PÉRIODES ET REPRÉSENTATIONS GALOISIENNES, NOTES DU COURS DE M2

par

Pierre Colmez

Table des matières

Introduction

Groupes de Galois et représentations p-adiques. — Si K est un corps, on note G_K son groupe de Galois absolu ; c'est un invariant subtil du corps K, et le groupe $\mathrm{G}_{\mathbf{Q}}$ (par exemple) est un groupe extrêmement mystérieux. Une manière efficace d'obtenir des renseignements à son sujet, est d'étudier ses représentations, et en particulier ses représentations p-adique (i.e. un module libre de rang fini sur $\mathbf{Z}_p$ ou un espace vectoriel de dimension finie[(1)] sur $\mathbf{Q}_p$ muni d'une action linéaire continue de G).

[(1)] Cela revient au même car si V est une représentation p-adique de G_K, il existe un $\mathbf{Z}_p$-réseau T de V stable par G_K. En effet, si T_0 est un $\mathbf{Z}_p$-réseau quelconque de V, $\mathrm{G}_K \times T_0$ est compact et son image Y par $(g,v) \mapsto g \cdot v$ est compacte et donc incluse dans un réseau T_1. Le sous-$\mathbf{Z}_p$-module de V engendré par Y est alors stable par G_K par construction, et est un réseau puisqu'il contient le réseau T_0 et est contenu dans le réseau T_1.

La géométrie algébrique fournit des représentations p-adiques de $\mathrm{G}_{\mathbf{Q}}$ en abondance (cohomologie étale des variétés algébriques définies sur $\mathbf{Q}$), et l'étude de ces représentations s'est révélée être une aide précieuse pour des tas de questions de théorie des nombres. Par exemple, la démonstration de Wiles du théorème de Fermat s'appuie de manière cruciale sur l'étude des représentations de $\mathrm{G}_{\mathbf{Q}}$ attachées aux courbes elliptiques et aux formes modulaires.

Maintenant, si on fixe un plongement de $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_\ell$, pour tout nombre premier ℓ, on peut voir $\mathrm{G}_{\mathbf{Q}_\ell}$ comme un sous-groupe de $\mathrm{G}_{\mathbf{Q}}$, et les $\mathrm{G}_{\mathbf{Q}_\ell}$ engendrent topologiquement $\mathrm{G}_{\mathbf{Q}}$. La manière dont les $\mathrm{G}_{\mathbf{Q}_\ell}$ se mélangent dans $\mathrm{G}_{\mathbf{Q}}$, est très mystérieuse, mais on peut obtenir énormément d'informations sur une représentation p-adique de $\mathrm{G}_{\mathbf{Q}}$ en regardant sa restriction à $\mathrm{G}_{\mathbf{Q}_\ell}$, pour ℓ premier. Pour des raisons topologiques, c'est la restriction à $\mathrm{G}_{\mathbf{Q}_p}$ qui fournit les renseignements les plus subtils.

Ces notes se veulent une introduction à ce sujet difficile à travers l'exemple concret du module de Tate des courbes elliptiques. L'étude de ce cas particulier permet d'illustrer un grand nombre de phénomènes généraux en réduisant le bagage de géométrie algébrique à un strict minimum.

$2i\pi$ et le caractère cyclotomique. — L'exemple le plus simple de telles représentations est le module de Tate[(2)] $T_p(\mathbf{G}_m)$ du groupe multiplicatif[(3)] $\mathbf{G}_m$, c'est-à-dire l'ensemble des suites $u = (1, u_1, \dots, u_n, \dots)$, où u_n est une racine p-ième de l'unité dans $\overline{K}$ et $u_{n+1}^p = u_n$ pour tout n. Si K n'est pas de caractéristique p, le groupe μ_{p^n} des racines p-ièmes de l'unité est cyclique isomorphe à $\mathbf{Z}/p^n\mathbf{Z}$, et stable par G_K qui agit par un caractère à valeurs dans $(\mathbf{Z}/p^n\mathbf{Z})^*$. En passant à la limite projective, cela montre que $T_p(\mathbf{G}_m)$ est un $\mathbf{Z}_p$-module de rang 1 muni d'une action de G_K agissant par un caractère $\chi : \mathrm{G}_K \to \mathbf{Z}_p^*$ appelé le *caractère cyclotomique*. Il est d'usage de noter $\mathbf{Z}_p(1)$ la représentation de G_K ainsi obtenue.

Pour faire le lien avec les périodes des courbes elliptiques, remarquons que $\mathbf{G}_m(\mathbf{C}) = \mathbf{C}^*$ n'est pas simplement connexe (le lacet correspondant au cercle unité parcouru dans le sens direct n'est pas contractile dans $\mathbf{C}^*$, et il engendre le groupe $H_1(\mathbf{C}^*, \mathbf{C}) \cong \mathbf{Z}$ des lacets à homotopie près dans $\mathbf{C}^*$ [rendu abélien, sinon on a défini $\pi_1(\mathbf{C}^*)$, mais ce dernier est déjà abélien]). Par ailleurs, si on note X la variable de la droite affine, la forme différentielle $\frac{dX}{X}$ est homolorphe sur $\mathbf{G}_m$ et invariante par translation par un élément de $\mathbf{G}_m$ (i.e. par multiplication). L'intégration d'une forme différentielle le long d'un chemin fournit alors une application $u \mapsto \int_u \frac{dX}{X}$ de $H_1(\mathbf{C}^*, \mathbf{Z})$ dans $\mathbf{C}$ dont l'image est $\Lambda = 2i\pi\mathbf{Z}$, et l'exponentielle $z \mapsto e^z$ est un isomorphisme de groupes (et de surfaces de Riemann) de $\mathbf{C}/\Lambda$ sur $\mathbf{C}^*$. On dispose alors d'une application naturelle de $H_1(\mathbf{C}^*, \mathbf{Z})$ dans $\mathbf{Z}_p(1)$, à savoir celle envoyant u sur $(1, u_1, \dots, u_n, \dots)$, où u_n est la racine

(2) Si A est un groupe abélien (i.e. un $\mathbf{Z}$-module), le module de Tate $T_p(A)$ de A est l'ensemble des suites $u = (0, u_1, \dots, u_n, \cdots)$ d'éléments de A vérifiant $[p] \cdot u_{n+1} = u_n$, pour tout n, où $[p]$ désigne la multiplication par p dans le $\mathbf{Z}$-module A. C'est aussi la limite projective (les applications de transition étant la multiplication par p) des $A[p^n]$, où $A[p^n]$ désigne le noyau de la multiplication par p dans A, et c'est un $\mathbf{Z}_p$-module de manière naturelle comme limite projective de $\mathbf{Z}_p$-modules, l'action de $\mathbf{Z}_p$ sur $A[p^n]$ se faisant à travers $\mathbf{Z}_p/p^n\mathbf{Z}_p = \mathbf{Z}/p^n\mathbf{Z}$.
Si G est un groupe algébrique défini sur un corps K, on note $T_p(G)$ le module de Tate de $T_p(G(\overline{K}))$.

(3) C'est la droite affine privée de 0 muni de la loi de groupe donnée par la multiplication.

p^n-ième de l'unité définie par $u_n = \exp\left(p^{-n}\int_u \frac{dX}{X}\right)$; d'où un isomorphisme naturel $\mathbf{Z}_p(1) \cong \mathbf{Z}_p \otimes H_1(\mathbf{C}^*, \mathbf{Z})$ qui permet de voir $\mathbf{Z}_p(1)$ comme un analogue galoisien de $2i\pi\mathbf{Z}$.

Périodes et module de Tate des courbes elliptiques. — Soit K un corps de nombres. Une courbe elliptique définie sur K est une courbe projective lisse E d'équation (affine) $Y^2 = 4X^3 - g_2X - g_3$ (il y a un point à l'infini dans la direction verticale). Une telle courbe est munie (prop. 1.8 et commentaires) d'une loi d'addition définie sur K, d'élément neutre le point à l'infini (noté 0), la somme de trois points étant nulle si et seulement si ces trois points sont alignés (avec des conventions évidentes dans le cas de points confondus). Une bonne manière de visualiser ce qu'on obtient est de plonger K dans $\mathbf{C}$; l'ensemble $E(\mathbf{C})$ des points de E dans $\mathbf{C}$ est une surface de Riemann qui est topologiquement un tore, et on dispose (th. 1.5) d'un isomorphisme de groupes de $\mathbf{C}/\Lambda$ sur $E(\mathbf{C})$, où Λ est un certain réseau de $\mathbf{C}$. Cela permet en particulier de montrer que $E(\mathbf{C})[p^n]$ est isomorphe à $(\mathbf{Z}/p^n\mathbf{Z})^2$ pour tout n.

Le réseau Λ est le réseau des périodes de la forme différentielle $\omega = \frac{dX}{Y}$. Plus généralement, l'intégration d'une forme différentielle le long d'un chemin fournit (th. 1.18) une application « périodes complexes » bilinéaire de $H^1_{\mathrm{dR}}(E) \times H_1(E(\mathbf{C}), \mathbf{Z})$ dans $\mathbf{C}$, où $H^1_{\mathrm{dR}}(E)$ est le K-espace vectoriel de dimension 2 engendré par les formes différentielles (de seconde espèce) ω et $\eta = X\frac{dX}{Y}$, et $H_1(E(\mathbf{C}), \mathbf{Z})$ est le groupe des lacets à homotopie près sur $E(\mathbf{C})$ (rendu abélien, mais il l'est déjà dans le cas d'un tore) ; l'application « périodes complexes » envoie le couple (α, u) sur l'intégrale $\int_u \alpha$ de α le long de u. On dispose de la formule de Legendre (th. 1.18)

$$\int_u \omega \int_v \eta - \int_v \omega \int_u \eta = 2i\pi, \quad \text{si } (u, v) \text{ est une base orientée de } H_1(E(\mathbf{C}), \mathbf{Z}),$$

qui montre en particulier que cet accouplement est non dégénéré puisque son déterminant est non nul.

Comme la loi d'addition est définie sur K, le groupe $E(\overline{K})[p^n]$, isomorphe à $(\mathbf{Z}/p^n\mathbf{Z})^2$ est stable par l'action de G_K pour tout n, et $T_p(E)$ est un $\mathbf{Z}_p$-module de rang 2 muni d'une action de G_K ; autrement dit, c'est une représentation p-adique de G_K. Si on reprend notre plongement de K dans $\mathbf{C}$, on dispose d'une application naturelle de $H_1(E(\mathbf{C}), \mathbf{Z})$ dans $T_p(E)$, à savoir celle envoyant $u \in H_1(E(\mathbf{C}), \mathbf{Z})$ sur $(0, u_1, \dots, u_n, \dots)$, où u_n est l'image de $p^{-n}\int_u \omega \in \mathbf{C}$ mod Λ via l'isomorphisme $\mathbf{C}/\Lambda \cong E(\mathbf{C})$ mentionné ci-dessus. On en déduit un isomorphisme naturel $T_p(E) \cong \mathbf{Z}_p \otimes_{\mathbf{Z}} H_1(E(\mathbf{C}), \mathbf{Z})$.

Nous allons établir un certain nombre de résultats concernant cette représentation p-adique.

(i) La représentation $\det T_p(E)$ est isomorphe (rem. 1.20) à $\mathbf{Z}_p(1)$; c'est un analogue algébrique de la formule de Legendre.

(ii) L'image de G_K dans $\mathrm{GL}(T_p(E)) \cong \mathrm{GL}_2(\mathbf{Z}_p)$ dépend beaucoup des endomorphismes de E ; dans le cas de multiplication complexe, cette image est abélienne (rem. 1.23), alors que dans le cas contraire, l'image est ouverte dans $\mathrm{GL}_2(\mathbf{Z}_p)$ d'après un théorème de Serre.

(iii) La restriction de $T_p(E)$ à $\mathrm{G}_{K_\mathfrak{l}}$, où $\mathfrak{l}$ est une place de K au-dessus de $\ell \neq p$ est non ramifiée, si E a bonne réduction[4] en $\mathfrak{l}$ (th. 1.29). Si E a réduction multiplicative, la représentation n'est plus non ramifiée, mais l'action de l'inertie est unipotente d'après un théorème de Tate (n° 1.3.5).

(iv) Un théorème général de Grothendieck (th. 1.37) montre que l'action de l'inertie devient toujours unipotente si on la restreint à une extension finie, dans le cas où $\ell \neq p$.

(v) L'étude du cas $\ell = p$ est nettement plus délicate (l'action de l'inertie est fort loin d'être unipotente en général) et relève de ce que l'on appelle la théorie des périodes p-adiques ou la théorie de Hodge p-adique. Par analogie avec le cas complexe, on aimerait construire une application « périodes p-adiques ». Comme $H^1_{\mathrm{dR}}(E)$ est défini sur K, il a un sens dans tout corps contenant K ; par contre $H_1(E(\mathbf{C}), \mathbf{Z})$ n'en a pas a priori, mais on peut utiliser l'isomorphisme $T_p(E) \cong \mathbf{Z}_p \otimes_{\mathbf{Z}} H_1(E(\mathbf{C}), \mathbf{Z})$ mentionné ci-dessus pour lui en donner un en p-adique. On est donc ramené à essayer de construire un accouplement bilinéaire de $H^1_{\mathrm{dR}}(E) \times T_p(E)$ dans $\mathbf{C}_p$, et comme le groupe $\mathrm{G}_{K_\mathfrak{p}}$ agit continûment sur $T_p(E)$ et $\mathbf{C}_p$, on veut que cet accouplement commute à cette action, et qu'il soit non dégénéré pour ne pas perdre d'information. Il y a une obstruction à l'existence d'un tel accouplement car Tate a démontré que $\mathbf{C}_p$ ne contient pas d'analogue de $2i\pi$, et la formule de Legendre montre que le déterminant de cet accouplement doit être égal à $2i\pi$. Ceci a conduit Fontaine à la construction de l'anneau $\mathbf{B}^+_{\mathrm{dR}}$ « des nombres complexes p-adiques », qui s'est révélé un outil incontournable pour l'étude des représentations p-adiques de G_K, où K est un corps de nombres ou une extension finie de $\mathbf{Q}_p$.

1. Courbes elliptiques

1.1. Généralités. — Une courbe elliptique[5] E sur un corps K de caractéristique différente[6] de 2 ou 3, est une courbe projective de $\mathbf{P}^2$ d'équation (*de Weierstrass*) $ZY^2 = 4X^3 - g_2XZ^2 - g_3Z^3$ (ou $Y^2 = X^3 + AX + B$ suivant ce qu'on veut faire), avec $g_2, g_3 \in K$ et $\Delta = g_2^3 - 27g_3^2 \neq 0$ (ou $4A^3 + 27B^2 \neq 0$), cette condition signifiant que le polynôme $4X^3 - g_2X - g_3$ (ou $X^3 + AX + B$) n'a que des racines simples et que E est une courbe lisse.

On préfère généralement se placer dans le plan affine $Z = 1$, et l'équation de E devient $Y^2 = 4X^3 - g_2X - g_3$ (ou $Y^2 = X^3 + AX + B$), le point $\infty = [0 : 1 : 0]$ devenant le seul point de E à l'infini ; il correspond à la direction des droites verticales.

On remarque que si $u \in K^*$, le changement de variables $X = u^{-2}X'$ et $Y = u^{-3}Y'$ transforme l'équation $Y^2 = 4X^3 - g_2X - g_3$ en $(Y')^2 = 4(X')^3 - u^4g_2X - u^6g_3$ et donc transforme le couple (g_2, g_3) en (u^4g_2, u^6g_3) et Δ en $u^{12}\Delta$. Par contre, $j = \frac{(12g_2)^3}{\Delta}$ reste inchangé ; c'est *l'invariant* j de

[4] Et réciproquement d'après le critère de Ogg-Néron-Shafaravich.

[5] On pourra consulter les ouvrages suivants :

- Koblitz, Introduction to elliptic curves and modular forms, GTM97
- Silverman, The arithmetic of elliptic curves, GTM106,
- Silverman, Advanced topics in the arithmetic of elliptic curves, GTM151.

[6] Le but de ces notes n'est pas de développer une théorie complète des courbes elliptiques. Pour traiter des caractéristiques 2 et 3, il faut partir d'une équation de Weierstrass générale, de la forme $Y^2 + a_1XY + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^6$, ce qui alourdit passablement les formules...

la courbe elliptique d'équation $Y^2 = 4X^3 - g_2X - g_3$. Réciproquement, *si K est algébriquement clos*, il est facile de montrer que si $Y^2 = 4X^3 - g_2X - g_3$ et $Y^2 = 4X^3 - g_2'X - g_3'$ sont deux équations de Weierstrass telles que $j = j'$, alors il existe $u \in K$ tel que $g_2' = u^4 g_2$ et $g_3' = u^6 g_3$, ce qui fait que $(X, Y) \mapsto (u^{-2}X, u^{-3}Y)$ induit un isomorphisme de E d'équation $Y^2 = 4X^3 - g_2X - g_3$ sur E' d'équation $Y^2 = 4X^3 - g_2'X - g_3'$. En résumé, *sur un corps algébriquement clos, deux courbes elliptiques ayant même invariant j sont isomorphes.*

Le corps $K(E)$ des fonctions rationnelles sur K est $K(X)[Y]/(Y^2 - 4X^3 + g_2X + g_3)$, et on note $\Omega^1_{K(E)/K}$ le quotient du module des différentielles de Kähler de $K(E)$ par les sous-module engendré par les da, pour $a \in K$ (autrement dit, on voit les éléments de K comme des constantes, et on peut appliquer les règles de dérivation dont on a l'habitude : $df = \frac{\partial f}{\partial X}dX + \frac{\partial f}{\partial Y}dY$, si $f \in K(E)$; de plus comme $Y^2 = 4X^3 - g_2X - g_3$, on a $2YdY = (12X^2 - g_2)dX$, ce qui montre que $\Omega^1_{K(E)/K}$ est un $K(E)$-espace vectoriel de dimension 1 engendré par dX (ou par dY). L'élément $\omega = \frac{dX}{Y}$ de $\Omega^1_{K(E)/K}$ joue un grand rôle dans ce qui va suivre.

1.2. Courbes elliptiques sur C

1.2.1. Réseaux et fonctions elliptiques. — Un *réseau* de $\mathbf{C}$ est un $\mathbf{Z}$-module engendré par une base ω_1, ω_2 de $\mathbf{C}$ sur $\mathbf{R}$. De manière équivalente, un sous-groupe Λ de $\mathbf{C}$ est un réseau si et seulement si la surface de Riemann $\mathbf{C}/\Lambda$ est compacte ; c'est alors un tore complexe, et le groupe $H_1(\mathbf{C}/\Lambda, \mathbf{Z})$, abélianisé du groupe $\pi_1(\mathbf{C}/\Lambda)$ des lacets (à homotopie près) dans $\mathbf{C}/\Lambda$ est un $\mathbf{Z}$-module de rang 2 engendré par les lacets images des segments $[a, a + \omega_1]$ et $[a, a + \omega_2]$, où $a \in \mathbf{C}$ est quelconque (en fait, le groupe $\pi_1(\mathbf{C}/\Lambda)$ est déjà abélien, et donc il n'y a pas besoin de l'abélianiser, mais dans le cas d'une surface de Riemann X quelconque, il faut effectivement abélianiser pour passer de $\pi_1(X)$ à $H_1(X, \mathbf{Z})$).

Si Λ est un réseau de $\mathbf{C}$, une *fonction elliptique* (pour le réseau Λ) est une fonction méromorphe sur $\mathbf{C}$, périodique de période Λ (i.e. $f(z + \omega) = f(z)$ quels que soient $z \in \mathbf{C}$ et $\omega \in \Lambda$; si ω_1, ω_2 est une base de Λ sur $\mathbf{Z}$, il suffit de vérifier que $f(z + \omega_1) = f(z)$ et $f(z + \omega_2) = f(z)$, quel que soit $z \in \mathbf{C}$).

On note $\mathbf{C}(\mathbf{C}/\Lambda)$ l'ensemble des fonctions elliptiques pour Λ ; c'est un corps de manière évidente qui peut être vu comme le corps des fonctions holomorphes de la surface de Riemann $\mathbf{C}/\Lambda$ dans la sphère de Riemann $\mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$.

Le résultat suivant est une conséquence immédiate du théorème de Liouville (une fonction holomorphe bornée sur $\mathbf{C}$ est constante), mais il a des tas de conséquences mirifiques.

Théorème 1.1. — *Une fonction elliptique holomorphe est constante.*

Si $w \in \mathbf{C}/\Lambda$, et si $f \in \mathbf{C}(\mathbf{C}/\Lambda)$, on note $v_w(f) \in \mathbf{Z}$ l'ordre de f en w (i.e. en n'importe quel point de $\mathbf{C}$ ayant pour image w modulo Λ).

Théorème 1.2. — *Si $f \in \mathbf{C}(\mathbf{C}/\Lambda)^*$, alors*

$$\sum_{w \in \mathbf{C}/\Lambda} v_w(f) = 0 \quad \text{et} \quad \sum_{w \in \mathbf{C}/\Lambda} v_w(f) w = 0 \text{ dans } \mathbf{C}/\Lambda.$$

Ce théorème se démontre, via la formule des résidus, en intégrant $\frac{f'(z)}{f(z)}\,dz$ et $z\frac{f'(z)}{f(z)}\,dz$ sur le bord d'un domaine fondamental bien choisi de $\mathbf{C}$ modulo l'action de Λ (de la forme $\{a+t_1\omega_1+t_2\omega_2, 0 \leqslant t_1, t_2 < 1\}$). Remarquons que les sommes ci-dessus sont en fait des sommes finies car une fonction méromorphe sur $\mathbf{C}$ n'a qu'un nombre fini de pôles et de zéros dans un ensemble borné (et donc dans un domaine fondamental du type précédent), et que $v_w(f)w$ a un sens dans $\mathbf{C}/\Lambda$ car $v_w(f) \in \mathbf{Z}$. Finalement, la première formule peut s'exprimer sous la forme : *une fonction elliptique a autant de zéros que de pôles* (comptés avec multiplicité) ; comme les pôles sont en général faciles à déterminer, cela permet d'en déduire des tas de renseignements concernant les zéros.

1.2.2. La fonction $\wp$ de Weierstrass. — Soit Λ un réseau de $\mathbf{C}$. On définit une fonction $\wp(z,\Lambda)$ (ou $\wp(z)$ si Λ est fixé) de $z \in \mathbf{C}$, et des nombres $G_{2k}(\Lambda) \in \mathbf{C}$ (série d'Eisenstein de poids $2k$, notée juste G_{2k}, si Λ est fixé), pour $k \geqslant 2$ (on a $G_{2k+1}(\Lambda) = 0$ car $\Lambda = -\Lambda$, si $k \geqslant 1$), en posant :

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda-\{0\}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big) \quad \text{et} \quad G_{2k}(\Lambda) = \sum_{\omega\in\Lambda-\{0\}} \frac{1}{\omega^{2k}}.$$

On montre facilement que la série définissant $\wp(z,\Lambda)$ converge uniformément sur tout compact de $\mathbf{C}$, et donc que $\wp(z,\Lambda)$ est une fonction méromorphe paire sur $\mathbf{C}$, holomorphe en dehors de pôles doubles en les points de Λ, et que $\wp$ est périodique de période Λ en commençant par démontrer que $\wp'(z,\Lambda) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$ l'est et en utilisant la parité de $\wp$. De plus, en développant $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$ en série entière autour de 0, on voit que l'on a, dans un voisinage de 0,

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{k\geqslant 1} (2k+1)G_{2k+2}\, z^{2k}.$$

Théorème 1.3. — *Soient Λ un réseau de $\mathbf{C}$, et $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$, $g_3 = g_3(\Lambda) = 140G_6(\Lambda)$.*

(i) *Pour tout $z \in \mathbf{C}/\Lambda$, on a $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.*

(ii) $\Delta = \Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0$.

(iii) *$z \mapsto \phi_\Lambda(z) = [\wp(z) : \wp'(z) : 1]$ est un isomorphisme de surfaces de Riemann compactes de $\mathbf{C}/\Lambda$ sur $E_\Lambda(\mathbf{C})$, où E_Λ est la courbe elliptique d'équation $ZY^2 = 4X^3 - g_2XZ^2 - g_3Z^3$ dans $\mathbf{P}^2(\mathbf{C})$, le point 0 étant envoyé sur le point à l'infini $[0:1:0]$ de E_Λ.*

(iv) *En envoyant $\wp$ sur X et $\wp'$ sur Y, on obtient un isomorphisme de $\mathbf{C}(\mathbf{C}/\Lambda)$ sur le corps $\mathbf{C}(X)[Y]/(Y^2 - 4X^3 + g_2XZ^2 + g_3Z^3)$ des fractions rationnelles sur E_Λ. En particulier, le corps des fonctions elliptiques est engendré par $\wp$ et $\wp'$.*

Démonstration. — Le (i) se démontre en constatant que $\wp'(z)^2 - 4\wp(z)^3 - g_2\wp(z) - g_3$ est une fonction elliptique holomorphe nulle en 0. Les points (ii) et (iii) reposent sur l'étude des zéros de la fonction $\wp - a$, pour a dans $\mathbf{C}$: comme cette fonction a pour seul pôle un pôle double en 0, elle a deux zéros comptés avec multiplicité, et comme elle est paire ses deux zéros sont de la forme w et $-w$ (avec un pôle double si $w = -w$ dans $\mathbf{C}/\Lambda$). Le point (iv) se démontre en remarquant que $\wp'$ est impaire et donc que toute fonction elliptique peut s'écrire sous la forme $f + \wp' g$, où f et g sont paires ; il n'y a plus qu'à démontrer qu'une fonction elliptique paire f est

une fraction rationnelle en $\wp$, ce qui se fait en comparant les zéros et pôles de f et un produit de $(\wp(z)-\wp(a))^{n_a}$.

Remarque 1.4. — (i) Une forme différentielle holomorphe sur $\mathbf{C}/\Lambda$ est de la forme $f(z)dz$, où $f(z)$ est une fonction elliptique holomorphe, et comme une telle fonction est constante, on voit que l'espace $H^0(\mathbf{C}/\Lambda,\Omega^1)$ est le $\mathbf{C}$-espace vectoriel de dimension 1 engendré par dz.

(ii) Comme $\mathbf{C}$ est simplement connexe, le groupe $\pi_1(\mathbf{C}/\Lambda,0)$ des lacets dans $\mathbf{C}/\Lambda$ de base 0 est égal à Λ, et donc $H_1(\mathbf{C}/\Lambda,\mathbf{Z})$ qui en est l'abélianisé est isomorphe à $\mathbf{Z}^2$, et on récupère Λ comme image du réseau des périodes de dz sur $\mathbf{C}/\Lambda$, c'est-à-dire comme l'image de $H_1(\mathbf{C}/\Lambda,\mathbf{Z})$ par $u\mapsto\int_u dz$.

(iii) Soit ω la forme différentielle $\frac{dX}{Y}$ sur E_Λ. On a $\phi_\Lambda^*\omega=\frac{d\wp(z)}{\wp'(z)}=\frac{\wp'(z)dz}{\wp'(z)}=dz$, ce qui prouve que ω est holomorphe sur E_Λ et que Λ est le réseau des périodes de ω sur $E_\Lambda(\mathbf{C})$, c'est-à-dire comme l'image de $H_1(E_\Lambda(\mathbf{C}),\mathbf{Z})\cong H_1(\mathbf{C}/\Lambda,\mathbf{Z})$ par $u\mapsto\int_u\omega$.

(iv) Si $\alpha\in\mathbf{C}^*$, le réseau des périodes de $\alpha\omega$ est $\alpha\Lambda$. Maintenant, l'application $f:\mathbf{C}\to\mathbf{C}$ définie par $f(z)=\alpha z$ induit un isomorphisme de $\mathbf{C}/\Lambda$ sur $\mathbf{C}/\alpha\Lambda$. L'application $g=\phi_{\alpha\Lambda}\circ f\circ\phi_\Lambda^{-1}$: $E_\Lambda(\mathbf{C})\to E_{\alpha\Lambda}(\mathbf{C})$ est celle envoyant (X,Y) sur $(X',Y')=(\alpha^{-2}X,\alpha^{-3}Y)$, l'équation de $E_{\alpha\Lambda}$ est $(Y')^2=4(X')^3-\alpha^{-4}g_2X'-\alpha^{-6}g_3$ et on a $g^*(\frac{dX'}{Y'})=\frac{\alpha^{-2}dX}{\alpha^{-3}Y}=\alpha\omega$. Autrement dit, un changement d'équation de Weierstrass correspond à remplacer la forme holomorphe ω par un de ses multiples.

1.2.3. Uniformisation des courbes elliptiques. — Le th. 1.3 montre quà tout réseau Λ de $\mathbf{C}$, on peut associer une courbe elliptique dont Λ est le réseau des périodes. Le th. 1.6 ci-dessous montre que toute courbe elliptique sur $\mathbf{C}$ est obtenue de cette façon. On en déduit le résultat suivant.

Théorème 1.5. — (i) *Si E est une courbe elliptique définie sur $\mathbf{C}$ d'équation $Y^2=4X^3-g_2X-g_3$, alors $E(\mathbf{C})$ est topologiquement un tore et donc $H_1(E(\mathbf{C}),\mathbf{Z})\cong\mathbf{Z}^2$.*

(ii) *La forme différentielle $\omega=\frac{dX}{Y}$ est holomorphe sur $\mathbf{C}$ et $\Lambda=\{\int_u\omega,\ u\in H_1(E(\mathbf{C}),\mathbf{Z})\}$ est un réseau de $\mathbf{C}$ tel que $g_2(\Lambda)=g_2$, $g_3(\Lambda)=g_3$ et ϕ_Λ induit un isomorphisme de surfaces de Riemann de $\mathbf{C}/\Lambda$ sur $E(\mathbf{C})$.*

(iii) *L'application $(E,\omega)\mapsto\Lambda$ qui, à une courbe elliptique E munie d'une forme différentielle holomorphe ω, associe $\Lambda=\{\int_u\omega,\ u\in H_1(E(\mathbf{C}),\mathbf{Z})\}$, est une bijection sur l'ensemble des réseaux de $\mathbf{C}$.*

Théorème 1.6. — *Si $A,B\in\mathbf{C}$ sont tels que $A^3-27B^2\neq0$, il existe un unique réseau Λ de $\mathbf{C}$ tel que $g_2(\Lambda)=A$ et $g_3(\Lambda)=B$.*

Démonstration. — L'unicité d'un tel Λ suit du th. 1.21 ; nous allons démontrer son existence. Pour cela, définissons l'invariant j d'un réseau Λ par $j(\Lambda)=\frac{(12g_2(\Lambda))^3}{\Delta(\Lambda)}$. Comme $g_2(\alpha\Lambda)=\alpha^{-4}g_2(\Lambda)$ et $g_3(\alpha\Lambda)=\alpha^{-6}g_3(\Lambda)$, on voit que j est invariant par homothétie. Commençons par prouver qu'il suffit de vérifier que j est surjectif sur $\mathbf{C}$. Si tel est le cas, il existe Λ_0 tel que $\frac{A^3}{A^3-27B^2}=\frac{g_2(\Lambda_0)^3}{g_2(\Lambda_0)^3-27g_3(\Lambda_0)^2}$.

• Si $A = 0$, on a $g_2(\Lambda_0) = 0$, $B \neq 0$ et $g_3(\Lambda_0) \neq 0$; on peut donc trouver $\alpha \in \mathbf{C}^*$ tel que $g_3(\alpha\Lambda_0) = B$, et comme $g_2(\alpha\Lambda_0) = 0 = A$ pour tout α, cela montre que (A, B) est bien dans l'image de $\Lambda \mapsto (g_2(\Lambda), g_3(\Lambda))$.
• Si $A \neq 0$, il existe $\alpha \in \mathbf{C}^*$, bien déterminé à multiplication près par une racine 4-ième de l'unité, tel que $g_2(\alpha\Lambda_0) = A$. On a alors $g_3(\alpha\Lambda_0)^2 = B^2$, ce qui montre que quitte à changer α en $i\alpha$, on peut se débrouiller pour que $g_3(\alpha\Lambda_0) = B$, et donc que (A, B) est dans l'image de $\Lambda \mapsto (g_2(\Lambda), g_3(\Lambda))$.

