbf{GL}(V_l)$$

satisfait aux hypothèses du th. 1 du n° 3.6, l'entier N de ce théorème étant pris égal à 1: cela résulte du lemme 4, et du fait que les ρ_l sont rationnelles, semi-simples (et même irréductibles si E n'a pas de multiplication complexe, cf. MG, p. IV – 9, n° 2.1), et forment un système strictement compatible. Le cor. au th. 1 montre alors que les ρ_l sont *abéliennes*, ce qui, d'après MG, p. IV – 11, entraîne que E a des multiplications complexes, cqfd.

4.3. Questions

Supposons E sans multiplication complexe. Le th. 2 affirme l'existence d'un entier N tel que $\varphi_l(G) = \mathrm{Aut}(E_l)$ pour tout nombre premier $l \geqq N$. Peut-on *déterminer effectivement* un tel N en fonction des coefficients d'une équation de E? C'est vraisemblable; toutefois, il semble qu'il faille d'abord établir une *forme effective du théorème de densité de Čebotarev*, ce qui n'a pas encore été fait. (Lorsque E est donnée explicitement, on peut souvent déterminer N en reprenant simplement la méthode de démonstration du th. 2; nous en verrons des exemples au § 5.)

La question suivante paraît plus difficile: peut-on prendre pour N un entier *qui ne dépende que de* K, et pas de E? Par exemple, peut-on prendre $N = 19$ lorsque $K = \mathbf{Q}$? On peut espérer que les méthodes de Manin et Demianenko, basées sur les propriétés des *hauteurs* des points de E, permettront de répondre à ce genre de question.

4.4. Image de φ_∞

La famille $(\rho_l)_{l \in P}$ définit un homomorphisme continu

$$\rho\colon\ G \to \prod_{l \in P} \mathbf{GL}(T_l) \simeq \prod_{l \in P} \mathbf{GL}_2(\mathbf{Z}_l);$$

c'est essentiellement l'homomorphisme $\varphi_\infty\colon\ G \to \mathrm{Aut}(E_\infty)$ de l'*Introduction*.

Théorème 3. *Si E n'a pas de multiplication complexe, $\rho(G)$ est un sous-groupe ouvert de* $\prod_{l \in P} \mathbf{GL}(T_l)$.

Cela résulte du th. 2 du n° 4.2, et de la proposition démontrée dans MG, p. IV – 19.

Comme on l'a déjà signalé, le th. 3 équivaut à:

Théorème 3'. *L'indice de $\varphi_n(G)$ dans* $\mathrm{Aut}(E_n)$ *reste borné lorsque n varie.*

Il entraîne:

Corollaire 1. *Pour presque tout l, $\rho(G)$ contient le l-ième facteur* $\mathbf{GL}(T_l)$ *du produit* $\prod_{l \in P} \mathbf{GL}(T_l)$.

Nous préciserons ce résultat plus loin (cf. th. 4 ci-après).

Corollaire 2. *Soit K^{cycl} le sous-corps de $\overline{K}$ obtenu en adjoignant à K toutes les racines de l'unité. L'image de* $\mathrm{Gal}(\overline{K}/K^{\mathrm{cycl}})$ *par ρ est un sous-groupe ouvert de* $\prod_{l \in P} \mathbf{SL}(T_l)$.

On sait que le composé des applications

$$\rho_l\colon G \to \mathbf{GL}(T_l) \quad \text{et} \quad \det\colon \mathbf{GL}(T_l) \to \mathbf{Z}_l^*$$

est le caractère l-adique $\chi_l\colon G \to \mathbf{Z}_l^*$ qui donne l'action de G sur les racines l^n-ièmes de l'unité (MG, p. I – 3 et I – 4). Comme $\mathrm{Gal}(\overline{K}/K^{\mathrm{cycl}})$ est l'intersection des noyaux des χ_l, on en déduit que son image par ρ est égale à l'intersection de $\rho(G)$ et de $\prod_{l \in P} \mathbf{SL}(T_l)$; le corollaire en résulte.

Remarque. Plus généralement, soit L un sous-corps de $\overline{K}$ contenant K^{cycl}, et galoisien sur K^{cycl} à groupe de Galois *résoluble*. Alors $\rho(\mathrm{Gal}(\overline{K}/L))$ est un sous-groupe *ouvert* de $\prod_{l \in P} \mathbf{SL}(T_l)$. Cela résulte du cor. 2, et de la propriété suivante, facile à vérifier: si U est un sous-groupe ouvert de $\prod_{l \in P} \mathbf{SL}_2(\mathbf{Z}_l)$, l'adhérence du groupe des commutateurs de U est *ouverte* dans U. On notera que ceci s'applique en particulier au cas où L est l'extension abélienne maximale de K.

Continuons à supposer que E n'a pas de multiplication complexe. Si $v \in \Sigma$, choisissons un prolongement w de v à $\overline{K}$ et soit I_w le sous-groupe d'inertie de G correspondant; notons J_v le plus petit sous-groupe distingué fermé de G contenant I_w; le groupe J_v ne dépend pas du choix de w.

Théorème 4. *Pour presque tout v, $\rho(J_v)$ est égal au p_v-ième facteur* $\mathbf{GL}(T_{p_v})$ *du produit* $\prod_{l \in P} \mathbf{GL}(T_l)$.

(Rappelons que p_v désigne la *caractéristique résiduelle* de v.)

Le théorème 4 résulte de l'énoncé plus précis suivant:

Théorème 4'. *Posons $l = p_v$. Supposons que $l \geqq 5$, que $\varphi_l\colon G \to \mathrm{Aut}(E_l)$ soit surjectif, que E ait bonne réduction en v, et que v soit non ramifiée sur* $\mathbf{Q}$. *Alors $\rho(J_v)$ est égal à* $\mathbf{GL}(T_l)$.

(Vu le th. 2, les hypothèses faites sur v sont satisfaites pour presque tout v.)

Puisque E a bonne réduction en v, le groupe d'inertie I_w opère trivialement sur les $T_{l'}$, $l' \neq l$, et il en est de même de J_v. Le groupe $\rho(J_v)$ est donc un sous-groupe H du l-ième facteur $\mathbf{GL}(T_l)$ du produit $\prod_{l \in P} \mathbf{GL}(T_l)$. L'image $\tilde{H}$ de H dans $\mathrm{Aut}(E_l) = \mathrm{Aut}(T_l/l\,T_l)$ est un sous-groupe distingué de $\varphi_l(G) = \mathrm{Aut}(E_l)$. Puisque v est non ramifiée sur $\mathbf{Q}$, les corollaires aux prop. 11 et 12 du n° 1.11 montrent que $\tilde{H}$ contient, soit un demi-sous-groupe de Cartan déployé, soit un sous-groupe de Cartan non déployé. Vu la prop. 18 du n° 2.7, on a donc $\tilde{H} = \mathrm{Aut}(E_l)$. Soit maintenant H' l'adhérence du groupe des commutateurs de H; on a $H' \subset \mathbf{SL}(T_l)$ et l'image $\tilde{H}'$ de H' dans $\mathbf{SL}(E_l)$ est égale au groupe des commutateurs de $\tilde{H}$, i.e. à $\mathbf{SL}(E_l)$. En appliquant à H' le lemme 3 de MG, p. IV – 23, on en conclut que $H' = \mathbf{SL}(T_l)$. D'autre part, le fait que v soit non ramifiée sur $\mathbf{Q}$ entraîne que $\chi_l(I_w) = \mathbf{Z}_l^*$, et l'image de H par l'homomorphisme

$$\det : \mathbf{GL}(T_l) \to \mathbf{Z}_l^*$$

est donc égale à $\mathbf{Z}_l^*$. Comme on vient de voir que H contient le noyau $\mathbf{SL}(T_l)$ de cet homomorphisme, il en résulte bien que $H = \mathbf{GL}(T_l)$.

Remarque. Lorsqu'on suppose seulement que E a bonne réduction en v, on peut montrer que $\rho(J_v)$ est un *sous-groupe ouvert* du p_v-ième facteur $\mathbf{GL}(T_{p_v})$ du produit $\prod_{l \in P} \mathbf{GL}(T_l)$.

4.5. Courbes à multiplications complexes

Comme on l'a indiqué dans l'*Introduction*, ce cas est connu depuis longtemps. Aussi vais-je me borner à en résumer rapidement les principaux résultats, renvoyant à [9], [10], [30] ou [34] pour plus de détails:

Soit $R = \mathrm{End}_{\bar{K}}(E)$. On suppose que $R \neq \mathbf{Z}$, auquel cas c'est un «ordre» dans un corps quadratique imaginaire $F = \mathbf{Q} \otimes R$. Supposons que les éléments de R soient définis sur K; leur action sur l'algèbre de Lie de E est donnée par un homomorphisme $R \to K$; par passage au corps des fractions, cela permet *d'identifier F à un sous-corps de K*.

Si $l \in P$, posons $R_l = \mathbf{Z}_l \otimes R$ et $F_l = \mathbf{Q}_l \otimes F$. Le module de Tate T_l est un R_l-module libre de rang 1 ([30], fin du § 4) et V_l est un F_l-espace vectoriel de dimension 1. L'image de G par

$$\rho_l : G \to \mathbf{GL}(T_l)$$

commute aux éléments de R_l, donc est contenue dans R_l^*. Elle est abélienne, et on peut l'identifier à un homomorphisme

$$\rho_l : I \to R_l^*,$$

où I est le groupe des idèles de K.

Théorème 5. *Il existe un homomorphisme continu* $\varepsilon: I \to F^*$, *et un seul, tel que* $\varepsilon(x) = N_{K/F}(x)$ *si* $x \in K^*$, *et que* $\rho_l(a) = \varepsilon(a)\, N_{K_l/F_l}(a_l^{-1})$ *pour tout* $l \in P$ *et tout* $a \in I$.

C'est une reformulation (due essentiellement à Weil [39], [40] – voir aussi [30], § 7) de résultats classiques.

Corollaire. *L'image de G par* ρ *est un sous-groupe ouvert du produit* $\prod_{l \in P} R_l^*$.

Puisque ε est continu, son noyau est ouvert, donc contient un sous-groupe $U_{\mathfrak{m}}$, pour $\mathfrak{m}$ convenable (si l'on prend le plus petit $\mathfrak{m}$ possible, son support est l'ensemble des places où E a mauvaise réduction, cf. [30], cor. 1 au th. 11). Il nous suffit de montrer que $\rho(U_{\mathfrak{m}})$ est ouvert dans $\prod_{l \in P} R_l^*$. Or, si $a \in U_{\mathfrak{m}}$, on a

$$\rho_l(a) = N_{K_l/F_l}(a_l^{-1}) \quad \text{pour tout } l \in P, \quad \text{cf. th. 5.}$$

Nous sommes alors ramenés à montrer que l'application

$$N_{K_l/F_l}: U_{l,\mathfrak{m}} \to R_l^*$$

est *ouverte* pour tout l, et *surjective* pour presque tout l, ce qui est bien connu.

Remarques. 1) Le corollaire ci-dessus est l'analogue du th. 3 du n° 4.4. Il existe aussi un analogue (partiel) du th. 4: pour presque tout v, $\rho(J_v)$ est égal à la composante de $R_{p_v}^*$ correspondant à la place de F induite par v; on notera cependant que, si l se décompose dans F, cette composante *n'est pas* égale à $R_{p_v}^*$.

2) On peut montrer que tout homomorphisme $\varepsilon: I \to F^*$ vérifiant les conditions du th. 5 correspond, comme ci-dessus, à une courbe elliptique E sur K telle que $\mathrm{End}_K(E)$ soit un ordre de F; de plus, E est unique, à K-isogénie près.

§ 5. Courbes elliptiques (exemples)

L'objet de ce § est de déterminer explicitement, pour certaines courbes elliptiques E, l'ensemble des nombres premiers l tels que $\varphi_l(G) = \mathrm{Aut}(E_l)$.

5.1. Notations

La courbe E est donnée sous forme de cubique non singulière:

$$(*) \qquad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

le point à l'infini étant pris comme origine.

On pose, suivant Néron et Tate[5]:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1 a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2 = \tfrac{1}{4}(b_2 b_6 - b_4^2),$$
$$c_4 = b_2^2 - 24 b_4, \quad c_6 = 36 b_2 b_4 - b_2^3 - 216 b_6,$$
$$\Delta = b_4^3 - 27 b_6^2 + b_8(36 b_4 - b_2^2) = \tfrac{1}{1728}(c_4^3 - c_6^2);$$

l'invariant modulaire j de E est égal à c_4^3/Δ.

Dans tout le § (n° 5.10 excepté), *le corps de base est le corps* $\mathbf{Q}$ *des nombres rationnels*, et l'équation (∗) est choisie de manière à donner un *modèle standard* de E, au sens de Néron [16]. En particulier, les coefficients $a_1, \ldots, c_6$ sont *entiers*.

On note S_E l'ensemble des $p \in P$ en lesquels E a mauvaise réduction; c'est l'ensemble des diviseurs premiers de Δ; on a $S_E \neq \emptyset$, cf. Šafarevič [23] ou Ogg [18]. On note N le *conducteur* de E, au sens de Weil; pour sa définition, voir Weil [41], Ogg [19] ainsi que [29], n° 2.4; on a

$$N = \prod_{p \in S_E} p^{n(p)},$$

avec $n(p) \geqq 1$ et même $n(p) \in \{1, 2\}$ si $p \geqq 5$.

Si $p \notin S_E$, on note $\tilde{E}(p)$ la réduction de E (mod. p), et t_p la trace de son endomorphisme de Frobenius. On a

$$t_p = 1 + p - A_p,$$

où A_p est le nombre de points de $\tilde{E}(p)$ sur $\mathbf{F}_p$.

