

Comptes rendus  
hebdomadaires des séances  
de l'Académie des sciences /  
publiés... par MM. les  
secrétaires perpétuels

Académie des sciences (France). Auteur du texte. Comptes rendus hebdomadaires des séances de l'Académie des sciences / publiés... par MM. les secrétaires perpétuels. 1936-07-01.

**1/** Les contenus accessibles sur le site Gallica sont pour la plupart des reproductions numériques d'oeuvres tombées dans le domaine public provenant des collections de la BnF. Leur réutilisation s'inscrit dans le cadre de la loi n°78-753 du 17 juillet 1978 :

- La réutilisation non commerciale de ces contenus ou dans le cadre d'une publication académique ou scientifique est libre et gratuite dans le respect de la législation en vigueur et notamment du maintien de la mention de source des contenus telle que précisée ci-après : « Source gallica.bnf.fr / Bibliothèque nationale de France » ou « Source gallica.bnf.fr / BnF ».

- La réutilisation commerciale de ces contenus est payante et fait l'objet d'une licence. Est entendue par réutilisation commerciale la revente de contenus sous forme de produits élaborés ou de fourniture de service ou toute autre réutilisation des contenus générant directement des revenus : publication vendue (à l'exception des ouvrages académiques ou scientifiques), une exposition, une production audiovisuelle, un service ou un produit payant, un support à vocation promotionnelle etc.

[CLIQUER ICI POUR ACCÉDER AUX TARIFS ET À LA LICENCE](#)

**2/** Les contenus de Gallica sont la propriété de la BnF au sens de l'article L.2112-1 du code général de la propriété des personnes publiques.

**3/** Quelques contenus sont soumis à un régime de réutilisation particulier. Il s'agit :

- des reproductions de documents protégés par un droit d'auteur appartenant à un tiers. Ces documents ne peuvent être réutilisés, sauf dans le cadre de la copie privée, sans l'autorisation préalable du titulaire des droits.

- des reproductions de documents conservés dans les bibliothèques ou autres institutions partenaires. Ceux-ci sont signalés par la mention Source gallica.BnF.fr / Bibliothèque municipale de ... (ou autre partenaire). L'utilisateur est invité à s'informer auprès de ces bibliothèques de leurs conditions de réutilisation.

**4/** Gallica constitue une base de données, dont la BnF est le producteur, protégée au sens des articles L341-1 et suivants du code de la propriété intellectuelle.

**5/** Les présentes conditions d'utilisation des contenus de Gallica sont régies par la loi française. En cas de réutilisation prévue dans un autre pays, il appartient à chaque utilisateur de vérifier la conformité de son projet avec le droit de ce pays.

**6/** L'utilisateur s'engage à respecter les présentes conditions d'utilisation ainsi que la législation en vigueur, notamment en matière de propriété intellectuelle. En cas de non respect de ces dispositions, il est notamment passible d'une amende prévue par la loi du 17 juillet 1978.

**7/** Pour obtenir un document de Gallica en haute définition, contacter [utilisation.commerciale@bnf.fr](mailto:utilisation.commerciale@bnf.fr).

## CORRESPONDANCE.

M. le **SECRÉTAIRE PERPÉTUEL** signale parmi les pièces imprimées de la Correspondance :

Les douze premiers volumes du *Recueil des Travaux de l'Institut de Chimie biologique de la Faculté de Médecine de Strasbourg*, dirigé par M. **MAURICE NICLOUX**.

THÉORIE DES NOMBRES. — *Les solutions de l'équation  $y^2 = x^3 - Ax - B$  dans les corps  $p$ -adiques*. Note de M<sup>lle</sup> **ÉLISABETH LUTZ**, présentée par M. Élie Cartan.

Les points à coordonnées rationnelles situés sur une cubique de genre 1,  $y^2 = x^3 - Ax - B$ ,  $A$  et  $B$  étant des nombres rationnels, forment, en vertu des formules d'addition des fonctions elliptiques, un groupe abélien  $G$ ; Mordell a démontré d'ailleurs que  $G$  est de base finie <sup>(1)</sup>. Si, plus généralement, on suppose que  $A$  et  $B$  appartiennent à un corps quelconque  $k$ , et qu'on veuille étudier les solutions  $(x, y)$  appartenant à  $k$ , celles-ci formeront encore un groupe abélien  $G$  <sup>(2)</sup>.