Nous sommes donc ramené à prouver que j est surjectif, et comme j est invariant par homothétie, il suffit de s'intéresser aux réseaux dont un des générateur est $2i\pi$. Un tel réseau est de la forme $2i\pi(\mathbf{Z} + \mathbf{Z}\tau)$, et on peut imposer à τ d'avoir une partie imaginaire > 0 (i.e. d'appartenir au demi-plan de Poincaré $\mathscr{H}$). On définit alors des fonctions g_2, g_3, Δ et j sur $\mathscr{H}$ en posant

$$g_2(\tau) = g_2(2i\pi(\mathbf{Z} + \mathbf{Z}\tau)) = \frac{60}{(2i\pi)^4} \sum_{(m,n)\neq(0,0)} \frac{1}{(m + n\tau)^4},$$

$$g_3(\tau) = g_3(2i\pi(\mathbf{Z} + \mathbf{Z}\tau)) = \frac{140}{(2i\pi)^6} \sum_{(m,n)\neq(0,0)} \frac{1}{(m + n\tau)^6},$$

$$\Delta(\tau) = \Delta(2i\pi(\mathbf{Z} + \mathbf{Z}\tau)) = g_2(\tau)^3 - 27g_3(\tau)^2 \qquad j(\tau) = j(2i\pi(\mathbf{Z} + \mathbf{Z}\tau)) = \frac{(12g_2(\tau))^3}{\Delta(\tau)}.$$

Alors g_2 et g_3 sont holomorphes sur $\mathscr{H}$, comme séries de fonctions holomorphes convergeant uniformément sur tout compact, et Δ ne s'annule pas sur $\mathscr{H}$ d'après le (ii) du th. 1.3, et donc j est aussi holomorphe sur $\mathscr{H}$. Par ailleurs, un calcul immédiat montre que, si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z})$, alors

$$g_2\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^4 g_2(\tau) \quad \text{et} \quad g_3\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^6 g_3(\tau).$$

(Cela peut aussi se voir en remarquant que les réseau $\mathbf{Z} + \mathbf{Z}\tau$ et $\mathbf{Z} + \mathbf{Z}\frac{a\tau+b}{c\tau+d}$ sont homothétiques.) On en déduit le fait que $j(\frac{a\tau+b}{c\tau+d}) = j(\tau)$.

Maintenant, les fonctions g_2, g_3 et j sont en particulier périodiques de période 1 ; elles ont donc des développements de Fourier en puissances de $q = e^{2i\pi\,\tau}$. On peut calculer explicitement ces développement de Fourier (voir n° 1.3.5), mais nous n'aurons besoin que de faire les remarques suivantes : g_2 admet comme limite $\frac{60}{(2i\pi)^4} \cdot 2\zeta(4) = \frac{1}{12}$ en $i\infty$ et g_3 admet comme limite $\frac{140}{(2i\pi)^6} \cdot 2\zeta(6) = \frac{-1}{216}$ en $i\infty$. On en déduit que Δ s'annule en $i\infty$ et donc que j a un pôle en $i\infty$, et que son développement de Fourier est de la forme $\sum_{n\geqslant -r} a_n q^n$, avec $a_{-r} \neq 0$ et $r > 0$ (en fait $r = 1$).

Soit alors $a \in \mathbf{C}$, et soit $f = j - a$. On veut prouver que f s'annule sur $\mathscr{H}$. Soit $\alpha = 2^{i\pi/3}$ et soit γ_T le lacet constitué (faire un dessin) des segments $[\alpha, \alpha + iT]$, $[\alpha + iT, \alpha^2 + iT]$, $[\alpha^2 + iT, \alpha^2]$, et de l'arc de cercle de rayon 1 et centre 0 allant de α^2 à α. Si f s'annule sur γ_T, on a gagné. Si f ne s'annule pas sur γ_T, on calcule $I = \frac{1}{2i\pi} \int_{\gamma_T} \frac{f'(z)}{f(z)}\, dz$. Comme $f(z) = f(z + 1)$, les deux intégrales sur les segments verticaux sont opposées. De même, comme $f(\frac{-1}{z}) = f(z)$, l'intégrale de α^2 à i est l'opposée de l'intégrale de i à α, et donc $I = \int_{\alpha+iT}^{\alpha^2+iT} \frac{f'(z)}{f(z)}\, dz$. Or $\frac{f'(z)}{f(z)}$ tend vers $-2i\pi r$ uniformément sur le segment $[\alpha + iT, \alpha^2 + iT]$, quand T tend vers $+\infty$, et donc I tend

vers $r > 0$ quand T tend vers $+\infty$. Comme I est le nombre de zéros de f à l'intérieur de γ_T, cela permet de conclure.

Remarque 1.7. — Les fonctions g_2, g_3, Δ définies ci-dessus sont des cas particuliers de formes modulaires et j est une fonction modulaire. La théorie des formes modulaires est d'une richesse inouïe, et le lecteur est invité à consulter le livre de Koblitz pour se faire une petite idée de ses tenants et aboutissants.

1.2.4. La loi de groupe sur une courbe elliptique. — Soit E une courbe elliptique sur $\mathbf{C}$ d'équation $Y^2 = 4X^3 - g_2X - g_3$, et soit Λ le réseau des périodes de $\omega = \frac{dX}{Y}$. Alors $z \mapsto \phi(z) = (\wp(z), \wp'(z))$ (et qui envoie 0 sur ∞) est un isomorphisme de surfaces de Riemann de $\mathbf{C}/\Lambda$ sur $E(\mathbf{C})$ et on a $\phi^*\omega = \frac{d\wp(z)}{\wp'(z)} = dz$. On peut utiliser cet isomorphisme pour transporter l'addition sur $\mathbf{C}/\Lambda$ en une loi de groupe $\oplus$ sur E en posant $P \oplus Q = \phi(\phi^{-1}(P) + \phi^{-1}(Q))$. L'élément neutre pour cette loi de groupe est $\phi(0) = \infty$ que l'on notera 0 dorénavant ; l'opposé de $P = (x, y) = \phi(z)$ est $[-1]P = \phi(-z) = (x, -y)$.

Proposition 1.8. — *On a $P_1 \oplus P_2 \oplus P_3 = 0$ si et seulement si P_1, P_2, P_3 sont les trois points d'intersection (avec multiplicité[7]) de E avec une droite de $\mathbf{P}^2$.*

Démonstration. — Si $P_1 = -P_2$, alors la droite (P_1, P_2) est verticale et son troisième point d'intersection avec E est le point à l'infini (i.e. 0), d'où le résultat dans ce cas particulier. Pour traiter le cas général, posons $z_i = \phi^{-1}(P_i)$, et soit $F(z)$ la fonction elliptique

$$F(z) = \frac{1}{z_1 - z_2} \det \begin{pmatrix} \wp(z) & \wp(z_1) & \wp(z_2) \\ \wp'(z) & \wp'(z_1) & \wp'(z_2) \\ 1 & 1 & 1 \end{pmatrix}$$

(en passant à la limite si $z_1 = z_2$). Alors $F(z) = 0$ si et seulement si $\phi(z)$ est sur la droite (P_1, P_2) (sur la tangente en P_1, si $P_1 = P_2$). D'autre part, F a pour seul pôle un pôle d'ordre triple en 0 et donc trois zéros dont z_1, z_2 ; notons z_3 le troisième. On a $z_1 + z_2 + z_3 - 3 \cdot 0 = 0$ dans $\mathbf{C}/\Lambda$ d'après le th. 1.2, et donc $P_1 \oplus P_2 \oplus \phi(z_3) = 0$. On en déduit le résultat.

Le résultat précédent permet d'écrire des formules pour l'addition de deux points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ de E. On suppose $y_1 \neq -y_2$ si $x_1 = x_2$, sinon on a $P_1 \oplus P_2 = 0$; la droite passant par P_1 et P_2 (ou la tangente à $P_1 = P_2$ si $P_1 = P_2$) est la droite d'équation $Y = y_1 + \lambda(X - x_1)$, avec

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y_2^2 - y_1^2}{(y_2 + y_1)(x_2 - x_1)} = \frac{4(x_1^2 + x_1x_2 + x_2^2) - g_2}{y_2 + y_1}.$$

En reportant l'équation de cette droite dans l'équation de E, on obtient une équation du troisième degré en X donc deux des racines sont x_1 et x_2 et la somme est $\frac{1}{4}\lambda^2$. On en déduit que $P_1 \oplus P_2 = P_3$, avec

$$P_3 = (\frac{\lambda^2}{4} - x_1 - x_2, -y_1 - \lambda(\frac{\lambda^2}{4} - 2x_1 - x_2)),$$

[7]Si $P_1 = P_2$, cela signifie que P_3 est sur la tangente à E en $P_1 = P_2$, et si $P_1 = P_2 = P_3$, cela signifie que E a un point d'inflexion en $P_1 = P_2 = P_3$.

ce qui n'a pas l'air très symétrique, mais le devient après quelques manipulations élémentaires.

On remarque que les formules ne font intervenir que des expressions polynomiales à coefficients dans $\mathbf{Z}[\frac{1}{2}]$ en x_1, x_2, y_1, y_2, g_2 et g_3, et λ et qu'on ne divise par 0 (pour définir λ) que si $P_1 = P_2$ et que l'on est en caractéristique 2 ; elles ont donc un sens sur tout corps qui n'est pas de caractéristique 2. De plus, pour vérifier que ce que l'on obtient est bien une loi de groupe, il s'agit de vérifier un certain nombre d'identités entre expressions polynomiales à coefficients dans $\mathbf{Z}[\frac{1}{2}]$; or celles-ci sont vérifiées quand on donne des valeurs complexes aux variables et donc elles le sont universellement (ceci demanderait à être précisé un peu...). On en déduit que la colinéarité définit une loi de groupe sur $E(K)$, si E est une courbe elliptique définie sur un corps K quelconque (de caractéristique différente de 2 (et de 3 car sinon, il faut une équation plus générale)). Un argument de continuité prouve que cela définit aussi une loi d'addition dans le cas où la courbe $Y^2 = 4X^3 - g_2X - g_3$ n'est pas une courbe lisse ; ce cas peut se traiter directement (prop. 1.13).

Le même genre d'arguments permet de montrer le résultat suivant (en utilisant le fait que $\phi_\Lambda^* \frac{dX}{Y} = dz$, cf. (iii) de la rem. 1.4).

Proposition 1.9. — *Si E est une courbe elliptique d'équation $Y^2 = 4X^3 - g_2X - g_3$ définie sur un corps K de caractéristique $\neq 2$, alors $\omega = \frac{dX}{Y}$ est invariante par translation par un élément de $E(K)$.*

Le groupe $E(K)$ est en général très difficile à calculer. Par exemple, on a le résultat suivant conjecturé par Poincaré en 1900 et démontré par Mordell (pour $\mathbf{Q}$) et par Weil (dans le cas général) dans les années 1930.

Théorème 1.10. — *Si K est un corps de nombres et si E est une courbe elliptique définie sur K, alors $E(K)$ est un groupe de type fini et donc isomorphe à $\mathbf{Z}^{r(E/K)} \oplus E(K)_{\mathrm{tors}}$, où $E(K)_{\mathrm{tors}}$ est un groupe fini.*

Le groupe $E(K)_{\mathrm{tors}}$ se calcule facilement en utilisant par exemple les techniques du § 1.3, mais on n'a aucun algorithme dont on peut prouver qu'il permettra de calculer le rang $r(E/K)$ et ses générateurs. La conjecture de Birch et Swinnerton-Dyer (un des 7 problèmes à un million de dollar), si elle s'avérait vraie, fournirait un tel algorithme.

Théorème 1.11. — *Soit K un corps de caractéristique[(8)] 0 et soit E une courbe elliptique définie sur K.*

(i) *Si $m \geqslant 1$, alors $E(\overline{K})[m] = \{P \in E(\overline{K}),\ [m]P = 0\} \cong (\mathbf{Z}/m\mathbf{Z})^2$ et est stable par G_K qui agit $(\mathbf{Z}/m\mathbf{Z})$-linéairement.*

(ii) *Si p est un nombre premier, alors $T_p(E) = T_p(E(\overline{K}))$ est un $\mathbf{Z}_p$-module libre de rang 2 muni d'un action linéaire continue de G_K.*

Démonstration. — Le (ii) suit du (i) puisque $T_p(E)$ est la limite projective des $E(\overline{K})[p^n]$. Le fait que $E(\overline{K})[m]$ soit stable par G_K vient juste de ce que l'équation $[m]P = 0$ est définie sur K

(8) Le résultat qui suit n'est pas valable tel quel en caractéristique $p > 0$, cf. th. 1.32.

puisque la loi d'addition est définie sur K ; pour la même raison, l'action de G_K est $\mathbf{Z}$-linéaire sur $E(\overline{K})$ et donc $(\mathbf{Z}/m\mathbf{Z})$-linéaire sur $E(\overline{K})[m]$. Il reste à prouver que $E(\overline{K})[m] \cong (\mathbf{Z}/m\mathbf{Z})^2$. Si $K = \mathbf{C}$, cela suit de ce que $E(\mathbf{C}) \cong \mathbf{C}/\Lambda$ et donc $E(\mathbf{C})[m] \cong \frac{1}{m}\Lambda/\Lambda \cong (\mathbf{Z}/m\mathbf{Z})^2$. Dans le cas général, si E est d'équation $Y^2 = 4X^3 - g_2X - g_3$, fixons un plongement de la clôture algébrique $\overline{F} \subset \overline{K}$ de $F = \mathbf{Q}(g_2, g_3) \subset K$ dans $\mathbf{C}$ (on ne peut pas forcément envoyer K et $\overline{K}$ dans $\mathbf{C}$ s'ils sont trop gros, mais F et $\overline{F}$ sont suffisamment petits pour se plonger dans $\mathbf{C}$). Soit alors $P = (x, y)$ un point de m torsion. Plongeons de même $F(x, y)$ dans $\mathbf{C}$. Alors P devient un point de m torsion de $E(\mathbf{C})$ et tous ses conjugués sous l'action de $\mathrm{Aut}_F(\mathbf{C})$ sont des points de $E(\mathbf{C})[m]$, et comme $E(\mathbf{C})[m]$ est fini, cela implique que $F(x, y) \subset \overline{F}$. Le même raisonnement montre que $E(\mathbf{C})[m] \subset E(\overline{F})[m]$ et donc finalement que $E(\overline{K})[m] = E(\overline{F})[m] = E(\mathbf{C})[m] \cong (\mathbf{Z}/m\mathbf{Z})^2$. Ceci permet de conclure.

Remarque 1.12. — La démonstration qui précède est un cas particulier du principe de Lefschetz suivant lequel tout énoncé algébrique valable sur $\mathbf{C}$ est valable sur un corps algébriquement clos de caractéristique 0.

Dans le cas singulier (i.e. où le polynôme $4X^3 - g_2X - g_3$ n'a pas toutes ses racines simples et la courbe n'est pas lisse), il y a exactement un point singulier, et une droite passant par deux points non singuliers recoupe E en un point non singulier (car sinon elle aurait au moins 4 points d'intersection avec E, en comptant les multiplicités, puisque le point singulier est de multplicité au moins 2). Les formules précédentes définissent donc une loi de groupe sur le lieu non singulier E^{ns} de E. La proposition suivante montre que le groupe ainsi défini n'est pas très mystérieux.

Proposition 1.13. — (i) *Si E est la courbe d'équation $Y^2 = 4(X-a)^2(X+2a)$, avec $a \neq 0$, alors $(x, y) \mapsto s = \frac{y-2\sqrt{3a}(x-a)}{y+2\sqrt{3a}(x-a)}$ induit un isomorphisme de groupes de $E^{\mathrm{ns}}(K)$ sur K^* (resp. sur le groupe des éléments de normes 1 dans l'extension quadratique $K(\sqrt{3a})$), si $\sqrt{3a} \in K$ (resp. si $\sqrt{3a} \notin K$).*

(ii) *Si E est la courbe d'équation $Y^2 = 4X^3$, alors $(x, y) \mapsto \frac{-2x}{y}$ induit un isomorphisme de groupes de $E^{\mathrm{ns}}(K)$ sur K.*

Dans le cas (i) on dit que E est *multiplicative* (*déployée* si $\sqrt{3a} \in K$ et *non déployée* si $\sqrt{3a} \notin K$), et dans le cas (ii), on dit que E est *additive*.

Démonstration. — (i) Une droite $Y = t(X - a)$ passant par $(a, 0)$ recoupe la courbe en au plus un point (et en exactement un point si cette droite n'est pas une des deux tangentes $Y = \pm 2\sqrt{3a}(x - a)$). On en déduit une paramétrisation de la courbe par $t \mapsto (\frac{t^2}{4} - 2a, t(\frac{t^2}{4}))$, pour $t \in \mathbf{P}^1(K) - \{\pm 2\sqrt{3a}\}$. On a alors $s = \frac{t-2\sqrt{3a}}{t+2\sqrt{3a}} \neq 0, \infty$ et $t = -2\sqrt{3a}\frac{s+1}{s-1}$. En coupant alors la courbe paramètŕee par s par une droite d'équation $\alpha X + \beta Y + \gamma = 0$, et en multipliant le tout par $(s-1)^3$, on tombe sur une équation du troisième degré en s dont les termes de degré 0 et 3 sont opposés. On en déduit que $P(s_1), P(s_2)$ et $P(s_3)$ sont alignés si et seulement si $s_1s_2s_3 = 1$, ce qui démontre le (i).

(ii) On se place dans le plan affine $Y = 1$ où l'équation de la courbe devient $W^3 + 2Z = 0$, si $W = \frac{-2X}{Y}$, et on vérifie facilement que (W_1, Z_1), (W_2, Z_2) et (W_3, Z_3) sont alignés si et seulement si $W_1 + W_2 + W_2 = 0$, ce qui permet de conclure.

1.2.5. Le théorème d'Abel. — On définit les fonctions σ et ζ de Weierstrass par

$$\sigma(z, \Lambda) = z \prod_{\omega \in \Lambda - \{0\}} \Big(\Big(1 - \frac{z}{\omega}\Big) e^{z/\omega + z^2/2\omega^2} \Big)$$

$$\zeta(z, \Lambda) = \frac{d}{dz} \log \sigma(z, \Lambda) = \frac{1}{z} + \sum_{\omega \in \Lambda - \{0\}} \Big(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \Big).$$

On remarque que $\zeta'(z, \Lambda) = -\frac{1}{z^2} - \sum_{\omega \in \Lambda - \{0\}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big) = -\wp(z, \Lambda)$ est périodique de période Λ, et donc qu'il existe, pour tout $\omega \in \Lambda$, des constantes $a(\omega), b(\omega) \in \mathbf{C}$ telles que

$$\zeta(z + \omega) - \zeta(z) = a(\omega) \quad \text{et} \quad \sigma(z + \omega) = e^{a(\omega) z + b(\omega)} \sigma(z), \quad \text{pour tout } z \in \mathbf{Z}.$$

Par ailleurs, il est apparent sur sa définition que σ a des zéros uniquement en les points de Λ et que ce sont des zéros simples.

On note $\mathrm{Div}(\mathbf{C}/\Lambda)$ le groupe des diviseurs sur $\mathbf{C}/\Lambda$, c'est-à-dire le $\mathbf{Z}$-module libre de base les éléments de $\mathbf{C}/\Lambda$, et on note $(w) \in \mathrm{Div}(\mathbf{C}/\Lambda)$ l'élément de la base correspondant à $w \in \mathbf{C}/\Lambda$. Un élément D de $\mathrm{Div}(\mathbf{C}/\Lambda)$ s'écrit donc, de manière unique, sous la forme $D = \sum_{w \in \mathbf{C}/\Lambda} n_w \, (w)$, où les $n_w \in \mathbf{Z}$ sont nuls sauf pour un nombre fini, et on définit le degré $\deg(D) \in \mathbf{Z}$ et la trace $\mathrm{Tr}(D) \in \mathbf{C}/\Lambda$ de D par

$$\deg\big(\sum n_w \, (w)\big) = \sum_{w \in \mathbf{C}/\Lambda} n_w \quad \text{et} \quad \mathrm{Tr}\big(\sum n_w \, (w)\big) = \sum_{w \in \mathbf{C}/\Lambda} n_w \, w,$$

et le sous-groupe $\mathrm{Div}^0(\mathbf{C}/\Lambda)$ des diviseurs de degré 0.

Si $f \in \mathbf{C}(\mathbf{C}/\Lambda)^*$, on définit son diviseur $\mathrm{div}(f)$, par

$$\mathrm{div}(f) = \sum_{w \in \mathbf{C}/\Lambda} v_w(f) \, (w).$$

Théorème 1.14. — (Abel) (i) *Si* $f \in \mathbf{C}(\mathbf{C}/\Lambda)^*$, *alors* $\deg(\mathrm{div}(f)) = 0$ *et* $\mathrm{Tr}(\mathrm{div}(f)) = 0$.

(ii) *Réciproquement, si* $D \in \mathrm{Div}(\mathbf{C}/\Lambda)$ *est de degré nul et de trace nulle, alors* D *est principal* (i.e. est de la forme $\mathrm{div}(f)$).

Démonstration. — Le (i) a déjà été démontré au th. 1.2, et pour démontrer le (ii), il suffit de constater que si $D = \sum_i n_i(w_i)$ est de degré nul et de trace nulle, on peut trouver des relèvements $\tilde{w}_i$ de w_i dans $\mathbf{C}$ tels que $\sum_i n_i \, \tilde{w}_i = 0$. Alors un petit calcul montre que $f(z) = \prod_i \sigma(z - \tilde{w}_i)^{n_i}$ est périodique de période Λ et son diviseur est D par construction.

Remarque 1.15. — On déduit du théorème d'Abel la caractérisation algébrique suivante de la loi d'addition sur une courbe elliptique définie sur $\mathbf{C}$: si $P, Q \in E(\mathbf{C})$, alors $R = P \oplus Q$ est l'unique élément de $E(\mathbf{C})$ tel qu'il existe $f \in \mathbf{C}(E)^*$ de diviseur $(R) - (P) - (Q) + (0)$. Cette caractérisation est valable sur n'importe quel corps, mais la démonstration demande d'autres outils (théorème de Riemann-Roch).

1.2.6. Périodes des formes de seconde espèce et formule de Legendre. — Une forme différentielle méromorphe α sur $\mathbf{C}/\Lambda$ est de la forme $f(z)\,dz$, avec $f \in \mathbf{C}(\mathbf{C}/\Lambda)$. On dit que :

- α est de *première espèce*, si f est holomorphe (et donc constante),
- α est de *seconde espèce*, si le résidu de f en chacun de ses pôles est nul,
- α est de *troisième espèce*, si f n'a que des pôles simples et si tous les résidus sont des entiers.

L'intersection de l'espace $\mathrm{DSE}(\mathbf{C}/\Lambda)$ des formes de seconde espèce avec l'espace $\mathrm{DTE}(\mathbf{C}/\Lambda)$ des formes de troisième espèce n'est autre que celui des formes de première espèce, noté $H^0(\mathbf{C}/\Lambda, \Omega^1)$ (ce qui signifie les sections globales du faisceau des formes différentielles holomorphes, i.e. les formes différentielles partout holomorphes). Par ailleurs, il est clair que si $F \in \mathbf{C}(\mathbf{C}/\Lambda)$, alors $dF = F'(z)dz$ est de seconde espèce, et si $F \in \mathbf{C}(\mathbf{C}/\Lambda)^*$, alors $d\log F = \frac{dF}{F} = \frac{f'(z)}{f(z)}\,dz$ est de troisième espèce ; une telle forme est dite exacte.

Finalement, remarquons que α est de seconde espèce si et seulement si α a une primitive méromorphe F sur $\mathbf{C}$, et que si $\omega \in \Lambda$, alors $F(z+\omega) - F(z)$ a une différentielle nulle et donc est constante. On en déduit le fait que si $u \in H_1(\mathbf{C}/\Lambda, \mathbf{Z})$, si γ est un lacet dans $\mathbf{C}/\Lambda$ représentant u et évitant les pôles de α, et si $\tilde{\gamma}$ est un chemin dans $\mathbf{C}$ relevant γ, alors $\int_{\tilde{\gamma}} \alpha$ ne dépend que de u et pas des choix de γ ou $\tilde{\gamma}$; on le note $\int_u \alpha$ et $\int_u \alpha$ est *la période de α le long de u*. De plus, on a $\int_{u+v} \alpha = \int_u \alpha + \int_v \alpha$, si $u, v \in H_1(\mathbf{C}/\Lambda, \mathbf{Z})$, et donc les *périodes de α* forment un sous-groupe de $\mathbf{C}$ appelé *réseau des périodes de α*, bien que ce ne soit pas forcément un réseau puisqu'il peut parfaitement être réduit à 0 [c'est le cas si $\alpha = 0$, ou si $\alpha = f'(z)dz$, avec $f \in \mathbf{C}(\mathbf{C}/\Lambda)$]. Par exemple, le réseau des périodes de $\alpha = dz$ est Λ, et le réseau des périodes de $\wp(z)\,dz$ est l'ensemble des $a(\omega)$, pour $\omega \in \Lambda$.

Si $u, v \in H_1(\mathbf{C}/\Lambda, \mathbf{Z})$, on note $u \sharp v$ le déterminant[(9)] de u, v dans une base directe de $H_1(\mathbf{C}/\Lambda, \mathbf{Z})$ (une base ω_1, ω_2 de $H_1(\mathbf{C}/\Lambda, \mathbf{Z}) \cong \Lambda$ est directe si $\mathrm{Im}(\frac{\omega_2}{\omega_1}) > 0$).

Théorème 1.16. — (i) *Une forme de seconde espèce est exacte si et seulement si son réseau des périodes est réduit à* 0.

(ii) *Si $u, v \in H_1(\mathbf{C}/\Lambda, \mathbf{Z})$, alors*

$$\int_u dz \int_v \wp(z)dz - \int_v dz \int_u \wp(z)dz = 2i\pi\ (u \sharp v), \quad \textit{(formule de Legendre).}$$

(iii) *Le $\mathbf{C}$-espace vectoriel $H^1_{\mathrm{dR}}(\mathbf{C}/\Lambda)$, quotient de l'espace des formes différentielles de seconde espèce par l'espace des formes exactes est de dimension* 2*, engendré par dz et $\wp(z)dz$.*

Démonstration. — Le (i) suit juste de ce que le réseau des périodes de α est réduit à zéro si et seulement si la primitive F de α sur $\mathbf{C}$ est périodique de période Λ, et donc appartient à $\mathbf{C}(\mathbf{C}/\Lambda)$.

Le (ii) se démontre en intégrant $\zeta(z)dz$ sur le parallélogramme de sommets $a, a+\omega_1, a+\omega_1+\omega_2, a+\omega_2$, avec $\omega_1 = \int_u dz$ et $\omega_e = \int_v dz$. Cette intégrale est égale au membre de gauche de manière immédiate, et la formule des résidus montre qu'elle est aussi égale au nombre de

(9) L'entier relatif $u \sharp v$ s'interprète comme le nombre de points d'intersection (avec multiplicité) de chemins dans $\mathbf{C}/\Lambda$ représentant u et v.

droite (en interprétant $u \sharp v$ comme le volume (avec un signe dépendant de l'orientation) du parallélogramme divisé par le volume d'un domaine fondamental pour Λ et donc aussi comme le nombre de points de Λ à l'intérieur du parallélogramme [en ayant bien sûr choisi a de sorte que le bord du parallélogramme ne contienne pas d'élément de Λ]).

Maintenant l'application $\alpha \mapsto \lambda_\alpha \in \mathrm{Hom}(H_1(\mathbf{C}/\Lambda, \mathbf{Z}), \mathbf{C})$ qui associe à α la forme linéaire $\lambda_\alpha(u) = \int_u \alpha$ est linéaire, et son noyau est précisément l'espace des formes exactes d'après le (i). Elle induit donc une injection de $H^1_{\mathrm{dR}}(\mathbf{C}/\Lambda)$ dans le $\mathbf{C}$-espace vectoriel $\mathrm{Hom}(H_1(\mathbf{C}/\Lambda, \mathbf{Z}), \mathbf{C})$ qui est de dimension 2. Or la formule de Legendre montre que les images de dz et $\wp(z)dz$ ne sont pas colinéaires puisque le déterminant dans la base naturelle est $2i\pi$; on en déduit le (iii).

Remarque 1.17. — Les notions de formes différentielles de pemière et seconde espèce et de formes différentielles exactes ont un sens pour une courbe lisse X sur un corps K quelconque : on choisit un paramètre local en chaque point P et on complète l'anneau local correspondant dont le corps des fractions est alors de la forme $L((T))$, où L est une extension finie de K (corps de définition de P) ; si $\alpha \in \Omega^1_{K(X)/K}$ est une forme différentielle sur X, le plongement de $K(X)$ dans $L((T))$ permet d'écrire localement α sous la forme $\sum_{n \geqslant n_0} a_n T^n dT$, et on dit que α est holomorphe en P, si $a_n = 0$ pour $n < 0$; on définit le résidu de α en P comme le coefficient a_{-1} de $T^{-1}dT$.

Théorème 1.18. — (i) *Si E est une courbe elliptique définie sur un corps K de caractéristique*[(10)] *0, d'équation $Y^2 = 4X^3 - g_2X - g_3$, alors l'espace $H^1_{\mathrm{dR}}(E)$ quotient de l'espace des formes de seconde espèce par celui des formes exactes est un espace vectoriel de dimension 2 engendré par $\omega = \frac{dX}{Y}$ et $\eta = X\frac{dX}{Y}$.*

(ii) *Si K est un sous-corps de $\mathbf{C}$ et si u, v est une base orientée de $H_1(E(\mathbf{C}), \mathbf{Z})$ sur $\mathbf{Z}$, alors*

$$\int_u \omega \int_v \eta - \int_v \omega \int_u \eta = 2i\pi \quad \textit{(formule de Legendre).}$$

Démonstration. — Soit $\alpha \in K(E)dX$ une forme différentielle de seconde espèce sur E définie sur K. On choisit un plongement dans $\mathbf{C}$ du corps F engendré sur $\mathbf{Q}$ par g_2, g_3 et les coefficients de la fraction rationnelle f en X et Y telle que $\alpha = f(X)dX$. D'après le (iii) du th. 1.16, on peut écrire α de manière unique sous la forme $\alpha = a\omega + b\eta + dg$, avec $a, b \in \mathbf{C}$ et $g \in \mathbf{C}(E)$. Mais l'unicité implique que a, b et g sont fixes par $\mathrm{Aut}_F(\mathbf{C})$ et donc $a, b \in F \subset K$ et $g \in F(E) \subset K(E)$. On en déduit le (i).

Le (ii) se déduit directement du (ii) du th. 1.16 via l'isomorphisme $\phi : \mathbf{C}/\Lambda \cong E(\mathbf{C})$.

1.2.7. L'accouplement de Weil

Théorème 1.19. — (i) *Si $m\alpha = 0$ dans $\mathbf{C}/\Lambda$, il existe, à multiplication près par un élément de $\mathbf{C}^*$, une unique fonction elliptique $f_{m,\alpha}$ de diviseur $m(\alpha) - m(0)$.*

(ii) *Si $m\alpha = m\beta = 0$ dans $\mathbf{C}/\Lambda$, et si $\tilde{\alpha}, \tilde{\beta} \in \frac{1}{m}\Lambda$ sont des relèvements quelconques de α et β, alors $\frac{f_{m,\beta}(z-\tilde{\alpha})f_{m,\alpha}(z)}{f_{m,\beta}(z)f_{m,\alpha}(z-\tilde{\beta})}$ est constante et égale à la racine m-ième de l'unité $e_m(\alpha, \beta) = e^{\frac{2i\pi}{m}(m\tilde{\alpha} \sharp m\tilde{\beta})}$.*

(10) Le résultat est faux en caractéristique $p > 0$.

(iii) *L'application* $e_m : (\frac{1}{m}\Lambda/\Lambda) \times (\frac{1}{m}\Lambda/\Lambda) \to \mu_m$ *est bilinéaire alternée et non dégénérée.*

Démonstration. — L'unicité de $f_{m,\alpha}$ suit de ce qu'une fonction elliptique est déterminée par son diviseur (à multiplication près par un élément de $\mathbf{C}^*$), et l'existence $f_{m,\alpha}$ découle du théorème d'Abel, dont la démonstration fournit la formule

$$f_{m,\alpha}(z) = \sigma(z-\tilde{\alpha})^m \sigma(z)^{1-m} \sigma(z-m\tilde{\alpha})^{-1}.$$

Un petit calcul utilisant l'équation fonctionnelle de la fonction σ montre alors que

$$\frac{f_{m,\beta}(z-\tilde{\alpha}) f_{m,\alpha}(z)}{f_{m,\beta}(z) f_{m,\alpha}(z-\tilde{\beta})} = e^{\tilde{\alpha} a(m\tilde{\beta}) - \tilde{\beta} a(m\tilde{\alpha})} = e^{\frac{2i\pi}{m}(m\tilde{\alpha} \sharp m\tilde{\beta})},$$

la dernière égalité provenant de la formule de Legendre. Le (iii) découle des propriétés de $(u,v) \mapsto u \sharp v$.

Remarque 1.20. — (i) Si E est une courbe elliptique définie sur un sous-corps K de $\mathbf{C}$, et si Λ est le réseau des périodes de E, alors e_m peut être vu comme un accouplement de $E(\overline{K})[m] \times E(\overline{K})[m] \to \mu_m$, et $f_{m,\alpha}$ peut être vue comme un élément de $\mathbf{C}(E)$ de diviseur $m((\alpha)-(0)$. Maintenant, si $g \in \mathrm{Aut}_K(\mathbf{C})$, alors $g(f_{m,\alpha}) \in \mathbf{C}(E)$ a pous diviseur $m((g(\alpha))-(0))$ et donc est égal à $f_{m,g(\alpha)}$ à multiplication près par un élément de $\mathbf{C}^*$. On en déduit $g(e_m(\alpha,\beta)) = e_m(g(\alpha), g(\beta))$, pour tout $g \in \mathrm{Aut}_K(\mathbf{C})$, et comme tout est défini sur $\overline{K}$, l'action se fait à travers G_K.

