Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques.

Par Mademoiselle *Elisabeth Lutz* à Strasbourg.

Introduction.

Dans l'étude des points rationnels situés sur une courbe algébrique, à coefficients rationnels c'est plutôt le genre, que le degré de la courbe qui intervient. Poincaré [1]) a montré qu'une courbe de genre 1, qui admet un point rationnel peut être ramenée par une transformation birationnelle à coefficients rationnels à la forme canonique $y^2 = x^3 - Ax - B$. On uniformise habituellement la courbe, au moyen de la fonction de Weierstrass, par les formules $x = \wp u$, $y = \frac{1}{2}\wp' u$. Nous savons d'autre part que les arguments elliptiques u des points à coordonnées rationnelles situés sur la courbe forment un module par rapport à l'anneau des entiers ordinaires, et que celui-ci est de base finie [2]).

Il en résulte, que sur les courbes de genre 1, les points rationnels peuvent se déduire par des opérations rationnelles d'un nombre fini d'entre eux.

Mais si l'on considère les solutions (x, y), dans un corps k quelconque, de l'équation $y^2 = x^3 - Ax - B$ d'une cubique de genre 1 (A et B appartenant au corps k), tout ce qu'on sait en général, c'est que ces solutions forment un groupe abélien G [3]). Nous donnerons dans ce travail quelques résultats relatifs au cas où le corps k est un corps $\mathfrak{p}$-adique $k_\mathfrak{p}$. Suivant l'usage [4]), on désignera par $\mathfrak{p} = (\pi)$ l'idéal premier du corps $k_\mathfrak{p}$, par p le nombre premier rationnel qui est multiple de $\mathfrak{p}$; on aura $(p) = \mathfrak{p}^e$, e étant l'ordre de ramification de p dans $k_\mathfrak{p}$; si de plus $N(\mathfrak{p}) = p^f$, le degré de $k_\mathfrak{p}$ par rapport à k_p sera $d = ef$. Soit φ la valuation $\mathfrak{p}$-adique dans $k_\mathfrak{p}$, déterminée par exemple par la condition $\varphi(\pi) = w$ et on sait que l'on a $w < 1$. Alors, A et B étant des entiers de $k_\mathfrak{p}$ tels que $x^3 - Ax - B$ ait son discriminant $\neq 0$, nous étudions la courbe $y^2 = x^3 - Ax - B$, qui est de genre 1. Nous appellerons *point rationnel* sur la courbe tout point (x, y) de la courbe dont les coordonnées sont dans $k_\mathfrak{p}$, ou bien le point à l'infini de la courbe; ces points forment un groupe qui sera appelé G.

A tout point rationnel P de coordonnées (x, y), on fera correspondre le plus petit entier naturel $n = n(P)$ tel que $x\pi^{2n}$ et $y\pi^{3n}$ soient entiers; si P est le point à l'infini on pose $n(P) = +\infty$. Nous démontrerons d'abord que les points P pour lesquels $n(P) \geqq m$ forment un sous-groupe G_m de G, et que ce sous-groupe est d'indice fini. En introduisant, pour les points de G_1, une représentation paramétrique convenable, nous ferons voir en-

[1]) H. Poincaré, Sur les propriétés des courbes algébriques planes, Journal de Liouville (V) **7** (1901), p. 161.

[2]) L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. of the Cambridge Philos. Soc. **21** (1922), p. 179. Cf. aussi A. Weil, Sur un théorème de Mordell, Bull. Sc. Math. (II) **54** (1930), p. 182.

[3]) Cf. H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Hamb. Abhandl. **10** (1934), p. 325.

[4]) Cf. par exemple C. Chevalley, Sur la théorie des corps de classes, Journal of the Faculty of Science Tokyo **2** (1933).

suite que, dès que m est assez grand (et plus précisément, dès que $4m > e$), G_m est isomorphe au groupe additif des entiers de $k_\mathfrak{p}$; en même temps, nous démontrons que $n(P)$ satisfait aux relations:

$$n(p^r P) = n(P) + ve \qquad n(lP) = n(P) \text{ pour } l \text{ premier à } p$$

valables dès que $4n(P) > e$.

De ce qui précède résulte en particulier, que le point P ne peut être d'ordre fini (dans le groupe G) que si $4n(P) \leqq e$. *Si en particulier $k_\mathfrak{p}$ se réduit au corps p-adique k_p* (d'où $d = e = 1$), *tout point d'ordre fini est à coordonnées entières.* Il est intéressant d'observer qu'on déduit immédiatement de là le même resultat pour le corps des nombres rationnels, si A et B sont des entiers rationnels, tout point rationnel P d'ordre fini sur la cubique $y^2 = x^3 - Ax - B$ de genre 1 est à coordonnées entières.

