Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Yvette Amice

Analyse p-adique

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 1 (1959-1960), exp. n° 4, p. 1-63

<http://www.numdam.org/item?id=SDPP_1959-1960__1__A3_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
1re année, 1959/60, n° 4

ANALYSE p-ADIQUE (*)

par Mme Yvette AMICE

I. Corps Q_p des nombres p-adiques.

A. Valeurs absolues de Q . Théorème d'Ostrowski.

Définition. - Une valeur absolue sur un corps K est une fonction $|a|$ à valeurs réelles positives, définie $\forall\ a \in K$, telle que :

(1) $\quad |a| = 0 \iff a = 0$,

(2) $\quad |ab| = |a||b|$, $\forall\ a , b \in K$,

(3) $\quad |a + b| \leqslant |a| + |b|$, $\forall\ a , b \in K$.

A une valeur absolue sur un corps K , on peut associer une distance en posant $d(x , y) = |y - x|$, la topologie induite par cette distance étant appelée topologie induite par la valeur absolue donnée.

Nous allons chercher toutes les valeurs absolues du corps Q des rationnels. Il est clair, grâce à l'axiome (2), qu'il suffit de définir $|a|$ pour $a \in Z^+$, ensemble des entiers positifs, pour qu'elle s'étende immédiatement à Q .

THÉORÈME 1 (OSTROWSKI). - Soit $|a|$ une valeur absolue définie sur Q , non identique à 1 sur Q^* .

1° S'il existe $b \in Z^+$, $b \neq 1$, tel que $|b| \leqslant 1$, alors $|a| \leqslant 1$, $\forall\ a \in Z^+$ et il existe p premier tel que $|p| = \omega < 1$.

Alors quel que soit $a \in Z^+$, $a = p^\lambda a'$, $\lambda \in Z^+$, $(a' , p) = 1$, $|a| = \omega^\lambda$.

2° S'il existe $b \in Z^+$ tel que $|b| > 1$, il existe α réel, $0 < \alpha \leqslant 1$ tel que $|a| = a^\alpha$, $\forall\ a \in Z^+$.

(*) Ce texte, rédigé par Mme Y. AMICE, en tenant compte des conférences faites par C. PISOT à Philadelphie, résume et complète les exposés faits par elle-même, par J.-J. PAYAN et par Marc KRASNER dans le cadre du Séminaire Delange-Pisot : Théorie des nombres, 1959/60.

Conséquence. - Il résulte de ce théorème qu'une valeur absolue sur Q est :

- soit la valeur absolue triviale : $|a| = 1$ pour $a \neq 0$, $|a| = 0$ si $a = 0$,
- soit associée à un nombre premier p (1°),
- soit associée à un nombre réel α (2°),

car soit $b > 1$, $b \in Z^+$, si $|b| \leqslant 1$ la valeur absolue est soit triviale, soit du premier type, si $|b| > 1$ elle est du second type.

Démonstration. - Remarquons tout d'abord que (1) $\Longrightarrow |1| = 1$. On a d'autre part les propriétés immédiates :

(i) $\forall\ a \in Z^+$, $|a| \leqslant a$, car $|a| = |a - 1 + 1| \leqslant |a - 1| + 1$,

(ii) si $p \in Z^+$, tout $a \in Z^+$ s'écrit de manière unique dans le système de base p :

$$a = a_0 + a_1 p + \ldots + a_h p^h \quad \text{où} \quad 0 \leqslant a_i < p \quad \text{et} \quad p^h \leqslant a < p^{h+1} .$$

Soit alors $\nu \in Z^+$ et $a^\nu = a'_0 + \ldots + a'_{h_\nu} p^{h_\nu}$, on a

$$h\nu \leqslant h_\nu < (h + 1)\nu .$$

1° a. S'il existe $b \neq 1$ tel que $|b| \leqslant 1 \Longrightarrow |a| \leqslant 1$, $\forall\ a \in Z^+$:

Soit $a = a_0 + a_1 b + \ldots + a_h b^h$ avec $0 \leqslant a_i < b$ et $b^h \leqslant a < b^{h+1}$.

$$|a| \leqslant |a_0| + |a_1||b| + \ldots + |a_h||b|^h \leqslant (h + 1)(b - 1)$$

de même si $a^\nu = a'_0 + a'_1 b + \ldots + a'_{h_\nu} b^{h_\nu}$,

$$|a^\nu| \leqslant (h_\nu + 1)(b - 1) \leqslant (b - 1)[1 + \nu(h + 1)]$$

donc, quel que soit $\nu \in Z^+$,

$$|a| \leqslant (b - 1)^{1/\nu} [1 + \nu(h + 1)]^{1/\nu} = \varphi(\nu) \Longrightarrow |a| \leqslant \overline{\lim_{\nu \to +\infty}} (\varphi(\nu)) = 1 .$$

b. $\exists$ p premier tel que $|p| = \omega < 1$, et $\forall\ q \in Z^+$, $(q , p) = 1$, $|q| = 1$. L'existence de p résulte de ce que $|a|$ n'est pas triviale.

Soit $q \in Z^+$, $(q , p) = 1$, alors, quel que soit $n \in Z^+$, $(q^n , p^n) = 1$ et $\exists$ μ_n et $\lambda_n \in Z$ tels que $\mu_n p^n + \lambda_n q^n = 1$, donc $1 \leqslant \omega^n + |q|^n$, ce qui serait absurde pour n assez grand si $|q| < 1$.

Il est alors clair que

$$a = p^{\lambda} a' \ , \quad (a' \ , p) = 1 \implies |a| = \omega^{\lambda} \ .$$

2° a. $\exists \ b \in Z^+ \ , \ |b| > 1 \implies |a| > 1 \ , \ \forall \ a \neq 1 \ , \ a \in Z^+ \ .$

En effet, s'il existe $a \in Z^+$ tel que $|a| \leqslant 1$, $(1^\circ \ , a) \implies |b| \leqslant 1$.

b. Soit $1 < |b| \leqslant b$ (d'après (i)), posons $|b| = b^{\beta}$, $0 < \beta \leqslant 1$, si $a = a_0 + \ldots + a_h \, b^h$,

$$|a| \leqslant (h + 1)(b - 1)|b|^h \leqslant (b - 1)(h + 1) \ b^{h\beta}$$

et

$$\frac{|a|}{a^{\beta}} \leqslant (b - 1)(h + 1)$$

de la même façon qu'au (1°) ceci entraîne que

$$\frac{|a|}{a^{\beta}} \leqslant (b - 1)^{1/\nu} \ (1 + (h + 1)\nu)^{1/\nu} \ , \qquad \forall \ \nu \in Z^+ \ ,$$

et que

$$|a| \leqslant a^{\beta} \ .$$

Soit $|a| = a^{\alpha}$, $0 < \alpha \leqslant 1$, nous avons montré que $\alpha \leqslant \beta$, en échangeant les rôles de a et b , on en déduit $\beta \leqslant \alpha$, donc $\beta = \alpha$.

C. Q. F. D.

THÉORÈME 2 (Existence).

1° Soient p un nombre premier et ω un nombre réel, $0 < \omega < 1$, si $a \in Q$, $a \neq 0$, posons $a = p^{\lambda(a)} a'$, $\lambda(a) \in Z$, $a' \in Q$ ne contenant que des facteurs premiers différents de p , la fonction

$|a| = \omega^{\lambda(a)}$ si $a \neq 0$, $|a| = 0$ si $a = 0$ est une valeur absolue sur Q .

La topologie induite est indépendante du choix de ω , on choisit $\omega = \frac{1}{p}$ et la valeur absolue ainsi obtenue est appelée <u>valeur absolue p-adique de</u> Q .

2° Soit $|a|_\infty$ la valeur absolue usuelle sur $\mathbb{Q}$ (définie par $|a| = a$, $\forall\ a \in \mathbb{Z}^+$), et α un nombre réel, $0 < \alpha \leqslant 1$, la fonction

$$|a| = |a|_\infty^\alpha \text{ est une valeur absolue sur } \mathbb{Q} \quad .$$

La topologie induite est indépendante du choix de α.

1° Il est clair que $|a|$ satisfait aux axiomes (1) et (2). Vérifions (3).

Si $ab(a + b) = 0$, (3) est évidemment vérifié.

Si $ab(a + b) \neq 0$, posons

$$a = p^\alpha \frac{a'}{a''}, \text{ avec } a' \in \mathbb{Z},\ a'' \in \mathbb{Z}^+$$

$$(a', a'') = (a', p) = (a'', p) = 1$$

et

$$b = p^\beta \frac{b'}{b''}, \text{ avec } b' \in \mathbb{Z},\ b'' \in \mathbb{Z}^+$$

$$(b', b'') = (b', p) = (b'', p) = 1 \quad .$$

Supposons $|a| \leqslant |b|$, soit $\alpha = \lambda(a) \geqslant \lambda(b) = \beta$, et $\mu = \alpha - \beta \in \mathbb{Z}^+$. Alors

$$a + b = p^\beta \frac{a' b'' p^\mu + a'' b'}{a'' b''} \quad ,$$

où $(a'' b'', p) = 1$ et $a' b'' p^\mu + a'' b' \in \mathbb{Z}$, donc

$$|a + b| \leqslant \frac{1}{p^\beta} = |b| = \max(|a|, |b|) \quad .$$

Si de plus $|a| \neq |b|$, soit $\mu \neq 0$, $(a' b'' p^\mu + a'' b', p) = 1$, et $|a + b| = |b|$.

(4) $$|a + b| \leqslant \max(|a|, |b|)$$

(4') $$|a| \neq |b| \implies |a + b| = \max(|a|, |b|) \quad .$$

Nous avons démontré (4) et (4') pour $ab(a + b) \neq 0$, ils se vérifient trivialement pour $ab(a + b) = 0$. Il est clair que (4) $\implies$ (3), nous étudierons plus loin les propriétés des valeurs absolues vérifiant (4).

La totologie induite est indépendante de ω : en effet une suite de boules de rayons $r_n \to 0$ centrées en a constitue un système fondamental de voisinages de

a . Or une boule de rayon r et de centre a , pour la métrique correspondant à ω , est une boule de rayon $r' = r^{\log \omega / \log \omega'}$ et de centre a , pour la métrique correspondant à ω' , et $\frac{\log \omega}{\log \omega'} > 0$, donc un point a quelconque possède un système fondamental de voisinages commun aux topologies correspondant à ω et ω' , ce qui prouve que ces topologies sont identiques.

2° Il est clair que $|a|_\infty^\alpha$ satisfait à (1) et (2). Vérifions (3).

Il suffit de le montrer pour $a > 0$, $b > 0$, car si $ab \leqslant 0$,

$$|a + b|_\infty \leqslant \sup(|a|_\infty , |b|_\infty) \quad \text{et} \quad |a + b|_\infty^\alpha \leqslant \sup(|a|_\infty^\alpha , |b|_\infty^\alpha)$$

d'où (3).

Supposons $a > b > 0$, alors

$$|a| = a^\alpha , \quad |b| = b^\alpha , \quad |a + b| = (a + b)^\alpha ,$$

et

$$|a + b| \leqslant |a| + |b| \iff (1 + \frac{b}{a})^\alpha \leqslant 1 + (\frac{b}{a})^\alpha \quad \text{pour} \quad 0 < b < a$$

ce qui résulte immédiatement des positions relatives de $1 + x^\alpha$ et $(1 + x)^\alpha$ pour $0 \leqslant x \leqslant 1$. La démonstration de l'identité des topologies induites est exactement la même, compte tenu de ce qu'une boule de rayon r correspondant à α est une boule de rayon $r' = r^{\alpha'/\alpha}$ correspondant à α' .

Il résulte de ce théorème que pour toutes les valeurs absolues du second type, le complété de Q est $\underset{\sim}{R}$, quel que soit $\alpha \in]0 , 1]$, nous allons étudier les complétés de Q relatifs aux valeurs absolues p-adiques, mais auparavant donnons quelques propriétés des valeurs absolues vérifiant (4).

B. Espaces ultramétriques. Corps valués non archimédiens.

1. Espaces ultramétriques.

Définition. - Un espace métrique E est dit ultramétrique si la distance d(x , y) vérifie

(4') $\qquad d(x , z) \leqslant \max(d(x , y) , d(y , z)) \qquad \forall \ x , y , z \in E$.

Nous écrirons EUM pour "espace ultramétrique".

PROPOSITION 1. - Soient E , un EUM, et $x , y , z \in E$

$$d(x , y) \neq d(y , z) \implies d(x , z) = \max(d(x , y) , d(y , z)) \quad .$$

(Enoncé géométrique : dans un EUM tout triangle est isocèle, la base étant inférieure ou égale à l'un des côtés.)

En effet, supposons par exemple $d(y , z) > d(x , y)$, alors

$$d(x , z) \leqslant \max(d(x , y) , d(y , z)) = d(y , z)$$

$$d(y , z) \leqslant \max(d(y , x) , d(x , z)) \quad ;$$

or

$$d(y , x) < d(y , z) \implies d(y , z) \leqslant d(x , z) \implies d(y , z) = d(x , z)$$

C. Q. F. D.

PROPOSITION 2. - Dans un EUM, tout point d'un disque (fermé ou ouvert) est centre de ce disque.

Démontrons-le pour un cercle fermé :

soit

$$C = \{x \in E \ ; \ d(x , a) \leqslant \rho\} , \text{ soit } b \in C , \ d(b , a) \leqslant \rho$$

alors

$$x \in C \implies d(x , a) \leqslant \rho \implies d(x , b) \leqslant \max(d(x , a) , d(b , a)) \leqslant \rho$$

$$d(x , b) \leqslant \rho \implies d(x , a) \leqslant \max(d(b , a) , d(b , x)) \leqslant \rho \implies x \in C$$

C. Q. F. D.

COROLLAIRE. - Dans un EUM, si deux disques ne sont pas disjoints, l'un est inclus dans l'autre.

2. Corps valués non archimédiens.

Définition. - Soit $|a|$ une valeur absolue sur un corps K , on dit que $|a|$ est non archimédienne, si elle satisfait à

$$|a + b| \leqslant \max(|a| , |b|) \quad \forall \ a , b \in K \quad . \tag{4}$$

Un corps valué non archimédien est un corps muni d'une valeur absolue non archimédienne. Désormais nous appellerons **corps valué** un corps valué non archimédien.

THÉORÈME 3. - Dans un corps valué K complet, pour qu'une série converge il faut et il suffit que son terme général tende vers zéro.

Soit $u_0 + u_1 + \dots + u_n + \dots$, $u_n \in K$, une série ; on dit évidemment qu'elle converge, et a pour somme S , si

$$S_n = u_0 + u_1 + \dots + u_n \to S \quad \text{quand} \quad n \to +\infty \quad .$$

Si S converge,

$$|S_{n+1} - S_n| = |u_n| \leqslant \max(|S - S_n| \ , \ |S - S_{n+1}|) \to 0 \quad \text{avec} \quad \frac{1}{n} \quad .$$

Si $|u_n| \to 0$ avec $\frac{1}{n}$,

$$|u_n + u_{n+1} + \dots + u_m| = |S_m - S_{n-1}| \leqslant \max_{n \leqslant j \leqslant m} |u_n| \to 0 \quad \text{avec} \quad \frac{1}{n} \quad ,$$

donc la suite S_n est une suite de Cauchy, et K étant complet, $S_n \to S$.

Notation. - Nous noterons Γ le sous-groupe multiplicatif de $\underset{\sim}{R}^{**}$ image de K^* par $a \to |a|$. Γ est un sous-groupe multiplicatif, car $|a|$ vérifie l'axiome (2).

PROPOSITION 3. - Soit K un corps valué ; la boule-unité de K est un anneau A dont K est le corps des quotients, A est appelé anneau des entiers de K. L'ensemble P des $x \in K$, tels que $|x| < 1$, est un idéal premier de A , le corps $k = A/P$ est appelé corps des restes de K .

- $A = \{x \in K \ ; \ |x| \leqslant 1\}$ est un anneau.

Soient $x , y \in A$, $|x| \leqslant 1$ et $|y| \leqslant 1 \implies |x - y| \leqslant 1$, donc A est un sous-groupe additif de K .

De même $x , y \in A \implies xy \in A$, car $|xy| = |x||y| \leqslant 1$, donc A est un anneau.

- K est le corps des quotients de A .

Soit $x \in K$, si $|x| \leqslant 1$, $x \in A$, si $|x| > 1$, $|\frac{1}{x}| \leqslant 1$ et $\frac{1}{x} \in A$.

- P est un sous-groupe additif, car

$$|x| < 1 \ , \ |y| < 1 \implies |x - y| < 1 \quad ;$$

c'est de plus un idéal de A car si $x \in A$, $y \in P$, $|xy| = |x|.|y| < 1$.

C'est un idéal premier, car, si $x , y \in A$, $xy \in P$, $y \notin P$, alors

$$|y| \leqslant 1 \text{ et } |y| \not< 1 \implies |y| = 1$$

$$|xy| < 1 \text{ et } |y| = 1 \implies |x| < 1$$

donc $x \in P$.

[PROPOSITION 4. - Les idéaux de A sont les boules de rayon < 1 et P .

- Soit $B = \{x \in K \ , \ |x| \leqslant \rho < 1\}$ (resp. $|x| < \rho' \leqslant 1$) ,

$$x , y \in B \implies |x - y| \leqslant \max(|x| \ , \ |y|) \leqslant \rho \quad \text{(resp. } < \rho')$$

$$x \in B \ , \ y \in A \implies |xy| \leqslant |x| \implies xy \in B \quad .$$

- Soit B un idéal de A , $\forall \ x \in B$, $|x| \leqslant 1$.