Nous donnerons ici quelques résultats relatifs au cas où le corps  $k$  est un corps de nombres  $p$ -adiques  $k_p$ ; comme d'habitude, on désignera par  $\mathfrak{p} = (\pi)$  l'idéal premier (unique) du corps  $k_p$ , 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  $k_p$ ; nous supposerons  $p \neq 2$ . Nous supposons, d'autre part, que  $A$  et  $B$  sont des entiers de  $k_p$  tels que  $x^3 - Ax - B$  n'ait pas, dans  $k_p$ , de racine double; la courbe  $y^2 = x^3 - Ax - B$  est alors de genre 1. Les points sur la courbe dont les coordonnées sont des nombres de  $k_p$  seront appelés *points rationnels* sur la courbe; et l'on considérera également comme tel le point à l'infini de la cubique.

Le groupe abélien  $G$  formé par les points rationnels peut être défini de la manière suivante : à deux points rationnels  $P, Q$  nous ferons correspondre le point  $R$  symétrique par rapport à  $Ox$  du troisième point d'intersection de la cubique avec la droite  $PQ$ , et nous écrirons  $R = P + Q$ ; si  $Q$  se confond avec  $P$ , on prendra, au lieu de  $PQ$ , la tangente en  $P$  à la cubique,

<sup>(1)</sup> MORDELL, *Proc. Cambridge Phil. Soc.*, 21, 1922, p. 179; cf. aussi A. WEIL, *Bull. Sc. Math.*, 2<sup>e</sup> série, 54, 1930, p. 182.

<sup>(2)</sup> Cf. H. HASSE, *Hamb. Abhandl.*, 10, 1934, p. 325.

et l'on écrira  $R = 2P$ . L'unité du groupe  $G$  est le point à l'infini de la courbe. Les formules donnant les coordonnées de  $R$  au moyen de celles de  $P$  et  $Q$  ne sont autres que les formules d'addition (ou, si  $P$  et  $Q$  se confondent, de duplication) des fonctions elliptiques.

On démontre facilement que tout point rationnel  $P$  sur la courbe a des coordonnées de la forme  $(\xi\pi^{-2n}, \eta\pi^{-3n})$ ,  $n$  étant un entier rationnel  $\geq 0$ , et  $\xi, \eta$  étant des entiers de  $k_p$  premiers à  $p$  si  $n \neq 0$ ; à tout point  $P$  correspond ainsi un entier  $n \geq 0$  bien déterminé, qu'on désignera par  $n(P)$ ; si  $P$  est le point à l'infini, on posera  $n(P) = \infty$ . Cela posé, il résulte des formules d'addition que *les points  $P$  pour lesquels  $n(P) \geq m$  forment un sous-groupe  $G_m$  de  $G$  quel que soit l'entier  $m > 0$* . En exprimant les conditions auxquelles doivent satisfaire  $P$  et  $Q$  pour que  $n(P - Q) \geq m$ , on trouve de plus que *le groupe-quotient  $G/G_m$  est fini quel que soit  $m > 0$* .

Pour aller plus loin, il est commode de se servir d'une représentation paramétrique du groupe  $G_1$ . Soit  $P = (x, y)$  un point de  $G_1$ ; on aura  $x = \xi\pi^{-2n}$ ,  $y = \eta\pi^{-3n}$ , où  $n \geq 1$  et  $\xi, \eta$  sont premiers à  $p$ ; on aura donc  $\eta^2 = \xi^3 - A\xi\pi^{4n} - B\pi^{6n}$ , d'où  $\eta^2 \equiv \xi^3 (p^{4n})$ ;  $\xi$  est donc résidu quadratique modulo  $p$ , et, puisque  $p \neq 2$ , il y aura un entier  $p$ -adique  $\tau$  (et un seul) tel que  $\tau^2 \equiv \xi$ ,  $\tau^3 \equiv \eta (p^{4n})$ . Si alors on pose  $t = \pi^n/\tau$ , on aura  $x \equiv t^{-2}$  et  $y \equiv t^{-3} (p^n)$ ; à tout point  $P$  de  $G_1$  correspond ainsi un entier  $t$  et un seul, qu'on désignera par  $t(P)$ ; et à tout entier  $t \equiv 0 (p)$  correspond un point de  $G_1$ . On déduit alors des formules d'addition les congruences suivantes :