Dans la deuxième partie nous retrouvons une partie des résultats précédent en définissant d'après A. Weil dans le corps $\mathfrak{p}$-adique, des fonctions analogues aux fonctions elliptiques de l'analyse ordinaire [5]).

Après avoir généralisé aux corps $\mathfrak{p}$-adiques le théorème de Cauchy sur l'existence des solutions d'un système d'équations différentielles, nous définissons au moyen d'un tel système les fonctions dont il s'agit. Elles permettent de démontrer à nouveau l'isomorphie du groupe G_m avec le groupe additif des entiers $\mathfrak{p}$-adiques dès que m est assez grand; et même la limite qu'on obtient pour m par cette méthode, est plus précise que celle que fournit le raisonnement direct, dans le cas où $p \geqq 7$.

Qu'il me soit permis d'exprimer ici ma sincère reconnaissance à M. A. Weil, pour l'aide qu'il m'a apportée au cours de ce travail.

§ 1. Etude algébrique du groupe G.

Le groupe abélien G formé par les points rationnels peut être défini de la manière suivante: à deux points rationnels $P_0(x_0, y_0)$, $P_1(x_1, y_1)$ nous ferons correspondre le point $P_2(x_2, y_2)$ symétrique par rapport à Ox du troisième point d'intersection de la droite P_0P_1 avec la cubique et nous écrirons $P_2 = P_0 + P_1$. On trouve facilement les coordonnées du point P_2 en fonction de celles des points P_0 et P_1; on a en particulier:

$$x_2 = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 - (x_1 + x_0).$$

Si P_1 se confond avec P_0 on prendra au lieu de la droite P_0P_1 la tangente en P_0 à la cubique et l'on écrira $2P_0 = P_2$, avec

$$x_2 = \left(\frac{3x_0^2 - A}{2y_0}\right)^2 - 2x_0.$$

Le point $-P_0$ sera le point de coordonnées $(x_0, -y_0)$ et le point à l'infini de la courbe étant considéré comme point rationnel, sera l'unité de notre groupe G.

Tout point rationnel P sur la courbe a des coordonnées de la forme $(\xi\pi^{-2n}, \eta\pi^{-3n})$ n étant un entier rationnel $\geqq 0$, ξ, η étant des entiers de $k_\mathfrak{p}$, *premiers à $\mathfrak{p}$ si $n > 0$.* En effet soit (x, y) un point rationnel: si x est entier $\mathfrak{p}$-adique, y l'est aussi. Si d'autre part $\varphi(x) > 1$, on aura

$\varphi(x^3) = [\varphi(x)]^3 > \varphi(Ax)$ et $\varphi(x^3) > \varphi(B)$ donc $\varphi(y^2) = \varphi(x^3 - Ax - B) = \varphi(x^3)$, en ce point nous avons donc:

$$\varphi(x) = w^{-2n} \qquad \varphi(y) = w^{-3n}, \qquad n > 0$$

de sorte que les coordonnées x, y sont bien de la forme

$$x = \xi\pi^{-2n} \qquad y = \eta\pi^{-3n}$$

[5]) A. Weil, Sur les fonctions elliptiques $\mathfrak{p}$-adiques, Comptes rendus Ac. des Sciences Paris **203** (1936).

avec ξ, η entiers premiers à $\mathfrak{p}$; et ξ, η satisfont à l'équation:

$$\eta^2 = \xi^3 - A\xi\pi^{4n} - B\pi^{6n}.$$

A tout point P correspond ainsi un entier $n \geqq 0$ bien déterminé qu'on désignera par $n(P)$; si P est le point à l'infini on posera $n(P) = \infty$.

Théorème I. *Les points P pour lesquels $n(P) \geqq m$ forment un sous-groupe G_m de G, d'indice fini dans G, quel que soit l'entier $m > 0$.*

Soient en effet deux points rationnels P_0 et P_1, et $P_2 = P_0 + P_1$; et supposons d'abord que $n(P_1) > n(P_0)$ donc $n(P_1) > 0$. Nous pouvons écrire la formule d'addition sous la forme:

$$x_2 = \frac{-A(x_0 + x_1) + x_1^2 x_0 + x_0^2 x_1 + 2y_1 y_0 - 2B}{(x_0 - x_1)^2}$$

d'où

$$\varphi(x_2) = \frac{\varphi(x_1^2 x_0)}{\varphi(x_1^2)} = \varphi(x_0)$$

et par suite:

$$n(P_0 + P_1) = \min[n(P_0), n(P_1)] \quad \text{si} \quad n(P_0) \neq n(P_1).$$

Nous aurions de même

$$n(P_0 - P_1) = \min[n(P_0), n(P_1)] \quad \text{si} \quad n(P_0) \neq n(P_1).$$

Supposons maintenant $n(P_0) = n(P_1)$; nous pouvons écrire $P_0 = P_2 - P_1$; si $n(P_2) \neq n(P_1)$ on aura

$$n(P_0) = \min[n(P_2), n(P_1)]$$

donc $n(P_2) \geqq n(P_0)$. *On a donc en tout cas*:

$$n(P_2) \geqq \min[n(P_0), n(P_1)]$$

ce qui montre bien que G_m est un sous-groupe de G.

