Séminaire Dubreil.
Algèbre et théorie
des nombres

Pierre Samuel

Extensions des corps valués complets

Séminaire Dubreil. Algèbre et théorie des nombres, tome 1 (1947-1948), exp. n° 4, p. 1-10
<http://www.numdam.org/item?id=SD_1947-1948__1__A4_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1947/48
-:-:-:-

Exposé n° 4

EXTENSIONS DES CORPS VALUÉS COMPLETS

par Pierre SAMUEL

1. Vocabulaire et notations.

Dans un corps K, une valuation est une fonction $v(x)$ des éléments x non nuls du corps, dont les valeurs sont dans un certain module, ou groupe abélien additif, M, appelé module de valuation, et qui vérifie les relations :

$$v(ab) = v(a) + v(b) , \quad v(-a) = v(a) ;$$

$$v(a + b) \geqslant \text{minimum } (v(a) , v(b)) .$$

La valeur absolue est l'exponentielle de l'opposée de la valuation :

$$\exp(-v(a)) = |a| \qquad (\exp 1 > 1) .$$

EXEMPLES. - Dans le corps K des nombres rationnels, ayant adopté un nombre premier p, on peut prendre :

$$v(a) = i , \quad a = p^i . \frac{u}{v} \qquad (u.v \text{ premiers avec } p)$$

Dans un ensemble de fonctions meromorphes, un point $z = a$ du plan complexe étant choisi, on peut prendre :

$v(a)$ = ordre du zéro a de la fonction

(un pôle étant considéré comme un zéro d'ordre négatif).

Une unité de K est un élément de valuation nulle.

L'anneau A de valuation de K est l'ensemble des éléments de valuation non négative, y compris 0, (dont on peut prendre $v(0) = +\infty$)

L'idéal P de valuation de K est l'ensemble des éléments de valuation positive : éléments de A non unités.

L'ensemble A est bien un anneau car :

$$a\,,\ a' \in A \iff v(a) \geqslant 0 \ \text{ et } \ v(a') \geqslant 0$$
$$\longrightarrow \begin{cases} v(aa') \geqslant 0 \longrightarrow aa' \in A \\ v(a + a') \geqslant 0 \longrightarrow a + a' \in A\,. \end{cases}$$

L'ensemble P est bien un idéal de l'anneau A.

$$d\,,\ d' \in P \longrightarrow v(d + d') \geqslant \min(v(d)\,,\ v(d')) > 0 \longrightarrow d + d' \in P\,.$$
$$d \in P \ \text{ et } \ a \in A \longrightarrow v(ad) = v(a) + v(d) > 0 \longrightarrow ad \in P$$

L'idéal P est maximal, donc l'anneau quotient $A|P$, des classes de A, mod P, est un corps R, appelé corps résiduel.

On supposera ici que le module de valuation M est un groupe cyclique infini, isomorphe au groupe additif des entiers. Dans ce cas, il existe dans P un élément p tel que $v(p)$ soit minimum. Alors P est l'idéal principal (p) (produits de p par les éléments de A). Les autres idéaux de A sont les idéaux principaux $P^i = (p^i)$ (puissances positives entières). La base p est appelée l'uniformisante pour la valuation (locale), (lorsque plusieurs valuations sont considérés simultanément).

2. Lemme de Hensel.

Dans un corps valué complet K, si un polynôme $f(x)$, à coefficients dans A (anneau de valuation), considéré mod P (idéal de valuation) est congru au produit de deux polynômes, à coefficients dans A, premiers entre eux :

$$f(x) \equiv g(x) \times h(x)\ ; \quad \exists\ U(x)\,,\ V(x) : \ U.g(x) + V.h(x) \equiv 1 \pmod{P}$$

et tels que degré$(f - gh) <$ degré f ;

ce polynôme est aussi décomposable dans A, en un produit de deux polynômes $g_0(x)$, $h_0(x)$, respectivement congrus à $g(x)$ et $h(x)$, mod P.

Nous construirons $g_0(x)$ et $h_0(x)$, par approximations successives, en formant une suite de polynômes $g_n(x)$, $h_n(x)$, qui pour n augmentant indéfiniment (par valeurs entieres), auront précisément pour valeurs les polynômes cherchés.

