Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Marc Krasner

Valuations des anneaux et des corps non commutatifs

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 11, n° 2 (1969-1970), exp. n° 20, p. 1-20
<http://www.numdam.org/item?id=SDPP_1969-1970__11_2_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
11e année, 1969/70, n° 20, 20 p.

25 mai 1970

VALUATIONS DES ANNEAUX ET DES CORPS NON COMMUTATIFS

par Marc KRASNER

En faisant, d'abord à la Faculté des Sciences de Clermont-Ferrand et, à partir de 1965, à celle de Paris, mes cours de la théorie des valuations, je me suis aperçu graduellement que toute la théorie des anneaux et des corps valués à l'aide des groupes totalement ordonnés reste valable, sans hypothèse de leur commutativité et, pour une grande part, sans supposer la commutativité du groupe des valeurs.

1. Quelques définitions et rappels.

On va employer le signe $\subset$ au sens d'inclusion stricte, et le complément d'un ensemble A dans un ensemble B (qui n'est pas supposé être son sur-ensemble) sera noté $B..A$.

Un espace métrique E , dont $d(x , y)$ soit la distance, est dit un espace <u>ultramétrique</u>, si $d(x , y)$ satisfait à l'axiome supplémentaire

$$d(x , z) \leqslant \max[d(x , y) , d(y , z)] .$$

Un ensemble E , muni d'une application $d : E \times E \to \Delta$, où Δ est un ensemble totalement ordonné quelconque ayant le plus petit élément noté 0 (zéro), est dit un espace <u>hyperultramétrique</u>, si l'application d (dite toujours sa <u>distance</u>) satisfait aux axiomes :

1° $d(x , y) = 0$ si, et seulement si, $x = y$;
2° $d(x , y) = d(y , x)$;
3° $d(x , z) \leqslant \max[d(x , y) , d(y , z)]$.

Les espaces hyperultramétriques ont des propriétés semblables, la plupart du temps, à celles des espaces ultramétriques (tout point d'un cercle est son centre, si deux cercles ne sont pas disjoints, un contient l'autre, etc.). On peut les compléter par la méthode générale de complétion des espaces uniformes, mais on peut le faire aussi par des méthodes plus proches de celles de la théorie des espaces ultramétriques : chaînes de Cauchy, chaînes de cercles emboîtés à rayons non bornés inférieurement, etc.

On appelle <u>groupe valué</u> (resp. <u>hypervalué</u>), un groupe g (dont xy soit la loi de composition, et e l'élément neutre) muni d'une distance ultramétrique (resp. hyperultramétrique) $d(x , y)$ préservée par les translations (à gauche et à droite) de g :

$$d(ax , ay) = d(xa , ya) = d(x , y) \ .$$

La fonction $|x| = d(x , e)$ est dite la <u>valuation</u> (resp. l'<u>hypervaluation</u>) de g , et on a

$$d(x , y) = |x^{-1} y| = |y^{-1} x| = |xy^{-1}| = |yx^{-1}| \ .$$

Cette fonction satisfait aux axiomes :

1° $|x| = 0 \iff x = e$;
2° $|x^{-1}| = |x|$;
3° $|xy| \leqslant \max(|x| , |y|)$;
4° $|cxc^{-1}| = |x|$.

Vice-versa, si on a une telle fonction satisfaisant à ces axiomes, g , muni de $d(x , y) = |x^{-1} y|$, est un groupe valué ou hypervalué.

Si g est un groupe abélien écrit additivement, l'axiome 4° est trivialement satisfait, et les axiomes 1°-3° prennent la forme :

1° $|x| = 0 \iff x = 0$;
2° $|-x| = |x|$;
3° $|x + y| \leqslant \max(|x| , |y|)$.

Un objet α est dit opérateur à gauche (resp. à droite) d'un groupe valué ou hypervalué g (dont $|..|$ soit la valuation ou l'hypervaluation), si (en plus de structure de groupe valué ou hypervalué de g) est donnée une multiplication αx à gauche (resp. $x\alpha$ à droite) des $x \in g$ par α , qui est un opérateur à gauche (resp. à droite) du groupe abstrait g [autrement dit, on a $\alpha(xy) = (\alpha x)(\alpha y)$ (resp. $(xy)\alpha = (x\alpha)(y\alpha)$)], et en plus $|\alpha x|$ (resp. $|x\alpha|$) ne dépend que de $|x|$ et en est une fonction croissante au sens large.

Si l'ensemble des valeurs Λ de l'hypervaluation $|x|$ [ou de la distance $d(x , y)$] de g est un presque-groupe totalement ordonné $\Gamma \cup \{0\}$, c'est-à-dire la réunion d'un groupe totalement ordonné (et pas forcément commutatif) Γ et d'un élément bilatéralement absorbant et minimum 0 [je rappelle qu'un groupe Γ est dit <u>totalement ordonné</u>, s'il est muni d'un ordre total $\alpha < \beta$ tel que

$$\alpha < \beta \implies \gamma\alpha < \gamma\beta \quad \text{et} \quad \alpha\gamma < \beta\gamma \ ;$$

on notera 1 l'élément neutre de Γ], un opérateur α à gauche (resp. à droite) du groupe hypervalué g est dit <u>spécial</u>, s'il existe un élément $\|\alpha\|$ de Γ , dit <u>norme</u> de α , tel que, pour tout $x \in g$, on ait

$$|\alpha x| = \|\alpha\| \, |x| \qquad (\text{resp. } |x\alpha| = |x| \, \|\alpha\|) \ .$$

Deux espaces hyperultramétriques

$$(E\ ,\ d : E \times E \to \Delta) \quad \text{et} \quad (E'\ ,\ d' : E' \times E' \to \Delta')$$

sont dits isomorphes, s'il existe deux bijections

$$f : E \to E' \ ,$$

$$\varphi : \Delta(E) \to \Delta'(E') \ ,$$

($\Delta(E)$, $\Delta'(E')$ sont les ensembles des valeurs prises par d sur $E \times E$ (resp. par d' sur $E' \times E'$)) telles que :

1° $d'(f.x\ ,\ f.y) = \varphi.d(x\ ,\ y)$;

2° φ est strictement croissante ;

3° Le minimum 0 de Δ est un point limite de $\Delta(E)$ par rapport à la topologie d'ordre de Δ , si, et seulement si, celui $0'$ de Δ' en est un de $\Delta'(E')$ par rapport à celle de Δ' .

Deux hyperultramétriques $d(x\ ,\ y)$ et $d'(x\ ,\ y)$ d'un même ensemble E sont dites <u>équivalentes</u>, si $(E\ ,\ d)$ et $(E\ ,\ d')$ sont isomorphes.

En particulier, si Δ est un presque-groupe totalement ordonné $\Gamma \cup \{0\}$, et si $\gamma \in \Gamma$, les hyperultramétriques $\gamma d(x\ ,\ y)$ et $d(x\ ,\ y)\gamma$, dites les <u>translatées</u> à gauche et à droite de l'<u>hyperultramétrique</u> $d(x\ ,\ y)$ de E par γ , sont équivalentes à cette hyperultramétrique. D'autre part, si ω est un opérateur (à gauche ou à droite) du groupe ordonné Γ [autrement dit, un automorphisme du groupe abstrait Γ tel que $\alpha < 1$ implique $\omega\alpha < 1$], $d(x\ ,\ y) \to d'(x\ ,\ y) = \omega.d(x\ ,\ y)$ est encore une équivalence d'hypervaluations, appelée une <u>potentiation</u>.

