Séminaire Dubreil.
Algèbre et théorie
des nombres

P. Samuel

## Le lemme de Hensel

*Séminaire Dubreil. Algèbre et théorie des nombres*, tome 7 (1953-1954), exp. n° 9, p. 1-5
<http://www.numdam.org/item?id=SD_1953-1954__7__A9_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire d'ALGÈBRE
Année 1953/1954
-:-:-:-



# LE LEMME DE HENSEL

Conférence faite par P. SAMUEL, le 8 mars 1954, rédigée par J. GUÉRINDON

-:-:-:-

## INTRODUCTION.

La méthode de Newton pour l'approximation des racines d'un polynôme réel repose sur l'idée suivante : si $a$ est une valeur "approchée" d'une racine $\alpha$ de $F(x) = 0$ , on cherche une meilleure valeur en déterminant $h$ pour que $F(a + h) = F(a) + h\,F'(a) + \frac{h^2}{2} F''(a) + \ldots$ soit le plus près possible de $0$ . On est amené à annuler $F(a) = h\,F'(a)$ en prenant $h = -\frac{F(a)}{F'(a)}$ et le processus converge si $h$ est assez petit, c'est-à-dire si $|F'(x)|$ n'est pas trop petit et $|F(x)|$ pas trop grand dans l'intervalle où on a pris $a$ .

I.- On va appliquer ce procédé en l'étendant au cas où $F(X) \in A[X]$ , $A$ étant l'anneau $Z_p$ des entiers p-adiques (p premier fixé). On sait que $A$ peut se définir d'au moins trois façons différentes :

1°) $A$ est l'ensemble des sommes infinies $a_0 + a_1 p + a_2 p^2 + \ldots$ où $a_i$ est un entier tel que $0 \leqslant a_i \leqslant p-1$ (on a $p \geqslant 2$ ).

2°) $A$ est le complété de l'anneau $Z$ des entiers relativement à la valuation p-adique .

3°) $A$ est le quotient $Z[[X]]/(X - p)$ de l'anneau des séries formelles à coefficients en $Z$ par l'idéal des séries multiples de $X - p$ . Cet anneau $Z_p$ est local d'idéal maximal $pZ_p$ et de corps résiduel $Z_p/pZ_p$ isomorphe au corps $F_p$ à p éléments. La valuation p-adique se prolonge de $Z$ à $Z_p$ , elle est en évidence sur le développement $u = a_\rho p^\rho + a_{\rho+1} p^{\rho+1} + \ldots$ $(a_\rho \neq 0)$ , on a : $v_p(u) = \rho$ . $Z_p$ est alors complet pour la topologie définie par la distance $d(u,v) = \exp\left[-v_p(u - v)\right]$ qui en fait un espace ultramétrique (on a $d(x,z) < \max d(x,y), d(z,y)$ ) ; celui-ci est séparé au sens de Hausdorf.

Soit l'équation $F(X) = 0$ sur $A = Z_p$ et partons d'un $a$ tel que $F(a) \equiv 0\ (p)$ et $F'(a) \not\equiv 0\ (p)$ . Déterminons de proche en proche des $a_n$ tels que $F(a_n) \equiv 0\ (p^n)$ et $F'(a_n) \not\equiv 0\ (p)$ en posant $a_{n+1} = a_n + p^n h$ , $h$ dépendant de $n$ et $h \in A$ . Alors on a $F(a_{n+1}) = F(a_n) + hp^n F'(a_n) + up^{2n}$, avec $u \in A$ , et comme $F(a_n) = b_n p^n$ $(b_n \in A)$ , il suffira de trouver $h$ pour que $b_n + hF'(a_n) \equiv 0\ (p)$ ce qui est possible car $A/A_p$ est un corps et $F'(a_n) \not\equiv 0\ (p)$ . La suite

$(a_{n+1} - a_n)$ est une suite nulle au sens p-adique, donc $(a_n)$ est une suite de Cauchy. On sait que les suites de Cauchy d'un espace ultramétrique sont celles pour lesquelles la différence de deux termes consécutifs tend vers 0 (utiliser l'inégalité ultramétrique).