Ces polynômes vérifieront la congruence de décomposition, mod P^n, nous allons les calculer par récurrence sur l'exposant n.

Supposons obtenus (pour $n \geqslant 1$), des polynômes $g_n(x)$ et $h_n(x)$ normés, tels que :

$$f(x) - g_n(x)\ h_n(x) = \varphi(x).p^n\,, \qquad \begin{matrix} g_n(x) \equiv g(x) \\ h_n(x) \equiv h(x) \end{matrix} \pmod{P}$$

et

$$\text{degré } \varphi(x) \leqslant m = \text{degré } f(x) \ .$$

Nous cherchons à calculer de nouveaux polynômes définis par :

$$g_{n+1}(x) = g_n(x) + p^n.g'(x) \ , \quad h_{n+1}(x) = h_n + p^n.h'$$

ils sont encore congrus, mod P (ou mod (p)) à g et h , et :

$$f(x) - g_{n+1}(x)\, h_{n+1}(x) \equiv \varphi(x).p^n + p^n(g_n\, h' + h_n\, g') \quad (P^{n+1})$$

(les termes négligés dans le deuxième membre, étant multiples de p^{2n} sont dans P^{n+1} , puisque $2n \geqslant n+1$) .

Pour obtenir le résultat cherché, il suffit de déterminer g' et h' , de degrés respectivement inférieurs à ceux de g et h (de façon à ne pas altérer les termes de plus haut degré), et tels que :

$$p^n(\varphi(x) + g_n(x)\, h'(x) + h_n(x)\, g'(x)) = 0 \ (\text{mod } P^{n+1})$$

ou, en divisant par p^n et tenant compte des congruences de g_n et h_n avec g et h :

$$\varphi(x) + g(x)\, h'(x) + h(x)\, g'(x) \equiv 0 \quad (\text{mod } P) \ .$$

Mais g(x) et h(x) étant, par hypothèse, premiers entre eux mod P , on peut trouver des polynômes (à coefficients définis mod P , dans A) , U(x) , V(x) , Q(x) , tels que :

$$(Q.h - \varphi.U).g(x) + (-Q.g - \varphi.V).h(x) \equiv -\varphi(x) \quad (\text{mod } P) \ ;$$

il suffit alors de prendre :

$$h'(x) = Q.h - \varphi.U \ , \quad g'(x) = -Q.f - \varphi.V$$

en déterminant Q de façon que h'(x) soit de degré inférieur à celui de h(x) . Puisque le degré de φ est inférieur à m , il en résultera que le degré de g'h sera aussi inférieur à m , et par suite que le degré de g' sera inférieur au degré de g . En outre la congruence sera bien vérifiée.

Les suites de polynômes g_n et h_n vérifient la condition de Cauchy (pour les valeurs absolues) puisque, par exemple :

$$g_n - g_{n+1} \equiv 0 \text{ mod } P^n, \text{ donc } v(g_n - g_{n+i}) \geqslant v(p^n) \ .$$

Le corps K étant complet, elles ont des limites, dans K , telles que :

$$v(f - g_0\, h_0) \geqslant v(p^n) \quad (\text{pour tout } n)$$

ce qui entraîne l'annulation de la différence.

La démonstration pourrait être étendue au cas d'un idéal de valuation P, non principal.

D'un point de vue opposé, un cas particulier de cette démonstration semble avoir été à l'origine de l'introduction des corps p-adiques (puis valués) par HENSEL.

Si un polynôme $f(x)$, à coefficients entiers (ordinaires) s'annule, mod p, pour une valeur a, qui n'est pas zéro double :

$$f(a) \equiv 0 , \quad f'(a) \not\equiv 0 , \quad (\text{mod } p)$$

(p nombre premier) ; elle admet un zéro simple a_n, pour tout module p^n (a_n étant congru à a, mod p)

3. Enoncé du problème.

A partir d'un corps K, valué, complet, d'éléments a, b, ..., de valuation $v(a)$, et d'une extension finie $L|K$, de degré $n = (L : K)$, d'éléments $\alpha, \beta, \ldots$ nous nous proposons d'en trouver une valuation $w(\alpha)$, ... de L telle que w induise v sur K :

$$a \in K \subset L \longrightarrow w(a) = v(a) .$$

Nous dirons que $L|K$ est une extension valuée et que w est le prolongement de v.