2. Anneaux valués et hypervalués.

Soit A un anneau. Faisons correspondre à tout $a \in A$ deux opérateurs a_g et a_d respectivement à gauche et à droite, dits <u>multiplicateurs</u> à gauche et à droite <u>par</u> a , tels que, pour tout $x \in A$, on ait

$$a_g.x = ax \ , \qquad x.a_d = xa \ .$$

Soit $|..|$ une hypervaluation du groupe additif de A à l'aide d'un presque-groupe totalement ordonné $\Delta = \Gamma \cup \{0\}$. Cette hypervaluation sera dite une <u>hypervaluation de l'anneau</u> A , si, pour tout $a \in A$, les opérateurs a_g (à gauche) et a_d (à droite) du groupe additif de A sont des opérateurs spéciaux (de même côté) de ce groupe hypervalué par $|..|$ Autrement dit, $|..| : A \to \Gamma \cup \{0\}$ est une telle hypervaluation, si elle satisfait aux axiomes :

1° $|x| = 0 \iff x = 0$;

2° $|-x| = |x|$;

3° $|x+y| \leqslant \max(|x|, |y|)$;

4° Il existe, pour tout $a \in A$, deux constantes $\|a_g\|$ et $\|a_d\| \in \Gamma \cup \{0\}$, telles que $|xy| = \|x_g\|\,|y| = |x|\,\|y_d\|$.

Un anneau A, muni d'une telle hypervaluation, sera dit un anneau hyperultramétrique (éventuellement, si Γ est un groupe multiplicatif des nombres réels positifs, il sera dit ultramétrique). On démontre :

Si A est hyperultramétrique, ou bien il est sans diviseurs de zéro, ou bien il est autoannulant ($A^2 = 0$).

On a $\|(xy)_g\| = \|x_g\|\,\|y_g\|$ et $\|(xy)_d\| = \|x_d\|\,\|y_d\|$.

S'il existe un $a \in A$ tel que $\|a_g\| = |a|$ ou $\|a_d\| = |a|$, on a, pour tout $x \in A$, $\|x_g\| = |x| = \|x_d\|$.

Une telle hypervaluation de A, dont l'existence exclue l'hypothèse $A^2 = 0$, sera dite une hypervaluation réduite de A, et un anneau hyperultramétrique sera dit hypervalué ([1]) (valué, dans le cas ultramétrique), si son hypervaluation est réduite, autrement dit s'il satisfait aux axiomes :

(I) $|x| = 0 \iff x = 0$;

(II) $|x+y| \leqslant \max(|x|, |y|)$;

(III) $|xy| = |x|\,|y|$.

(En effet, l'axiome $|-x| = |x|$ est superflue, car elle résulte de (III).) Si le groupe Γ est commutatif, A (qui peut être non commutatif) est dit commutativement hypervalué. Si A est un corps (pas forcément commutatif), il sera dit corps hypervalué (commutativement, si Γ est commutatif).

Si $A^2 \neq 0$, il existe les translatées $\lambda|..|$ à gauche et $|..|\lambda$ à droite ($\lambda \in \Gamma$) de $|..|$, qui sont des hypervaluations réduites ; autrement dit, les anneaux hyperultramétriques, qui ne sont pas autoannulants, coïncident, à l'équivalence d'hypervaluation près, avec les anneaux hypervalués.

Un corps K est dit un corps-quotient d'un anneau (pas forcément commutatif) $A \subseteq K$, si tout $\alpha \in K$ peut se mettre, à la fois, sous chacune des deux formes $\alpha = ab^{-1}$ (A-représentation à gauche) et $\alpha = b'^{-1}a'$ (A-représentation à droite), où a, $b \neq 0$, a', $b' \neq 0$, appartiennent à A.

([1]) Ou valué au sens de Krull.

On montre facilement que, si un anneau hypervalué A possède un corps-quotient K , son hypervaluation se prolonge, et d'une seule manière, en une hypervaluation de K .

Le cercle

$$i(A) = C(0\ ,\ 1) = \{a \in A\ ;\ \ |a| \leqslant 1\}\ ,$$

de centre 0 et de rayon 1 dans A , est un anneau, appelé anneau d'intégrité de A . Tout cercle de centre 0 dans A est, évidemment, un $i(A)$-module bilatère (et, en particulier, un idéal bilatère de $i(A)$, s'il y est contenu). Le cercle non circonférencié

$$p(A) = C(0\ ,\ 1^-) = \{a \in A\ ;\ \ |a| < 1\}$$

est un idéal bilatère premier de $i(A)$, et $\bar{A} = i(A)/p(A)$ est un anneau sans diviseurs de zéro, dit anneau résiduel de A .

Le complété $\hat{A}$ d'un anneau hypervalué A est encore un anneau hypervalué, si l'on prolonge par continuité uniforme à $\hat{A}$ l'addition et la multiplication de A .

L'ensemble des valeurs $\Delta(\hat{A}) = \Delta^*(\hat{A}) \cup \{0\}$ (où $\Delta^*(\hat{A}) = \Delta(A) \cap \Gamma$) que prennent sur $\hat{A}$ son hypervaluation et l'anneau résiduel $\bar{\hat{A}}$ de $\hat{A}$, sont les mêmes (avec l'identification évidente pour les éléments des anneaux résiduels) que les objets correspondants de A .

3. Anneaux proprement valués et hypervalués. Anneaux d'hypervaluation (et de valuation).

Un anneau hypervalué (et, en particulier, valué) l'est dit proprement, si, en plus des axiomes (I)-(III), il vérifie l'axiome :

(IV) Si $a\ ,\ b \in A$ sont tels que $|a| \leqslant |b|$, il existe $c\ ,\ c' \in A$ tels que $a = bc = c'b$.

[Visiblement, on a $c\ ,\ c' \in i(A)$. On peut formuler cet axiome en disant que, si $|a| \leqslant |b|$, b divise a à gauche et à droite.]

Si A est proprement hypervalué, il est unitaire, et les cercles de centre 0 sont les seuls $i(A)$-sous-modules à gauche et les seuls $i(A)$-sous-modules à droite de A . Ainsi, tout $i(A)$-module (et en particulier, tout idéal de i) à gauche ou à droite est bilatère, et $p(A) = C(0\ ,\ 1^-)$ est un idéal maximal de $i(A)$, d'où il résulte que $\bar{A} = i(A)/p(A)$ est un corps.

Si Γ_A est le groupe engendré par $\Delta^*(A)$, $\Delta^*(A)$ est la classe inférieure d'une coupure de Γ_A (ordonné par l'ordre induit par celui de Γ). (Puisque $|1| = 1 \in \Delta^*(A)$, cette coupure est telle que 1 appartient à sa classe inférieure.)

Un anneau proprement hypervalué A admet un corps-quotient K, et on a $\Delta^*(K) = \Gamma_A$ et $A = \{\alpha \in K \; ; \; |\alpha| \in \Delta(A)\}$.

PROPOSITION 1. - L'hypervaluation d'un anneau hypervalué A est complètement déterminée, à l'équivalence près, par sa structure d'anneau et par la donnée de son sous-anneau $i(A)$.

On peut la définir à partir du couple $(A , i(A))$ par le même procédé que dans le cas commutatif.

$\Delta(A)$ est l'ensemble $\{ai(A) = i(A)a \; ; \; a \in A\}$ muni de la composition

$$(ai(A))(bi(A)) = ai(A)\, bi(A) = abi(A)$$

[dont $0i(A) = \{0\}$ est un élément bilatéralement absorbant], qu'y induit la multiplication de A, et d'un ordre

$$ai(A) < bi(A) \iff_{\text{déf}} ai(A) \subset bi(A) \; .$$

On prouve que $\Delta^*(A) = \Delta(A)..0i(A)$ est un semi-groupe (c'est-à-dire un demi-groupe bilatéralement simplifiable) admettant un groupe des fractions Γ_A, auquel on peut prolonger l'ordre de $\Delta(A)$ de manière qu'il devienne un groupe totalement ordonné. On pose $|a| = ai(A)$.

THÉORÈME 1. - Un couple d'anneaux unitaires et sans diviseurs de zéro, $(A , i \subseteq A)$, est tel qu'il existe une hypervaluation de A dont i soit l'anneau d'intégrité si, et seulement si :

1° Pour tout $a \in A$, $ai = ia$;
2° La famille $\Delta = \{ai \; ; \; a \in A\}$ est totalement ordonnée par la relation d'inclusion.