(ii) La formule $e_m(\alpha,\beta) = e^{\frac{2i\pi}{m}(m\tilde{\alpha} \sharp m\tilde{\beta})}$ montre que si $u_{n+1}, v_{n+1} \in E(\overline{K})[p^{n+1}]$, alors $e_{p^{n+1}}(u_{n+1}, v_{n+1})^p = e_{p^n}([p]u_{n+1}, [p]v_{n+1})$, ce qui montre que les e_{p^n} se recollent pour donner, en passant à la limite projective, une forme bilinéaire alternée non dégénérée $\langle\ ,\rangle : T_p(E) \times T_p(E) \to \mathbf{Z}_p(1)$, qui commute à l'action de G_K.

1.2.8. Morphismes. — Soient E_1 et E_2 deux courbes elliptiques définies sur $\mathbf{C}$, de réseaux des périodes respectifs Λ_1 et Λ_2, et soit $\phi_i : \mathbf{C}/\Lambda_i \cong E_i(\mathbf{C})$ l'isomorphisme habituel de surfaces de Riemann (qui est aussi un isomorphisme de groupes par construction de la loi de groupe). Notre but est de décrire de manière concrète l'ensemble des morphismes de courbes algébriques de E_1 dans E_2. Comme on peut toujours composer un tel morphisme avec une translation de manière à imposer que 0 s'envoie sur 0, il suffit de décrire ces morphismes particuliers pour avoir une description du cas général.

Remarquons que, si $\alpha \in \mathbf{C}$ est tel que $\alpha\Lambda_1 \subset \Lambda_2$, alors $z \mapsto \alpha z$ induit, par passage au quotient, une application holomorphe $f_\alpha : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$. Remarquons aussi que si $g : E_1 \to E_2$ est un morphisme de courbes algébriques, alors $\phi_2^{-1} \circ g \circ \phi_1 : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ est holomorphe.

Théorème 1.21. — (i) $\alpha \mapsto f_\alpha$ *induit une bijection de* $\{\alpha \in \mathbf{C},\ \alpha\Lambda_1 \subset \Lambda_2\}$ *sur* $\{f : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2,\ \text{holomorphe},\ f(0)=0\}$.

(ii) $g \mapsto \phi_2^{-1} \circ g \circ \phi_1$ *induit une bijection de* $\{g : E_1 \to E_2,\ \text{algébrique},\ g(0)=0\}$ *sur* $\{f : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2,\ \text{holomorphe},\ f(0)=0\}$.

Démonstration. — Si : $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ est holomorphe et vérifie $f(0) = 0$, alors il existe une unique $\tilde{f} : \mathbf{C} \to \mathbf{C}$ holomorphe, relevant[11] f, telle $\tilde{f}(0) = 0$. Alors $\tilde{f}(z+\omega) - \tilde{f}(z) \in \Lambda_2$, si $\omega \in \Lambda_1$, et comme Λ_2 est discret, cela prouve que $z \mapsto \tilde{f}(z+\omega) - \tilde{f}(z)$ est constante, et donc que $\tilde{f}'(z+\omega) = \tilde{f}'(z)$, quels que soient $z \in \mathbf{C}$ et $\omega \in \Lambda_1$. La fonction $\tilde{f}'$ est donc une fonction elliptique holomorphe et donc constante. On en déduit le (i).

Pour le (ii), on remarque que si $\phi_2 \circ g : \mathbf{C}/\Lambda_1 \to E_2(\mathbf{C})$ est donnée par $z \mapsto (F_1(z), F_2(z))$, alors F_1 et F_2 sont des fonctions elliptiques de période Λ_1 et donc peuvent s'exprimer comme des fonctions rationnelles en $\wp(z, \Lambda_1)$ et $\wp'(z, \Lambda_1)$. Ceci implique que $\phi_2 \circ g \circ \psi_1^{-1}$ est donné par des fonctions rationnelles sur E_1.

Corollaire 1.22. — (i) *E_1 et E_2 sont isomorphes en tant que courbes algébriques si et seulement si les réseaux Λ_1 et Λ_2 sont homothétiques (i.e. il existe $\alpha \in \mathbf{C}^*$ avec $\Lambda_2 = \alpha\Lambda_1$).*

(ii) *Un morphisme de courbes algébriques $g : E_1 \to E_2$ est automatiquement un morphisme de groupes (à translation près), et si g n'est pas constant alors il est surjectif.*

(iii) *Si E est une courbe elliptique sur $\mathbf{C}$, alors l'ensemble* $\mathrm{End}(E)$ *des morphismes $g : E \to E$ de courbes algébriques avec $g(0) = 0$ est un anneau commutatif, et si $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ est le réseau des périodes de E, alors* $\mathrm{End}(E) = \mathbf{Z}$ *sauf si $K = \mathbf{Q}(\frac{\omega_2}{\omega_1})$ est un corps quadratique imaginaire, auquel cas* $\mathrm{End}(E)$ *est un ordre du corps K.*

Si $\mathrm{End}(E) \neq \mathbf{Z}$, on dit que E *a de la multiplication complexe* ou bien *est CM*. Si K est un corps quadratique imaginaire, on dit que E a de la multiplication complexe par K ou encore que E est CM par K si $\mathbf{Q} \otimes \mathrm{End}(E) = K$. On fabrique sans difficulté, par voie transcendante, des courbes elliptiques à multiplication complexe : il suffit de prendre un corps quadratique imaginaire $K \subset \mathbf{C}$, de prendre un réseau Λ de K et de faire le quotient $\mathbf{C}/\Lambda$; alors $\mathrm{End}(E)$ est l'ordre de K stabilisant Λ.

Remarque 1.23. — (i) On déduit du principe de Lefschetz que, si E est une courbe elliptique définie sur un corps K de caractéristique 0, alors l'anneau $\mathrm{End}_K(E)$ des endomorphismes de E définis sur K est soit $\mathbf{Z}$ soit un ordre d'un corps quadratique imaginaire. Ce résultat est faux en caractéristique p, où certaines courbes *supersingulières* ont un anneau d'endomorphismes qui est de rang 4 sur $\mathbf{Z}$.

(ii) Si E a de la multiplication complexe par K, le $\mathbf{Q}$-espace vectoriel $\mathbf{Q} \otimes_{\mathbf{Z}} H_1(E(\mathbf{C}), \mathbf{Z})$ est un K-module de rang 1, et donc $\mathbf{Q} \otimes_{\mathbf{Z}} T_p(E)$ est un $K \otimes_{\mathbf{Z}} \mathbf{Z}_p = \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$-module de rang 1. Comme l'action de G_K commute à $\mathrm{End}_K(E)$, on en déduit que G_K agit par des éléments de $(K \otimes_{\mathbf{Z}} \mathbf{Z}_p)^* = \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}^*$ sur $T_p(E)$; en particulier, l'image est un groupe commutatif.

Les exemples les plus simples de courbes CM sont :

[11] cela suit de ce que $\mathbf{C}$ est contractile, et peut se démontrer à la main en prenant r maximal tel que $\tilde{f}$ existe sur $D(0, r^-)$, en recouvrant $C(0, r)$ par des disques $D(a_i, r_i^-)$, pour $i \in I$ ensemble fini, et $r_i < \frac{r}{2}$, sur lesquels $\tilde{f}$ existe (elle est alors bien déterminée à addition près d'un élément de Λ_2, que l'on peut choisir de telle sorte que les deux déterminations de $\tilde{f}$ coïncident sur $D(a_i, r_i^-) \cap D(0, r^-)$). Alors $\tilde{f}$ est holomorphe sur la réunion de $D(0, r^-)$ et des $D(a_i, r_i^-)$ et contient $D(0, s^-)$ avec $s > r$.

• la courbe d'équation $Y^2 = 4X^3 - 4X$ d'invariant $j = 1728$, qui est à multiplication complexe par $\mathbf{Q}(\sqrt{-1})$, avec action de $\sqrt{-1}$ par $[\sqrt{-1}] \cdot (X, Y) = (-X, \sqrt{-1}Y)$;

• la courbe d'équation $Y^2 = 4X^3 - 4$ d'invariant $j = 0$, qui est à multiplication complexe par $\mathbf{Q}(\sqrt{-3})$, avec action de la racine 3-ième de l'unité $\rho = \frac{-1+\sqrt{-3}}{2}$ par $[\rho] \cdot (X, Y) = (X, \rho Y)$.

On remarque que ces deux courbes sont définies sur $\overline{\mathbf{Q}}$; c'est le cas général : si E est à multiplication complexe, alors $j(E) \in \overline{\mathbf{Q}}$ (cela suit de la finitude du nombre de classes d'idéaux pour un ordre d'un corps quadratique imaginaire : si $\sigma \in \mathrm{Aut}(\mathbf{C})$, alors $j(\sigma(E)) = \sigma(j(E))$ et $\sigma(E)$ a le même anneau d'endomorphismes que E ; la finitude du nombre de classes permet alors d'en déduire que $\sigma(j(E))$ ne peut prendre qu'un nombre fini de valeurs). On peut même montrer, par exemple en utilisant la courbe de Tate, que $j(E)$ est un entier algébrique.

$\alpha_1 = 2\int_1^{+\infty} \frac{dX}{\sqrt{4X^3-4X}}$ appartient au réseau des périodes de $Y^2 = X^3 - X$ (en effet, $(1, 0)$ est un point de 2-torsion). Or un petit calcul montre que

$$\alpha_1 = \int_1^{+\infty} \frac{dX}{\sqrt{X^3 - X}} = \frac{1}{2}\int_0^1 \frac{1}{\sqrt{t^{-3/2} - t^{-1/2}}} \frac{dt}{t^{3/2}} = \frac{1}{2}\int_0^1 t^{\frac{1}{4}-1}(1-t)^{\frac{1}{2}-1} = \frac{1}{2}\,\frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/2)}.$$

Comme E a de la multiplication complexe, on en déduit que les périodes de $\omega = \frac{dX}{Y}$ s'expriment en termes de la fonction Γ en des nombres rationnels, et la formule de Legendre montre qu'il en est de même des périodes de $\eta = X\frac{dX}{Y}$. C'est un cas particulier de la formule de Chowla-Selberg : si $E/\overline{\mathbf{Q}}$ est à multiplication complexe par $\mathbf{Q}(\sqrt{-D})$, avec $-D \equiv 0$ ou $1 \bmod 4$, alors les périodes de E, à multiplication près par un élément de $\overline{\mathbf{Q}}^*$, sont des produits des $\Gamma(a/D)^{\pm 1}$, avec $1 \leqslant a \leqslant D - 1$.

1.3. Courbe elliptique sur un corps p-adique

Dans ce qui suit, K est une extension finie de $\mathbf{Q}_p$ (et $p \geqslant 5$ pour nous simplifier la vie), $\mathscr{O}_K$ est l'anneau des entiers de K, π_K une uniformisante (i.e. un générateur de l'idéal maximal $\mathfrak{m}_K$ de $\mathscr{O}_K$), et $k_K = \mathscr{O}_K/\mathfrak{m}_K$ est le corps résiduel de K. On choisit une clôture algébrique $\overline{K}$ de K, et les extensions finies de K considérées sont supposées être des sous-corps de $\overline{K}$. Si L est une de ces extensions ou $\overline{K}$, on note $\mathscr{O}_L$, $\mathfrak{m}_L$ et k_L les objets évidents ; en particulier, $k_{\overline{K}}$ est une clôture algébrique de k_K. On note souvent $\overline{x}$ la « réduction de x modulo p », i.e. l'image de $x \in \mathscr{O}_L$ dans k_L.

1.3.1. La réduction modulo p. — Soit E une courbe elliptique définie sur K d'équation $Y^2 = X^3 + AX + B$. Le changement de variables $X \mapsto u^{-2}X$ et $Y \mapsto u^{-3}Y$ transforme cette équation en $Y^2 = X^3 + u^4AX + u^6B$ et $\Delta = 4A^3 + 27B^2$ en $u^{12}\Delta$. On voit donc que, quitte à faire ce changement de variables, avec u de la forme π_K^n, $n \in \mathbf{Z}$, on peut s'arranger pour que A et B soient dans $\mathscr{O}_K$, ce qui permettra de les réduire modulo $\mathfrak{m}_K$. Par contre, on ne peut pas imposer que $\overline{\Delta} \neq 0$ même si $\Delta \neq 0$, mais on peut essayer de maximiser les chances qu'il en soit ainsi en prenant $n \in \mathbf{Z}$ minimal (ceci a pour but que la réduction modulo p perde le moins d'information possible) ; on dit qu'on a un modèle de Weierstrass minimal de E.

Dans toute la suite, on part d'une équation de E de la forme $Y^2 = X^3 + AX + B$, avec $A, B \in \mathscr{O}_K$; beaucoup de choses dépendent de l'équation en question, mais pas si on a pris

la précaution de prendre un modèle de Weierstrass minimal. La réduction $\overline{E}$ modulo p de E d'équation $Y^2 = X^3+\overline{A}X+\overline{B}$ n'est pas forcément une courbe elliptique, et on note $\overline{E}^{\mathrm{ns}}$ l'ensemble de ses points non singuliers. On dit que E a *bonne réduction* si $\overline{E}$ est une courbe elliptique (auquel cas, $\overline{E} = \overline{E}^{\mathrm{ns}}$), a *réduction multiplicative* (déployée ou non), si $Y^2 = X^3 + \overline{A}X + \overline{B}$ est multiplicative (déployée ou non), et a *réduction additive* si $Y^2 = X^3 + \overline{A}X + \overline{B}$ est additive (i.e. $\overline{A} = \overline{B} = 0$).

On dispose d'une application $P \mapsto \overline{P}$ de « réduction modulo p » de $E(L)$ dans $\overline{E}(k_L)$, si L est une extension finie de K ou si $L = \overline{K}$; celle-ci est définie de la manière suivante. Si $[x : y : z] \in \mathbf{P}^2(L)$, et si $a \in L^*$ est tel que $v_p(a) = \min(v_p(x), v_p(y), v_p(z))$, alors $[a^{-1}x, a^{-1}y, a^{-1}z]$ est à coordonnées dans $\mathscr{O}_L$ et l'une des coordonnées appartient à $\mathscr{O}_L^*$; sa réduction modulo $\mathfrak{m}_L$ est donc un point bien défini de $\mathbf{P}^2(k_L)$, et ce point ne dépend pas du choix de a. On obtient donc de la sorte une application $P \mapsto \overline{P}$ de réduction modulo p de $\mathbf{P}^2(L)$ dans $\mathbf{P}^2(k_L)$, et l'image de $E(L)$ est incluse dans $\overline{E}(k_L)$.

Proposition 1.24. — *Soient $E_0(L)$ et $E_1(L)$ définis par*

$$E_0(L) = \{P \in E(L),\ \overline{P} \in \overline{E}^{\mathrm{ns}}(k_L)\} \quad \text{et} \quad E_0(L) = \{P \in E(L),\ \overline{P} = 0\}.$$

Alors $E_1(L) \subset E_0(L)$ sont des sous-groupes de $E(L)$ et la réduction modulo p induit un morphisme de groupes de $E_0(L)$ dans $\overline{E}^{\mathrm{ns}}(k_L)$ qui est surjectif et dont le noyau est $E_1(L)$.

Démonstration. — Les additions dans $E(L)$ et $\overline{E}^{\mathrm{ns}}(k_L)$ sont définies en termes d'alignement dans $\mathbf{P}^2$. Or la réduction modulo p d'une droite de $\mathbf{P}^2(L)$ est une droite de $\mathbf{P}^2(k_L)$; on en déduit la proposition à l'exception de la surjectivité de $E_0(L) \to \overline{E}^{\mathrm{ns}}(k_L)$. Celle-ci suit du lemme de Hensel : si $(x_0, y_0) \in \overline{E}^{\mathrm{ns}}(k_L)$, et si $\hat{x}_0, \hat{y}_0 \in \mathscr{O}_L$ sont des relèvements de x_0 et y_0, alors au moins l'une des deux dérivées partielles $\frac{\partial f}{\partial X}(\hat{x}_0, \hat{y}_0)$, $\frac{\partial f}{\partial Y}(\hat{x}_0, \hat{y}_0)$ (où $f(X, Y) = Y^2 - X^3 - AX - B$) est une unité de $\mathscr{O}_L$; comme $f(\hat{x}_0, \hat{y}_0) \in \mathfrak{m}_L$, le lemme de Hensel montre que l'une des deux équations $f(X, \hat{y}_0) = 0$ ou $f(\hat{x}_0, Y) = 0$ a une solution dont la réduction modulo p est ce qu'on veut.

Remarque 1.25. — Si L est une extension finie de K, alors k_L est un corps fini et donc $\overline{E}^{\mathrm{ns}}(k_L)$ est un groupe fini et donc de torsion. On en déduit le fait que $\overline{E}^{\mathrm{ns}}(k_{\overline{K}})$ est un groupe de torsion puisque c'est la réunion des $\overline{E}^{\mathrm{ns}}(k_L)$, pour L extension finie de K.

1.3.2. Le groupe $E_1(K)$ et la loi de groupe formel. — Pour étudier le groupe $E_1(K)$ qui vit dans un voisinage du point à l'infini, on a intérêt à ramener ce dernier en $(0, 0)$. On se place donc dans le plan affine $Y = 1$ et on pose $Z = \frac{X}{Y}$, $W = \frac{1}{Y}$ (et donc $X = \frac{Z}{W}$, $Y = \frac{1}{W}$). L'équation de la courbe (en affine) devient alors $W = Z^3 + AZW^2 + BW^3$.

Lemme 1.26. — (i) *Il existe $W \in Z^3(1 + Z\mathscr{O}_K[[Z]])$ unique tel que $(Z, W(Z)) \in E(\mathscr{O}_K[[Z]])$* (i.e. vérifie l'équation $W = Z^3 + AZW^2 + BW^3$).

(ii) *$P = (w, z) \in E_1(L)$ si et seulement si $z \in \mathfrak{m}_L$ et $w = W(z)$.*

Démonstration. — (i) Soit $\Phi_Z : Z^3(1+Z\mathscr{O}_K[[Z]]) \to Z^1(1+Z\mathscr{O}_K[[Z]])$ l'application définie par $\Phi_Z(F) = Z^3+AZF^2+BF^3$. On a $\Phi_Z(F_1)-\Phi_Z(F_2) = (F_1-F_2)(AZ(F_1+F_2)+B(F_1^2+F_1F_2+F_2^2)$, et donc $v_Z(\Phi_Z(F_1)-\Phi_Z(F_2)) \geqslant v_Z(F_1-F_2)+1$. On en déduit que Φ_Z est contractante et donc a un unique point fixe $W(Z)$; ce point fixe répond à la question.

(i) Si $\overline{P}=0$, alors $v_p(y)<0$ ou $v_p(x)<0$. Mais alors l'égalité $y^2=x^3+Ax+B$ et le fait que $v_p(A)\geqslant 0$ et $v_p(B)\geqslant 0$ impliquent que $2v_p(y)=3v_p(x)$ et donc que $v_p(z)=-\frac{1}{2}v_p(x)>0$ et $v_p(w)=-v_p(y)>0$. Mais l'application $\Phi_z : \mathfrak{m}_L \to \mathfrak{m}_L$ définie par $\Phi_z(u)=z^3+Azu^2+Bu^3$ est contractante pour les mêmes raisons que ci-dessus et son unique point fixe w est la solution de l'équation $w=z^3+azw^2+Bw^3$ dans $\mathfrak{m}_L$; on a donc $w=W(z)$ puisque $W(z)$ est une solution de cette équation. Comme $v_p(W(z))=3v_p(z))$, on en déduit que $P=(z,W(z))$ est bien dans le noyau de la réduction modulo p car les valuations de x et y sont <0.

Il résulte de la proposition précédente que $P=(z,w)\mapsto z$ est une bijection de $E_1(L)$ sur $\mathfrak{m}_L$, et comme $E_1(L)$ est un groupe, cela munit, en transportant la loi de groupe via cette bijection, $\mathfrak{m}_L$ d'une loi de groupe. On note $\widehat{E}(\mathfrak{m}_L)$ le groupe ainsi obtenu ; nous allons expliciter la loi d'addition.

Comme on a fait un changement de coordonnées projectives pour passer de (X,Y) à (W,Z), la loi de groupe sur $E_1(L)$ est encore définie par l'alignement. Soient donc $P_1=(z_1,W(z_1))$ et $P_2=(z_2,W(z_2))$ deux éléments de $E_1(L)$ (et donc $z_1,z_2\in\mathfrak{m}_L$). La droite passant par P_1 et P_2 est la droite d'équation $W=W(z_1)+\lambda(Z-z_1)$, avec $\lambda=\frac{W(z_2)-W(z_1)}{z_2-z_1}\in(z_1,z_2)^2\mathscr{O}_K[[z_1,z_2]]$. En injectant la valeur de W dans l'équation $W=Z^3+AZW^2+BW^3$, on obtient une équation du troisième degré dont deux des racines sont z_1 et z_2 et la somme est

$$S(z_1,z_2)=\frac{-2A(W(z_1)-\lambda z_1)-3B(W(z_1)-\lambda z_1)^2}{1+A\lambda^2+B\lambda^3}\in(z_1,z_2)^3\mathscr{O}_K[[z_1,z_2]].$$

Comme la troisième racine est l'opposé de z_3, si $P_1\oplus P_2=(z_3,W(z_3))$, on voit que $z_3=z_1+z_2-S(z_1,z_2)$, avec $S(z_1,z_2)\in(z_1,z_2)^3\mathscr{O}_K[[z_1,z_2]]$. On reconnait là une loi de groupe formel[(12)] définie sur $\mathscr{O}_K$ que l'on notera $z_1+_{\widehat{E}}z_2$.

[(12)] De manière générale, une loi de groupe formel (de dimension 1) définie sur un anneau A est une série $F(X,Y)=X+Y+R(X,Y)$, avec $R(X,Y)\in(X,Y)^2A[[X,Y]]$ vérifiant les conditions
• $F(F(X,Y),Z)=F(X,F(Y,Z))$ dans $A[[X,Y,Z]]$,
• il existe $i(X)\in XA[[X]]$ tel que $F(X,i(X))=F(i(X),X)=0$,
la première condition reflétant l'associativité de la loi de groupe formel, et la seconde, l'existence d'un inverse. Une loi de groupe formel est commutative si $F(X,Y)=F(Y,X)$ dans $A[[X,Y]]$.
À partir d'une loi de groupe formel F définie sur un anneau A, on fabrique des tas de groupes : il suffit de partir d'une A-algèbre B séparée et complète pour une topologie I-adique, où I est un idéal de B. Alors F munit I d'une loi de groupe $\oplus$ définie par $a\oplus b=F(a,b)$; l'inverse de $a\in I$ étant $i(a)$ et l'associativité de la loi de groupe étant assurée par l'identité $F(F(X,Y),Z)=F(X,F(Y,Z))$ et par le caractère ultramétrique de la topologie sur I qui permet de réarranger les séries comme on veut du moment que le terme général tend vers 0. On note $\mathscr{F}(I)$ le groupe ainsi obtenu ; c'est le groupe des points à valeurs dans I du groupe formel $\mathscr{F}$ associé à F. On note aussi souvent $+_{\mathscr{F}}$ la loi de groupe sur $\mathscr{F}(I)$.
Parmi les exemples de groupes formels commutatifs que l'on rencontre souvent, on trouve, outre le groupe formel associé à une courbe elliptique qui est apparu ci-dessus :

Si $n \in \mathbf{N}$, on note $[n]_{\widehat{E}}Z = nZ + \cdots$ la multiplication par n dans $\widehat{E}$; elle est définie par récurrence en posant $[n+1]_{\widehat{E}}Z = [n]_{\widehat{E}}Z +_{\widehat{E}} Z$. On a bien évidemment

$$[n]_{\widehat{E}}Z +_{\widehat{E}} [m]_{\widehat{E}}Z = [n+m]_{\widehat{E}}Z \quad \text{et} \quad [n]_{\widehat{E}}([m]_{\widehat{E}}Z) = [nm]_{\widehat{E}}, \quad \text{si } n, m \in \mathbf{N}.$$

Proposition 1.27. — (i) *Si $\alpha \in \mathbf{Z}_p$ et $(k_n)_{n\in\mathbf{N}}$ est une suite croissante d'éléments de $\mathbf{N}$ tendant vers α dans $\mathbf{Z}_p$, alors $[k_n]_{\widehat{E}}Z$ a une limite $[\alpha]_{\widehat{E}}Z = \alpha Z + \cdots \in Z\mathscr{O}_K[[Z]]$ qui ne dépend pas de la suite $(k_n)_{n\in\mathbf{N}}$.*

(ii) *On a $[\alpha]_{\widehat{E}}Z +_{\widehat{E}} [\beta]_{\widehat{E}}Z = [\alpha+\beta]_{\widehat{E}}$ et $[\alpha]_{\widehat{E}}([m]_{\widehat{E}}Z) = [\alpha\beta]_{\widehat{E}}Z$, si $\alpha, \beta \in \mathbf{Z}_p$.*

(iii) *$\widehat{E}(\mathfrak{m}_L)$ est un $\mathbf{Z}_p$-module, si L est une extension de K.*

Démonstration. — On a $[p]_{\widehat{E}}Z \in Z(p,Z)\mathscr{O}_K[[Z]]$. On en déduit, par récurrence que $[p^m]_{\widehat{E}}Z \in Z(p,Z)^m\mathscr{O}_K[[Z]]$, si $m \in \mathbf{N}$. Maintenant, si la suite $(k_n)_{n\in\mathbf{N}}$ a une limite dans $\mathbf{Z}_p$, on a $k_{n+1}-k_n = p^m a_n$, avec $a_n \in \mathbf{N}$, si n est assez grand. En écrivant $[k_{n+1}]_{\widehat{E}}Z$ sous la forme $[k_{n+1}]_{\widehat{E}}Z +_{\widehat{E}} [a_n]_{\widehat{E}}([p^m]_{\widehat{E}}Z)$, on en déduit que la suite $[k_n]_{\widehat{E}}Z$ est stationnaire modulo $Z(p,Z)^m\mathscr{O}_K[[Z]]$ à partir d'un certain rang, et comme $\mathscr{O}_K[[Z]]$ est séparé et complet pour la topologie (p,Z)-adique, cela prouve que $[k_n]_{\widehat{E}}Z$ a une limite dans $Z\mathscr{O}_K[[Z]]$. L'indépendance de la limite par rapport au choix de la suite est alors immédiate, et le (ii) ainsi que le développement $[\alpha]_{\widehat{E}}Z = \alpha Z + \cdots$ se démontrent facilement par un passage à la limite. Le (iii) quant à lui est une réécriture du (ii).

1.3.3. Le module de Tate $T_\ell(E)$ dans le cas $\ell \neq p$. — Nous allons nous intéresser aux propriétés de ramification du module de Tate d'une courbe elliptique. Comme p est déjà la caractéristique du corps résiduel de K, on choisit un second nombre premier ℓ.

Lemme 1.28. — *Si E a bonne réduction, alors la réduction modulo p induit une injection de $E(L)[m]$ dans $\overline{E}(k_L)[m]$, pour tout m premier à p et toute extension L de K.*

Démonstration. — Le noyau de cette réduction modulo p est $E_1(L) \cong \widehat{E}(\mathfrak{m}_L)$ qui ne contient pas de point d'ordre m puisque c'est un $\mathbf{Z}_p$-module et que m est inversible dans $\mathbf{Z}_p$.

Théorème 1.29. — *Soit E ayant bonne réduction.*

(i) *Si $(m,p) = 1$, alors $E(\overline{K})[m] = E(K^{\mathrm{nr}})[m]$ et la réduction modulo p induit un isomorphisme $(K^{\mathrm{nr}})[m] \cong \overline{E}(k_{\overline{K}})[m]$. En particulier, $\overline{E}(k_{\overline{K}})[m] \cong (\mathbf{Z}/m\mathbf{Z})^2$.*

(ii) *Si $\ell \neq p$, alors $T_\ell(E)$ est une représentation non ramifiée de G_K.*

Démonstration. — Soit $\overline{P} \in \overline{E}(k_{\overline{K}})[m]$. Il existe $L \subset K^{\mathrm{nr}}$ tel que $\overline{P} \in \overline{E}(k_L)$, et comme $\overline{E}$ est lisse, on peut utiliser le lemme de Hensel pour montrer qu'il existe $\tilde{P} \in E(L)$ ayant $\overline{P}$ comme réduction modulo p. Mais alors $[m]_E\tilde{P} \in E_1(L) \cong \widehat{E}(\mathfrak{m}_L)$, et comme m est premier à p, il existe $Q \in E_1(L)$ tel que $[m]_E\tilde{P} = [m]_E Q$ (si $z \in \widehat{E}(\mathfrak{m}_L)$ est l'image de $[m]_E\tilde{P}$, il suffit de prendre pour Q l'image inverse de $[m^{-1}]_{\widehat{E}}z$). Mais alors $\tilde{P} -_E Q$ est un point de m-torsion défini sur $L \subset K^{\mathrm{nr}}$ ayant pour réduction $\overline{P}$. On en déduit que la réduction modulo p induit une surjection

---

• le groupe formel additif $\mathbf{G}_a$, dont la loi est $F(X,Y) = X + Y$,

• le groupe formel multiplicatif $\mathbf{G}_m$, dont la loi est $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$.

de $E(K^{\mathrm{nr}})[m]$ sur $\overline{E}(k_{\overline{K}})[m]$ et donc une bijection puisque l'on a déjà démontré l'injectivité (cf. lemme 1.28).

Maintenant, si $P \in E(\overline{K})[m]$, il existe $P' \in E(K^{\mathrm{nr}})[m]$ ayant même réduction modulo p d'après ce qui précède, et on a $P = P'$ par injectivité de cette réduction modulo p. Ceci termine la démonstration du (i).

Enfin, si $u = (0, u_1, \dots, u_n, \dots) \in T_\ell(E)$, alors $u_n \in E(K^{\mathrm{nr}})$ pour tout n, d'après le (i). Ceci implique que u_n est fixe par I_K pour tout n, et donc que I_K agit trivialement sur u. On en déduit le (ii).

1.3.4. Le cas $\ell = p$. — . Ce cas repose sur une analyse plus fine de la multiplication par p dans le groupe formel $\widehat{E}(\mathfrak{m}_{\overline{K}})$.

Lemme 1.30. — (i) *Si $a \in \mathfrak{m}_{\overline{K}}$, et si t_a désigne la translation par a dans $\widehat{E}(\mathfrak{m}_{\overline{K}})$ (i.e. $t_a(z) = z +_{\widehat{E}} a$), alors t'_a ne s'annule pas sur $\mathfrak{m}_{\overline{K}}$.*

(ii) *La dérivée de $[p]_{\widehat{E}}Z$ ne s'annule pas sur $\mathfrak{m}_{\overline{K}}$.*

Démonstration. — On a $t_{-a} \circ t_a = \mathrm{id}$, et en dérivant, on en déduit que t'_a ne s'annule pas (on peut aussi le démontrer par un argument de valuation p-adique). Maintenant, on a $[p]_{\widehat{E}} \circ t_a = t_{pa} \circ [p]_{\widehat{E}}$; on en déduit, en dérivant que $t'_a(z)\ [p]'_{\widehat{E}}(z+a) = [p]'_{\widehat{E}}(z)t'_{pa}([p]_{\widehat{E}}z)$. Ceci implique que si $[p]'_{\widehat{E}}(z) = 0$, alors $[p]'_{\widehat{E}}(z+a) = 0$ pour tout a, et donc que $[p]_{\widehat{E}}$ est constante, ce qui est absurde. On en déduit le résultat.

Proposition 1.31. — *Si E n'a pas réduction additive, alors $[p]_{\widehat{E}}Z \notin \mathfrak{m}_K[[Z]]$.*

Démonstration. — On a $k_K(\overline{E}) = k_K(Z)[W]/(W - Z^3 - \overline{A}ZW^2 - \overline{B}W^3)$. On en déduit que $k_K(\overline{E})$ s'injecte dans $k_K((Z))$, en envoyant W sur la réduction modulo $\mathfrak{m}_K$ de l'élément $W(Z)$ de $Z^3(1 + Z\mathscr{O}_K[[Z]])$ de la prop. 1.26. Maintenant, la multiplication par p sur $\overline{E}^{\mathrm{ns}}$ dans les coordonnées (Z, W) est donnée par une paire $(f_1(Z,W), f_2(Z,W))$ d'éléments de $k_K(\overline{E})$, et la réduction de $[p]_{\widehat{E}}Z$ modulo $\mathfrak{m}_K$ n'est autre que l'image de $f_1(Z,W)$ dans $k_K((Z))$ par le morphisme ci-dessus. On en déduit que cette réduction est nulle si et seulement si la multiplication par p sur $\overline{E}^{\mathrm{ns}}$ est identiquement nulle, ce qui n'est possible ni dans le cas de réduction multiplicative (il existe des racines de l'unité d'ordre premier à p dans $k_{\overline{K}}^*$), ni dans le cas de bonne réduction puisque $\overline{E}(k_{\overline{K}})$ contient des points d'ordre m premier à p, pour tout m (th. 1.29). Ceci permet de conclure.