Nous désignerons les éléments de L par les lettres successives de celles qui désignent les éléments de K :

B anneau de valuation : $A = [B , K]$;
Q idéal de valuation : $P = [Q , K]$
N module de valuation, d'uniformisante q $M \subset N$;
S corps résiduel $B|Q$: $R = [B , K]/[Q , K]$ sous-corps S

Il en résulte évidemment :

- La dimension $n = (L : K)$ de l'espace vectoriel L sur K est le degré de l'extension :

- Le degré $f = (S : R)$ est appelé le degré résiduel ;
l'indice $e = (N : M)$ (tel que $p = q^e$) est appelé le nombre de ramification.

4. Unicité du prolongement w .

Si le prolongement $w(\alpha)$ existe dans l'extension L , il est unique.

Propriété préalable. - Tout espace vectoriel topologique V , de dimension n , sur un corps valué complet K , a la topologie de la puissance directe K^n .

La demonstration se fait par récurrence sur n , la propriété étant évidente pour $n = 1$.

En raison de l'additivité, il suffit d'établir la bicontinuité au voisinage de 0 .

L'espace V étant construit comme la somme d'un espace U' de dimension 1 et d'un espace U'' de dimension $n - 1$, tout vecteur x de V est ainsi, de façon unique, somme de deux vecteurs :

$$x = u'(x) + u''(x) ;$$
$$u'(x) = a.\lambda(x) \in U' , \lambda(x) \in K ;$$
$$u''(x) \in U'' .$$

L'isomorphisme étant algébrique :

u' tend vers 0 et u'' tend vers $0 \longrightarrow$ x tend vers 0

En sens inverse on raisonne par l'absurde : si la continuité n'avait pas lieu, on pourrait trouver une suite x_n telle que $u'(x_n)$ ne tende pas vers 0 , donc une suite incluse x_m telle que :

$$|\lambda_m| > \delta$$

Mais alors :

$x_m : \lambda_m$ tend vers 0 ; $-a + x_m : \lambda_m$ tend vers $-a$.

Le vecteur premier membre ainsi formé est dans U'' ; sa limite $-a$ devrait être aussi dans U'' , ce qui est absurde.

CONSÉQUENCES. - Dans K , la valuation $v(a)$ définit une topologie ; on peut définir topologiquement l'idéal P : l'ensemble des éléments a , tels que a^n tende vers 0 lorsque n entier augmente indéfiniment, car :

$$v(a^n) = n.v(a)$$

augmente indéfiniment.

S'il existe une valuation $w(a)$ dans le corps L , elle définit une topologie,

telle que l'idéal Q soit defini par les éléments :

$$w(\alpha) > 0 \qquad \text{ou} \qquad \alpha^n \text{ augmente indefiniment.}$$

Cette topologie sera donc entièrement définie par la valuation de l'uniformisante q, laquelle est elle-même définie par la valuation de l'uniformisante p de M (qui en est un multiple).

5. Construction d'une valuation.

Tout élément α de L est algébrique sur K, il est zéro d'un polynôme irréductible normé, déterminé (polynôme minimal, ou fondamental) :

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n , \quad f(\alpha) = 0 .$$

nous poserons

$$w(\alpha) = (v(a_n) : n) .$$

Cette définition reste valable quand on remplace $f(x)$ irréductible par une de ses puissances : a_n est remplacé par a_n^h et n par nh.