Soit $\rho = \sup\limits_{x \in B} |x|$, si $\rho = 0$, $B = \{0\}$, supposons $\rho \neq 0$;

- s'il existe $b \in B$ tel que $|b| = \rho$, $|x| \leqslant \rho$, $\forall \ x \in B$; soit x tel que $|x| \leqslant \rho$, alors si $y = \frac{x}{b}$, $|y| \leqslant 1$, $y \in A$ et $x = yb \in B$, de plus $\rho < 1$ car sinon $|b| = 1 \implies |\frac{1}{b}| = 1 \implies \frac{1}{b} \in A \implies 1 \in B \implies B = A$;

- s'il n'existe aucun $b \in B$ tel que $|b| = \rho$, $|x| < \rho$, $\forall \ x \in B$; soit y tel que $|y| < \rho$, il existe $y' \in B$ tel que $|y| \leqslant |y'| < \rho$, alors $\frac{y}{y'} \in A$ et $y = \frac{y}{y'} y' \in B$.

[PROPOSITION 5. - Si Γ est discret dans R , les idéaux de A sont les puissances P^n de P $(n > 0)$.

Si Γ est discret dans R , $\Gamma = \{\omega^n\}$ où $\omega < 1$ et $n \in Z$.

Soient B l'idéal $|x| \leqslant \rho < 1$ et n tel que $\omega^n \leqslant \rho < \omega^{n-1}$ $(n > 0)$

(resp. B l'idéal $|x| < \rho \leqslant 1$ et n tel que $\omega^n < \rho \leqslant \omega^{n-1}$ $(n > 0)$) ;

alors $x \in K$, $|x| \leqslant \rho$ (resp. $|x| < \rho$) $\iff x \in K$, $|x| \leqslant \omega^n \iff x \in K$, $|x| < \omega^{n+1}$ et $P = \{x \in K \ ; \ |x| \leqslant \omega\}$, alors $B = P^n$.

[PROPOSITION 6. - Si Γ est discret, toute boule est à la fois ouverte et fermée, et K est totalement discontinu.

Soit B la boule fermée $|x - a| \leqslant \rho$, et soit n tel que $\omega^n \leqslant \rho < \omega^{n-1}$. B est aussi la boule fermée $|x - a| \leqslant \omega^n$ et la boule ouverte $|x - a| < \omega^{n-1}$.

De même si B est ouverte : $|x - a| < \rho$ et n tel que $\omega^{n+1} \leqslant \rho < \omega^n$, B est la boule fermée $|x - a| \leqslant \omega^{n+1}$ et la boule ouverte $|x - a| < \omega^n$.

Alors tout point de K ayant un système fondamental de voisinages à la fois ouverts et fermés, K est totalement discontinu.

PROPOSITION 7. - Soit $U = \{x \in K ; |x| = 1\}$, U est l'ensemble des unités ou éléments inversibles de A, c'est un sous-groupe multiplicatif de K^*. Si de plus Γ est discret, K^* est isomorphe à $U \times \Gamma$.

$$u \in U \iff |u| = 1 \iff |u| \leqslant 1 \text{ et } \left|\frac{1}{u}\right| \leqslant 1 \iff u \in A \text{ et } \frac{1}{u} \in A .$$

Il est clair que U est un sous-groupe multiplicatif.

Si Γ est discret, soit $\pi \in K$ tel que $|\pi| = \omega$, et soit $\Pi = \{\pi^n\}$, Π est isomorphe à Γ, et si $x \in K$, $|x| = \omega^n$, $x = \pi^n u$ où $u \in U$ et cette décomposition est unique.

PROPOSITION 8. - Si Γ est discret et k fini, de caractéristique p, toute boule fermée (resp. ouverte) de rayon r est recouverte par p boules disjointes fermées (resp. ouvertes) de rayon ωr,

- $r = 1$. A est recouvert par les p classes modulo P, qui sont des boules disjointes fermées de rayon ω, et P ($|x| < 1$) est recouvert par les p classes modulo P^2 qui sont p boules ouvertes disjointes de rayon ω.

- $r \neq 1$. Soit n défini par $\omega^n \leqslant r < \omega^{n-1}$, soit $|x - a| \leqslant r$ (resp. $< r$) la boule donnée, et $y = \pi^{-n}(x - a)$, l'application $x \to y$ envoie biunivoquement la boule donnée sur A (resp. P), et les images réciproques des p boules $|y - a_i| \leqslant \omega$ (resp. $< \omega$) ($i = 1, \ldots, p$) sont p boules disjointes $|x - a - \pi^n a_i| \leqslant \omega^{n+1}$ (resp. $< \omega^{n+1}$), soit $|x - a - \pi^n a_i| \leqslant \omega r$ (resp. $< \omega r$).

PROPOSITION 9. - Si Γ est discret et k fini, K est localement compact.

Il suffit de montrer que A est compact. Soit M une partie infinie de A, $M_1, \ldots, M_p$ la partition de M suivant les p classes modulo P, l'un au moins des M_i est infini, soit M^1, choisissons $m_1 \in M^1$, construisons ainsi une suite de parties infinies de M, $M \supset M^1 \supset \ldots \supset M^n \ldots$ telles que M^n soit contenu dans une classe modulo P^n, et choisissons à chaque fois $m_n \in M^n$, $m_n \neq m_p$ pour $p < n$, alors pour q et $n \geqslant n_0$, $|m_n - m_q| \leqslant \omega^{n_0}$

et la suite m_n est de Cauchy.

Remarque. - Soit K un corps valué non archimédien de caractéristique 0 , il contient un sous-corps isomorphe à Q et la valeur absolue induite sur Q par celle de K est nécessairement de première espèce, dans un corps valué, on a donc toujours $|n| \leq 1$ pour $n \in Z$.

C. Corps Q_p des nombres p-adiques.

Définition. - Soient p un nombre premier et $|x|_p$ la valeur absolue p-adique de Q . Le complété de Q pour cette valeur absolue est un corps appelé corps Q_p des nombres p-adiques.

Le complété de Q est le quotient de l'ensemble A des suites (a_n) , $a_n \in Q$, qui sont des suites de Cauchy, par la relation $(a_n) \sim (b_n) \iff |a_n - b_n|_p \to 0$ avec $\frac{1}{n}$.

L'ensemble A , muni de l'addition et de la multiplication terme à terme, est un anneau (vérification immédiate). Dans A , l'ensemble I des suites équivalentes à 0 , est un idéal premier de A :

C'est un idéal, car si $(a_n) \in A$, $|a_n|_p$ est borné car $|a_n - a_m|_p \leq \varepsilon$ pour $n , m \geq n_0 \implies |a_n|_p \leq \sup(|a_{n_0}|_p , \varepsilon)$, $\forall\ n \geq n_0$. Alors si $(a_n) \in I$, $(b_n) \in I$, $(a_n) - (b_n) = (a_n - b_n) \in I$ car

$$|a_n - b_n|_p \leq \sup(|a_n|_p , |b_n|_p) \implies |a_n - b_n|_p \to 0 \text{ avec } \frac{1}{n}$$

et $(a_n) \in I$, $(b_n) \in A \implies \exists\ M$ tel que $|b_n|_p \leq M$, $\forall\ n$, alors

$$|a_n b_n|_p \leq M|a_n|_p \text{ et tend vers zéro avec } \frac{1}{n} .$$

I est premier. Si $(b_n) \in A$, $(b_n) \notin I$,

$$|b_n|_p \to \beta \neq 0 \text{ quand } n \to +\infty ,$$

et même

$$|b_n|_p = \beta \text{ pour } n \geq n_0 .$$

En effet $\forall\ \varepsilon$, $\exists\ n_0$ tel que $n , m \geqslant n_0 \implies |b_n - b_m|_p \leqslant \varepsilon$, et $n \geqslant n_0 \implies |b_n|_p \leqslant \sup(|b_{n_0}|_p , \varepsilon)$. Si $\forall\ \varepsilon$, $|b_{n_0}|_p \leqslant \varepsilon$, $|b_n|_p \to 0$, donc si $|b_n|_p \not\to 0$, $\exists\ n_0$ tel que $|b_{n_0}|_p > \varepsilon$, alors pour $n \geqslant n_0$

$$|b_n|_p = |b_{n_0}|_p \quad .$$

Soit donc $(b_n) \in A$, $(b_n) \notin I$, et n_0 tel que, pour $n \geqslant n_0$, $|b_n|_p = \beta \neq 0$. Si $(a_n).(b_n) \in I$,

$$|a_n\ b_n|_p \to 0 \quad ,$$

or, pour $n \geqslant n_0$

$$|a_n\ b_n|_p = |a_n|_p\ \beta$$

avec $\beta \neq 0$, donc

$$(a_n) \in I \quad .$$

Soit $(a_n) \in A$,

$$(b_n) \sim (a_n) \iff (b_n - a_n) \in I \quad ,$$

donc le complété de Q est le quotient $A/I = Q_p$ que la structure d'anneau de A munit d'une structure de corps.

THÉORÈME 4. - Si $(a_n) \in A$,

$$|(a_n)|_p = \lim_{n \to +\infty} |a_n|_p$$

définit sur Q_p une valeur absolue non archimédienne prolongeant celle de Q .

$|(a_n)|_p = \lim_{n \to +\infty} |a_n|_p$ est une fonction définie sur Q_p : en effet, si $(a_n - b_n) \in I$,

$$|a_n - b_n|_p \to 0 \quad \text{avec} \quad \frac{1}{n} \quad ,$$

donc

$$\lim_{n \to +\infty} |a_n|_p = \lim_{n \to +\infty} |b_n|_p \quad .$$

C'est une valeur absolue non archimédienne : soient $a \in Q_p$, $b \in Q_p$, $ab \neq 0$, $(a_n) \in A$ et $(b_n) \in A$ des représentants de a et b . $\exists$ n_1 et n_2 tels que

$$n \geqslant n_1 \implies |a_n|_p = |a|_p \quad \text{et} \quad n \geqslant n_2 \implies |b_n|_p = |b|_p \quad .$$

En appliquant les axiomes (2) et (4) à a_n et b_n , on obtient

$$|ab|_p = |a_n\, b_n|_p = |a_n|_p\, |b_n|_p = |a|_p\, |b|_p \quad \text{pour} \quad n \geqslant n_1 \quad \text{et} \quad n \geqslant n_2$$

et

$$|a + b|_p = |a_n + b_n|_p \leqslant \max(|a_n|_p , |b_n|_p) = \max(|a|_p , |b|)_p$$

pour $n \geqslant n_1$, n_2 et n_3 tel que $|a_n + b_n|_p = |a + b|_p$ pour $n \geqslant n_3$ si $a + b \neq 0$.

Si $(a + b)(ab) = 0$, on vérifie trivialement (2) et (4).

Soit de plus $a \in Q_p$, $|a|_p = 0$, $(a_n) \in A$ un représentant de a , alors

$$|a|_p = 0 \iff \lim_{n \to +\infty} |a_n|_p = 0 \iff (a_n) \in I \iff a = 0 \quad .$$

Cette valeur absolue prolonge celle de Q : Q est canoniquement plongé dans Q_p en identifiant à $a \in Q$ la classe dans A de la suite $a_n = a$, $\forall$ n , dont la valeur absolue dans Q_p est

$$\lim_{n \to +\infty} |a_n|_p = |a|_p \quad .$$

Remarquons que le groupe Γ des valeurs prises par les valeurs absolues de $x \in Q_p^*$ est le groupe des puissances p^n , $n \in Z$.

THÉORÈME 5. - Soit $A_p = \{x \in Q_p \ ; \ |x|_p \leqslant 1\}$ l'anneau des entiers (boule-unité) de Q_p . Z est dense dans A_p .

Q est dense dans Q_p . Soit $A = \{x \in Q \ ; \ |x|_p \leqslant 1\}$ la boule-unité de Q , il est clair que A est dense dans A_p . Montrons que Z est dense dans A . Il suffit pour cela de montrer que $\forall$ $x \in A$ et $\forall$ $n \in Z^+$, $\exists$ $x_n \in Z$ tel que $|x - x_n| < \frac{1}{p^n}$. Soit donc $x = \frac{u}{v} \in A$,

$$(u , v) = 1 \quad \text{et} \quad \left|\frac{u}{v}\right|_p \leqslant 1 \implies (v , p) = 1 \quad .$$

$$(v\ ,\ p) = 1 \implies \exists\ a_0 \in Z\ ,\ 0 \leqslant a_0 < p - 1 \quad ,$$

a_0 unique, tel que $u - va_0 = u_0\, p$, $u_0 \in Z$. Alors

$$\frac{u}{v} = a_0 + \frac{u_0}{v}\, p \quad \text{et} \quad \left|\frac{u}{v} - a_0\right| \leqslant \frac{1}{p} \left|\frac{u_0}{v}\right| \leqslant \frac{1}{p} < 1 \quad .$$

De même il existe $a_1 \in Z$, $0 \leqslant a_1 < p - 1$, a_1 unique, tel que $u_0 - va_1 = u_1 p$, $u_1 \in Z$ et $\frac{u}{v} = a_0 + a_1\, p + \frac{u_1}{v}\, p^2$, soit $x_1 = a_0 + a_1\, p$, $\left|\frac{u}{v} - x_1\right| < \frac{1}{p}$.

Supposons qu'on ait construit $x_n = a_0 + a_1\, p + \dots + a_n\, p^n$, $0 \leqslant a_i < p$, tel que

$$\left|\frac{u}{v} - x_n\right|_p = \left|\frac{u_{n+1}}{v}\, p^{n+1}\right|_p < \frac{1}{p^n} \ , \quad u_{n+1} \in Z \quad .$$

Alors il existe a_{n+1} unique, $0 \leqslant a_{n+1} < p$ tel que

$$u_{n+1} - a_{n+1}\, v = u_{n+2}\, p \ , \quad u_{n+2} \in Z \quad ,$$

et si $x_{n+1} = x_n + a_{n+1}\, p^{n+1}$,

$$\left|\frac{u}{v} - x_{n+1}\right|_p = \left|\frac{u_{n+2}}{v}\, p^{n+2}\right|_p < \frac{1}{p^{n+1}} \quad .$$

Nous avons donc construit une suite $x_n \in Z$, telle que $\left|\frac{u}{v} - x_n\right|_p \leqslant \frac{1}{p^{n+1}}$. Remarquons que $0 \leqslant x_n < p^{n+1}$, et $\left|\frac{u}{v} - x_n\right|_p \leqslant \frac{1}{p^{n+1}}$ détermine la suite x_n de façon unique puisque, si x'_n vérifie aussi ces conditions,

$$|x_n - x'_n|_p \leqslant \frac{1}{p^{n+1}} \implies x_n - x'_n \equiv 0 \pmod{p^{n+1}} \implies x_n = x'_n \quad .$$

COROLLAIRE. Développement de Hensel. - Soit $x \in A_p$, il existe une suite unique $a_0\ ,\ \dots\ ,\ a_n\ ,\ \dots\ ,\ a_n \in Z$, $0 \leqslant a_n < p - 1$ telle que

$$x = a_0 + a_1\, p + \dots + a_n\, p^n + \dots$$

Il est clair que la série ci-dessus est convergente quels que soient les $a_n \in Z$, car

$$|a_n\, p^n|_p \leqslant \frac{1}{p^n} \quad .$$

Soient $x \in A_p$ et n un entier positif, Z étant dense dans A_p, il existe un entier y_n tel que $|x - y_n|_p \leqslant \frac{1}{p^{n+1}}$.

Soit $y_n = x_n + z_n p^{n+1}$, $0 \leqslant x_n < p^{n+1}$, $z_n \in Z$. Alors

$$|x - x_n|_p \leqslant \max(|x - y_n|_p , |y_n - x_n|_p) \leqslant \frac{1}{p^{n+1}} ,$$

et, comme nous l'avons remarqué ci-dessus x_n est le seul entier tel que

$$\begin{cases} |x - x_n|_p \leqslant \frac{1}{p^{n+1}} \\ 0 \leqslant x_n < p^{n+1} \end{cases} .$$

Soit x_{n+1} entier, $0 \leqslant x_{n+1} < p^{n+2}$ tel que $|x - x_{n+1}|_p \leqslant \frac{1}{p^{n+2}}$. Alors

$$|x_{n+1} - x_n|_p \leqslant \frac{1}{p^{n+1}} \implies x_{n+1} \equiv x_n \mod(p^{n+1}) .$$

Soit $x_{n+1} = x_n + a_{n+1} p^{n+1}$, $0 \leqslant x_n < p^{n+1}$ et $0 \leqslant x_n < p^{n+2} \implies 0 \leqslant a_{n+1} < p$. L'unicité de x_n et x_{n+1} entraîne celle de a_{n+1}, et on a

$$x = \lim_{n \to +\infty} x_n = a_0 + \dots + a_n p^n + \dots$$

[Conséquence. - Le corps des restes de Q_p est le corps $\frac{Z}{(p)}$.

Soit en effet $x = a_0 + a_1 p + \dots + a_n p^n + \dots$ le développement de Hensel de $x \in A_p$.

$$x \in U \iff a_0 \neq 0$$

$$x \in P \iff a_0 = 0 ,$$

le système $0, 1, \dots, p-1$ de valeurs de a_0 représente donc les classes modulo p dans A, si on le munit des opérations usuelles de $\frac{Z}{(p)}$.

Nous avons remarqué que le groupe Γ de Q_p^* est le groupe des p^n, il est donc discret, k étant de plus fini, toutes les propriétés démontrées dans B sont valables pour Q_p et, en particulier :

- Q_p est totalement discontinu, localement compact, isomorphe à $\Gamma \times U$,

toute boule est recouverte par p boules de même nature, de rayon $\frac{1}{p} r$, de plus par construction Q_p est complet.

Remarque. - L'idéal P est l'idéal principal (p) , et tout idéal de A est un idéal principal (p^n) .

Nous avons remarqué que si $x = a_0 + a_1 p + \dots + a_n p^n + \dots$

$$x \in P \iff a_0 = 0 \quad ,$$

donc

$$x \in P \iff p^{-1} x \in A \quad .$$

Valuation de Q_p .

Il est commode d'utiliser une notation différente de $|x|_p$ quoique équivalente.

Définition. - Si $x \in Q_p$, $x \neq 0$, on pose $\lambda(x) = - \log_p |x|_p$, $\lambda(x)$ est appelé valuation de x , ou ordre de x . On convient de poser $\lambda(0) = + \infty$.

Remarquons que, pour $a \in Q$, la fonction $\lambda(a)$ ici définie est la même que celle qui fut définie au théorème 2, 1°.