5.2. Remarques sur $\varphi_l(G)$

Nous disposons d'un certain nombre de renseignements sur le sous-groupe $\varphi_l(G)$ de $\mathrm{Aut}(E_l)$:

i) Ses *groupes d'inertie* sont essentiellement connus, cf. § 1.

ii) Tout $p \notin S_E \cup \{l\}$ donne un élément de Frobenius $\pi_p \in \varphi_l(G)$, défini à conjugaison près, et tel que

$$\mathrm{Tr}(\pi_p) \equiv t_p \pmod{l} \quad \text{et} \quad \det(\pi_p) \equiv p \pmod{l}.$$

---

[5] Ogg [18] écrit l'équation de E sous la forme:

$$y^2 + a_1 x y + a_3 y + x^3 + a_2 x^2 + a_4 x + a_6 = 0.$$

On passe de ses notations à celles de Néron-Tate par les substitutions:

$$(x, y; a_1, a_2, a_3, a_4, a_6) \mapsto (-x, y; -a_1, -a_2, a_3, a_4, -a_6)$$

et

$$(\beta_2, \beta_4, \beta_6, \beta_8; \gamma_4, \gamma_6; \Delta; j) \mapsto (b_2, b_4, b_6, -b_8; c_4, -c_6; \Delta; j).$$

iii) L'homomorphisme det: $\varphi_l(G) \to \mathbf{F}_l^*$ est *surjectif*; en effet, on sait que son image est le groupe de Galois du l-ième corps cyclotomique.

iv) $\varphi_l(G)$ contient un élément c de valeurs propres $\{1, -1\}$: celui fourni par la conjugaison complexe (relativement à un plongement de $\bar{\mathbf{Q}}$ dans $\mathbf{C}$). Il en résulte que, si $l \neq 2$, $\varphi_l(G)$ *n'est pas contenu dans un sous-groupe de Cartan non déployé de* $\mathrm{Aut}(E_l)$.

Les renseignements fournis par ii), combinés à la prop. 19 du n° 2.8, suffisent parfois à prouver que $\varphi_l(G)$ est égal à $\mathrm{Aut}(E_l)$. Prenons par exemple pour E la courbe

$$y^2 + y = x^3 - x^2,$$

de conducteur 11. Elle a 5 points (mod. 2) et 5 points (mod. 3), d'où:

$$\mathrm{Tr}(\pi_2) = t_2 = 1 + 2 - 5 = -2, \quad \det(\pi_2) = 2, \quad \mathrm{Tr}(\pi_2)^2 - 4\det(\pi_2) = -4,$$

et:

$$\mathrm{Tr}(\pi_3) = t_3 = 1 + 3 - 5 = -1, \quad \det(\pi_3) = 3, \quad \mathrm{Tr}(\pi_3)^2 - 4\det(\pi_3) = -11.$$

Supposons que $l \geqq 13$ et $\left(\frac{11}{l}\right) = -1$. L'un des nombres $\{-4, -11\}$ est un carré (mod. l) et l'autre ne l'est pas. De plus, l'élément

$$u = \mathrm{Tr}(\pi_3)^2 / \det(\pi_3)$$

satisfait aux relations:

$$u \not\equiv 0, 1, 2, 4 \pmod{l} \quad \text{et} \quad u^2 - 3u + 1 \not\equiv 0 \pmod{l}.$$

Toutes les conditions de la prop. 19 sont donc vérifiées par $\varphi_l(G)$. On en conclut que, pour un tel l (par exemple 13, 17, 23, 29, ...), *on a* $\varphi_l(G) = \mathrm{Aut}(E_l)$. C'est essentiellement la méthode suivie par Shimura [32]; elle a l'inconvénient de ne s'appliquer qu'à des valeurs de l satisfaisant à certaines congruences, et ne peut pas donner de résultat valable «pour presque tout l». Nous verrons au n° 5.5 qu'on peut obtenir, avec moins de calculs, un résultat plus complet, à condition d'utiliser les renseignements du type i) ci-dessus.

5.3. Les cas particuliers $l = 2$ et $l = 3$

Ces cas sont bien connus. Rappelons-les brièvement:

a) $l = 2$

La courbe E possède 3 points d'ordre 2, dont les abscisses $\{e_1, e_2, e_3\}$ sont les solutions de l'équation

$$4x^3 + b_2 x^2 + 2b_4 x + b_6 = 0.$$

La racine carrée de Δ s'exprime au moyen des e_i par:

$$\Delta^{\frac{1}{2}} = \pm 4(e_1 - e_2)(e_2 - e_3)(e_3 - e_1).$$

Le groupe $\mathrm{Aut}(E_2) \simeq \mathbf{GL}_2(\mathbf{F}_2)$ s'identifie au groupe $\mathfrak{S}_3$ opérant par permutation des indices sur $\{e_1, e_2, e_3\}$. Notons ε: $\mathfrak{S}_3 \to \{\pm 1\}$ l'homomorphisme «signature». En composant φ_2: $G \to \mathrm{Aut}(E_2)$ avec ε, on obtient un homomorphisme de G dans $\{\pm 1\}$ qui correspond à une extension du corps de base de degré $\leqq 2$. La formule ci-dessus montre que cette extension est celle définie par $\Delta^{\frac{1}{2}}$. Ainsi, *pour que* $\varphi_2(G)$ *soit contenu dans* $\mathfrak{A}_3$, *il faut et il suffit que* Δ *soit un carré* (lorsque $j \neq 1728$, cela équivaut aussi à dire que $j - 1728$ est un carré, vu que $j - 1728 = c_6^2/\Delta$).

b) $l = 3$

La courbe E possède 8 points d'ordre 3, répartis en 4 couples de points opposés. Leurs abscisses x_i $(i = 1, \ldots, 4)$ sont les racines de l'équation

$$3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8 = 0.$$

Le groupe $\mathrm{Aut}(E_3)/\{\pm 1\} \simeq \mathbf{PGL}_2(\mathbf{F}_3)$ s'identifie au groupe $\mathfrak{S}_4$ opérant par permutations des indices sur $\{x_1, x_2, x_3, x_4\}$. Il y a trois façons de décomposer $\{1, 2, 3, 4\}$ en deux parties $\{i, j\}$ et $\{k, l\}$ à 2 éléments; à chacune de ces décompositions correspond une racine cubique de Δ par la formule:

$$\Delta^{\frac{1}{3}} = b_4 - 3(x_i x_j + x_k x_l).$$

Notons alors σ l'homomorphisme de $\mathfrak{S}_4$ sur $\mathfrak{S}_3$ donnant l'action de $\mathfrak{S}_4$ sur les 3 décompositions du type précédent. En composant les homomorphismes

$$G \xrightarrow{\varphi_3} \mathrm{Aut}(E_3) \to \mathrm{Aut}(E_3)/\{\pm 1\} \simeq \mathfrak{S}_4 \xrightarrow{\sigma} \mathfrak{S}_3,$$

on obtient un homomorphisme de G dans $\mathfrak{S}_3$; d'après la formule ci-dessus, cet homomorphisme est celui qui donne l'action de G sur les 3 racines cubiques de Δ. En particulier, *l'ordre de* $\varphi_3(G)$ *est divisible par* 3 *si et seulement si* Δ *n'est pas un cube* (lorsque $j \neq 0$, cela équivaut aussi à dire que j n'est pas un cube, vu que $j = c_4^3/\Delta$).

On trouvera d'autres renseignements sur le cas $l = 3$ dans Neumann [17], § 1. Signalons également que l'on peut exprimer $\Delta^{\frac{1}{3}}$ au moyen des coordonnées des points d'ordre 4 de E.

5.4. Courbes semi-stables

Dans ce n°, ainsi que dans le suivant, nous traitons le cas le plus simple, celui où le modèle de Néron de E est *semi-stable*. Cela signifie (cf. n° 4.2) que, si E a mauvaise réduction en un nombre premier p (i.e.

si $p \in S_E$), cette mauvaise réduction est *de type multiplicatif*; on a alors

$$v_p(j) = -v_p(\Delta) < 0, \qquad \text{où } v_p \text{ est la valuation } p\text{-adique de } \mathbf{Q}.$$

Par passage à une extension non ramifiée de $\mathbf{Q}_p$ (que l'on peut prendre égale à $\mathbf{Q}_p(\sqrt{-c_6})$) la courbe E devient isomorphe à la *courbe de Tate* attachée à j (n° 1.12).

Le *conducteur* N de E est le produit des nombres premiers p appartenant à S_E; il est *sans facteur carré*.

Nous allons voir que, pour une telle courbe, la présence d'un point rationnel d'ordre l est essentiellement le seul obstacle à $\varphi_l(G) = \mathrm{Aut}(E_l)$. De façon plus précise:

Proposition 21. *Soit E une courbe elliptique semi-stable sur $\mathbf{Q}$, et soit l un nombre premier. Supposons*:

a) *que* $\varphi_l(G) \neq \mathrm{Aut}(E_l)$;

b) *que* $l \neq 2, 3, 5$, *ou que l ne divise pas l'un des* $v_p(j)$, *avec* $p \in S_E$.

Alors:

i) $\varphi_l(G)$ *est contenu dans un sous-groupe de Borel de* $\mathrm{Aut}(E_l)$;

ii) *le G-module E_l a une suite de Jordan-Hölder dont les quotients sont isomorphes à $\mathbf{Z}/l\mathbf{Z}$ et μ_l*;

iii) *on a* $t_p \equiv 1 + p \pmod{l}$ *pour tout* $p \in P - S_E$.

(Rappelons que μ_l désigne le groupe des racines l-ièmes de l'unité.)

Démonstration de i). Supposons d'abord qu'il existe $p \in S_E$ tel que $v_p(j) \not\equiv 0 \pmod{l}$. D'après MG, p. IV − 37, $\varphi_l(G)$ contient un élément d'ordre l, fourni par l'inertie en p. D'après la prop. 15 du n° 2.4, il en résulte que $\varphi_l(G)$ est contenu dans un sous-groupe de Borel, ou contient $\mathbf{SL}(E_l)$. Mais, dans ce dernier cas, on aurait $\varphi_l(G) = \mathrm{Aut}(E_l)$, puisque det: $\varphi_l(G) \to \mathbf{F}_l^*$ est surjectif, cf. n° 5.2, et cela contredirait l'hypothèse a). D'où i) dans le cas considéré.

Supposons maintenant $l \geqq 7$. D'après ce qu'on a vu au §1 (appliqué au corps l-adique $\mathbf{Q}_l$), le groupe $\varphi_l(G)$ contient, soit un groupe de Cartan non déployé, soit un demi-sous-groupe de Cartan déployé. Vu la prop. 17 du n° 2.7, on a seulement les trois possibilités suivantes:

1) $\varphi_l(G)$ est contenu dans un sous-groupe de Borel;

2) $\varphi_l(G)$ est contenu dans un sous-groupe de Cartan non déployé;

3) $\varphi_l(G)$ est contenu dans le normalisateur N_l d'un sous-groupe de Cartan C_l, et n'est pas contenu dans C_l.

Le cas 2) est impossible, cf. n° 5.2. Le cas 3) l'est aussi; en effet, le composé $G \to \varphi_l(G) \to N_l/C_l \simeq \{\pm 1\}$ donnerait une extension quadratique de $\mathbf{Q}$ qui serait *non ramifiée* (cf. lemme 2, n° 4.2). Il ne reste donc que le cas 1), ce qui achève de prouver i).

Démonstration de ii). Supposons que $\varphi_l(G)$ soit contenu dans un sous-groupe de Borel. On a tout d'abord:

Lemme 5. *En l, la courbe E a, soit bonne réduction de hauteur* 1, *soit mauvaise réduction de type multiplicatif.*

Sinon, en effet, E aurait bonne réduction de hauteur 2 et $\varphi_l(G)$ contiendrait un sous-groupe de Cartan non déployé, cf. n° 1.11, prop. 12; or un sous-groupe de Borel ne contient pas de sous-groupe de Cartan non déployé.

Soit maintenant E'_l une droite de E_l stable par G. L'action de G sur E'_l et sur $E''_l = E_l/E'_l$ se fait par deux caractères

$$\chi', \chi'' : G \to \mathbf{F}_l^*,$$

et φ_l est représentable sous forme matricielle par $\begin{pmatrix} \chi' & * \\ 0 & \chi'' \end{pmatrix}$. Tout revient à déterminer χ' et χ''.

Lemme 6. *Les caractères χ' et χ'' sont non ramifiés en dehors de l. L'un d'eux est non ramifié en l.*

Si $p \neq l$ et $p \notin S_E$, la représentation φ_l est non ramifiée en p, et il en est de même de χ' et χ''. Si $p \neq l$ et $p \in S_E$, on vérifie facilement sur le modèle de Tate que le groupe d'inertie de $\varphi_l(G)$ en p est, soit trivial, soit d'ordre l; dans les deux cas, son image par χ' et χ'' est triviale. D'autre part, le lemme 5 montre que, en l, on a, soit bonne réduction de hauteur 1, soit mauvaise réduction de type multiplicatif. D'après les corollaires aux prop. 11 et 13 du §1, il en résulte que l'un des deux caractères χ' et χ'' est non ramifié en l, d'où le lemme.

L'assertion ii) est maintenant immédiate. En effet, $\mathbf{Q}$ n'admet pas d'extension non ramifiée de degré >1, et par suite tout caractère de G qui est non ramifié est égal à 1. On a donc, soit $\chi' = 1$, soit $\chi'' = 1$. Comme le produit $\chi'\chi''$ est égal au caractère χ donnant l'action de G sur μ_l, on voit que l'on a:

$$\chi' = 1, \quad \chi'' = \chi \quad \text{ou} \quad \chi' = \chi, \quad \chi'' = 1,$$

ce qui équivaut à

$$E'_l \simeq \mathbf{Z}/l\mathbf{Z}, \quad E''_l \simeq \mu_l \quad \text{ou} \quad E'_l \simeq \mu_l, \quad E''_l \simeq \mathbf{Z}/l\mathbf{Z}.$$

Remarque. Le premier cas est celui où *E a un point rationnel d'ordre l*; le second, celui *où la courbe $E' = E/E'_l$ a un point rationnel d'ordre l*; on notera que E' est liée à E par une isogénie de degré l.