Théorème 1.32. — *Soit E une courbe elliptique définie sur K ayant bonne réduction modulo p.*

(i) *Le groupe $E_1(\overline{K})$ est p-divisible (i.e la multiplication par p est surjective).*

(ii) *Il existe $h = 1, 2$* (c'est la hauteur du groupe formel $\widehat{E}$) *tel que $E_1(\overline{K})[p^n] \cong (\mathbf{Z}/p^n\mathbf{Z})^h$ et $\overline{E}(k_{\overline{K}})[p^n] \cong (\mathbf{Z}/p^n\mathbf{Z})^{2-h}$, pour tout $n \in \mathbf{N}$.*

(iii) *$T_p(E)$ est une représentation ramifiée de G_K.*

Démonstration. — On a vu que $[p]_{\widehat{E}}Z = pZ + a_2Z^2 + a_3Z^3 + \cdots$ n'est pas nul modulo $\mathfrak{m}_K$. On note m le plus petit entier tel que a_m soit une unité de $\mathscr{O}_K^*$. L'équation $[p]_{\widehat{E}}Z = 0$ a alors m solutions (avec multiplicité) dans $\mathfrak{m}_{\overline{K}}$, et comme la dérivée de $[p]_{\widehat{E}}Z$ ne s'annule pas sur $\mathfrak{m}_{\overline{K}}$, ces solutions sont toutes simples, et donc l'équation $[p]_{\widehat{E}}Z = 0$ a alors m solutions distinctes dans

$\mathfrak{m}_{\overline{K}}$. De plus, l'ensemble de ces solutions est le groupe des points d'ordre p de $\widehat{E}(\mathfrak{m}_{\overline{K}}) \cong E_1(\overline{K})$, et donc s'identifie à un sous-groupe de $E(\overline{K})[p] \cong (\mathbf{Z}/p\mathbf{Z})^2$. On en déduit que $m = p^h$, avec $h = 1$ ou $h = 2$.

Le même argument prouve que l'équation $[p]_{\widehat{E}}Z = x$ a p^h solutions dans $\mathfrak{m}_{\overline{K}}$, si $x \in \mathfrak{m}_{\overline{K}}$, et en examinant le polygone de Newton de $[p]_{\widehat{E}}Z - x$ (dont tous les coefficients des termes de degré entre 1 et $p^h - 1$ sont divisibles par π_K par définition de h), que ces solutions ont toutes une valuation $\leqslant \sup(p^{-h}v_p(x), v_p(x) - v_p(\pi_K))$.

En d'autres termes, la multiplication par p sur le $\mathbf{Z}_p$-module $\widehat{E}(\mathfrak{m}_{\overline{K}}) \cong E_1(\overline{K})$ est surjective et son noyau est $(\mathbf{Z}/p\mathbf{Z})^h$. On en déduit que $E_1(\overline{K})$ est la somme directe de $(\mathbf{Q}_p/\mathbf{Z}_p)^h$ et d'un $\mathbf{Q}_p$-espace vectoriel ; en particulier, $E_1(\overline{K})[p^n] \cong (\mathbf{Z}/p^n\mathbf{Z})^h$, pour tout $n \in \mathbf{N}$.

Maintenant, si $P \in \overline{E}(k_{\overline{K}})[p^n]$, on peut relever P en $\tilde{P} \in E(K^{\mathrm{nr}})$ (grâce au lemme de Hensel, comme on l'a vu précédemment), et on a $[p^n]\tilde{P} \in E_1(K^{\mathrm{nr}})$. Comme la multiplication par p sur $E_1(\overline{K})$ est surjective, d'après ce qui précède, il existe $Q \in E_1(\overline{K})$ tel que $[p^n]Q = [p^n]\tilde{P}$. Mais alors $\hat{P} = \tilde{P} -_E Q \in E(\overline{K})[p^n]$ et a P pour réduction modulo p. On en déduit que la suite

$$0 \to E_1(\overline{K})[p^\infty] \to E(\overline{K})[p^\infty] \to \overline{E}(k_{\overline{K}})[p^\infty] \to 0$$

est exacte. Comme $E_1(\overline{K})[p^\infty] \cong (\mathbf{Q}_p/\mathbf{Z}_p)^h$, et $E(\overline{K})[p^\infty] \cong (\mathbf{Q}_p/\mathbf{Z}_p)^2$, on en déduit que $\overline{E}(k_{\overline{K}})[p^\infty] \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{2-h}$, et donc que $\overline{E}(k_{\overline{K}})[p^n] \cong (\mathbf{Z}/p^n\mathbf{Z})^{2-h}$, pour tout $n \in \mathbf{N}$.

Enfin, il résulte de la minoration ci-dessus pour les valuations des solutions de l'équation $[p]_{\widehat{E}}Z = x$ que si $u = (0, u_1, \dots, u_n, \dots) \in T_p(\widehat{E}(\mathfrak{m}_{\overline{K}}))$, alors $v_p(u_n) > 0$ tend vers 0 quand n tend vers $= \infty$. En particulier, les u_n ne sont pas dans K^{nr}, si n est assez grand, ce qui prouve que $T_p(\widehat{E}(\mathfrak{m}_{\overline{K}}))$ est une représentation ramifiée de G_K, et comme $T_p(\widehat{E}(\mathfrak{m}_{\overline{K}})) \subset T_p(E)$, la représentation $T_p(E)$ est a fortiori ramifiée.

1.3.5. La courbe de Tate. — Si E est une courbe elliptique sur $\mathbf{C}$, on peut choisir la forme différentielle invariante ω de telle sorte qu'une des périodes soit $2i\pi$ et donc que le réseau des périodes Λ soit de la forme $\Lambda = 2i\pi(\mathbf{Z} + \mathbf{Z}\tau)$, avec $\mathrm{Im}(\tau) > 0$. On pose alors $w = e^z$ et $q = e^{2i\pi\,\tau}$ (on a $|q| < 1$), et on a des isomorphismes

$$\mathbf{C}/\Lambda \cong E(\mathbf{C}) \quad \text{et} \quad \mathbf{C}/\Lambda \cong \mathbf{C}^*/q^{\mathbf{Z}}$$

de groupes de lie (ou de surfaces de Riemann), le premier étant l'isomorphisme usuel induit par $z \mapsto \phi(z) = (\wp(z), \wp'(z))$, et le second étant induit par $z \mapsto w = e^z$. D'où un isomorphisme $\mathbf{C}^*/q^{\mathbf{Z}} \cong E(\mathbf{C})$ envoyant w sur $(X(w), Y(w))$, avec

$$X(w) = \frac{1}{12} + \sum_{m\in\mathbf{Z}} \frac{q^m w}{(1-q^m w)^2} - 2\sum_{m\geqslant 1} \frac{q^m}{(1-q^m)^2}$$

$$Y(w) = w\frac{d\,X(w)}{dw} = \sum_{m\in\mathbf{Z}} \frac{q^m w}{(1-q^m w)^2} + 2\frac{(q^m w)^2}{(1-q^m w)^3}$$

(Pour montrer que l'on a bien $X(e^z) = \wp(z)$, on constate que la différence est une fonction elliptique holomorphe, donc constante, et on regarde ce qu'elle vaut en 0.) L'équation de la

courbe elliptique E devient $Y^2 = 4X^3 - g_2X - g_3$, avec

$$g_2 = \frac{1}{12} + 20\sum_{n\geqslant 1}\sigma_3(n)q^n, \qquad g_2 = \frac{-1}{216} + \frac{7}{3}\sum_{n\geqslant 1}\sigma_5(n)q^n$$

$$\Delta = g_2^3 - 27g_3^2 = q\prod_{n\geqslant 1}(1-q^n)^{24} \qquad j = \frac{1728\, g_2^3}{\Delta} = \frac{1}{q} + 744 + 196884q + \cdots$$

et les coefficients de j sont des entiers riches d'information arithmétique et autre (ils sont liés aux dimensions des représentations du monstre, le plus grand groupe simple sporadique, phénomème connu sous le nom de « monster moonshine »).

Tate a remarqué que les formules précédentes avaient un sens dans tout corps complet où 2 et 3 sont inversibles (si 2 ou 3 n'est pas inversible, il faut se ramener à une équation de Weierstrass plus générale) ; cela l'a mené au résultat d'uniformisation p-adique suivant.

Théorème 1.33. — *Soient $p \geqslant 5$, K une extension finie de $\mathbf{Q}_p$, et E une courbe elliptique définie sur K ayant réduction multiplicative déployée. Alors :*

(i) *$|j(E)|_p > 0$ et il existe $q \in K^*$ unique, avec $|q|_p < 1$ et $j(q) = j(E)$;*

(ii) *E est isomorphe sur K à la courbe d'équation $Y^2 = 4X^3 - g_2(q)X - g_3(q)$;*

(iii) *l'application $w \mapsto (X(w), Y(w))$ induit un isomorphisme de groupe $\overline{K}^*/q^{\mathbf{Z}} \cong E(\overline{K})$ qui commute à l'action de G_K.*

Remarque 1.34. — (i) Si la réduction est multiplicative non déployée, il suffit de faire une extension quadratique pour la rendre déployée.

(ii) Contrairement au cas complexe, le théorème ne s'applique pas à toute courbe elliptique ; en particulier au cas de bonne réduction.

(iii) Le fait que $\overline{K}^*/q^{\mathbf{Z}} \cong E(\overline{K})$ commute à l'action de G_K implique que pour toute extension finie L de K, on a $L^*/q^{\mathbf{Z}} \cong E(L)$. En effet, si $P \in E(L)$ est l'image de $w \in \overline{K}^*$, alors $g(w)/w \in q^{\mathbf{Z}}$, pour tout $g \in \mathrm{G}_L$, mais comme $|g(w)|_p = |w|_p$, cela implique $g(w) = w$ et donc $w \in L^*$.

(iv) À part la surjectivité de $w \mapsto (X(w), Y(w))$ qui demande des techniques un peu plus sophistiquées, les arguments utilisés sont tous du type : les relations à vérifier en p-adique (comme $Y(w)^2 = 4X(w)^3 - g_2X(w) - g_3$) sont vraies au niveau des séries formelles puisqu'elles le sont sur $\mathbf{C}$, et donc sont vraies en tout point où tout converge.

Le théorème de Tate fournit une description particulièrement simple des points de torsion d'une courbe elliptique à réduction multiplicative déployée. On choisit, pour chaque m une racine primitive m-ième ζ_m de l'unité et une racine m-ième q_m de q en imposant que $\zeta_{mn}^n = \zeta_m$ et q_{mn}^n, pour tout couple d'entiers $m, n \geqslant 1$. On remarque que $(q_m)^m = q \in K^*$ est fixe par tout élément g de G_K, et donc qu'il existe $c_m(g) \in \mathbf{Z}/m\mathbf{Z}$ tel que $g(q_m) = q_m\zeta_m^{c_m(g)}$. Il n'est pas difficile de voir que, si ℓ est un nombre premier, alors les $c_{\ell^n}(g)$ définissent un élément $c_{\ell,q}(g)$ de $\mathbf{Z}_\ell$. Le résultat suivant est alors une conséquence immédiate du théorème de Tate en utilisant les éléments ci-dessus pour passer d'une notation multiplicative à une notation additive.

Corollaire 1.35. — (i) *Sous les hypothèses du th. 1.33, si* $m \geqslant 1$, *alors* $E(\overline{K})[m] \cong (\mathbf{Z}/m\mathbf{Z})^2$ *admet* ζ_m, q_m *comme base sur* $\mathbf{Z}/m\mathbf{Z}$.

(ii) *Si* ℓ *est un nombre premier, alors* $T_\ell(E) = \mathbf{Z}_\ell e_1 + \mathbf{Z}_\ell e_2$, *où* $e_1 = (1, \zeta_\ell, \dots)$ *est le générateur habituel de* $\mathbf{Z}_\ell(1)$ *et* $e_2 = (q, q_\ell, \dots)$ *; l'action de* $g \in \mathrm{G}_K$ *étant donnée par* $g(e_1) = \chi_\ell(g)e_1$ *et* $g(e_2) = e_2 + c_{\ell,q}(g)e_1$.

Remarque 1.36. — (i) La représentation $T_\ell(E)$ est ramifiée pour tout ℓ car la valuation de q_{ℓ^n} tend vers 0 (en étant > 0), ce qui montre que les q_{ℓ^n} ne vivent pas tous dans une extension non ramifiée de K, et donc que I_K ne fixe pas e_2.

(ii) Si $\ell \neq p$, le caractère χ_ℓ est trivial sur I_K, et donc l'action de I_K est unipotente (i.e. est donnée par des matrices dont la seule valeur propre est 1).

1.3.6. L'unipotence potentielle de l'action de l'inertie. — Le théorème qui suit montre qu'un représentation ℓ-adique du groupe de Galois G_K d'un corps p-adique est un objet relativement simple[(13)] si $\ell \neq p$.

Théorème 1.37. — (Grothendieck) *Soient* K *une extension finie de* $\mathbf{Q}_p$ *et* $\ell \neq p$. *Alors l'action de* I_K *est potentiellement unipotente sur toute représentation* ℓ*-adique de* G_K (i.e. si V est une représentation ℓ-adique de G_K, il existe une extension finie L de K et une base de V sur $\mathbf{Q}_\ell$ dans laquelle les matrices des éléments de I_L sont triangulaires supérieures avec des 1 sur la diagonale).

Démonstration. — La démonstration de ce théorème repose sur la structure du groupe G_K et son dévissage faisant intervenir le sous-groupe d'inertie sauvage (cf. prop. 4.26). On choisit un réseau T de V stable par G_K et une base $e_1, \dots, e_d$ de T sur $\mathbf{Z}_\ell$. On obtient donc, en écrivant l'action de G_K dans cette base, un morphisme de groupes $\rho : \mathrm{G}_K \to \mathbf{GL}_d(\mathbf{Z}_\ell)$. Maintenant, on a une suite exacte de groupes

$$1 \mapsto 1 + \ell\mathrm{M}_d(\mathbf{Z}_\ell) \to \mathbf{GL}_d(\mathbf{Z}_\ell) \to \mathrm{GL}_d(\mathbf{F}_\ell) \to 1,$$

et $1 \mapsto 1 + \ell\mathrm{M}_d(\mathbf{Z}_\ell)$ est un pro-ℓ-groupe (c'est la limite projective des $G_n = 1 + \ell\mathrm{M}_d(\mathbf{Z}_\ell)/1 + \ell^n\mathrm{M}_d(\mathbf{Z}_\ell)$, et le noyau de $G_{n+1} \to G_n$ égal à $1 + \ell^n\mathrm{M}_d(\mathbf{Z}_\ell)/1 + \ell^{n+1}\mathrm{M}_d(\mathbf{Z}_\ell)$ est isomorphe à $\mathrm{M}_d(\mathbf{F}_\ell)$ par $U \mapsto \ell^{-n}(U-1) \bmod \ell$, et donc aussi à $(\mathbf{Z}/\ell\mathbf{Z})^{d^2}$). Soit L le corps fixé par le noyau de $\overline{\rho} : \mathrm{G}_K \to \mathrm{GL}_d(\mathbf{F}_\ell)$, où $\overline{\rho}$ est le composé de ρ avec la réduction modulo ℓ. Comme $\mathrm{GL}_d(\mathbf{F}_\ell)$ est un groupe fini, L est une extension finie de K, et l'image de G_L par ρ est incluse dans $1 + \ell\mathrm{M}_d(\mathbf{Z}_\ell)$.

Maintenant, le sous-groupe d'inertie sauvage I_L^+ de I_L est un pro-p-groupe, et comme $\ell \neq p$, son image dans le pro-ℓ-groupe $1+\ell\mathrm{M}_d(\mathbf{Z}_\ell)$ est triviale. L'action de G_L se factorise donc à travers $\mathrm{Gal}(K^{\mathrm{mod}}/K)$ qui est une extension de $\widehat{\mathbf{Z}}$ (engendré par le frobenius $x \mapsto x^q$ sur $k_{\overline{K}}$, où $q = |k_K|$)

(13) La classification complète, connue sous le nom de correspondance de Langlands locale, a quand même pris une trentaine d'années, le résultat final ayant été obtenu par Harris-Taylor et simplifié par Henniart en 1999. La classification des représentations p-adiques de G_K repose sur des techniques radicalement différentes (programme de Fontaine).

par $\prod_{\ell'\neq p}\mathbf{Z}_{\ell'}(1)$. Pour la même raison, l'image de $\mathbf{Z}_{\ell'}(1)$ est triviale si $\ell'\neq\ell$, et donc l'action de I_L se factorise à travers $\mathbf{Z}_\ell(1)$, et celle de G_L à travers un groupe H extension de $\widehat{\mathbf{Z}}$ par $\mathbf{Z}_\ell(1)$.

Choisissons un élément φ de H relevant le frobenius, et un générateur topologique u de $\mathbf{Z}_\ell(1)$. On a $\varphi u\varphi^{-1}=u^q$ (c'est le sens de la notation $\mathbf{Z}_\ell(1)$ plutôt que $\mathbf{Z}_\ell$), et donc aussi $\rho(\varphi)\rho(u)\rho(\varphi)^{-1}=\rho(u)^q$. On en déduit que $\rho(u)$ et $\rho(u)^q$ ont les même valeurs propres (avec multiplicité) et que $\lambda\mapsto\lambda^q$ induit une permutation de l'ensemble des valeurs propres de $\rho(u)$. La puissance $d!$-ième de cette permutation étant l'identité, on en déduit que les valeurs propres de $\rho(u)$ sont des racines n-ièmes de l'unité, si $n=q^{d!}-1$, et donc que $\rho(u^n)$ est une matrice unipotente. Finalement, ceci implique que si on pose $M=L(\mu_n,\pi_L^{1/n})$, où π_L est une uniformisante de L, alors I_M agit de manière unipotente (en effet I_M est le sous-groupe d'indice n de I_L image inverse du sous-groupe d'indice n de $\mathrm{Gal}(L^{\mathrm{mod}}/L^{\mathrm{nr}})\cong\prod_{\ell'\neq p}\mathbf{Z}_{\ell'}(1)$; son image dans $\mathbf{Z}_\ell(1)$ est le sous-groupe fermé engendré par u^n).

2. L'anneau des nombres complexes p-adiques

2.1. Le corps $\mathbf{C}_p$

Soit $\overline{\mathbf{Q}}_p$ une clôture algébrique de $\mathbf{Q}_p$. D'après la théorie générale, v_p se prolonge de manière unique en une valuation sur $\overline{\mathbf{Q}}_p$. On note $\mathbf{C}_p$ le complété de $\overline{\mathbf{Q}}_p$ pour v_p. C'est un corps algébriquement clos d'après le th. 2.1. Ce corps joue, pour beaucoup de questions, le rôle de $\mathbf{C}$ en p-adique. Il est abstraitement isomorphe à $\mathbf{C}$ pour des raisons de cardinal, mais Tate a démontré (voir plus tard), qu'il ne contenait pas d'analogue raisonnable de $2i\pi$.

2.1.1. Le complété d'un corps algébriquement clos. — Comme on le sait, il existe une unique manière de prolonger une valuation à la clôture algébrique d'un corps valué complet. Cette clôture algébrique n'a aucune raison d'être complète (et elle ne l'est, en général, pas), donc on peut la compléter, reprendre la clôture algébrique, recompléter... Le théorème suivant montre qu'en fait le procédé converge très vite.

Théorème 2.1. — *Si K est un corps algébriquement clos muni d'une valuation, son complété $\widehat{K}$ est algébriquement clos.*

Démonstration. — Soit $P(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_0$ un polynôme unitaire irréductible de $\widehat{K}[X]$. Notre but est de prouver que P a une racine dans $\widehat{K}$. Quitte à remplacer P par $\alpha^nP(\frac{X}{\alpha})$, ce qui multiplie a_i par α^{n-i}, on peut supposer que P est à coefficients entiers. Commençons par supposer que P est séparable, c'est-à-dire que P et P' sont premiers entre eux. Il existe alors des polynômes U et V tels que l'on ait $UP+VP'=1$.

Soit, comme d'habitude, v_G la valuation de Gauss sur $\widehat{K}[X]$. Soit $C>\sup(0,-v_G(U),-2v_G(V))$, et, si $0\leqslant i\leqslant n-1$, soit $b_i\in K$ tels que l'on ait $v(b_i-a_i)\geqslant C$. Soit $x_0\in K$ une racine du polynôme $Q(X)=X^n+b_{n-1}X^{n-1}+\cdots+b_0$. On a $v(x_0)\geqslant 0$ car Q est à coefficients entiers. Ceci implique $v(U(x_0)P(x_0))\geqslant C+v_G(U)>0$ et donc $v(P'(x_0)V(x_0))=0$, d'où l'on tire $v(P'(x_0))\leqslant -v_G(V)$, et $v(P(x_0))\geqslant C>2v(P'(x_0))$. Le lemme de Hensel permet de conclure au fait que l'équation $P(x)=0$ a une solution dans $\widehat{K}$.

Si P est irréductible mais pas séparable, on est en caractéristique $p \neq 0$, et il existe Q irréductible et séparable et $m \in \mathbf{N}$ tel que l'on ait $P(X) = Q(X^{p^m})$. Si x est une racine de Q et x_n une suite d'éléments de K tendant vers x dans $\widehat{K}$, alors $x_n^{p^{-m}}$ est une suite d'éléments de K tendant vers une racine P (elle est de cauchy car $v(x^{p^{-m}} - y^{p^{-m}}) = p^{-m}v(x-y)$).

2.1.2. Le corps résiduel d'un corps algébriquement clos

Lemme 2.2. — *Soient K un corps ultramétrique complet et L une extension finie de K, alors k_L est une extension algébrique de k_K de degré $\leqslant [L : K]$.*

Démonstration. — On a $\mathscr{O}_K \cap \mathfrak{m}_L = \mathfrak{m}_K$ et donc k_K s'injecte dans k_L. Soient $\overline{\alpha}_1, \ldots, \overline{\alpha}_d$ des éléments de k_L formant une famille libre sur k_K. Choisissons pour chaque $i \in \{1, \ldots, d\}$ un élément α_i de $\mathscr{O}_L$ dont l'image dans k_L est $\overline{\alpha}_i$. Supposons que les α_i forment une famille liée sur K et soit $(\lambda_1, \ldots, \lambda_d)$ une famille d'éléments non tous nuls de K tels que l'on ait $\lambda_1\alpha_1 + \cdots + \lambda_d\alpha_d = 0$. Quitte à diviser tous les λ_i par celui qui a la plus grande norme, on peut supposer qu'ils sont tous éléments de $\mathscr{O}_K$ et que l'un d'entre eux est égal à 1, ce qui conduit à une contradiction quand on réduit modulo $\mathfrak{m}_L$. Ceci permet de conclure.

Lemme 2.3. — *Si K est un corps ultramétrique algébriquement clos, alors k_K est algébriquement clos.*

Démonstration. — Soit $\overline{P}(X) \in k_K[X]$ unitaire de degré $n \geqslant 1$ et soit $P(X) \in \mathscr{O}_K[X]$ unitaire de degré n relevant $\overline{P}$. Soit $\alpha \in K$ une racine de P. On a $\alpha \in \mathscr{O}_K$ (les pentes du polygone de Newton de P sont négatives, donc ses racines ont des valuations $\geqslant 0$), et l'image de α dans k_K est une racine de $\overline{P}$, ce qui permet de conclure.

Lemme 2.4. — *Si K est un corps ultramétrique et $\widehat{K}$ dénote son complété, alors $k_K = k_{\widehat{K}}$.*

Démonstration. — $\mathscr{O}_K \cap \mathfrak{m}_{\widehat{K}} = \{x \in \mathscr{O}_K \mid v(x) > 0\} = \mathfrak{m}_K$ et donc l'application naturelle de k_K dans $k_{\widehat{K}}$ est injective. D'autre part, comme $\mathscr{O}_K$ est dense dans $\mathscr{O}_{\widehat{K}}$, cette application est surjective, ce qui permet de conclure.

Corollaire 2.5. — *Si K est un corps valué complet, alors le corps résiduel de $\widehat{\overline{K}}$ est une clôture algébrique de k_K.*

2.1.3. Le théorème d'Ax-Sen-Tate. — $\sigma \in \mathrm{G}_K = \mathrm{Aut}(\overline{K}/K)$ agit par une isométrie sur $\overline{K}$; on peut donc étendre l'action de G_K par continuité en une action sur $\widehat{\overline{K}}$ qui est un corps algébriquement clos d'après le théorème 2.1.

Théorème 2.6. — *Soit H un sous-groupe fermé de G_K ; alors $(\widehat{\overline{K}})^H$ est le complété de $\overline{K}^H$. Autrement dit, $(\overline{K})^H$ est dense dans $(\widehat{\overline{K}})^H$.*

Soit $L = \overline{K}^H$; c'est un sous-corps parfait de $\overline{K}$. Si $\alpha \in \overline{K}$, on définit le *diamètre* $\Delta_L(\alpha)$ de α par rapport à L par $\Delta_L(\alpha) = \inf_{\sigma \in H} v(\sigma(\alpha) - \alpha)$. Notons que $\alpha \in L$ si et seulement si $\Delta_L(\alpha) = +\infty$.

La démonstration du théorème 2.6 repose sur la proposition suivante.

***Proposition 2.7* (Ax).** — *Il existe une constante C telle que si $\alpha \in \overline{K}$, alors il existe $a \in L$ vérifiant $v(\alpha - a) \geqslant \Delta_L(\alpha) - C$.*

Autrement dit, si α est presque fixe par H, alors $\alpha \in \overline{K}$ est proche d'un élément de L. Soit $x \in \widehat{\overline{K}}$ fixe par H. Si α_n est une suite d'éléments de $\overline{K}$ tendant vers x, alors $\Delta_L(\alpha_n)$ tend vers $+\infty$ car $v(\sigma(\alpha_n) - \alpha_n) = v(\sigma(\alpha_n) - \sigma(x) + x - \alpha_n) \geqslant \inf(v(\sigma(x - \alpha_n), v(x - \alpha_n)) = v(x - \alpha_n)$, et donc si a_n est un élément de L vérifiant $v(a_n - \alpha_n) \geqslant \Delta_L(\alpha_n) - C$, la suite a_n est une suite d'éléments de L tendant vers x, et $x \in \widehat{L}$, ce qu'il fallait démontrer pour déduire le th. 2.6 de la prop. 2.7.

Passons à la démonstration de la proposition 2.7. La démonstration est un peu différente suivant qu'on est en égale ou inégale caractéristique.

• *Le cas d'égale caractéristique.* Notons M le corps $L(\alpha)$; c'est une extension finie de L qui est séparable car L est parfait.

Le cas où K est de caractéristique 0 et son corps résiduel aussi est évident : on peut prendre $C = 0$, et poser $a = \mathrm{Tr}_{M/L}(y\alpha)$, avec $y = \frac{1}{[M:L]}$; on a alors $v(y) = 0$, et

$$a - \alpha = \sum_{\sigma \in \mathrm{Hom}_L(M, \overline{K})} \big(\sigma(y\alpha) - y\alpha\big) = y \cdot \sum_{\sigma \in \mathrm{Hom}_L(M, \overline{K})} (\sigma(\alpha) - \alpha))$$

a une valuation $\geqslant \inf_{\sigma \in \mathrm{Hom}_L(M, \overline{K})} v(\sigma(\alpha) - \alpha) = \Delta_L(\alpha)$.

Si K est de caractéristique p, l'application trace $\mathrm{Tr}_{M/L}$ est surjective (car M/L est séparable comme nous l'avons remarqué), et il existe $x \in M$ tel que l'on ait $\mathrm{Tr}_{M/L}(x) = 1$. Mais alors $\mathrm{Tr}_{M/L}(x^{p^{-n}}) = 1$ quel que soit $n \in \mathbf{N}$; on en déduit le fait que quel que soit $\delta > 0$, il existe $y \in M$ vérifiant $\mathrm{Tr}_{M/L}(y) = 1$ et $v(y) > -\delta$. Maintenant, on a $a = \mathrm{Tr}_{M/L}(y\alpha) \in L$ et

$$a - \alpha = \sum_{\sigma \in \mathrm{Hom}_L(M, \overline{K})} \big(\sigma(y\alpha) - \sigma(y)\alpha\big) = \sum_{\sigma \in \mathrm{Hom}_L(M, \overline{K})} \sigma(y)(\sigma(\alpha) - \alpha))$$

a un valuation $\geqslant \inf_{\sigma \in \mathrm{Hom}_L(M, \overline{K})} v(\sigma(y)) + v(\sigma(\alpha) - \alpha) \geqslant -\delta + \Delta_L(\alpha)$. On peut donc prendre pour C n'importe quel nombre strictement positif.

• *Le cas d'inégale caractéristique.* Supposons maintenant que K est de caractéristique 0 et que son corps résiduel est de caractéristique p ; quitte à renormaliser v, on peut supposer que $v = v_p$ (i.e. que $v(p) = 1$). Nous aurons besoin du lemme suivant.

Lemme 2.8. — *Soit $P \in \overline{K}[X]$ unitaire de degré n dont toutes les racines vérifient $v_p(\alpha) \geqslant u$*

(i) *Si $n = p^k d$ avec $(d, k) = 1$ et $d > 0$ et si $q = p^k$, alors le polynôme $P^{(q)}$, dérivée q-ième de P, a au moins une racine β vérifiant $v_p(\beta) \geqslant u$.*

(ii) *Si $n = p^{k+1}$ et $q = p^k$, alors $P^{(q)}$ a au moins une racine β vérifiant $v_p(\beta) \geqslant u - \frac{1}{p^{k+1} - p^k}$.*

Démonstration. — On a $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, avec $v_p(a_{n-i}) \geqslant iu$ d'après la théorie des polygônes de Newton (ou, ce qui revient au même, par un développement brutal). On a $\frac{1}{q!}P^{(q)}(X) = \sum_{i=0}^{n-q} \binom{n-i}{q} a_{n-i} X^{n-i-q}$, et le produit des racines de $P^{(q)}$ est, au signe près, $\frac{a_q}{\binom{n}{q}}$. On a donc $\sum_\beta v_p(\beta) = v_p(a_q) - v_p(\binom{n}{q}) \geqslant (n-q)u - v_p(\binom{n}{q})$, et il existe β vérifiant

$v_p(\beta) \geqslant u - \frac{1}{n-q} v_p(\binom{n}{q})$. D'autre part, on a $\binom{n}{q} = \frac{n}{q} \prod_{i=1}^{q-1} \frac{n-i}{i}$ et, comme $q = p^k$ et $v_p(n) \geqslant k$, on a $v_p(\frac{n-i}{i}) = 0$ et $v_p(\binom{n}{q}) = v_p(n) - v_p(q)$. On en déduit le résultat.

La proposition suivante montre que l'on peut prendre $C = \frac{p}{(p-1)^2}$.

Proposition 2.9. — *Si $[L(\alpha) : L] = n$ et $\ell(n)$ est le plus grand entier ℓ tel que $p^\ell \leqslant n$, il existe $a \in L$ vérifiant $v_p(a - \alpha) \geqslant \Delta_L(\alpha) - \sum_{i=1}^{\ell(n)} \frac{1}{p^i - p^{i-1}}$.*

Démonstration. — Par récurrence sur n, le cas $n = 1$ étant évident. On va appliquer le lemme précédent à $P = Q(X + \alpha)$, où Q est le polynôme minimal de α sur L. Remarquons que les racines de P sont les $\sigma(\alpha) - \alpha$, pour $\sigma \in H$, et donc que le u du lemme précédent peut être pris égal à $\Delta_L(\alpha)$. Il y a deux cas.

• Si n n'est pas une puissance de p, il existe $q \in \mathbf{N}$ tel que le polynôme $P^{(q)}$ ait une racine β vérifiant $v_p(\beta - \alpha) \geqslant \Delta_L(\alpha)$. D'autre part, si $\sigma \in H$, alors

$$v_p(\sigma(\beta) - \beta) = v_p(\sigma(\beta) - \sigma(\alpha) + \sigma(\alpha) - \alpha + \alpha - \beta) \geqslant \min(v_p(\sigma(\beta - \alpha), v_p(\sigma(\alpha) - \alpha), v_p(\beta - \alpha)),$$

et comme $v_p(\sigma(\beta - \alpha)) = v_p(\beta - \alpha) \geqslant \Delta_L(\alpha)$ et $v_p(\sigma(\alpha) - \alpha) \geqslant \Delta_L(\alpha)$ par définition, on en tire l'inégalité $\Delta_L(\beta) \geqslant \Delta_L(\alpha)$, et comme $[L(\beta) : L] < n$, cela permet de conclure en utilisant l'hypothèse de récurrence.

• Si $n = p^{k+1}$, on peut trouver une racine β de $P^{(p^k)}$ vérifiant $v_p(\beta - \alpha) \geqslant \Delta_L(\alpha) - \frac{v_p(p)}{p^{k+1} - p^k}$ et on obtient par le même raisonnement l'existence de $\beta \in \overline{K}$ vérifiant $\Delta_L(\beta) \geqslant \Delta_L(\alpha) - \frac{1}{p^{k+1} - p^k}$ et $[L(\beta) : L] < n = p^{k+1}$. On tire de l'hypothèse de récurrence l'existence de $a \in L$ vérifiant $v_p(\beta - a) \geqslant \Delta_L(\beta) - \sum_{i=1}^{k} \frac{1}{p^i - p^{i-1}} \geqslant \Delta_L(\alpha) - \sum_{i=1}^{k+1} \frac{1}{p^i - p^{i-1}}$ et comme $v_p(\alpha - \beta) \geqslant \Delta_L(\alpha) - \sum_{i=1}^{k+1} \frac{1}{p^i - p^{i-1}}$, cela permet de conclure.