Lorsque x parcourt Q_p , $\lambda(x)$ parcourt Z . Cette valuation vérifie les axiomes

$$(2') \qquad \lambda(ab) = \lambda(a)\ \lambda(b)$$

$$(4'') \qquad \lambda(a + b) \geqslant \min(\lambda(a) , \lambda(b))$$

$$(1') \qquad \lambda(x) = + \infty \iff x = 0 \quad .$$

On peut définir les corps valués non archimédiens par la valuation vérifiant les axiomes ci-dessus et en déduire la valeur absolue, les deux définitions étant équivalentes.

Propriétés immédiates :

- $x \in A_p \iff \lambda(x) \geqslant 0$,
- $x \in P \iff \lambda(x) \geqslant 1$,
- $|x - a| \leqslant r \iff \lambda(x - a) \geqslant - \log r$;

- soit $u_n \in Q_p$ une suite, $u_n \to 0$ avec $\frac{1}{n} \iff \lambda(u_n) \to +\infty$ avec n ;

- soit $a \neq 0$, $p^{-\lambda(a)}.a \in U$, d'où, quel que soit $a \in Q_p$, un développement de Hensel unique

$$a = \sum_{-\infty}^{+\infty} a_i \, p^i$$

$0 \leqslant a_i < p$, avec $a_i = 0$ pour $i < \lambda(a)$.

II. Extensions algébriques de Q_p.

Notations. - Nous appellerons Ω_p la clôture algébrique de Q_p, $q_p = \frac{Z}{(p)}$ le corps des restes de Q_p ; K désignera généralement une extension algébrique finie de Q_p ; nous montrerons que K se munit canoniquement d'une structure de corps valué prolongeant celle de Q_p, et noterons k son corps des restes.

Définition. - Soient $x \in \Omega_p$ et $P(x) = x^n + a_1 x^{n-1} + \dots + a_n$, $P(x) \in Q_p[x]$ le polynôme irréductible unitaire qui lui est associé, on pose

$$|x|_p = |a_n|^{1/n} = \text{valeur absolue de } x \quad \text{et} \quad \lambda(x) = \frac{1}{n}\lambda(a_n) = \text{ordre de } x \ .$$

Pour montrer que $|x|_p$ et $\lambda(x)$ sont une valeur absolue et un ordre sur Ω_p, il nous faut passer par les extensions finies.

Rappels sur les extensions algébriques finies d'un corps commutatif k.

Soit $K \supset k$ une extension de degré n de k.

Soit $\omega_1, \dots, \omega_n$ une base de K sur k ; si $\alpha = \alpha_1 \omega_1 + \dots + \alpha_n \omega_n \in K$, $\alpha_i \in k$, soient

$$\begin{aligned} \alpha\omega_1 &= \alpha_{11}\omega_1 + \alpha_{12}\omega_2 + \dots + \alpha_{1n}\omega_n \\ &\vdots \\ \alpha\omega_n &= \alpha_{n1}\omega_1 + \alpha_{n2}\omega_2 + \dots + \alpha_{nn}\omega_n \end{aligned}$$

et $A = (\alpha_{ij})$ la matrice du tableau ainsi formé. Si $P(x) = \det(xI - A)$ (I matrice unité), on sait que $P(\alpha) = 0$. On appelle [illegible] de α dans K le nombre

$$N(\alpha) = \det A = (-1)^n P(0) \quad .$$

On sait que

$$N(\alpha).N(\beta) = N(\alpha\beta) \quad .$$

L'équation $P(x) = 0$ est appelée équation normale de α dans K, elle est indépendante de la base $\omega_1 , \ldots , \omega_n$ choisie.

LEMME. - Soient $\alpha \in K$, $\varphi(x)$ le polynôme unitaire irréductible qui lui est associé, alors

$$P(x) = \varphi(x)^f \quad \text{où} \quad f \quad \text{est un entier} \geqslant 1 \quad .$$

Soient n le degré de K, d celui de φ, il est clair que $d \leqslant n$.

- Si $d = n$, $P(x)$ étant unitaire, de même degré que φ, et multiple de φ (puisque $P(\alpha) = 0$), $P = \varphi$ et $f = 1$.

- Si $d \leqslant n$, d divise n car alors, soit $k(\alpha)$ l'extension de k par α, $k \subset k(\alpha) \subset K$, et K est algébrique et de degré $\frac{n}{d} = f$ sur $k(\alpha)$.

Soient

$$\alpha_1 , \ldots , \alpha_d \quad \text{une base de} \quad k(\alpha) \quad \text{sur} \quad k$$

$$\theta_1 , \ldots , \theta_f \quad \text{une fase de} \quad K \quad \text{sur} \quad k(\alpha) \quad .$$

Le système $\omega_r = \alpha_i \theta_j$, $i = 1 , \ldots , d$, $j = 1 , \ldots , f$ forme une base de K sur k ; supposons qu'ils soient rangés dans l'ordre lexicographique des couples (j , i), c'est-à-dire $\omega_1 = \alpha_1 \theta_1$, $\omega_2 = \alpha_2 \theta_1$, etc.

Soient A la matrice associée à α pour la base $\alpha_1 \ldots \alpha_d$ et B la matrice associée à α dans K pour la base $\omega_1 \ldots \omega_n$. On a

$$B = \begin{pmatrix} A & 0 & 0 & \ldots \\ 0 & A & 0 & \ldots \\ 0 & . & A & \\ & \vdots & & \ddots \\ 0 & . & & A \end{pmatrix}$$

en notant dans le tableau de B les carrés "$d - d$" par un seul signe. Alors

$$P(x) = \det(xI - B) = [\det(xI - A)]^f = [\varphi(x)]^f \quad .$$

THÉORÈME 6. - Soit K une extension de degré r de Q_p, si $\alpha \in K$, $|\alpha|_p = |N(\alpha)|_p^{1/n}$ est la fonction $|\alpha|_p$ définie ci-dessus dans Ω_p.

Soit en effet $\varphi(x)$ de degré d le polynôme unitaire irréductible de α, la valeur absolue définie dans Ω_p est $|\alpha|_p = |\varphi(0)|_p^{1/d}$.

Or

$$N(\alpha) = (-1)^n P(0) \quad ,$$

et

$$P(x) = [\varphi(x)]^{n/d} \implies |N(\alpha)|_p = |\varphi(0)|_p^{n/d} \quad ,$$

donc

$$|N(\alpha)|_p^{1/n} = |\varphi(0)|_p^{1/d} \quad .$$

Nous allons maintenant montrer que, dans K, cette $|\alpha|_p$ est une valeur absolue, il est clair qu'elle vérifie (1) et (2). Pour démontrer (4), il nous faut le très important lemme de Hensel :

LEMME de Hensel. - Soient $f(x) \in A_p[x]$ et $\overline{f}(x) \in q_p[x]$ sa classe modulo p. Si $\overline{f} = \overline{g}.\overline{h}$ où $\overline{g} \in q_p[x]$ et $\overline{h} \in q_p[x]$ sont premiers entre eux, il existe $g(x) \in A_p[x]$, $g \in \overline{g}$ et $h(x) \in A_p[x]$, $h \in \overline{h}$, tels que

$$f = g.h \quad .$$

Nous représenterons $\overline{f}$, $\overline{g}$, $\overline{h}$ par des polynômes f^*, g^*, $h^* \in Z[x]$ et tels que $dg.f^* = dg.f$, $f^* = g^* h^*$. On a $(g^*, h^*) \equiv 1 \pmod p$. Nous dirons qu'un polynôme $P \equiv 0 \pmod{p^n}$, $P \in A_p[x]$, si chacun de ses coefficients est dans l'idéal (p^n).

Nous allons construire deux suites de polynômes

$$g_1 = g^*, g_2, \ldots, g_n, \ldots, g_n \in A_p[x]$$

et

$$h_1 = h^*, \ldots, h_n, \ldots, h_n \in A_p[x] \quad ,$$

telles que

$$(c)\qquad \begin{cases} g_n - g_{n-1} \equiv 0 \pmod{p^{n-1}} \\ h_n - h_{n-1} \equiv 0 \pmod{p^{n-1}} \\ (g_n , h_n) \equiv 1 \pmod{p} \\ f - g_n h_n \equiv 0 \pmod{p^n} \\ dg.(f - g_n h_n) < dg\ f \end{cases} .$$

En ajoutant $g_0 = x^n$, $h_0 = a_0$ si $f = a_0 x^n + \dots$, les conditions (c) sont réalisées pour $n = 1$.

Supposons qu'on ait construit deux telles suites jusqu'à l'ordre n , et soit

$$\varphi_n(x) = \frac{f - g_n h_n}{p^n} , \quad \varphi_n(x) \in A_p[x] \quad \text{et} \quad dg\ \varphi_n(x) < dg\ f .$$

Alors il existe $u_n(x)$ et $v_n(x) \in A_p[x]$ tels que

$$dg\ u_n < dg\ g_n ,$$

$$dg\ v_n < dg\ h_n ,$$

et

$$u_n h_n + v_n g_n \equiv \varphi_n(x) \pmod{p} .$$

Posons

$$g_{n+1} = g_n + u_n p^n \quad \text{et} \quad h_{n+1} = h_n + v_n p^n ,$$

on a

$$g_{n+1} h_{n+1} \equiv g_n h_n + \varphi_n p^n \mod(p^{n+1})$$

donc

$$f - g_{n+1} h_{n+1} \equiv 0 \mod(p^{n+1}) ,$$

$$dg(f - g_{n+1}\, h_{n+1}) < dg\, f$$

$$g_{n+1} \equiv g_0 \pmod{p} \quad \text{et} \quad h_{n+1} \equiv h_0 \pmod{p} \implies (g_{n+1}\, ,\, h_{n+1}) \equiv 1 \mod p$$

et les conditions (c) sont réalisées à l'ordre $n + 1$.

Les polynômes g_n et h_n sont de degré fixe, donc ils convergent vers des polynômes g et $h \in A_p[x]$ de même degré (Q_p complet) et tels que $f = gh$.

COROLLAIRE. - Si $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ est irréductible,

$$|a_n|_p \leqslant 1 \implies |a_i|_p \leqslant 1 \quad \text{pour} \quad i = 1\, ,\, \ldots\, ,\, n-1 \quad .$$

Supposons que $\min_i(\lambda(a_i)) = -\lambda < 0$, et soit a_{i_0} le coefficient de plus haut indice tel que $\lambda(a_{i_0}) = -\lambda$, $i_0 \neq n$.

$$\varphi(x) = p^\lambda f(x) \in A_p[x]$$

et

$$\varphi(x) = p^\lambda x^n + a_1\, p^\lambda x^{n-1} + \ldots + a_{i_0}\, p^\lambda x^{n-i_0} + \ldots + a_n\, p^\lambda \quad ;$$

or, pour $i > i_0$,

$$\lambda(a_i) > -\lambda \quad ,$$

donc

$$\lambda(a_i\ p^\lambda) > 0 \quad \text{et} \quad a_i\ p^\lambda \in (p) \quad .$$

De plus, $\varepsilon_0 = a_{i_0}\, p^\lambda$ est une unité, donc

$$\varphi(x) \equiv x^{n-i_0} (\varepsilon_0 + \alpha_1 x + \ldots + \alpha_{i_0} x^{i_0}) \pmod{p} \; ; \; \alpha_i \in A_p \quad .$$

Soient

$$g^*(x) = x^{n-i_0} \quad \text{et} \quad h^*(x) = \varepsilon_0 + \alpha_1 x + \ldots + \alpha_{i_0} x^{i_0} \quad ,$$

on a

$$(g^* , h^*) \equiv 1$$

car $|\varepsilon_0| = 1$ et $n - i_0 \neq 0$, d'où en appliquant le lemme de Hensel

$$\varphi(x) = g(x)\, h(x) \quad \text{où} \quad f = p^{-\lambda}\, g(x)\, h(x) \qquad g , h \in A_p[x] \quad ,$$

ce qui est absurde puisque f est irréductible. Donc

$$\min_i(\lambda(a_i) \geqslant 0 \text{ , et } |a_i|_p \leqslant 1 \quad .$$

THÉORÈME 7. - Soit K une extension de degré n de Q_p . La fonction

$$|\alpha|_p = |N(\alpha)|_p^{1/n} , \qquad \alpha \in K \quad ,$$

définit une valeur absolue sur K prolongeant celle de Q_p .

Si $\alpha \in Q_p$, $N(\alpha) = \alpha^n$ et $|\alpha|_p = |\alpha^n|_p^{1/n}$ est bien la valeur absolue usuelle sur Q_p .

Nous avons remarqué qu'il suffit de démontrer que (4) est vérifié, soit :

$$|\alpha + \beta|_p \leqslant \max(|\alpha|_p , |\beta|_p) \quad . \tag{4}$$

Pour $\alpha , \beta = 0$ c'est évident. Supposons $|\alpha|_p > |\beta|_p$, il suffit de montrer que $|1 + u|_p \leqslant 1$ si $|u|_p \leqslant 1$.

Or

$$|u|_p \leqslant 1 \iff |N(u)|_p \leqslant 1 \quad .$$

Soit

$$P(x) = x^n + u_1 x^{n-1} + \ldots + u_n = [\varphi(x)]^{n/d}$$

où $\varphi(x) = x^d + v_1 x^{d-1} + \ldots + v_d$ est le polynôme unitaire irréductible de u .

$$|u|_p \leqslant 1 \iff |u_n|_p \leqslant 1 \implies |v_d|_p \leqslant 1 \quad .$$

$\varphi(x)$ étant irréductible, et grâce au corollaire ci-dessus, ceci entraîne que

$$\varphi(x) \in A_p[x] \quad ,$$

donc

$$P(x) \in A_p[x] \quad .$$

Soit $x = y - 1$, alors

$$P(y - 1) = Q(y) \in A_p[x] \quad ;$$

or Q est le polynôme normal de $1 + u$, donc $N(1 + u) \in A_p$ et $|1 + u|_p \leqslant 1$.

COROLLAIRE. - La fonction $|x|_p$ définie pour $x \in \Omega_p$ est une valeur absolue non archimédienne sur Ω_p , et $\lambda(x)$ une valuation, elles prolongent celles de Q_p .

En effet, pour démontrer une relation entre les valeurs absolues d'un nombre fini d'éléments de Ω_p , il suffit de considérer une extension finie K de Q_p contenant ces éléments, et de démontrer la relation cherchée dans K . Les axiomes des valeurs absolues étant satisfaits par $|x|_p$ dans toute extension finie de Q_p le sont donc aussi dans Ω_p . On démontre que ce sont les seules valeur absolue et valuation sur Ω_p prolongeant celles de Q_p .

THÉORÈME 8. - Soit K une extension séparable de degré n de Q_p , le corps des restes de K a p^f éléments où $f|n$, et K est localement compact et complet.

On peut démontrer sans utiliser le corps des restes, que K est localement compact et complet, en effet : K étant métrique et séparé, Q_p est complet non discret, or (BOURBAKI : Espaces vectoriels topologiques, I, § 2, n° 3, théorème 2) "tout EVT séparé E , de dimension finie n , sur un corps valué k complet non discret, est isomorphe à k^n ". Donc K est isomorphe à Q_p^n , et comme produit fini d'espaces localement compacts complets, il est localement compact et complet.

Le corps des restes est cependant intéressant en lui-même et nous allons démontrer le lemme suivant.

LEMME. - Soit A l'anneau des entiers de K (au sens du I, § B, 2, proposition 3), c'est aussi :

- l'ensemble des entiers algébriques sur A_p appartenant à K .

- un A_p-module de dimension n sur A_p .

$$x \in A \iff \lambda(x) \geq 0 \iff N(x) \in A_p \implies x \text{ entier sur } A_p$$

comme nous l'avons vu dans la démonstration du théorème 7.

$$x \text{ entier sur } A_p \implies N(x) \in A_p \implies \lambda(x) \geq 0 \implies x \in A \quad .$$

Il est clair que A est un A_p-module. Nous allons montrer que :

"Il existe une base $\omega_1, \dots, \omega_n$ de k qui est une base de A en tant que module sur A_p ".

Si $\omega_1, \dots, \omega_n$ est une base de k, $\omega_i \in A$,

$$\gamma = \sum \gamma_i \omega_i \text{ avec } \gamma_i \in A_p \implies \gamma \in A \quad .$$

Soit $\Delta(\omega) = \det(T_r(\omega_i \omega_j))$ le discriminant de la base ω.

Si $\omega \in A_p^n$, $\Delta(\omega) \in A_p$, choisissons une base ω telle que $|\Delta(\omega)|_p$ soit maximum parmi les $|\Delta(\omega)|_p$ des bases $\omega \in A_p^n$, et soit $\gamma \in A$, $\gamma \neq 0$,

$$\gamma = a_1 \omega_1 + \dots + a_n \omega_n \quad ,$$

supposons $a_1 \neq 0$, alors

$$\omega' = (a_1 \omega_1, \omega_2, \dots, \omega_n)$$

est encore une base de $k \in A_p^n$ et

$$\Delta(\omega') = \Delta(\omega) \times \begin{vmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 1 & 0 & 0 \\ & & 1 & \\ 0 & & & \ddots \\ & & & & 1 \end{vmatrix}^2 = a_1^2 \, \Delta(\omega) \quad .$$

Or $|\Delta(\omega')|_p \leq |\Delta(\omega)|_p$ d'après le choix de $\omega \implies |a_1^2| \leq 1$, $a_1 \in A_p$.

Il résulte de ce lemme que le corps des restes de K est à p^f éléments, car : soit $\mathfrak{P}$ l'idéal $|x|_p < 1$ de A, $p \in \mathfrak{P}$, l'idéal principal engendré par p dans A, soit $pA \subset \mathfrak{P}$, or (I, § B, 2, proposition 5) pA est une puissance

$\mathfrak{P}^e$ de $\mathfrak{P}$. L'existence de la base de A_p/A montre qu'il y a p^n classes modulo pA dans A , donc $p^{n/e} = p^f$ classes modulo $\mathfrak{P}$. On sait alors par la proposition 9 que K est localement compact.

Relations entre les extensions finies de Q et celles de Q_p .

