Faculté des Sciences de Paris

Séminaire A. Châtelet et P. Dubreil (Algèbre et Théorie des nombres) Année 1947-1948

Exposé n° 1

Espace ultramétrique et valuation

Marc Krasner

1. Espace topologique (Rappel de définitions)

On dit habituellement qu'un ensemble E est muni d'une structure topologique, ou est un espace topologique, lorsqu'on a défini une transformation des parties de E, qui, à une partie (quelconque) X fait correspondre une partie $\overline{X}$ appelée sa fermeture, telle que :

$$X \subset \overline{X} \; ; \; \overline{\overline{X}} = \overline{X} \; ; \; = \; ; \; (\overline{X \cup Y}) = (\overline{X} \cup \overline{Y}) \; .$$

Dans un espace topologique, une partie est fermée, si elle est égale à sa fermeture. Toute intersection et toute réunion de parties fermées est fermée.

L'intérieur $\overset{\circ}{X}$ d'une partie X est la partie complémentaire de la fermeture de la complémentaire :

$$E - \overset{\circ}{X} = (\overline{E - X});$$

tout élément de l'intérieur est un point intérieur de la partie X.

Une partie est ouverte, si sa partie complémentaire est fermée, autrement dit si elle est égale à son interieur.

La dérivée d'une partie X peut être définie par la condition :

$$x' \in X' \iff x' \in \overline{X \cap (E - \{x'\})}.$$

C'est l'ensemble des éléments x', tels que chacun appartient à la fermeture de l'intersection de X avec la complémentaire de la partie constituée par le seul élément x'.

Une partie X de E est voisinage d'un point a de E, lorsque a est point interieur de X $(a \in \overset{\circ}{X})$.

La famille $V(a)$ des voisinages de a possède les propriétés suivantes ([1], chapitre 1, paragraphe 1)

1° Toute partie de E qui contient un ensemble, élément de la famille $V(a)$ est un élément de $V(a)$;

(d'après les notes prises par J. Riguet, pendant la conférence)
Référence : http://www.numdam.org/item?id=SD$_1$947 − 1948$_{_1{}_A1_0}$.
Transcription : Denise Vella-Chemla, 27.4.2022.

2º Toute intersection finie d'ensembles de $V(a)$ appartient à $V(a)$;

3º a appartient à tout ensemble de $V(a)$;

4º Pour tout ensemble U de $V(a)$, il existe un ensemble U' tel que, quel que soit l'élément x de U', V soit de la famille $V(x)$.

Un sous-ensemble $S(a)$ de $V(a)$ est appelé système fondamental de voisinage de a, si $V(a)$ est identique à l'ensemble des parties qui contiennent un élément de $S(a)$ ([1], chapitre 1, paragraphe 5).

Un point x appartient à l'ensemble dérivé X' de la partie X, si et seulement si tout voisinage de x a, en commun avec X, un elément différent de x.

Il existe d'autres définitions d'un espace topologique, constituées par un ordre différent des notions. On peut notamment partir des concepts :

- de voisinage (défini par les conditions 1 à 4) ;
- de dérivation [2]
- d'ensemble ouvert ou fermé ([1], chapitre 1, paragraphe 1).

Qualités des espaces topologiques. Un espace topologique est connexe s'il n'est pas réunion de deux parties fermées, non vides, disjointes.

Il est compact au sens de Bourbaki si tout recouvrement ouvert de E (formé d'ensembles ouverts) contient un recouvrement fini ([1], chapitre 1, paragraphe 10).

Il est compact an sens de Fréchet si, quelle que soit une partie infinie, sa dérivée n'est pas vide.

2. Espace métrique.

Un ensemble E est appelé un espace métrique lorsque, à tout couple (a, b) d'éléments de E (élément du produit $E \times E$), on sait faire correspondre un nombre réel $d(a, b)$, appelé distance de a, b, tel que :

$$d(a,b) = 0 \iff a = b \; ; \qquad d(a,c) \leq d(a,b) + d(c,b).$$

Il résulte de ces conditions que :

$$d(a,b) \geq 0 \; ; \qquad d(a,b) = d(b,a).$$

Il suffit de remplacer dans la deuxième condition c par b, ou b par a.