Cette hypervaluation (dont l'unicité résulte de la proposition 1) est à valeurs commutatives, si, et seulement si, on a, en plus :

3° Pour tous $a , b \in A$, on a $abi = bai$.

On peut donner à ces conditions d'autres formulations. Rappelons qu'un sous-ensemble B d'un anneau A est dit invariant (par rapport à sa multiplication), si l'on a, pour tout $a \in A$, $aB = Ba$. [Si A est plongeable dans un corps K, et si $A^* = A..\{0\}$, la condition de l'invariance peut s'écrire aussi : $(\forall a \in A^*)$ $[aBa^{-1} = B]$. Si, en plus, K est un corps-quotient de A, un $B \subseteq A$ invariant dans A l'est aussi dans K.] On peut donc formuler le 1° sous la forme suivante: i est invariant dans A. On peut aussi formuler 1°, 2°, 3° en termes de divisibilité. On dira que a i-divise b $(a , b \in A)$ à gauche (resp. à droite) (notation:

$a \mid_{\overleftarrow{i}} b$ (resp. $a \mid_{\overrightarrow{i}} b$)), si $b = ac$ (resp. $b = ca$), où $c \in i$. On dira que a , b sont i-associés à gauche (resp. à droite), si chacun d'eux i-divise l'autre à gauche (resp. à droite) (notation : $a \overleftarrow{\leftarrow}_i b$ (resp. $a \overrightarrow{\rightarrow}_i b$)). [Si A est sans diviseurs de zéro, $a \overleftarrow{\leftarrow}_i b$ signifie que $a = ub$, où $u \in i$ en est un élément inversible, et corélativement pour $\overrightarrow{\rightarrow}_i$.] On écrira $a \mid_i b$ si l'on a à la fois $a \mid_{\overleftarrow{i}} b$ et $a \mid_{\overrightarrow{i}} b$, et on écrira $a \equiv_i b$ si l'on a à la fois $a \overleftarrow{\leftarrow}_i b$ et $a \overrightarrow{\rightarrow}_i b$. Alors, on peut formuler 1°, 2°, 3° comme suit :

1° $a \mid_{\overleftarrow{i}} b \iff a \mid_{\overrightarrow{i}} b$;

2° Pour tous a , $b \in A$, on a $a \mid_i b$ ou $b \mid_i a$;

3° $ab \equiv_i ba$.

Un anneau A est dit un anneau d'hypervaluation (resp. de valuation), s'il existe une hypervaluation (en particulier, une valuation) de A , telle que $i(A) = A$. Autrement dit, pour que A soit un anneau d'hypervaluation, il faut et il suffit que le couple (A , A) satisfasse aux conditions 1°, 2°, du théorème précédent. On dira que A est un anneau d'hypervaluation commutative (à distinguer de l'anneau commutatif d'hypervaluation, notion plus particulière), si l'unique hypervaluation de A , telle que $i(A) = A$, est à valeurs commutatives (mais on ne suppose pas que A lui-même l'est), ce qui a lieu si, et seulement si, (A , A) satisfait à la condition 3°.

THÉORÈME 2. - Un anneau proprement hypervalué A est un anneau d'hypervaluation, si, et seulement si, il est invariant par rapport à sa multiplication. Si A est commutativement hypervalué, il est toujours un anneau d'hypervaluation commutative. En particulier, si A est proprement valué, il est un anneau de valuation, qui coïncide avec la valuation initiale de A, si A n'est pas un corps, et est triviale si A l'est.

Comme tout anneau proprement hypervalué possède un corps-quotient, la caractérisation de tels anneaux parmi les sous-anneaux d'un corps arbitraire K constitue déjà la caractérisation complète des anneaux de cette sorte.

THÉORÈME 3. - Soient K un corps (pas forcément commutatif), K^* son groupe multiplicatif, et

$$C = \{c(a , b) = aba^{-1} b^{-1} ; (a , b) \in K^* \times K^*\}$$

l'ensemble des commutateurs de K^* . Un anneau $i \subseteq K$ est un anneau d'hypervaluation, si, et seulement si :

1° i est invariant dans K ;

2° Pour tout $\alpha \in K^*$, on a $\alpha \in i$ ou $\alpha^{-1} \in i$.

i est un anneau d'hypervaluation commutative, si, et seulement s'il satisfait à la condition 2° et à la condition :

1°' $i \supseteq C$.

i est un anneau de valuation, si, et seulement s'il est un anneau d'hypervaluation tel qu'il n'existe aucun anneau A tel que $i \subset A \subset K$ [donc $i = K$, auquel cas il s'agit d'anneau de valuation triviale, où i est un sous-anneau maximal de K].

Un anneau $A \subseteq K$ est proprement hypervaluable, si, et seulement s'il existe un sous-anneau i de A , qui est un anneau d'hypervaluation.

Conséquence : Si $i \subseteq K$ est un anneau d'hypervaluation, tout sur-anneau de i dans K est hypervaluable, et est un anneau d'hypervaluation, si, et seulement s'il est invariant. Si i est un anneau d'hypervaluation commutative, tout sur-anneau dans K l'est aussi.

A^{-1} désignant l'ensemble des inverses a^{-1} des $a \in A$, et A étant un sur-anneau d'un anneau d'hypervaluation $i \subseteq K$, dans K , $(K..A)^{-1}$ est un idéal premier p_A de i , qui est invariant dans K si, et seulement si, A l'est. Vice-versa, si p est un idéal premier de i , $A_p = K..p^{-1}$ est un sur-anneau de i dans K , qui est invariant dans K si, et seulement si, p l'est. On a $p_{A_p} = p$ et $A_{p_A} = A$, et $p \to A_p$ est une bijection de l'ensemble des idéaux premiers de i sur celui des sur-anneaux de i , qui applique celui des idéaux invariants sur celui des anneaux d'hypervaluation $\subseteq K$ contenant i .

Visiblement, $p \subset p'$ (où p , p' sont deux idéaux premiers de i) implique $A_p \supset A_{p'}$, et vice-versa. p est un idéal de A_p (et pas seulement de i), qui est son idéal maximal (donc tous les éléments de $A_p..p$ sont inversibles dans p). Si p est invariant, A_p est le "localisé" de i par p , autrement dit l'ensemble de tous les $\alpha \in K$ qui sont de la forme ab^{-1} , où a , $b \in i$ et $b \notin p$ [cet ensemble, à cause de l'invariance de p , coïncide avec celui des $\alpha \in K$, qui sont de la forme $b'^{-1} a'$, où a' , $b' \in i$ et $b' \notin p$].

Le complété d'un anneau proprement hypervalué est aussi hypervalué proprement.

4. Groupes totalement ordonnés. Corps hypervalués.

Soit Γ un groupe totalement ordonné, qu'on ne suppose pas commutatif. On définira sur Γ la relation suivante $\succcurlyeq$ de préordre (large) : $\alpha \succcurlyeq \beta$, s'il existe des entiers n , m tels que $\alpha^n \leqslant \beta \leqslant \alpha^m$. La relation d'équivalence $\sim$ de ce préordre sera appelée la comparabilité, et on dira que α est comparable avec β

si $\alpha \sim \beta$. Ceci a donc lieu si, à la fois, il existe $m , n \in Z$ tels que $\alpha^m \leqslant \beta \leqslant \alpha^n$ et $m' , n' \in Z$ tels que $\beta^{m'} \leqslant \alpha \leqslant \beta^{n'}$. On montre que chaque classe de comparabilité C est la réunion de deux intervalles $C_<$ et $C_>$ de Γ au sens de son ordre $<$, qui sont les intersections de C avec

$$\Gamma_< = \{\gamma \in \Gamma \ ; \ \gamma \leqslant 1\} \qquad \text{et} \qquad \Gamma_> = \{\gamma \in \Gamma \ ; \ \gamma \geqslant 1\} \ .$$

$C_>$ est l'intervalle symétrique $C_<^{-1}$ de $C_<$. $C_<$ et $C_>$ sont disjoints, sauf si $C = \{1\}$ est la classe de comparabilité de l'élément neutre 1 de Γ , auquel cas on a $\{1\}_< = \{1\}_> = \{1\}$. Le préordre $\succcurlyeq$ induit un ordre sur l'ensemble $\Gamma/\sim$ des classes de comparabilité dans Γ , qu'on notera encore $\succcurlyeq$ s'il s'agit d'ordre large, et $\succ$ s'il s'agit d'ordre strict. Il en induit un, également, dans $\Gamma_</\sim$ et $\Gamma_>/\sim$, qui sera noté de la même manière sur $\Gamma_>/\sim$, cet ordre coïncide avec celui induit par $>$, tandis que sur $\Gamma_</\sim$ il lui est opposé.