Pour démontrer la seconde partie du théorème, nous devons examiner à quelles conditions deux points P_1, P_0 de G doivent satisfaire pour que $P_1 - P_0$ soit dans G_m, c'est-à-dire pour que $n(P_1 - P_0) \geqq m$; nous pouvons supposer que ni P_0 ni P_1 ne soient dans G_m; alors, on devra avoir, tout d'abord, $n(P_0) = n(P_1) = n < m$. Soient $(\xi_0\pi^{-2n}, \eta_0\pi^{-3n})$ et $(\xi_1\pi^{-2n}, \eta_1\pi^{-3n})$ les coordonnées de P_0 et P_1, avec:

$$\eta_0^2 = \xi_0^3 - A\xi_0\pi^{4n} - B\pi^{6n}, \qquad \eta_1^2 = \xi_1^3 - A\xi_1\pi^{4n} - B\pi^{6n}.$$

Il est clair, d'après la formule d'addition, que la condition nécessaire et suffisante pour que $n(P_1 - P_0) \geqq m$, si $n(P_0) = n(P_1) < m$, est que l'on ait:

$$\frac{x_1 - x_0}{y_1 + y_0} (\equiv 0 \bmod \mathfrak{p}^m);$$

c'est-à-dire:

$$\frac{\xi_1 - \xi_0}{\eta_1 + \eta_0} \equiv 0 \pmod{\mathfrak{p}^{m-n}}.$$

Or on a:

$$\frac{\xi_1 - \xi_0}{\eta_1 + \eta_0} = \frac{\eta_1 - \eta_0}{\xi_0^2 + \xi_1\xi_0 + \xi_1^2 - A\pi^{4n}}.$$

Une condition nécessaire, pour que $n(P_1 - P_0) \geqq m$, est donc que

$$\xi_1 \equiv \xi_0, \qquad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{m-n}}$$

et même cela est suffisant si $n > 0$, car alors, si $p \neq 2$,

$$\eta_1 + \eta_0 \equiv 2\eta_0 \not\equiv 0 \pmod{\mathfrak{p}}$$

et si $p \neq 3$,

$$\xi_0^3 + \xi_0\xi_1 + \xi_1^2 - A\pi^{4m} \equiv 3\xi_0^3 \not\equiv 0 \pmod{\mathfrak{p}}.$$

Il s'ensuit en particulier que G_{m-1}/G_m est un groupe fini, si $m > 1$, donc déjà que G_m est d'indice fini dans G_1. Reste à examiner G/G_1. Pour cela, nous allons faire voir que si $n(P_0) = n(P_1) = 0$, on peut trouver r assez grand pour que $n(P_1 - P_0) \geqq m$ dès que les congruences

$$\xi_1 \equiv \xi_0, \quad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{r+m}}$$

seront satisfaites.

En effet, si elles le sont et que $n(P_1 - P_0) < m$, on devra avoir, d'après ce qui précède:

$$\eta_1 + \eta_0 \equiv 0, \quad \xi_0^2 + \xi_0\xi_1 + \xi_1^2 - A \equiv 0 \pmod{\mathfrak{p}^r}.$$

On en déduit:

$$2\eta_0 \equiv 0, \quad 3\xi_0^2 - A \equiv 0 \pmod{\mathfrak{p}^r}.$$

Mais on a l'identité:

$$4A^3 - 27B^2 = (x^3 - Ax - B)\,P(x) + (3x^2 - A)\,Q(x)$$

où: $P(x) = -18Ax + 27B$ et $Q(x) = 6Ax^2 - 9Bx - 4A^2$ sont des polynômes à coefficients entiers; en y faisant $x = \xi_0$, on voit donc que

$$2(4A^3 - 27B^2) \equiv 0 \pmod{\mathfrak{p}^r}.$$

Si donc on désigne par $\mathfrak{p}^R$ la plus haute puissance de $\mathfrak{p}$ qui divise $2(4A^3 - 27B^2)$, on voit que les congruences

$$\xi_1 \equiv \xi_0, \quad \eta_1 \equiv \eta_0 \pmod{\mathfrak{p}^{r+m}}$$

entraînent bien que $n(P_1 - P_0) \geqq m$, pourvu qu'on ait pris $r > R$. Le théorème est ainsi complètement démontré.