Pour éviter une confusion de langage qui peut se produire dans le cas des espaces ultramétriques, M. Krasner propose d'adopter les dénominations suivantes pour, x_0 étant un élément fixe et r un nombre réel positif (ou nul), les lieux des points (ou ensemble des éléments) x :

- $d(x_0, x) = r$: sphère ;

- $d(x_0, x) \leq r$: boule de première espèce (au lieu de fermé)
- $d(x_0, x) < r$: boule de deuxième espèce (au lieu d'ouvert)

Dans un espace métrique, on obtient une structure topologique en convenant que les boules (de l'une ou l'autre espèce) de centre x_0, et dont les rayons sont les inverses des entiers (positifs), constituent un système fondamental de voisinage de x_0.

3. Espace ultramétrique.

Un ensemble E est appelé espace ultramétrique, lorsqu'on peut y définir une distance (de tout couple d'éléments a, b), vérifiant les conditions (plus restrictives) :

$$d(a,b) = 0 \iff a = b \ , \qquad d(a,c) \leq \max\,(d(a,b), d(c,b)).$$

Il en résulte comme pour les précédentes :

$$d(a,b) \geq 0 \ ; \qquad d(a,b) = d(b,a).$$

Elles entraînent par suite les conditions précédentes, puisque, pour tout couple de nombres réels, positifs, α, β :

$$\max\,(\alpha, \beta) \leq \alpha + \beta.$$

Un espace ultramétrique est donc, a fortiori, métrique et peut être pourvu d'une structure topologique.

Tout triangle est isocèle : l'un des sommets est également distant des deux autres, qui sont de distance au plus égale à la distance commune.

On peut toujours numéroter 3 éléments i, j, k de façon que :

$$d(a_i, a_j) = d(a_i, a_k) \geq d(a_j, a_k).$$

Il suffit en effet de numéroter les éléments, de façon que :

$$d(a_j, a_k) \leq d(a_k, a_i) \leq d(a_i, a_j) \ ;$$

il en résulte :

$$d(a_i, a_j) \leq \max\,(d(a_j, a_k)\ ,\ d(a_i, a_k)) = d(a_i, a_k) \ ;$$

d'où l'égalité et l'inégalité annoncées.

Dans un espace métrique linéaire, ou pour un triangle aplati, le plus grand côté est égal à la somme de deux autres :

$$d(ab) \geq d(ac) \geq d(bc) \implies d(ab) = d(ac) + d(bc) \ .$$

Il en résulte que si un espace métrique linéaire est ultramétrique, il est nécessairement réduit à 2 points : car le plus petit côté de tout triangle ne peut être que nul.

Au lieu de boules, M. Krasner emploie cette fois les termes :

- $d(x_0, x) = r$: circonférence de centre x_0, de rayon r ;
- $d(x_0, x) \leq r$: cercle circonférencié ;
- $d(x_0, x) < r$: cercle non circonférencié[1].

Tout point d'un cercle (circonférencié ou non) peut être considéré comme centre.

- $d(a, b) < r$ et $d(a, x) < r \implies d(b, x) < r$;
- $d(a, b) \leq r$ et $d(a, x) \leq r \implies d(b, x) < r$ [2].

Ces proprietés étant symétriques en a et b, résultant de l'implication :

$$d(a, b) < r \text{ et } d(a, x) < r \implies d(b, x) \leq \max\left(d(a, b), d(a, x)\right) < r$$

et de celle obtenue en remplaçant les $<$ par $\leq$.

Deux cercles (circonférenciés ou non) ou bien sont disjoints, ou bien sont concentriques et l'un contient l'autre (l'inclusion résultant de la comparaison des rayons).

Tout cercle est une partie de l'espace E, à la fois ouverte et fermée.

Un cercle C est une partie ouverte, tout point x de C lui est intérieur, car le cercle de centre x et de rayon inférieur à r , rayon de C, est contenu dans C.

La partie complémentaire de C est aussi ouverte : si y est dans $E - C$, le cercle c de centre y et de rayon r' inférieur à r est dans $E - C$. Car si y' est un point de c, il en résulte les inégalités :

$$d(y, y') < r\ ,\ d(x, y) > r\ ,\ (\text{ou} \geq r)\ ;$$

le triangle xyy' étant isocèle, le 3$^{\text{ème}}$ côté $d(x, y')$ est égal à $d(x, y)$, donc est plus grand que r (ou au moins égal à r).

Toute circonférence $S(a, r)$, de rayon r, est réunion de cercles $C(x, r^-)$, (non circonférenciés), de rayon r^-

$$\left\{ \begin{array}{ll} & x \in S(a, r) \\ \text{et} & \\ & x' \in C(x, r^-) \end{array} \right\} \iff \left\{ \begin{array}{l} d(a, x) = r \\ \\ d(x, x') < r) \end{array} \right\} \implies d(a, x') = r.$$

car a, x, x' forment un triangle nécessairement isocèle, dont $d(x, x')$ est le plus petit côté.