On peut d'abord vérifier que :

$$a \in K \longrightarrow w(a) = v(a) , \quad w(\alpha\beta) = w(\alpha) + w(\beta) .$$

α étant zéro de $f(x)$ de degré n et $f(0) = a_n$;
β étant zéro de $g(x)$ de degré m et $g(0) = b_m$;
$\alpha\beta$ est zéro de $F(x)$ de degré mn (peut être à zéros multiples) et

$$F(0) = a_n^m b_m^n , \quad v(a_n^m b_m^n) : mn = v(a_n) : n + v(b_m) : m$$

Il reste à vérifier :

$$w(\alpha + \beta) \geqslant \min(w(\alpha) , w(\beta)) ;$$

ou

$$w(\theta) \geqslant 0 \longrightarrow w(1 + \theta) \geqslant 0$$

Cette deuxième condition est un cas particulier de la première pour :

$$\alpha = 1 , \quad \beta = \theta ;$$

inversement elle entraîne la première en prenant :

$$w(\beta) \geqslant w(\alpha) , \quad \theta = \beta : \alpha .$$

Je forme le polynôme fondamental de θ irréductible et au moins de degré 1 :

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

$$w(\Theta) \geqslant 0 \longrightarrow v(a_n) \geqslant 0 \quad \text{où} \quad a_n \in A .$$

Le polynôme fondamental de $1 + \Theta$ a pour terme consfant :

$$b = (-1)^n + (-1)^{n-1} a_1 + \ldots + a_n$$

Il suffit de montrer, en raisonnant par l'absurde, que la valuation

$$v(b) \geqslant \min v(a_i)$$

ne peut être négative.

Si non, un ou plusieurs des coefficients a_i aurait une valuation négative, soit $-r$ la plus petite d'entre elles et soit a_k le coefficient de plus grand indice dont la valuation soit égale à $-r$.

Formons le produit $g(x) = p^r f(x)$, les coefficients de ce nouveau polynôme vérifient les conditions :

$i > k$: $v(p^r a_i) = r + v(a_i) > 0$, où $p^r a_i \in P$

$i = k$: $v(p^r a_k) = r + v(a_k) = 0$, où $p^r a_k$ unité $\in A$

$i < k$: $v(p^r a_i) = r + v(a_i) \geqslant 0$, où $p^r a_i \in A$

Le polynôme $x^k g_1(x)$ formé par les termes de degré au moins égaux à k vérifie les conditions :

$g(x) - x^k g_1(x) \equiv 0 \pmod{P}$;

degré $(g(x) - x^k g_1(x)) <$ degré $(g(x))$.

En outre ces divers polynômes ont leurs coefficients dans A , et k est au moins égal à 1 , puisque $v(a_h x)$ n'est pas négatif.

Nous nous trouvons dans les conditions d'application du lemme de Hensel ; le polynôme $g(x)$ décomposable, mod P , le serait aussi dans A ; mais alors $f(x)$ serait lui-même décomposable, ce qui est contraire à l'hypothèse puisqu'il est polynôme fondamental de Θ , donc irréductible.

6. Egalité $n = ef$: n degré de $L|K$, e degré résiduel, f nombre de ramification.

Prenons pour module de valuation de L , l'ensemble z des entiers $(w(q) = 1)$; le module M de K sera ez (puisque $N : M = e$) .

Prenons f éléments ω_i unités de B , linéairement indépendants dans R , de

façon à constituer une base de S :

$$(\sum e_i \omega_i = 0 \pmod{Q} \quad , \quad e_i \in A) \longrightarrow e_i = 0 \pmod{P}$$

Les ef éléments de B :

$$\omega'_{ij} = \omega_i q^j \quad (0 \leq j < e) \quad , \quad w(\omega'_{ij}) = w(\omega_i) + j$$

sont indépendants, relativement à A (ou à K) de sorte que $ef \leq n$.

Cherchons à déterminer les $a_{ij} \in A$, tels que :

$$0 = \sum a_{ij} \omega'_{ij} = \sum a_i \omega_i q^j \quad , \quad w(\omega_i) = 0$$

la valuation d'un élément de cette somme est :

$$w(a_{ij} \omega'_{ij}) = w(a_{ij} \omega_i q^j) = v(a_{ij}) + j = j + ek$$

k étant un entier dépendant de a_{ij} . Si les coefficients a_{ij} ne sont pas tous nuls, considérons les termes dont la valuation est minimum, et désignons sa valeur par h_0 ; elle est nécessairement obtenue pour une (même) valeur j_0 de j et k_0 de k et peut être pour plusieurs valeurs s de i . Pour ces termes, on aurait :

$$a_{sj_0} = b_s p^{k_0} \quad \text{ou} \quad q^{-h_0} a_{sj_0} \omega_s q^{j_0} = b_s \omega_s = \text{unités de } B$$

et pour tous les autres :

$$w(q^{-h_0} a_{ij} \omega_i q^j) > 0 \quad , \quad \text{ou} \quad q^{-h_0} a_{ij} \omega_i q^j \in Q \ .$$