Pour aller plus loin, il est utile de se servir d'une représentation paramétrique de la courbe; nous considérons la suivante:

$$x = \frac{1}{t^2}, \quad y = \frac{\varepsilon(t)}{t^3},$$

où $\varepsilon(t)$ est défini par

$$\varepsilon(t) = (1 - At^4 - Bt^6)^{\frac{1}{2}} = 1 + \sum_{\nu=2}^{\infty} \gamma_\nu t^{2\nu}$$

avec $\gamma_2 = -A/2$, $\gamma_3 = -B/2$, etc. Il est clair que si $t \equiv 0 \pmod{\mathfrak{p}^m}$ et si la série $\varepsilon(t)$ est convergente, les formules ci-dessus définissent un point P de la courbe, et que ce point appartient à G_m.

Or on sait que dans la série

$$(1 + u)^{\frac{1}{2}} = 1 + \tfrac{1}{2}u - \tfrac{1}{8}u^2 + \tfrac{1}{16}u^3 - \cdots$$

les dénominateurs des coefficients ne contiennent pas d'autre facteur premier que 2, et que le dénominateur du coefficient de u^ν divise $2^{2\nu}$. Il en résulte que la série $\varepsilon(t)$ converge, si $p \neq 2$, dès que $t \equiv 0 \pmod{\mathfrak{p}}$, et, si $p = 2$, dès que $t \equiv 0 \pmod{\mathfrak{p}^\mu}$, μ étant le plus petit entier plus grand que $\frac{e}{2}$; si $p \neq 2$ nous poserons $\mu = 1$, de sorte qu'en tout cas les formules ci-dessus définissent, pour $t \equiv 0 \pmod{\mathfrak{p}^\mu}$, un point de G_μ. Mais réciproquement, tout point P de G_μ correspond ainsi à une valeur de t, définie par les formules

$$t = \frac{x}{y}\,\varepsilon,$$

$$\varepsilon = \left(1 - \frac{A}{x^2} - \frac{B}{x^3}\right)^{\frac{1}{2}} = 1 + \sum_{\nu=2}^{\infty} \gamma_\nu x^{-\nu}$$

la série étant convergente pourvu que P appartienne à G_μ.

Soient maintenant P_0, P_1 deux points de G_μ, correspondant aux valeurs t_0, t_1, du paramètre t; posons $\varepsilon_0 = \varepsilon(t_0)$, $\varepsilon_1 = \varepsilon(t_1)$. Désignons encore par t_2 le paramètre du point $P_2 = P_0 + P_1$; nous allons calculer t_2 en fonction de t_0, t_1. On a d'abord:

$$\frac{y_1 - y_0}{x_1 - x_0} = \frac{\varepsilon_1 t_0^3 - \varepsilon_0 t_1^3}{t_0 t_1 (t_0^2 - t_1^2)} = \frac{t_0^3 - t_1^3 + t_0^3 t_1^3 \sum_{\nu=2}^{\infty}{}' \gamma_\nu (t_1^{2\nu-3} - t_0^{2\nu-3})}{t_0 t_1 (t_0^2 - t_1^2)} = \frac{t_0^2 + t_0 t_1 + t_1^2 - t_0^3 t_1^3 \theta}{t_0 t_1 (t_0 + t_1)}$$

en posant:

$$\theta = \sum_{\nu=2}^{\infty}{}' \gamma_\nu \frac{t_1^{2\nu-3} - t_0^{2\nu-3}}{t_1 - t_0}.$$

Alors la formule d'addition pour x s'écrit:

$$x_2 = \frac{1}{t_2^2} = \frac{1}{(t_0 + t_1)^2} [1 - 2 t_0 t_1 (t_0^2 + t_0 t_1 + t_1^2)\, \theta + t_0^4 t_1^4 \theta^2].$$