Note. r^-, appelé nombre semi réel, peut être considéré comme l'ensemble des nombres inférieurs à r, de sorte que :

$$x \leq r^- \iff x < r.$$

[1] $d(x, x)$ au lieu de $d(x_0, x)$ dans l'article original ?

[2] Le dernier $<$ ne devrait-il pas être un $\leq$?

4. Diviseurs d'un espace ultramétrique.

Dans un espace ultramétrique E, une relation d'équivalence (mod P), ou (P) (ou de congruence) est appelée diviseur de E, lorsque :

$$\begin{array}{cc} & a \equiv a' \ (\text{mod } P) \\ \text{et} & \\ & d(x, x') \leq d(a, a') \end{array} \implies x \equiv x' \ (\text{mod } 1).$$

Une telle relation est équivalente à une répartition de E en classes C_a (ou $C(a)$) d'éléments (congrus entre eux), formant un ensemble quotient $E|(P)$:

$$x \in C_a \iff x \equiv a \ (\text{mod } P), \quad C_a \in E|(P).$$

Les classes sont des cercles (disjoints) de même rayon φ,

$$\varphi = r^- \ \ (C \ \text{ non circonférencié}) \ , \ \text{ou } r \ \ (C \text{ circonférencié}).$$

Ce rayon φ est l'ensemble des nombres réels au plus égaux aux nombres $d(x, x')$ pour tous couples $x \equiv x' \ (P)$.

φ, désigné par P, est appelé la valuation de P.

$\omega(P) = -\log \varphi$ est l'ordre de P.

Un diviseur P_1 est diviseur d'un diviseur P_2 lorsque :

$$(x \equiv x' \ (P_2)) \implies (x \equiv x' \ (P_1)) \ ;$$

ce qui est équivalent à :

$$\text{classe } C_a \text{ de } E/(P_2) \ \subset \ \text{classe } C'_a \text{ de } E/(P_1), \ \text{ou } |P_1| \geq |P_2|.$$

On peut définir, à la manière habituelle le p.g.c.d. et le p.p.c.m. d'un système de diviseurs.

La distance de points de deux classes (disjointes) est constante :

$$\begin{array}{cc} & a' \equiv a \\ \text{et} & \\ & b' \equiv b \end{array} \ (\text{mod } P) \implies d(a', b') = d(a, b).$$

Dans le triangle a, a', b, les côtés $d(a, b), d(a', b)$ supérieurs à $d(a, a')$ sont égaux, et de même pour $d(a, b), d(a, b')$.

On peut convenir de définir la distance des classes C_a, C_b :

$$d(C_a, C_b) \begin{cases} = d(a, b), & \text{si } C_a \neq C_b, \quad \text{ou } d(a, b) > \varphi \\ = 0, & \text{si } C_a = C_b, \quad \text{ou } d(a, b) \leq \varphi \end{cases}$$

Cette distance des classes, ainsi précisée, définit sur $E/(P)$, une structure d'espace ultramétrique, dont la topologie est discrète.

Deux distances $d_1(a,b), d_2(a,b)$, définissant dans un ensemble E des structures d'espaces ultramétriques, sont appelées équivalentes lorsque les diviseurs définis par d_1 et par d_2 sont les mêmes.

Pour cela, il faut et il suffit que d_2 soit fonction monotone croissante de d_1 et que $d_1(a,b)$ tende vers 0, lorsque $d_2(a,b)$ tend vers 0.

5. Complétion d'un espace ultramétrique.

On connait diverses méthodes pour compléter un espace métrique (Fréchet, Bourbaki,...) On peut former des suites de cercles emboîtés, dont les rayons tendent vers 0^+ (infiniment petits et non nuls). Deux suites sont équivalentes, si, à partir d'un certain rang, tout cercle de l'une est contenu dans un cercle de l'autre. Un élément de l'espace complété est caractérisé par une suite de cercles, définie à une équivalence près.

Cette méthode est applicable à un espace ultramétrique. Si l'on se fixe, a priori, la suite des rayons φ_i, deux suites équivalentes sont alors identiques (composées des mêmes cercles C_i).

Au lieu des rayons φ_i, on peut se donner une suite de diviseurs (P_i de valuation φ_i), les cercles de la suite sont des classes, suivant les diviseurs P_i, emboîtées les unes dans les autres. Le complété de l'espace est ainsi l'ensemble correspondant des suites de classes emboîtées.