Donc $a_n$ a pour limite $a \in A$, A étant complet et $F(a_n)$ tend vers $F(a)$ qui ne peut être que nul car $F(a_n) \equiv 0\ (p^n)$. La condition de possibilité est $F'(a_n) \not\equiv 0\ (p)$ pour n grand, ce qui s'énonce en passant aux quotients par $A_p$, $\overline{F}(X)$ désignant la classe de $F(X)$ : $\overline{F}(X)$ a une racine simple $\overline{a}$ dans $A/A_p$, $\overline{a}$ désignant la classe de a.

Les raisonnements précédents sont valables dans tout anneau valué complet A, dont l'idéal de valuation est M, et plus généralement dans tout anneau local complet A d'idéal maximal M.

Exemple 1 : Les polynômes $X^2 + 1$, $X^2 - 2$, $X^2 - 3$ ayant en $F_5$, $F_7$ et $F_{13}$ respectivement les racines simples $\overline{2}$, $\overline{3}$ et $\overline{4}$ (classes de 2, 3 et 4 modulo $5\,Z_5$, $7\,Z_7$ et $13\,Z_{13}$) on a donc : $\sqrt{-1} \in Z_5$, $\sqrt{2} \in Z_7$, $\sqrt{13} \in Z_{13}$. La première par exemple s'écrit au sens de la topologie 5-adique : $\sqrt{-1} = 2 + 5 + 2.5^2 + \ldots$ .

Exemple 2 : K étant un corps, l'anneau A des séries $K[[X]]$ étant valué au moyen du plus bas degré on est assuré lorsque 1 a 2 racines carrées distinctes en K (c'est-à-dire si la caractéristique de K est $\neq 2$ que la série formelle $1 + X\,s(X)$, $s(X) \in K[[X]]$, a 2 racines carrées dans A.

Exemple 3 : Soit $F(X,T)$ un polynôme en X dont les coefficients appartiennent à $A = K[[T]]$ et tel que $F(X,0) = 0$ ait une racine simple a dans K. Il existe alors $s(T) = a + a_1 T + \ldots$ unique telle que $F(s(T),T) = 0$ : c'est l'analogue du théorème des fonctions implicites.

II.- La généralisation des résultats précédents utilisera les définitions suivantes sur les modules filtrés et leurs topologies.

Un anneau A sera dit filtré par une suite descendante de sous-groupes (additifs) $A_n$, $n \in Z$ si l'on a : $A_p A_q \subset A_{p+q}$ et $\bigcup_{-\infty}^{+\infty} A_n = A$. Par exemple on prendra $A_1 = M$, idéal de A, $A_{-q} = A$ pour $q \geqslant 0$ et $A_n = M^n$ pour $n \geqslant 0$.

Un A-module E sur un anneau filtré A sera dit filtré par une chaîne descendante $E_n$ de sous-groupes additifs de E si l'on a : $A_p E_q \subset E_{p+q}$ et $\bigcup_{n \in Z} E_n = E$. Une filtration, dite canonique, sera obtenue sur E en choisissant $E_n = A_n E$, les $A_n$ filtrant A. En particulier on aura des filtrations de E du type $E_n = M^n E$, avec $E_0 = E$. Lorsqu'en plus on suppose que l'on a

$\bigcap_1^\infty M^n = (0)$ , les $(M^n)$ constituent un système fondamental de voisinages de 0 pour une topologie séparée de A (au sens de Hausdorf) et les $E_n = M^n E$ de même pour E , si $\bigcap_1^\infty E_n = (0)$ . Si $\omega(\alpha)$ est le maximum des n tels que $\alpha \in E_n$ , E devient un espace ultramétrique relativement à la distance $d(x,y) = e^{-\omega(x-y)}$ par exemple. Les anneaux que nous considérons sont commutatifs et munis d'un élément unité. Un anneau local (Stellenringen de Krull) sera tout anneau du type précédent où les éléments non inversibles forment un idéal M , maximum dans A . On sait avec Krull que si A est nœthérien, on a $\bigcap_1^\infty M^n = (0)$ : ce sont les anneaux M-adiques.