Démonstration de iii). Conservons les notations ci-dessus. Soit $p \notin S_E$, $p \neq l$, et soit $\pi_p \in \varphi_l(G)$ l'élément de Frobenius correspondant (défini à conjugaison près). On a

$$t_p \equiv \mathrm{Tr}(\pi_p) \equiv \alpha'_p + \alpha''_p \pmod{l},$$

où α'_p (resp. α''_p) désigne la valeur propre de π_p relativement au sous-espace E'_l (resp. au quotient E''_l) de E_l. Comme $E'_l \oplus E''_l$ est isomorphe à $\mathbf{Z}/l\mathbf{Z} \oplus \mu_l$, on a $\{\alpha'_p, \alpha''_p\} = \{1, p\}$, d'où

$$(*) \qquad t_p \equiv 1 + p \pmod{l} \quad \text{pour tout} \quad p \notin S_E, p \neq l,$$

ce qui démontre iii) pour $p \neq l$. [Inversement, si $(*)$ est vérifié pour presque tout p (ou même seulement pour des p de densité 1), le semi-simplifié de E_l est isomorphe à $\mathbf{Z}/l\mathbf{Z} \oplus \mu_l$, cf. MG, p. IV – 6, exerc.]

Il reste à montrer que, lorsque $l \notin S_E$, la formule ci-dessus est encore vraie pour $p = l$, autrement dit que l'on a $t_l \equiv 1 \pmod{l}$. Distinguons deux cas:

iii$_1$) $l = 2$.

D'après le lemme 5, la courbe elliptique $\tilde{E}(2)$ déduite de E par réduction (mod. 2) est de hauteur 1; elle a donc un point d'ordre 2 et un seul; ce point est rationnel sur $\mathbf{F}_2$. Le nombre de points de $\tilde{E}(2)$ sur $\mathbf{F}_2$ est donc *pair*, ce qui prouve que

$$A_2 = 1 + 2 - t_2 \equiv 0 \pmod{2}, \quad \text{i.e.} \quad t_2 \equiv 1 \pmod{2}.$$

iii$_2$) $l \geqq 3$.

Supposons que E'_l soit isomorphe à $\mathbf{Z}/l\mathbf{Z}$, i.e. que E possède un point rationnel d'ordre l. Par réduction (mod. l) ce point donne un élément d'ordre 1 ou l de $\tilde{E}(l)$. Le premier cas est en fait impossible: en effet, on a vu au n° 1.11 que le groupe d'inertie en l opère sur le noyau de la réduction (mod. l) au moyen du caractère fondamental de niveau 1, et ce caractère est non trivial pour $l \geqq 3$, puisque son image est $\mathbf{F}_l^*$. Ainsi, $\tilde{E}(l)$ possède un point d'ordre l rationnel sur $\mathbf{F}_l$, d'où:

$$A_l = 1 + l - t_l \equiv 0 \pmod{l}, \quad \text{i.e.} \quad t_l \equiv 1 \pmod{l}.$$

Lorsque c'est E''_l qui est isomorphe à $\mathbf{Z}/l\mathbf{Z}$, on utilise la courbe $E' = E/E'_l$ au lieu de la courbe E; comme les t_p ne changent pas par isogénie, cela donne bien le résultat cherché.

Remarque. L'argument employé ci-dessus pour traiter le cas $p = l$ peut servir aussi dans le cas $p \neq l$: un point d'ordre l de E donne par réduction (mod. p) un point d'ordre l de $\tilde{E}(p)$, ce qui montre que $A_p = 1 + p - t_p$ est divisible par l.

Donnons maintenant quelques applications de la prop. 21:

Corollaire 1. *Soit p le plus petit nombre premier en lequel E a bonne réduction. On a $\varphi_l(G) = \mathrm{Aut}(E_l)$ pour tout $l > (p^{\frac{1}{2}} + 1)^2$.*

(On obtient ainsi une majoration *effective* des l pour lesquels $\varphi_l(G)$ est distinct de $\mathrm{Aut}(E_l)$.)

Raisonnons par l'absurde, et supposons que $l>(p^{\frac{1}{2}}+1)^2$ et que $\varphi_l(G)\neq \mathrm{Aut}(E_l)$. Comme $p\geqq 2$, on a $l\geqq 1+2+2\sqrt{2}>5$, et la prop. 21 montre que l'entier $A_p=1+p-t_p$ est divisible par l. On a donc $A_p\geqq l>1+p+2p^{\frac{1}{2}}$, d'où $t_p<-2p^{\frac{1}{2}}$, ce qui contredit «l'hypothèse de Riemann» pour $\tilde{E}(p)$.

Corollaire 2. *On a* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *si* $l=11$ *ou* 17.

Sinon, en effet, l'une des courbes E et $E'=E/E'_l$ aurait un point rationnel d'ordre l, ce que l'on sait être impossible pour $l=11$ et $l=17$, cf. [2], [20].

5.5. Courbes semi-stables: exemples numériques [6]

5.5.1. Reprenons la courbe

$$y^2+y=x^3-x^2,$$

de conducteur $N=11$ (cf. n° 5.2). On a $\Delta=-11, j=-2^{12}/11$,

$$\text{d'où}\quad v_{11}(j)=-v_{11}(\Delta)=-1,$$

ce qui montre que la condition b) de la prop. 21 est satisfaite quel que soit l. On en déduit que $\varphi_l(G)=\mathrm{Aut}(E_l)$ pourvu que l'un au moins des $A_p=1+p-t_p$ ($p\neq 11$) ne soit pas divisible par l. Comme $A_2=5$, ceci a lieu *pour tout* $l\neq 5$. Le cas $l=5$ fait exception: le point $(0,0)$ est d'ordre 5, et le groupe $\varphi_5(G)$ est un «demi-sous-groupe de Borel», représentable matriciellement par $\begin{pmatrix}1 & *\\ 0 & *\end{pmatrix}$.

La courbe 5.5.1 correspond au groupe modulaire $\Gamma_1(11)$. Elle est liée par une isogénie de degré 5 (explicitée par Vélu [35]) à la courbe

5.5.2.

$$y^2+y=x^3-x^2-10x-20\qquad(\Delta=-11^5, j=-2^{12}\,31^3/11^5),$$

qui correspond au groupe $\Gamma_0(11)$, cf. Shimura [31]. Pour cette dernière, *on a* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 5$, et $\varphi_5(G)$ est un demi-sous-groupe de Cartan déployé $\begin{pmatrix}1 & 0\\ 0 & *\end{pmatrix}$.

5.5.3. Courbe

$$y^2+xy+y=x^3-x;\qquad N=2.7;\qquad \Delta=-2^2\,7;\qquad j=-5^6/2^2\,7.$$

On a $A_3=6$, *d'où* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 2, 3$. Les cas $l=2$ et $l=3$ font exception: $(0,0)$ est un point d'ordre 3, et $(-1,0)$ un point d'ordre 2; les groupes $\varphi_2(G)$ et $\varphi_3(G)$ sont des demi-sous-groupes de Borel $\begin{pmatrix}1 & *\\ 0 & *\end{pmatrix}$.

[6] Les exemples des n^{os} 5.5 et 5.7 sont extraits d'une liste de courbes elliptiques à bas conducteurs que Swinnerton-Dyer m'a obligeamment communiquée.

5.5.4. Courbe

$y^2+xy+y=x^3-x^2-3x+3$; $N=2.13$; $\Delta=-2^7 13$; $j=-3^3 43^3/2^7 13$.

On a $A_3=7$, *d'où* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 7$. Le cas $l=7$ fait exception: $(1,0)$ est un point d'ordre 7; le groupe $\varphi_7(G)$ est un demi-sous-groupe de Borel.

5.5.5. Courbe

$y^2+xy+y=x^3+x^2-4x+5$; $N=2.3.7$; $\Delta=-2^8 3^2 7$; $j=-193^3/2^8 3^2 7$.

On a $A_5=8$, *d'où* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 2$. Le cas $l=2$ fait exception: $(-1,3)$ est un point d'ordre 8; le groupe $\varphi_2(G)$ est représentable par $\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}$.

5.5.6. Courbe

$$y^2+y=x^3-x; \quad N=37; \quad \Delta=37; \quad j=2^{12}\,3^3/37.$$

On a $A_2=5$ et $A_3=7$, *d'où* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour tout* l.

(Noter qu'ici le point $(0,0)$ est *d'ordre infini*; il en est de même dans les deux exemples qui suivent.)

5.5.7. Courbe

$$y^2+y=x^3+x^2; \quad N=43; \quad \Delta=-43; \quad j=-2^{12}/43.$$

On a $A_2=5$ et $A_3=6$, *d'où* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour tout* l.

5.5.8. Courbe

$$y^2+xy+y=x^3-x^2; \quad N=53; \quad \Delta=53; \quad j=-3^3\,5^3/53.$$

On a $A_2=4$ et $A_3=7$, *d'où* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour tout* l.

Remarque. Dans les trois derniers exemples, on a $\varphi_l(G)=\mathrm{Aut}(E_l)$ pour tout $l\in P$. On peut se demander (la question m'a été posée par Tate) si l'on a plus généralement $\varphi_n(G)=\mathrm{Aut}(E_n)$ pour tout entier $n\geqq 1$, ou, ce qui revient au même, si l'homomorphisme

$$\varphi_\infty: G\to \mathrm{Aut}(E_\infty)\simeq \prod_{l\in P}\mathbf{GL}_2(\mathbf{Z}_l)$$

est *surjectif*. La réponse est négative:

Proposition 22. *Pour toute courbe elliptique* E *sur* $\mathbf{Q}$, *l'image de*

$$\varphi_\infty: G\to \mathrm{Aut}(E_\infty)$$

est contenue dans un sous-groupe d'indice 2 *de* $\mathrm{Aut}(E_\infty)$.

Si $a \in \mathrm{Aut}(E_\infty)$, notons a_n l'image de a dans $\mathrm{Aut}(E_n)$; pour $n=2$, on a $\mathrm{Aut}(E_2) \simeq \mathfrak{S}_3$, et la *signature* $\varepsilon(a_2)$ de a_2 est définie. On a vu au n° 5.3 que, pour tout $s \in G$, on a

$$\varepsilon(\varphi_2(s)) = \chi_\Delta(s),$$

où $\chi_\Delta : G \to \{\pm 1\}$ est le caractère de G défini par l'extension $\mathbf{Q}(\sqrt{\Delta})$. Comme toute extension abélienne de $\mathbf{Q}$ est contenue dans une extension cyclotomique, on peut trouver un entier m (par exemple $4\,|\Delta|$) tel que χ_Δ soit le composé de l'homomorphisme canonique

$$G \to \mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q}) = (\mathbf{Z}/m\mathbf{Z})^*$$

et d'un caractère $\alpha_\Delta : (\mathbf{Z}/m\mathbf{Z})^* \to \{\pm 1\}$ («symbole de Kronecker» relatif à Δ). La formule ci-dessus peut donc se récrire sous la forme

$$\varepsilon(\varphi_2(s)) = \alpha_\Delta(\det \varphi_m(s)) \quad \text{pour tout } s \in G.$$

Elle montre que $\varphi_\infty(G)$ est contenu dans le sous-groupe H_Δ de $\mathrm{Aut}(E_\infty)$ formé des éléments a tels que

$$\varepsilon(a_2) = \alpha_\Delta(\det a_m).$$

Il est clair que H_Δ est un sous-groupe ouvert d'indice 2 de $\mathrm{Aut}(E_\infty)$, d'où la proposition.

(Lorsque E est l'une des courbes 5.5.5, 5.5.6, 5.5.7, on peut montrer que $\varphi_\infty(G)$ est *égal* à H_Δ. En particulier, les homomorphismes

$$\rho_l : G \to \mathbf{GL}(T_l)$$

sont surjectifs pour tout l.)

5.6. Courbes non semi-stables: les groupes Φ_p

Lorsque E n'est pas semi-stable en un nombre premier p, il y a lieu d'introduire un certain groupe fini $\Phi_p \neq \{1\}$ qui mesure le défaut de semi-stabilité en p; ce groupe joue un rôle essentiel dans les représentations

$$\varphi_l : G \to \mathrm{Aut}(E_l), \quad \text{pour } l \neq p.$$

On le définit de façon différente suivant que j est, ou non, entier en p.

a) *Définition de Φ_p lorsque j est entier en p*

Il y a «potentiellement bonne réduction» en p, et l'on peut appliquer les résultats de Serre-Tate [30], § 2. Notons I_p le sous-groupe d'inertie de G en p (défini à conjugaison près). D'après [30], *loc. cit.*, l'action de I_p sur les E_n (avec n non divisible par p) se fait par l'intermédiaire d'un certain quotient fini Φ_p de I_p:

$$I_p \to \Phi_p \to \mathrm{Aut}(E_n),$$

et $\Phi_p \to \mathrm{Aut}(E_n)$ est injectif si $n \geqq 3$. Si $\mathbf{Q}_{p,nr}$ est une extension non ramifiée maximale de $\mathbf{Q}_p$, on peut également interpréter Φ_p comme $\mathrm{Gal}(L/\mathbf{Q}_{p,nr})$, où L est la plus petite extension de $\mathbf{Q}_{p,nr}$ où E acquiert bonne réduction ([30], p. 498, cor. 3). De plus ([30], p. 497, dém. du th. 2), Φ_p est isomorphe à un sous-groupe du groupe des automorphismes de la courbe elliptique $\tilde{E}$ sur $\bar{\mathbf{F}}_p$ déduite de $E_{/L}$ par réduction. Vu la structure connue des groupes d'automorphismes des courbes elliptiques, cela conduit à distinguer les trois cas suivants:

a_1) $p \neq 2, 3$. Le groupe Φ_p est alors cyclique d'ordre 2, 3, 4, 6. Plus précisément, on vérifie sur les modèles de Néron ([16], p. 124–125) que:

$$\mathrm{Card}(\Phi_p)=2 \Leftrightarrow E \text{ de type } c_4 \quad \Leftrightarrow v_p(\Delta) \equiv 6 \pmod{12}$$

$$\mathrm{Card}(\Phi_p)=3 \Leftrightarrow E \text{ de type } c_3 \text{ ou } c_6 \Leftrightarrow v_p(\Delta) \equiv 4 \text{ ou } 8 \pmod{12}$$

$$\mathrm{Card}(\Phi_p)=4 \Leftrightarrow E \text{ de type } c_2 \text{ ou } c_7 \Leftrightarrow v_p(\Delta) \equiv 3 \text{ ou } 9 \pmod{12}$$

$$\mathrm{Card}(\Phi_p)=6 \Leftrightarrow E \text{ de type } c_1 \text{ ou } c_8 \Leftrightarrow v_p(\Delta) \equiv 2 \text{ ou } 10 \pmod{12}.$$

Le corps L s'obtient en adjoignant à $\mathbf{Q}_{p,nr}$ les racines 12-ièmes de Δ.

a_2) $p=3$. Le groupe Φ_p est, soit cyclique d'ordre 2, 3, 4, 6, soit produit semi-direct non abélien d'un groupe cyclique d'ordre 4 par un sous-groupe distingué d'ordre 3.

a_3) $p=2$. Le groupe Φ_p est isomorphe à un sous-groupe de $\mathbf{SL}_2(\mathbf{F}_3)$. Son ordre est 2, 3, 4, 6, 8 ou 24.