La distance de deux éléments différents de l'espace complété est égale à la distance $d(C_i, C'_j)$ de deux cercles quelconques, mais disjoints, pris dans chacune des suites qui définissent les éléments.

Le complété d'un espace ultramétrique est encore un espace ultramétrique ; on peut notamment lui appliquer la propriété de l'uniforme continuité :

Si V est un voisinage d'un point a, d'un espace ultramétrique E non complet, $f(x)$ étant une fonction définie et uniformément continue sur V ; on peut prolonger $f(x)$ sur le complété V' de V. Il suffit, pour cela, si y est un point de V' défini par une suite x_i, de poser $f(y) = \lim f(x_i)$, pour i infini.

6. Module normé ou valué.

Un module (ensemble où est défini une addition de signe +) est normé (ou valué) si à tout élément a,on fait correspondre un nombre réel positif $|a|$ tel que :

$$\begin{array}{lll} & |a| = 0 \iff a = 0, \qquad |a| = |-a| \ ; & \\ & |a+b| \leq |a| + |b| \ ; & \text{normé} \\ \text{ou} & & \\ & |a+b| \leq \max\,(|a|, |b|) \ ; & \text{valué.} \end{array}$$

$|x|$ est la norme (ou la valuation) de x (dans le module) et :

$$\begin{aligned}&\omega(x) = -\mathrm{Log}\,|x| \ \text{ est l'ordre de } x;\\ &\pi(a,b) = \omega(b-a) \ \text{ est la proximité de } a \text{ et } b\,.\end{aligned}$$

Dans un module normé (ou valué) on peut définir une distance de structure métrique (ou ultramétrique), en posant :

$$d(a,b) = |b-a|\ .$$

Réciproquement si, dans un module, il existe une distance métrique (ou ultramétrique) telle que :

$$d(a+x,b+x) = d(a,b) \qquad \text{(pour tout } x\text{)},$$

le module est normé (ou valué) par l'égalité :

$$|a| = d(a,0) = d(a+x,x).$$

M. Krasner dit qu'un tel module est Bg-métrique (ou Bg-ultramétrique, abréviation d'espace de Banach généralisé).

Dans un module valué, P etant un diviseur, la classe nulle (mod P), (ou le cercle $C(0,\varphi)$, de centre 0 et de rayon φ = valuation de P), est un sous-module.

$$\begin{array}{c}x \equiv 0\\ \text{et} \qquad\qquad\qquad (\mathrm{mod}\ P)\\ x' \equiv 0\end{array} \iff \left\{\begin{array}{l}|x| = d(x,0) \le \varphi\\ \\ |x'| = d(x',0) \le \varphi\end{array}\right.$$
$$\implies |x-x'| \le \max\,(|x|,|x'|) \le \varphi \iff |x-x'| \equiv 0 \ (\mathrm{mod}\ P).$$

Les classes (mod P) sont les classes suivant le sous-module :

$$x \in C_a \iff x \equiv a\ (P) \iff x-a \in C(0,\varphi).$$

7. Somme de cercles.

1º La somme d'un point a' avec tous les points d'un cercle $C(a,\varphi)$ est le cercle $C(a+a',\varphi)$.

$$\begin{aligned}&(\exists y : y \in C(a,\varphi) \text{ et } (x = y+a')\\ &\quad\iff (|y-a| \le \varphi \text{ et } x = y+a') \iff (|x-(a+a')| \le \varphi).\end{aligned}$$

2º Les sommes des points de deux cercles $C(a,\varphi)$ et $C(a',\varphi')$ forment le cercle (somme des cercles) :

$$C(a+a',\max\,(\varphi,\varphi')).$$

D'une part :

$$\begin{aligned}&(|u-a| \le \varphi, |u'-a'| \le \varphi' \text{ et } x = u+u')\\ &\qquad\implies |x-(a+a')| = |(u-a)-(u'-a')| \le \max\,(|u-a|,|u'-a'|).\end{aligned}$$

Réciproquement, supposons $\varphi = \max\,(\varphi,\varphi')$:

$$|x-(a+a')| \le \varphi \implies (\exists x, u', |u-a| \le \varphi' \le \varphi,\ \text{et } u = x-u')$$

ce qui entraîne aussi :

$$|u-a| = |(x-(a+a'))-(u'-a')| \leq \max\,(x-(a+a')|, |u'-a'|) \max\,(\varphi,\varphi') = \varphi.$$