L'ambiguité de signe pour t_2 se lève aisément en considérant aussi y_2; et l'on obtient:

$$\frac{t_2}{t_0 + t_1} = [1 - 2 t_0 t_1 (t_0^2 + t_0 t_1 + t_1^2)\, \theta + t_0^4 t_1^4 \theta^2]^{-\frac{1}{2}}$$

le second membre réprésentant le développement en série qui lui correspond au moyen de la formule du binôme, pourvu que ce développement soit convergent: il en est évidemment ainsi pour $p \neq 2$, car alors θ est entier, et l'on obtient, dans ce cas:

$$\frac{t_2}{t_0 + t_1} \equiv 1 \pmod{\mathfrak{p}^{3n(P_0) + n(P_1)}}$$

en supposant par exemple $n(P_0) \leqq n(P_1)$. On a donc à fortiori, pour $p \neq 2$, chaque fois que P_0, P_1 appartiennent tous deux à G_m:

$$t_2 \equiv t_0 + t_1 \pmod{\mathfrak{p}^{5m}}$$

et en particulier, par récurrence sur l:

$$t(lP_0) \equiv l \cdot t(P_0) \pmod{\mathfrak{p}^{5m}}$$

d'où, pour $l = p$, et si $n(P_0) = n$:

$$\frac{t(pP_0)}{pt(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n-e}}$$

et par récurrence sur ν:

$$\frac{t(p^\nu P_0)}{p^\nu t(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n-e}}$$

donc enfin, en combinant les résultats ci-dessus:

$$\frac{t(lP_0)}{lt(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4n-e}}$$

quel que soit l. Il en résulte en particulier que, si $4n(P_0) > e$, l'on aura, si p^ν est la plus haute puissance de p contenue dans l:

$$n(lP_0) = n(P_0) + \nu e.$$

Soit donc, pour $p \neq 2$, α le plus petit entier plus grand que $\frac{e}{4}$; de ce qui précède résulte évidemment que, si P_0 appartient à G_α, et si la suite d'entiers ordinaires l_i converge p-adiquement vers un entier p-adique L, les nombres $t(l_i P_0)$ convergeront p-adiquement vers une certaine valeur de t: le point de la courbe qui correspond à celle-ci sera désigné par $L \cdot P_0$; et l'on voit ainsi que G_α peut être considéré comme un module par rapport à l'anneau des entiers p-adiques.

Pour $p = 2$, on a des résultats semblables, mais un peu moins précis. Une évaluation facile montre que l'on a, si P_0 et P_1 appartiennent à G_m, et pourvu que $m \geqq e$:

$$t_2 \equiv t_0 + t_1 \pmod{\mathfrak{p}^{5m-2e}}$$

résultat qu'on pourrait d'ailleurs encore améliorer quelque peu. On en déduit, comme plus haut:

$$t(lP_0) \equiv lt(P_0) \pmod{\mathfrak{p}^{5m-2e}}$$

$$\frac{t(2P_0)}{2t(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4m(P_0)-3e}}$$

$$\frac{t(lP_0)}{lt(P_0)} \equiv 1 \pmod{\mathfrak{p}^{4m(P_0)-3e}}$$

et si 2^r est la plus haute puissance de 2 qui divise l:

$$n(lP_0) = n(P_0) + re$$

pourvu que $n(P_0) \geqq e$. En posant $\alpha = e$ pour $p = 2$, il en résulte, comme plus haut, que G_α peut être considéré comme module par rapport à l'anneau des entiers p-adiques. De là on déduit aussitôt la structure de G_α; plus généralement, on a le théorème suivant.

Théorème II. *Soit β un entier $> \frac{e}{4}$, si $p \neq 2$, et $\geqq e$ si $p = 2$. Alors G_β est isomorphe au groupe additif des entiers $\mathfrak{p}$-adiques.*

Il suffit de faire voir que G_β possède une base de $d = ef$ éléments indépendants par rapport à l'anneau des entiers p-adiques. Pour cela, choisissons, parmi les valeurs de t qui sont $\equiv 0 \pmod{\mathfrak{p}^\beta}$, f valeurs $t_1^{(0)}, t_2^{(0)}, \ldots, t_f^{(0)}$ formant une base minima de $\mathfrak{p}^\beta/\mathfrak{p}^{\beta+1}$; et de même choisissons pour $\varrho = 1, 2, \ldots, e-1$, des valeurs $t_1^{(\varrho)}, t_2^{(\varrho)}, \ldots, t_f^{(\varrho)}$ qui soient $\equiv 0 \pmod{\mathfrak{p}^{\beta+\varrho}}$ et formant une base minima de $\mathfrak{p}^{\beta+\varrho}/\mathfrak{p}^{\beta+\varrho+1}$. Soient $P_i^{(\varrho)}$ les points correspondant à ces ef valeurs de t; et soit $t_i^{(\varrho+\nu e)}$ la valeur t du paramètre, qui correspond au point $P_i^{(\varrho+\nu e)} = p^\nu P_i^{(\varrho)}$. Soient P_0 un point quelconque de G_β, et t_0 son paramètre; il y aura des entiers $n_i^{(0)}$, bien déterminés mod p, tels que