III.- Le Lemme "bilinéaire".

"Soit A un anneau complet filtré par les puissances d'un idéal M ; E , E' et F des A-modules de type fini, F étant séparé pour la filtration canonique. Supposons fixée une application bilinéaire $\varphi$ du produit $E \times E'$ en F et désignons par $\bar{\varphi}$ l'application bilinéaire, canoniquement déduite de $\varphi$ , qui applique $(E/ME) \times (E'/ME')$ en $F/MF$ . Alors à tout système d'éléments $y \in F$ , $\alpha \in E/ME$ , $\alpha' \in E'/ME'$ satisfaisant aux deux conditions :

1°) la classe $\bar{y}$ de y mod. MF est $\bar{\varphi}(\alpha,\alpha')$

2°) $F/MF = \bar{\varphi}(\alpha, E'/ME') + \bar{\varphi}(E/ME, \alpha')$

on peut associer des éléments $a \in E$ et $a' \in E'$ tels que $\alpha = \bar{a}$ , $\alpha' = \bar{a'}$ et $y = \varphi(a,a')$ ".

On raisonne par induction sur n en prouvant que pour tout n il existe $a_n \in E$ et $a'_n \in E'$ tels que $\alpha = \overline{a_n}$ et $\alpha' = \overline{a'_n}$ et $y \equiv \varphi(a_n,a'_n) \bmod (M^n F)$ C'est vrai pour n = 1 d'après 1° . Supposons-le vrai pour $n \geqslant 1$ et démontrons-le pour n+1 : comme $y - \varphi(a_n,a'_n) \in M^n F$ on a $y - \varphi(a_n,a'_n) = \sum m_j z_j$ $(m_j \in M^n, z_j \in F)$ . Chaque $z_j$ satisfait d'après 2° à : $z_j \equiv \varphi(a_n,w'_j) + \varphi(w_j,a'_n)$ (mod MF) avec $w_j \in E$ , $w'_j \in E'$ et donc, $\varphi$ étant bilinéaire :

$$y - \varphi(a_n + \sum m_j w_j \, , \, a'_n + \sum m_j w'_j) = y - \varphi(a_n,a'_n) - \sum m_j z_j +$$
$$+ \sum_j m_j (z_j - \varphi(a_n,w'_j) - \varphi(w_j,a'_n)) - \sum_{i,j} m_i m_j \varphi(w_i,w'_j) \in M^{n+1}F \, ,$$

car $m_j \in M^n$ et $z_j - \varphi(a_n,w'_j) - \varphi(w_j,a'_n) \in MF$ . On posera $a_{n+1} = a_n + \sum m_j w_j$ et $a'_{n+1} = a'_n + \sum m_j w'_j$ . On aura alors $a_{n+1} \equiv a_n (M^n E)$ et $a'_{n+1} \equiv a'_n (M^n E')$ d'où $\overline{a_{n+1}} = \alpha$ , $\overline{a'_{n+1}} = \alpha'$ et $y - \varphi(a_{n+1},a'_{n+1}) \in M^{n+1}F$ .

Les suites $(a_n)$ et $(a'_n)$ sont des suites de Cauchy en E et E' qui sont complets puisqu'ils sont des modules de type fini sur A qui est complet. Désignons les limites par a et a' . On a à la limite $\bar{a} = \alpha$ , $\overline{a'} = \alpha'$ .

Alors $y - \varphi(a,a') = y - \varphi(a_n,a'_n) + \varphi(a_n, a'_n) - \varphi(a,a') \in M^nF$ , car $y - \varphi(a_n,a'_n) \in M^nF$ et la 2e différence aussi puisque $\varphi$ est bilinéaire et $a_n - a \in M^nE$ et $a'_n - a' \in M^nE'$ . Ceci étant vrai quel que soit $n$ et $F$ étant séparé, on a $y - \varphi(a,a') = 0$ . C.Q.F.D.