8. Corps valué.

Un corps R est valué, ou normé, s'il l'est en tant que module et si, en outre la valuation (ou la norme) vérifie la propriété (de multiplication) :

$$|a|.|b| = |a.b|.$$

Il en résulte :

$$|\pm 1| = 1, |a^n| = |a|^n \qquad (n \text{ entier positif, négatif ou nul}).$$

Dans le cas ultramétrique :

$$|n| \leq 1 \qquad (n \text{ somme de } n \text{ unités du corps}).$$

Dans un corps valué (ultramétrique), l'ordre $\omega(x) = -\mathrm{Log}\ x$ est une application du corps dans l'ensemble des nombres réels, vérifiant les conditions :

$$\begin{array}{l}\omega(xy) = \omega(x)+\omega(y), (\omega(x) = +\infty) \iff (x=0),\\ \omega(x+y) \geq \min(\omega(x),\omega(y))\end{array}$$

Réciproquement s'il existe une telle application, le corps est valué par la valuation :

$$x = \exp(-\omega(x)).$$

L'ensemble des $\omega(x)$ constitue un module M, appelé module de valuation.

1° Si M est un ensemble dense (dans l'ensemble des nombres réels) R est à valuation dense,

2° Si M est un ensemble discret, c'est un groupe cyclique (infini) :

$$\omega_i = \alpha_0 + ia \qquad (i \text{ entier}).$$

Tout cercle est, à la fois circonférencié de rayon r_i, et non circonférencié de rayon r_{i+1}^- Les cercles de même centre, sont rangés par rayons en progression géométrique décroissant.

9. Produit de cercles.

1° Les produits d'un point a' par tous les points d'un cercle $C(a,\varphi)$ forment le cercle $C(aa',a'\varphi)$.

$$(\exists y : y \in C(a,\varphi) \text{ et } x = ya') \iff (|y-a| \leq \varphi \text{ et } x = ya') \iff |x-aa'| = |a'||y-a] \leq |a'|\varphi$$

On peut considérer que ce produit est une similitude, par extension du sens géométrique de ce terme.

2º Les produits des points de deux cercles $C(a, \varphi), C(a', \varphi')$ forment le cercle :

$$C(aa', \max\,(\varphi|m'|, \varphi'|m|))\ ;$$

$|m|$ et $|m'|$ étant les maxima respectifs des valuations des points des cercles.

Le cercle produit est ainsi, suivant les cas :

- extérieur aux cercles : $C(aa', \max\,(\varphi(|a'|), \varphi'(|a|))$;
- intérieur à $C(a, \varphi)$: $C(aa', \varphi|a'|)$;
  extérieur à $C(a', \varphi')$: idem
- extérieur aux cercles : $C(aa', \varphi\varphi')$.

D'une part :

$$(|u-a| \leq \varphi \text{ et } |u'-a'| \leq \varphi' \text{ et } x = uu') \implies |x - aa'| = |(u-a)u' + (u'-a')a|$$
$$\leq \max\,(|u-a|.|u'|, |u'-a'|.|a|) \leq \max\,(\varphi|m'|, \varphi'|m|).$$

Réciproquement, supposons $\varphi|m'| = \max\,(\varphi|m'|, \varphi'|m|)$:

$$|x - aa'| \leq \varphi|m'| \implies (\exists x, u' : |u'-a'| \leq \varphi' \text{ et } x = uu')\ ;$$

ce qui entraîne aussi :

$$|u-a|.|u'| = |(x-aa') - (u'-a')a| \leq \max\,(\varphi|m'|, \varphi'|m|) = \varphi|m'|\ ;$$

donc :

$$|u-a|.|m'| \leq \varphi|m'| \quad \text{et} \quad |u-a| \leq \varphi.$$

Par ailleurs dans un cercle $C(a, \varphi)$ ne contenant pas 0, la valuation u d'un point est constante et notamment égale à $|a|$, car, dans le triangle $0, a, u$, le côté $d(au)$ est le plus petit et les autres sont égaux : $|a| = d(a, 0) = d(u, 0) = |u|$.

Si d'autre part 0 appartient à un cercle, il en est le centre, la valuation des points u varie et son maximum $|m|$ est égal à φ.

10. Idéaux d'un corps valué.

Dans un corps valué, on peut définir, d'une façon générale, des entiers et des diviseurs de 1 (ou unités) :
a est entier, si $|a| \leq 1$;
e est diviseur de 1, si $|e| = 1$ (e et e^{-1} sont entiers).