$$t_0 \equiv \sum_i n_i^{(0)} t_i^{(0)} \pmod{\mathfrak{p}^{\beta+1}};$$

alors le point $P_1 = P_0 - \Sigma n_i^{(0)} P_i^{(0)}$ appartiendra à $G_{\beta+1}$, et, s'il correspond à la valeur t_1 du paramètre, il y aura des entiers $n_i^{(1)}$, bien déterminés mod p, tels que

$$t_1 \equiv \sum_i n_i^{(1)} t_i^{(1)} \pmod{\mathfrak{p}^{\beta+2}};$$

en continuant ainsi, on voit que le point

$$P_n = P_0 - \sum_{\nu=0}^{n-1} \sum_i n_i^{(\nu)} P_i^{(\nu)}$$

appartient à $G_{\beta+1}$; et l'on a donc:

$$P_0 = \sum_{\varrho=0}^{e-1} \sum_{i=1}^{f} P_i^{(\varrho)} \left[\sum_{\nu=0}^{\infty} n_i^{(\varrho+\nu e)} p^\nu \right],$$

on voit en même temps que cette expression de P_0 est unique, de sorte que le théorème est démontré.

Une conséquence intéressante des résultats ci-dessus, c'est qu'un point P de G ne peut être d'ordre fini dans G s'il appartient à G_β; en particulier, *si $e = 1$, un point P d'ordre fini dans G est à coordonnées entières.*

Si maintenant nous considérons les solutions, *dans le corps des nombres rationnels ordinaires*, d'une équation $y^2 = x^3 - Ax - B$ à coefficients entiers rationnels, elles

forment un groupe qui est contenu dans le groupe des solutions p-adiques de la même équation, et cela quel que soit p. Une solution en nombres rationnels ne peut donc être d'ordre fini que si x et y sont entiers dans tout corps p-adique, c'est-à-dire s'ils sont entiers rationnels. Cela étant, la détermination effective de ces solutions est fournie par le théorème suivant:

Théorème III. *Soit $y^2 = x^3 - Ax - B$ une cubique de genre 1 à coefficients entiers rationnels. Tout point $P(x, y)$ à coordonnées rationnelles, et d'ordre fini dans le groupe des points rationnels sur la cubique, est à coordonnées entières, et tel que y^2 soit égal à 0 ou à un diviseur de $4A^3 - 27B^2$.*

La première partie étant déjà démontrée, considérons le second point. Si P est d'ordre fini, il en est de même de $2P$, qui doit donc être aussi à coordonnées entières s'il n'est à l'infini; ce dernier cas se présente si $y = 0$; s'il n'en est pas ainsi il faut et il suffit, pour qu'il soit à coordonnées entières, que l'on ait:

$$3x^2 - A \equiv 0 \pmod{2y}.$$

Mais on a l'identité:

$$(3x^2 - A)^2 (3x^2 - 4A) \equiv -4A^3 + 27B^2 \pmod{x^3 - Ax - B}$$

et par conséquent, dans le cas présent:

$$-4A^3 + 27B^2 \equiv 0 \pmod{y^2}$$

ce qu'il fallait démontrer.

§ 2. Les fonctions elliptiques $\mathfrak{p}$-adiques.

On peut obtenir une partie des résultats précédents par une autre méthode en utilisant les fonctions elliptiques $\mathfrak{p}$-adiques définies par A. Weil [5]). Nous allons reprendre cette définition, en l'étendant au cas $p = 2$.

Nous définirons d'une façon formelle la dérivée d'une fonction développée en série entière: par le développement dérivé, ceci est possible puisque ce développement est convergent dans le corps $\mathfrak{p}$-adique dès que le premier l'est. Dans ces conditions les propriétés habituelles de la dérivation sont encore valables.

Nous commencerons par donner une démonstration générale du théorème d'existence des solutions d'un système d'équations différentielles dans le corps $\mathfrak{p}$-adique, théorème que l'on peut énoncer de la manière suivante.

Théorème IV. *Soit un système d'équations différentielles*

$$\frac{dy_i}{dx} = F_i(x, y_1, y_2, \ldots, y_n) \qquad (i = 1, 2, \ldots, n) \tag{1}$$

les F_i étant des séries de puissances en $x, y_1, \ldots, y_n$ à coefficients dans $k_\mathfrak{p}$ convergentes dans un certain voisinage $\mathfrak{p}$-adique de $x = y_i = 0$. Ce système admet une solution et une seule de la forme $y_i = f_i(x)$ telle que $f_i(0) = 0$, les f_i étant des séries de puissances de x convergentes dans un certain voisinage de $x = 0$.