Soit $P(x) \in Q[x]$ irréductible définissant une extension séparable $Q(\theta)$ de Q , et soit p premier fixé, $P(x) \in Q_p[x]$.

Soit

$$P(x) = \prod_{j=1}^{K} P_j(x)$$

où $P_j(x) \in Q_p[x]$ sa décomposition en facteurs irréductibles de $Q_p[x]$. Pour $i \neq j$, $P_i \neq P_j$, sinon P ne serait pas premier à sa dérivée. Soit θ_i une racine de P_i dans Ω_p ,

$$|\theta_i|_p = |P_i(0)|^{1/s_i} \quad \text{si} \quad s_i = dg.P_i \quad .$$

Soit $N_Q(\theta) = \pm P(0)$ la norme de θ relativement à Q .

$$N_Q(\theta) = \pm \prod_{j=1}^{k} P_j(0)$$

$$|N_Q(\theta)|_p = \prod_{j=1}^{k} |\theta_i|_p^{s_i} \quad .$$

Si $P \in Z[x]$, $P_i \in A_p[x]$ et $|\theta_i|_p \leq 1$, $\forall$ i , $\forall$ p . Si $(N_Q(\theta) , p) = 1$, $|\theta_i|_p = 1$. Donc :

PROPOSITION 10. - Soit θ un entier algébrique sur Q . Quel que soit le nombre premier p c'est un entier sur Q_p ; si de plus p est premier à $N_Q(\theta)$, θ est une unité algébrique sur Q_p .

Clôture algébrique Ω_p de Q_p .

Ω_p n'est pas complet, cependant son complété est algébriquement clos, ce qui permet de disposer d'un surcorps valué complet algébriquement clos de Q_p .

LEMME de Krasner. - Soit k un corps valué non archimédien, Ω sa fermeture algébrique, $x \in \Omega$, et $x = x_1, x_2, \cdots, x_n$ ses conjugués distincts.

Soit $y \in \Omega$, tel que $|x - y| < |x_i - y|$, $i \geq 2$, alors si x est séparable sur k, $x \in k(y)$.

Soient en effet $x = x_{i_1}, \cdots, x_{i_q}$ les conjugués distincts de x par rapport à $k(y)$,

$$|y - x_{i_j}| = |y - x| \quad \text{pour} \quad 1 \leq j \leq q \quad ,$$

donc

$$q = 1 \quad \text{et} \quad x \in k(y) \quad .$$

THÉORÈME 9. - Soit $f(x) \in k[x]$ irréductible séparable de degré n,

$$f(x) = \sum_{j=1}^{n} f_j x^j$$

et soit

$$g(x) = \sum_{j=1}^{n} g_j x^j \quad , \quad g_n f_n \neq 0 \quad ,$$

il existe une constante m ne dépendant que de f telle que

$$\sup_j |g_j - f_j| \leq m \implies g(x)$$

est irréductible, séparable, et définit la même extension de k que f.

Soit $y \in \Omega$, $g(y) = 0$, soient $x_1, \cdots, x_n$ les racines de f.

$$f(y) = \prod_{j=1}^{n} (y - x_j) \quad \text{et} \quad \sup_j |g_j - f_j| \leq m \implies |f(y)| \leq m[\sup(1, |y|^n)] \quad .$$

Pour m assez petit, ceci entraîne

$$|f(y)| < [\inf_{i \neq j} |x_i - x_j|]^n \implies \exists\ i_0 \text{ tel que } |y - x_{i_0}| < |x_{i_0} - x_j| \ , \ j \neq i_0$$

alors

$$j \neq i_0 \implies |y - x_j| \leqslant \max(|y - x_{i_0}| , |x_{i_0} - x_j|)$$

et

$$|y - x_j| = |x_{i_0} - x_j| > |y - x_{i_0}| \quad .$$

En appliquant le lemme précédent, on en déduit $x_{i_0} \in \mathfrak{t}(y)$, donc $\mathfrak{t}(y)$ est de degré n , contient $\mathfrak{t}(x_{i_0})$ également de degré n , et

$$\mathfrak{t}(y) = \mathfrak{t}(x_{i_0}) \quad .$$

C. Q. F. D.

COROLLAIRE. - Soient Ω_p la clôture algébrique de Q_p et $\hat{\Omega}_p$ son complété. $\hat{\Omega}_p$ est algébriquement clos.

Soit en effet $f(x) \in \hat{\Omega}_p[x]$ irréductible séparable et de degré n ; tout $g \in \hat{\Omega}_p[x]$ de degré n et assez voisin de f est irréductible et séparable ; choisissons un tel g dans $\Omega_p[x]$; il est irréductible donc de degré 1 , et f est de degré n . D'autre part l'application $x \to x^n$ est un homéomorphisme de Ω_p , il se prolonge par continuité à $\hat{\Omega}_p$, donc $\hat{\Omega}_p$ est parfait. Il en résulte que $\hat{\Omega}_p$ est algébriquement clos.

Remarque sur les unités d'une extension finie de Q_p .

Soit η une unité d'un corps K de degré n sur Q_p . Alors quel que soit $\varepsilon > 0$, il existe m tel que $|\eta^m - 1|_p < \varepsilon$.

Soit $\omega_1 , \ldots , \omega_n$ une base de A sur A_p .

$$\eta = a_1 \omega_1 + \ldots + a_n \omega_n \quad \text{où} \quad a_i \in A_p \quad .$$

Quel que soit h entier $\geqslant 0$,

$$\eta^h = a_{h_1} \omega_1 + \ldots + a_{h_n} \omega_n \quad \text{avec} \quad a_{h_i} \in A_p \quad .$$

Soit M un entier tel que $\frac{1}{p^M} < \varepsilon$, les systèmes $(a_{h_1}, \dots, a_{h_n})$ n'ont que p^{nM} valeurs possibles modulo p^M, il existe donc deux valeurs h et $h+m$, $0 \leqslant h < h+m \leqslant p^{nM}$, telles que $\eta^{h+m} - \eta^h \equiv 0 \pmod{p^M}$, d'où

$$|\eta^m - 1|_p < \varepsilon \quad .$$

(On peut choisir M tel que $\varepsilon \leqslant \frac{1}{p^{M-1}}$, alors $p^M \leqslant \frac{p}{\varepsilon}$ et il existe m, $m < \frac{p^n}{\varepsilon^n}$, tel que $|\eta^m - 1|_p < \varepsilon$.)

III. Fonctions analytiques. Fonctions usuelles.

A. Séries entières et fonctions analytiques.

THÉORÈME 10 (H[illegible]). - Soient K un corps valué complet, $K[[X]]$ l'anneau des séries formelles sur K ; si

$$f(x) = \sum_{n \geqslant 0} a_n x^n \in K[[X]] \quad , \text{ et } \quad \frac{1}{R} = \overline{\lim_{n \to +\infty}} |a_n|^{1/n} \quad ,$$

$f(x)$ converge pour $|x| < R$ et diverge pour $|x| > R$.

En effet, la condition nécessaire et suffisante pour que $f(x)$ converge est que

$$\lim_{n \to +\infty} |a_n| |x|^n = 0 \qquad \text{(théorème 3)} \quad .$$

Pour n assez grand, $|a_n| \leqslant \frac{1}{(R-\varepsilon)^n}$, donc pour $|x| < R - \varepsilon$,

$$\overline{\lim_{n \to +\infty}} |a_n| |x|^n \leqslant \lim_{n \to +\infty} \left(\frac{|x|}{R-\varepsilon} \right)^n = 0 \quad ,$$

et f converge pour $|x| < R$.

Il existe une infinité de n tels que $|a_n| > \frac{1}{(R+\varepsilon)^n}$, donc pour $|x| > R + \varepsilon$,

$$\overline{\lim_{n \to +\infty}} |a_n| |x|^n \geqslant \overline{\lim_{n \to +\infty}} \left(\frac{|x|}{R+\varepsilon} \right)^n = +\infty$$

et f diverge pour $|x| > R$.

COROLLAIRE. - $f(x) = \sum_{n\geqslant 0} a_n x^n$ converge pour

$$\lambda(x) > \omega = \underline{\lim}_{n\to+\infty} \left(-\frac{\lambda(a_n)}{n}\right)$$

et diverge pour

$$\lambda(x) < \omega \quad .$$

Remarque. - S'il existe $a \in K$, tel que $|a| = R$ et que $f(a)$ converge, alors f converge $\forall\ x \in K$ tel que $|x| = R$.

Si $f(a)$ converge, $|a_n||a|^n \to 0$ avec $\frac{1}{n}$, donc $|a_n||x|^n \to 0$ avec $\frac{1}{n}$ lorsque $|x| = |a| = R$.

THÉORÈME 11 (de translation). - Soient $f(X) = \sum_{n\geqslant 0} a_n X^n \in K[[X]]$ et D son disque de convergence, et soit $\alpha \in D$, alors $g(Y) = f(Y + \alpha)$ a pour disque de convergence le disque $Y \in D$, qui est aussi le disque $X \in D$.

$$g(Y) = \sum_{n\geqslant 0} a_n \left(\sum_{m=0}^{n} \binom{m}{n} Y^m \alpha^{n-m}\right) = \sum_{m\geqslant 0} Y^m \left(\sum_{n\geqslant 0} \binom{m+n}{m} a_{m+n} \alpha^n\right) \quad .$$

Or

$$\binom{m+n}{m} \in Z \quad ,$$

donc

$$\left|\binom{m+n}{m}\right| \leqslant 1 \quad .$$

Soit $u_m = y^m \left(\sum_{n\geqslant 0} \binom{m+n}{n} a_{m+n} \alpha^n\right)$;

$$|u_m| \leqslant \sup_{n\geqslant 0} |a_{m+n}||\alpha|^n |y|^m \quad .$$

Soit $r = \sup(|\alpha|, |y|)$,

$$|u_m| \leqslant \sup_{n\geqslant 0} |a_{m+n}|\ r^{m+n} \quad .$$

Donc si $y \in D$,

$$|u_m| \to 0 \quad \text{avec} \quad \frac{1}{n} \quad ,$$

et $g(y)$ converge. Soit $y \in D'$ le disque de convergence de $g(y)$, nous venons de montrer que $D' \supset D$, en échangeant g et f on a $D = D'$. Or si $\alpha \in D$ le disque de centre α translaté du disque D de centre 0 est D lui-même (proposition 2).

Conséquence. - Soit $f(x)$ la fonction somme de $f(X)$ pour $x \in D$; d'après le théorème précédent, il est impossible de prolonger $f(x)$ hors de D par translation.

Définition. - Soient D un disque de K et $f(x)$ une fonction définie sur D à valeurs dans K , $f(x)$ est dite analytique sur D si, en tout point $\alpha \in D$, il existe une série entière en $x - \alpha$ dont la somme coïncide avec f dans un voisinage de α .

THÉORÈME 12. - La somme d'une série entière $f(x)$ convergente dans le disque D est analytique dans D .

Il résulte immédiatement du théorème 11.

THÉORÈME 13. - Une fonction analytique dans D est continue en tout point de D .

Il suffit de montrer qu'une série entière convergente est continue à l'origine.

Soit $f(x) = \sum_{n \geqslant 0} a_n x^n$ convergente pour $|x| \leqslant r$.

Pour $|x| \leqslant r$,

$$|f(x) - a_0| \leqslant |x| \cdot \left| \sum_{n \geqslant 1} a_n x^{n-1} \right| \leqslant M|x|$$

car

$$\left| \sum_{n \geqslant 1} a_n x^{n-1} \right| \leqslant \sup_{n \geqslant 1} |a_n| |x|^{n-1} \leqslant \sup_{n \geqslant 1} (|a_n| \cdot r^{n-1}) = M \quad ,$$

fini puisque f converge pour $|x| = r$.

COROLLAIRE 1. - Les zéros d'une série entière non nulle sont isolés.

Soit α un zéro de $f(x)$ et soit

$$g(y) = f(y + \alpha) = \sum_{m \geq 1} v_m y^m \quad .$$

Si f n'est pas nulle, g non plus, soit v_k le premier coefficient non nul de g : alors

$$g(y) = y^k (v_k + h(y))$$

où $h(y) \in K[[y]]$ a même rayon de convergence que f et g, avec $h(0) = 0$, h étant continue à l'origine, $|h(y)| \leq \frac{1}{2} |v_k|$ pour $|y| \leq \eta$, alors, pour $|y| \leq \eta$,

$$|g(y)| = |y|^k \, |v_k| \neq 0 \quad \text{pour} \quad y \neq 0 \quad .$$

COROLLAIRE 2. - Si K est localement compact, une série entière non nulle n'a qu'un nombre fini de zéros dans un disque fermé de K.

Soit en effet D un disque fermé dans lequel $f(x)$ a une infinité de zéros, ces zéros ont un point d'accumulation $\alpha \in D$ (D compact, K complet). Alors, par continuité en α, $f(\alpha) = 0$ et α est un zéro non isolé de f donc f est nulle.

B. Fonctions usuelles.

Soit $\exp X = \sum_{n \geq 0} \frac{X^n}{n!}$.

PROPOSITION 11. Exponentielle. - Soit K une extension finie ou non de Q_p, dans K ; $\exp X$ converge pour $\lambda(x) > \frac{1}{p-1}$ et diverge pour $\lambda(x) \leq \frac{1}{p-1}$. Sa somme est appelée fonction exponentielle.

Montrons que

$$\omega = \underline{\lim} \left(- \lambda\left(\frac{1}{n!}\right) \frac{1}{n} \right) = \frac{1}{p-1} \quad .$$

$\lambda(n!) = [\frac{n}{p}] + [\frac{n}{p^2}] + \ldots + [\frac{n}{p^n}] + \ldots$ où $[x]$ désigne la partie entière de x

$= [\frac{n}{p}] + [\frac{n}{p^2}] + \ldots + [\frac{n}{p^h}]$ si $p^h \leq n < p^{h+1}$

$\lambda(n!) \leq n(\frac{1}{p} + \ldots + \frac{1}{p^n}) = \frac{n}{p-1} (1 - \frac{1}{p^h}) \leq \frac{n-1}{p-1}$,

et pour $n = p^h$,

$$\lambda(n!) = \frac{n-1}{p-1} \quad .$$

Donc

$$\underline{\lim}\ \frac{1}{n}\ \lambda(n!) = \underline{\lim}\ \frac{1}{n}\frac{n-1}{p-1} = \frac{1}{p-1} \quad .$$

Il reste à montrer que $\exp X$ diverge pour $\lambda(x) = \frac{1}{p-1}$, s'il existe $x \in K$ tel que $\lambda(x) = \frac{1}{p-1}$.

Or si $\lambda(x) = \frac{1}{p-1}$, et pour $n = p^h$,

$$\lambda\left(\frac{x^n}{n!}\right) = \frac{n}{p-1} - \frac{n-1}{p-1} = \frac{1}{p-1} \neq +\infty \quad ,$$

donc $\exp x$ diverge.

PROPOSITION 12. - Pour $\lambda(x) > \frac{1}{p-1}$,

$$\lambda(\exp x - 1) = \lambda(x) \quad .$$

En effet

$$\min_{n\geq 2}(n\lambda(x) - \lambda(n!)) \geq \min_{n\geq 2}(n\lambda(x) - \frac{n-1}{p-1}) = \frac{1}{p-1} + 2(\lambda(x) - \frac{1}{p-1}) > \lambda(x) \ .$$

Donc

$$\lambda(\exp x - 1) = \min_{n\geq 1}(\lambda(\frac{x^n}{n!})) = \lambda(\frac{x}{1!}) = \lambda(x) \quad .$$

Remarque. - Si deux des quantités $\exp x$, $\exp y$, $\exp(x+y)$ sont définies, la troisième l'est aussi et elles vérifient

$$(\exp x)(\exp y) = \exp(x+y) \quad ;$$

en effet, la boule $\lambda(x) > \frac{1}{p-1}$ est un sous-groupe additif de K . De plus les séries formelles $\exp X$, $\exp Y$, $\exp(X+Y)$ vérifient l'identité ci-dessus, donc si ces trois séries convergent, leur somme la vérifie aussi.

PROPOSITION 13. Logarithme. - La série $\sum_{n\geq 1} (-1)^n \frac{x^n}{n}$ converge pour $\lambda(x) > 0$ et diverge pour $\lambda(x) \leq 0$, sa somme est appelée logarithme de $1 + x$ $(\log(1 + x))$. Lorsque $\lambda(x) > \frac{1}{p-1}$,

$$\exp(\log(1 + x)) = x \quad .$$

On a

$$0 \leq \lambda(n) \leq \frac{\log n}{\log p} \quad \text{avec} \quad \lambda(n) = 0 \quad \text{si} \quad (n , p) = 1$$

et

$$\lambda(n) = \frac{\log n}{\log p} \quad \text{si} \quad n = p^h \quad .$$

Donc

$$\omega = \underline{\lim}\left(-\frac{\lambda(1/n)}{n}\right) = 0$$

et la série logarithme converge pour $\lambda(x) > 0$. De plus

$$\lambda(\log(1 + x)) \geq \min_{n\geq 0}(n\,\lambda(x) - \lambda(n)) \geq \min_{n\geq 0}(n\lambda(x) - \frac{\log n}{\log p})$$

soit

$$\lambda(\log(1 + x)) \geq \min_{h\geq 0}(p^h\,\lambda(x) - h) \quad ,$$

or $p^h - h$ atteint son minimum pour $hp^{h-1}\,\lambda = 1$; pour $\lambda(x) > \frac{1}{p-1}$ ce minimum est atteint une seule fois pour $h = 0$ et vaut $\lambda(x) > \frac{1}{p-1}$, alors $\exp(\log(1 + x)) = x$. Nous étudierons plus loin à l'aide du polygône de Newton, les valeurs prises par $\lambda(\log(1 + x))$.

PROPOSITION 14. Fonction puissance a^x . - Soient $a \in K$, $\lambda(a - 1) > 0$, et x tel que $\lambda(x) > \frac{1}{p-1} - \lambda(\log a)$ alors $a^x = \exp(x \log a)$ est définie, et si $\lambda(y) > \frac{1}{p-1} - \lambda(\log a)$

$$a^x\, a^y = a^{x+y} \quad .$$

COROLLAIRE. - Si $\lambda(a-1) > \frac{1}{p-1}$, a^x est défini quel que soit x, $|x| \leqslant 1$.