L'ensemble des unités forme un anneau d'intégrité I, constitué par le cercle de centre 0 et de rayon 1 :

$$(a \neq 0 \text{ et } |a| \leq 1, a' \neq 0 \text{ et } |a'| \leq 1) \implies |aa'| \leq 1.$$

Les diviseurs de 1[3], qui constituent un groupe multiplicatif, forment la circonférence de ce cercle.

On peut appeler idéal du corps R (relativement eu domaine d'intégrité I), tout sous-module A de R, qui reste invariant dans la multiplication par tout élément de I :

$$A \subset R, \quad A \text{ module}, \quad A.I \subset A.$$

L'ensemble réduit à l'élément 0 et le corps R lui-même sont des idéaux triviaux.

Les idéaux d'un corps valué R, relativement au domaine d'intégrité I, coïncident avec ses diviseurs, ou avec les cercles $C(0, \varphi)$ (circonférenciés ou non).

D'une part un cercle $C(0, \varphi)$ est un module :

$$|x| \leq \varphi \quad \text{et} \quad |y| \leq \varphi \implies |x+y| \leq \max\left(|x|, |y|\right) \leq \varphi$$

en outre :

$$x \in C(0, \varphi) \quad \text{et} \quad i \in I \iff |x| \leq \varphi \;\text{ et }\; |i| \leq 1 \implies |xi| \leq \varphi \iff xi \in C(0, \varphi).$$

Réciproquement tout idéal A est un cercle, car si φ est la borne supérieure des valuations $|x|$ des éléments de A (ce qui peut être un nombre semi-réel) ; d'une part $x \in A \implies |x| \leq \varphi$; d'autre part

$$|y| \leq \varphi \implies \exists x, x \in A \;\text{ et }\; |y| = |x| \implies y = xi \;\text{ et }\; i \in I \implies y \in A.$$

Les produits des éléments de deux idéaux forment un idéal dont la valuation (du diviseur) est le produit des valuations :

$$x \in C(0, \varphi) \;\text{ et }\; x' \in C(0, \varphi') \iff x \in C(0, \varphi\varphi').$$

C'est un cas particulier de la propriété du produit de deux cercles.

11. Idéal premier.

Un idéal est entier s'il est contenu dans le domaine d'intégrité I. Ce domaine est lui-même un idéal entier (trivial) contenant tous les autres.

Un idéal entier est premier, s'il ne peut contenir un produit qu'en contenant au moins l'un des facteurs (les classes suivant cet idéal, qui forment un anneau, ne contiennent pas de diviseur de 0)

$$xy \in P \implies x \in P \;\text{ ou }\; y \in P.$$

Dans un corps valué, il y a un et un seul idéal premier P, constitué par le cercle de centre 0 et de rayon 1^- (contenant tous les entiers non diviseurs de 1).

Ce cercle est un idéal premier car :

$$xy \in P \iff |xy| < 1 \implies |x| < 1 \;\text{ ou }\; |y| < 1.$$

[3]Les diviseurs de I ?

Tout autre idéal A entier n'est pas premier (supposé différent de I) car il existe au moins un élément p contenu dans P et non dans A. On peut toujours. trouver un exposant n (entier positif) tel que :

$$|p^{n-1}| > \text{ valuation de } A, \quad |p^n| \leq \text{ valuation de } A,$$

A contenant le produit $p.p^{n-1}$ sans contenir aucun des facteurs n'est pas premier.

Suivant l'idéal premier P le domaine E (des entiers) est réparti en classes qui constituent un corps quotient.

Ces classes, en plus de P lui-même, sont (en raison des propriétés d'addition des cercles) des cercles (disjoints), de rayon 1^-, dont le centre est l'un quelconque de leurs points et dont tous les points sont de valuation $|x| = 1$.

En effet :

$$x + P = x + C(0, 1^-) = C(x, 1^-).$$

On peut vérifier directement que ces cercles forment un corps (contenant la somme, la différence, le produit et le quotient).

12. Idéaux de première espèce.

Un idéal est de première espèce, s'il est défini par un cercle ciraonférencié ($|x| \leq r$ (réel)).

Les idéaux de première espèce forment un groupe isomorphe du groupe de leurs valuations.

Car si r et r' sont les rayons réels de deux cercles :

$$C(0, r) \times C(0, r') = C(0, rr');$$

en outre l'inverse du cercle de rayon r est le cercle de rayon r^{-1}.

Un idéal de première espèce est principal, ou encore est constitué par l'ensemble des multiples (produits par des entiers) d'un de ses éléments convenablement choisi.