Appelons unitaire un polynôme dont le coefficient du terme de plus haut degré est 1 .

Lemme de Hensel : Soit $A$ un anneau local complet, d'idéal maximal $M$ et $f(X) \in A[X]$ un polynôme unitaire de degré $n$ . Désignons pour tout $h(X) \in A[X]$ par $\overline{h}(X)$ son résidu modulo $M$ . S'il existe deux polynômes unitaires premiers entre eux $\alpha(X)$ et $\alpha'(X)$ de degrés $r$ et $n-r$ dans $(A/M)[X]$ tels que $\overline{f}(X) = \alpha\alpha'$ , il existe deux polynômes unitaires $g(X)$ et $g'(X)$ de degrés $r$ et $n-r$ en $A[X]$ tels que $f(X) = g(X)g'(X)$ et $\overline{g}(X) = \alpha(X), \overline{g'}(X) = \alpha'(X)$ .

On appliquera le lemme en prenant pour $F$ , $E$ et $E'$ les $A$-modules constitués par les polynômes sur $A$ de degrés respectivement inférieurs ou égaux à $n$ , $r$ et $n-r$ et en prenant pour $\varphi$ la multiplication, ce qui vérifie immédiatement la condition 1°, les polynômes étant unitaires. Pour la seconde on utilise le fait que $\alpha$ et $\alpha'$ étant premiers entre eux chaque polynôme de degré $\leq n$ sur $A/M$ s'écrit $\alpha\beta' + \alpha'\beta$ . Par division euclidienne par $\alpha'$ de $\beta'$ on peut réaliser cette représentation avec : $d^0(\beta') < n - r$ ; alors $\beta$ est bien de degré $\leq r$ .

Il existe donc en $A[X]$ des polynômes $a(X)$ et $a'(X)$ de degré $\leq r$ et $n-r$ respectivement tels que $aa' = f$ , $\overline{a} = \alpha$ , $\overline{a'} = \alpha'$ . Comme $\alpha$ et $\alpha'$ sont des polynômes unitaires de degrés $r$ et $n-r$ , $a$ et $a'$ sont de degré $r$ et $n-r$ exactement, et leurs coefficients dominants sont dans $1 + M$ , et donc inversibles. Soit $1 + m'$ l'inverse du plus haut coefficient $1 + m$ de $a(X)$ $(m,m' \in M)$ . Alors le polynôme $g(x) = (1 + m')a(X)$ est unitaire. En posant $g'(x) = (1 + m)a'(x)$ , on a bien $gg' = f$ , $\overline{g} = \alpha$ , $\overline{g'} = \alpha'$ et $g'$ est aussi unitaire puisque $f$ et $g$ le sont . Le lemme de Hensel est établi.

Corollaire : Si $A$ est un anneau local complet d'idéal maximal $M$ , si $f(X) \in A[X]$ est normé et si son résidu $\overline{f}(X)$ en $(A/M)[X]$ a une racine simple $\xi$ en $A/M$ , alors $f(X)$ a une racine $x \in A$ telle que $\overline{x} = \xi$ .

Il suffit de décomposer $\overline{f}(X)$ en $(X - \xi)\gamma(X)$ , de remarquer que $X - \xi$ et $\gamma(X)$ sont premiers entre eux et d'appliquer le théorème précédent. On retrouve les résultats de I.

IV.- Le théorème de décomposition. "Soit $A$ un anneau complet séparé filtré par les puissances d'un idéal $M$ et tel que $A/M$ soit la somme directe de deux idéaux

$V/M$ et $V'/M$ . Alors $A$ est la somme directe de $N = \bigcap_1^\infty V^n$ et $N' = \bigcap_1^\infty V'^n$ et on a $N \cap M^n = M^n N$ , $N' \cap M^n = M^n N'$ . L'anneau $N$ (resp. $N'$ ) filtré par les $M^n N$ (resp. $M^n N'$ ) est séparé et complet. On a les isomorphismes $N/MN \simeq A/V' \simeq V/M$ et $N'/MN' \simeq A/V \simeq V'/M$ ."