Application.

THÉORÈME 14 (MAHLER [Voir la bibliographie à la fin de l'exposé]. - Soit $R(z)$ une fraction rationnelle dont les coefficients sont des nombres algébriques (sur $\mathbb{Q}$). Supposons que

$$R(z) = \sum_{n=0}^{+\infty} w_n z^n$$

soit la série de Taylor de R à l'origine. S'il y a une infinité d'indices n tels que $w_n = 0$, les n tels que $w_n = 0$ sont, sauf peut-être un nombre fini d'entre eux, les termes d'un nombre fini de progressions arithmétiques de même raison.

Soient en effet $1/\alpha_1, \ldots, 1/\alpha_r$ les pôles de $R(z)$, $\frac{1}{\alpha_i}$ ayant la multiplicité ν_i. On a

$$R(z) = r(z) + \sum_{i=1}^{r} \left(\frac{\mu_i^0}{(1-\alpha_i z)^{\nu_i}} + \frac{\mu_i^1}{(1-\alpha_i z)^{\nu_i - 1}} + \ldots + \frac{\mu_i^{\nu_i - 1}}{(1-\alpha_i z)} \right)$$

où $r(z)$ est un polynôme de degré $n_0 - 1$.

Or

$$\frac{\mu}{(1-\alpha z)^{\nu}} = \sum_{n=0}^{+\infty} \mu \frac{(k+n-1)\ldots(n+1)}{(k-1)!} \alpha^n z^n .$$

Donc pour $n \geqslant n_0$, on a

$$w_n = \sum_{r=1}^{s} P_r(n) \alpha_r^n$$

où $P_r(n)$ est un polynôme en n de degré $\nu_r - 1$.

$R(z)$ est à coefficients algébriques, et les $P_r(n)$ aussi.

Soit $a \in \mathbb{Z}$ tel que $a\alpha_1 = \gamma_1, \ldots, a\alpha_r = \gamma_r$ où $\gamma_1 \ldots \gamma_r$ sont des entiers algébriques. Posons

$$v_n = a^n w_n = \sum_{r=1}^{s} P_r(n) \gamma_r^n$$

et

$$R^*(z) = \sum_{n=0}^{\infty} v_n z^n \quad ,$$

alors $R^*(z) - R(az)$ est un polynôme.

Soient maintenant p un nombre premier fixé, premier à $N(\gamma_1)$, ... , $N(\gamma_r)$, et K une extension finie de Q_p contenant γ_1 , ... , γ_r , qui sont des unités de K d'après la proposition 10.

Nous avons montré qu'il existe des entiers positifs m_1 , ... , m_r tels que

$$\lambda(\gamma_i^{m_i} - 1) > \frac{1}{p-1} \quad ;$$

soit m un multiple commun de m_1 , ... , m_r , alors

$$\lambda(\gamma_i^{m} - 1) > \frac{1}{p-1} \quad \text{pour} \quad i = 1 \ , \ \dots \ , \ r$$

$$f_h(x) = \sum_{i=1}^{r} P_i(mx + h)\, \gamma_i^h\, \gamma_i^{mx}$$

a donc, pour $h = 0$, 1 , ... , $m - 1$, un développement en série entière convergent pour $x \in K$, $|x|_p < 1$.

Or $f_h(k) = w_{mk+h}$ pour $mk + h \geq n_0$ donc, pour l'une au moins des valeurs de h , $f_h(x)$ a une infinité de zéros tels que $|x|_p < 1$, donc $f_h(x)$ est identiquement nulle dans A .

Soit alors $k_0 - 1 = [\frac{n_0 - h}{m}]$; pour $k \geq k_0$ on a

$$w_{mk+h} = 0 \ , \text{ donc } v_{mk+h} = 0 \quad \text{pour} \quad k \geq k_0 \quad ,$$

et ceci est vrai pour chaque valeur de h pour laquelle $f_h(k)$ a une infinité de zéros.

Remarque. - Soit $R(z) = \frac{P(z)}{Q(z)}$ tel que $dg\ P < dg\ Q$. Alors $n_0 = 0$.

Soit S une racine primitive m-ième de 1 .

Soit $Q^*(z^m) = Q(z).Q(Sz) \dots Q(S^{m-1} z)$, et soit

$$P^*(z) = P(z).Q(Sz) \dots Q(S^{m-1} z) \ , \quad R(z) = \frac{P^*(z)}{Q^*(z)} \quad .$$

Alors

$$P^*(z) = Q^*(z^m) \sum_{n=0}^{+\infty} w_n z^n \quad ,$$

où $w_n = 0$ lorsque $n \equiv h \pmod m$. Donc si $P^*(z) = \sum_{n=0}^{d} c_n z^n$, $c_n = 0$ pour $n \equiv h \pmod m$. Alors

$$P^*(z) + S^{-h} P^*(Sz) + \ldots + S^{-(m-1)h} P^*(S^{m-1} z) = 0$$

et

$$R(z) + S^{-h} R(Sz) + \ldots + S^{-(m-1)h} R(S^{m-1} z) \equiv 0$$

entraînent que, si α est un pôle de $R(z)$, il existe un pôle β de $R(z)$ tel que

$$\beta = S^{h} \alpha \, , \qquad h \not\equiv 0 \pmod m \quad .$$

IV. Polygones de Newton. Séries de Laurent.

A. Définitions.

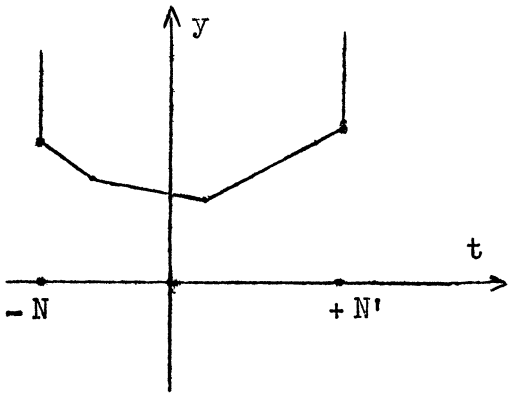
Soient K une extension algébrique finie ou non de Q_p , A son anneau des entiers.

Point représentatif de $a_n x^n$. - Soit $a_n x^n$, $a_n \neq 0$, $a_n \in K$, un monôme ($n \in Z$, de signe quelconque). On convient de représenter ce monôme dans le plan des (t , y) par le point A_n : $t = n$, $y = + \log_p |a_n|_p = - \lambda(a_n)$.

Ensemble représentatif d'une série de Laurent. - Soit $f(x) = \sum_{n=-\infty}^{+\infty} a_n x^n$ une série de Laurent, $a_n \in K$; l'ensemble F des points représentant les monômes non nuls de F est appelé ensemble représentatif de f .

Polygone de Newton de f . - Le polygone de Newton $P(f)$ de f est l'enveloppe inférieure convexe de F (éventuellement réduite à $y = - \infty$ si $\lambda(a_n) \to - \infty$ quand $|n| \to + \infty$, ou à $y = + \infty$ si $f = 0$).

Remarques. - Pour une partie finie de F comprise entre les abscisses $-N$ et $+N'$, l'enveloppe inférieure convexe est la réunion d'une ligne polygonale convexe finie, dont les sommets sont des points de F, et de deux demi-droites d'abscisses $+N'$ et $-N$. Le polygone de Newton de F, qui est l'enveloppe inférieure de ces lignes polygonales, est donc tel que toutes ses parties finies sont des lignes polygonales dont les sommets sont des points de F.



Supposons que $P(f)$ ne soit ni $y = +\infty$ ni $y = -\infty$, et soit μ_n la pente du côté de $P(f)$ qui rencontre les droites $t = n$ et $t = n+1$. Si $a_m = 0$ pour $m \geqslant n$, $\mu_n = +\infty$ et si $a_m = 0$ pour $m \leqslant n$, $\mu_n = -\infty$.

On appelle pentes asymptotiques $\nu_1 < \nu_2$ de $P(f)$ les nombres

$$\nu_1 = \underline{\lim_{|n|\to+\infty}}\ \mu_n$$

et

$$\nu_2 = \overline{\lim_{|n|\to+\infty}}\ \mu_n \quad .$$

Puisque, si $P(f)$ est $y = +\infty$, on convient que $\nu_1 = +\infty$, $\nu_2 = +\infty$, et si $P(f)$ est $y = -\infty$ on convient que $\nu_1 = \nu_2 = -\infty$, on a aussi

$$\mu_n \leqslant \mu_{n'} \text{ pour } n \leqslant n' \quad ,$$

$$\nu_1 = \lim_{n\to-\infty} \mu_n \text{ et } \nu_2 = \lim_{n\to+\infty} \mu_n \quad .$$

Soit μ_i la pente d'un côté de $P(f)$, $y = \mu_i t + m_i$ l'équation de son support, alors $\lambda(a_n) \geqslant n\mu_i + m_i$, $\forall\ n$, et il existe $n_i \geqslant i+1$ et $n_i' \leqslant i$ tels que $\lambda(a_{n_i}) = n_i \mu_i + m_i$ et $\lambda(a_{n_i'}) = n_i' \mu_i + m_i$.

PROPOSITION 15. - $\nu_1 = -\overline{\lim_{n\to-\infty}} \dfrac{\lambda(a_n)}{n}$ et $\nu_2 = \underline{\lim_{n\to+\infty}} \dfrac{\lambda(a_n)}{n}$.

Si $n \geqslant 0$, $\dfrac{\lambda(a_n)}{n} \geqslant \mu_i + \dfrac{m_i}{n}$, et il existe $n_i \geqslant i + s$ pour lequel on a égalité, donc

$$\varliminf_{n \to +\infty} \frac{\lambda(a_n)}{n} \geqslant \mu_i \quad \text{quel que soit } i \quad ,$$

d'où

$$\varliminf_{n \to +\infty} \frac{\lambda(a_n)}{n} \geqslant \nu_2 \quad .$$

De plus, pour $i > 0$, $m_{i+1} \leqslant m_i \leqslant m$ fixé , donc

$$\frac{\lambda(a_{n_i})}{n_i} \leqslant \mu_i + \frac{m}{n_i} \leqslant \mu_i + \frac{m}{i+1} \quad ,$$

donc

$$\varliminf_{n_i \to +\infty} \frac{\lambda(a_{n_i})}{n_i} \leqslant \nu_2 \quad ;$$

or

$$\varliminf_{n_i \to +\infty} \frac{\lambda(a_{n_i})}{n_i} \geqslant \varliminf_{n \to +\infty} \frac{\lambda(a_n)}{n} \quad ,$$

d'où

$$\nu_2 = \varliminf_{n \to +\infty} \frac{\lambda(a_n)}{n} \quad .$$

Si $n \leqslant 0$,

$$\frac{\lambda(a_n)}{n} \leqslant -\mu_i = \frac{m_i}{n} \quad ,$$

et il existe $n'_i \leqslant i$ pour lequel on a égalité. Donc

$$\varlimsup_{n \to -\infty} \frac{\lambda(a_n)}{n} \leqslant -\mu_i \quad \text{quel que soit } i \quad .$$

Soit

$$\overline{\lim_{n\to\infty}} \frac{\lambda(a_n)}{n} \leqslant \underline{\lim_{|i|\to+\infty}} (-\mu_i) = -\nu_1 \quad .$$

De même

$$\underline{\lim_{i\to-\infty}} \left(\frac{\lambda(a_{n'_i})}{n'_i}\right) = \underline{\lim_{i\to-\infty}} \left(-\mu_i + \frac{m_i}{n'_i}\right) \geqslant \underline{\lim_{i\to-\infty}} \left(-\mu_i + \frac{m_i}{i}\right) = -\nu_1$$

d'où

$$\overline{\lim_{n\to-\infty}} \frac{\lambda(a_n)}{n} = -\nu_1 \quad .$$

B. Application aux séries de Laurent.

THÉORÈME 15. - Soient ν_1 et ν_2 les pentes asymptotiques du polygone de Newton de la série de Laurent

$$f(x) = \sum_{n=-\infty}^{+\infty} a_n x^n \quad .$$

Si $-\nu_2 < \lambda(x) < -\nu_1$, $f(x)$ converge, et si $-\nu_1 < \lambda(x)$ ou $-\nu_2 > \lambda(x)$, $f(x)$ diverge.

Ce théorème résulte presque immédiatement de la proposition 15 :

Soit $\lambda(x) = -\nu_2 + \lambda_2$, $\lambda_2 > 0$ et $\lambda(x) = -\nu_1 + \lambda_1$, $\lambda_1 < 0$,

$$\lambda(a_n x^n) = n\lambda(x) + \lambda(a_n) = n\left(\lambda_2 + \frac{\lambda(a_n)}{n} - \nu_2\right) = n\left(\lambda_1 + \frac{\lambda(a_n)}{n} - \nu_1\right)$$

pour $n \geqslant 0$, $\underline{\lim_{n\to+\infty}} \frac{1}{n} \lambda(a_n x^n) = \lambda_2 > 0$, donc $|a_n x^n| \to 0$ quand $n \to +\infty$,

pour $n < 0$, $\overline{\lim_{n\to-\infty}} \left(\frac{1}{|n|} \lambda(a_n x^n)\right) = -\lambda_1 > 0$, donc $|a_n x^n| \to 0$ quand $n \to -\infty$.

Si $\lambda(x) > -\nu_1$, $\overline{\lim_{n\to-\infty}} \left(\frac{1}{|n|} \lambda(a_n x^n)\right) = -\lambda_1 < 0 \Longrightarrow |a_n x^n| \to +\infty$ quand n décrit une suite $\to -\infty$.

Si $\lambda(x) < -\nu_2$, $\underline{\lim}_{n\to-\infty} [\frac{1}{n}\lambda(a_n x^n)] = \lambda_2 < 0 \implies |a_n x^n| \to +\infty$ quand $n \to +\infty$.

Le polygone de Newton d'une série de Laurent permet donc de déterminer son domaine de convergence. Nous allons maintenant voir qu'il permet de situer ses zéros.

THÉORÈME 16 (SNIREIMAN). - Soient K une extension algébrique complète de Q_p , $f(x)$ une série de Laurent à coefficients dans K , $B_j B_{j+1}$ un côté fini de $P(f)$, λ_j la pente de $B_j B_{j+1}$, n_j la longueur de la projection sur l'axe des t de $B_j B_{j+1}$, alors :

il existe un polynôme $P(x) \in K[x]$, de degré n_j , dont les zéros dans Ω_p sont d'ordre $-\lambda_j$, et une série de Laurent $g(x)$, à coefficients dans K , ayant même domaine de convergence que f , tel que $P(g)$ n'ait aucun côté de pente λ_j , et l'on a

$$f(x) = P(x)\, g(x) \quad .$$

De plus, cette décomposition est unique si on fixe par exemple $P(0) = 1$.

1. - Soient N_j et $N_j + n_j$ les abscisses de B_j et B_{j+1} ; démontrons le théorème pour $N_j = 0$, $\lambda_j = 0$, $a_{N_j} = 1$. Nous ramènerons ensuite le cas général à celui-là.

Si $\lambda_j = 0$, f converge pour $|x| = 1$, et $a_0 = 1 \implies \lambda(a_n) \geqslant 0$, $\forall$ n .

Notations. - Soit $h(x) = \sum_{n=-\infty}^{+\infty} h_n x^n$ convergente pour $|x| = 1$, nous poserons

$$M(h) = \sup_n(|h_n|) \quad \text{et} \quad \lambda(h) = \inf_n(\lambda(h_n)) = \lambda(M(h)) \quad .$$

Nous appellerons pseudo-polynôme une série de Laurent finie $\psi(x)$ que nous écrirons

$$\psi(x) = \sum_{i=m}^{q} \psi_i x^i \quad \text{avec} \quad \psi_m \psi_q \neq 0 \quad .$$

Alors $x^{-m}\psi(x)$ est un polynôme de degré $q - m$.

LEMME 16. 1. - Soient $\psi(x) = \sum_{i=m}^{q} \psi_i x^i$ un pseudo-polynôme, et $P(x) = \sum_{j=0}^{n} b_j x^j$ un polynôme de degré n tel que $|b_0| = |b_n| = 1$ et $|b_i| \leqslant 1$.

Alors il existe un pseudo-polynôme $\varphi(x)$ et un polynôme $R(x)$ de degré $< n$ tels que :

$$\psi(x) = P(x)\ \varphi(x) + R(x)$$

avec

$$M(\varphi) \leqslant M(\psi) \quad \text{et} \quad M(R) \leqslant M(\psi) \qquad .$$

En effet, si $m \geqslant 0$, ceci est le théorème classique de division des polynômes suivant les puissances décroissantes.

Si $m < 0$, on a

$$x^{-m}\ \psi(x) = P(x)\ Q_1(x) + x^{-m}\ R_1(x)$$

par division de $x^{-m}\,\psi$ par P suivant les puissances croissantes, arrêtée à l'ordre m , où Q_1 et R_1 sont des polynômes tels que $M(Q_1) \leqslant M(\psi)$ et $M(R_1) \leqslant M(\psi)$.

Puis, en divisant R_1 par P suivant les puissances décroissantes :

$$R_1(x) = P(x)\ Q_2(x) + R(x) \ , \quad \text{avec} \quad dg\ R < n$$

et

$$M(Q_2) \leqslant M(R_1) \quad \text{et} \quad M(R) \leqslant M(R_1) \qquad .$$

Alors

$$\psi(x) = P(x)[Q_1(x) + x^{-m}\ Q_2(x)] + R(x)$$

est la décomposition annoncée, en posant

$$\varphi(x) = Q_1(x) + x^{-m}\ Q_2(x) \qquad .$$

LEMME 16. 2. - Soit $f(x)$ une série de Laurent à coefficients dans K complet, si $f(x) = P(x) + g(x)$, où $P(x) = a_0 + a_1 x + \ldots + a_q x^q$, $|a_0| = |a_q| = 1$,

$|a_i| \leqslant 1$, et $g(x) = \sum_{n=-\infty}^{+\infty} g_n x^n$, où $|g_n| < 1$, alors il existe un polynôme $\Pi(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_q x^q$, $|\alpha_0| = |\alpha_q| = 1$, $|\alpha_i| \leqslant 1$, et une série de Laurent $\gamma(x) = \sum_{-\infty}^{+\infty} \gamma_n x^n$, $|\gamma_n| < 1$ pour $n \neq 0$ et $|\gamma_0| = 1$, tels que $f(x) = \pi(x)\ \gamma(x)$, et γ a même domaine de convergence que f .