Dans les deux derniers cas, la connaissance de $v_p(\Delta)$ ne suffit pas à déterminer l'ordre de Φ_p. On peut simplement affirmer que l'on a

$$\mathrm{Card}(\Phi_p) \cdot v_p(\Delta) \equiv 0 \pmod{12},$$

puisque la valuation de Δ devient divisible par 12 dans le corps L.

b) *Définition de Φ_p lorsque j n'est pas entier en p*

Sur $\mathbf{Q}_p$, la courbe E se déduit de la courbe de Tate de même invariant j par «torsion» au moyen de l'extension quadratique $L=\mathbf{Q}_p(\sqrt{-c_6})$; puisqu'on suppose que E n'est pas semi-stable, cette extension est ramifiée en p. Son groupe de Galois est le groupe Φ_p qui nous intéresse; comme précédemment, on le considère comme un quotient du groupe d'inertie I_p; on a $\Phi_p \simeq \{\pm 1\}$. Si $s \in I_p$ a pour image $\varepsilon(s) = \pm 1$ dans Φ_p, l'automorphisme $\varphi_l(s)$ de E_l ($l \neq p$) a ses deux valeurs propres égales à $\varepsilon(s)$: c'est le produit de $\varepsilon(s)$ par un élément unipotent.

Application au cas où $\varphi_l(G)$ est contenu dans un sous-groupe de Borel

Soit l un nombre premier tel que $\varphi_l(G)$ soit contenu dans un sous-groupe de Borel, et soient $\chi', \chi'' : G \to \mathbf{F}_l^*$ les caractères correspondants.

Vu la théorie du corps de classes, on peut identifier χ' et χ'' à des *caractères de Dirichlet*

$$\chi' : (\mathbf{Z}/f'\mathbf{Z})^* \to \mathbf{F}_l^* \quad \text{et} \quad \chi'' : (\mathbf{Z}/f''\mathbf{Z})^* \to \mathbf{F}_l^*,$$

où f' et f'' sont les conducteurs de χ' et χ''. Ecrivons f' sous la forme $\prod_{p \in P} p^{n'(p)}$. Le groupe $(\mathbf{Z}/f'\mathbf{Z})^*$ se décompose en produit des $(\mathbf{Z}/p^{n'(p)}\mathbf{Z})^*$. La restriction de χ' au p-ième facteur $(\mathbf{Z}/p^{n'(p)}\mathbf{Z})^*$ sera appelée *la p-composante de χ'*, et notée χ'_p; la connaissance de χ'_p équivaut à celle de la restriction de χ' à I_p. Définissons de même la p-composante χ''_p de χ''. Notons S'_E le sous-ensemble de S_E formé des p en lesquels E n'est pas semi-stable. On a alors:

Proposition 23. (a) *Les caractères χ' et χ'' sont non ramifiés en dehors de l et de S'_E. On a*

$$t_p \equiv \chi'(p) + \chi''(p) \pmod{l}$$
$$p \equiv \chi'(p)\,\chi''(p) \pmod{l}$$

pour tout $p \notin S_E$, $p \neq l$.

(b) *Supposons $l \geqq 5$. Soit $p \in S'_E$, $p \neq l$. Alors l'image de χ'_p (resp. χ''_p) dans $\mathbf{F}_l^*$ est isomorphe au groupe Φ_p; c'est un groupe cyclique d'ordre 2, 3, 4 ou 6.*

(c) *Supposons $l \notin S_E$. Alors l'un des caractères χ' et χ'' est non ramifié en l. Si on le note α_l, on a*

$$t_p \equiv \alpha_l(p) + p\,\alpha_l(p)^{-1} \pmod{l} \quad \text{pour tout } p \notin S_E.$$

L'assertion (a) se démontre par des arguments déjà employés à plusieurs reprises. Dans (b) l'hypothèse $l \geqq 5$ sert à assurer qu'un automorphisme d'une courbe elliptique qui laisse fixe un point d'ordre l est l'identité; vu ce qui précède, cela entraîne que χ'_p et χ''_p appliquent *injectivement* Φ_p dans $\mathbf{F}_l^*$. Le groupe Φ_p est donc cyclique, et d'ordre 2, 3, 4 ou 6. La première assertion de (c) se démontre en remarquant que E a, soit bonne réduction de hauteur 1 en l, soit mauvaise réduction de type multiplicatif, et en appliquant les prop. 11 et 13 du § 1. La congruence

$$t_p \equiv \alpha_l(p) + p\,\alpha_l(p)^{-1} \pmod{l} \quad \text{pour } p \notin S_E,$$

résulte de (a) lorsque $p \neq l$. Reste le cas où $p = l \notin S_E$, où l'on doit prouver que $t_l \equiv \alpha_l(l) \pmod{l}$. On remarque d'abord que la réduction $\tilde{E}$ de E en l est de hauteur 1, donc contient un unique sous-groupe d'ordre l. De plus, on sait que l'endomorphisme de Frobenius π_l de $\tilde{E}$ opère sur le sous-groupe en question par multiplication par t_l. La formule cherchée résulte facilement de là, par un argument analogue à celui utilisé au n° 5.4; nous en laissons les détails au lecteur.

Corollaire 1. *Supposons $l \notin S_E$ et $l \geqq 5$. Alors les Φ_p sont cycliques. Avec les notations de* (c), *l'ordre de α_l est le ppcm des ordres des Φ_p; en particulier, on a $\alpha_l^{12} = 1$.*

Le fait que les Φ_p soient cycliques résulte de (b). D'autre part, l'ordre du caractère α_l est le *ppcm* des ordres de ses p-composantes, i.e. des ordres des Φ_p; comme ceux-ci sont des diviseurs de 12, on a $\alpha_l^{12} = 1$.

Corollaire 2. *Les hypothèses étant celles du cor.* 1, *soit p le plus petit nombre premier en lequel E a bonne réduction. On a*:

$$l \leqq (p^{\frac{1}{2}} + 1)^8.$$

D'après (c), on a

$$t_p \equiv z + p z^{-1} \pmod{l},$$

où z est une racine 12-ième de l'unité du corps $\mathbf{F}_l$ (cor. 1). Soient d l'ordre de z, $S_d(X)$ le d-ième polynôme cyclotomique, et $T_p(X) = X^2 - t_p X + p$. La congruence ci-dessus montre que S_d et T_p ont une racine commune (mod. l). Leur *résultant* R est donc un entier divisible par l. Or, on peut décomposer R sous la forme

$$R = \prod (x - \zeta)(x' - \zeta),$$

où x et x' sont les deux racines de T_p (les valeurs propres de π_p), et ζ parcourt l'ensemble des racines primitives d-ièmes de l'unité. On a $|x| = |x'| = p^{\frac{1}{2}}$ et $|\zeta| = 1$, d'où:

$$0 < |R| \leqq (p^{\frac{1}{2}} + 1)^{2n}, \quad \text{où} \quad n = \deg. S_d = \varphi(d).$$

Comme d divise 12, on a $\varphi(d) \leqq 4$, et $|R| \leqq (p^{\frac{1}{2}} + 1)^8$. Puisque l divise R, on a la même inégalité pour l, cqfd.

Donnons une application du corollaire 2:

Proposition 24. *Supposons que j ne soit pas entier; soit $p_0 \in P$ tel que $v_{p_0}(j) < 0$. Soit p le plus petit nombre premier en lequel E a bonne réduction. Si $l \notin S_E$, l ne divise pas $v_{p_0}(j)$ et $l > (p^{\frac{1}{2}} + 1)^8$, on a $\varphi_l(G) = \mathrm{Aut}(E_l)$.*

(Ici encore, on obtient une majoration *effective* des l pour lesquels $\varphi_l(G)$ est distinct de $\mathrm{Aut}(E_l)$.)

On a évidemment $l \geqq 5$. Il en résulte que l ne divise pas $2 v_{p_0}(j)$. Or il existe une extension de $\mathbf{Q}_{p_0}$ de degré $\leqq 2$ sur laquelle E devient du type de Tate; la valuation de j dans cette extension est $v_{p_0}(j)$ ou $2 v_{p_0}(j)$, donc n'est pas divisible par l. D'après MG, p. IV – 20, le groupe d'inertie de $\varphi_l(G)$ en p_0 contient un élément d'ordre l. Si l'on avait $\varphi_l(G) \neq \mathrm{Aut}(E_l)$, le groupe $\varphi_l(G)$ serait contenu dans un sous-groupe de Borel, ce qui est impossible d'après le cor. 2 ci-dessus.

5.7. Courbes à j non entier : exemples numériques

5.7.1. Courbe

$$y^2=x^3+x^2-x; \quad N=2^2 5; \quad \Delta=2^4 5; \quad j=2^{14}/5.$$

Il y a mauvaise réduction de type multiplicatif en 5, et $v_5(\Delta)=1$. Le groupe $\varphi_l(G)$ contient donc un élément d'ordre l, et, s'il est distinct de $\mathrm{Aut}(E_l)$, il est contenu dans un sous-groupe de Borel. D'autre part, il y a mauvaise réduction en 2, et l'on vérifie [7] que le groupe Φ_2 correspondant est cyclique d'ordre 3. On en conclut (cf. n° 5.6) que, si $\varphi_l(G)$ est contenu dans un sous-groupe de Borel, et si $l\geqq 5$, les caractères χ', χ'': $G\to \mathbf{F}_l^*$ correspondants ont une 2-composante dont l'image dans $\mathbf{F}_l^*$ est d'ordre 3; or c'est impossible, car aucun quotient de $(\mathbf{Z}/2^n\mathbf{Z})^*$ n'est d'ordre 3. Cette contradiction *montre que* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 2, 3$. Les cas $l=2$ et $l=3$ font exception: $(0,0)$ est un point d'ordre 2 et $(1,1)$ un point d'ordre 3.

5.7.2. Courbe

$$y^2=x^3-x^2+x; \quad N=2^3 3; \quad \Delta=-2^4 3; \quad j=2^{11}/3.$$

Le fait que $v_2(\Delta)=4$ entraîne que l'ordre de Φ_2 est divisible par 3. Le même argument qu'en 5.7.1 montre alors que $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\geqq 5$. Cette formule est également *vraie pour* $l=3$: il suffit de montrer que $\varphi_3(G)$ contient un élément qui n'est pas contenu dans un sous-groupe de Borel, et l'on peut prendre pour cela l'élément de Frobenius π_5; on a en effet:

$$A_5=8, \quad \text{d'où} \quad \mathrm{Tr}(\pi_5)^2-4\det(\pi_5)=4-20=-16,$$

et -16 n'est pas un carré (mod. 3). Le cas $l=2$ fait exception: $(0,0)$ est un point d'ordre 2.

[Comparer avec MG, p. IV−21, où la même courbe est traitée par une méthode différente, basée sur les résultats de Ogg [18].]

5.7.3. Courbe

$$y^2+xy=x^3-x^2-5; \quad N=-3^2 5; \quad \Delta=-3^7 5; \quad j=-1/3.5.$$

La mauvaise réduction de type multiplicatif en 5 montre que, si $\varphi_l(G)$ est distinct de $\mathrm{Aut}(E_l)$, il est contenu dans un sous-groupe de Borel. Supposons que ce soit le cas, et que $l\geqq 5$; notons χ', χ'': $G\to \mathbf{F}_l^*$ les caractères correspondants. Comme Φ_3 est d'ordre 2, on voit que

[7] Cela se voit, par exemple, en faisant le changement de variables:

$$x=\pi^2 X+1, \quad y=\pi^3 Y+1, \quad \text{où} \quad \pi=\sqrt[3]{2};$$

on obtient l'équation $Y^2+Y=X^3+\pi^4 X^2+\pi^2 X$, où la bonne réduction en l'idéal (π) est évidente.

l'un des caractères χ' et χ'' est non ramifié en dehors de 3, et que sa 3-composante est d'ordre 2; c'est donc le caractère $x \mapsto \left(\frac{x}{3}\right)$, et l'on a

$$t_p \equiv \left(\frac{p}{3}\right) + p\left(\frac{p}{3}\right) \quad \text{(mod. } l\text{)} \qquad \text{pour tout } p \neq 3, 5.$$

Or $A_2 = 2$, $t_2 = 1$ et $\left(\frac{2}{3}\right) = -1$; on a donc $1 \equiv -3$ (mod. l), ce qui est impossible. Cette contradiction montre que $\varphi_l(G) = \mathrm{Aut}(E_l)$ *pour* $l \geqq 5$. Cette formule est également *vraie pour* $l = 3$: cela se voit comme en 5.7.2, en remarquant que $\mathrm{Tr}(\pi_2)^2 - 4\det(\pi_2) = -7$ n'est pas un carré (mod. 3). Le cas $l = 2$ fait exception: $(2, -1)$ est un point d'ordre 2 [8].