L'ensemble $\Gamma/\sim \setminus \{1\}$, ordonné par l'ordre $\succ$, sera dit la <u>charpente de comparabilité</u> de Γ , et le type ordinal de cet ensemble ordonné sera dit le <u>rang de</u> Γ (2).

On peut définir sur Γ un préordre $\succcurlyeq_{inv}$, moins fin (au sens large) que $\succcurlyeq$, en posant

$\alpha \succcurlyeq_{inv} \beta \iff_{déf}$ il existe des entiers m , n et des éléments γ , δ de Γ tels que $\gamma\alpha^m \gamma^{-1} \leqslant \beta \leqslant \delta\alpha^n \delta^{-1}$.

La relation d'équivalence $\sim_{inv}$ de ce préordre, qui est, visiblement, moins fine (au sens large) que $\sim$, s'appelle la <u>comparabilité invariante</u> (ou <u>normale</u>), et α , β seront dits <u>normalement comparables</u> si $\alpha \sim_{inv} \beta$. Une classe de comparabilité normale est une réunion de classes de comparabilité, qui forment un intervalle de la charpente de comparabilité. Il peut y avoir deux cas : ou bien une classe de comparabilité C est déjà une classe de comparabilité invariante, ce qui a lieu si, et seulement si, C est un sous-ensemble invariant de Γ ; ou bien l'intervalle de $\Gamma/\sim$, que constituent les classes de comparabilité contenues dans une classe de comparabilité invariante, n'a ni premier, ni dernier élément, ce qui implique, en particulier, que cet intervalle est infini. Ainsi, si le rang $r(\Gamma)$ de Γ est fini, toute classe de comparabilité dans Γ est invariante, et $\succcurlyeq_{inv}$, $\sim_{inv}$ coïncident avec $\succcurlyeq$, $\sim$.

L'ensemble $\Gamma/\sim_{inv}$, ordonné par l'ordre induit par $\succcurlyeq_{inv}$ (on le désigne par

---

(2) D'autres notions de rang ont été employées dans la théorie des valuations, par exemple le type ordinal de l'ensemble des sous-groupes isolés (voir plus loin) ; mais elles sont moins adéquates et peuvent en être dérivées.

$>_{inv}$ ou $\geqslant_{inv}$, selon qu'il s'agit d'ordre strict ou large), sera appelé la <u>charpente de comparabilité invariante</u> de Γ , et le type ordinal de cet ensemble sera dit le <u>rang invariant de</u> Γ , et sera noté $r_i(\Gamma)$.

Un automorphisme intérieur $\omega(\gamma)$: $\xi \to \gamma\xi\gamma^{-1}$ est une bijection de Γ , préservant son ordre $>$ et sa comparabilité $\sim$. Il permute les classes de comparabilité de Γ contenues dans une même classe de comparabilité invariante, en conservant leur ordre $>$. Si C_γ est la classe de comparabilité de γ , $\omega(\gamma)$ préserve toute classe de comparabilité $C \in \Gamma/\sim$ telle que $C \geqslant C_\gamma$. Si C' est une classe de comparabilité invariante, et si C est une classe de comparabilité $\subseteq C'$ arbitraire, l'ensemble des classes de comparabilité contenues dans C' est le plus petit intervalle de $\Gamma/\sim$ contenant tous les conjugués $\gamma C\gamma^{-1}$ $(\gamma \in \Gamma)$ de C .

Un sous-groupe $\bar\Gamma$ de Γ est dit <u>isolé</u>, si $\alpha \in \bar\Gamma$ et $\alpha \geqslant \beta$ impliquent $\beta \in \bar\Gamma$. Un sous-ensemble de Γ en est un groupe isolé, si, et seulement s'il est la réunion des classes de comparabilité formant un intervalle commençant de la charpente $\Gamma/\sim$. Il est une réunion de classes de comparabilité invariante (qui forment alors un intervalle commençant de $\Gamma/\sim_{inv}$), si, et seulement s'il est un sous-groupe invariant de Γ . Si $\gamma \notin \bar\Gamma$, les classes à droite $\gamma\bar\Gamma$ et à gauche $\bar\Gamma\gamma$ de γ (mod $\bar\Gamma$) sont des intervalles de Γ , dont tous les éléments sont comparables. Ainsi, l'ordre $>$ de Γ en induit un sur les partitions $\Gamma\nearrow\bar\Gamma$, $\Gamma\swarrow\bar\Gamma$ de Γ en classe à droite (resp. à gauche) (mod $\bar\Gamma$) . En plus, ces partitions, limitées à $\Gamma..\bar\Gamma$, sont plus fines (au sens large) que $\Gamma..\bar\Gamma/\sim$ (et, a fortiori, $\Gamma..\bar\Gamma/\sim_{inv}$), et les classes (à droite, resp. à gauche) mod $\bar\Gamma$ contenues dans $C_<$ ou $C_>$, où C est une classe de comparabilité, ou de comparabilité invariante disjointe avec $\bar\Gamma$, forment un intervalle de $\Gamma\nearrow\bar\Gamma$ (resp. $\Gamma\swarrow\bar\Gamma$). En particulier, si $\bar\Gamma$ est invariant, ces intervalles constituent précisément les classes de comparabilité ou de comparabilité invariante du groupe $\Gamma/\bar\Gamma$, qui est totalement ordonné par l'ordre induit par $>$. On voit que les charpentes de comparabilité et de comparabilité invariante de $\Gamma/\bar\Gamma$ sont semblables aux parties des charpentes correspondantes de Γ formées par les classes (mod $\sim$, resp. $\sim_{inv}$) non contenues dans $\bar\Gamma$, ces parties étant précédées par la classe $\{\bar\Gamma\}$ de l'élément neutre $\bar\Gamma$ de $\Gamma/\bar\Gamma$. Il en résulte que, si $\bar\Gamma$ est un sous-groupe isolé invariant de Γ ,

$$r(\Gamma) = r(\bar\Gamma) + r(\Gamma/\bar\Gamma) \qquad \text{et} \qquad r_i(\Gamma) = r_i(\bar\Gamma) + r_i(\Gamma/\bar\Gamma) \quad .$$

Soit C une classe de comparabilité. Les réunions

$$\Gamma(C) = \bigcup_{\substack{X\in\Gamma/\sim \\ C\geqslant X}} X$$

des classes de comparabilité $X \leqslant C$, et

$$\Gamma^{-}(C) = \bigcup_{\substack{X \in \Gamma/\sim \\ C > X}}$$

de telles classes $X < C$, sont des sous-groupes isolés de Γ . Ces deux groupes sont, ou ne sont pas, invariants en même temps, et ils le sont si, et seulement si, C est invariant. Toutefois, $\Gamma^{-}(C)$ est toujours invariant dans $\Gamma(C)$, et le rang de $\Gamma(C)/\Gamma^{-}(C)$ est 1 .

Il est facile de donner des exemples de groupes totalement ordonnés Γ dont certains sous-groupes isolés $\bar{\Gamma}$ ne sont pas invariants. Par contre, il résulte d'un théorème de Mal'cev ([3]) que tout groupe totalement ordonné est un RN-groupe au sens de Kouroch-Tchernikov. Ainsi, s'il est simple, son rang est 1 , donc il est isomorphe à un sous-groupe du groupe additif des nombres réels, et, par suite, est abélien.