Par hypothèse on a $A = V + V'$ avec $V \cap V' = M$ . Alors l'unité 1 de $A/M$ s'écrit de manière unique $1 = \varepsilon + \varepsilon'$ avec $\varepsilon\varepsilon' = 0$ ( $\varepsilon \in V/M$ , $\varepsilon' \in V'/M$ ). Le lemme bilinéaire est alors applicable avec $E = E' = F = A$ , $y = 0$ et en prenant pour $\varphi$ la multiplication. Il existe alors $a$ , $a' \in A$ tels que $aa' = 0$ et dont les classes modulo $M$ sont $\varepsilon$ et $\varepsilon'$ . On a donc $a + a' \equiv 1(M)$ , donc $a + a'$ est inversible en $A$ qui est complet (si $a + a' = 1 - \mu$ , cet inverse est $1 + \mu + \mu^2 + \ldots$ ) . Soit $1 + m$ ($m \in M$) l'inverse de $a + a'$ , alors $e = a(1 + m)$ et $e' = a'(1 + m)$ satisfont à $e + e' = 1$ et $ee' = 0$ et par conséquent à $e^n = e$ , $e'^n = e'$ quel que soit $n$ : ce sont des idempotents orthogonaux de $A$ . Leurs résidus modulo $M$ sont encore $\varepsilon$ et $\varepsilon'$ . $A$ est la somme de $Ae$ et $Ae'$ et cette somme est directe car $Ae.Ae' = Ae \cap Ae' = (0)$

Comme $e \in V$ , on a $e = e^n \in V^n$ et donc $Ae \subset N = \bigcap_n V^n$ . De même $Ae' \subset N' = \bigcap_n V'^n$ . Or $A = Ae + Ae' = Ae^n + Ae'^n$ d'où $A = V^n + V'^n$ et $V^n$ et $V'^n$ étant premiers entre eux $V^n \cap V'^n = V^n V'^n$ , notamment $VV' = M$ et donc $V^n \cap V'^n = M^n$ . Or $A$ étant séparé $\bigcap_1^\infty M^n = (0)$ donc $N \cap N' = (0)$ . De $N \supset Ae$ , $N' \supset Ae'$ et $N \cap N' = (0)$ on déduit que $N = Ae$ et $N' = Ae'$ . En effet si $n \in N$ , on a $n = u + u'$ avec $u \in Ae$ et $u' \in Ae'$ . Alors $u' = n - u \in N$ donc $u' = n - u = 0$ et $n \in Ae$ donc $N = Ae$ , et de même $N' = Ae'$ .

On a $M^n N \subset N \cap M^n$ . Inversement si $xe \in N$ et $xe \in M$ on a $xe = xe.e \in M^n N$ donc $M^n N = N \cap M^n$ , ce qui prouve que la topologie canonique sur $N$ coïncide avec la topologie induite. Alors $N$ est fermé dans $A$ comme intersection d'idéaux fermés, car les ouverts $V^n$ sont aussi fermés (Cf. Bourbaki, Topologie générale, Ch.III § 2, prop. 4). On a alors $N/MN = N/M \cap N \simeq M + N/M = M + Ae/M = V/M$ et $V/M \simeq A/V'$ puisque $A/M$ est la somme directe de $V/M$ et $V'/M$ .

BIBLIOGRAPHIE :

I.- M. KRASNER : Séminaire sur les corps valués (1953/1954) (Espaces ultramétriques)

II.- P. SAMUEL : Commutative algebra. Cours de l'Université de Cornell, 1953 (rédigé par D. Hertzig) Chapitres IV et V.

III.- P. SAMUEL : Algèbre locale (Mémorial des Sciences mathématiques, 1953) Ch.I.