5.7.4. Courbe

$$y^2 + xy + y = x^3 + x^2 - 3x + 1; \quad N = 2.5^2; \quad \Delta = -2^5 5^2; \quad j = -5.29^3/2^5.$$

Le fait que $v_5(\Delta) = 2$ montre que Φ_5 est cyclique d'ordre 6. Or il n'existe pas de caractère de G dont la 5-composante ait une image d'ordre 6 (ou 3). Cela suffit à prouver, comme ci-dessus, que, pour $l \neq 3, 5$, $\varphi_l(G)$ ne peut pas être contenu dans un sous-groupe de Borel. D'autre part, la mauvaise réduction de type multiplicatif en 2, jointe au fait que $v_2(\Delta) = 5$, montre que, pour tout $l \neq 5$, $\varphi_l(G)$ contient un élément d'ordre l. On en conclut *que* $\varphi_l(G) = \mathrm{Aut}(E_l)$ *pour* $l \neq 3, 5$. Les cas $l = 3$ et $l = 5$ font exception: $(1, 0)$ est un point d'ordre 5, et E_3 contient un sous-groupe d'ordre 3 stable par G, à savoir celui formé par le point à l'infini et les deux points d'abscisse 0; pour tout $p \neq 2, 5$, on a

$$t_p \equiv 1 + p \text{ (mod. 5)} \quad \text{et} \quad t_p \equiv \left(\frac{p}{5}\right) + p\left(\frac{p}{5}\right) \text{ (mod. 3)}.$$

5.8. Courbes à j entier

C'est le cas le plus difficile: on ne dispose plus des éléments unipotents fournis par la théorie de Tate.

On est amené à examiner les possibilités suivantes:

(a) $\varphi_l(G)$ *est contenu dans un sous-groupe de Borel.*

Ce cas se traite par la méthode du n° 5.6; on trouve une borne *effective* pour l.

(b) $\varphi_l(G)$ *est contenu dans un sous-groupe de Cartan.*

---

[8] Une autre façon de traiter cette courbe consiste à la «tordre» par l'extension quadratique $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$; on la transforme ainsi en la courbe

$$y^2 + xy + y = x^3 + x^2 \qquad (N = 3.5; \Delta = -3.5),$$

qui a l'avantage d'être *semi-stable.*

Ce sous-groupe est nécessairement déployé (si $l \geqq 3$), cf. n° 5.2; il est donc contenu dans un sous-groupe de Borel, et l'on est ramené au cas précédent.

(c) *$\varphi_l(G)$ est contenu dans le normalisateur N_l d'un sous-groupe de Cartan C_l, et n'est pas contenu dans C_l.*

Ce cas se traite de la manière suivante. Supposons $l \geqq 5$ pour simplifier. Notons ε le caractère d'ordre 2 de G défini par composition:

$$G \to \varphi_l(G) \to N_l/C_l \simeq \{\pm 1\}.$$

On dispose des renseignements suivants sur ε:

(c_1) ε est *non ramifié en dehors de* $S_E \cup \{l\}$. C'est clair.

(c_2) Si $l \notin S_E$, ε est *non ramifié en* l, et $\varepsilon(l) = 1$ ou $\varepsilon(l) = -1$ suivant que la réduction de E en l est de hauteur 1 ou de hauteur 2. Cela se voit sur la structure du *groupe de décomposition* D_l de $\varphi_l(G)$ relativement à l, structure qui est donnée par le n° 1.11. Lorsque la hauteur de $\tilde{E}(l)$ est 1, le groupe d'inertie de D_l est un demi-sous-groupe de Cartan, ou un demi-sous-groupe de Borel; comme il est contenu dans N_l, seul le premier cas est possible, et il entraîne que le groupe en question est l'un des demi-sous-groupes de Cartan de C_l (c'est ici que l'hypothèse $l \geqq 5$ intervient, cf. n° 2.2, prop. 14); le groupe D_l est alors contenu dans C_l, ce qui prouve à la fois que ε est non ramifié en l, et que $\varepsilon(l) = 1$. Lorsque la hauteur de $\tilde{E}(l)$ est 2, le groupe d'inertie de D_l est un sous-groupe de Cartan non déployé, donc égal à C_l, et D_l est égal à N_l (n° 1.11, prop. 12); cela prouve bien que ε est non ramifié en l et que $\varepsilon(l) = -1$.

(c_3) Si E a mauvaise réduction de type multiplicatif en p, ε est *non ramifié en p.* Cela se vérifie sur le modèle de Tate.

(c_4) Supposons que E ne soit pas semi-stable en p, et que $p \neq l$. Si le groupe Φ_p correspondant (n° 5.6) est d'ordre 2, 3 ou 6, ε est *non ramifié en p.* En effet, il faut voir que l'image de Φ_p dans $\varphi_l(G)$ est contenue dans C_l; or un élément d'ordre 2 de Φ_p a pour image -1 dans $\mathrm{Aut}(E_l)$, donc appartient à C_l; d'autre part, il est clair qu'un élément d'ordre 3 de Φ_p a une image triviale dans N_l/C_l qui est d'ordre 2.

(c_5) *Si $p \notin S_E$, et $\varepsilon(p) = -1$, on a $t_p \equiv 0 \pmod{l}$.*

Si $p \neq l$, cela revient à dire que la trace de l'élément π_p de $\varphi_l(G)$ est nulle, ce qui est clair puisque π_p appartient à $N_l - C_l$. Si $p = l$, l'hypothèse $\varepsilon(l) = -1$ entraîne que la réduction de E en l est de hauteur 2 (cf. (c_2) ci-dessus) et l'on sait que cela équivaut à $t_l \equiv 0 \pmod{l}$.

Les propriétés (c_1) à (c_4) permettent de faire la liste des caractères ε possibles. Pour chacun d'eux, on considère les p tels que $\varepsilon(p) = -1$, et l'on cherche s'il existe un tel p avec $t_p \neq 0$. Si oui, la condition $t_p \equiv 0 \pmod{l}$ donne une majoration pour l. Sinon, la courbe E a des multiplications complexes par le corps quadratique correspondant à ε.

5.9. Courbes à j entier: exemples numériques

5.9.1. Courbe

$$y^2=x^3-2x^2-x; \quad N=2^7; \quad \Delta=2^7; \quad j=2^5 7^3.$$

Le fait que $v_2(\Delta)=7$ montre que l'ordre de Φ_2 est divisible par 12, donc égal à 12 ou 24; mais $\mathbf{SL}_2(\mathbf{F}_3)$ n'a pas de sous-groupe d'ordre 12; le premier cas est donc impossible, ce qui prouve que Φ_2 est isomorphe à $\mathbf{SL}_2(\mathbf{F}_3)$. L'image de Φ_2 dans $\mathrm{Aut}(E_l)$, $l\geqq 3$, est un groupe d'ordre 24, qui agit de façon irréductible; de plus, ce groupe n'est pas abélien, et ne contient pas de sous-groupe abélien d'indice 2. On déduit de là que $\varphi_l(G)$, pour $l\geqq 3$, ne peut être contenu, ni dans un sous-groupe de Borel, ni dans un normalisateur de sous-groupe de Cartan; comme en outre il contient un sous-groupe de Cartan ou un demi-sous-groupe de Cartan déployé (provenant de l'inertie en l), la prop. 17 du n° 2.7 montre *que* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\geqq 3$ (pour $l=5$, il faut en outre vérifier que $\varphi_l(G)$ contient un élément s tel que $\mathrm{Tr}(s)^2/\det(s)=3$, ce qui se fait en prenant $s=\pi_3$; on a en effet $A_3=6$, d'où $\mathrm{Tr}(\pi_3)^2/\det(\pi_3)=2^2/3\equiv 3 \pmod 5$). Le cas $l=2$ fait exception: $(0,0)$ est un point d'ordre 2.

5.9.2. Courbe[9]

$$y^2=x^3+6x-2; \quad N=2^6 3^3; \quad \Delta=-2^6 3^5; \quad j=2^9 3.$$

Il y a mauvaise réduction en 2 et 3. Le fait que $v_3(\Delta)=5$ montre que Φ_3 est d'ordre 12. L'image de Φ_3 dans $\mathrm{Aut}(E_2)$ est $\Phi_3/\{\pm 1\}$ qui est d'ordre 6; on a *a fortiori* $\varphi_2(G)=\mathrm{Aut}(E_2)$. Pour $l=3$, le fait que Δ ne soit pas un cube montre que $\varphi_3(G)$ contient un élément d'ordre 3 (cf. n° 5.3); d'autre part, on a $A_5=4$, d'où $\mathrm{Tr}(\pi_5)^2-4\det(\pi_5)=-16$ qui n'est pas un carré (mod. 3), et $\varphi_3(G)$ n'est pas contenu dans un sous-groupe de Borel; de ces deux renseignements résulte que $\varphi_3(G)=\mathrm{Aut}(E_3)$. Supposons maintenant $l\geqq 7$; comme $\varphi_l(G)$ contient Φ_3, $\varphi_l(G)$ ne peut être contenu, ni dans un sous-groupe de Borel, ni dans un sous-groupe de Cartan; d'autre part, il contient un sous-groupe de Cartan, ou un demi-sous-groupe de Cartan déployé (dû à l'inertie en l); la prop. 17 du n° 2.7 montre alors que $\varphi_l(G)$ est, soit égal à $\mathrm{Aut}(E_l)$, soit contenu dans le normalisateur N_l d'un sous-groupe de Cartan C_l. Montrons que ce dernier cas est impossible. S'il avait lieu, on en déduirait par

$$\varepsilon\colon G\to\varphi_l(G)\to N_l/C_l\simeq\{\pm 1\}$$

un caractère d'ordre 2 de G, et l'on aurait (cf. n° 5.8):

(*) $\qquad t_p\equiv 0 \pmod l$ si $\varepsilon(p)=-1$ et $p\neq 2,3$.

Le caractère ε est ramifié en 3 (vu la structure de Φ_3), et n'est pas ramifié en dehors de $\{2,3\}$. Prenons alors $p=17$. Comme $p\equiv 1 \pmod 8$, la

[9] Cette courbe m'a été signalée par J. Vélu.

2-composante de ε prend la valeur 1 en p; comme $p \equiv -1 \pmod 3$, la 3-composante de ε prend la valeur -1 en p. On a donc $\varepsilon(p) = -1$, d'où $t_{17} \equiv 0 \pmod l$. Or on trouve que $A_{17} = 24$, d'où $t_{17} = -6$. La congruence ci-dessus est donc impossible, d'où $\varphi_l(G) = \mathrm{Aut}(E_l)$. Le même argument s'applique à $l = 5$, à cela près qu'il faut en outre vérifier l'existence dans $\varphi_5(G)$ d'un élément s tel que $\mathrm{Tr}(s)^2/\det(s) = 3$; l'élément π_{17} convient. En définitive, *on a* $\varphi_l(G) = \mathrm{Aut}(E_l)$ *pour tout* l.

5.9.3. Courbe

$$y^2 + xy = x^3 - x^2 - 2x - 1; \quad N = 7^2; \quad \Delta = -7^3; \quad j = -3^3 5^3.$$

Il y a mauvaise réduction en 7, et Φ_7 est d'ordre 4. Cherchons si, pour $l \neq 2, 7$, il est possible que $\varphi_l(G)$ soit contenu dans le normalisateur N_l d'un sous-groupe de Cartan C_l, sans être contenu dans C_l. Le caractère $\varepsilon\colon G \to \{\pm 1\}$ correspondant est ramifié seulement en 7; c'est donc le caractère de Legendre $a \mapsto \left(\frac{a}{7}\right)$. On en conclut que, si $\left(\frac{p}{7}\right) = -1$, on a $t_p \equiv 0 \pmod l$. Les plus petites valeurs de p telles que $\left(\frac{p}{7}\right) = -1$ sont 3, 5, 13, 17; on trouve chaque fois que $t_p = 0$. Cela suggère que E *a des multiplications complexes* par le corps $\mathbf{Q}(\sqrt{-7})$; effectivement, on constate (cf. [5], p. 295) que $-3^3 5^3 = j\left(\frac{1+\sqrt{-7}}{2}\right)$, de sorte que E a pour anneau d'endomorphismes (sur $\bar{\mathbf{Q}}$) l'anneau des entiers de $\mathbf{Q}(\sqrt{-7})$. On déduit facilement de là que, pour $l \neq 2, 7$, $\varphi_l(G)$ est un normalisateur de sous-groupe de Cartan, alors que, pour $l = 2, 7$, $\varphi_l(G)$ est contenu dans un sous-groupe de Borel; en particulier, *on a* $\varphi_l(G) \neq \mathrm{Aut}(E_l)$ *pour tout* l.

5.9.4. Courbe

$$y^2 + xy = x^3 + x^2 - 2x - 7; \quad N = 11^2; \quad \Delta = -11^4; \quad j = -11^2.$$

(Cette courbe a la propriété remarquable d'avoir un sous-groupe d'ordre 11 stable par G, cf. Vélu [35].)

Il y a mauvaise réduction en 11, et Φ_{11} est d'ordre 3. Soit $l \neq 11$; si $\varphi_l(G)$ était contenu dans un sous-groupe de Borel, les deux caractères $\chi', \chi''\colon G \to \mathbf{F}_l^*$ correspondants auraient une 11-composante dont l'image serait d'ordre 3, ce qui est impossible puisque $11 - 1$ n'est pas divisible par 3; ainsi $\varphi_l(G)$ ne peut pas être contenu dans un sous-groupe de Borel, ni *a fortiori* dans un sous-groupe de Cartan déployé. Il ne peut pas être contenu dans un sous-groupe de Cartan non déployé (n° 5.2). Il ne peut pas être contenu dans le normalisateur N_l d'un sous-groupe de Cartan C_l, car le caractère d'ordre 2 correspondant serait partout non ramifié

(du fait que Φ_{11} est d'ordre 3), ce qui est impossible. Enfin, pour $l=5$, $\varphi_l(G)$ contient un élément s tel que $\mathrm{Tr}(s)^2/\det(s)=3$, à savoir π_2 (on vérifie en effet que $A_2=2$, d'où $t_2=1$ et $t_2^2/2=1/2\equiv 3 \pmod 5$). Ces divers renseignements entraînent *que* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 11$, cf. n° 2.7. Le cas $l=11$ fait exception, en vertu du résultat de Vélu cité ci-dessus; on a $t_p\equiv p^4+p^7 \pmod{11}$ pour tout $p\neq 11$.