Soit K un corps hypervalué (dont $|..|$ soit l'hypervaluation) tel que $\Delta(K) = \Gamma \cup \{0\}$, soit $\bar{\Gamma}$ un sous-groupe isolé de Γ , et soient

$$(\Gamma..\bar{\Gamma})_{<} = \Gamma_{<}..\bar{\Gamma} \ , \qquad (\Gamma..\bar{\Gamma})_{>} = \Gamma_{>}..\bar{\Gamma} \ .$$

Alors

$$p = p(\bar{\Gamma}) = \{\alpha \in K \ ; \quad |\alpha| \in (\Gamma..\bar{\Gamma})_{<} \cup \{0\}\}$$

est un idéal premier de i , et

$$A(\bar{\Gamma}) = \{\alpha \in K \ ; \quad |\alpha| \notin (\Gamma..\bar{\Gamma})_{>}\}$$

est l'anneau hypervalué correspondant à A_p . Inversement, si p est un idéal premier, et si $\bar{\Gamma} = \bar{\Gamma}(p) = \{|a| \ ; \quad a \notin p \cup p^{-1}\}$, on a $p = p(\bar{\Gamma})$. Ainsi, <u>les idéaux premiers et les sur-anneaux de</u> $i(K)$ <u>dans</u> K <u>forment un ensemble en bijection canonique avec celui des sous-groupes isolés de</u> Γ . Si $\bar{\Gamma}$, $\bar{\Gamma}'$ sont deux sous-groupes isolés de Γ , $\bar{\Gamma} \subset \bar{\Gamma}'$ implique $A(\bar{\Gamma}) \subset A(\bar{\Gamma}')$ [et $p(\bar{\Gamma}) \supset p(\bar{\Gamma}')$]. $A(\bar{\Gamma})$ [et $p(\bar{\Gamma})$] est invariant dans K , autrement dit est un anneau d'hypervaluation, si, et seulement si, $\bar{\Gamma}$ l'est dans Γ . Ainsi, <u>les anneaux d'hypervaluation</u> $A \subseteq K$ <u>contenant</u> $i(K)$ <u>forment un ensemble en bijection canonique avec celui des sous-groupes isolés invariants de</u> Γ .

Soit $\bar{\Gamma}$ un sous-groupe isolé invariant de Γ , et soit $|..|^{\bar{\Gamma}}$ l'hypervaluation de K dont l'anneau d'hypervaluation est $A(\bar{\Gamma})$. On démontre que le groupe de cette hypervaluation (à l'équivalence près) est $\Gamma/\bar{\Gamma}$, ordonné comme plus haut, et on obtient cette hypervaluation en posant $|a|^{\bar{\Gamma}} = |a|\bar{\Gamma}$. D'autre part, si $(\bar{K})^{\bar{\Gamma}}$

([3]) MAL'CEV (A. I.). - Sur les groupes ordonnés [en russe], Izvest. Akad. Nauk SSSR, Serija mat., t. 13, 1949, p. 473-482.

est le corps résiduel $A(\overline{\Gamma})/p(\overline{\Gamma})$ de K par rapport à $|..|^{\overline{\Gamma}}$, dont le zéro est $\overline{0}^{\overline{\Gamma}} = p(\overline{\Gamma})$, on obtient une hypervaluation de ce corps telle que $\Delta((\overline{K})^{\overline{\Gamma}}) = \overline{\Gamma} \cup \{0\}$, qui sera notée $|..|_{\overline{\Gamma}}$, en posant

$$|\overline{0}^{\overline{\Gamma}}|_{\overline{\Gamma}} = |p(\overline{\Gamma})|_{\overline{\Gamma}} = 0 \quad ,$$

$$|a + p(\overline{\Gamma})|_{\overline{\Gamma}} = |a| \ , \qquad \text{si} \quad a \notin p(\overline{\Gamma}) \ .$$

[En effet, $a + p(\overline{\Gamma})$ est un cercle de K hypervalué par $|..|$, et si $a \notin p(\overline{\Gamma})$, on a $0 \notin a + p(\overline{\Gamma})$; par suite, pour tout $b \in a + p(\overline{\Gamma})$, on a $|b| = |a|$, ce qui assure la cohérence de la définition.]

On dira que l'hypervaluation $|..|$ de K *se décompose* en produit $|..|_{\overline{\Gamma}} \times |..|^{\overline{\Gamma}}$ de la valuation $|..|_{\overline{\Gamma}}$ de $(\overline{K})^{\overline{\Gamma}}$ et de la valuation (moins finie) $|..|^{\overline{\Gamma}}$ de K . On dira qu'une hypervaluation $|..|'$ d'un certain corps K' est une *composante* de $|..|$, si l'on peut y arriver à partir de $|..|$ par décompositions successives des composantes déjà obtenues [d'ailleurs, on peut donner à ce mot "successives", soit un sens strictement fini, soit des sens infinitistes (ou "ordinalistes") variés]. Si $C \in \Gamma/\sim$ est invariant, l'hypervaluation $|..|^{C} = (|..|_{\Gamma(C)})^{\Gamma^{-}(C)}$ de $(\overline{K})^{\Gamma(C)}$, qui a, comme groupe d'hypervaluation, le groupe $\Gamma_C = \Gamma(C)/\Gamma^{-}(C)$ de rang 1 (donc équivaut à une valuation), est dite la composante *atomique* de $|..|$, qui correspond à la classe de comparabilité C . La même méthode permet de définir, pour toute classe de comparabilité invariante $C' \in \Gamma/\sim_{inv}$, une composante "*normalement atomique*" $|..|^{C'}$ de $|..|$. Mais, d'autre part, si l'on adopte une interprétation suffisamment infinitiste de la locution "par décompositions successives", on peut définir, grâce au théorème cité de Mal'cev, la composante atomique $|..|^{C}$ de $|..|$ pour toute classe de comparabilité $C \in \Gamma/\sim$. Le rang de cette hypervaluation est 1 , et on peut lui faire correspondre, comme invariant, le sous-groupe $R(C)$ du groupe additif des nombres réels, ce groupe $R(C)$ étant, toutefois, défini à un multiplicateur réel près. Je laisse de côté d'autres invariants qu'on peut attacher à tout $C \in \Gamma/\sim$ (corps résiduels, caractéristiques, squelettes, etc.).

On voit que K est un corps valué (à équivalence d'hypervaluations près), si, et seulement si, $r(\Gamma) = 0$ [auquel cas la valuation de K est triviale] ou $r(\Gamma) = 1$.

5. Extensions hypervaluées. Existence du prolongement des hypervaluations.

k , K étant deux corps hypervalués (dont aucun n'est supposé commutatif), et $|..|$, $\|..\|$ étant leurs hypervaluations respectives, on dit que K est une *extension hypervaluée* de k , ou que le couple (K, k) [qu'on écrit K/k] *est une extension hypervaluée*, si $k \subseteq K$ [donc K/k est une extension de corps], et $|..|$

est la restriction à k de l'hypervaluation $\|\ldots\|$ de K. Si l'on sait déjà que $k \subseteq K$, on exprime le même fait en disant que $\|\ldots\|$ prolonge $|\ldots|$ dans K.