Posons en effet:

$$F_i(x, y_1, \ldots, y_n) = \sum a^{(i)}_{\mu\nu_1\ldots\nu_n} x^\mu y_1^{\nu_1} \cdots y_n^{\nu_n}$$

les coefficients a étant des nombres de $k_\mathfrak{p}$.

Le deuxième membre, série entière par rapport aux puissances positives croissantes de x et des y_i, est supposé convergent dans le corps $\mathfrak{p}$-adique dès que:

$$x \equiv 0 \pmod{\mathfrak{p}^\alpha}, \qquad y_i \equiv 0 \pmod{\mathfrak{p}^{\beta_i}}. \tag{2}$$

Dans chacune des séries F_i, tous les termes, sauf un nombre fini d'entre eux, sont des entiers $\mathfrak{p}$-adiques dès que x et y satisfont à (2), ou en d'autres termes les nombres

$$a^{(i)}_{\mu\nu_1\dots\nu_n}\pi^{\mu\alpha+\nu_1\beta_1+\cdots+\nu_n\beta_n}$$

sont entiers à l'exception au plus d'un nombre fini d'entre eux; et par suite on peut trouver ϱ_i tels que ces nombres deviennent entiers si on les multiplie par π^{ϱ_i}.

Faisons alors dans les équations proposées la transformation:

$$x = \pi^\nu x', \quad y_i = \pi^{\beta_i} y'.$$

Les coefficients des nouvelles équations seront

$$a^{(i)}_{\mu\nu_1\nu_2\dots\nu_n}\pi^{\gamma-\beta_i+\mu\gamma+\nu_1\beta_1+\cdots+\nu_n\beta_n}$$

et ils seront tous entiers si l'on prend pour γ le plus grand des nombres $\alpha, \beta_i + \varrho_i$.

Nous sommes donc ramenés au cas où tous les coefficients des séries F_i sont entiers.

Or les équations (1) nous permettent par différentiations successives de calculer formellement les dérivées d'un ordre quelconque de y_i par rapport à x pour $x = 0$, qui seront des polynômes à coefficients numériques entiers par rapport aux coefficients $a^{(i)}_{\mu\nu_1\dots\nu_n}$ des séries F_i; les séries

$$y_i = \left(\frac{dy_i}{dx}\right)_0 x + \left(\frac{d^2y_i}{dx^2}\right)_0 \frac{x^2}{2!} + \cdots + \left(\frac{d^ny_i}{dx^n}\right)_0 \frac{x^n}{n!} + \cdots \tag{3}$$

satisfont formellement aux équations (1). Mais elles convergent en même temps que la série exponentielle c'est-à-dire pour $x \equiv 0 \pmod{\mathfrak{p}^\varrho}$ si $\varrho > \frac{e}{p-1}$. Le théorème est donc démontré.

Ce résultat va nous permettre de définir dans le corps $\mathfrak{p}$-adique $k_\mathfrak{p}$ des fonctions analogues aux fonctions elliptiques de l'analyse ordinaire. Habituellement on exprime les coordonnées x, y d'un point de la courbe $y^2 = x^3 - Ax - B$ par les formules $x = \wp u$, $y = \frac{1}{2}\wp' u$; pour obtenir une représentation semblable dans $k_\mathfrak{p}$ le plus commode sera de se servir de la fonction auxiliaire $t(u) = (\wp u)^{-\frac{1}{2}}$ qui n'est pas autre chose que le paramètre t dont nous nous sommes servis au § 1; en analyse ordinaire cette fonction satisfait à l'équation différentielle

$$\frac{dt}{du} = (1 - At^4 - Bt^6)^{\frac{1}{2}}.$$

Plaçons-nous maintenant dans le corps $\mathfrak{p}$-adique, et considérons l'équation différentielle

$$\frac{dt}{du} = (1 - At^4 - Bt^6)^{\frac{1}{2}} = 1 + \sum_{\nu=2}^{\infty} \gamma_\nu t^{2\nu}.$$

D'après le théorème IV, cette équation définit une fonction $t(u)$ telle que $t(0) = 0$, développable suivant les puissances entières de u:

$$t(u) = \sum_1^\infty \frac{1}{\nu!}\left(\frac{d^\nu t}{du^\nu}\right)_0 u^\nu = u - \frac{A}{10}u^5 - \frac{B}{14}u^7 + \cdots$$

le développement étant convergent dans un voisinage de $u = 0$ qu'il est facile de déterminer. En effet, soit ϱ, comme plus haut, le plus petit entier $> \frac{e}{p-1}$; si $p \neq 2$ l'équation différentielle est à coefficients entiers, et la série $t(u)$ converge pour $u \equiv 0 \pmod{\mathfrak{p}^\varrho}$; si $p \neq 2$ on transformera l'équation différentielle en une équation à coefficients entiers

par le changement de variables $t = \pi^\lambda t'$, $u = \pi^\lambda u'$ si λ est le plus petit entier $\geqq \frac{e}{2}$, donc la série $t'(u')$ converge pour $u' \equiv 0 \pmod{\mathfrak{p}^e}$, et $t(u)$ converge pour $u \equiv 0 \pmod{\mathfrak{p}^{e+\lambda}}$.