Ce lemme se démontre par récurrence.

Posons

$$\varphi_0 = 1 \ , \quad P_0 = 1 + x^q \ , \quad g_0 = f(x) - (1 + x^q)$$

$$\varphi_1 = 1 \ , \quad P_1 = P(x) \ , \quad g_1 = g(x) \ .$$

Et supposons qu'on ait construit des suites φ_j , P_j , g_j , jusqu'à l'ordre k de telle sorte que :

$$f(x) = \varphi_k(x)\ P_k(x) + g_k(x)$$

où $P_k(x)$ est un polynôme de degré q à coefficients $a_{k,j}$ entiers, avec $|a_{k,} \ | = a_{k,q}| = 1$,

$\varphi_k(x)$ est un pseudo-polynôme tel que $|\varphi_{k,0}| = 1$, $|\varphi_{k,n}| < 1$ pour $n \neq 0$,

$g_k(x)$ est une série de Laurent, convergente pour $\lambda(x) = 0$,

avec :

$$\lambda(\varphi_k - \varphi_{k-1}) \geqslant k - 1$$

$$\lambda(P_k - P_{k-1}) \geqslant k - 1$$

$$\lambda(g_k) \geqslant k \ .$$

Ceci est vrai pour $k = 1$.

$g_k(x)$ converge pour $\lambda(x) = 0$, donc ne contient qu'un nombre fini de monômes dont le coefficient a un ordre $\leqslant k + 1$, soit donc

$$g_k(x) = \psi_k(x) + h_k(x)$$

où $\psi_k(x)$ est un pseudo-polynôme, $\lambda(\psi_k) \geqslant k$, et $h_k(x)$ est une série de Laurent convergente pour $\lambda(x) = 0$, $\lambda(h_k) \geqslant k + 1$.

Appliquons le lemme 1 à ψ_k et P_k, nous obtenons :

$$\psi_k(x) = P_k(x)\ \gamma_k(x) + R_k(x) \quad \text{avec} \quad \lambda(\gamma_k) \geqslant k \quad \text{et} \quad \lambda(R_k) \geqslant k \quad .$$

Posons

$$P_{k+1} = P_k + R_k$$

$$\varphi_{k+1} = \varphi_k + \gamma_k$$

$$g_{k+1} = h_k - R_k[\varphi_k + \gamma_k - 1]$$

P_{k+1} est un polynôme de degré q ; $\lambda(P_{k+1} - P_k) \geqslant k$, donc si $k > 1$, $|a_{k+1,0}| = |a_{k+1,q}| = 1$,

φ_{k+1} est un pseudo-polynôme et $\lambda(\varphi_{k+1} - \varphi_k) \geqslant k$, donc si $k > 0$, $|\varphi_{k+1,0}| = |\varphi_{k,q}| = 1$ et $|\varphi_{k+1,n}| < 1$ pour $n \neq 0$, q ,

g_{k+1} est une série de Laurent, convergente comme h_k pour $\lambda(x) = 0$, et

$$\lambda(g_{k+1}) \geqslant \min[\lambda(h_k)\ ;\ \lambda(R_k) + \lambda(\varphi_k + \gamma_k - 1)]$$

or

$$\lambda(\varphi_k - 1) = \lambda(\varphi_k - \varphi_1) \geqslant 1\ ,\ \lambda(\gamma_k) \geqslant k\ ,\ \lambda(R_k) \geqslant k\ ,\ \lambda(h_k) \geqslant k + 1 \quad ,$$

donc

$$\lambda(g_{k+1}) \geqslant \min(k + 1\ ,\ k + 1) \geqslant k + 1 \quad .$$

Il est alors clair que, K étant complet,

P_k converge vers un polynôme $H(x)$ vérifiant les conditions de l'énoncé,

g_k converge vers 0 ,

φ_k converge vers une série de Laurent γ, convergente pour $\lambda(x) = 0$, car $\lambda(\gamma - \varphi_k) > k$, et telle que $|\gamma_0| = 1$ et $|\gamma_n| < 1$ pour $n \neq 0$,

$f(X) = P(X)\ g(X)$ en tant que séries formelles.

Il reste à montrer que γ a même domaine de convergence que f. On a

$$f_n = \alpha_0\ \gamma_n + \alpha_1\ \gamma_{n-1} + \cdots + \alpha_q\ \gamma_{n-q} \quad .$$

Or, $\gamma(x)$ converge pour $\lambda(x) = -\nu \iff \lambda(\gamma_n) \geq \nu n + \mu$, μ fini, si ν n'est pas une pente asymptotique de γ, alors

$$\lambda(f_n) \geq \inf(\lambda(\gamma_n), \dots, \lambda(\gamma_{n-q})) = \inf(\nu n + \mu, \dots, \nu(n-q) + \mu)$$

soit

$$\text{si } \nu > 0, \quad \lambda(f_n) \geq \nu n + (\mu - nq)$$

$$\text{si } \nu < 0, \quad \lambda(f_n) \geq \nu n + \mu \quad .$$

Donc $f(x)$ converge lorsque $\gamma(x)$ converge.

D'autre part, soit $-\nu$ tel que $f(x)$ converge pour $\lambda(x) = -\nu$, alors $\lambda(f_n) \geq \nu n + \mu$, μ fini. Soit μ' tel que $\mu' \leq \mu$, et $\lambda(\gamma_i) \geq i\nu + \mu'$ pour $i = 0, 1, \dots, q-1$.

On a

$$\lambda(\gamma_n) \geq \inf(\lambda(f_n), \lambda(\gamma_{n-1}), \dots, \lambda(\gamma_{n-q})), \text{ supposons } \lambda(\gamma_k) \geq \nu k + \mu' \text{ pour } 0 \leq k \leq n-1$$

$$\geq \inf(\nu n + \mu', \nu(n-1) + \mu', \dots, \nu(n-q) + \mu') \quad .$$

Donc si $\nu < 0$, on a

$$\lambda(\gamma_n) \geq \nu n + \mu' \quad \text{pour} \quad n \geq 0 \quad .$$

La partie entière de $\gamma(x)$ converge donc à l'extérieur de $|x| = 1$ dans le même domaine que f, or $\sum_{n<0} \gamma_n x^n$ converge pour $|x| \geq 1$, donc pour $|x| \geq 1$, f et g ont même domaine de convergence.

De même,

$$\lambda(\gamma_n) \geq \inf(\lambda(f_{n+q}), \lambda(\gamma_{n+1}), \dots, \lambda(\gamma_{n+q})) \quad .$$

Soit μ' tel que $\lambda(f_{n+q'}) \geq n\nu + \mu'$, $\lambda(\gamma_i) \geq \nu i + \mu'$ pour $i = 0, 1, \dots, q-1$.

Si $\nu > 0$, supposons que $\lambda(\gamma_k) \geq \nu k + \mu$ pour $n+1 \leq k \leq q-1$, alors

$$\lambda(\gamma_n) \geqslant \inf(\nu n + \mu' , \nu(n+1) + \mu' , \ldots) \geqslant \nu n + \mu' \quad ,$$

pour $n \leqslant 0$ on a

$$\lambda(\gamma_n) \geqslant \nu n + \mu'$$

et $\sum_{n \leqslant 0} \gamma_n x^n$ converge en même temps que f pour $|x| \leqslant 1$. La partie entière de γ converge quel que soit x, $|x| \leqslant 1$, donc γ et f ont même domaine de convergence, et le lemme est démontré.

LEMME 16.3. - Soient $f(x)$ une série de Laurent et $P(f)$ son polygone de Newton. Soit ν un nombre réel qui ne soit pas la pente d'un côté du polygone $P(f)$, et tel que $f(x)$ converge pour $\lambda(x) = -\nu$, alors, si $x \in \hat{\Omega}_p$, $\lambda(x) = -\nu$,

$$|f(x)| = M(|x|) = \sup_n |a_n| |x|^n$$

sur ce cercle.

Supposons qu'il existe n et n', $n < n'$ par exemple, tels que

$$|a_n| |x|^n = |a_{n'}| |x|^{n'} = M(|x|) \quad ,$$

alors on a

$$\lambda(a_n) + n\lambda(x) = \lambda(a_{n'}) + n' \lambda(x)$$

soit

$$\frac{\lambda(a_{n'}) - \lambda(a_n)}{n' - n} = \lambda(x) = -\nu \quad .$$

Or A_n et $A_{n'}$ sont sur $P(f)$ car

$$\lambda(M(|x|)) = \inf_q(-q\nu + \lambda(a_q)) = \lambda(a_n) - n\nu = \lambda(a_{n'}) - n\nu \quad ,$$

alors $P(f)$ aurait un côté de pente ν, ce qui est contraire à l'hypothèse. Donc il existe au plus un n tel que $|a_{n_0}| |x^{n_0}| = M(|x|)$, et il en existe un puisque

$$\lim_{|n| \to +\infty} |a_n| |x|^n = 0 \quad .$$

Soit n_0 cet indice, alors

$$|a_0 x_0^{n_0} + \sum_{n \neq n_0} a_n x^n| = |a_0 x_0^{n_0}| \quad \text{pour} \quad \lambda(x) = -\nu \quad .$$

Or si f n'est pas nulle, $M(|x|) \neq 0$, donc :

COROLLAIRE. - f n'a aucun zéro dans $\hat{\Omega}_p$ sur le cercle $\lambda(x) = -\nu$ si $P(f)$ n'a aucun côté de pente ν.

Nous sommes maintenant en mesure d'achever la démonstration du théorème : la série $\gamma(x)$ n'a aucun zéro sur le cercle $\lambda(x) = 0$, donc Π et γ sont uniques, car, si R' et γ' satisfaisaient au lemme, avec $\Pi(0) = \Pi'(0) = 1$, $f(x)$ aurait, dans $\hat{\Omega}_p$ sur le cercle $|x| = 1$, les zéros de Π et ceux-là seulement, puisque $f = \Pi\gamma$, $\gamma(x) \neq 0$, $|x| = 1$, et de même ceux de Π' et ceux-là seulement, du fait que $f = \Pi' \gamma'$, $\gamma'(x) \neq 0$ si $|x| = 1$, ce qui est absurde si $\Pi \neq \Pi'$. Or le lemme 2, avec unicité de Π et γ, est exactement le théorème 15 dans le cas 1.

2. - Posons

$$f_1(x) = \frac{1}{a_{N_j} x^{N_j}} f(x) \quad \text{et} \quad f_2(y) = f_1(ry)$$

où r est un nombre algébrique sur K, et tel que $\lambda(r) = \lambda_j$. Soit $K' = K(r)$.

$f_2(y)$ est à coefficients dans K', son polygone de Newton a un côté de pente 0 de longueur n_j commençant au point $(0, 0)$, donc il existe P_2 et g_2 tels que $f_2(y) = P_2(y)\, g_2(y)$, P_2 et g_2 étant déterminés de façon unique.

$P_2(y)$ polynôme de degré n a, dans Ω_p, toutes ses racines sur le cercle $|x| = 1$. Soient alors

$$P(x) = P_2\left(\frac{x}{r}\right) \quad \text{et} \quad g(x) = a_{N_j} x^{N_j} g_2\left(\frac{x}{r}\right) \quad ,$$

on a

$$f = Pg \quad .$$

P et g sont à coefficients dans K' , le polygone de Newton de g n'a aucun côté de pente λ_i (celui de g_2 n'a aucun côté de pente 0) et les zéros de P , dans Ω_p , sont sur le cercle $\lambda(x) = -\lambda(r) = -\lambda_i$, de plus g a même domaine de convergence que f (g_2 ayant même domaine que f_2). Une telle décomposition $f = Pg$ est donc nécessairement unique, puisque déterminée par les zéros de f sur le cercle $\lambda(x) = -\lambda_i$.

Supposons que les coefficients de P et g , qui sont dans K' , ne soient pas tous dans K . Soient $K_1 = K'$, K_2 , ... , K_m les corps conjugués de K' par rapport à K , P_i et g_i les conjugués de P et g , alors on a aussi $f = P_i g_i$ qui satisfait aux conditions du lemme, et il existe $i \neq 1$ tel que $P_i \neq P$ ou $g_i \neq g$, ceci est absurde à cause de l'unicité, donc P et g sont à coefficients dans K et le théorème est démontré.

COROLLAIRE 1. - Dans la clôture algébrique $\hat{\Omega}_p$ de Q_p , les zéros d'une série de Laurent f(x) à coefficients dans une extension K de Q_p , intérieurs à la couronne de convergence, sont situés sur les cercles $\lambda(x) = -\lambda_i$ où λ_i est la pente d'un côté fini du polygone de Newton de f , et ce sont les zéros du polynôme P(x) intervenant dans la décomposition de Šnirelman de f .

COROLLAIRE 2. - Soit f(x) une série de Laurent non nulle, convergente pour $a \leqslant |x|_p \leqslant b$, f(x) n'a, dans Ω_p , qu'un nombre fini de zéros ξ tels que $a < |\xi| < b$.

COROLLAIRE 3. - Soit $f(x) = \sum_{-\infty}^{+\infty} a_n x^n$ une série de Laurent telle que $a_0 = 0$; si le corps K est complet algébriquement clos, les valeurs prises par f(x) forment un disque ouvert ou fermé.

Soit $a \in K$, f(x) - a a même couronne D de convergence que f .

- Supposons que $f(x) \neq a$ quel que soit $x \in D$, alors le polygone de Newton de f(x) - a n'a aucun côté fini, Soit a' tel que $|a'| \geqslant |a|$, alors le polygone de Newton de f(x) - a' , n'a a fortiori aucun côté fini, et $f(x) \neq a'$, $\forall\ x \in D$.

- Supposons que f(x) - a ait des zéros dans D , alors son polygone de Newton a un côté fini au moins, et a fortiori celui de f(x) - a' aussi pour $|a'| \leqslant |a|$.

Inégalités de Cauchy pour une série de Laurent.

THÉORÈME 17. - Soit $f(x) = \sum a_n x^n$ une série de Laurent, $a_n \in K$, et soit

r tel que $f(x)$ converge pour $x \in \Omega_p$, $|x| = r$.

Si $M(r) = \sup_n(|a_n| r^n)$, alors $\forall\ x \in \Omega_p$ tel que $|x| = r$, on a $|f(x)| \leqslant M(r)$

1° si $-\log r$ n'est pas la pente d'un côté de $P(f)$, on a

$$|f(x)| = M(r) \ , \quad \forall\ x \in \hat{\Omega}_p \ , \quad |x| = r \qquad ,$$

2° si $-\log r$ est la pente d'un côté de $P(f)$,

$|f(x)|$ prend toute valeur γ , $0 \leqslant \gamma \leqslant M(r)$, lorsque $x \in \Omega_p$, $|x| = r$.

Le (1°) est le lemme 16.3.

(2°). Soit $f = P(x)\, g(x)$ la décomposition de Snirelmann de f relative au côté de pente $-\log r$. Supposons $r = 1$ en faisant éventuellement une homothétie dans Ω_p . Alors $M_g(r) = M_f(r)$, pour $|x| = 1$, $|g(x)| = Mg(r)$. Il suffit donc de montrer que $|P(x)|$ prend, pour $|x| = 1$, toute valeur γ , $0 \leqslant \gamma \leqslant 1$. Soit $P(x) = 1 + a_1 x + \ldots + a_n x^n$, et soit $\alpha \in \Omega_p$ tel que $|1 - \alpha| = 1$ et $|\alpha| = \gamma$, l'équation $P(x) - \alpha = 0$ a n racines sur le cercle $|x| = 1$ de Ω_p .

COROLLAIRE (Théorème de Riemann). - Si $f(x) = \sum_{-\infty}^{+\infty} a_n x^n$ est une série de Laurent convergente pour $0 < |x|_p \leqslant R$, et si pour ces valeurs $|f(x)|$ est borné, $f(x)$ est une série entière.

Soit en effet $R > r_1 > \ldots > r_n > \ldots$, $r_n \to 0$, une suite de nombres tels que $-\log r_n$ ne soit pas la pente d'un côté de $P(f)$, et soit M tel que $|f(x)| \leqslant M$ pour $0 < |x| \leqslant R$ alors quels que soient n et m , $|a_n| r_m^n \leqslant M$, en particulier soit $n > 0$,

$$|a_{-n}| \leqslant M r_m^n \ , \qquad \forall\ m \qquad ,$$

donc

$$|a_{-n}| = 0 \quad \text{pour} \quad n > 0 \qquad .$$

C. Applications aux séries entières.

Les séries entières sont des cas particuliers de séries de Laurent. De plus on a, pour les fonctions entières, le théorème suivant.

THÉORÈME 18. Produit de Weierstrass. - Soit $f(X)$ une série entière $\in K[[X]]$ qui ne soit pas un polynôme, convergente quel que soit $x \in \hat{\Omega}_p$, alors il existe une suite $P_n(x)$ de polynômes de $K[X]$, tels que $P_n(0) = 1$, les racines de P_n dans Ω_p ont un module r_n, $0 < r_1 < \ldots < r_n < \ldots$ et $r_n \to +\infty$ avec n,

$$f(X) = a_h X^h P_1(X) \ldots P_n(X) \ldots ,$$

et le produit

$$a_h x^h P_1(x) \ldots P_n(x) \ldots$$

converge vers $f(x)$ quel que soit $x \in \hat{\Omega}_p$.

Réciproquement un tel produit définit une fonction entière.

Soit $a_h x^h$ le premier monôme non nul de f, $f(x) = a_h x^h g(x)$ où g est une fonction entière telle que $g(0) = 1$.