Soient $A(|\ldots|)$, p, $\bar{k}$, $\Gamma(k)$, l'anneau de valuation, l'idéal maximal, le corps résiduel, et le groupe d'hypervaluation de $|\ldots|$, et $A(\|\ldots\|)$, $\mathfrak{P}$, $\bar{K}$, $\Gamma(\bar{K})$, les objets correspondants pour $\|\ldots\|$. Si $k \subseteq K$, la condition nécessaire et suffisante pour que $\|\ldots\|$ prolonge $|\ldots|$ peut se mettre sous une des formes équivalentes :

$$A(\|\ldots\|) \cap k = A(|\ldots|) \ ; \qquad \mathfrak{P} \cap k = p \ ; \qquad \mathfrak{P} \cap A(|\ldots|) = p \ ,$$
$$pA(\|\ldots\|) \cap A(|\ldots|) = p \ .$$

Si $\|\ldots\|$ prolonge $|\ldots|$, $\Gamma(k)$ est un sous-groupe de $\Gamma(K)$, et $\bar{k}$ s'identifie avec un sous-corps de $\bar{K}$ par application canonique

$$\bar{a}_k = a + p \ \rightarrow\ \bar{a}_k + \mathfrak{P} = a + \mathfrak{P} = \bar{a}_K \ .$$

On appelle $\bar{K}/\bar{k}$, l'<u>extension résiduelle</u> de K/k. Elle est, en général, non commutative, donc il y a lieu de distinguer les <u>degrés résiduels</u> $f_g = [\bar{K}:\bar{k}]_g$ <u>à gauche</u> et $f_d = [\bar{K}:\bar{k}]_d$ <u>à droite</u> de K/k. Par contre, on peut parler d'<u>ordre de ramification</u> de K/k tout court, qui est l'indice $e = (\Gamma(K):\Gamma(k))$ de $\Gamma(K)$ par rapport à $\Gamma(k)$. On a $f_g\, e \leqslant n_g = [K:k]_g$ et $f_d\, e \leqslant n_d = [K:k]_d$. Donc, si le degré droit ou gauche de K/k est fini, son ordre de ramification et son degré résiduel du même côté le sont aussi.

Appelons une extension (non commutative) K/k <u>algébrique</u> (à gauche ou à droite), si, pour tout $a \in K$, $k(a)/k$ est de degré fini du même côté. On voit que, si K/k l'est, tout $\gamma \in \Gamma(K)$ est d'ordre fini par rapport à $\Gamma(k)$ [ce qui implique $r(\Gamma(K)) = r(\Gamma(k))$ et $r_i(\Gamma(K)) = r_i(\Gamma(k))$], et $\bar{K}/\bar{k}$ est algébrique du même côté. En particulier, si K/k est algébrique de quelque côté, et $|\ldots|$ est une valuation, toute hypervaluation $\|\ldots\|$ de K prolongeant $|\ldots|$ est de rang $\leqslant 1$, donc, à l'équivalence d'hypervaluation près, une valuation. Et deux valuations équivalentes de K prolongeant une même valuation $|\ldots|$ de k coïncident.

K/k étant une extension, $\|\ldots\|$ une hypervaluation de K, et A un sous-anneau unitaire de k tel que $A \subseteq A(\|\ldots\|)$, on appelle le <u>centre</u> de $\|\ldots\|$ sur A, l'intersection $A \cap \mathfrak{P}$ de A avec l'idéal maximal $\mathfrak{P}$ de $\|\ldots\|$. Désignons par $C(K)$ l'ensemble des commutateurs du groupe multiplicatif K^* de K. Alors, on a :

THÉORÈME 4. - <u>Soient</u> q <u>un idéal unilatère d'un anneau unitaire</u> A <u>de</u> k, <u>et</u> K <u>un sur-corps de</u> k. <u>Alors, il existe une hypervaluation commutative</u> $\|\ldots\|$ <u>de</u> K, <u>telle que</u> $A(\|\ldots\|) \supseteq A$, <u>et que son centre sur</u> A <u>contienne</u> q <u>si, et seulement si,</u> $qA[C(K)] \cap A \neq A$.

Idée de démonstration. - La nécessité de la condition est évidente, car autrement on aurait eu $1 \in A \subseteq qA[C(K)] \subseteq \mathfrak{P}$, ce qui est absurde. Si elle est satisfaite, il suffit de prouver le théorème pour l'anneau $A[C(K)]$ et son idéal $qA[C(K)]$, qui est bilatère (comme, d'ailleurs, tous les idéaux de $A[C(K)] \supset C(K)$). On peut donc supposer que $A \supset C(K)$ et que tous ses idéaux (y compris q) sont, par suite, bilatères. On démontre, ensuite, par application du lemme de Zorn, qu'il existe un élément maximal (donc premier) p de A contenant q , et il suffit de prouver le théorème pour A et p . Par le lemme de Zorn, on prouve qu'il existe un sur-anneau maximal $A' \subseteq K$ de A tel que $pA' \cap A = p$, et le sur-idéal maximal $\mathfrak{P}'$ de p dans A' tel que $\mathfrak{P}' \cap A = p$. On démontre que $\mathfrak{P}'$ est un idéal premier de A' , et que, puisque $A' \supseteq A \supseteq C(K)$, il existe le "localisé" $A'_{\mathfrak{P}'}$ de A' par $\mathfrak{P}'$. Son idéal maximal est $\mathfrak{P}'A'_{\mathfrak{P}'}$, et on a $\mathfrak{P}'A'_{\mathfrak{P}'} \cap A' = \mathfrak{P}'$, ce qui implique $\mathfrak{P}'A'_{\mathfrak{P}'} \cap A = \mathfrak{P}' \cap A = p$, d'où résulte que $A' = A'_{\mathfrak{P}'}$, et tout élément de A' n'appartenant pas à $\mathfrak{P}'$ est inversible. Puisque $A' \supseteq C(K)$, tout produit

$$a_1 \alpha^{i_1} a_2 \alpha^{i_2} \dots a_s \alpha^{i_s} ,$$

où $a_1 , a_2 , \dots , a_s$ appartiennent à A' , $i_1 , i_2 , \dots , i_s$ sont des entiers naturels, et $\alpha \in K$, peut être mis sous la forme

$$a\alpha^{i_1+i_2+\dots+i_s} , \qquad \text{où } a \in A' .$$

Supposons que, ni $\alpha \in K$, $\alpha \neq 0$, ni α^{-1} , n'appartiennent à A' . Alors $pA'[\alpha] \cap A = pA'[\alpha^{-1}] \cap A = A$, et on a $1 \in pA'[\alpha]$ et $1 \in pA'[\alpha^{-1}]$. Il existe donc des représentations

$$1 = a_0 + a_1 \alpha + \dots + a_n \alpha^n ,$$

$$1 = b_0 + b_1 \alpha^{-1} + \dots + b_m \alpha^{-m} .$$

On applique ensuite la méthode bien connue de Chevalley pour obtenir une contradiction, montrant que, ou bien $\alpha \in A'$, ou bien $\alpha^{-1} \in A'$.

Cas particuliers :

(I) $K = k$. - Le théorème devient :

Si q est un idéal unilatère d'un anneau unitaire A de k , il existe une hypervaluation commutative $|..|$ de k , telle que $A(|..|) \supseteq A$ et $p \cap A \supset q$ si, et seulement si, $qA[C(k)] \cap A \neq A$.

(II) $A = A(|..|)$, $q = p$, où $|..|$ est une hypervaluation commutative donnée de k . - Le théorème devient :

Pour qu'une hypervaluation commutative $|..|$ *de* k *soit prolongeable à* $K \supseteq k$, *il faut et il suffit que* $pA(|..|)[C(K)] \cap A(|..|) = p$.

[Cette condition est trivialement vérifiée quand K est commutatif.] On appelle ce cas particulier, le *théorème d'existence* pour les prolongements d'hypervaluations.