2.1.4. L'extension cyclotomique de $\mathbf{Q}_p$ et son complété

Rappelons que si F est un corps, et si G_F est son groupe de Galois absolu, alors on dispose, pour tout p (différent de la caractèristique de F) d'un caractère $\chi : \mathrm{G}_F \to \mathbf{Z}_p^*$, le *caractère cyclotomique*, défini par le fait que si ζ est une racine de l'unité d'ordre une puissance de p, alors $g(\zeta) = \zeta^{\chi(g)}$ pour tout $g \in \mathrm{G}_F$.

Soit F une extension non ramifiée de $\mathbf{Q}_p$. Choisissons pour chaque n une racine p^n-ième primitive de l'unité $\varepsilon^{(n)}$, de telle sorte que $(\varepsilon^{(n+1)})^p = \varepsilon^{(n)}$. Si $n \geqslant 1$, soit $F_n = F(\varepsilon^{(n)})$, et soit $F_\infty = \cup_n F_n$.

Proposition 2.10. — (i) *Si $n \geqslant 1$, F_n est une extension totalement ramifiée de degré $(p-1)p^{n-1}$ de F, et $\pi_n = \varepsilon^{(n)} - 1$ en est une uniformisante.*

(ii) *Si $n \geqslant 1$, F_n est une extension galoisienne de F, et χ induit un isomorphisme de $\mathrm{Gal}(F_n/F)$ sur $(\mathbf{Z}/p^n\mathbf{Z})^*$.*

(iii) *F_∞ est une extension galoisienne de F, et χ induit un isomorphisme de $\Gamma_F = \mathrm{Gal}(F_\infty/F)$ sur $\mathbf{Z}_p^*$.*

Démonstration. — Soit P_n le polynôme cyclotomique d'indice p^n donné par la formule $P_n(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$. Le polynôme $Q_n(X) = P_n(X+1)$ est un polynôme d'Eisenstein (son terme constant est p et sa réduction modulo p est $X^{p^n-p^{n-1}}$) donc est irréductible sur F. On en déduit le (i).

Le corps F_n est le corps de décomposition du polynôme $X^{p^n}-1$; il est donc galoisien sur F. De plus, $\mathrm{Gal}(F_n/F)$ et $(\mathbf{Z}/p^n\mathbf{Z})^*$ ont même cardinal, et χ_n est injectif de manière évidente ; on en déduit le (ii), et le (iii) en passant à la limite projective.

Soit $\widehat{F}_\infty$ le complété de F_∞ pour v_p ; c'est aussi l'adhérence de F_∞ dans $\mathbf{C}_p$.

Lemme 2.11. — *Si $n \geqslant 1$ et $x \in F_\infty$, alors $p^{-k}\mathrm{Tr}_{F_{n+k}/F_n}(x)$ de dépend pas de l'entier k tel que $x \in F_{n+k}$.*

Démonstration. — Cela suit de ce que $\mathrm{Tr}_{F_{n+k+i}/F_n}(x) = [F_{n+k+i} : F_{n+k}]\mathrm{Tr}_{F_{n+k}/F_n}(x)$ si $x \in F_{n+k}$ et de ce que $[F_{N+k+i} : F_{n+k}] = p^i$.

Notons $\mathrm{R}_n : F_\infty \to F_n$ l'application dont le lemme ci-dessus assure l'existence.

Lemme 2.12. — (i) *L'application $\mathrm{R}_n : F_\infty \to F_n$ est F_n-linéaire, commute avec l'action de Γ_F, et on a $\mathrm{R}_n \circ \mathrm{R}_{n+k} = \mathrm{R}_n$.*

(ii) *Si $k \in \mathbf{Z}$, alors « $v_p(x) \geqslant kv_p(\pi_n)$ » $\Rightarrow$ « $v_p(\mathrm{R}_n(x)) \geqslant kv_p(\pi_n)$ ».*

Démonstration. — R_n commute à l'action de Γ_F car, si L/K est une extension de corps, et si $\sigma : L \to L^\sigma$ est un isomorphisme de corps, alors $\mathrm{Tr}_{L^\sigma/K^\sigma}(\sigma(x)) = \sigma(\mathrm{Tr}_{L/K}(x))$. Le reste du (i) est immédiat.

Pour démontrer le (ii), constatons que les π_{n+k}^i, pour $0 \leqslant i \leqslant p^k-1$ forment une base de $\mathscr{O}_{F_{n+k}}$ sur $\mathscr{O}_{F_n}$ puisque l'extension F_{n+k}/F_n est totalement ramifiée. On peut donc écrire $x \in \mathscr{O}_{F_{n+k}}$ de manière unique sous la forme

$$x = \sum_{j=0}^{p^k-1} a_j(1+\pi_{n+k})^j, \quad \text{avec } a_j \in \mathscr{O}_{F_n}.$$

Maintenant, on a $(1+\pi_{n+k})^{p^{k-i}} = 1+\pi_{n+i}$ si $i \leqslant k$, et

$$p^{-1}\mathrm{Tr}_{F_{n+i}/F_{n+i-1}}((1+\pi_{n+i})^j) = \begin{cases} (1+\pi_{n+i})^j & \text{si } p \mid j, \\ 0 & \text{si } (p,j) = 1. \end{cases}$$

On en déduit, par une récurrence immédiate, que $\mathrm{R}_n(x) = a_0$. Ceci permet de montrer que, si $v_p(x) \geqslant 0$, alors $v_p(\mathrm{R}_n(x)) \geqslant 0$. Le cas général s'en déduit en remarquant que « $v_p(x) \geqslant kv_p(\pi_n)$ » équivaut à « $x \in \pi_n^k\mathscr{O}_{F_n}$ », et en utilisant la F_n-linéarité de R_n.

Proposition 2.13. — *(i) La « trace de Tate normalisée » R_n s'étend par continuité en une application F_n-linéaire de $\widehat{F}_\infty$ dans F_n commutant à l'action de Γ_F. De plus, on a $v_p(\mathrm{R}_n(x)) \geqslant v_p(x) - v_p(\pi_n)$, pour tout $x \in \widehat{F}_\infty$.*

(ii) Si $x \in \widehat{F}_\infty$, alors $x = \lim_{n\to+\infty} \mathrm{R}_n(x)$.

Démonstration. — Il résulte du (ii) du lemme **??** que $v_p(\mathrm{R}_n(x)) \geqslant v_p(x) - v_p(\pi_n)$, pour tout $x \in F_\infty$, ce qui montre que R_n est uniformément continue sur F_∞, et donc s'étend par continuité à $\widehat{F}_\infty$. Le reste du (i) s'en déduit par passage à la limite.

Pour montrer le (ii), on commence par constater que $\mathrm{R}_n(x) = x$ si $x \in F_\infty$ et $n \gg 0$. Par ailleurs, comme $v_p(\pi_n) \leqslant v_p(\pi_1)$, la famille R_n est bornée dans l'ensemble des applications F_n-linéaires continues de $\widehat{F}_\infty$ dans F_n. On en déduit que, si $(x_k)_{k\in\mathbf{N}}$ est une suite d'éléments de F_∞ tendant vers x dans $\widehat{F}_\infty$, alors $\mathrm{R}_n(x - x_k)$ tend vers 0 uniformément pour $n \in \mathbf{N}$, ce qui permet d'inverser les limites :

$$\lim_{n\to+\infty}(\mathrm{R}_n(x)) = \lim_{n\to+\infty}(\lim_{k\to+\infty}\mathrm{R}_n(x_k)) = \lim_{k\to+\infty}(\lim_{n\to+\infty}\mathrm{R}_n(x_k)) = \lim_{k\to+\infty} x_k = x.$$

2.1.5. Il n'y a pas de $2i\pi$ dans $\mathbf{C}_p$!

Un analogue p-adique de $2i\pi$ devrait être défini par la formule $2i\pi = \lim_{n\to+\infty} p^n \log \varepsilon^{(n)}$. Le problème est que l'on a $\log_p \varepsilon^{(n)} = 0$ quel que soit $n \in \mathbf{N}$ et donc la formule précédente donne $2i\pi = 0$, ce qui n'est pas très raisonnable. Si on regarde ce que donne la formule précédente d'un point de vue galoisien et que l'on utilise la formule $\sigma(\varepsilon^{(n)}) = (\varepsilon^{(n)})^{\chi(\sigma)}$, si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on voit que le minimum que l'on puisse demander à un analogue p-adique de $2i\pi$ est de vérifier la formule $\sigma(2i\pi) = \chi(\sigma)2i\pi$ quel que soit $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$. Malheureusement (ou heureusement...), on a le résultat suivant.

Théorème 2.14. — *Si $k \in \mathbf{Z}$, alors $\{x \in \mathbf{C}_p,\ \sigma(x) = \chi(\sigma)^k x,\ \text{quel que soit } \sigma \in \mathrm{G}_{\mathbf{Q}_p}\} = \{0\}$, si $k \neq 0$ et est égal à $\mathbf{Q}_p$, si $k = 0$.*

Démonstration. — Le cas $k = 0$ suit directement du théorème d'Ax-Sen-Tate. Supposons donc dans ce qui suit que $k \neq 0$, et soit $x \in \mathbf{C}_p$ vérifiant $\sigma(x) = \chi(\sigma)^k x$, pour tout $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$. On a en particulier $\sigma(x) = x$ quel que soit $\sigma \in \ker\chi$, et donc $x \in \widehat{F}_\infty$, d'après le théorème d'Ax-Sen-Tate. On a alors

$$\sigma(\mathrm{R}_n(x)) = \mathrm{R}_n(\sigma(x)) = \chi(\sigma)^k \mathrm{R}_n(x),$$

quel que soit $\sigma \in \Gamma_{\mathbf{Q}_p}$, ce qui implique $\mathrm{R}_n(x) = 0$ car $\mathrm{R}_n(x) \in F_n$ n'a qu'un nombre fini de conjugués, et $\chi(\sigma)^k$ prend un nombre infini de valeurs. On en conclut que $x = 0$ puisque $x = \lim_{n\to+\infty} \mathrm{R}_n(x)$.

Corollaire 2.15. — *Soit K une extension finie de $\mathbf{Q}_p$. Si $k \in \mathbf{Z}$, alors $\{x \in \mathbf{C}_p,\ \sigma(x) = \chi(\sigma)^k x,\ \text{quel que soit } \sigma \in \mathrm{G}_K\} = \{0\}$, si $k \neq 0$ et est égal à K, si $k = 0$.*

Démonstration. — Le cas $k = 0$ suit directement du théorème d'Ax-Sen-Tate. Supposons donc dans ce qui suit que $k \neq 0$, et soit $x \in \mathbf{C}_p$ vérifiant $\sigma(x) = \chi(\sigma)^k x$, pour tout $\sigma \in \mathrm{G}_K$. Soit $y = \prod_{h\in S} \chi(h)^{-k} h(x)$, où S est un système de représentants de $\mathrm{G}_{\mathbf{Q}_p}/\mathrm{G}_K$ (y ne dépend pas du choix de S). Si $g \in \mathrm{G}_{\mathbf{Q}_p}$, il existe une permutation $h \mapsto h'$ de S dans S telle que $gh = h'g'$, avec $g' \in \mathrm{G}_K$ et comme χ est un morphisme de groupes, on a $\chi(h)^{-k} = \chi(g)^k \chi(h')^{-k} \chi(g')^{-k}$; on en déduit que

$$g(y) = \prod_{h\in S} \chi(h)^{-k} gh(x) = \prod_{h'\in S} \chi(g)^k \chi(h')^{-k} h'(\chi(g')^{-k} g'(x)) = \chi(g)^{[K:\mathbf{Q}_p]k} y.$$

On en déduit, en utilisant le th. 2.14, que $y = 0$ et donc que $x = 0$, ce qui permet de conclure.

2.2. La construction de $\mathbf{B}_{\mathrm{dR}}$

2.2.1. Généralités sur les p-anneaux

Définition 2.16. — Un anneau R de caractéristique p est *parfait* si l'élévation à la puissance p est un isomorphisme. (Si R est un corps on retombe sur la définition usuelle.) Si R est un anneau parfait de caractéristique p, *un idéal* $\mathfrak{n}$ *de* R *est parfait* s'il est stable par extraction de racines p-ièmes, ce qui équivaut à ce que $R/\mathfrak{n}$ soit parfait.

Définition 2.17. — Soient A un anneau et R un anneau de caractéristique p. On dit que A est *un p-anneau d'anneau résiduel* R s'il existe $\pi \in A$ tel que A soit séparé et complet pour la topologie π-adique et $R = A/\pi A$. Comme R est de caractéristique p, on a en particulier $p \in \pi A$. Un p-anneau est dit *strict* si $\pi = p$ et p n'est pas nilpotent dans A, et *parfait* s'il est strict et R est parfait.

Exemple 2.18. — (i) $\mathbf{Z}_p$ est un p-anneau parfait, car $\mathbf{F}_p$ est un corps parfait.

(ii) Si J est un ensemble quelconque, soit $W_J = \mathbf{Z}_p[X_j^{p^{-\infty}},\ j \in J] = \cup_{m\in\mathbf{N}}\mathbf{Z}_p[X_j^{p^{-m}},\ j \in J]$. On note $\widehat{W}_J$ le séparé complété de W_J pour la topologie p-adique (i.e $\widehat{W}_J = \varprojlim W_J/p^nW_J$), ce qui fait de $\widehat{W}_J$ un p-anneau strict d'anneau résiduel $\overline{W}_J = \mathbf{F}_p[X_j^{p^{-\infty}},\ j \in J]$ qui est parfait (on s'est clairement débrouillé pour).

Remarque 2.19. — Soit R un anneau parfait de caractéristique p. Le morphisme naturel de $\overline{W}_R$ dans R qui à $X_x \in \overline{W}_R$ associe x est surjectif, ce qui permet de voir tout anneau parfait comme un quotient d'un anneau du type $\overline{W}_J$ par un idéal parfait. Ceci permet de ramener beaucoup de questions concernant les anneaux parfaits de caractéristique p au cas des anneaux du type $\overline{W}_J$.

Proposition 2.20. — *Si A est un p-anneau d'anneau résiduel R et si $x \in A$, les deux conditions suivantes sont équivalentes :*

(i) *x est inversible dans A ;*

(ii) *l'image $\overline{x}$ de x modulo π est inversible dans R.*

Démonstration. — Si y est un inverse de x dans A, alors $\overline{y}$ est un inverse de $\overline{x}$ dans R. Réciproquement, si $\overline{y}$ est un inverse de $\overline{x}$ dans R, et si y est n'importe quel relèvement de $\overline{y}$ dans A, alors $z = 1 - xy \in \pi A$ et x admet comme inverse $y(\sum_{n=0}^{+\infty} z^n)$.

Corollaire 2.21. — *Si A est un p-anneau strict dont l'anneau résiduel est un corps, alors $B = A[\frac{1}{p}]$ est un corps.*

Démonstration. — Si $x \in B - \{0\}$, il existe un unique entier $n \in \mathbf{Z}$ tel que $p^n x \in A - pA$ et la proposition précédente montre que $p^n x$ est inversible dans A, ce qui permet de conclure.

2.2.2. Représentants de Teichmüller. — Si A est un anneau, on note $\mathbb{R}(A)$ l'ensemble des suites $x = (x^{(n)})_{n\in\mathbf{N}}$ d'éléments de A telles que l'on ait $(x^{(n+1)})^p = x^{(n)}$ quel que soit $n \in \mathbf{N}$. Dans tout ce qui suit, A est un p-anneau d'anneau résiduel R.

Lemme 2.22. — *Si x, y sont deux éléments de A vérifiant $x-y \in \pi A$, alors $x^{p^n} - y^{p^n} \in \pi^{n+1}A$ quel que soit $n \in \mathbf{N}$.*

Démonstration. — La formule du binôme montre que si $a \in A$ et $u \in \pi^n A$, alors $(a+u)^p - a^p \in \pi^{n+1}A$; on en déduit par récurrence sur n, le fait que si $a \in A$ et $u \in \pi A$, alors $(a+u)^{p^n} - a^{p^n} \in \pi^{n+1}A$, ce qui, appliqué à $a = x$ et $u = y - x$, permet de conclure.

Corollaire 2.23. — *Si $x = (x^{(n)})_{n\in\mathbf{N}} \in \mathbb{R}(R)$ et $\tilde{x}^{(n)}$ est un relèvement de $x^{(n)}$, alors la suite de terme général $(\tilde{x}^{(n+m)})^{p^m}$ converge dans A vers une limite $\psi_A^{(n)}(x)$ qui ne dépend que de x et $\psi_A(x) = (\psi_A^{(n)}(x))_{n\in\mathbf{N}} \in \mathbb{R}(A)$. De plus, on a $\psi_A(xy) = \psi_A(x)\psi_A(y)$.*

Démonstration. — Par construction, $(\tilde{x}^{(n+m+1)})^p - \tilde{x}^{(n+m)} \in \pi A$, et donc $(\tilde{x}^{(n+m+1)})^{p^{m+1}} - (\tilde{x}^{(n+m)})^{p^m} \in \pi^{m+1}A$, ce qui montre que la suite de terme général $(\tilde{x}^{(n+m)})^{p^m}$ converge dans A. Le fait que la limite ne dépende pas du choix des $\tilde{x}^{(n)}$ suit du fait que si on a deux choix, on en fabrique un troisième en panachant et que les trois limites sont égales. On démontre que $(\psi_A^{(n+1)}(x))^p = \psi_A^{(n)}(x)$ par passage à la limite, ce qui prouve que $\psi_A(x) = (\psi_A^{(n)}(x))_{n\in\mathbf{N}} \in \mathbb{R}(A)$. Finalement, la multiplicativité de ψ_A suit de ce que l'on peut prendre $\tilde{x}^{(n)}\tilde{y}^{(n)}$ comme relèvement de $(xy)^{(n)}$ dans A.

Remarque 2.24. — (i) On déduit du corollaire précédent que l'application naturelle $\mathbb{R}(A) \to \mathbb{R}(R)$ est une bijection.

(ii) Si R est parfait, l'application qui à $x = (x^{(n)})_{n\in\mathbf{N}}$ associe $x^{(0)}$ est une bijection de $\mathbb{R}(R)$ sur R et l'application qui à $x \in R$ associe $[x] = \psi_A^{(0)}(x)$, (où x est considéré comme un élément de $\mathbb{R}(R)$) est multiplicative (i.e. $[xy] = [x][y]$ si $x, y \in R$) et l'image de $[x]$ dans $R = A/\pi A$ est x.

Définition 2.25. — L'élément $[x]$ de A est *le représentant de Teichmüller* de x dans A.

2.2.3. L'anneau $\widetilde{\mathbf{E}}^+$. — Rappelons que l'on a défini, si A est un anneau, l'ensemble $\mathbb{R}(A)$ des suites $(x^{(n)})_{n\in\mathbf{N}}$ d'éléments de A telles que l'on ait $(x^{(n+1)})^p = x^{(n)}$ quel que soit $n \in \mathbf{N}$. On a aussi montré que, si A est un p anneau d'anneau résiduel R, alors l'application naturelle de $\mathbb{R}(A)$ dans $\mathbb{R}(R)$, est une bijection, la réciproque étant définie par $x \mapsto \psi_A(x)$, où $\psi_A^{(n)}(x) = \lim_{k\to+\infty}(\hat{x}^{(n+k)})^{p^k}$, et où $\hat{x}^{(n)}$ est un relèvement quelconque de $x^{(n)} \in R$ dans A.

Maintenant, R étant un anneau de caractéristique p, l'application $x \mapsto x^p$ est un morphisme d'anneaux de R dans R, et l'ensemble $\mathbb{R}(R)$ est un sous-anneau de $R^{\mathbf{N}}$. Ceci permet de munir $\mathbb{R}(A)$ d'une structure d'anneau parfait de caractéristique p. La somme et le produit de $x = (x^{(n)})_{n\in\mathbf{N}}$ et $y = (y^{(n)})_{n\in\mathbf{N}}$ étant donnés par les formules

$$(x+y)^{(n)} = \lim_{k\to+\infty}(x^{(n+k)} + y^{(n+k)})^{p^k} \quad \text{et} \quad (xy)^{(n)} = x^{(n)}y^{(n)},$$

la racine p-ième de $x = (x^{(n)})_{n\in\mathbf{N}}$ étant $x^{1/p} = (x^{(n+1)})_{n\in\mathbf{N}}$.

On note $\widetilde{\mathbf{E}}^+$ l'anneau $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$ que l'on peut aussi, d'après ce qui précède, voir comme $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\varpi\mathscr{O}_{\mathbf{C}_p})$, pour n'importe que choix de $\varpi \in \mathscr{O}_{\mathbf{C}_p}$ vérifiant $0 < v_p(\varpi) \leqslant 1$. On remarquera que $\overline{\mathbf{F}}_p$ étant un sous-anneau parfait de $\mathscr{O}_{\mathbf{C}_p}/\varpi\mathscr{O}_{\mathbf{C}_p}$, l'anneau $\widetilde{\mathbf{E}}^+$ contient $\mathbb{R}(\overline{\mathbf{F}}_p)$ qui s'identifie naturellement à $\overline{\mathbf{F}}_p$ par l'application $x = (x^{(n)})_{n\in\mathbf{N}} \mapsto x^{(0)}$.

Si $x = (x^{(n)})_{n\in\mathbf{N}} \in \widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$, on pose $v_{\mathbf{E}}(x) = v_p(x^{(0)})$, ce qui fait que l'on a $v_{\mathbf{E}}(x) = p^n v_p(x^{(n)})$ quel que soit $n \in \mathbf{N}$.

Finalement, si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on fait agir σ sur $\widetilde{\mathbf{E}}^+$, en définissant $\sigma(x)$, si $x = (x^{(n)})_{n\in\mathbf{N}}$ par la formule $\sigma(x) = (\sigma(x^{(n)}))_{n\in\mathbf{N}}$.

Théorème 2.26. — (i) $\widetilde{\mathbf{E}}^+$ *est un anneau de caractéristique p qui est parfait et l'application $v_{\mathbf{E}}$ en est une valuation pour laquelle il est complet.*

(ii) *L'action de $\mathrm{G}_{\mathbf{Q}_p}$ sur $\widetilde{\mathbf{E}}^+$ est continue, respecte sa structure d'anneau, et commute à l'action de d'endomorphisme de Frobenius φ défini par $\varphi(x) = x^p$.*

Démonstration. — (i) On a déjà vu que $\widetilde{\mathbf{E}}^+$ est un anneau parfait de caractéristique p. Si $x = (x^{(n)})_{n\in\mathbf{N}}$ et $(y^{(n)})_{n\in\mathbf{N}}$ sont deux éléments de $\widetilde{\mathbf{E}}^+$, on a

$$v_p((x^{(n)} + y^{(n)})^{p^n}) = p^n v_p(x^{(n)} + y^{(n)}) \geqslant \inf(p^n v_p(x^{(n)}), p^n v_p(y^{(n)})) = \inf(v_{\mathbf{E}}(x), v_{\mathbf{E}}(y)),$$

ce qui, passant à la limite, nous fournit l'inégalité $v_{\mathbf{E}}(x + y) \geqslant \inf(v_{\mathbf{E}}(x), v_{\mathbf{E}}(y))$ et permet de montrer que $v_{\mathbf{E}}$ est une valuation (les autres propriétés à vérifier étant immédiates).

D'autre part, on a $v_{\mathbf{E}}(x-y) \geqslant p^n$ si et seulement si $x^{(0)} = y^{(0)}, \ldots, x^{(n)} = y^{(n)}$ dans $\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$, ce qui montre que la base de voisinages de x pour la topologie induite par $v_{\mathbf{E}}$ constituée des $\{y \mid v_{\mathbf{E}}(x - y) \geqslant p^n\}$ est aussi une base de voisinages de x pour la topologie de $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})$ induite par la topologie produit sur $(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})^{\mathbf{N}}$, chacun des facteurs étant muni de la topologie discrète. On en tire la complétude de $\widetilde{\mathbf{E}}^+$ car un produit d'espaces discrets est complet (une suite de Cauchy étant stationnaire dans chaque composante).

(ii) Le fait que l'action de $\mathrm{G}_{\mathbf{Q}_p}$ respecte la structure d'anneau de $\widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})$ est évident. D'autre part, si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on a $v_{\mathbf{E}}(\sigma(x)) = v_{\mathbf{E}}(x)$ ce qui fait que $\mathrm{G}_{\mathbf{Q}_p}$ agit par des isométries et donc continûment et le fait que cette action commute à φ est une évidence. Reste à vérifier que, si $x = (x^{(n)})_{n\in\mathbf{N}} \in \widetilde{\mathbf{E}}^+$, alors l'application $\sigma \mapsto \sigma(x)$ est continue, mais cela suit de ce que $\mathrm{G}_{\mathbf{Q}_p}$ agit continûment sur $\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p} \cong \mathscr{O}_{\overline{\mathbf{Q}}_p}/p\mathscr{O}_{\overline{\mathbf{Q}}_p}$ muni de la topologie discrète.

Proposition 2.27. — (i) $(\widetilde{\mathbf{E}}^+)^{\varphi=1} = \mathbf{F}_p$.

(ii) *Si K est une extension finie de F, alors $(\widetilde{\mathbf{E}}^+)^{\mathrm{G}_K} = k_K$.*

Démonstration. — (i) $\varphi(x) = x$ si et seulement si $x^p - x = 0$ et donc si et seulement si $x \in \mathbf{F}_p$ puisque $\widetilde{\mathbf{E}}^+$ est intègre (car muni d'une valuation).

(ii) Par définition de l'action de G_K, on a $(\widetilde{\mathbf{E}}^+)^{\mathrm{G}_K} = \mathbb{R}((\mathscr{O}_{\mathbf{C}_p})^{\mathrm{G}_K})$. Par ailleurs, d'après le theórème d'Ax-Sen-Tate, $\mathbb{R}((\mathscr{O}_{\mathbf{C}_p})^{\mathrm{G}_K}) = \mathbb{R}(\mathscr{O}_K)$. Finalement, $\mathscr{O}_K$ étant un p-anneau (pas strict) d'anneau résiduel k_K, on a $\mathbb{R}(\mathscr{O}_K) = \mathbb{R}(k_K)$, et comme k_K est parfait, $\mathbb{R}(k_K) \cong k_K$.

• *Les éléments ε et $\overline{\pi}$.* Soit $\varepsilon = (1, \varepsilon^{(1)}, \dots, \varepsilon^{(n)}, \dots) \in \widetilde{\mathbf{E}}^+$, avec $\varepsilon^{(1)} \neq 1$, ce qui fait que $\varepsilon^{(n)}$ est une racine primitive p^n-ième de l'unité. Soit $\overline{\pi} = \varepsilon - 1$ On a

$$v_{\mathbf{E}}(\overline{\pi}) = \lim_{n \to +\infty} p^n v_p(\varepsilon^{(n)} - 1) = \frac{p}{p-1} > 1 > 0.$$

Proposition 2.28. — *Si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, alors $\sigma(\varepsilon) = \varepsilon^{\chi(\sigma)}$, où χ est le caractère cyclotomique.*

Démonstration. — On a $\binom{x}{n} \in \mathbf{Z}_p$, si $x \in \mathbf{Z}_p$ (en effet, si $x \in \mathbf{N}$, alors $\binom{x}{n} \in \mathbf{N}$ est le nombre de parties à n éléments dans un ensemble à x éléments, et on conclut en utilisant la densité de $\mathbf{N}$ dans $\mathbf{Z}_p$). On en déduit que la série $(1+T)^x = \sum_{n=0}^{+\infty} \binom{x}{n} T^n$ converge dans tout corps complet pour une valuation v, dès que $v(T) > 0$, et définit une fonction continue sur $\mathbf{Z}_p$ comme série uniformément convergente de polynômes. Dans le cas qui nous intéresse, on a $v_p(\varepsilon^{(n)} - 1) > 0$ et $v_{\mathbf{E}}(\varepsilon - 1) > 0$, ce qui donne un sens à $\varepsilon^{\chi(\sigma)}$ et $(\varepsilon^{(n)})^{\chi(\sigma)}$. On a alors, par définition du caractère cyclotomique,

$$\sigma(\varepsilon) = (\sigma(\varepsilon^{(n)}))_{n \in \mathbf{N}} = ((\varepsilon^{(n)})^{\chi(\sigma)})_{n \in \mathbf{N}} = \varepsilon^{\chi(\sigma)}.$$

2.2.4. L'anneau des vecteurs de Witt d'un anneau parfait de caractéristique p. — On a vu que l'on pouvait écrire tout élément de $\mathbf{Z}_p$ de manière unique sous la forme $\sum_{i=0}^{+\infty} p^i \omega_i$, où les ω_i sont des représentants de Teichmüller d'éléments de $\mathbf{F}_p$ (i.e. des racines de l'équation $X^p - X = 0$). On peut se demander s'il est possible de décrire les lois d'addition et multiplication en utilisant cette écriture. C'est le cas et cela va nous mener à introduire les vecteurs de Witt.

Théorème 2.29. — *Si R est un anneau parfait de caractéristique p, il existe un p-anneau strict $W(R)$* (anneau des vecteurs de Witt à coefficients dans R)*, unique à isomorphisme unique près, dont l'anneau résiduel est R.*

De plus, $W(R)$ vérifie la propriété universelle suivante. Si A est un p-anneau d'anneau résiduel R', si $\overline{\theta} : R \to R'$ un morphisme d'anneaux, et si $\tilde{\theta} : R \to A$ est une application multiplicative relevant $\overline{\theta}$, il existe un unique morphisme d'anneau $\theta : W(R) \to A$ tel que si $x \in R$, alors $\theta([x]) = \tilde{\theta}(x)$.

Proposition 2.30. — *Si A est un p-anneau parfait d'anneau résiduel R, alors tout élément de A s'écrit de manière unique sous la forme $\sum_{i=0}^{+\infty} p^i [x_i]$, où les x_i sont des éléments de R.*

Démonstration. — C'est vrai pour tout système de représentants de R dans A (lemme 4.2).

Lemme 2.31. — *Soit J un ensemble d'indices. Si A est un p-anneau d'anneau résiduel R, si $\overline{\theta} : \overline{W}_J \to R$ un morphisme d'anneaux, et si $\tilde{\theta} : \overline{W}_J \to A$ est une application multiplicative relevant $\overline{\theta}$, il existe un unique morphisme d'anneau $\theta : \widehat{W}_J \to A$ tel que si $x \in \overline{W}_J$, alors $\theta([x]) = \tilde{\theta}(x)$.*

Démonstration. — L'unicité est claire : on doit avoir $\theta(\sum_{i=0}^{+\infty} p^i [x_i]) = \sum_{i=0}^{+\infty} p^i \tilde{\theta}(x_i)$. Montrons l'existence. Soit $f : W_J \to A$ le morphisme d'anneaux défini par $f(X_j^{p^{-m}}) = \tilde{\theta}(X_j^{p^{-m}})$ si $j \in J$ et $m \in \mathbf{N}$. On prolonge f par continuité en un morphisme $\hat{f} : \widehat{W}_J \to A$ et pour conclure, il suffit de prouver que si $x \in \overline{W}_J$, alors $\hat{f}([x]) = \tilde{\theta}(x)$. Le morphisme $\overline{f} : \overline{W}_J \to R$ induit par $\hat{f}$ coïncide par construction avec $\overline{\theta}$ sur $X_j^{p^{-m}}$ si $j \in J$ et $m \in \mathbf{N}$ et comme ces éléments engendrent $\overline{W}_J$,

on en déduit l'égalité de $\overline{f}$ et $\overline{\theta}$. Ceci implique en particulier que si $x \in \overline{W}_J$ et $n \in \mathbf{N}$, alors $\hat{f}([x^{p^{-n}}]) - \tilde{\theta}(x^{p^{-n}}) \in \pi A$ et donc, d'après le lemme 2.22, que $\hat{f}([x]) - \tilde{\theta}(x) \in \pi^{n+1}A$ quel que soit $n \in \mathbf{N}$, et permet de conclure.

Soit $\mathbf{N} \amalg \mathbf{N}$ la réunion disjointe de deux copies de $\mathbf{N}$. Pour alléger un peu les notations, notons X_i et Y_i au lieu de $X_{1,i}$ et $X_{2,i}$ les variables de $W_{\mathbf{N}\amalg\mathbf{N}}$ Un élément $P(X,Y)$ de $\overline{W}_{\mathbf{N}\amalg\mathbf{N}}$ peut s'écrire de manière unique sous la forme

$$P(X,Y) = \sum_{\mathbf{r},\mathbf{s}} a_{\mathbf{r},\mathbf{s}} \Big(\prod_{i=0}^{+\infty} X_i^{r_i}\Big)\Big(\prod_{j=0}^{+\infty} Y_j^{s_j}\Big),$$

la somme portant sur les couples $(\mathbf{r},\mathbf{s})$ de familles d'éléments de $\mathbf{Z}[\frac{1}{p}]$ n'ayant qu'un nombre fini de termes non nuls et les $a_{\mathbf{r},\mathbf{s}}$ étant des éléments de $\mathbf{F}_p$ presque tous nuls.