Il en résulte, pour l'égalité considérée :

$$0 = q^{-h_0} \sum a_{ij} \omega'_{ij} = \sum b_s \omega_s \pmod{Q} \ ;$$

mais les b_s étant dans A

$$b_s \equiv 0 \pmod{P}$$

ce qui est contraire à l'indépendance des ω_i et, a fortiori, des ω_s . L'égalité supposée entraîne donc l'annulation de tous les a_{ij} , ce qui démontre l'indépendance des ω'_{ij} .

Pour établir que ces ef éléments forment effectivement une base de L , sur K ,

nous allons former, pour un élément arbitraire α de L une expression d'approximation (congrue mod Q^n) dont la limité (pour n infini) donnera une construction de α .

On peut supposer que la valuation de α vérifie la condition

$$0 \leqslant v(\alpha) = j_n < e \ ;$$

il suffit au bescin de multiplier l'élément par une puissance convenable p^h , qui étant dans K , ne fera que modifier les coefficients a_{ij} des ω'_{ij} .

D'après le choix fait des ω_i , (base des éléments de B , mod Q) , on peut trouver des $a_i \in A$, tels que, pour αq^{-j_0} , qui est dans B :

$$\alpha q^{-j_0} - \sum a_i \omega_i = 0 \quad (\text{mod } Q) \ ;$$

ou

$$\alpha - \sum a_i \omega_i q^{j_0} = \alpha - \sum a_i \, {}_{j_0} \omega'_{ij_0} = 0 \quad (\text{mod } Q) \ .$$

Nous allons établir, par récurrence sur n , une congruence analogue pour le module Q^n .

Supposons trouvés des coefficients $a_{ij}^{(n)}$, que nous noterons provisoirement a_{ij} , tels que :

$$\alpha - \sum a_{ij} \omega'_{ij} \in Q^n \quad \text{ou} \quad \alpha - \sum a_{ij} \omega'_{ij} = q^n . \beta \ , \quad \beta \in B$$

(ceci est vérifié pour n = 1 , avec les seules valeurs j_0 de j) .

On peut trouver des coefficients $c_i \in A$ tels que :

$$\beta - \sum c_i \omega_i \in Q \quad \text{ou} \quad \beta - \sum c_i \omega_i = q . \beta' \ , \ \beta' \in B \ .$$

Effectuons la division de n par e :

$$n = \lambda e + j_n \quad (0 \leqslant j_n < e \ , \ \lambda \text{ entier})$$

on a :

$$q^{n+1} \beta' = q^n (\beta - \sum c_i \omega_i) = q^n \beta - \sum c'_{ij_n} (\omega_i \, q^{j_n})$$

$$= q^n \beta - \sum c'_{ij_n} \omega'_{ij_n} \quad (c'_{ij_n} = c_i P^{\lambda}) \ .$$

En revenant a α , ceci donne l'approximation cherchée pour $n + 1$:

$$\alpha - \sum a'_{ij} \omega'_{ij} = q^{n+1} \beta' \in Q^{n+1} \quad (a'_{ij} = a_{ij} + c'_{ij})$$

(on prend bien entendu $c'_{ij} = 0$, pour $j \neq j_n$) .

Les éléments $a_{ij}^{(n)}$ (notés a_{ij}) , suivis par $a_{ij}^{(n+1)}$ (notés a'_{ij}) forment une suite convergnete, puisque :

$$(a_{ij} - a'_{ij}) = c_{ij} \in P^{\lambda} \text{ d'où } (a_{ij}^{(n)} - a_{ij}^{(n+h)}) \in P^{\lambda} \ ;$$

les P^{λ} s'emboîtent dans tous les suivants, de sorte que la suite vérifie la condition de Cauchy.

Elle a donc une limite qui est égale à α .