(III) $K = k$, $A \supseteq C(k)$ un sous-anneau maximal de k, $q \neq (0)$ un idéal de A [l'existence de tels idéaux unilatères résulte de ce que A n'est pas un corps]. - En vertu du théorème, il existe une hypervaluation $|..|$ de K telle que $A(|..|) \supseteq A$ et $p \cap A \supseteq q$, donc $p \neq \{0\}$. Ainsi, $|..|$ n'est pas la valuation triviale, ce qui implique $A(|..|) \neq k$ et (puisque A est maximal) $A(|..|) = A$. Ainsi :

Tout anneau maximal de k, *qui contient* $C(k)$, *est un anneau d'hypervaluation commutative. Il en résulte qu'un anneau* $A \subseteq k$ *est un anneau de valuation, si, et seulement si, ou bien* $A = k$ *(valuation triviale), ou bien* $A \supseteq C(k)$, *et* $A \subset k$ *est un anneau maximal de* k. *Si* $|..|$ *et* $|...|'$ *sont deux valuations non équivalentes de* K, *et* A, A' *leurs anneaux de valuation, on a* $A \not\subseteq A'$ *et* $A' \not\subseteq A$, *ce qui implique que leurs topologies sont différentes.*

6. Espaces vectoriels sur les corps valués complets. Unicité du prolongement des valuations des corps complets.

Soit k un corps (non nécessairement commutatif) valué complet, et considérons les espaces vectoriels normés V de quelque côté (par exemple à gauche) sur k. Alors, par transposition facile de la démonstration du cas commutatif, on prouve, pour ce cas plus général, le théorème suivant :

THÉORÈME 5. - V *étant un espace vectoriel (à gauche ou à droite) de dimension finie sur un corps valué complet* k, *toutes les normes possibles* $\|..\|$ *de* V [*autrement dit, toutes les valuations* $\|..\|$ *de son groupe additif telles que* $\|\alpha v\| = |\alpha|\ \|v\|$ (*resp.* $\|v\alpha\| = \|v\|\ |\alpha|$) $(\alpha \in k\ ,\ v \in V)$] *induisent sur* V *une même structure uniforme (donc aussi une même topologie), et* V *est un espace ultramétrique complet par rapport à chacune de ces normes.*

Si K/k est une extension (où aucun des corps k, K n'est supposé commutatif), où k est un corps valué complet, et si la dimension gauche ou droite de K/k est finie, K peut être considéré comme un espace vectoriel de dimension finie du même côté, en prenant comme multiplication externe par les $\alpha \in k$ la multiplication dans K. Dès lors, tout prolongement $\|...\|$ à K de la valuation $|..|$ de k est une norme de K, en tant qu'espace vectoriel considéré. Il résulte, du théorème précédent, que deux prolongements de $|..|$ à K sont des valuations équivalentes, donc égales. Finalement, on vient au :

THÉORÈME 6 (*d'unicité*). - *Si* k *est un corps valué complet, et si* K/k *est une extension algébrique de quelque côté, il existe au plus un prolongement* $\|..\|$ *de* $|..|$ *à* k . *Si un tel prolongement existe, toute sous-extension* L/k *de* K/k , *qui est de degré fini du côté considéré, est complète par rapport à* $\|..\|$.

k étant valué complet, soient K , K' deux extensions algébriques (d'un certain côté) valuées de k , et $\varphi : K \to K'$ un isomorphisme de K dans K' . Alors, φ *est une isométrie*. En particulier, *les automorphismes de* K/k , *où* K/k *est une extension valuée unilatéralement algébrique, sont des isométries*. Seule l'absence d'une théorie des extensions et d'une théorie de Galois suffisamment bonnes empêche de tirer de ce "principe d'Ostrovski" le même parti que dans le cas commutatif.

Soient K/k une extension valuée de degré fini n de quelque côté (par exemple à gauche), $(\alpha_1 , \alpha_2 , \ldots , \alpha_n)$ sa base linéaire, et $\hat{K}$ un complété de K . Alors, l'adhérence $\hat{k}$ de k dans $\hat{K}$ en est un complété, et $\hat{k}\alpha_1 + \hat{k}\alpha_2 + \ldots + \hat{k}\alpha_n$ est un corps, à savoir le composé $\hat{k} \vee K$ des sous-corps $\hat{k}$ et K de $\hat{K}$. C'est en plus un $\hat{k}$-espace vectoriel de dimension finie (d'un côté), donc il est complet par rapport à la valuation de $\hat{K}$. Par suite, ce corps coïncide avec $\hat{K}$. *On a* $\hat{K} = K \vee \bar{k}$.

7. Prolongements de valuation dans une extension de degré (unilatéral) fini (travail de F. MOTHON). Exemple de prolongement des valuations.

On connaît la méthode de Hasse pour obtenir, dans le cas commutatif, tous les prolongements possibles de la valuation $|..|$ d'un corps valué (pas forcément complet) k dans une extension de degré fini K de k . Soit K' un sur-corps de K contenant un corps k' k-isomorphe au complété $\hat{k}$ de k , et qui soit composé $(k' \vee K)$ de ses sous-corps k' et K . φ étant un k-isomorphisme de $\hat{k}$ à k' , transportons par φ la valuation de $\hat{k}$ sur k' . Le degré de l'extension K'/k' est fini [car il ne dépasse pas celui de K/k], donc la valuation $|..|'$ de k' (qui prolonge celle de k) se prolonge, et d'une seule manière, à K' , et ce prolongement induit sur $K \subset K'$ une valuation, qui prolonge celle de k , $|..|$. Vice-versa, si $\|..\|$ est un prolongement de valuation $|..|$ de k à K , et si $\hat{K}$ est le complété de K par rapport à $\|...\|$, l'adhérence $\hat{k}$ de k par rapport à $\|..\|$, valuée par la valuation que $\|...\|$ y induit, est un complété de k , et on a $\hat{K} = \hat{k} \vee K$. Par suite, le degré $[\hat{K}:\hat{k}] \leqslant [K:k]$ de $\hat{K}/\hat{k}$ est fini, et la valuation de $\hat{K}$ (qui induit $\|...\|$ dans K) est l'unique prolongement de celle de $\hat{k}$. Ainsi, tous les prolongements de $|..|$ s'obtiennent de cette manière à partir des corps K' , qui sont k-isomorphes à quelque $\hat{k} \vee K$. Or, tous les corps K'

de cette forme sont des images $\hat{k}$-homomorphes du produit tensoriel $\hat{L} = \hat{k} \bigotimes_k K$, considéré comme une $\hat{k}$-algèbre, le noyau étant un idéal maximal de $\hat{L}$, deux images à noyaux différents donnant des prolongements différents de $|..|$ dans K . Comme $\hat{L}/\hat{k}$ est une algèbre commutative de rang fini (donc anneau artinien), on a la décomposition primaire unique

$$\hat{L} = A_1 \oplus A_2 \oplus \dots \oplus A_s \quad .$$

Si R_i est le radical de A_i , et $R = R_1 \oplus R_2 \oplus \dots \oplus R_s$ celui de $\hat{L}$, les idéaux maximaux possibles sont les

$$N_i = A_i \oplus \dots \oplus A_{i-1} \oplus R_i \oplus A_{i+1} \oplus \dots \oplus A_s \qquad \text{et} \qquad K_i = \hat{L}/N_i \simeq A_i/R_i \quad ,$$

où $\hat{k}$ et K s'insèrent, d'une certaine manière canonique, dans K_i , qui est leur composé. On a aussi

$$\hat{L}/R \simeq A_1/R_1 \oplus A_2/R_2 \oplus \dots \oplus A_s/R_s = K_1 \oplus K_2 \oplus \dots \oplus K_s \quad .$$

Ainsi, les prolongements de $|..|$ dans K sont en correspondance biunivoque avec les composantes primaires de $\hat{L}$.

Il est tentant de généraliser cette méthode au cas non commutatif, et cela a constitué le but (partiellement atteint) de la thèse de 3e cycle "Prolongements des valuations dans le non commutatif" de mon élève François MOTHON, qui a été soutenue en juin 1970. Mais cette tentative rencontre plusieurs difficultés ou complications qui n'existent pas dans le cas commutatif. Ainsi :

1° Dans le cas non commutatif, il n'est pas, en général, possible, par des méthodes algébriques, de munir $\hat{L}$ de structure de $\hat{k}$-algèbre, mais seulement de celles, soit de $\hat{k}$-module à gauche, soit de $\hat{k}$-module à droite [toutefois, cette difficulté n'existe pas si k est contenu dans le centre de K].

2° Supposant que, par quelque moyen, $\hat{L}$ soit muni de structure d'anneau artinien, il n'admet pas, en général, de décomposition primaire.

3° Si, sous la même hypothèse, R est le radical de $\hat{L}$, $\hat{L}/R$ admet bien une décomposition $\bar{A}_1 \oplus \bar{A}_2 \oplus \dots \oplus \bar{A}_s$ en composantes simples, mais, en général, ces composantes ne sont pas toutes des corps.