Soient $(S_i(X,Y))_{i\in\mathbf{N}}$ et $(P_i(X,Y))_{i\in\mathbf{N}}$ les suites d'éléments de $\overline{W}_{\mathbf{N}\amalg\mathbf{N}}$ définie par

$$\sum_{i=0}^{+\infty} p^i[X_i] + \sum_{i=0}^{+\infty} p^i[Y_i] = \sum_{i=0}^{+\infty} p^i[S_i(X,Y)] \quad \text{et} \quad \Big(\sum_{i=0}^{+\infty} p^i[X_i]\Big)\Big(\sum_{i=0}^{+\infty} p^i[Y_i]\Big) = \sum_{i=0}^{+\infty} p^i[P_i(X,Y)].$$

Les polynômes S_i et P_i sont des polynômes universels permettant de décrire les lois d'addition et multiplication dans un p-anneau parfait si on écrit les éléments sous la forme $\sum_{i=0}^{+\infty} p^i[x_i]$, où les x_i sont des éléments de l'anneau résiduel. De manière précise, on a la proposition suivante.

Proposition 2.32. — *Si A est un p-anneau parfait d'anneau résiduel R, et si $x = (x_i)_{i\in\mathbf{N}}$ est une suite d'éléments de R, on note $\Sigma(x)$ l'élément $\sum_{i=0}^{+\infty} p^i[x_i]$ de A.*

Si $x = (x_i)_{i\in\mathbf{N}}$ et $y = (y_i)_{i\in\mathbf{N}}$ sont deux suites d'éléments de R, alors

$$\Sigma(x) + \Sigma(y) = \sum_{i=1}^{+\infty} p^i[S_i(x,y)] \quad \text{et} \quad \Sigma(x)\Sigma(y) = \sum_{i=1}^{+\infty} p^i[P_i(x,y)].$$

Démonstration. — Soit $\overline{\theta} : \overline{W}_{\mathbf{N}\amalg\mathbf{N}} \to R$ le morphisme défini par $\overline{\theta}(X_i) = x_i$ et $\overline{\theta}(Y_i) = y_i$ si $i \in \mathbf{N}$. Soit $\tilde{\theta} : \overline{W}_{\mathbf{N}\amalg\mathbf{N}} \to A$ l'application multiplicative définie par $\tilde{\theta}(x) = [\overline{\theta}(x)]$. D'après le lemme 2.31, il existe un unique morphisme $\theta : \widehat{W}_{\mathbf{N}\amalg\mathbf{N}} \to A$ tel que l'on ait $\theta([z]) = [\overline{\theta}(z)]$ quel que soit $z \in \overline{W}_{\mathbf{N}\amalg\mathbf{N}}$. Soient alors $X = (X_i)_i$ et $Y = (Y_i)_{i\in I}$ les deux suites naturelles d'éléments de $W_{\mathbf{N}\amalg\mathbf{N}}$. On a par construction $\Sigma(x) = \theta(\Sigma(X))$ et $\Sigma(y) = \theta(\Sigma(Y))$, ce qui nous donne les formules

$$\begin{aligned}\Sigma(x) + \Sigma(y) =& \theta(\Sigma(X)) + \theta(\Sigma(Y)) = \theta(\Sigma(X) + \Sigma(Y)) \\ =& \theta(\sum_{i=0}^{+\infty} p^i[S_i(X,Y)]) = \sum_{i=0}^{+\infty} p^i[\overline{\theta}(S_i(X,Y))] = \sum_{i=0}^{+\infty} p^i[S_i(x,y)],\end{aligned}$$

ce qui donne le résultat pour la somme ; le produit se traitant exactement de la même manière, cela permet de conclure.

Remarque 2.33. — (i) La proposition 2.30 décrit un anneau parfait d'anneau résiduel R de manière ensembliste, en fonction de R, et la prop. 2.32 montre qu'il existe au plus une structure

de p-anneau strict sur cet ensemble, qui fasse de R l'anneau résiduel. On en déduit l'unicité de $W(R)$.

(ii) Du fait de la distributivité de la multiplication par rapport à l'addition et de la continuité de l'addition, pour être capable de multiplier, additionner ou soustraire deux éléments de la forme $\Sigma(x)$ et $\Sigma(y)$, il suffit d'avoir une formule pour $[X]-[Y]$.

(iii) Comme $\Sigma(0)=0$, on a $\Sigma(x)+\Sigma(y)=0$, si $x=0$ et $y=0$; cela implique que les S_i, $i\in\mathbf{N}$, n'ont pas de terme constant. De même, $\Sigma(x)\Sigma(y)=0$ si $x=0$ ou $y=0$, cela implique que les P_i n'ont pas de termes de degré 0 en les X_j ou en les Y_j.

Lemme 2.34. — *Soit A un p-anneau strict d'anneau résiduel R parfait et $\mathfrak{n}$ un idéal parfait de R distinct de R, l'ensemble $W(\mathfrak{n})=\{\sum_{i=0}^{+\infty}p^i[x_i]\mid x_i\in\mathfrak{n}$ quel que soit $i\in\mathbf{N}\}$ est un idéal fermé de A et $A/W(\mathfrak{n})$ est un p-anneau parfait d'anneau résiduel $R/\mathfrak{n}$.*

Démonstration. — On déduit de la prop 2.32 que $W(\mathfrak{n})$ est un sous-groupe additif de A, et qu'il est stable par multiplication par un élément de A car $v_X(P_i)=v_Y(P_i)>0$ (rem. 2.33). Par ailleurs, $W(\mathfrak{n})$ est fermé par construction, et l'anneau résiduel de $A/W(\mathfrak{n})$ est $A/W(\mathfrak{n})+pA=R/\mathfrak{n}$, ce qui termine la démonstration.

Revenons à la démonstration du théorème 2.29. L'unicité a déjà été démontrée au (i) de la rem. 2.33. Si R est parfait de caractéristique p, on peut l'écrire (de manière non unique) comme un quotient d'un $\overline{W}_J$ par un idéal parfait $\mathfrak{n}$. Le lemme précédent montre que $W(R)=\widehat{W}_J/W(\mathfrak{n})$ est un p-anneau parfait d'anneau résiduel R.

Il reste à prouver que $W(R)$ satisfait la propriété universelle demandée, mais cela se déduit du lemme 2.31 en composant tout avec la projection de $\overline{W}_J$ sur R et en remarquant que le morphisme de $\widehat{W}_J$ dans A que l'on obtient se factorise à travers $W(R)$.

Exemple 2.35. — (i) $W(\mathbf{F}_p)=\mathbf{Z}_p$.

(ii) Plus généralement, si K est un corps local de caractéristique 0 dont le corps résiduel k_K est parfait de caractéristique p, et dont p est une uniformisante, alors $K\cong W(k_K)[\frac{1}{p}]$.

Démonstration. — l'anneau des entiers de K est un p-anneau parfait d'anneau résiduel k_K, donc isomorphe à $W(k_K)$.

Exercice 1. — On définit par récurrence sur n, une suite $(U_n)_{u\in\mathbf{N}}$ d'éléments de $\mathbf{Z}[\frac{1}{p}][X,Y]$, en posant

$$U_n(X,Y)=\frac{1}{p^n}\Big(X^{p^n}+Y^{p^n}-\Big(\sum_{i=0}^{n-1}p^iU_i(X,Y)^{p^{n-i}}\Big)\Big).$$

(i) Calculer U_0 et U_1 et vérifier que $U_0,U_1\in\mathbf{Z}[X,Y]$.

(ii) On se place dans l'anneau $S_{X,Y}=\mathbf{Z}[\widehat{X^{p^{-\infty}},Y^{p^{-\infty}}}]$ et on écrit $X+Y$ sous la forme

$$X+Y=\sum_{i=0}^{+\infty}p^i[V_i(X,Y)],\quad\text{avec } V_i\in\mathbf{F}_p[X^{p^{-\infty}},Y^{p^{-\infty}}].$$

(a) Montrer que $X^{p^n}+Y^{p^n}=\sum_{i=0}^{+\infty}p^i[V_i(X,Y)^{p^n}]$.

(b) On suppose que, quel que soit $i \leqslant n-1$, $U_i \in \mathbf{Z}[X,Y]$ et que l'image $\overline{U}_i$ de U_i dans $\mathbf{F}_p[X,Y]$ vérifie $\overline{U}_i = V_i^{p^i}$. Montrer que

$$\sum_{i=0}^{n-1} p^i U_i(X,Y)^{p^{n-i}} \equiv \sum_{i=0}^{n-1} p^i [V_i(X,Y)^{p^n}] \mod p^{n+1}.$$

En déduire que $U_n \in \mathbf{Z}[X,Y]$ et que $\overline{U}_n = V_n^{p^n}$.
(iii) Montrer que V_n est un polynôme en $X^{p^{-n}}$ et $Y^{p^{-n}}$, puis que S_n et P_n, donnant l'addition et la multiplication des vecteurs de Witt, sont des polynômes en les $X_j^{p^{j-n}}, Y_j^{p^{j-n}}$, avec $j \leqslant n$.

Proposition 2.36. — *Si R et R' sont deux anneaux parfaits de caractéristique p, l'application naturelle de* $\mathrm{Hom}(W(R), W(R'))$ *dans* $\mathrm{Hom}(R, R')$ *est une bijection.*

En particulier, le morphisme de Frobenius $x \to x^p$ sur R se relève en un automorphisme φ (de Frobenius) de $W(R)$.

Démonstration. — Si $\overline{\theta}$ est un morphisme de R dans R', on pose $\tilde{\theta}(x) = [\overline{\theta}(x)]$ et $\tilde{\theta}$ est une application multiplicative de R dans $W(R')$ relevant $\overline{\theta}$; on en déduit, utilisant la seconde partie du théorème, la surjectivité de l'application naturelle de $\mathrm{Hom}(W(R), W(R'))$ dans $\mathrm{Hom}(R, R')$.

Si θ est un morphisme de $W(R)$ dans $W(R')$, on a $\theta([x]) = \lim_{n\to+\infty} = \theta([x^{p^{-n}}])^{p^n} = [\overline{\theta}(x)]$ d'après le corollaire 2.23 (et la remarque 2.24), puisque $\theta([x^{p^{-n}}])$ est un relèvement dans $W(R')$ de $\overline{\theta}(x^{p^{-n}}) = (\overline{\theta}(x))^{p^{-n}}$, et l'injectivité suit de ce que $W(R)$ étant un p-anneau strict, la connaissance de $\theta([x])$ pour tout $x \in R$ est équivalente à la connaissance de θ d'après la proposition 2.30.

Exercice 2. — Soit k un corps algébriquement clos de caractéristique p.
(i) Montrer que $\varphi - 1 : W(k) \to W(k)$ est surjectif. Quel est son noyau ?
(ii) Montrer que, si $u \in W(k)^*$, alors il existe $x \in W(k)^*$ tel que $\frac{\varphi(x)}{x} = u$.

2.2.5. L'anneau $\widetilde{\mathbf{A}}^+$. — On note $\widetilde{\mathbf{A}}^+$ l'anneau des vecteurs de Witt $W(\widetilde{\mathbf{E}}^+)$ à coefficients dans l'anneau parfait $\widetilde{\mathbf{E}}^+$. Tout élément de $\widetilde{\mathbf{A}}^+$ peut s'écrire de manière unique sous la forme $x = \sum_{n=0}^{+\infty} p^n[x_n]$, où $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\widetilde{\mathbf{E}}^+$. D'après les résultats généraux sur les vecteurs de Witt, les actions de $\mathrm{G}_{\mathbf{Q}_p}$ et φ sur $\widetilde{\mathbf{E}}^+$ se relèvent de manière unique en des actions de $\mathrm{G}_{\mathbf{Q}_p}$ et φ sur $\widetilde{\mathbf{A}}^+$. De manière explicite, on a

$$\varphi\big(\sum_{n=0}^{+\infty} p^n[x_n]\big) = \sum_{n=0}^{+\infty} p^n[x_n^p] \quad \text{et} \quad \sigma\big(\sum_{n=0}^{+\infty} p^n[x_n]\big) = \sum_{n=0}^{+\infty} p^n[\sigma(x_n)], \text{ si } \sigma \in \mathrm{G}_{\mathbf{Q}_p}.$$

On a $\widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}) = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$. On note $\overline{\theta} : \widetilde{\mathbf{E}}^+ \to \mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$ l'application qui, à $x = (x_n)_{n\in\mathbf{N}} \in \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})$ associe $x_0 \in \mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$. Ceci fait de $\overline{\theta}$ un morphisme d'anneaux de $\widetilde{\mathbf{E}}^+$ dans $\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$ qui, de manière évidente, est surjectif et commute à l'action de $\mathrm{G}_{\mathbf{Q}_p}$.

On note $\tilde{\theta} : \widetilde{\mathbf{E}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ l'application qui, à $x = (x^{(n)})_{n\in\mathbf{N}} \in \mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$ associe $x^{(0)} \in \mathscr{O}_{\mathbf{C}_p}$. Ceci fait de $\tilde{\theta}$ une application multiplicative de $\widetilde{\mathbf{E}}^+$ dans $\mathscr{O}_{\mathbf{C}_p}$, dont la réduction modulo p est $\overline{\theta}$. Il résulte de la propriété universelle des vecteurs de Witt, que l'application $\theta : \widetilde{\mathbf{A}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ définie

par

$$\theta\big(\sum_{n=0}^{+\infty} p^n[x_n]\big) = \sum_{n=0}^{+\infty} p^n x_n^{(0)},$$

est un morphisme d'anneaux.

Il y a deux topologies naturelles que l'on peut mettre sur $\widetilde{\mathbf{A}}^+$. La *topologie forte*, qui n'est autre que la topologie p-adique, fait de l'application $\sum_{n=0}^{+\infty} p^n[x_n] \mapsto (x_n)_{n\in\mathbf{N}}$ un homéomorphisme de $\widetilde{\mathbf{A}}^+$ sur $(\widetilde{\mathbf{E}}^+)^{\mathbf{N}}$, où l'on a muni $\widetilde{\mathbf{E}}^+$ de la topologie discrète. La topologie naturelle sur $\widetilde{\mathbf{A}}^+$ est celle qui fait de $\sum_{n=0}^{+\infty} p^n[x_n] \mapsto (x_n)_{n\in\mathbf{N}}$ un homéomorphisme de $\widetilde{\mathbf{A}}^+$ sur $(\widetilde{\mathbf{E}}^+)^{\mathbf{N}}$, où l'on a muni $\widetilde{\mathbf{E}}^+$ de la topologie définie par $v_{\mathbf{E}}$. Cette topologie, la *topologie faible*, est plus faible que la topologie p-adique, mais $\widetilde{\mathbf{A}}^+$ est encore complet pour cette topologie puisque $\widetilde{\mathbf{E}}^+$ est complet pour $v_{\mathbf{E}}$.

Comme $\mathrm{G}_{\mathbf{Q}_p}$ agit continûment sur $\widetilde{\mathbf{E}}^+$ pour la topologie définie par $v_{\mathbf{E}}$, il agit aussi continûment sur $\widetilde{\mathbf{A}}^+$ muni de la topologie faible. Par contre, $\mathrm{G}_{\mathbf{Q}_p}$ n'agit pas continûment sur $\widetilde{\mathbf{A}}^+$ pour la topologie forte.

Proposition 2.37. — (i) *Le morphisme $\theta : \widetilde{\mathbf{A}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ est surjectif, et commute avec l'action de $\mathrm{G}_{\mathbf{Q}_p}$.*

(ii) *Le noyau de θ est principal, et un élément $x = \sum_{n=0}^{+\infty} p^n[x_n]$ en est un générateur, si et seulement si $v_{\mathbf{E}}(x_0) = 1$.*

Démonstration. — Le (i) est plus ou moins immédiat ; montrons le (ii). Si $x = \sum_{n=0}^{+\infty} p^n[x_n] \in \widetilde{\mathbf{A}}^+$, on note $\overline{x} = x_0$ son image dans $\widetilde{\mathbf{E}}^+$. Si $x \in \ker\theta$, on a $x_0^{(0)} = -\sum_{n=1}^{+\infty} p^n x_n^{(0)}$, ce qui implique $v_{\mathbf{E}}(\overline{x}) = v_p(x_0^{(0)}) \geqslant 1$. Soit alors $x = \sum_{n=0}^{+\infty} p^n[x_n]$ vérifiant $v_{\mathbf{E}}(\overline{x}) = 1$, et soit $y \in \ker\theta$. D'après ce qui précède, on a $v_{\mathbf{E}}(\overline{y}) \geqslant 1$; il existe donc $a_0 \in \widetilde{\mathbf{E}}^+$ tel que $\overline{y} = a_0\overline{x}$. On peut alors écrire y sous la forme $y = [a_0]x + py_1$, avec $y_1 \in \widetilde{\mathbf{A}}^+$. De plus, $p\theta(y_1) = \theta(y) - \theta([a_0])\theta(x) = 0$, ce qui prouve que $y \in \ker\theta$. On peut donc refaire avec y_1 ce que l'on a fait avec y, ce qui permet de construire, par récurrence, une suite $(a_n)_{n\in\mathbf{N}}$ d'éléments de $\widetilde{\mathbf{A}}^+$, telle que l'on ait, pour tout $n \in \mathbf{N}$, $y = ([a_0] + \cdots + p^n[a_n])x + p^{n+1}y_{n+1}$, avec $y_{n+1} \in \ker\theta$. On a donc $y = \big(\sum_{n=0}^{+\infty} p^n[a_n]\big)x$, ce qui montre que x est un générateur de $\ker\theta$, et permet de conclure.

Exemple 2.38. — (i) Si $\tilde{p} = (p, p^{1/p}, \dots) \in \widetilde{\mathbf{E}}^+$, alors $[\tilde{p}] - p$ est un générateur de $\ker\theta$.

(ii) Si on pose $\omega = \frac{[\varepsilon]-1}{[\varepsilon^{1/p}]-1} = 1 + [\varepsilon^{1/p}] + \cdots + [\varepsilon^{1/p}]^{p-1}$, on a $\theta(\omega) = 0$ puisque $\theta([\varepsilon]) = 1$ et $\theta([\varepsilon^{1/p}]) = \varepsilon^{(1)} \neq 1$. Par ailleurs, l'image $\overline{\omega}$ de ω dans $\widetilde{\mathbf{E}}^+$ est $\frac{\varepsilon-1}{\varepsilon^{1/p}-1} = (\varepsilon-1)^{1-1/p}$, et on a donc $v_{\mathbf{E}}(\overline{\omega}) = (1-1/p)v_{\mathbf{E}}(\varepsilon-1) = 1$. Ceci montre que ω est un générateur de $\ker\theta$.

Exercice 3. — Soit F une extension non ramifiée de $\mathbf{Q}_p$. Soit K une extension totalement ramifiée de F de degré $e > 1$, soit π_K une uniformisante de K, soit $P \in \mathscr{O}_F[X]$ le polynôme minimal de π_K sur F, et soit $\tilde{\pi}_K \in \widetilde{\mathbf{A}}^+$ vérifiant $\theta(\tilde{\pi}_K) = \pi_K$. Montrer que $P(\tilde{\pi}_K)$ est un générateur de $\ker\theta$.

Proposition 2.39. — *La topologie faible sur $\widetilde{\mathbf{A}}^+$ est aussi la topologie $(p, \ker\theta)$-adique.*

Démonstration. — On a $[x+y]-[x]=\sum_{i=0}^{+\infty}p^i[R_i(x,y)]$, avec $R_i(x,y)=S_i((x+y,0,\dots),(-x,0,\dots))$. Comme $R_i(x,0)=0$, il existe n_i tel que $v_{\mathbf{E}}(R_i(x,y))\geqslant p^{-n_i}v_{\mathbf{E}}(y)$. On en déduit que, si $v_{\mathbf{E}}(y)\geqslant k\sup_{i\leqslant k-1}p^{n_i}$, alors $[x+y]-[x]\in p^k\widetilde{\mathbf{A}}^+ + [\tilde{p}]^k\widetilde{\mathbf{A}}^+\subset(p,\ker\theta)^k$, ce qui permet de montrer la continuité de l'identité de $\widetilde{\mathbf{A}}^+$ muni de la topologie faible dans $\widetilde{\mathbf{A}}^+$ muni de la topologie $(p,\ker\theta)$-adique.

Réciproquement, si $\sum_{i=0}^{+\infty}p^i[x_i]-\sum_{i=0}^{+\infty}p^i[y_i]\in(p,\ker\theta)^k$, alors en particulier, $v_{\mathbf{E}}(x_0-y_0)\geqslant k$. En utilisant ce qui précède, on en déduit l'existence de $a_1:\mathbf{N}\to\mathbf{N}$ tendant vers $+\infty$ en $+\infty$ tel que $[x_0]-[y_0]\in(p,\ker\theta)^{a_1(k)+1}$, et donc $\sum_{i=1}^{+\infty}p^{i-1}[x_i]-\sum_{i=0}^{+\infty}p^{i-1}[y_i]\in(p,\ker\theta)^{a_1(k)}$. Par récurrence, cela perme de construire une suite d'applications $a_i:\mathbf{N}\to\mathbf{N}$ tendant vers $+\infty$ en $+\infty$ telles que $v_{\mathbf{E}}(x_i-y_i)\geqslant a_i(k)$. On en déduit la continuité de l'identité de $\widetilde{\mathbf{A}}^+$ muni de la topologie $(p,\ker\theta)$-adique dans $\widetilde{\mathbf{A}}^+$ muni de la topologie faible.

Ceci permet de conclure.

2.2.6. L'anneau $\mathbf{B}_{\mathrm{dR}}$. — On étend θ par $\mathbf{Q}_p$-linéarité en un morphisme d'anneaux de $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$ dans $\mathbf{C}_p$. Le noyau de θ est encore principal engendré par ω, et on note $\mathbf{B}_{\mathrm{dR}}^+$ le séparé complété de $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$ pour la topologie ω-adique. On note v_H la valuation définie par ω sur $\mathbf{B}_{\mathrm{dR}}^+$. Par construction, cette valuation est discrète et $\mathbf{B}_{\mathrm{dR}}^+$ est complet ; le corps résiduel est le même que celui de $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$; c'est donc $\mathbf{C}_p$. Comme $\ker\theta$ est stable par $\mathrm{G}_{\mathbf{Q}_p}$ l'action de $\mathrm{G}_{\mathbf{Q}_p}$ sur $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$ s'étend par continuité à $\mathbf{B}_{\mathrm{dR}}^+$; par contre, celle de φ ne s'étend pas car $\ker\theta$ n'est pas stable par φ.

La topologie naturelle sur $\mathbf{B}_{\mathrm{dR}}^+$ n'est pas la topologie définie par v_H ; celle-ci est beaucoup trop forte pour que $\mathrm{G}_{\mathbf{Q}_p}$ agisse continûment sur $\mathbf{B}_{\mathrm{dR}}^+$ (chaque $g\in\mathrm{G}_{\mathbf{Q}_p}$ agit continûment sur $\mathbf{B}_{\mathrm{dR}}^+$, mais on peut trouver des $x\in\mathbf{B}_{\mathrm{dR}}^+$ tels que $g\mapsto g(x)$ ne soit pas continue sur $\mathrm{G}_{\mathbf{Q}_p}$). La topologie naturelle sur $\mathbf{B}_{\mathrm{dR}}^+$ est celle pour laquelle les $p^k\widetilde{\mathbf{A}}^+ + \omega^n\mathbf{B}_{\mathrm{dR}}^+$, avec $k,n\in\mathbf{N}$, forment une base de voisinage de 0. Elle est (beaucoup) plus faible que la topologie induite par v_H et $\mathrm{G}_{\mathbf{Q}_p}$ agit continûment sur $\mathbf{B}_{\mathrm{dR}}^+$ muni de la topologie naturelle.

Remarque 2.40. — (i) Comme $\mathbf{B}_{\mathrm{dR}}^+$ est un anneau complet pour la valuation discrète v_H, que t en est une uniformisante, et que le corps résiduel est $\mathbf{C}_p$, il est abstraitement isomorphe à $\mathbf{C}_p[[t]]$, mais ce résultat n'est d'aucune utilité car on peut montrer (ce n'est pas du tout trivial) qu'il n'existe aucun isomorphisme de ce type qui soit compatible à l'action de $\mathrm{G}_{\mathbf{Q}_p}$ ou qui soit continue.

(ii) La topologie naturelle sur $\widetilde{\mathbf{A}}^+$ ou $\mathbf{B}_{\mathrm{dR}}^+$ a l'air un peu compliquée, mais on peut très souvent raisonner comme si on travaillait dans $\mathscr{O}_{\mathbf{C}_p}[[T]]$ ou $\mathbf{C}_p[[T]]$ de la manière suivante. On choisit une section $\mathbf{Z}_p$-linéaire $s:\mathscr{O}_{\mathbf{C}_p}\to\widetilde{\mathbf{A}}^+$ de θ (i.e. $s(ax+by)=as(x)+bs(y)$ si $a,b,\in\mathbf{Z}_p$ et $x,y\in\mathscr{O}_{\mathbf{C}_p}$), que l'on étend par $\mathbf{Q}_p$-linéarité en $s:\mathbf{C}_p\to\widetilde{\mathbf{A}}^+[\frac{1}{p}]\subset\mathbf{B}_{\mathrm{dR}}^+$, et on choisit un générateur ξ de $\ker\theta$ dans $\widetilde{\mathbf{A}}^+$. Alors tout élément de $\widetilde{\mathbf{A}}^+$ (resp. de $\mathbf{B}_{\mathrm{dR}}^+$) peut s'écrire de manière unique (exercice) sous la forme $\sum_{n=0}^{+\infty}s(a_n)\xi^n$ avec $(a_n)_{n\in\mathbf{N}}\in(\mathscr{O}_{\mathbf{C}_p})^{\mathbf{N}}$ (resp. $(a_n)_{n\in\mathbf{N}}\in(\mathbf{C}_p)^{\mathbf{N}}$), et la topologie naturelle sur $\widetilde{\mathbf{A}}^+$ (resp. $\mathbf{B}_{\mathrm{dR}}^+$) correspond à la topologie produit sur $(\mathscr{O}_{\mathbf{C}_p})^{\mathbf{N}}$ (resp. $(\mathbf{C}_p)^{\mathbf{N}}$). Comme s n'est pas multiplicative, il faut faire un peu plus attention que d'habitude, mais on est en général sauvé par le fait $s(ab)-s(a)s(b)\in p^{n+m}\xi\widetilde{\mathbf{A}}^+$ si $a\in p^n\mathscr{O}_{\mathbf{C}_p}$ et $b\in p^m\mathscr{O}_{\mathbf{C}_p}$.

Exercice 4. — (i) Montrer que, si $x \in \widetilde{\mathbf{E}}^+$, et si $v_{\mathbf{E}}(x-1) > 0$, alors la série $\log[x] = -\sum_{n=1}^{+\infty} \frac{(1-[x])^n}{n}$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$.

(ii) Plus généralement, montrer que, si $(a_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{Q}_p$, et si $x \in \mathbf{B}_{\mathrm{dR}}^+$ est tel que la série $\sum_{n=0}^{+\infty} a_n \theta(x)^n$ converge dans $\mathbf{C}_p$, alors $\sum_{n=0}^{+\infty} a_n x^n$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$.

Comme il est dit dans la remarque précédente, $\mathbf{B}_{\mathrm{dR}}^+$ ne contient pas $\mathbf{C}_p$ de manière naturelle, par contre, il contient $\overline{\mathbf{Q}}_p$. En effet :

Proposition 2.41. — *Si M désigne la clôture intégrale de $\mathbf{Q}_p$ dans $\mathbf{B}_{\mathrm{dR}}^+$, alors θ induit un isomorphisme de M sur $\overline{\mathbf{Q}}_p$.*

Démonstration. — Soit $x \in \overline{\mathbf{Q}}_p$, et soit $P \in \mathbf{Q}_p[X]$ le polynôme minimal de x sur $\mathbf{Q}_p$. Comme x est racine simple de P, le lemme de Hensel montre que l'équation $P(X) = 0$ a une unique solution dans $\mathbf{B}_{\mathrm{dR}}^+$ vérifiant $\theta(X) = x$. On en déduit que θ induit un isomorphisme de la clôture séparable de $\mathbf{Q}_p$ dans $\mathbf{B}_{\mathrm{dR}}^+$ sur $\overline{\mathbf{Q}}_p$, et comme $\mathbf{B}_{\mathrm{dR}}^+$ est intègre et de caractéristique 0, cette clôture séparable n'est autre que M, ce qui permet de conclure.

Comme $[\varepsilon] - 1 \in \ker\theta$, la série $\log[\varepsilon] = -\sum_{n=1}^{+\infty} \frac{(1-[\varepsilon])^n}{n}$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$. On note t la somme. Si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on a

$$\sigma(t) = \sigma(\log[\varepsilon]) = \log[\sigma(\varepsilon)] = \log[\varepsilon^{\chi(\sigma)}] = \log[\varepsilon]^{\chi(\sigma)} = \chi(\sigma)\log[\varepsilon] = \chi(\sigma)t.$$

Ceci fait de t un analogue p-adique de $2i\pi$ (c'est le « $2i\pi$ de Fontaine »). On a $\theta(t) = 0$, ce qui explique que l'on ne le voit pas dans $\mathbf{C}_p$.

Proposition 2.42. — *t est une uniformisante de $\mathbf{B}_{\mathrm{dR}}^+$.*

Démonstration. — On a $\theta(\omega^{-1}t) = \theta\Big(([\varepsilon^{1/p}] - 1)\sum_{n=1}^{+\infty} \frac{(1-[\varepsilon])^{n-1}}{n}\Big) = \varepsilon^{(1)} - 1 \neq 0$, et comme ω est une uniformisante de $\mathbf{B}_{\mathrm{dR}}^+$ (puisque c'est un générateur de $\ker\theta$), cela permet de conclure.

En particulier, cela montre que l'action de $\mathrm{G}_{\mathbf{Q}_p}$ se prolonge au corps des fractions $\mathbf{B}_{\mathrm{dR}} = \mathbf{B}_{\mathrm{dR}}^+[\frac{1}{t}]$ de $\mathbf{B}_{\mathrm{dR}}^+$ et que cette action respecte la valuation v_H (prolongée à $\mathbf{B}_{\mathrm{dR}}$).

Proposition 2.43. — *Si K est une extension finie de $\mathbf{Q}_p$, alors $(\mathbf{B}_{\mathrm{dR}})^{\mathrm{G}_K} = K$.*

Démonstration. — Soit $x \in \mathbf{B}_{\mathrm{dR}} - \{0\}$ fixe par G_K, et soit $k = v_H(x)$, de telle sorte que $\theta(t^{-k}x) \neq 0$. On a alors, pour tout $g \in \mathrm{G}_{\mathbf{Q}_p}$,

$$g(\theta(t^{-k}x)) = \theta(\chi(g)^{-k}t^{-k}x) = \chi(g)^{-k}\theta(t^{-k}x),$$

et on déduit du théorème de Tate (cor. 2.15), que $k = 0$ et $\theta(x) \in K$. Mais alors $x - \theta(x)$ est fixe par G_K et vérifie $v_H(x - \theta(x)) \geqslant 1$, ce qui prouve, d'après ce qui précède, que $x = \theta(x)$, et donc que $x \in K$, ce qu'il fallait démontrer.

2.2.7. Représentations de de Rham

Proposition 2.44. — *Si K est une extension finie de $\mathbf{Q}_p$, et si V est une $\mathbf{Q}_p$-représentation de G_K de dimension finie, alors*

$$\dim_K(\mathrm{Hom}_{\mathrm{G}_K}(V,\mathbf{B}_{\mathrm{dR}}))\leqslant\dim_{\mathbf{Q}_p}V.$$

Démonstration. — La notation $\mathrm{Hom}_{\mathrm{G}_K}(V,\mathbf{B}_{\mathrm{dR}})$ désigne l'espace des applications $\mathbf{Q}_p$-linéaires $\lambda:V\to\mathbf{B}_{\mathrm{dR}}$ commutant à l'action de G_K (i.e. $\lambda(g(v))=g(\lambda(v))$, pour tous $v\in V$ et $g\in G$). On introduit la représentation duale $V^*=\mathrm{Hom}(V,\mathrm{G}_K)$ de V (munie de l'action $g\cdot\lambda(v)=\lambda(g^{-1}v)$), et alors $\mathrm{Hom}(V,\mathbf{B}_{\mathrm{dR}})=\mathbf{B}_{\mathrm{dR}}\otimes_{\mathbf{Q}_p}V^*$ est muni de l'action tensorielle de G_K (i.e. $g\cdot\lambda(v)=g(\lambda(g^{-1}v))$), et $\mathrm{Hom}_{\mathrm{G}_K}(V,\mathbf{B}_{\mathrm{dR}})=(\mathbf{B}_{\mathrm{dR}}\otimes_{\mathbf{Q}_p}V^*)^{\mathrm{G}_K}$.