5.10. Un exemple sur le corps $\mathbf{Q}(\sqrt{29})$

Dans ce n°, le corps de base K est le corps quadratique réel $\mathbf{Q}(\sqrt{29})$. L'anneau O_K des entiers de K est principal. On a

$$O_K=\mathbf{Z}[\varepsilon], \quad \text{où } \varepsilon=\frac{5+\sqrt{29}}{2} \text{ est l'unité fondamentale.}$$

La norme de ε est -1. Le groupe des unités totalement positives est engendré par $\varepsilon^2=1+5\varepsilon$.

On prend pour courbe elliptique E la cubique d'équation

$$y^2+xy+\varepsilon^2 y=x^3.$$

On a:

$$b_2=1, \quad b_4=\varepsilon^2, \quad b_6=\varepsilon^4, \quad b_8=0, \quad c_4=1-24\varepsilon^2,$$

et

$$\Delta=b_4^3-27b_6^2=\varepsilon^6-27\varepsilon^8=-\varepsilon^{10}.$$

Le fait que Δ soit une unité montre que E *a partout bonne réduction*[10].

Si v est une place ultramétrique de K, nous notons comme d'habitude A_v le nombre de points de la réduction de E en v; on a

$$A_v=1+Nv-t_v, \quad \text{où } t_v=\mathrm{Tr}(\pi_v).$$

Nous aurons besoin de quelques valeurs de A_v:

$p_v=2$, $Nv=4$ donne $A_v=6$, $t_v=-1$, $\mathrm{Tr}(\pi_v)^2-4\det(\pi_v)=-15$;

$p_v=5$, $Nv=5$ donne $A_v=9$, $t_v=-3$, $\mathrm{Tr}(\pi_v)^2-4\det(\pi_v)=-11$;

$p_v=7$, $Nv=7$ donne $A_v=6$, $t_v=2$, $\mathrm{Tr}(\pi_v)^2-4\det(\pi_v)=-24$.

Passons à la détermination des $\varphi_l(G)$. Commençons par quelques cas particuliers:

a) $l=2$. *On a* $\varphi_2(G)=\mathrm{Aut}(E_2)$. En effet, on a vu que $Nv=5$ donne $t_v=-3\equiv 1 \pmod 2$, ce qui montre que $\varphi_2(G)$ contient un élément d'ordre 3. D'autre part, $\Delta=-\varepsilon^{10}$ n'est pas un carré dans K, et $\varphi_2(G)$ contient donc un élément d'ordre 2, cf. n° 5.3.

[10] La courbe E m'a été signalée par Tate, qui a obtenu des exemples analogues sur d'autres corps quadratiques, aussi bien réels qu'imaginaires.

b) $l=3$. Le point $(0,0)$ est d'ordre 3. D'autre part Δ n'est pas un cube, donc $\varphi_3(G)$ contient un élément d'ordre 3 (n° 5.3); comme $\det \varphi_3(G)=\mathbf{F}_3^*$, on en conclut que $\varphi_3(G)$ *est un demi-sous-groupe de Borel* $\begin{pmatrix}1 & * \\ 0 & *\end{pmatrix}$. On a $t_v \equiv 1+Nv \pmod 3$ pour tout v.

c) $l=29$. Le corps $\mathbf{Q}(\sqrt{29})$ est contenu dans le corps cyclotomique $\mathbf{Q}(\mu_{29})$. Il en résulte que $\det \varphi_{29}(G)$ est l'ensemble des *carrés* de $\mathbf{F}_{29}^*$. D'autre part, on a vu que

$$Nv=4 \quad \text{donne} \quad \mathrm{Tr}(\pi_v)^2-4\det(\pi_v)=-15 \quad \text{et} \quad \left(\frac{-15}{29}\right)=-1,$$

$$Nv=7 \quad \text{donne} \quad \mathrm{Tr}(\pi_v)^2-4\det(\pi_v)=-24 \quad \text{et} \quad \left(\frac{-24}{29}\right)=1.$$

En appliquant la prop. 19 du n° 2.8, on en déduit *que* $\varphi_{29}(G)$ *est le sous-groupe d'indice* 2 *de* $\mathrm{Aut}(E_{29})$ *formé des éléments dont le déterminant est un carré dans* $\mathbf{F}_{29}$.

Supposons maintenant $l \geqq 5$ et $l \neq 29$. Le corps $\mathbf{Q}(\sqrt{29})$ est disjoint du corps cyclotomique $\mathbf{Q}(\mu_l)$, ce qui montre que $\det \varphi_l(G)$ est égal à $\mathbf{F}_l^*$. D'autre part:

i) Le groupe $\varphi_l(G)$ *ne peut pas être contenu dans un sous-groupe de Cartan non déployé*: cela se voit comme dans le cas de $\mathbf{Q}$, en utilisant la conjugaison complexe, cf. n° 5.2, iv).

ii) Le groupe $\varphi_l(G)$ *ne peut pas être contenu dans le normalisateur* N_l *d'un sous-groupe de Cartan* C_l *sans être contenu dans* C_l. En effet, le caractère $G \to \{\pm 1\}$ correspondant serait non ramifié (n° 4.2, lemme 2); or un tel caractère n'existe pas, puisque O_K est principal et contient une unité de norme -1 (le groupe des classes d'idéaux «au sens strict» est réduit à $\{1\}$).

iii) Cherchons *si* $\varphi_l(G)$ *peut être contenu dans un sous-groupe de Borel.* Supposons que ce soit le cas, et notons $\chi', \chi'': G \to \mathbf{F}_l^*$ les caractères correspondants. Ces caractères sont non ramifiés en dehors des places v divisant l. Supposons d'abord qu'il n'y ait qu'une telle place, i.e. que $\left(\frac{l}{29}\right)=-1$. D'après le n° 1.11, la réduction de E en v est de hauteur 1, et l'un des caractères χ', χ'' est non ramifié en v, donc partout, et il est égal à 1, cf. ci-dessus. On a donc

$$t_v \equiv 1+Nv \pmod l \quad \text{si} \quad p_v \neq l.$$

En prenant $Nv=4$, $t_v=-1$, on a $6 \equiv 0 \pmod l$, ce qui est impossible puisque $l \geqq 5$.

Supposons maintenant qu'il y ait deux places v_1 et v_2 divisant l, i.e. que $\left(\frac{l}{29}\right)=1$. D'après le n° 1.11, la réduction de E en v_1 (resp. v_2) est de hauteur 1, et l'un des caractères χ', χ'' est non ramifié en v_1 (resp. v_2). Si c'est le même caractère qui est non ramifié en v_1 et v_2, ce caractère est égal à 1, et le même raisonnement que ci-dessus montre que c'est impossible. Reste le cas où, par exemple, χ' est non ramifié en v_1, et ramifié en v_2 (auquel cas c'est le «caractère fondamental de hauteur 1» en v_2, d'après le n° 1.11). *Un tel caractère n'existe que si* $l=5$. En effet, notons $\mathfrak{p}_2$ l'idéal premier correspondant à v_2. La théorie du corps de classes permet d'interpréter χ' comme un homomorphisme de $(O_K/\mathfrak{p}_2)^*$ dans $\mathbf{F}_l^*$, égal à 1 sur toute unité totalement positive; de plus, le fait que χ' soit le caractère fondamental signifie que, si l'on identifie $O_K/\mathfrak{p}_2$ au corps $\mathbf{F}_l$, l'homomorphisme $\chi'\colon \mathbf{F}_l^* \to \mathbf{F}_l^*$ ainsi obtenu est *l'application identique*. Comme ε^2 engendre le groupe des unités totalement positives, on voit que $\varepsilon^2-1=5\varepsilon$ doit être contenu dans $\mathfrak{p}_2$, ce qui équivaut à $l=5$.

Enfin, si $l\neq 29$, le groupe $\varphi_l(G)$ contient, soit un sous-groupe de Cartan non déployé, soit un demi-sous-groupe de Cartan déployé, cf. n° 1.11. En combinant ce renseignement avec ceux fournis par i), ii), iii) ci-dessus, on voit *que* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\geqq 7$, $l\neq 29$.

Reste le cas $l=5$. On a vu que $Nv=4$ donne un élément π_v tel que $\mathrm{Tr}(\pi_v)=-1$, $\det(\pi_v)=4$, d'ou $\mathrm{Tr}(\pi_v)^2-4\det(\pi_v)=-15$. Comme la valuation 5-adique de -15 est 1, on déduit de là (cf. Shimura [32], lemme 1) que l'image de π_v dans $\mathrm{Aut}(E_5)$ est représentable matriciellement par $\begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix}$, donc est d'ordre 10. En particulier, $\varphi_5(G)$ contient un élément d'ordre 5. Vu ce qui a été démontré plus haut, cela ne laisse que les deux possibilités suivantes:

5_1) On a $\varphi_5(G)=\mathrm{Aut}(E_5)$.

5_2) Le groupe $\varphi_5(G)$ est un sous-groupe de Borel $\begin{pmatrix}* & *\\ 0 & *\end{pmatrix}$ et les deux caractères χ', χ'' correspondants sont les caractères fondamentaux relatifs aux deux places v_1 et v_2 de K de caractéristique résiduelle 5, cf. iii) ci-dessus. En termes des t_v, cette dernière propriété se traduit de la manière suivante: pour tout $v\in\Sigma$, choisissons un générateur totalement positif α_v de l'idéal premier de O_K défini par v; on a alors:

$$t_v\equiv \mathrm{Tr}_{K/\mathbf{Q}}(\alpha_v) \pmod 5.$$

On notera que cette congruence est satisfaite lorsque $Nv=4$, 5 et 7, comme on le voit en prenant $\alpha_v=2$, $1+\varepsilon$ (ou $6-\varepsilon$), et $1+2\varepsilon$ (ou $11-2\varepsilon$). Cela laisse penser que c'est 5_2) qui est correct et non 5_1), autrement dit *que* $\varphi_5(G)$ *est un sous-groupe de Borel de* $\mathrm{Aut}(E_5)$. C'est effectivement le cas.

Pour le démontrer, il suffit de vérifier que E_5 contient un sous-groupe d'ordre 5 stable par G, ou, ce qui revient au même (cf. Fricke [11], p. 399) que l'invariant modulaire j de E peut s'écrire sous la forme $(\tau^2+10\tau+5)^3/\tau$, avec $\tau\in K$; or c'est bien exact: on prend $\tau=\varepsilon-14=-(1+\varepsilon)^3/\varepsilon^2$.

En définitive, *on a* $\varphi_l(G)=\mathrm{Aut}(E_l)$ *pour* $l\neq 3, 5, 29$.

La courbe de Shimura

Dans [33], § 7.5 (voir aussi [32]), Shimura construit une certaine courbe elliptique E_1 sur $K=\mathbf{Q}(\sqrt{29})$ qui a des propriétés très voisines de celles de la courbe E ci-dessus: elle a bonne réduction partout (Casselman [3]), et même nombre de points que E aux places divisant 2, 3, 5, 7, 13; les traces $t_v(E_1)$ des éléments de Frobenius de E_1 satisfont aux mêmes congruences que les $t_v(E)$, à savoir:

$$t_v(E_1)\equiv 1+Nv \qquad (\mathrm{mod.}\ 3)$$

$$t_v(E_1)\equiv \mathrm{Tr}_{K/\mathbf{Q}}(\alpha_v) \quad (\mathrm{mod.}\ 5).$$

(La seconde congruence est démontrée dans [33], p. 206; la première résulte de l'expression de la fonction zêta de E_1 donnée par Shimura, combinée avec les formules de Hecke [13], p. 787 et p. 905.)

La courbe E_1 possède une isogénie de degré 5 sur sa conjuguée E_1^σ, où σ désigne l'automorphisme non trivial de K. La courbe E jouit d'une propriété analogue: cela se vérifie à partir des résultats de Fricke (*loc. cit.*) en remarquant que l'on a $\tau\,\tau^\sigma=125$, avec les notations ci-dessus.

Les arguments utilisés dans le cas de E pour déterminer $\varphi_l(G)$ s'appliquent sans changement à E_1. En particulier, *le groupe de Galois de* $(E_1)_l$ *est* $\mathbf{GL}_2(\mathbf{F}_l)$ *pour* $l\neq 3, 5, 29$. Il serait intéressant de voir si E_1 est isogène (ou même isomorphe) à E.

§ 6. Produits de deux courbes elliptiques

Dans ce §, E et E' désignent deux courbes elliptiques sur un corps de nombres algébriques K. Les notations E_n, φ_n, ρ_l, T_l, V_l relatives à E sont celles définies dans l'*Introduction* et dans le § 4. On utilise pour E' les notations correspondantes E'_n, φ'_n, ρ'_l, T'_l, V'_l.

Les notations relatives à K sont celles des §§ 3, 4. En particulier, la lettre G désigne le groupe de Galois $\mathrm{Gal}(\bar{K}/K)$.

6.1. Courbes sans multiplication complexe

Si n est un entier $\geqq 1$, les homomorphismes

$$\varphi_n\colon G\to \mathrm{Aut}(E_n), \qquad \varphi'_n\colon G\to \mathrm{Aut}(E'_n)$$

définissent un homomorphisme

$$\psi_n\colon G\to \mathrm{Aut}(E_n)\times \mathrm{Aut}(E'_n).$$

Comme $\det \varphi_n = \det \varphi'_n$, l'image de ψ_n est contenue dans le sous-groupe A_n de $\mathrm{Aut}(E_n) \times \mathrm{Aut}(E'_n)$ formé des couples (s, s') tels que $\det(s) = \det(s')$ dans $(\mathbf{Z}/n\mathbf{Z})^*$.