4° Si une composante simple $\bar{A}_i$ de $\hat{L}/R$ est un corps, elle peut bien être considérée canoniquement comme extension finie unilatérale de $\hat{k}$, mais la valuation $|..|$ de k peut ne pas y être prolongeable.

F. MOTHON a surmonté la première difficulté (qui est la seule essentielle), sous certaines hypothèses de continuité concernant la multiplication des éléments de k par un élément de K , et est parvenu à définir sur $\hat{L}$, par un procédé topologique, la structure adéquate d'un sur-anneau de $\hat{k}$ quand cette condition est vérifiée.

Quant aux 2°, 3°, 4°, ce ne sont que des complications techniques, et, une fois la difficulté 1° surmontée, F. MOTHON n'a pas eu trop de difficulté à donner la solution du problème tenant compte de ces complications.

Supposons donc, par exemple, que $n = [K:k]_g$ est fini, et soit $(e_1, e_2, \dots, e_n)$ une base de K considéré comme k-espace vectoriel à gauche. $\hat{L} = \hat{k} \bigotimes_k K$ est un $\hat{k}$-espace vectoriel à gauche ayant la même base, et, puisque $\hat{k}$ est complet, toutes les normes $\|..\|$ de cet espace vectoriel y induisent une même structure uniforme U (et une même topologie T), et L est complet par rapport à cette structure uniforme. Considérons sur $K \subset L$ sa topologie $T(K)$ induite par T. Munissons, d'autre part, k de la topologie de sa valuation, et considérons, pour tout $a \in K$, l'application

$$\varphi_a : \xi \to a\xi$$

de k dans K. Alors, l'<u>hypothèse de Mothon</u> est la condition suivante :

<u>Pour tout</u> $a \in K$, φ_a <u>est une application continue de</u> k <u>dans</u> K.

En réalité, cette condition est déjà satisfaite pour tout $a \in K$, si elle l'est pour les éléments $e_1, e_2, \dots, e_n$ d'une seule base linéaire gauche quelconque de K/k.

Sous son hypothèse, MOTHON définit, d'abord, pour tout $\hat{a} = \sum_i \hat{\lambda}_i e_i$ $(\lambda_i \in \hat{k})$, le produit $\hat{a}\hat{\lambda}$ de $\hat{a}$ par $\hat{\lambda} \in \hat{k}$, en posant $\hat{a}\hat{\lambda} = \sum_i \hat{\lambda}_i (e_i \hat{\lambda})$, et en définissant $e_i \hat{\lambda}$ comme limite (au sens de T) des $e_i \lambda_n$, où les λ_n appartiennent à k, et $\lambda_n \to \hat{\lambda}$. On a donc $e_i \hat{\lambda} = \sum \alpha_{i,j}(\hat{\lambda}) e_j$; on pose, si $b = \sum_i \hat{\mu}_i e_i$,

$$ab = \sum_i \hat{\lambda}_i \sum_j (e_i \hat{\mu}_j) e_j = \sum_i \sum_j (\hat{\lambda}_i \alpha_{i,j}(\hat{\mu}_j))(e_i e_j) .$$

Ensuite, on effectue le premier produit dans $\hat{k}$ et le second produit dans K, ce qui donne la définition cherchée du produit. On vérifie aisément que $\hat{L}$ est artinien.

Une fois $\hat{L}$ défini, MOTHON montre que tous les prolongements de $|..|$ dans K proviennent, de la même manière que dans le cas commutatif, des corps K' qui sont des images homomorphes de $\hat{L}$. Ainsi, si

$$\hat{L}/R = \bar{A}_1 \oplus \bar{A}_2 \oplus \dots \oplus \bar{A}_s$$

est la décomposition de $\hat{L}/R$ en composantes simples, les composantes $\bar{A}_i$, qui ne sont pas les corps, ne donnent aucun prolongement de $|..|$ dans K. Si $\bar{A}_i$ est un corps, il est canoniquement une extension de degré fini à gauche de $\hat{k}$, et il fournit un prolongement de $|..|$ dans K si, et seulement si, la valuation $|..|$

de $\hat{k}$ est prolongeable à $\bar{A}_i$. Or, si C_i est l'ensemble des commutateurs du groupe multiplicatif de $\bar{A}_i$, et si $\hat{i} = i(\hat{k})$ est l'anneau d'intégrité de $\hat{k}$, et $\hat{p}$ l'idéal maximal de $\hat{i}$, ceci a lieu si, et seulement si, $\hat{p}\hat{i}[C_i] \cap \hat{i} = \hat{p}$. Les $\bar{A}_i$, pour lesquels cette condition est satisfaite, fournissent les prolongements $|..|_i$ de $|..|$ à K , en prolongeant (de la seule manière possible) la valuation de $\hat{k}$ à $\bar{A}_i$, et en prenant la valuation induite par celle de $\bar{A}_i$ dans $K \subseteq \bar{A}_i$, et on obtient ainsi tous les prolongements de $|..|$ à K .

Exemple : Soit K une k-algèbre normale de division de degré fini. Alors, si $|..|$ est une valuation de k , et si $\hat{k}$ est le complété de k par rapport à $|..|$, $\hat{L} = \hat{k} \otimes_k K$ est une $\hat{k}$-algèbre simple normale, c'est-à-dire l'algèbre complète des matrices de degré $m \geqslant 1$ sur un corps (commutatif ou pas). Si $m > 1$, $|..|$ n'est pas prolongeable dans K . Si $m = 1$, $\hat{L}$ est un corps, et un théorème d'Artin montre que la valuation de $\hat{k}$ se prolonge à $\hat{L}$. Donc $|..|$ ne se prolonge pas à K ou s'y prolonge d'une seule manière, selon que $\hat{L}$ n'est pas ou est un corps. On peut montrer que $\hat{L}$ est un corps seulement pour un nombre fini de valuations $|..|$ de k .

Montrons-le pour les algèbres cycliques normales de division, en supposant que k est un corps de nombres algébriques. Ces algèbres sont décrites par les symboles $A = [Z/k , \sigma , \alpha]$, où Z/k est une extension cyclique d'un certain degré m , σ un générateur de son groupe de Galois $G_{Z/k}$, et $\alpha \in k$. Cette algèbre a la forme

$$A = Z + Z\sigma + Z\sigma^2 + \dots + Z\sigma^{m-1} ,$$

avec les relations

$$\sigma a = a^\sigma \sigma , \qquad \text{où } \sigma = \{a \to a^\sigma ;\ a \in Z\} ,$$

$$\sigma^m = \alpha .$$

Si $N_{Z/k}$ désigne le groupe des normes $N_{Z/k}(a)$ dans Z/k des $a \in Z$ non nuls, A est un corps si, et seulement si, l'ordre de α par rapport au groupe multiplicatif $N_{Z/k}$ est m .

On peut montrer que $\hat{L} = \hat{k} \otimes_k K$ est un corps, si, et seulement si, le symbole de Hasse

$$\left(\frac{Z/k , \alpha}{p(|..|)}\right) ,$$

où $p(|..|)$ est le centre de $|..|$ sur l'anneau des entiers algébriques de k , est un générateur de $G_{Z/k}$. Or, si $p(|..|)$ ne divise pas le discriminant $D_{Z/k}$ de Z/k , et n'entre pas, ni au numérateur, ni au dénominateur, de l'idéal (fractionnaire) principal (α) de k , on a

$$\left(\frac{Z/k\ ;\ \alpha}{p(|..|)}\right) = 1 \quad .$$

Ainsi, seulement pour un nombre fini de places $|..|$, on a $\left(\frac{Z/k\ ;\ \alpha}{p(|..|)}\right) \neq 1$, et, a fortiori, $\left(\frac{Z/k\ ;\ \alpha}{p(|..|)}\right)$ engendre $G_{Z/k}$.

(Texte reçu en décembre 1970)

Marc KRASNER
1 rue Ernest Gouin
75 - PARIS 17