Montrons alors que si $\lambda_1,\dots,\lambda_r\in(\mathbf{B}_{\mathrm{dR}}\otimes_{\mathbf{Q}_p}V^*)^{\mathrm{G}_K}$ sont colinéaires sur $\mathbf{B}_{\mathrm{dR}}$, alors ils le sont déjà sur K. Pour cela, considérons une relation linéaire $\sum_{i\in I}\alpha_i\lambda_i=0$ minimale (i.e. ayant le nombre minimal possible de α_i (en supprimant les α_i nuls)). Comme $\mathbf{B}_{\mathrm{dR}}$ est un corps, en divisant par l'un des α_i, on peut supposer que l'un des α_i est égal à 1. De plus, si $g\in\mathrm{G}_K$, on a $g(\sum_{i\in I}\alpha_i\lambda_i)=\sum_{i\in I}g(\alpha_i)\lambda_i=0$, et en soustrayant cette relation de la relation initiale on obtient une relation de longueur plus petite (puisque l'un des coefficients s'annule) ; on en déduit que tous les coefficients sont nuls et donc que $g(\alpha_i)=\alpha_i$, quels que soient $i\in I$ et $g\in\mathrm{G}_K$. D'après la prop. 2.43, cela implique que $\alpha_i\in K$, pour tout $i\in I$, et donc que les λ_i sont colinéaires sur K. On en déduit que

$$\dim_K\mathrm{Hom}_{\mathrm{G}_K}(V,\mathbf{B}_{\mathrm{dR}})=\dim_K(\mathbf{B}_{\mathrm{dR}}\otimes_{\mathbf{Q}_p}V^*)^{\mathrm{G}_K}\leqslant\dim_{\mathbf{B}_{\mathrm{dR}}}\mathbf{B}_{\mathrm{dR}}\otimes_{\mathbf{Q}_p}V^*=\dim_{\mathbf{Q}_p}V,$$

ce qu'il fallait démontrer.

Remarque 2.45. — (i) On dit que V est *de de Rham* si $\dim_K\mathrm{Hom}_{\mathrm{G}_K}(V,\mathbf{B}_{\mathrm{dR}})=\dim_{\mathbf{Q}_p}V$. Fontaine a conjecturé, et Faltings et Tsuji ont démontré, que les représentations de G_K provenant de la géométrie algébrique (comme $V_p(E)=\mathbf{Q}_p\otimes_{\mathbf{Z}_p}T_p(E)$, si E est une courbe elliptique sur K) sont de de Rham. Ceci nous fournit une contrainte très forte pour qu'une représentation provienne de la géométrie, et a des tas d'applications en géométrie arithmétique.

(ii) On montre que $V_p(E)$ est de de Rham en construisant un accouplement « périodes p-adiques »

$$H^1_{\mathrm{dR}}(E)\times T_p(E)\to\mathbf{B}_{\mathrm{dR}},\quad(\alpha,u)\mapsto\int_u\alpha$$

qui commute à l'action de G_K, et en prouvant une formule de Legendre p-adique (cf. th. 1.16)

$$\int_u\omega\int_v\eta-\int_v\omega\int_u\eta=\langle u,v\rangle,$$

où $\langle u,v\rangle\in\mathbf{Z}_p(1)=\mathbf{Z}_pt$ est l'accouplement de Weil ((ii) de la rem. 1.20).

2.2.8. Le logarithme sur une courbe elliptique. — La construction de l'accouplement « périodes p-adiques » peut se faire en intégrant sur la courbe elliptique comme dans le cas complexe ; nous montrons ci-dessous comment définir une primitive de ω.

Théorème 2.46. — *Soient K une extension finie de $\mathbf{Q}_p$, E une courbe elliptique définie sur K, d'équation $Y^2 = 4X^3 - g_2X - g_3$, et $\omega = \frac{dX}{Y}$. Alors il existe une unique fonction F_ω localement analytique sur E, telle que :*

- $dF_\omega = \omega$ (i.e. F_ω est une primitive de ω).
- $F_\omega(x \oplus y) = F_\omega(x) + F_\omega(y)$, *quels que soient* $x, y \in E(\overline{K})$

Démonstration. — On commence par se placer dans un voisinage de 0, i.e. on se place dans $E_1(\overline{K}) = \widehat{E}(\mathfrak{m}_{\overline{K}})$, et l'on dispose (lemme 1.26) d'un isomorphisme analytique $Z \mapsto \phi(Z) = (Z, W(Z))$ de $\widehat{E}(\mathfrak{m}_{\overline{K}})$ sur $E_1(\overline{K})$. Comme ω est holomorphe sur E, $\phi^*\omega$ est de la forme $f(Z)dZ$, où f converge sur $U_r = \{v_p(Z) > r\}$, qui est un sous-groupe ouvert de $\widehat{E}(\mathfrak{m}_{\overline{K}})$.

Si $f(Z) = \sum_{n=0}^{+\infty} a_n T^n$, on note $F(Z) = \sum_{n=0}^{+\infty} a_n \frac{T^{n+1}}{n+1}$ la primitive formelle de $f(Z)dZ$. Alors F converge encore sur U_r. De plus, la forme différentielle ω étant invariante par translation sur E (prop. 1.9), la forme $f(Z)dZ$ est invariante par translation par un élément de U_r, et on en déduit que si $a \in U_r$, alors $F(Z +_{\widehat{E}} a) - F(Z)$ est constante sur U_r et donc que $F(\phi^{-1}(x) \oplus \phi^{-1}(y)) = F(\phi^{-1}(x)) + F(\phi^{-1}(y))$, si $x, y \in V_r = \phi(U_r)$.

Comme $d(F \circ \phi^{-1}) = \omega$, on voit que si on définit F_ω sur V_r par $F_\omega = F \circ \phi^{-1}$, alors F_ω vérifie les propriétés voulues. Notre problème est donc d'étendre F_ω à $E(\overline{K})$. Or $E(\overline{K})$ est la réunion des $E(L)$, pour L extension finie de K, et chaque $E(L)$ est un groupe compact (car c'est un fermé dans $\mathbf{P}^2(\mathscr{O}_L)$ qui est compact), et comme $V_r \cap E(L)$ est ouvert, le groupe $E(L)/(V_r \cap E(L))$ est un groupe fini. On en déduit que si, $x \in E(\overline{K})$, il existe $n \in \mathbf{N} - \{0\}$ tel que $[n]x \in V_r$, et donc que l'on doit poser $F_\omega(x) = \frac{1}{n} F_\omega([n]x)$, si l'on veut que la seconde propriété de F_ω soit vérifiée. Comme F_ω est additif sur V_r, on a

$$\frac{1}{n} F_\omega([n]x) = \frac{1}{nm} F_\omega([nm]x) = \frac{1}{m} F_\omega([m]x),$$

si $[n]x \in V_r$ et $[m]x \in V_r$, ce qui prouve que la définition ci-dessus ne dépend pas du choix de n. De plus, on a $d(\frac{1}{n} F_\omega([n]x)) = \omega$ en un point tel que $[n]x \in V_r$ (car $[n]^*\omega = n\omega$), ce qui prouve que F_ω est une primitive de ω sur $E(\overline{K})$ tout entier. Finalement, si $[n]x \in V_r$ et $[n]y \in V_r$, alors $[n](x \oplus y) \in V_r$ et

$$F_\omega(x \oplus y) = \frac{1}{n} F_\omega([n](x \oplus y)) = \frac{1}{n} F_\omega(([n]x) \oplus ([n]y)) = \frac{1}{n} F_\omega([n]x) + \frac{1}{n} F_\omega([n]y) = F_\omega(x) + F_\omega(y),$$

ce qui montre que F_ω est additive et permet de conclure.

La fonction F_ω construite ci-dessus est le *logarithme* de la courbe elliptique E. La différence avec le cas complexe est, comme dans le cas du groupe multiplicatif, que ce logarithme est monovalué, et donc qu'il faut se fatiguer un peu plus pour faire apparaître les périodes p-adiques de la courbe elliptique (de la même manière qu'il a fallu se fatiguer un peu pour faire apparaître $2i\pi$ en p-adique).

3. Fonctions analytiques sur un corps ultramétrique

Dans tout ce qui suit, L est un corps complet pour une valuation v.

3.1. Polygones de Newton

Lemme 3.1. — *Soit $P(X) = a_nX^n + \cdots + a_0 \in L[X]$, un polynôme de degré n et soient $\alpha_1, \ldots, \alpha_n$, les racines (avec leur multiplicité) de P dans $\overline{L}$ rangées de telle sorte que l'on ait*

$$v(\alpha_1) \geqslant v(\alpha_2) \geqslant \cdots \geqslant v(\alpha_n).$$

Alors, si $i \in \{0, \ldots, n\}$, on a

$$v(a_i) \geqslant v(a_n) + \sum_{k=0}^{n-i-1} v(\alpha_{n-k}).$$

avec égalité si $v(\alpha_i) > v(\alpha_{i+1})$.

Démonstration. — L'inégalité est une conséquence du lien entre les coefficients de P et les fonctions symétriques des racines de P (on a $a_i = (-1)^{n-i}a_n \sum_{k_1<\cdots<k_{n-i}} \alpha_{k_1} \cdots \alpha_{k_{n-i}}$) et le cas d'égalité vient de ce que, si $v(\alpha_i) > v(\alpha_{i+1})$, alors dans la fonction symétrique d'ordre $n-i$, tous les autres termes ont une valuation strictement plus grande que $\prod_{k=1}^{n-i-1} \alpha_{n-k}$.

Soit $\lambda_P : [0, n[\to \mathbf{R} \cup \{+\infty\}$ la fonction définie par $\lambda_P(x) = -v(\alpha_i)$ si $x \in [i-1, i[$ et $\mathrm{Newt}_P(x) = v(a_n) + \int_n^x \lambda_P(t)dt$. La fonction $\lambda_P(x)$ est croissante et en escalier et la fonction $\mathrm{Newt}_P(x)$ est donc convexe et affine par morceaux sur $[0, n]$. Le lemme précédent peut se traduire aussi par $v(a_i) \geqslant \mathrm{Newt}_P(i)$ avec égalité si $v(\alpha_i) > v(\alpha_{i+1})$, c'est-à-dire si les dérivées à droite et à gauche de la fonction Newt_P au point i sont différentes (autrement dit, si $(i, \mathrm{Newt}_P(i))$ est un *sommet* (du graphe) de Newt_P). L'ensemble $\{(x, y) \mid x \in [0, 1],\ y \geqslant \mathrm{Newt}_P(x)\}$ s'appelle le *polygone de Newton de P* ; c'est aussi l'enveloppe convexe de l'ensemble de $(i, v(a_i))$ et de $[0, n] \times \{+\infty\}$. On appelle *pente de* Newt_P ou *pente du polygône de Newton de P* un élément de $\lambda_P([0, n])$ et, si λ est une pente de Newt_P, on appelle *segment de pente λ* de Newt_P l'ensemble $\{(x, \mathrm{Newt}_P(x)) \mid \lambda_P(x) = \lambda\}$; la *longueur* de ce segment est, par définition, la longueur de sa projection sur l'axe des x.

Le théorème suivant est une traduction du lemme 3.1, en utilisant le langage des polygones de Newton.

Théorème 3.2. — *Il existe une racine de P de valuation λ si et seulement si $-\lambda$ est une pente de* Newt_P. *De plus, le nombre de racines de P (comptées avec multiplicité) de valuation λ est la longueur du segment de pente $-\lambda$ de* Newt_P.

Exercice 5. — Soient $P, Q \in L[X]$. On suppose que Q divise P. Comment obtient-on le polygone de Newton de $\frac{P}{Q}$ en fonction de ceux de P et Q.

3.2. Séries entières

Si $r \in \mathbf{R}$, on note $D(0, r)$ (resp. $D(0, r^+)$) le disque fermé $v(T) \geqslant r$ (resp. le disque ouvert $v(T) > r$) du complété C de $\overline{L}$.

3.2.1. Valuation de convergence raffinée d'une série entière. — Soit $\widetilde{\mathbf{R}} = \mathbf{R} \cup (\mathbf{R} \times \{-,+\}) \cup \{-\infty, +\infty\}$. Si $r \in \mathbf{R}$, on note simplement r^- [resp. r^+] l'élément $(r,-)$ [resp. $(r,+)$] de $\widetilde{\mathbf{R}}$. On munit $\widetilde{\mathbf{R}}$ de la relation d'ordre totale évidente définie par

(i) $-\infty \leqslant x$ et $x \leqslant +\infty$ quel que soit $x \in \widetilde{\mathbf{R}}$;

(ii) $r^- < r < r^+$ si $r \in \mathbf{R}$;

(iii) $r^+ < s^-$ si $r, s \in \mathbf{R}$ vérifient $r < s$.

Finalement, si $x \in \widetilde{\mathbf{R}}$, on définit $-x \in \widetilde{\mathbf{R}}$ de la manière habituelle si $x \in \mathbf{R}$ et par

$$-(-\infty) = +\infty \text{ et } -(+\infty) = -\infty; \quad -(r^-) = (-r)^+ \text{ et } -(r^+) = (-r)^- \text{ si } r \in \mathbf{R}.$$

Si $(x_k)_{k\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{R}$, on note $\operatorname{linf} x_k \in \mathbf{R} \cup \{-\infty, +\infty\}$ la limite inférieure de la suite $(x_k)_{k\in\mathbf{N}}$ et on définit la *limite inférieure raffinée* $\operatorname{linf}' x_k \in \widetilde{\mathbf{R}}$ de la suite $(x_k)_{k\in\mathbf{N}}$, par la formule

$$\operatorname{linf}' x_k = \begin{cases} -\infty & \text{si } \operatorname{linf} x_k = -\infty, \\ r^- & \text{si } \operatorname{linf} x_k = r \text{ et } \operatorname{linf} k \cdot (x_k - r) = -\infty, \\ r & \text{si } \operatorname{linf} x_k = r \text{ et } \operatorname{linf} k \cdot (x_k - r) \in \mathbf{R}, \\ r^+ & \text{si } \operatorname{linf} x_k = r \text{ et } \lim k \cdot (x_k - r) = +\infty, \\ +\infty & \text{si } \lim x_k = +\infty, \end{cases}$$

Si $f = \sum_{k=0}^{+\infty} a_k T^k \in L[[T]]$, on définit la *valuation de convergence* $\operatorname{Val}(f) \in \widetilde{\mathbf{R}}$ et la *valuation de convergence raffinée* $\operatorname{Val}'(f) \in \widetilde{\mathbf{R}}$ par les formules

$$\operatorname{Val}(f) = -\Big(\operatorname{linf} \frac{v(a_k)}{k}\Big) \quad \text{et} \quad \operatorname{Val}'(f) = -\Big(\operatorname{linf}' \frac{v(a_k)}{k}\Big).$$

Proposition 3.3. — *Si $f \in L[[T]]$, alors $f(T)$ converge si $v(T) > \operatorname{Val}(f)$ et $f(T)$ diverge si $v(T) < \operatorname{Val}(f)$. Plus précisément,*

$$\operatorname{Val}'(f) = \begin{cases} -\infty & \Leftrightarrow f \text{ est analytique sur } C \text{ tout entier}, \\ r^- & \Leftrightarrow f \text{ est analytique sur } D(0,r) \text{ et ne converge pas si } v(T) < r, \\ r & \Leftrightarrow f \text{ est analytique bornée sur } D(0,r^+) \text{ et ne converge pas si } v(T) \leqslant r, \\ r^+ & \Leftrightarrow f \text{ est analytique non bornée sur } D(0,r^+) \text{ et ne converge pas si } v(T) \leqslant r, \\ +\infty & \Leftrightarrow f \text{ ne converge que pour } T = 0. \end{cases}$$

Démonstration. — Exercice

3.2.2. Le polygone de Newton d'une série entière. — Si $f = \sum_{k\in\mathbf{N}} a_k T^k \in L[[T]]$, soit $\operatorname{Newt}_f : \mathbf{R}_+ \to \mathbf{R} \cup \{\pm\infty\}$ la plus grande fonction convexe vérifiant $\operatorname{Newt}_f(k) \leqslant v(a_k)$ quel que soit $k \in \mathbf{N}$. Comme dans le cas d'un polynôme, cette fonction est affine par morceaux (et même affine sur chaque segment de la forme $[k, k+1]$, où $k \in \mathbf{N}$) et vaut $+\infty$ sur le segment $[0, v_T(f)]$; son graphe est *le polygone de Newton* de f, une *pente du polygone de Newton* est une valeur prise par la dérivée λ_f de Newt_f (qui est une fonction croissante puisque Newt_f est convexe). Par rapport au cas des polynômes, il peut se passer plusieurs phénomènes nouveaux.

• La fonction Newt_f peut ne prendre aucune valeur finie (même si $f \neq 0$) par exemple, si $f = \sum_{k=1}^{+\infty} p^{-k^2} T^k$, la fonction $\operatorname{Newt}_f(x)$ vaut $+\infty$ sur $[0,1[$ et $-\infty$ sur $[1,+\infty[$.

• Le polygone de Newton peut posséder une infinité de pentes : par exemple, si $f = \sum_{n=1}^{+\infty} p^{-n} T^{\frac{n(n+1)}{2}}$, la fonction $\mathrm{Newt}_f(x)$ vaut $-n - \frac{1}{n+1}(x - \frac{n(n+1)}{2})$ sur $[\frac{n(n+1)}{2}, \frac{(n+1)(n+2)}{2}]$ et la fonction λ_f prend donc les valeurs $-1, -\frac{1}{2}, -\frac{1}{3}, \dots$. Autre exemple, la fonction $\sum_{k=0}^{+\infty} p^{k^2} T^k$ dont les pentes sont $1, 3, 5, 7, \dots$ et tendent vers $+\infty$.

• Si le polygone de Newton ne possède qu'un nombre fini de pentes, alors le dernier « segment » est une demi-droite. Si cette demi-droite ne contient qu'un nombre fini de points de la forme $(k, v(a_k))$, on rajoute le dernier de ces points aux *sommets du polygone de Newton*, i.e. aux points de la forme $(k, v(a_k))$ appartenant au polygone de Newton en lesquels les dérivées à gauche et à droite ne sont pas les mêmes.

Proposition 3.4. — $\mathrm{Val}(f) = -\lim_{x \to +\infty} \lambda_f(x)$.

Démonstration. — Exercice

Exercice 6. — (i) Montrer que les sommets du polygone de Newton de $\log(1+T)$ sont les $(p^n, -n)$, pour $n \in \mathbf{N}$. Calculer ses pentes.

(ii) Montrer que le polygone de Newton de $\exp T$ est la droite $y = -\frac{x}{p-1}$.

3.2.3. Le théorème de préparation de Weierstrass. — Soit $L\{T\}$ l'anneau des séries convergeant sur la boule $\{v(x) \geqslant 0\}$; c'est aussi l'ensemble des séries $f = \sum_{k=0}^{+\infty} a_k T^k$ vérifiant $\lim_{k \to +\infty} v(a_k) = +\infty$; on l'obtient en complétant $L[T]$ pour la valuation de Gauss v_G.

Proposition 3.5. — (Lemme de Gauss) $v_G(fg) = v_G(f) + v_G(g)$.

Démonstration. — Par continuité à partir du cas des polynômes.

Proposition 3.6. — (Continuité de la division euclidienne) *Si $P \in \mathscr{O}_L[T]$ est un polynôme unitaire, alors tout élément f de $L\{T\}$ peut s'écrire de manière unique sous la forme $f = Pq(f) + r(f)$, où $q(f) \in L\{T\}$ et $r(f) \in L[T]$ est de degré $\leqslant \deg P - 1$. De plus, $v_G(q(f)) \geqslant v_G(f)$ et $v_G(r(f)) \geqslant v_G(f)$.* (Le polynôme $r(f)$ est le *reste de la division euclidienne* de f par P, et $q(f)$ est le *quotient de la division euclidienne* de f par P.)

Démonstration. — Pour démontrer l'unicité, il suffit de vérifier que l'application $(g, R) \to Pg + R$ est injective et donc que si $Pg = -R$, alors $g = R = 0$. Or P, étant unitaire à coefficients entiers, a $\deg P$ zéros appartenant à la boule $\{v(x) \geqslant 0\}$, alors que R en a au plus $\deg P - 1$ s'il n'est pas nul ; ceci permet de conclure.

Pour démontrer l'existence, constatons que P étant unitaire à coefficients dans $\mathscr{O}_L$, le reste $r(Q)$ et le quotient $q(Q)$ de la division euclidienne d'un polynôme $Q \in \mathscr{O}_L[T]$ par P appartiennent aussi $\mathscr{O}_L[T]$; les applications r et q de $L[T]$ dans $L[T]$ vérifient donc $v_G(r(Q)) \geqslant v_G(Q)$ et $v_G(q(Q)) \geqslant v_G(Q)$, et elles s'étendent par continuité à $L\{T\}$ en des applications vérifiant les mêmes propriétés, ce qui permet de conclure.

Proposition 3.7. — (i) *$g = \sum_{k \in \mathbf{N}} b_k T^k \in L\{T\}$ est inversible dans $L\{T\}$ si et seulement si $b_0 \neq 0$ et $v(b_k) > v(b_0)$ si $k \geqslant 1$.*

(ii) *Si $f = \sum_{k\in\mathbf{N}} a_k T^k \in L\{T\}$ est non nul, alors f peut s'écrire de manière unique sous la forme $f = Pg$, où $P \in \mathscr{O}_L[T]$ est un polynôme unitaire, et $g = \sum_{k=0}^{+\infty} b_k T^k$ est une unité de $L\{T\}$*

Démonstration. — Soit $g \in L\{T\}$ inversible. Quitte à diviser g par un élément de L^*, on peut supposer que $v_G(g) = 0$. On a alors $v_G(g^{-1}) = 0$, ce qui permet de réduire l'identité $gg^{-1} = 1$ modulo $\mathfrak{m}_L$, et d'obtenir $\overline{g}\cdot\overline{g}^{-1} = 1$ dans $k_K[T]$. On en déduit que $\overline{g}$ est une constante non nulle, ce qui prouve l'implication « $g = \sum_{k\in\mathbf{N}} b_k T^k$ inversible »⇒« $b_0 \neq 0$ et $v(b_k) > v(b_0)$ si $k \geqslant 1$ ». Réciproquement, si $b_0 \neq 0$ et $v(b_k) > v(b_0)$ si $k \geqslant 1$, alors $v_G(b_0^{-1}g - 1) > 0$, ce qui implique que $b_0^{-1}g$ est inversible et donc que g est inversible. On en déduit le (i).

Passons au (ii). La suite $v(a_k)$ tendant vers $+\infty$, il existe $d \in \mathbf{N}$ tel que l'on ait $v(a_d) \leqslant v(a_k)$ (resp. $v(a_d) < v(a_k)$) si $k \in \mathbf{N}$ (resp. si $k > d$). Soient $\alpha_0 = a_d$ et $P_0 = \sum_{k=0}^{d} \frac{a_k}{a_d} T^k$. Nous allons prouver que l'on peut trouver $R \in \mathfrak{m}_L[T]$, de degré $\leqslant d-1$, et $u \in \mathfrak{m}_L\{T\}$, tels que l'on ait $\alpha_0^{-1} f = (P_0 + R)(1+u)$, ce qui peut se réécrire sous la forme $P_0 u + R = \alpha_0^{-1} f - P_0 - Ru$. Pour ce faire, considérons l'application θ qui à (u, R) associe le couple $\theta(u, R)$ obtenu en prenant le quotient et le reste de la division euclidienne de $\alpha_0^{-1} f - P_0 - Ru$ par P_0. Comme $\alpha_0^{-1} f - P_0 \in \mathfrak{m}_L\{T\}$ par construction de α_0 et P_0, l'application θ envoie $\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1}$ dans lui-même d'après la proposition précédente. D'autre part, cette même proposition montre que, si on pose $v_G(u, R) = \inf(v_G(u), v_G(R))$, alors

$$\begin{aligned} v_G(\theta(u,R) - \theta(u'R')) \geqslant v_G(uR - u'R') &\geqslant \inf(v_G(u) + v_G(R-R'), v_G(R') + v_G(u-u')) \\ &\geqslant \inf(v_G(u-u'), v_G(R-R')) + \inf(v_G(u), v_G(R')), \end{aligned}$$

ce qui permet de prouver que θ est une application contractante de $\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1}$; son unique point fixe (u_0, R_0) répond à la question.

Pour démontrer l'unicité d'une telle décomposition, remarquons que si $Pg = P'g'$, avec g, g' inversibles dans $L\{T\}$, la fraction rationnelle $\frac{P'}{P}$ n'a aucun zéro ni pôle sur la boule $\{v(x) \geqslant 0\}$ et, comme P et P' sont des polynômes unitaires dont tous les zéros appartiennent à cette boule (puisque P et P' sont à coefficients dans $\mathscr{O}_L$), on doit avoir $P = P'$, et donc aussi $g = g'$. Ceci permet de conclure.

Exercice 7. — Montrer que $\mathrm{Newt}_f - \mathrm{Newt}_P$ est constante sur $[0, \deg P]$, et que, si $x \in \mathbf{R}_+$, alors $\mathrm{Newt}_g(x) = \mathrm{Newt}_f(x + \deg P)$,

Corollaire 3.8. — *Si $f \in L[[T]]$ et $\lambda \in \mathbf{R}$, alors le nombre de zéros de F dans $\overline{L}$ (comptés avec multiplicité) de valuation λ est égal à la longueur du plus grand segment de pente $-\lambda$ dont les extrémités sont des sommets du polygone de Newton de f.*

Démonstration. — Si $\lambda \notin v(\overline{L}^*)$, il n'y a rien à prouver. Sinon, soit α un élément de $\overline{L}$ de valuation λ et soit $f_\lambda(T) = f(\frac{T}{\alpha})$. Le polygone de Newton de F et celui de f_λ sont reliés par la formule $\mathrm{Newt}_{f_\lambda}(x) = \mathrm{Newt}_f(x) - \lambda x$; ce qui permet de se ramener au cas $\lambda = 0$ qui suit immédiatement de la proposition précédente et de la théorie des polygones de Newton pour les polynômes.

3.3. L'anneau des séries convergentes

3.3.1. Le théorème des fonctions implicites. — Le résultat suivant est un analogue ultramétrique du classique théorème des fonctions implicites (en dimension 1).

Proposition 3.9. — *Soit A un anneau commutatif et soit $\Phi(X,Y)\in A[[X,Y]]$, avec $\Phi(0,0)=0$ et $\frac{\partial\Phi}{\partial X}(0,0)=1$.*

(i) *Il existe $U\in YA[[Y]]$ unique tel que $\Phi(U,Y)=0$.*

(ii) *Plus généralement, si B est une A-algèbre séparée et complète pour une topologie I-adique, alors pour tout $y\in I$, l'équation $\Phi(x,y)=0$ admet $u=U(y)$ comme unique solution dans I.*

Démonstration. — (i) Soit $\Psi : YA[[Y]]\to YA[[Y]]$ l'aplication définie par $\Psi(U)=U-\Phi(U,Y)$. Alors $\Psi(U)-\Psi(U')=(U-U')\Psi_1(U,U',Y)$, avec $\Psi_1(U,U',Y)\in(U,U',Y)A[[U,U',Y]]$. On en déduit le fait que Ψ est contractante (pour la topologie Y-adique) sur $YA[[Y]]$, et donc qu'elle admet un unique point fixe qui est donc l'unique solution de $\Phi(U,Y)=0$.

(ii) Le (ii) se démontre de même en constatant que $u\mapsto\Psi_y(u)=u-\Psi(u,y)$ est contractante sur I et donc admet un unique point fixe qui est l'unique solution de $\Phi(u,y)=0$, et comme $U(y)$ est une solution, cela permet de conclure.

3.3.2. Séries convergentes. — Soit K un corps complet pour une valuation v, et soit $\pi\in K^*$, avec $v(\pi)>0$ (par exemple π uniformisante de K, si K est de valuation discrète). On note $K[[T]]^\dagger$ l'ensemble des séries de valuation de convergence finie. Si $F=\sum_{n=0}^{+\infty}a_nT^n\in K[[T]]$, alors $F\in K[[T]]^\dagger$, si et seulement si il existe $A,r\in\mathbf{R}$ tels que $v(a_n)\geqslant A-nr$, pour tout n, ou encore, de manière équivalente, si et seulement si il existe $a,b\in\mathbf{N}$ tels que $\pi^aF(\pi^bT)\in\mathscr{O}_K[[T]]$.

Théorème 3.10. — (i) *$K[[T]]^\dagger$ est un anneau dont le corps des fractions est $K[[T]]^\dagger[\frac{1}{T}]$.*

(ii) *Si $U\in K[[T]]^\dagger$ vérifie $U(0)=0$ et $U'(0)\neq 0$, alors $F(U)\mapsto F(U(T))$ induit un isomorphisme de $K[[U]]^\dagger$ sur $K[[T]]^\dagger$.* (Autrement dit l'anneau des séries convergentes ne change pas si on fait un changement de variable convergent.)

Démonstration. — (i) Soient $F,G\in K[[T]]^\dagger$. Il existe $a,b\in\mathbf{N}$ tels que $\pi^aF(\pi^bT),\pi^aG(\pi^bT)\in\mathscr{O}_K[[T]]$, et on a $\pi^a(F+G)(\pi^bT)\in\mathscr{O}_K[[T]]$ et $\pi^{2a}(FG)(\pi^bT)\in\mathscr{O}_K[[T]]$, ce qui prouve que $F+G$ et FG appartiennent à $K[[T]]^\dagger$ et donc que $K[[T]]^\dagger$ est un anneau.

Pour montrer que $K[[T]]^\dagger[\frac{1}{T}]$ est un corps (et donc est le corps des fractions de $K[[T]]^\dagger$), il suffit de prouver que si $F\in K[[T]]^\dagger$ vérifie $F(0)=1$, alors $\frac{1}{F}\in K[[T]]^\dagger$. Pour cela, on remarque qu'il existe alors $b\in\mathbf{N}$ tel que $F(\pi^bT)\in 1+T\mathscr{O}_K[[T]]$, et alors $F(\pi^bT)$ admet comme inverse $\sum_{n=0}^{+\infty}(1-F(\pi^bT))^n\in 1+T\mathscr{O}_K[[T]]\subset K[[T]]^\dagger$. On en déduit l'appartenance de $\frac{1}{F}$ à $K[[T]]^\dagger$ que l'on cherchait à établir.

(ii) Écrivons U sous la forme $U(T)=\sum_{n=1}^{+\infty}u_nT^n$. Comme $U\in K[[T]]^\dagger$, il existe $r\in\mathbf{R}$ tel que $v(u_n)\geqslant nr$, pour tout $n\geqslant 1$. Si maintenant $F=\sum_{n=1}^{+\infty}a_nU^n\in K[[U]]^\dagger$, il existe $A,s\in\mathbf{R}$ tels que $v(a_n)\geqslant A+ns$ et un calcul brutal montre que si $F(U(T))=\sum_{n=1}^{+\infty}b_nT^n$, alors $v(b_n)\geqslant A+(r+s)n$, et donc que $F(U(T))\in K[[T]]^\dagger$. Pour montrer que l'on obtient bien un isomorphisme, il suffit de prouver que T est dans l'image (i.e. que l'on peut exprimer T comme

une série convergente $T(U)$ de U, car alors $G(T) \mapsto G(T(U))$ est un morphisme de $K[[T]]^\dagger$ dans $K[[U]]^\dagger$ inverse de $F(U) \mapsto F(U(T))$).

Quitte à faire des changements de variables $T = \pi^k T'$ et $U = u_1 \pi^k U'$ (qui sont trivialement inversibles de manière convergente), on se ramène au cas où $U(T) = \sum_{n=1}^{+\infty} u_n T^n \in T\mathscr{O}_K[[T]]$, et $u_1 = 1$, mais alors le (i) de la prop. 3.9 permet de conclure (avec $\Phi(T,U) = -U + \sum_{n=1}^{+\infty} u_n T^n$).

3.3.3. Fonctions localement analytiques sur une courbe. — On suppose toujours que K est complet pour une valuation v et que $v(\pi) > 0$.

Proposition 3.11. — *Soient $f \in K[X,Y]$ irréductible, avec $f(0,0) = 0$ et $\frac{\partial f}{\partial Y}(0,0) \neq 0$, et C la courbe d'équation $f(X,Y) = 0$.*

(i) *Il existe $i, j \in \mathbf{N}$ et $F \in T\mathscr{O}_K[[T]]$ tels que $Y = \pi^i F(\pi^{-j} X)$ soit l'unique solution $f(X,Y) = 0$ dans $K[[X]]$.*

(ii) *Si $v(x) > jv(\pi)$, alors $y = \pi^i F(\pi^{-j} x)$ est l'unique solution de $f(x,y) = 0$ vérifiant $v(y) > iv(\pi)$.* (Autrement dit, $x \mapsto (x, \pi^i F(\pi^{-j} x))$ est une bijection de $D(0, (jv(\pi))^+)$ sur $C(K) \cap \big(D(0,(jv(\pi))^+) \times D(0,(iv(\pi))^+)\big)$).