Dans $C(0, r)$, il existe au moins un élément α, de valuation r ; alors :

$$x \in C(0, r) \implies x = \alpha i \ \ |i| \leq 1 \ \text{ ou } \ i \in I.$$

Dans un corps de valuation discrète, il n'y a que des idéaux de première espèce, tout cercle pouvant être considéré comue circonférencié.

13. Exemple d'espace ultramétrique.

Nombres p-males. On adopte un nombre premier p et on considère l'ensemble des nombres p-males, c'est-à-dire les fractions dont le dénominateur est une puissance de p (y compris les entiers et notamment 0). C'est manifestement un domaine d'intégrité. On peut mettre chacun de ses nombres sous la forme (unique) :

$$a = p^{\omega(a)}.a' \quad (a' \text{ premier avec } p, \omega(a) \text{ entier quelconque}).$$

Il peut être mis de plusieurs façons sous forme d'une somme :

$$a = \sum_i u_i p^i \quad (u_i \text{ entiers}, i \geq \omega(a))$$

cette somme est égale à une seule forme canonique :

$$a = \sum a_i p^i \quad (0 \leq a_i < p)\ ;$$

c'est l'écriture du nombre dans le système p-male.

Dans le système, considéré comme module, on peut prendre pour ordre d'un élément a l'exposant $\omega(a)$ de la puissance de p qui est en facteur, et pour valuation une exponentielle de cet exposant, changé de signe, par exemple $p^{-\omega(a)} = |a|$. (L'ordre de 0 serait $-\infty$ et sa valeur absolue $= 0$).

On vérifie aisément :

$$\omega(a+b) \geq \min\,(\omega(a), \omega(b)), |a+b| \leq \max\,(|a|, |b|).$$

Dans le calcul de la somme de nombres mis sous forme de sommes, il ne peut s'introduire de puissances de p, d'exposants inférieurs au plus petit des deux, si certaines des puissances peuvent disparaître.

L'ensemble des ordres (module de valuation) est discret, c'est l'ensemble des entiers.

Dans l'ensemble considéré comme espace la distance de deux points est la valuation de leur différence : $d(a, b) = a - b$; de sorte que :

$$d(a, b) \leq \max\,(d(a, c), d(b, c)).$$

Cercles. Le cercle de centre $a = p^{\omega(a)}.a'$ et de rayon p^{-r} est l'ensemble des points x tels que :

$$x = a + p^r.x', \quad x'\text{entier}.$$

Il est manifeste que, dans cette définition, on peut remplacer le centre par tout point $a + p^r.x_0$, c'est-à-dire par tout point du cercle qui en est un centre. En particulier si $\omega(a) \geq r$, l'origine 0 est dans le cercle :

$$0 = p^{\omega(a)}.a' - p^r(p^{\omega(a)-r}.a')$$

elle en est un centre et le cercle est l'ensemble des points x tels que

$$\omega(x) \geq r \quad \text{ou} \quad |x| \leq p^{-r}.$$

La circonférence (du cercle) est l'ensemble des points pour lesquels x' est premier avec p. Elle est formée évidemment par la réunion des ensembles de points :

$$(a + p^r.a') + p^{r+1}x'' \quad (a' \text{ premier avec } p, \quad x''\text{quelconque})$$

c'est une réunion de cercles de rayons $p^{-(r+1)}$ inférieurs au rayon p^{-r}.

Si deux cercles $a+p^r.x, b+p^s.y$, ont un point c, commun, on peut les écrire $c+p^r.x, c+p^s.y$; l'un est inclus dans l'autre.

La partie (de l'espace) complémentaire d'un cercle de centre a et de rayon p^r est l'ensemble des points x tels que $x-a$ ne soit pas multiple de p^r ; elle contient évidemment tout cercle $x+p^r.x'$ (de centre x); c'est une partie ouverte.

Les sommes des points de deux cercles $(a,p^r),(b,p^{-s})$ est :

$$a+p^r.x+b+p^s.y=(a+b)+p^{\min\,(r,s)}.z$$

c'est le cercle de centre $(a+b)$ et de rayon max (p^{-r},p^{-s}).