Par passage à la limite sur n, on obtient un homomorphisme

$$\psi_\infty : G \to A_\infty = \varprojlim A_n,$$

où A_∞ est un certain sous-groupe fermé du groupe $\mathrm{Aut}(E_\infty) \times \mathrm{Aut}(E'_\infty)$. Plus précisément, on a

$$A_\infty = \prod_{l \in P} A_{l\infty},$$

où $A_{l\infty}$ est le sous-groupe de $\mathbf{GL}(T_l) \times \mathbf{GL}(T'_l)$ formé des couples (s, s') tels que $\det(s) = \det(s')$ dans $\mathbf{Z}_l^*$.

Théorème 6. *Faisons les hypothèses suivantes:*

i) *E et E' n'ont pas de multiplication complexe.*

ii) *Les systèmes de représentations l-adiques (ρ_l) et (ρ'_l) attachés à E et E' ne deviennent isomorphes sur aucune extension finie de K.*

Le groupe $\psi_\infty(G)$ est alors un sous-groupe ouvert du groupe A_∞ défini ci-dessus.

La démonstration sera donnée au n° 6.2.

Corollaire 1. *Pour tout $l \in P$, l'image de G dans $\mathbf{GL}(T_l) \times \mathbf{GL}(T'_l)$ par (ρ_l, ρ'_l) est un sous-groupe ouvert de $A_{l\infty}$; pour presque tout l, cette image est égale à $A_{l\infty}$.*

En particulier:

Corollaire 2. *Pour presque tout $l \in P$, on a $\psi_l(G) = A_l$.*

Remarques. 1) L'hypothèse ii) entraîne:

iii) *E et E' ne sont pas $\bar{K}$-isogènes.*

Il est probable que ii) et iii) sont *équivalentes*; c'est vrai lorsque l'invariant modulaire j de E n'est pas un entier (MG, p. IV – 14); il serait très intéressant de le démontrer dans le cas général.

2) Supposons i) vérifiée. On peut montrer que ii) est alors équivalente à chacune des conditions suivantes:

iv) *Il n'existe pas de caractère continu $\varepsilon : G \to \{\pm 1\}$ tel que ρ'_l soit isomorphe à $\varepsilon \otimes \rho_l$ pour tout l* (ou pour *un* l, cela revient au même).

v) *Il existe $v \in \Sigma$ tel que E et E' aient bonne réduction en v et que $t_v(E') \neq \pm t_v(E)$.*

(L'équivalence de ii) et iv) se démontre par un argument de descente galoisienne; l'implication v) $\Rightarrow$ iv) est immédiate; l'implication ii) $\Rightarrow$ v) résulte du th. 6.)

3) Soit K^{cycl} le sous-corps de $\bar{K}$ obtenu en adjoignant à $\bar{K}$ toutes les racines de l'unité (cf. n° 4.4). On peut reformuler le th. 6 de la manière suivante:

Théorème 6'. *Sous les hypothèses* i) *et* ii), *l'image de* $\mathrm{Gal}(\bar{K}/K^{\mathrm{cycl}})$ *dans* $\prod_{l\in P} \mathbf{SL}(T_l)\times\mathbf{SL}(T_l')$ *est ouverte.*

Convenons de dire que deux extensions galoisiennes M et M' d'un corps L sont *presque disjointes* si $M\cap M'$ est de degré fini sur L, ou, ce qui revient au même, si $\mathrm{Gal}(M'M/L)$ est un sous-groupe *ouvert* de $\mathrm{Gal}(M/L)\times\mathrm{Gal}(M'/L)$. Le th. 6' équivaut à:

Théorème 6''. *Soient* $K(E_\infty)$ *et* $K(E'_\infty)$ *les sous-corps de* $\bar{K}$ *obtenus en adjoignant à* K *les coordonnées des points de* E_∞ *et de* E'_∞. *Ces corps contiennent* K^{cycl}. *Si les hypothèses* i) *et* ii) *sont satisfaites, les extensions* $K(E_\infty)/K^{\mathrm{cycl}}$ *et* $K(E'_\infty)/K^{\mathrm{cycl}}$ *sont presque disjointes.*

6.2. Démonstration du théorème 6

Elle utilise plusieurs lemmes:

Lemme 7. *Pour tout* $l\in P$, *l'image* G_{l^∞} *de* G *dans* $\mathbf{GL}(T_l)\times\mathbf{GL}(T_l')$ *est un sous-groupe ouvert de* A_{l^∞}.

Notons $\mathfrak{g}_l$ (resp. $\mathfrak{h}_l$) la $\mathbf{Q}_l$-algèbre de Lie du groupe de Lie l-adique G_{l^∞} (resp. A_{l^∞}). Vu la définition de A_{l^∞}, $\mathfrak{h}_l$ est la sous-algèbre de

$$\mathrm{End}(V_l)\times\mathrm{End}(V_l')$$

formée des couples (u,u') tels que $\mathrm{Tr}(u)=\mathrm{Tr}(u')$. On a $\mathfrak{g}_l\subset\mathfrak{h}_l$, et le lemme revient à dire que $\mathfrak{g}_l=\mathfrak{h}_l$. Comme E et E' n'ont pas de multiplication complexe, les projections $\mathfrak{g}_l\to\mathrm{End}(V_l)$ et $\mathfrak{g}_l\to\mathrm{End}(V_l')$ sont surjectives. Or, il est facile de déterminer les sous-algèbres de $\mathfrak{h}_l$ qui ont cette propriété. On trouve que, si $\mathfrak{g}_l\neq\mathfrak{h}_l$, $\mathfrak{g}_l$ est le graphe d'un isomorphisme de $\mathbf{Q}_l$-algèbres de Lie

$$\alpha\colon \mathrm{End}(V_l)\to\mathrm{End}(V_l')$$

transformant 1 en 1; cette dernière propriété montre que α est bien déterminé par sa restriction à $\mathfrak{sl}(V_l)$. Or, tout automorphisme de l'algèbre de Lie $\mathfrak{sl}_2$ provient d'un élément de $\mathbf{PGL}_2$; on en conclut qu'il existe une application $\mathbf{Q}_l$-linéaire bijective f de V_l sur V_l' telle que $\alpha(u)=f\circ u\circ f^{-1}$ pour tout $u\in\mathrm{End}(V_l)$, et $\mathfrak{g}_l$ est l'ensemble des couples $(u,f\circ u\circ f^{-1})$. L'application $f\colon V_l\to V_l'$ est un isomorphisme de $\mathfrak{g}_l$-modules. D'après la théorie de Lie, il existe donc un sous-groupe ouvert U de G_{l^∞} tel que f soit un *isomorphisme de U-modules.* Si K' est l'extension finie de K correspondant à U, on voit que ρ_l et ρ_l' deviennent isomorphes après extension des scalaires à K', ce qui contredit l'hypothèse ii). On a donc nécessairement $\mathfrak{g}_l=\mathfrak{h}_l$, d'où le lemme.

Lemme 8. *Soit l un nombre premier $\geqq 5$. Supposons que les homomorphismes*

$$\varphi_l\colon G \to \mathrm{Aut}(E_l) \quad et \quad \varphi'_l\colon G \to \mathrm{Aut}(E'_l)$$

soient surjectifs, et que $\psi_l\colon G \to A_l$ ne le soit pas. Il existe alors un caractère continu $\varepsilon_l\colon G \to \{\pm 1\}$ et un isomorphisme f du groupe E_l sur le groupe E'_l tels que

$$f \circ \varphi_l(s) = \varepsilon_l(s)\, \varphi'_l(s) \circ f \quad pour\ tout\ s \in G.$$

En outre, ε_l est non ramifié en toute place ultramétrique non ramifiée sur **Q** *en laquelle E et E' ont bonne réduction.*

Posons $B = \mathrm{Aut}(E_l)$, $B' = \mathrm{Aut}(E'_l)$, $H = \psi_l(G)$ et $A = A_l$, de sorte que l'on a:

$$H \subset A \subset B \times B', \quad H \neq A, \quad \mathrm{pr}_1 H = B, \quad \mathrm{pr}_2 H = B'.$$

Identifions B au sous-groupe $B \times \{1\}$ de $B \times B'$, et posons $N = B \cap H$. Définissons de même $N' = B' \cap H$. Il résulte des propriétés ci-dessus que N est distingué dans B et N' distingué dans B'; de plus, l'image de H dans $B/N \times B'/N'$ est le graphe d'un isomorphisme $\alpha\colon B/N \to B'/N'$ (cf. Bourbaki, A.I, p. 124, exerc. 7). Du fait que H est contenu dans A, on a $N \subset \mathbf{SL}(E_l)$; on voit facilement que, si N était *égal* à $\mathbf{SL}(E_l)$, on aurait $H = A$. On a donc $N \neq \mathbf{SL}(E_l)$; comme N est distingué dans $B = \mathrm{Aut}(E_l)$, cela entraîne que N est contenu dans le centre $\{\pm 1\}$ de $\mathbf{SL}(E_l)$. On a de même $N' \subset \{\pm 1\}$. Le *centre* de B/N est $\mathbf{F}_l^*/N$ et celui de B'/N' est $\mathbf{F}_l^*/N'$. L'isomorphisme $\alpha\colon B/N \to B'/N'$ applique donc $\mathbf{F}_l^*/N$ sur $\mathbf{F}_l^*/N'$ et induit par passage au quotient un isomorphisme $\tilde{\alpha}$ du groupe $B/\mathbf{F}_l^* = \mathbf{PGL}(E_l)$ sur le groupe $\mathbf{PGL}(E'_l)$. Mais on sait que tout automorphisme de $\mathbf{PGL}_2(\mathbf{F}_l)$ est intérieur. On en conclut qu'il existe un isomorphisme $f\colon E_l \to E'_l$ tel que $\tilde{\alpha}(u) = f \circ u \circ f^{-1}$ pour tout $u \in \mathbf{PGL}(E_l)$. Cela signifie que, si $h = (u, u')$ est un élément de H, il existe une homothétie $\varepsilon(h) \in \mathbf{F}_l^*$ telle que

$$u' = \varepsilon(h)\, f \circ u \circ f^{-1}.$$

Prenant les déterminants des deux membres, on obtient $\varepsilon(h)^2 = 1$, et ε est une application de H dans $\{\pm 1\}$; on vérifie immédiatement que c'est un homomorphisme. Le composé de ε et de l'homomorphisme $\psi_l\colon G \to H$ est le caractère ε_l cherché. La formule ci-dessus montre que l'on a bien

$$f \circ \varphi_l(s) = \varepsilon_l(s)\, \varphi'_l(s) \circ f \quad \text{pour tout } s \in G.$$

En d'autres termes, f définit un isomorphisme du G-module E_l sur le G-module déduit de E'_l par «torsion» au moyen de ε_l.

Soit $v \in \Sigma$. Supposons que E et E' aient bonne réduction en v, et que v soit non ramifiée sur **Q**, i.e. que son indice de ramification $e(v)$ soit égal à 1. Il nous faut prouver que ε_l *est non ramifié en* v. C'est clair si $p_v \neq l$. Supposons que $p_v = l$. Choisissons une clôture algébrique k_l de $\mathbf{F}_l$;

notons λ_1 et λ_2 (resp. λ'_1 et λ'_2) les caractères du groupe d'inertie modérée en v, à valeurs dans k_l^*, intervenant dans le module galoisien $E_l \otimes k_l$ (resp. $E'_l \otimes k_l$), cf. n° 1.11. Si l'on note ε_v la restriction de ε_l au groupe d'inertie en v, on a (quitte à permuter λ'_1 et λ'_2):

$$(*) \qquad \lambda_1 = \varepsilon_v \lambda'_1 \quad \text{et} \quad \lambda_2 = \varepsilon_v \lambda'_2 .$$

Comme $e(v)=1$, les corollaires aux prop. 11 et 12 montrent que les λ_i et λ'_i sont, soit le caractère 1, soit un caractère fondamental de niveau 1 ou 2. Leurs invariants dans $(\mathbf{Q}/\mathbf{Z})'$ (cf. n° 1.7) appartiennent à l'ensemble

$$X = \left\{0, \frac{1}{l-1}, \frac{1}{l^2-1}, \frac{l}{l^2-1}\right\}.$$

Puisque $\varepsilon_v^2 = 1$, l'invariant de ε_v est 0 ou $\frac{1}{2}$; d'autre part les formules (*) montrent que cet invariant est de la forme $x - x'$, avec $x, x' \in X$. Or, si $l \geqq 5$, on vérifie que $\frac{1}{2}$ n'est pas de la forme $x - x'$. L'invariant de ε_v est donc égal à 0, ce qui signifie que $\varepsilon_v = 1$, i.e. que ε_l est non ramifié en v, et achève la démonstration du lemme.

Lemme 9. *On a $\psi_l(G) = A_l$ pour presque tout l.*

Raisonnons par l'absurde, et soit L une partie infinie de P telle que $\psi_l(G) \neq A_l$ pour tout $l \in L$. Quitte à retrancher de L un ensemble fini, on peut supposer que, pour tout $l \in L$, on a $l \geqq 5$ et que les homomorphismes

$$\varphi_l : G \to \mathrm{Aut}(E_l) \quad \text{et} \quad \varphi'_l : G \to \mathrm{Aut}(E'_l)$$

sont surjectifs (cf. n° 4.2, th. 2). Si $l \in L$, notons ε_l le caractère de G à valeurs dans $\{\pm 1\}$ défini dans le lemme 8. Il résulte de ce lemme que les ε_l sont non ramifiés en dehors d'un ensemble fini de places de K, indépendant de l. Cela entraîne, comme on sait, que les ε_l sont *en nombre fini*. Quitte à remplacer L par une partie infinie, on peut donc supposer que ε_l est indépendant de l; notons-le ε. Le caractère ε correspond à une extension K' de K de degré $\leqq 2$; posons $G' = \mathrm{Gal}(\bar{K}/K') = \mathrm{Ker}(\varepsilon)$. D'après le lemme 8, pour tout $l \in L$, les G'-modules E_l et E'_l sont isomorphes. On en déduit que, si v est une place de K' en laquelle E et E' ont bonne réduction, les traces des endomorphismes de Frobenius des réductions de E et E' en v satisfont aux congruences:

$$t_v(E) \equiv t_v(E') \pmod{l} \quad \text{pour tout } l \in L, \quad l \neq p_v .$$

Comme L est infini, cela entraîne $t_v(E) = t_v(E')$, ce qui montre que les systèmes de représentations l-adiques attachés à E et E' deviennent isomorphes sur K' (cf. MG, p. IV – 15); cela contredit l'hypothèse ii).