Soit λ_1 la pente du premier côté de $P(g)$, il existe P_1 tel que $g = P_1 g_1$, $P_1(0) = 1$, les racines de P_1 ayant le module $r_1 = p^{\lambda_1}$, g_1, ayant même rayon de convergence que g, est aussi une fonction entière, $g_1(0) = 1$, et g_1 n'a aucun zéro de module $\leqslant r_1$. On construit ainsi par récurrence $P_1, \ldots, P_n$ satisfaisant aux conditions de l'énoncé, avec $r_k = p^{\lambda_k}$, λ_k pente du k-ième côté de $P(g)$, et tels que $g(x) = P_1(x) P_2(x) \ldots P_k(x) g_k(x)$ avec $g_k(0) = 0$, g_k étant une fonction entière dont le polygone de Newton a son premier côté de pente λ_{k+1}. Alors, si

$$g_k(x) = 1 + \sum_{n \geqslant 1} g_{n,k} x^n , \qquad \lambda(g_{n,k}) \geqslant nk ,$$

donc quand $k \to +\infty$,

$$\lambda(g_k - 1) \to +\infty ,$$

donc

$$g_k(x) \to 1 ,$$

de plus soient $\xi_{n,1}, \ldots, \xi_{n,\nu_n}$ les racines de $P_n(x)$, on a

$$P_n(x) = \prod_{k=1}^{\nu_n} (1 - \frac{x}{\xi_{n,k}}) \quad ,$$

et le produit

$$\prod_{n=1}^{+\infty} P_n(x) = \prod_{j=1}^{+\infty} (1 - \frac{x}{\xi_j})$$

où $|\xi_j| \leqslant |\xi_{j+1}|$ et $|\xi_j| \to +\infty$ avec j est convergent quel que soit x, vers $f(x)$.

Il est clair que réciproquement un tel produit définit une fonction entière.

COROLLAIRE 1. - Soient Ω un corps valué complet algébriquement clos, et $f(x)$ une fonction entière sur Ω qui ne soit pas un polynôme. Alors quel que soit $a \in \Omega$, l'équation $f(x) = a$ a une infinité dénombrable de solutions.

En effet $f(x) - a$ satisfait au théorème 18, et chaque polynôme $P_i(x)$ a toutes ses racines dans Ω.

COROLLAIRE 2. (LIOUVILLE). - Soit $f(x)$ une fonction entière sur Ω complet et algébriquement clos, s'il existe $a \in \Omega$ tel que $f(x) \neq a$, $\forall\ x \in \Omega$, $f(x)$ est une constante.

En effet $f(x)$ est nécessairement un polynôme d'après le corollaire 1, soit n son degré, $f(x) - a$ a n racines dans Ω, donc $n = 0$.

Ce corollaire est voisin du théorème de Liouville, mais plus fort.

Série de Taylor de $1/f(x)$.

PROPOSITION 16. - Soient $f(x)$ une série entière, telle que $f(0) \neq 0$, et $-\log R$ la pente du premier côté du polygone de Newton de f. Alors la série formelle $F(x) = \frac{1}{f(x)}$ a pour rayon de convergence R.

Supposons $f(0) = 1$, et posons $f(x) = 1 - \varphi(x)$, $\varphi(x) = \sum_{n \geqslant 1} a_n x^n$,

$$F(X) = \sum_{m \geqslant 0} (\varphi(X))^m = \sum_{n \geqslant 0} b_n X^n \quad .$$

Soit $r < R$, pour $|x| = r$, $|\varphi(x)| = \lambda < 1$ (car le polygone de Newton de φ est strictement au-dessus de celui de f, au moins pour $0 \leqslant r < 1$), alors

$$f(x) = \sum_{m \geqslant 0} (\varphi(x))^m$$

converge, donc aussi

$$\sum_{n \geqslant 0} b_n x^n$$

(ces deux séries formelles étant identiques).

Soit $r > R$, tel que $-\log r$ ne soit pas la pente d'un côté de $P(f)$, alors pour $|x| = r$, $|\varphi(x)| = \lambda > 1$ et $F(x)$ diverge.

V. Prolongement analytique.

Nous avons déjà remarqué, à propos du théorème 11, que la méthode de Weierstrass utilisée dans le plan complexe pour le prolongement analytique, ne permet pas de prolonger une fonction analytique dans un corps valué non archimédien. Nous utiliserons ici des suites uniformément convergentes de fractions rationnelles. Pour l'étude de ces suites nous avons besoin de quelques propriétés plus fines des séries de Laurent.

Inégalités de Cauchy.

PROPOSITION 17. - Soit Ω un corps valué complet, contenant Q_p, et tel qu'il existe une infinité d'entiers k tel que l'équation $x^k - 1 = 0$ ait k racines dans Ω (par exemple $\Omega = \hat{\Omega}_p$). Soit

$$f(x) = \sum_{n=-\infty}^{+\infty} a_n x^n \quad ,$$

$a_n \in \Omega$, une série de Laurent convergente pour $|x| = r$, et s'il existe $x \in \Omega$ tel que $|x| = r$, soit

$$M_f(r) = \sup_{|x|=r, x \in \Omega} |f(x)| \quad , \text{ alors } \forall \ n \ , \ |a_n| \leqslant \frac{M_f(r)}{r^n} \quad .$$

- Si $\Omega = \hat{\Omega}_p$, cette proposition découle du théorème 17.

- Si $-\log r$ n'est pas la pente d'un côté du polygone $P(f)$, la proposition résulte du (1°) du théorème 17.

- Si $-\log r$ est la pente d'un côté de $P(f)$, soit $\alpha \in \Omega$ tel que $f(\alpha) = r$, et soit $\beta \in \Omega$ tel que $|\beta| = M_f(r)$, alors

$$g(x) = \frac{1}{\beta} f(\alpha x) = \sum_{-\infty}^{+\infty} g_n x^n$$

converge pour $|x| = 1$, on a $M_g(1) = 1$, et il suffit de montrer que si

$$g(x) = \sum_{-\infty}^{+\infty} g_n x^n$$

converge pour $|x| = 1$ avec $M_g(1) = 1$, et si $\lambda = 0$ est la pente d'un côté de $P(g)$,

$$|g_n| \leqslant 1 \ , \ \forall \ n$$

Ceci revient encore à montrer que si $|g_n| \leqslant 1$, $\forall$ n, et s'il existe au moins deux indices tels que $|g_n| = 1$, $M_g(1) = 1$. Il est clair qu'alors $M_g(1) \leqslant 1$.

Soit

$$g(x) = \gamma(x) + h(x) \quad \text{où} \quad \gamma(x) = \sum_{j=m}^{s} \gamma_j x^j$$

est un pseudo-polynôme tel que $|\gamma_j| = 0$ ou 1, et $h(x)$ une série de Laurent telle que $\lambda(h) = \eta > 0$, il existe au moins deux indices j tels que $|\gamma_j| = 1$. On a $M_h(1) = \frac{1}{p^\eta} < 1$. Si nous montrons que $M_\gamma(1) = 1$, nous aurons démontré que $M_g(1) = 1$.

Soit $k > s - m$, $(k , p) = 1$, telle que $x^k - 1 = 0$ ait k racines $\xi_i \in \Omega$. Alors, pour j fixé,

$$\sum_{i=1}^{k} \xi_i^{-j} \gamma(\xi_i) = k\gamma_j$$

donc, quel que soit j, $m \leqslant j \leqslant s$, soit j tel que $|\gamma_j| = 1$, alors

$$|k\gamma_j| = |\gamma_j| = 1 \leqslant M_\gamma(j) \leqslant 1 \implies M_\gamma(1) = 1 \quad ,$$

et la proposition est démontrée.

Remarquons que $|g_n| = 1$ pour un nombre fini d'indices n seulement, donc

$$|a_n| = \frac{1}{r^n} M_f(r)$$

pour un nombre fini d'indices n seulement.

Définition. - Dans la suite Ω désignera toujours un corps vérifiant les hypothèses de la proposition 17.

THÉORÈME 19 (WEIERSTRASS). - Soit dans un corps Ω une suite de séries de Laurent

$$f_n(x) = \sum_{j=-\infty}^{+\infty} a_{n,j}\, x^j \quad ,$$

toutes convergentes pour $R' \leqslant |x| \leqslant R$.

Si $f_n(x)$ converge uniformément par rapport à x, pour $R' \leqslant |x| \leqslant R$, vers une fonction $f(x)$, alors $f(x)$ est la somme d'une série de Laurent convergente pour $R' < |x| < R$,

$$f(x) = \sum a_j\, x^j \text{ , et } a_j = \lim_{n\to\infty} a_{n,j} \quad .$$

Soit $f_{n,m} = f_n - f_m$, alors

$$f_{n,m} = \sum (a_{n,j} - a_{m,j})\, x^j \quad .$$

Soit alors r, $R' \leqslant r \leqslant R$, comme $f_n(x)$ converge uniformément en x, on a pour $n, m \geqslant N(\varepsilon)$,

$$M_{f_{n,m}}(r) \leqslant \varepsilon \quad ,$$

or

$$|a_{n,j} - a_{m,j}| \leqslant M_{f_{n,m}}(r)\, \frac{1}{r^j} \quad .$$

Donc, pour j fixé, $a_{n,j}$ est une suite de Cauchy, soit a_j sa limite. Pour $n \geqslant N(\varepsilon)$,

$$|a_{n,j} - a_j|\, r^j \leqslant \varepsilon \quad .$$

Or, $f(x)$, limite uniforme de fonctions continues, est continue, donc il existe M tel que $|f(x)| \leqslant M$ pour $R' \leqslant |x| \leqslant R$, soit $M \geqslant \varepsilon$, alors pour $n \geqslant N(\varepsilon)$

$$|f_n(x)| \leqslant \max(|f(x)|\ ,\ \varepsilon) \leqslant M \quad \text{pour} \quad R' \leqslant |x| \leqslant R \quad .$$

$$\left.\begin{array}{l} \text{Alors } |a_{n,j}|\, r^j \leqslant M \\ \text{[illegible]}\ |a_j|\, r^j \leqslant M \end{array}\right\} \quad \begin{array}{l} \text{pour } n \geqslant N(\varepsilon)\ ,\ \forall\ j \text{ et } R' \leqslant r \leqslant R \\ \text{pour tout } j \text{ et tout } r\ ,\ R' \leqslant r \leqslant R \end{array} \quad ,$$

la série de Laurent $\varphi(x) = \sum a_j\, x^j$ converge donc pour $R' < |x| < R$, et dans ce domaine, pour $n \geqslant N(\varepsilon)$,

$$|f_n(x) - \varphi(x)| \leqslant \varepsilon \quad ,$$

donc

$$\varphi(x) = f(x) \quad .$$

Valeur absolue d'une fraction rationnelle.

Commençons par étudier la valeur absolue d'un polynôme.

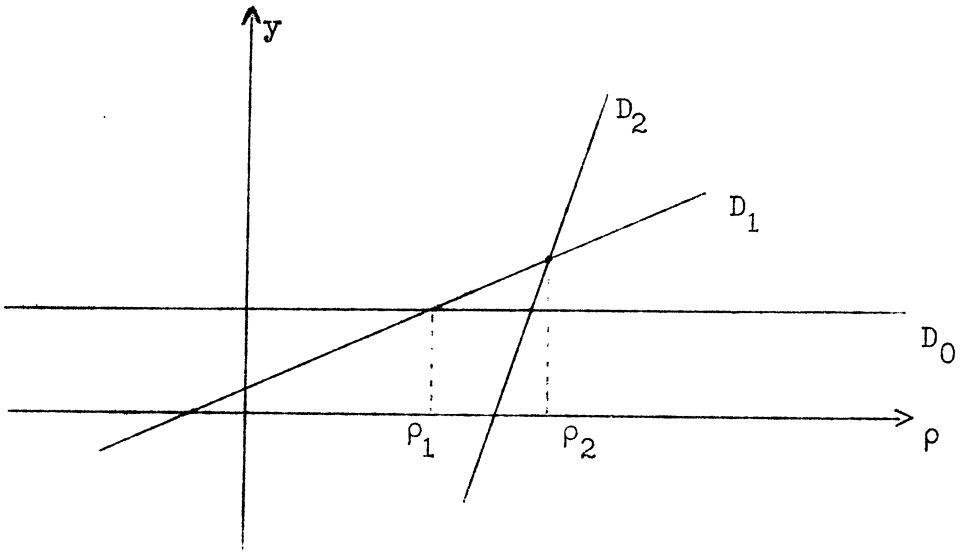
Soit

$$P(x) = a_0 + a_1\, x + \ldots + a_s\, x^s \ ,$$

à $a_j\, x^j$ associons, dans le plan des $(\rho\ ,\ y)$, la droite D_j : $y = j\rho + \log|a_j|$. Alors, pour $\log|x| = \rho$, $\log|a_j\, x^j| = y$, le point $(y\ ,\ \rho)$ décrivant D_j lorsque ρ varie,

$$|P(x)| \leqslant \max_j |a_j\, x^j| \quad ,$$

et on a égalité si ce maximum n'est atteint que pour un seul indice. L'intersection des demi-plans $y \geqslant j\rho + \log|a_j|$, limités par les D_j pour $0 \leqslant j \leqslant s$, est limitée par une courbe polygonale, convexe, $y = \mu_p(\rho)$, continue, croissante, convexe et linéaire par morceaux.



Soient $\rho_1 , \dots , \rho_n$ les abscisses des sommets de cette courbe. Nous les appellerons valeurs exceptionnelles de ρ .

Alors

$$\text{pour } \log|x| = \rho , \quad \log|P(x)| = \mu_p(\rho) \quad \text{si} \quad \rho \neq \rho_i \quad ,$$

et

$$\text{pour } \log|x| = \rho_i , \quad \log|P(x)| \leqslant \mu_p(\rho) \quad .$$

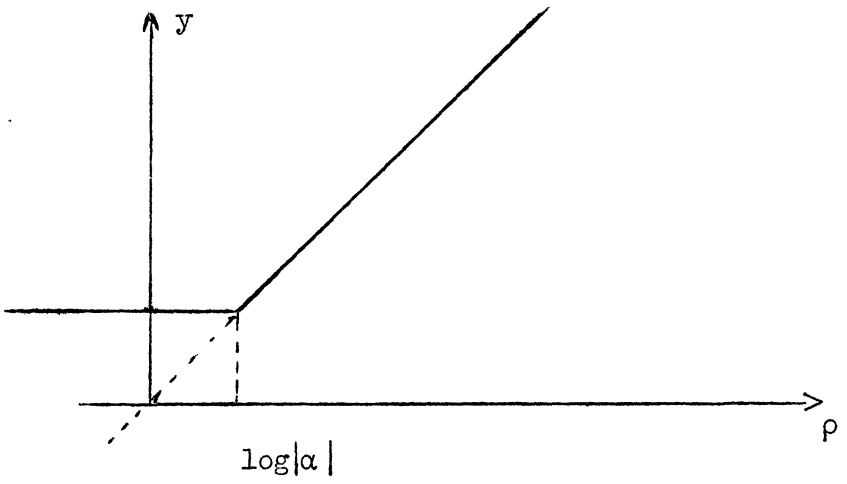
Si $\alpha \in \Omega$ est un zéro de P , on a donc nécessairement $\log|\alpha| = \rho_j$ pour un indice j . On peut obtenir le même résultat différemment : supposons que Ω soit un corps de décomposition de P , alors

$$P(x) = \lambda \prod_{j=1}^{s} (x - \alpha_j)$$

et

$$\log|P(x)| = \log|\lambda| + \sum_{j=1}^{s} \log|x - \alpha_j| \quad .$$

Soit $\mu_\alpha(\rho)$ la fonction $\mu_p(\rho)$ pour $P = x - \alpha$. Alors



$$\mu_\alpha(\rho) = \log|\alpha| \quad \text{si} \quad \rho < \log|\alpha|$$
$$= \rho \quad \text{si} \quad \rho > \log|\alpha| \quad .$$

Et si $\rho \neq \log|\alpha|$, on a

$$\log|x - \alpha| = \mu_\alpha(\rho) \quad \text{pour} \quad \log|x| = \rho \quad .$$

Donc, pour $\rho \neq \log|\alpha_i|$ et $\log|x| = \rho$, on a

$$\mu_P(\rho) = \log|P(x)| = \log|\lambda| + \sum_j \mu_{\alpha_j}(\rho) \quad .$$

Donc les sommets de $\mu_P(\rho)$ ont pour abscisses les valeurs ρ_s , ... , ρ_h de $\log|\alpha_j|$, et le nombre de zéros de P , tels que $\log|x| = \rho_i$, est la différence des pentes des côtés ayant une extrémité commune d'abscisse ρ_i .

Soit maintenant $f(x) = \frac{Q(x)}{P(x)}$ une <u>fraction rationnelle</u> ; P et Q étant de des polynômes, soient

ρ_j , $j = 1$, ... , h les valeurs exceptionnelles pour $P(x)$

ρ'_i , $i = 1$, ... , k les valeurs exceptionnelles pour $Q(x)$.

Posons

$$\mu_f(\rho) = \mu_Q(\rho) - \mu_P(\rho) \quad .$$

$\mu_f(\rho)$ est une fonction continue de ρ , linéaire par intervalles, convexe pour $\rho_j \leqslant \rho \leqslant \rho_{j+1}$. Alors, soit C le cercle $\log|x| = \rho$,

- si $\rho \neq \rho_j$ et $\rho \neq \rho'_i$, $\forall$ i , j , $\log|f(x)| = \mu_f(\rho)$, $\forall$ $x \in C$,
- si $\rho = \rho_j$, $\rho \neq \rho'_i$, $\forall$ i , $\inf\limits_{x\in C} (\log|f(x)|) = \mu_f(\rho)$,
- si $\rho = \rho'_i$, $\rho \neq \rho_j$, $\forall$ j , $\sup\limits_{x\in C} (\log|f(x)|) = \mu_f(\rho)$,
- s'il existe i et j tels que $\rho'_i = \rho_j$, on ne peut rien dire sur $|f(x)|$.

Pour l'étude des fractions rationnelles, il sera donc intéressant de considérer des domaines ne comprenant pas les cercles $\log|x| = \rho'_i$ ou ρ_j .