De plus, considérons, pour $p \neq 2$, la série

$$\frac{t(u)}{u} - 1 = \sum_{3}^{\infty} \frac{1}{\nu!} \left(\frac{d^\nu t}{du^\nu}\right)_0 u^{\nu-1}$$

on vérifie facilement que tous ses termes sont $\equiv 0 \pmod{\mathfrak{p}}$ pourvu que $u \equiv 0 \pmod{\mathfrak{p}^{\varrho'}}$, ϱ' désignant le plus petit entier tel que

$$\varrho' > \frac{p^2 e}{(p^2-1)(p-1)}$$

et de même, pour $p = 2$, la série $\frac{t'(u')}{u'} - 1$ a tous ses termes $\equiv 0 \pmod{\mathfrak{p}}$ si $u' \equiv 0 \pmod{\mathfrak{p}^{\varrho'}}$, ϱ' étant le plus petit entier $> \frac{9e}{8}$. Désignons donc par σ l'entier ϱ' si $p \neq 2$ et l'entier $\varrho' + \lambda$ si $p = 2$; on voit qu'en tout cas, si

$$u \equiv 0 \pmod{\mathfrak{p}^\sigma}$$

la fonction $t(u)$ est définie et telle que

$$\frac{t(u)}{u} \equiv 1 \pmod{\mathfrak{p}}.$$

A partir de cette fonction $t(u)$, nous pouvons maintenant, pour $u \equiv 0 \pmod{\mathfrak{p}^\sigma}$, définir les fonctions

$$\wp u = \frac{1}{t^2(u)}, \qquad \wp' u = \frac{-2\,dt}{t^3(u)\,du}$$

qui satisfont évidemment à l'équation

$$\frac{1}{4}\wp'^2 u = \wp^3 u - A\wp u - B$$

de sorte que le point

$$x = \wp u, \qquad y = \frac{1}{2}\wp' u$$

est un point de la courbe $y^2 = x^3 - Ax - B$, et plus précisément un point du groupe G_m si $u \equiv 0 \pmod{\mathfrak{p}^m}$ et $m \geqq \sigma$. Et réciproquement, tout point de G_m correspond ainsi à une valeur de u et une seule; car on a vu dans le § 1 qu'à tout point P de G_m correspond, si $m \geqq \mu$ (avec $\mu = 1$ pour $p \neq 2$ et μ étant le plus petit entier $> \frac{e}{2}$ si $p = 2$) une valeur de t bien déterminée, $\equiv 0 \pmod{\mathfrak{p}^m}$; alors u est déterminé au moyen de t par l'équation

$$\frac{du}{dt} = (1 - At^4 - Bt^6)^{-\frac{1}{2}}$$

d'où

$$u(t) = \int_0^t (1 - At^4 - Bt^6)^{-\frac{1}{2}}\,dt = t + \frac{A}{10}t^5 + \frac{B}{14}t^7 + \cdots$$

et l'on vérifie immédiatement que la série $u(t)$ est convergente, et a tous ses termes, à partir du second, $\equiv 0 \pmod{\mathfrak{p}^\sigma}$, pour $t \equiv 0 \pmod{\mathfrak{p}^\sigma}$.

Enfin, considérons le théorème d'addition auxquelles satisfont, en analyse ordinaire, $\wp u$ et $\wp' u$: ce théorème s'exprime par des identités algébriques auxquelles satisfont les coefficients du développement en série de $t(u)$, coefficients qui sont des polynômes en A, B à coefficients numériques rationnels; il reste donc valable en analyse $\mathfrak{p}$-adique. On en déduit que si les points P_0, P_1 de G correspondent aux valeurs u_0, u_1 du paramètre u, le point $P_2 = P_0 + P_1$ correspond à $u_2 = u_0 + u_1$. *Il y a donc isomorphie entre G_a et le groupe additif des nombres $u \equiv 0 \pmod{\mathfrak{p}^\sigma}$*: c'est là un résultat moins précis que celui du théorème II pour $p = 2, 3, 5$, mais plus précis dès que $p \geqq 7$.

Eingegangen 28. Dezember 1936.