Lemme 10. *Soit l un nombre premier $\geqq 5$, et soit H un sous-groupe fermé de $\mathbf{GL}_2(\mathbf{Z}_l) \times \mathbf{GL}_2(\mathbf{Z}_l)$. On suppose que l'image de H dans*

$$\mathbf{GL}_2(\mathbf{F}_l) \times \mathbf{GL}_2(\mathbf{F}_l)$$

par réduction (mod. l) *contient* $\mathbf{SL}_2(\mathbf{F}_l) \times \mathbf{SL}_2(\mathbf{F}_l)$. *Alors H contient* $\mathbf{SL}_2(\mathbf{Z}_l) \times \mathbf{SL}_2(\mathbf{Z}_l)$.

Soit H' l'adhérence du groupe des commutateurs de H. C'est un sous-groupe de $\mathbf{SL}_2(\mathbf{Z}_l) \times \mathbf{SL}_2(\mathbf{Z}_l)$ et son image par réduction (mod. l) contient le groupe dérivé de $\mathbf{SL}_2(\mathbf{F}_l) \times \mathbf{SL}_2(\mathbf{F}_l)$, qui est $\mathbf{SL}_2(\mathbf{F}_l) \times \mathbf{SL}_2(\mathbf{F}_l)$ lui-même puisque $l \geqq 5$. Tout revient à montrer que $H' = \mathbf{SL}_2(\mathbf{Z}_l) \times \mathbf{SL}_2(\mathbf{Z}_l)$. Soit X l'intersection de H' et de $\mathbf{SL}_2(\mathbf{Z}_l) \times \{1\}$; soit Y l'ensemble des éléments de H' dont la seconde composante est congrue à 1 (mod. l). On a $Y \supset X$, et le quotient Y/X est un pro-l-groupe. Soient $\tilde{Y}$ et $\tilde{X}$ les images de Y et de X dans $\mathbf{SL}_2(\mathbf{F}_l)$ par réduction (mod. l) de la première composante. Par hypothèse, on a $\tilde{Y} = \mathbf{SL}_2(\mathbf{F}_l)$; d'autre part, $\tilde{Y}/\tilde{X}$ est isomorphe à un quotient de Y/X, donc est un l-groupe. Comme $\mathbf{SL}_2(\mathbf{F}_l)$ n'a aucun sous-groupe distingué (à part lui-même) d'indice une puissance de l, on a $\tilde{X} = \tilde{Y} = \mathbf{SL}_2(\mathbf{F}_l)$. D'après le lemme 3 de MG, p. IV – 23, cela entraîne que $X = \mathbf{SL}_2(\mathbf{Z}_l) \times \{1\}$. Ainsi, H' contient le premier facteur du produit $\mathbf{SL}_2(\mathbf{Z}_l) \times \mathbf{SL}_2(\mathbf{Z}_l)$; un argument analogue montre qu'il contient le second; il est donc égal à $\mathbf{SL}_2(\mathbf{Z}_l) \times \mathbf{SL}_2(\mathbf{Z}_l)$, ce qui démontre le lemme.

Dans l'énoncé suivant, J_v désigne le plus petit sous-groupe distingué fermé de G contenant les groupes d'inertie relatifs aux places de $\overline{K}$ prolongeant v, cf. n° 4.4.

Lemme 11. *Pour presque tout v, $\psi_\infty(J_v)$ est égal au l-ième facteur $A_{l\infty}$ de A, avec $l = p_v$.*

Posons $H_v = \psi_\infty(J_v)$. D'après le lemme 9 et le th. 4 du n° 4.4, on a, pour presque tout v:

a) H_v est contenu dans le l-ième facteur $A_{l\infty}$ de A, où $l = p_v$.
b) Les projections $H_v \to \mathbf{GL}(T_l)$ et $H_v \to \mathbf{GL}(T_l')$ sont surjectives.
c) $\psi_l(G) = A_l$.

Supposons ces propriétés vérifiées, ainsi que l'inégalité $l \geqq 5$. Soit $\tilde{H}_v = \psi_l(J_v)$ l'image de H_v dans $\mathrm{Aut}(E_l) \times \mathrm{Aut}(E_l')$ par réduction (mod. l). D'après b) et c), les deux projections $\tilde{H}_v \to \mathrm{Aut}(E_l)$ et $\tilde{H}_v \to \mathrm{Aut}(E_l')$ sont surjectives, et $\tilde{H}_v$ est un sous-groupe distingué de $A_l = \psi_l(G)$. Il est facile de voir que ces propriétés entraînent $\tilde{H}_v = A_l$. Appliquant le lemme 10, on en conclut que H_v contient $\mathbf{SL}(T_l) \times \mathbf{SL}(T_l')$; vu b), cela entraîne bien $H_v = A_{l\infty}$.

Fin de la démonstration du théorème 6

Le lemme 11 montre qu'il existe une partie finie S de P telle que $\psi_\infty(G)$ contienne les facteurs $A_{l\infty}$ de A_∞ pour $l \in P - S$. Tout revient donc

à prouver que l'image de $\psi_\infty(G)$ dans le produit des $A_{l\infty}$, pour $l \in S$, est *ouverte*, ce qui résulte du lemme 7 combiné à un argument standard sur les groupes de Sylow (MG, p. IV – 24, démonstration du lemme 4).

Remarque. La démonstration ci-dessus se prête à des calculs numériques du genre de ceux du § 5. Par exemple, le lecteur vérifiera que, si l'on prend pour E et E' les courbes 5.5.6 et 5.5.7 du n° 5.5, et pour K le corps $\mathbf{Q}$, on a $\psi_l(G) = A_l$ pour tout $l \in P$.

6.3. Courbes à multiplications complexes

On a un résultat analogue à celui du théorème 6'' :

Théorème 7. *Supposons que les courbes E et E' ne soient pas $\bar{K}$-isogènes, et que l'une au moins ait des multiplications complexes. Alors les extensions $K(E_\infty)/K^{\mathrm{cycl}}$ et $K(E'_\infty)/K^{\mathrm{cycl}}$ sont presque disjointes.*

(On peut aussi formuler ce résultat dans le style des ths. 6 et 6'; nous en laissons le soin au lecteur.)

Comme E et E' jouent des rôles symétriques, il suffit de prouver le th. 7 dans chacun des cas suivants:

a) E' a des multiplications complexes (que l'on peut supposer définies sur K), et E n'en a pas. Si l'on pose $L = K(E_\infty) \cap K(E'_\infty)$, l'extension L/K est abélienne, puisque contenue dans $K(E'_\infty)/K$. Il en résulte (cf. n° 4.4, *Remarque*) que $\mathrm{Gal}(K(E_\infty)/L)$ est un sous-groupe ouvert de $\prod_{l \in P} \mathbf{SL}(T_l)$, donc un sous-groupe ouvert de $\mathrm{Gal}(K(E_\infty)/K^{\mathrm{cycl}})$, ce qui montre bien que l'extension L/K^{cycl} est de degré fini.

b) E et E' ont des multiplications complexes par des corps quadratiques imaginaires F et F', que l'on peut supposer contenus dans K. Puisque E et E' ne sont pas $\bar{K}$-isogènes, les corps F et F' sont distincts. De plus, l'action de G sur E_∞ et E'_∞ est une action abélienne, décrite par le th. 5 du n° 4.5. En particulier le groupe de Galois de $K(E_\infty)/K$ s'identifie à un sous-groupe ouvert du produit des $U_l(F)$. En explicitant ce que signifie le th. 7, on est ramené à l'énoncé suivant, dont la vérification est élémentaire:

Soit $\theta_l : U_l(K) \to U_l(F) \times U_l(F')$ l'homomorphisme défini par N_{K_l/F_l} et N_{K_l/F'_l}; l'image de θ_l est contenue dans le groupe H_l formé des couples (u, u') tels que $N_{F_l/\mathbf{Q}_l}(u) = N_{F'_l/\mathbf{Q}_l}(u')$, et, pour tout l (resp. pour presque tout l), θ_l est une application *ouverte* (resp. *surjective*) de $U_l(K)$ dans H_l.

Bibliographie

1. Artin, E.: Geometric algebra. New York: Interscience Publ. 1957 (trad. française par M. Lazard. Paris: Gauthier-Villars 1962).
2. Billing, G., Mahler, K.: On exceptional points on cubic curves. J. London Math. Soc. **15**, 32 – 43 (1940).

3. Casselman, W.: On abelian varieties with many endomorphisms and a conjecture of Shimura. Inventiones math. **12**, 225–236 (1971).
4. Cassels, J.: Diophantine equations with special reference to elliptic curves. J. London Math. Soc. **41**, 193–291 (1966).
5. Cassels, J., Fröhlich, A. (*ed.*): Algebraic number theory. New York: Academic Press 1967.
6. Curtis, C., Reiner, I.: Representation theory of finite groups and associative algebras. New York: Interscience Publ. 1962.
7. Deligne, P.: Formes modulaires et représentations l-adiques. Séminaire Bourbaki, 1968/69, exposé **355**: Lecture Notes in Math. **179**. Berlin-Heidelberg-New York: Springer 1971.
8. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg **14**, 197–272 (1941).
9. Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. Gött. Nach., 85–94 (1953); II, *ibid.*, 13–42 (1955); III, *ibid.*, 37–76 (1956); IV, *ibid.*, 55–80 (1957).
10. Deuring, M.: Die Klassenkörper der komplexen Multiplikation. Enz. Math. Wiss., Band I–2, Heft 10, Teil II. Stuttgart: Teubner 1958.
11. Fricke, R.: Lehrbuch der Algebra, Bd. III. Braunschweig: Fried. Vieweg & Sohn 1928.
12. Fröhlich, A.: Formal groups. Lecture Notes in Math. **74**. Berlin-Heidelberg-New York: Springer 1968.
13. Hecke, E.: Mathematische Werke. Göttingen: Vandenhoeck und Ruprecht 1959.
14. Lubin, J.: Finite subgroups and isogenies of one-parameter formal Lie groups. Ann. of. Math. **85**, 296–302 (1967).
15. Mumford, D.: Abelian varieties. Oxford Univ. Press 1970.
16. Néron, A.: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Publ. Math. I.H.E.S. **21**, 1–128 (1964).
17. Neumann, O.: Zur Reduktion der elliptischen Kurven. Math. Nach. **46**, 285–310 (1970).
18. Ogg, A.: Abelian curves of 2-power conductor. Proc. Camb. Phil. Soc. **62**, 143–148 (1966).
19. Ogg, A.: Elliptic curves and wild ramification. Amer. J. of Math. **89**, 1–21 (1967).
20. Ogg, A.: Rational points of finite order on elliptic curves. Inventiones math. **12**, 105–111 (1971).
21. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. En préparation.
22. Roquette, P.: Analytic theory of elliptic functions over local fields. Göttingen: Vandenhoeck und Ruprecht 1970.
23. Šafarevič, I.: Corps de nombres algébriques (en russe). Proc. Inter. Congr. Math. Stockholm, 163–176 (1962) [Trad. anglaise: Amer. Math. Transl., ser. 2, vol. **31**, 25–39 (1963)].
24. Serre, J.-P.: Sur les corps locaux à corps résiduel algébriquement clos. Bull. Soc. Math. France **89**, 105–154 (1961).
25. Serre, J.-P.: Corps Locaux (2ème édition). Paris: Hermann 1968.
26. Serre, J.-P.: Groupes de Lie l-adiques attachés aux courbes elliptiques. Colloque Clermont-Ferrand, 239–256, C.N.R.S. 1964.
27. Serre, J.-P.: Abelian l-adic representations and elliptic curves. New York: Benjamin 1968 (cité MG).
28. Serre, J.-P.: Une interprétation des congruences relatives à la fonction τ de Ramanujan. Séminaire Delange-Pisot-Poitou, 1967/68, n° **14**.
29. Serre, J.-P.: Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou, 1969/70, n° **19**.

30. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. of Math. **88**, 492 – 517 (1968).
31. Shimura, G.: A reciprocity law in non-solvable extensions. J. Crelle **221**, 209 – 220 (1966).
32. Shimura, G.: Class fields over real quadratic fields in the theory of modular functions. Lecture Notes **185** (Several complex variables II), p. 169 – 188. Berlin-Heidelberg-New York: Springer 1971.
33. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, n° 11, Tokyo-Princeton, 1971.
34. Shimura, G., Taniyama, Y.: Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan **6** (1961).
35. Vélu, J.: Courbes elliptiques sur **Q** ayant bonne réduction en dehors de {11}. C.R. Acad. Sci. Paris **273**, 73 – 75 (1971).
36. Weber, H.: Lehrbuch der Algebra, Bd. II (zw. Auf.). Braunschweig 1899.
37. Weil, A.: Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. **55**, 497 – 508 (1949).
38. Weil, A.: Jacobi sums as "Größencharaktere". Trans. Amer. Math. Soc. **73**, 487 – 495 (1952).
39. Weil, A.: On a certain type of characters of the idèle-class group of an algebraic number-field. Proc. Int. Symp., Tokyo-Nikko, 1 – 7 (1955).
40. Weil, A.: On the theory of complex multiplication. Proc. Int. Symp., Tokyo-Nikko, 9 – 22 (1955).
41. Weil, A.: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. **168**, 149 – 156 (1967).
42. Weil, A.: Basic number theory. Berlin-Heidelberg-New York: Springer 1967.

J.-P. Serre
Collège de France
F-75 Paris 5
France

(Reçu le 29 novembre 1971)