Définitions.

Ensemble ultra-ouvert en a . - Soit D un ensemble de $\hat{\Omega}_p$, comprenant au moins deux points, si $a \in D$, D est dit ultra-ouvert en a si, $\forall$ $b \in D$, $b \neq a$, les points $y \notin D$ situés dans le disque $|y - a| \leqslant |b - a|$ sont sur un nombre fini de cercles $|y - a| = r$, où $r \leqslant |b - a|$.

Ensembles quasi-connexes. - D est dit quasi-connexe s'il est non vide et ultra-ouvert en chacun de ses points.

Un ensemble quasi-connexe est ouvert, car si $a \in D$ et si r_1 est le plus petit des cercles de centre a rencontrant le complémentaire de D , le disque ouvert $|x - a| < r_1$ est contenu dans D .

Si D et D' sont quasi-connexes, et si $\emptyset \neq D \cap D'$, $D \cap D'$ est quasi-connexe.

En effet si $a \in D$ et D' , il existe $r \neq 0$ tel que $|x - a| < r \Rightarrow x \in D \cap D'$, donc $D \cap D'$ contient au moins deux points, et il est clair qu'il est quasi-connexe.

PROPOSITION 18. - Soit E un ensemble tel que, quels que soient $a \in E$ et $b \in E$, il existe un nombre fini d'ensembles quasi-connexes D_1 , ... , D_n tels que $D_j \subset E$, $D_j \cap D_{j+1}$ ne soit pas vide, $a \in D_1$, $b \in D_n$. Alors E est quasi-connexe.

Posons $a_0 = a$, $a_n = b$, et choisissons $a_j \in D_j \cap D_{j+1}$ pour $j \neq n$. Si

$\max|a_j - a| = |b - a|$ et si $|a_j - a| < |b - a|$ pour $j \neq n$,

$$|a_{n-1} - b| = \max(|b - a| , |a_{n-1} - a|) = |b - a| \quad ,$$

donc, en échangeant éventuellement les rôles de a et b , il existe a_k , $k \neq n$, tel que $|a_k - a| = \max|a_j - a|$, et le disque $|y - a| \leqslant |b - a|$ est contenu dans $|y - a| \leqslant |y - a_k|$. On procède alors par induction sur n , ce qui montre que E est quasi-connexe.

Point à l'infini. - Soit Ω' obtenu par adjonction à Ω d'un "point à l'infini" ω , ayant les propriétés usuelles :

$$x + \omega = \omega \ , \quad x.\omega = \omega \ \text{ si } \ x \neq 0 \ , \quad x.\omega = 1 \ \text{ si } \ x = 0 \ , \quad |\omega| = +\infty \quad ,$$

un voisinage fermé de ω étant un cercle $|x| \geqslant A$ dit de centre ω .

THÉORÈME 20. - Soit $x' = \ell(x) = \dfrac{\alpha x + \beta}{\gamma x + \delta}$ une transformation homographique non dégénérée de Ω' , et soit $D' = \ell(D)$ le transformé de D par ℓ . Si D est quasi-connexe, D' l'est aussi.

Si $\ell(x) = \alpha x + \beta$, c'est évident. Il suffit donc de la démontrer pour $\ell(x) = \dfrac{1}{x}$.

Soit x' tel que $|x' - a'| = r'$, $a' \neq 0$, $\dfrac{1}{a'} = a$, alors

$$|x - a| = \frac{|x' - a'|}{|x' a'|} \ , \ \text{si } \ r' < |a'| \ , \quad |x - a| = r'|a|^2 \quad .$$

Soient a' , $b' \in D'$, $a = \dfrac{1}{a'}$ et $\dfrac{1}{b'} = b \in D$, et soit $y' \notin D$, avec $|y' - a'| = r' \leqslant |b' - a'|$. Nous allons montrer que Ω' ne peut prendre qu'un nombre fini de valeurs, excluons $|b' - a'|$, et soit $y = \dfrac{1}{y'} \notin D$, $|y' - a'| = r' < |b' - a'|$. Plusieurs cas se présentent :

a. $a \neq 0$, $a \neq \omega$, $b \neq 0$, $b \neq \omega$.

1° Si $|a - b| \leqslant |b|$,

$$|b' - a'| = \frac{|b - a|}{|ab|} \leqslant \frac{1}{|a|} = |a'| \quad ,$$

alors $r' < |a'|$ et $r = |y - a| = r'|a|^2$, donc r' n'a qu'un nombre fini de valeurs.

2° Si $|a - b| > |b|$,

$$|a - b| = |a| \quad .$$

si $r' < |a'|$, $r = |y - a| = r'|a|^2$ et r' n'a qu'un nombre fini de valeurs,

si $r' < |a'|$, $|y' - a'| > |a'| \implies |y'| = r'$, $\implies |y| = \frac{1}{r}$,

Alors

$$|a'| < |y' - a'| < |b' - a'| \implies |a' - b'| = |b'| > |y' - a'| = r'$$

et

$$|y| = \frac{1}{r'} > |b| \quad ,$$

alors

$$|y - b| = \frac{1}{r'} < \frac{1}{|a'|} = |a| = |a - b| \quad ,$$

et D étant ultra-ouvert en b , r' n'a qu'un nombre fini de valeurs. (Remarquons que ceci montre que $x' = \frac{1}{x}$ ne conserve pas la notion d'ultra-ouvert en a .)

b. $b = 0$; $a \neq 0$, $a \neq \omega$.

Alors $|b' - a'| = + \infty$,

si $r' > |a'|$, $|y'| < r'$ et $|y| = \frac{1}{r'} < |a|$,

si $r' < |a'|$, $|y - a| = \frac{r'}{|y'| \cdot |a'|} = r'|a|^2 < |a|$.

Dans ces deux cas, D ultra-ouvert en $b = 0$ entraîne que r' n'a qu'un nombre fini de valeurs.

c. $b = \omega$, $a \neq 0$, $a \neq \omega$.

On a alors $r' < |a'|$ et $|y - a| = r'|a|^2 < |a|$ et r' n'a qu'un nombre fini de valeurs.

Elément analytique.

Définition. - Soit D quasi-connexe, une fonction $f(x)$ définie sur D , est appelée élément analytique si $f(x)$ est limite uniforme sur D d'une suite $f_n(x)$

de fractions rationnelles n'ayant pas de pôles dans D (nous supposons Ω algébriquement clos).

Soit $\varepsilon > 0$, pour m , $n \geqslant N(\varepsilon)$,

$$|f_n(x).f_m(x)| \leqslant \varepsilon \quad \text{pour} \quad x \in D \quad ,$$

soit m fixé, $m \geqslant N(\varepsilon)$ et D_ε la partie de D définie par

$$|f_m(x)| > \varepsilon \iff x \in D_\varepsilon \quad ,$$

alors pour $n \geqslant N(\varepsilon)$ et $x \in D_\varepsilon$

$$|f_n(x)| > \varepsilon$$

et si $x \in D$, $x \notin D_\varepsilon$ et $n \geqslant N(\varepsilon)$,

$$|f_n(x)| \leqslant \max(|f_m(x)| \ , \ \varepsilon) \leqslant \varepsilon \quad ,$$

donc D_ε ne dépend que de $N(\varepsilon)$, soit de ε . Alors D_ε est aussi la partie de D définie par $x \in D_\varepsilon \iff |f(x)| > \varepsilon$, et pour $x \in D_\varepsilon$ et $n \geqslant N(\varepsilon)$ on a

$$|f(x)| = |f_n(x)| \quad .$$

Supposons (en effectuant au besoin une translation) que $0 \in D$, et soient $\rho_1 < \rho_2 < \ldots < \rho_j < \ldots$ les rayons exceptionnels de D relativement à 0 , alors pour $\rho \neq \rho_j$, posons

$$\mu_f(\rho) = \mu_{f_n}(\rho) \quad \text{pour} \quad n \geqslant N(\varepsilon)$$

s'il existe $x \in D_\varepsilon$,

$$\log|x| = \rho \quad .$$

Pour $\varepsilon' < \varepsilon$,

$$D_{\varepsilon'} \supset D_\varepsilon \quad \text{et} \quad D = \bigcup_{\varepsilon > 0} D_\varepsilon \quad .$$

Soit $\rho_D = \sup \log|x|$, $x \in D$, alors quel que soit $\rho < \rho_D$, $\rho \neq \rho_j$,

$\exists\ x \in D$ avec $\log|x| = \rho$, et $\mu_f(\rho)$ est défini.

Si pour $\rho_j < \rho < \rho_{j+1}$, $\mu_f(\rho) > -\infty$, alors $\mu_f(\rho)$ est convexe dans cet intervalle, car si $\log_\varepsilon < \inf \mu_f(\rho)$, $\mu_f(\rho) = \mu_{f_n}(\rho)$ pour $n \geq N(\varepsilon)$ et f_n est une fraction rationnelle n'ayant pas de pôle dans cette couronne.

Donc, pour $\rho_j < \rho < \rho_{j+1}$, ou bien $\mu_f(\rho) = -\infty$, ou bien $\mu_f(\rho)$ est convexe, continue et bornée et on peut la prolonger à ρ_j et ρ_{j+1} par continuité. Nous pouvons maintenant démontrer le théorème fondamental.

THÉORÈME 21. - Soit $f(x)$ un élément analytique défini dans un domaine quasi-connexe D. S'il existe un disque ouvert Δ dans D, tel que $f(x) = 0$ ait une infinité de racines dans Δ, alors $f(x) = 0$ quel que soit $x \in D$.

1° $f(x) = 0$, $\forall\ x \in \Delta$, en effet, supposons (par translation) Δ centré à l'origine ; les $f_n(x)$ n'ont pas de pôle dans Δ, donc d'après la proposition 16 (fin du IV) elles admettent un développement de Taylor à l'origine, convergent dans Δ, elles convergent uniformément dans D, donc dans Δ, vers f, donc d'après le théorème 19 (de Weierstrass) leur limite $f(x)$ a aussi un développement en série de Taylor convergeant vers f dans Δ. Alors, d'après le corollaire 2 du théorème 16 (IV, B, 2) $f(x)$ est identiquement nulle dans Δ.

2° $f(x) = 0$, $\forall\ x \in \Delta \Longrightarrow f(x) = 0$, $\forall\ x \in D$, en effet soit

$$R = \{\rho \text{ tels qu'il existe } x \in D, \text{ avec } \log|x| = \rho\},$$

R est dense sur un segment de la droite réelle (ou sur la demi-droite $0, +\infty$), $x \to |x|$ est une fonction continue de x, $f(x)$ est continue en x pour $x \in$ [illegible], donc $x \to |f(x)|$ est continue en x et $\mu_f(\rho) = \sup_{|x|=\rho} \mu_f(\rho)$ est continue en ρ sur R.

S'il existe un segment ρ_i, ρ_{i+1} tel que, pour $\rho \in R \cap]\rho_i, \rho_{i+1}[$ on ait $\mu_f(\rho) = -\infty$, alors $\mu_f(\rho) = -\infty$, $\forall\ \rho \in R$.

C. Q. F. D.

COROLLAIRE. - Soit $\varphi(x)$ une fonction définie sur un disque ouvert borné M de $\hat{\Omega}_p$, et soit D un domaine quasi-connexe, $D \supset M$, il existe au plus un élément analytique sur D tel que $f(x) = \varphi(x)$ pour $x \in M$.

Remarque. - Les éléments analytiques sur un ensemble quasi-connexe D forment un anneau, et si D* est l'ensemble D privé des points tels que $f(x) = 0$, f étant un élément analytique sur D, $\frac{1}{f}$ est un élément analytique sur D*.

BIBLIOGRAPHIE

des fonctions p-adiques

A. Généralités.

ARTIN (Emil). - Algebraic numbers and algebraic functions. - Princeton, Princeton University, 1950/51 (multigraphié).

CHEVALLEY (Claude). - Sur la théorie du corps de classe dans les corps finis et les corps locaux, J. Fac. Sc. Univ. Tokyo, Section 1, t. 2, 1929-1934, p. 365-474.

DWORK (Bernard). - On the zeta function of a hypersurface. - Paris, Presses universitaires de France, 1962 (Institut des hautes Etudes scientifiques, Publications mathématiques, 12) ; p. 5-68.

HASSE (H.). - Zahlentheorie. - Berlin, Akademie-Verlag, 1949.

HENSEL (K.). - Zahlentheorie. - Berlin, G. J. Göschen, 1913.

MAHLER (K.). - Lectures on diophantine approximations. - Notre-Dame (Ind.), University Press, 1961.

B. Fonctions analytiques.

STRASSMANN (Reinhold). - Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen, J. für reine und angew. Math., t. 159, 1928, p. 13-28 et 65-66.

[Il semble être fait mention ici, pour la première fois, du polygône de Newton et du prolongement analytique de $\exp x$ et de $\log x$.]

SCHÖBE (W.). - Beiträge zur Funktionentheorie in nichtarchimedisch bewerteten Körpern (Dissertation. Universität Münster. 1930).

ŠNIREL'MAN (L.). - Sur les fonctions dans les corps normés et algébriquement fermés [en russe, avec un résumé en français], Bull. Acad. Sc. URSS, Cl. Sc. math. natur., Série mathématique, 1938, p. 487-498.

[Théorème de Šnirel'man ; généralisation de la formule intégrale de Cauchy.]

LOONSTRA (Frans). - Analytische Untersuchungen über bewertete Körper (Thèse. Univ. Amsterdam. 1941).

DIEUDONNÉ (Jean). - Sur les fonctions continues p-adiques, Bull. Sc. math., Série 9, t. 68, 1944, 1re partie, p. 79-95.

[Théorème d'approximation de Weierstrass dans Q_p, fonctions non constantes dont la dérivée est identiquement nulle.]

KRASNER (Marc). - Essai d'une théorie des fonctions analytiques dans les corps valués complets, C. R. Acad. Sc. Paris, t. 222, 1946, p. 37-40, 165-167, 363-365 et 581-583.

[Théorie générale des fonctions analytiques, premières idées sur le prolongement analytique.]

CHABAUTY (Claude). - Sur la théorie des fonctions sur un corps valué, C. R. Acad. Sc. Paris, t. 231, 1950, p. 396-397 et 432-434.

[Théorème d'approximation de Weierstrass dans les corps p-adiques généraux. Perfectionnement de la théorie du prolongement analytique.]

KRASNER (Marc). - Prolongement analytique dans les corps valués complets, C. R. Acad. Sc. Paris, t. 239, 1954, p. 468-470 et 745-747.

[Dernières formulations du prolongement analytique, ensembles quasi-connexes.]

LEOPOLDT (H. W.). - Zur Approximation des p-adischen Logarithmus, Abh. math. Sem. Univ. Hamburg, t. 25, 1961/62, p. 77-81.

[Définition du logarithme p-adique par $(y^{p^n(p-1)})/(p^n(p-1)$.]

C. Fonctions spéciales.

WEIL (André). - Sur les fonctions elliptiques p-adiques, C. R. Acad. Sc. Paris, t. 203, 1936, p. 22-24.

[Fonctions elliptiques p-adiques.]

CHABAUTY (Claude). - Sur la répartition modulo 1 de certaines suites p-adiques, C. R. Acad. Sc. Paris, t. 231, 1950, p. 465-466.

[Généralisation dans Q_p des nombres P. V.]

DWORK (Bernard). - On the rationality of the zeta function of an algebraic variety, Amer. J. of Math., t. 82, 1960, p. 631-648.

[Théorème de Borel et application à la fonction ζ de Riemann.]

MONNA (A. F.). - Sur les espaces normés non archimédiens, I-IV, Proc. Ned. Akad. Wet., Série A, t. 59, 1956, p. 475-483 et 483-489 ; t. 60, 1957, p. 459-467 et 468-476.

MONNA (A. F.). - Sur les espaces linéaires normés, I-VI, Proc. Ned. Akad. Wet., t. 49, 1946, p. 1045-1055, 1056-1062, 1134-1141 et 1142-1152 ; t. 51, 1948, p. 197-210 ; t. 52, 1949, p. 151-160.

MONNA (A. F.). - Sur une classe d'espaces linéaires normés, Proc. Ned. Akad. Wet., Série A, t. 55, 1952, p. 513-525.

[Espaces de Banach p-adiques, opérateurs linéaires.]

DWORK (Bernard). - On the zeta function of a hypersurface. - Paris, Presses universitaires de France, 1962 (Institut des hautes Etudes scientifiques, Publications mathématiques, 12) ; p. 5-68.

SERRE (Jean-Pierre). - Endomorphismes complètement continus des espaces de Banach p-adiques. - Paris, Presses universitaires de France, 1962 (Institut des hautes Etudes scientifiques, Publications mathématiques, 12) ; p. 69-85.

[Théorie de Fredholm.]

D. Application aux équations diophantiennes.

SKOLEM (T.). - Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen, Math. Annalen, t. 111, 1935, p. 399-424.

[Exposé de la méthode de Skolem utilisant le théorème de Šnirel'man.]

CHABAUTY (Claude). - Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques finis, Annali di Mat. pura ed appl., 4e Série, t. 17, 1938, p. 127-168.

[Application de la méthode de Skolem.]

CHABAUTY (Claude). - Démonstration nouvelle d'un théorème de Thue et Mahler sur les formes binaires, Bull. Sc. math., Série 2, t. 65, 1941, 1re partie, p. 112-130.

[Théorème de Thue par la méthode de Skolem.]

MAHLER (Kurt). - Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, Proc. Ned. Akad. Wet., t. 38, 1935, p. 50-60.

[Récurrences linéaires avec une infinité de termes nuls par la méthode de Skolem.]

LUTZ (Elisabeth). - Les solutions de l'équation $y^2 = x^2 - Ax - B$ dans les corps p-adiques, C. R. Acad. Sc. Paris, t. 203, 1936, p. 20-22.

[Méthode p-adique pour les points rationnels d'une courbe cubique.]

MATTUCK (Arthur). - Abelian varieties over P-adic ground fields, Annals of Math., Series 2, t. 62, 1955, p. 92-119.

[Théorie de Mlle Lutz.]