$$1^\circ \text{ si } n(P) = n, n(Q) \geq n,$$

$$\frac{t(P+Q)}{t(P)+t(Q)} \equiv 1 \quad (p^{4n});$$

$$2^\circ \text{ si } n(P) = n,$$

$$t(kP) \equiv k.t(P) \quad (p^{5n}) \text{ quel que soit } k;$$

$$3^\circ \text{ si } n(P) = n,$$

$$\frac{t(kP)}{k.t(P)} \equiv 1 \quad (p^{4n-e}) \text{ quel que soit } k.$$

Il en résulte en particulier que si  $4n(P) > e$ , l'on aura  $n(kP) = n(P)$  pour  $k$  premier à  $p$ , et  $n(p^v P) = n(P) + ve$ ; et qu'alors, si les  $k_i$  forment une suite d'entiers ordinaires convergeant  $p$ -adiquement vers un entier  $p$ -adique  $K$ , les  $t(k_i P)$  convergeront  $p$ -adiquement vers un entier  $T$  : le point correspondant à  $T$  sera désigné par  $KP$ . Soit alors  $a$  le plus petit entier naturel tel que  $4a > e$ ; on déduit facilement de ce qui précède la structure du groupe  $G_a$  :  $G_a$  peut en effet être considéré comme module par rapport au groupe des entiers  $p$ -adiques, et, comme tel, on trouve qu'il



possède une base de  $d$  éléments,  $d$  étant le degré de  $k_p$  par rapport au corps  $p$ -adique  $k_p$ ; autrement dit,  $G_a$  est un produit direct de  $d$  groupes isomorphes au groupe additif des entiers  $p$ -adiques.

De ce qui précède résulte en particulier que le point  $P$  ne peut être d'ordre fini (dans le groupe  $G$ ) si  $4n(P) > e$ . Si en particulier  $k_p$  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 que le même résultat subsiste pour le corps des nombres rationnels : si  $A$  et  $B$  sont des entiers rationnels, tout point rationnel  $P$  d'ordre fini, sur la cubique de genre 1  $y^2 = x^3 - Ax - B$ , est à coordonnées entières; en appliquant ce résultat à la fois à  $P$  et à  $2P$ , on trouve que pour un tel point l'entier  $y$  doit être un diviseur du discriminant  $4A^3 - 27B^2$ , d'où l'on déduit aisément, pour toute équation donnée de cette forme, la détermination complète des solutions d'ordre fini.

THÉORIE DES NOMBRES. — *Sur les fonctions elliptiques  $p$ -adiques.*

Note de M. **ANDRÉ WEIL**, présentée par M. Élie Cartan.

On peut retrouver une partie des résultats contenus dans la Note ci-dessus de M<sup>lle</sup> E. Lutz par une autre voie, en uniformisant la courbe  $y^2 = x^3 - Ax - B$ , dans le corps  $p$ -adique, au moyen de développements en série formellement identiques à ceux des fonctions elliptiques en analyse ordinaire. On uniformise habituellement la courbe au moyen de la fonction de Weierstrass, par les formules  $x = pu$ ,  $y = p'u/2$ ; mais ces fonctions se prêtent mal à des développements en série autour de l'origine qu'on puisse aisément généraliser au cas  $p$ -adique; et l'on a vu dans la Note de M<sup>lle</sup> Lutz comment l'étude arithmétique du problème conduit à introduire le paramètre  $t = x^{-\frac{1}{2}}$ . Nous allons donc montrer comment on peut étendre aux corps  $p$ -adiques la définition de la fonction  $\varphi(u) = [pu]^{-\frac{1}{2}}$ ; cette fonction satisfait à l'équation différentielle

$$(1) \quad \varphi'(u) = \frac{d\varphi}{du} = \sqrt{1 - A\varphi^4 - B\varphi^6},$$

ou encore

$$(2) \quad du = \frac{d\varphi}{\sqrt{1 - A\varphi^4 - B\varphi^6}},$$

et au moyen de cette fonction les coordonnées  $x, y$  d'un point de la courbe