(iii) *Si T est n'importe quel paramètre local algébrique en* $(0,0)$ (i.e. $T \in K(C)$, vérifie $T(0) = 0$ et $\big(\frac{\partial T}{\partial X}\frac{\partial f}{\partial Y} - \frac{\partial T}{\partial Y}\frac{\partial f}{\partial Y}\big)(0,0) \neq 0$), *alors $K(C)$ s'injecte dans $K[[T]]^\dagger[\frac{1}{T}]$.*

Démonstration. — On a $f(X,Y) = aX + bY + \sum_{r+s \geqslant 2} c_{r,s} X^r Y^s$, avec $b \neq 0$. En posant $X = \pi^j X'$ et $Y = \pi^i Y'$ et en divisant par $b\pi^i$, l'équation de C devient

$$Y' + a'X' + \sum_{r+s \geqslant 2} c'_{r,s} (X')^r (Y')^s, \quad \text{avec } a' = ab^{-1}\pi^{j-i} \text{ et } c'_{r,s} = b^{-1}\pi^{rj+(s-1)i} c_{r,s},$$

et en prenant $j \gg i \gg 0$, on peut s'arranger pour que a' et les $c'_{r,s}$ soient dans $\mathscr{O}_K$. On peut alors utiliser le thèorème des fonctions implicites (prop. 3.9), pour en déduire les (i), (ii) et le (iii) dans le cas du paramètre local X' (on a $K(C) = K(X', Y')$, et $Y' \in K[[X']]$, ce qui permet d'utiliser le (i) du th. 3.10). Le (ii) du th. 3.10 permet alors d'en conclure que le (iii) est valable pour n'importe quel choix de paramètre local algébrique puisque en changer revient à faire un changement de variable convergent.

Soit maintenant C une courbe projective lisse dans $\mathbf{P}^2$ (c'est pour nous simplifier la vie ; la théorie est la même pour une courbe lisse dans $\mathbf{P}^n$). D'après la proposition précédente, si $P \in C(K)$, et si $T \in K(C)$ est un paramètre local en P, alors T induit un isomorphisme analytique entre un voisinage de P dans $C(K)$ et une boule de K. On dit que g est *analytique dans un voisinage de P*, s'il existe $F \in K[[T]]$ convergeant pour $v(T) > r$, telle que $g(x) = F(T(x))$, si $v(T(x)) > r$. D'après le (iii) de la proposition ci-dessus et le (ii) du th. 3.10, ceci ne dépend pas du choix de T (par contre, la taille du voisinage sur lequel $g(x) = F(T(x))$ dépend du choix de T). On dit que g est *localement analytique* sur C si elle est analytique au voisinage de tout point. En particulier, une fonction localement constante est localement analytique, et la topologie ultramétrique étant totalement discontinue, il y a des tas de fonctions localement constantes, contrairement au cas d'une courbe sur $\mathbf{C}$.

4. Corps locaux

4.1. Définition et exemples

Un *corps local* est un corps complet pour une valuation discrète. En particulier, si K est un corps local, et v est la valuation sur K, alors il existe $a > 0$ unique tel que $v(K^*) = a\mathbf{Z}$. Une *uniformisante* de K est alors n'importe quel élément π de K vérifiant $v(\pi) = a$.

Lemme 4.1. — *L'idéal maximal $\mathfrak{m}_K$ de l'anneau des entiers $\mathscr{O}_K$ de K est principal et un élément de K en est un générateur si et seulement si c'est une uniformisante.*

Démonstration. — Évident.

Exemple 4.2. — (i) $\mathbf{Q}_p$ muni de la valuation v_p est un corps local dont p est une uniformisante.

(ii) Si K est un corps, alors $K((T))$ muni de la valuation v_T est un corps local dont T est une uniformisante.

(iii) Le corps $\mathbf{Q}_p\{\{T\}\}$ des séries de Laurent $\sum_{n\in\mathbf{Z}} a_n T^n$, où $(a_n)_{n\in\mathbf{Z}}$ est une suite bornée d'éléments de $\mathbf{Q}_p$ tendant vers 0 quand n tend vers $-\infty$, devient un corps local si on le munit de la valuation v_p définie par $v_p(\sum_{n\in\mathbf{Z}} a_n T^n) = \inf_{n\in\mathbf{Z}} v_p(a_n)$. Son corps résiduel est $\mathbf{F}_p((T))$ qui n'est pas parfait (mais est un corps local) ; le corps $\mathbf{Q}_p\{\{T\}\}$ est un exemple de corps local de dimension 2.

Le théorème suivant, dont la démonstration utilise le lemme de Zorn, montre que l'exemple (ii) est typique.

Théorème 4.3. — *Si K est un corps local, et si k_K a même caractéristique que K, alors il existe un système de représentants de k_K dans $\mathscr{O}_K$ qui est un corps isomorphe à k_K, et le choix d'une uniformisante π de K induit un isomorphisme $K \cong k_K((T))$ envoyant π sur T.*

Définition 4.4. — Si A est un anneau et I est un idéal de A, on dit que A est *séparé et complet pour la topologie I-adique* si l'application naturelle de A dans $\varprojlim(A/I^nA)$ est un isomorphisme. La topologie I-adique sur A est alors celle qui fait de l'isomorphisme précédent un isomorphisme d'anneaux topologiques, $\varprojlim(A/I^nA)$ étant muni de la topologie produit, chacun des A/I^nA étant muni de la topologie discrète.

Lemme 4.5. — (i) *Si K est un corps complet pour une valuation v, et si $\pi \in K$ vérifie $v(\pi) > 0$, alors $\mathscr{O}_K$ est séparé et complet pour la topologie π-adique.*

(ii) *Si A est un anneau, si $\pi \in A$, si S est un et S est un système de représentants de $A/\pi A$ dans A, et si A est séparé et complet pour la topologie π-adique, alors tout élément de A peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n\pi^n$ avec $s_n \in S$.*

Démonstration. — (i) On note $\iota : \mathscr{O}_K \to \varprojlim(\mathscr{O}_K/\pi^n\mathscr{O}_K)$ l'application qui, à $x \in \mathscr{O}_K$, associe la suite des images de x modulo π^n. On a alors

• $\iota(x) = 0 \Leftrightarrow v(x) \geqslant nv(\pi)$ quel que soit $n \in \mathbf{N} \Leftrightarrow v(x) = +\infty \Leftrightarrow x = 0$, ce qui montre que ι est injective.

• Si $(x_n)_{n\in\mathbf{N}} \in \varprojlim(\mathscr{O}_K/\pi^n\mathscr{O}_K)$ et si $\hat{x}_n \in \mathscr{O}_K$ est un relêvement quelconque de x_n, alors $v(\hat{x}_{n+k} - \hat{x}_n) \geqslant nv(\pi)$ quels que soient $n, k \in \mathbf{N}$. Ceci montre que la suite $\hat{x}_n$ est de Cauchy, et sa limite x verifie $v(x - \hat{x}_n) \geqslant nv(\pi)$ quel que soit $n \in \mathbf{N}$. On en déduit que $\iota(x) = (x_n)_{n\in\mathbf{N}}$, ce qui prouve la surjectivité de ι.

• « $v(x-y) \geqslant nv(\pi)$ » $\Leftrightarrow$ « $x = y$ dans $\mathscr{O}_K/\pi^k\mathscr{O}_K$, quel que soit $i \leqslant n$ », ce qui montre que la topologie induite par v sur $\mathscr{O}_K$ correspond à la topologie produit sur $\varprojlim(\mathscr{O}_K/\pi^n\mathscr{O}_K)$, chaque $\mathscr{O}_K/\pi^n\mathscr{O}_K$ étant muni de la topologie discrète.

(ii) Soit $s : A \to S$ l'application qui à x associe l'unique élément $s(x)$ de S vérifiant $x - s(x) \in \pi A$. Si $x \in A$, on définit par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de A en posant $x_0 = x$ et, si $n \geqslant 1$, $x_n = \frac{1}{\pi}(x_{n-1} - s(x_{n-1}))$. On a alors $x = \sum_{i=0}^{n} s(x_i)\pi^i + \pi^{n+1}x_{n+1}$ quel que soit $n \in \mathbf{N}$, et donc $x = \sum_{n=0}^{+\infty} s(x_n)\pi^n$ ce qui prouve l'existence d'une écriture sous la forme mentionnée plus haut. D'autre part, si $\sum_{n=0}^{+\infty} s_n\pi^n = \sum_{n=0}^{+\infty} s'_n\pi^n$, alors réduisant modulo π, on obtient $s_0 = s'_0$ et une récurrence immédiate nous montre que $s_n = s'_n$ quel que soit $n \in \mathbf{N}$ d'où l'unicité de l'écriture.

Corollaire 4.6. — *Si K est un corps local, si S est un système de représentants de k_K dans $\mathscr{O}_K$, si π est une uniformisante de K, alors tout élément de $\mathscr{O}_K$ peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n\pi^n$ avec $s_n \in S$.*

Exemple 4.7. — Si $K = \mathbf{Q}_p$, on a $\mathscr{O}_K = \mathbf{Z}_p$ et $k_K = \mathbf{F}_p$, on peut prendre p comme uniformisante et $\{0, 1, \ldots, p-1\}$ ou $\{[x],\ x \in \mathbf{F}_p\}$ comme système de représentants de $\mathbf{F}_p$ dans $\mathbf{Z}_p$.

4.2. Extensions de corps locaux

Dans tout ce § (sauf mention explicite du contraire), F est un corps complet pour une valuation discrète, et le corps résiduel k_F est de caractéristique p.

4.2.1. Ramification et inertie. — Si F est un corps complet pour une valuation discrète et K est une extension finie de F , le corps résiduel k_K est une extension finie de k_F de degré $f = f(K/F)$ appelé indice d'inertie de l'extension K/F.

D'autre part, on a $v(K^*) \subset \frac{1}{[K:F]}v(F^*)$ et $v(F^*)$ est donc d'indice fini $e = e(K/F)$ dans $v(K^*)$. Cet indice est appelé indice de ramification de l'extension K/F.

Lemme 4.8. — *Soient $e = e(K/F)$ et $f = f(K/F)$. Soient $u_1, \ldots, u_f$ des éléments de $\mathscr{O}_K$ dont les réductions modulo $\mathfrak{m}_K$ forment une base de k_K sur k_F et π_K une uniformisante de $\mathscr{O}_K$. Alors, les $\pi_K^j u_i$ pour $0 \leqslant j \leqslant e-1$ et $1 \leqslant i \leqslant f$ forment une base de $\mathscr{O}_K$ sur $\mathscr{O}_F$.*

Démonstration. — Soit S_F un système de représentants de k_F dans $\mathscr{O}_F$ et soit $S_K = S_F u_1 + \cdots + S_F u_f$, ce qui fait de S_K un système de représentants de k_K dans $\mathscr{O}_K$. Soit π_F une uniformisante de F. Comme $\mathscr{O}_K/\pi_F\mathscr{O}_K = \mathscr{O}_K/\pi_K^e\mathscr{O}_K$, on déduit du corollaire 4.6, le fait que $S_K + \pi_K S_K + \cdots + \pi_K^{e-1} S_K$ est un système de représentants de $\mathscr{O}_K/\pi_F\mathscr{O}_K$ et donc que tout élément de $\mathscr{O}_K$

peut s'écrire de manière unique sous la forme

$$\sum_{n=0}^{+\infty}\pi_F^n\Big(\sum_{j=0}^{e-1}\pi_K^j\Big(\sum_{i=1}^{f}s_{i,j,n}u_i\Big)\Big)=\sum_{j=0}^{e-1}\sum_{i=1}^{f}\pi_K^j u_i\Big(\sum_{n=0}^{+\infty}\pi_F^n s_{i,j,n}\Big)$$

avec $s_{i,j,n}\in S_F$, ce qui implique, utilisant le fait que tout élément de $\mathscr{O}_F$ peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty}\pi_F^n s_n$ avec $s_n\in S_F$, que tout élément de $\mathscr{O}_K$ peut s'écrire de manière unique sous la forme $\sum_{j=0}^{e-1}\sum_{i=1}^{f}\pi_K^j u_i y_{i,j}$ avec $y_{i,j}\in\mathscr{O}_F$. Ceci permet de conclure.

Corollaire 4.9. — $e(K/F)f(K/F)=[K:F]$.

Démonstration. — Une base de $\mathscr{O}_K$ sur $\mathscr{O}_F$ est aussi une base de K sur F.

Définition 4.10. — L'extension K/F est *non ramifiée* si $e(K/F)=1$, et si k_K/k_F est séparable. Elle est *totalement ramifiée* si $e(K/F)=[K:F]$. Elle est *modérément ramifiée* si $e(K/F)$ est premier à la caractéristique du corps résiduel et si k_K/k_F est séparable, et *sauvagement ramifiée* dans le cas contraire.

Lemme 4.11. — *Si L/K et K/F sont deux extensions finies, alors $e(L/F)=e(L/K)e(K/F)$ et $f(L/F)=f(L/K)f(K/F)$*

Démonstration. — exercice.

4.2.2. Extensions totalement ramifiées

Si K est un corps local, un *polynôme d'Eisenstein* de degré d est un polynôme unitaire $P(X)=X^d+a_{d-1}X^{d-1}+\cdots+a_0\in K[X]$ tel que a_0 soit une uniformisante de K, et $a_1,\dots,a_{d-1}\in\mathfrak{m}_K$.

Lemme 4.12. — *Un polynôme d'Eisenstein est irréductible.*

Démonstration. — Si $P=QR$, avec Q et R unitaire, alors Q et R sont à coefficients dans $\mathscr{O}_K$ d'après le lemme de Gauss ($0=v_G(QR)=v_G(Q)+v_G(R)$ et $v_G(Q)\geqslant 0$, $v_G(R)\geqslant 0$). En réduisant modulo $\mathfrak{m}_K$, on obtient $\overline{QR}=X^d$, ce qui implique que les termes constants de Q et R sont dans $\mathfrak{m}_K$ et donc que celui de P est dans $\mathfrak{m}_K^2$, contrairement à l'hypothèse.

Lemme 4.13. — *Soit K un corps complet pour une valuation discrète et P un polynôme d'Eisenstein de degré d. Soit $L=K[X]/P$ et x l'image de X dans L. Alors*

(i) *Si $v(K^*)=u\mathbf{Z}$ avec $u>0$, alors $v(x)=\frac{u}{d}$ et L/K est totalement ramifiée.*
(ii) *x est une uniformisante de L.*
(iii) *si $y=\sum_{i=0}^{d-1}a_ix^i$, alors $v(y)=\inf_i v(a_i)+i\frac{u}{d}$.*
(iv) *$1,x,\dots,x^{d-1}$ forment une base de $\mathscr{O}_L$ (resp. L) sur $\mathscr{O}_K$ (resp. K).*

Démonstration. — Le (i) est une conséquence de la formule $v(x)=\frac{1}{[K:F]}v(\mathrm{N}_{K/F}(x))$ et du fait que P est d'Eisenstein. Le (ii) en est un corollaire immédiat. Le (iii) est une conséquence du fait que tous les termes de la somme ont une valuation différente. Le (iv) est une conséquence immédiate du (iii).

Proposition 4.14. — *Si K/F est totalement ramifiée et si π_K est une uniformisante de K, alors π_K engendre $\mathscr{O}_K$ en tant que $\mathscr{O}_F$-algèbre et le polynôme minimal de π_K sur F est un polynôme d'Eisenstein.*

Réciproquement, si $P \in F[X]$ est un polynôme d'Eisenstein, si $K = F[X]/P$, et si x est l'image de X dans K, alors K est une extension totalement ramifiée de F et x en est une uniformisante.

Démonstration. — Le fait que π_K engendre $\mathscr{O}_K$ est une conséquence du lemme 4.8 appliquée à $f = 1$ et $u_1 = 1$. Si $[K : F] = d$, le polynôme minimal P de π_K est donc irréductible de degré d, et si $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0$, on a $a_0 = \pm \mathrm{N}_{K/F}(\pi_K)$ et donc $v(a_0) = dv(\pi_K)$, ce qui implique que a_0 est une uniformisante de F. De plus, les conjugués de π_K ont une valuation > 0, et donc tous les a_i appartiennent à $\mathfrak{m}_K$. En conclusion P est d'Eisenstein. La réciproque est une conséquence du lemme 4.13.

4.2.3. Monogénéité de l'anneau des entiers

Remarque 4.15. — On vient de démontrer que si K est une extension finie de F totalement ramifiée, alors $\mathscr{O}_K$ est monogène sur $\mathscr{O}_F$ (i.e. il existe $x \in \mathscr{O}_K$ tel que l'on ait $\mathscr{O}_K = \mathscr{O}_F[x]$). Il s'agit là d'un cas particulier de la très utile proposition suivante.

Proposition 4.16. — *Si K est une extension finie de F, et si k_K/k_F est séparable, alors $\mathscr{O}_K$ est une extension monogène de $\mathscr{O}_F$.*

Démonstration. — Soient π_F et π_K des uniformisantes de F et K respectivement. Soit $y \in \mathscr{O}_K$ dont la réduction $\overline{y}$ modulo π_K est un élément primitif de k_K sur k_F (l'existence d'un tel élément est assurée par l'hypothèse k_K/k_F séparable). Soit $P \in \mathscr{O}_F[X]$ unitaire dont la réduction $\overline{P}$ modulo π_F est le polynôme minimal de $\overline{y}$ sur k_F. On a donc $P(y) \equiv 0$ mod. π_K et $P'(y) \not\equiv 0$ mod π_K car $\overline{y}$ est racine simple de $\overline{P}$. On en déduit le fait que $a \mapsto P(y+a\pi_K) = P(y)+a\pi_K P'(y)$ mod π_K^2 n'est pas identiquement nul sur $\mathscr{O}_K$, et donc qu'il existe $x = y + a\pi_K$ tel que $P(x)$ soit une uniformisante de K. On peut alors utiliser le lemme 4.8 pour démontrer que les $x^i P(x)^j$ pour $0 \leqslant x \leqslant f-1$ et $0 \leqslant j \leqslant e-1$ forment une base de $\mathscr{O}_K$ sur $\mathscr{O}_F$, et donc que x engendre $\mathscr{O}_K$ comme $\mathscr{O}_F$-algèbre.

4.2.4. Extensions non ramifiées et dévissage des extensions finies

Théorème 4.17. — (i) *Si k est une extension finie séparable de k_F, il existe une unique extension non ramifiée $F(k)$ de F dont le corps résiduel est k.*

(ii) *Si L est une extension finie de F et si k_L/k_F est séparable, alors $F(k_L) \subset L$, l'extension $L/F(k_L)$ est totalement ramifiée, et $F(k_L)$ est l'unique extension non ramifiée de F ayant ces deux propriétés.*

Démonstration. — Soit $\overline{\alpha}$ un élément primitif de k/k_F, et soient $\overline{P} \in k_F[X]$ son polynôme minimal, et $P \in \mathscr{O}_F[X]$ unitaire dont la réduction est $\overline{P}$. D'après le lemme de Hensel, si L est une extension finie de F dont le corps résiduel contient k, alors L contient un unique racine α de P dont l'image dans k_L est $\overline{\alpha}$. On a alors $[F(\alpha) : F] \leqslant \deg P = [k : k_F]$. Comme d'autre part, le corps résiduel de $F(\alpha)$ contient $\overline{\alpha}$ par construction, on a $f(F(\alpha)/F) \geqslant [k : k_F]$; on

en déduit l'égalité $[F(\alpha) : F] = [k : k_F] = f(F(\overline{\alpha})/F)$, ce qui implique que $F(\alpha)/F$ est non ramifiée. Maintenant, si L est une extension finie de F de corps résiduel k, on a $F(\alpha) \subset L$, d'après la discussion précédente, et $F(\alpha)$ ayant même corps résiduel que L, l'extension $L/F(\alpha)$ est totalement ramifiée ; en particulier, si L/F est non ramifiée, alors $L = F(\alpha)$. Ceci permet de conclure, avec $F(k) = F(\alpha)$.

Remarque 4.18. — Soit $\overline{F}$ une clôture algébrique de F. Comme la composée de deux extensions non ramifiée est non ramifiée, *l'extension maximale non ramifiée* F^{nr} de F, réunion de toutes les extensions non ramifiées de F, est un sous-corps de $\overline{F}$.

Exemple 4.19. — Le polynôme $X^q - X$ n'a que des racines simples dans $\overline{\mathbf{F}}_p$, et ses racines sont exactement les éléments de $\mathbf{F}_q$. On en déduit le fait que $\mathbf{Q}_p(\mathbf{F}_q)$ est le corps engendré par les racines du polynôme $X^q - 1$, c'est-à-dire par les racines $(q-1)$-ièmes de l'unité. L'extension maximale non ramifiée $\mathbf{Q}_p^{\mathrm{nr}}$ de $\mathbf{Q}_p$ est donc le sous-corps de $\overline{\mathbf{Q}}_p$ engendré par les racines de l'unité d'ordre premier à p.

4.2.5. Extensions modérément ramifiées

Proposition 4.20. — *Soit L/F une extension totalement ramifiée de degré $n = n_0 p^k$ avec $(n_0, p) = 1$. Alors L contient une unique extension K de F vérifiant $[K : F] = n_0$. De plus, il existe une uniformisante π_K de K telle que $\pi_K^{n_0} \in F$.*

Démonstration. — Soit π_L une uniformisante de L. On sait que π_L est racine d'un polynôme d'Eisenstein, et il existe donc π_F uniformisante de F, et $a_1, \dots, a_{n-1} \in \mathscr{O}_F$ tels que l'on ait $\pi_L^n = u\pi_F$ avec $u = (1 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}) \in \mathscr{O}_L^*$ vérifiant $v(u-1) > 0$. Comme $(n_0, p) = 1$, le lemme de Hensel permet de montrer que l'équation $v^{n_0} = u$ a une unique solution dans $1 + \mathfrak{m}_L$. On a alors $(v^{-1}\pi_L^{p^k})^{n_0} = \pi_F$, ce qui implique que L contient l'extension K définie par le polynôme d'Eisenstein $P(X) = X^{n_0} - \pi_F$ qui est totalement ramifiée de degré n_0 sur F.

Supposons maintenant que L contienne deux extensions K_1 et K_2 de F de degré n_0. Si on applique ce qui précède à ces deux extensions, on voit que si $i \in \{1, 2\}$, il existe une uniformisante π_i de K_i telle que $\pi_i^{n_0} \in F$. Mais alors $v(\pi_i) = \frac{1}{n_0}$, ce qui implique que $x = \frac{\pi_1}{\pi_2}$ est un élément de $\mathscr{O}_L^*$ dont la puissance n_0-ième appartient à F. Comme les corps résiduels de L et F sont les mêmes (puisque L/F est totalement ramifiée), on peut trouver $u \in \mathscr{O}_F$ tel que $v(xu^{-1} - 1) > 0$. Mais alors xu^{-1} est l'unique racine n_0-ième de $x^{n_0}u^{-n_0} \in 1 + \mathfrak{m}_F$ vérifiant $v(xu^{-1} - 1) > 0$, et on a $xu^{-1} \in 1 + \mathfrak{m}_F$ d'après le lemme de Hensel. On a donc $x \in F$, ce qui prouve que $K_1 = K_2$.

4.2.6. Extensions galoisiennes

Si L est une extension galoisienne finie de F et $\sigma \in \mathrm{Gal}(L/F)$, on a $v(\sigma(x)) = v(x)$ quel que soit $x \in L$. On en déduit le fait que $\sigma(\mathscr{O}_L) = \mathscr{O}_L$ et $\sigma(\mathfrak{m}_L) = \mathfrak{m}_L$ et donc que σ passe au quotient. On a donc une application naturelle de $\mathrm{Gal}(L/K)$ dans $\mathrm{Aut}_{k_F}(k_L)$ qui est de manière évidente un morphisme de groupes.

Définition 4.21. — On appelle *sous-groupe d'inertie* de $\mathrm{Gal}(L/F)$ le noyau $I_{L/F}$ de l'application naturelle de $\mathrm{Gal}(L/F)$ sur $\mathrm{Aut}_{k_F}(k_L)$. C'est un sous-groupe distingué de $\mathrm{Gal}(L/F)$.

Proposition 4.22. — *Soit L une extension finie de F telle que k_L/k_F soit séparable.*

(i) *Si L/F est galoisienne, alors k_L est une extension galoisienne de k_F.*

(ii) *Si L/K est non ramifiée, et si k_L/k_F est galoisienne, alors L/F est aussi galoisienne, et on a* $\mathrm{Gal}(F(k)/F) \cong \mathrm{Gal}(k/k_F)$.

(iii) *Si L/F est galoisienne, alors l'application naturelle* $\mathrm{Gal}(L/F) \to \mathrm{Gal}(k_L/k_F)$ *est surjective, et le corps fixé par le sous-groupe d'inertie $I_{L/F}$ est $F(k_L)$.*

Démonstration. — Si L/F est galoisienne et $\overline{\alpha} \in k_L$ est un élément primitif de k_L/k_k, soit $\overline{P} \in k_F[X]$ son polynôme minimal, $P \in \mathscr{O}_F[X]$ unitaire dont la réduction est $\overline{P}$ et $\alpha \in \mathscr{O}_{\overline{F}}$ se réduisant sur $\overline{\alpha}$. D'après la démonstration du th. 4.17, on a $\alpha \in F(k_L) \subset L$ et, comme L est galoisienne, le polynôme P se décompose sur L sous la forme $P(X) = (X - \alpha_1)\dots(X - \alpha_f)$. D'autre part, P étant unitaire à coefficients entiers, ses racines sont des entiers et les réductions $\overline{\alpha}_i$ sont les racines de $\overline{P}$ qui se décompose sur k_L ce qui montre que k_L/k_F est normale donc galoisienne.

Réciproquement, si on suppose L/F non ramifiée et k_L/k_F galoisienne, alors $\overline{P}$ se décompose sur k_L sous la forme $\overline{P}(X) = (X - \overline{\alpha}_1)\dots(X - \overline{\alpha}_f)$ et P a une racine unique $\alpha_i \in F(k_L) = L$ se réduisant sur $\overline{\alpha}_i$. On en déduit le fait que P est scindé sur L et, comme $L = F(\alpha) = F(\alpha_1, \dots, \alpha_f)$, que L est une extension galoisienne de F. De plus, $\mathrm{Gal}(L/F)$ et $\mathrm{Gal}(k_L/k_F)$ sont en bijection naturelle avec les conjugués de $\overline{\alpha}$ et l'application naturelle de $\mathrm{Gal}(L/F)$ dans $\mathrm{Gal}(k_L/k_F)$ est une bijection.

Finalement, si L est une extension galoisienne de F, comme $\mathrm{Gal}(F(k_L)/F) \cong \mathrm{Gal}(k_L/k_F)$ est le quotient de $\mathrm{Gal}(L/F)$ par $I_{L/F}$, on a $\mathrm{Gal}(L/F(k_L)) = I_{L/F}$ et $F(k_L) = L^{I_{L/F}}$.

Proposition 4.23. — *Si L/F est une extension galoisienne telle que k_L/k_F est séparable, et si $I_{L/F}$ est le sous-groupe d'inertie de* $\mathrm{Gal}(L/F)$*, alors $I_{L/F}$ a un unique p-sous-groupe de Sylow $I^+_{L/F}$ qui est distingué dans $I_{L/F}$ et* $\mathrm{Gal}(L/F)$.

Démonstration. — Soit $K = L^{I_{L/F}}$. D'après la proposition 4.22, K est l'extension maximale non ramifiée de F contenue dans L et L/K est galoisienne totalement ramifiée de groupe de Galois $I_{L/F}$. Les p-sous-groupes de Sylow de $I_{L/F}$ correspondent donc, via la correspondance de Galois, aux extensions de K, contenues dans L et de degré premier à p, et comme il n'y a qu'une seule extension ayant ces propriétés d'après la prop. 4.20, le groupe $I_{L/F}$ n'a qu'un seul sous-groupe de Sylow que l'on notera $I^+_{L/F}$. Maintenant, si $g \in \mathrm{Gal}(L/F)$, alors $gI^+_{L/F}g^{-1}$ est un p-groupe contenu dans $I_{L/F}$ puisque $I_{L/F}$ est distingué dans $\mathrm{Gal}(L/F)$. Il est donc inclus dans $I^+_{L/F}$ puisque $I^+_{L/F}$ est l'unique p-Sylow de $I_{L/F}$. Ceci permet de conclure.

Définition 4.24. — Le p-Sylow $I^+_{L/F}$ de $I_{L/F}$ est *le sous-groupe d'inertie sauvage.*

4.2.7. Structure des extensions finies

Si on regroupe ce qui précède (propositions 4.20, 4.22 et 4.23 et théorème 4.17), on obtient le théorème suivant décrivant la structure des extensions finies d'un corps complet pour une valuation discrète.

Théorème 4.25. — *Si L est une extension finie de F telle que k_L/k_F soit séparable, alors L contient deux sous-extensions $L_0 \subset L_1$ de F qui sont uniquement déterminées par les propriétés suivantes.*

(i) *L_0/F est non ramifiée,*

(ii) *L_1/L_0 est totalement et modérément ramifiée,*

(iii) *L/L_1 est totalement ramifiée de degré une puissance de p.*

De plus, $L_0 = F(k_L)$, et il existe une uniformisante π de L_1 telle que $\pi^{[L_1:L_0]} \in L_0$. Finalement, si L/F est galoisienne, alors $L_0 = L^{I_{L/F}}$ et $L_1 = L^{I^+_{L/F}}$.

4.2.8. Premier dévissage du groupe G_K. — On note K^{nr} (resp. K^{mod}) l'extension maximale non ramifiée (resp. modérément ramifiée) de K ; c'est la réunion de toutes les extensions finies non ramifiées (resp. modérément ramifiées) de K. Ce sont deux extensions galoisiennes de K et $K^{\mathrm{mod}} = \cup_{(n,p)=1} K^{\mathrm{nr}}(\pi_K^{1/n})$, où π_K est une uniformisante K (cela ne dépend pas du choix de π_K car, si $a \in \mathscr{O}_K^*$, alors $a^{1/n} \in K^{\mathrm{nr}}$, pour tout $(n,p)=1$).

Soit K^{sep} une clôture séparable de K. Alors $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{nr}})$ est le sous-groupe d'inertie I_K de G_K ; le quotient $\mathrm{G}_K/I_K = \mathrm{Gal}(K^{\mathrm{nr}}/K)$ est isomorphe à $\mathrm{Gal}(k_K^{\mathrm{sep}}/k_K)$. Par définition, $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{mod}})$ est le sous-groupe d'inertie sauvage I_K^+ de G_K. Le groupe I_K/I_K^+ est le groupe de Galois de K^{mod} sur K^{nr}. Comme l'application $g \mapsto \zeta_n(g) = \frac{g(\pi_K^{1/n})}{\pi_K^{1/n}}$ induit un morphisme de groupes de $\mathrm{Gal}(K^{\mathrm{nr}}(\pi_K^{1/n})/K^{\mathrm{nr}})$ sur μ_n (qui ne dépend pas du choix de π_K), on voit que I_K/I_K^+ est isomorphe à la limite projective des μ_n, pour $(n,p)=1$, c'est-à-dire à $\prod_{\ell\neq p} T_\ell(\mathbf{G}_m) = \prod_{\ell\neq p} \mathbf{Z}_\ell(1)$. En tant que groupe, ce groupe est juste le produit des $\mathbf{Z}_\ell$, pour $\ell \neq p$, mais, comme il est commutatif, il est en plus muni d'une action de $\mathrm{Gal}(K^{\mathrm{nr}}/K)$. En effet, si $g \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$, on peut relever g en $\tilde{g} \in \mathrm{Gal}(K^{\mathrm{mod}}/K) = \mathrm{G}_K/I_K^+$, et $\tilde{g}$ est bien défini à multiplication près, à droite, par un élément de I_K/I_K^+, ce qui fait que si $h \in I_K/I_K^+$, alors $\tilde{g}h\tilde{g}^{-1}$ est un élément de I_K/I_K^+ qui ne dépend que de g, et pas du choix de $\tilde{g}$; on le note $g \cdot h$. On a alors

$$\zeta_n(g\cdot h) = \frac{\tilde{g}h\tilde{g}^{-1}(\pi_K^{1/n})}{\tilde{g}(\tilde{g}^{-1}(\pi_K^{1/n}))} = \tilde{g}\big(\frac{h(\tilde{g}^{-1}(\pi_K^{1/n}))}{\tilde{g}^{-1}(\pi_K^{1/n})}\big),$$

et comme $\tilde{g}^{-1}(\pi_K) = \pi_K$, la dernière expression n'est autre que $\tilde{g}(\zeta_n(h)) = g(\zeta_n(h))$ puisque $\zeta_n(h) \in K^{\mathrm{nr}}$. En d'autres termes, on a le résultat suivant :

Proposition 4.26. — *On a une suite exacte de groupes*

$$1 \mapsto \prod_{\ell\neq p} \mathbf{Z}_\ell(1) \to \mathrm{Gal}(K^{\mathrm{mod}}/K) \to \mathrm{Gal}(K^{\mathrm{nr}}/K) \to 1,$$

et l'action de $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ *sur le module galoisien* $\prod_{\ell\neq p} \mathbf{Z}_\ell(1)$ *est celle que l'on obtient en faisant agir* $\mathrm{Gal}(K^{\mathrm{mod}}/K)$ *par conjugaison.*