Valuation dans l'anneau. Dans l'ensemble considéré comme domaine d'intégrité, la valuation vérifie la condition multiplicative

$$\omega(ab)=\omega(a)+\omega(b), \qquad |ab|=|a|.|b|.$$

Pour préciser l'ensemble des produits des points de deux cercles, il convient de préciser les valuations de leurs centres :

$$a=p^{\omega(a)}.a'\ ,\quad b=p^{\omega(b)}.b'\ ,\quad a',b' \text{ premiers avec } p$$

les produits des points sont :

$$ab+p^{\omega(a)+s}.(a'y)+p^{\omega(b)+r}.(b'x)+p^{r+s}.xy\ ,$$

ils forment un cercle de centre ab et de rayon $p^{-\min(\text{exposants})}$ ce qui donne les 3 cas :

- intérieur aux cercles : $r\leq\omega(a), s\leq\omega(b), p^{-(r+s)}$
- intérieur au cercle a : $r\leq(\omega(a),\omega(b)<s, p^{-(\omega(b)+r)}$
  extérieur au cercle b : idem
- extérieur aux cercles : $\omega(a)<r,\omega(b)<s, p^{-\min(\varphi(a)+s,\omega(b)+r)}$

Corps des quotients. Le domaine d'intégrité définit un corps de quotients :

$$a:b=p^{\omega(a)-\omega(b)}.(a':b') \qquad (a',b' \text{ premiers avec } P)$$

Ce n'est autre que l'ensemble des nombres rationnels, mais considéré, plus spécialement, au point de vue de la puissance de chaque nombre. p qui est en facteur dans chaque nombre.

On peut encore écrire chaque elément sous forme d'une somme :

$$a\ :\ b=\sum u_i.p^i \qquad (i \text{ depuis } \omega(a)-\omega(b))$$

somme finie si $(a\ :\ b)$ est dans le domaine précédent, infinie dans le cas contraire. L'égalité doit être comprise au sens d'une congruence suivant toute puissance de p (d'exposant positif).

$$(a\ :\ b)-\sum u_i\ ,\quad p^i\equiv 0 \pmod{p^n} \qquad (i \text{ de } i_0 \text{ à } n-1,\ \text{les } u_i \text{ entiers limites}).$$

Il existe encore une seule forme canonique :

$$\sum a_i.p^i \qquad (0 \leq a_i < p)\ .$$

Le calcul des coefficients a_i peut se faire par récurrence sur n. Si :

$$(a\ :\ b) - \sum a_i.p^i = p^n.(a'\ :\ b') \begin{cases} b' \text{ premier avec } p \\ i \text{ de } i_0 \text{ à } n-1 \end{cases}$$

le coefficient a_{n+1} (peut-être nul) est défini par :

$$(a'\ :\ b') - a_n \equiv 0\ (p) \quad \text{ou} \quad a' = b'a_n \pmod{p}$$

Il est facile de vérifier que le développement est périodique. Si :

$$a\ :\ b = p^{\omega(a\,:\,b)}.(a'\ :\ b') \qquad (a', b' \text{ premiers avec } p)$$

d'après le théorème de Fermat :

$$p^m - 1 \equiv 0 \bmod b'\ , \qquad m = \varphi(b')\ ;$$

d'où :

$$(a'\ :\ b') - (a'\ :\ b').p^m = N \quad (N \text{entier})$$

Il en résultera :

$$(a'\ :\ b') = N + N.p^m + N.p^{2m} + \ldots + N.p^{(k-1)m}\ (p^m)$$

Le deuxième membre est périodique et il le restera après avoir été mis sous forme canonique.

Dans le corps ainsi considéré, les entiers sont les fractions dont le dénominateur (après éventuellement reduction) ne contient pas de puissance de p (est premier à p). Ils forment un domaine d'intégrité qui est le cercle de centre 0 et de rayon 1.

Les unités (de valuation 1) sont les fractions dont les deux termes sont premiers à p ; leurs inverses sont encore des unités. Elles forment un groupe (multiplicatif) qui est la circonférence du cercle précédent.

Un idéal est l'ensemble des "multiples" (par les entiers) d'une puissance p^r ; c'est un cercle de centre 0 et de rayon p^{-r}. Les idéaux triviaux sont 0 et l'anneau A des entiers (cercle de rayon 1). Les idéaux entiers sont donnés par les puissances de p d'exposants positifs. L'idéal est l'ensemble des multiples de p (cercle de rayon p^{-1}).

Complétion. Pour compléter le corps ainsi défini, on peut y considérer des sommes :

$$\alpha = \sum u_i p^i \quad (i \text{ depuis } i_0\ ;\ u_i \text{ entiers limités})$$

ou, plus exactement la suite des sommes S_n des n premiers termes ; une telle suite vérifie la condition de Cauchy car

$$|S_{n+i} - S_{n+j}| < p^{-n} \qquad (i,\ j \text{ positifs})$$

elle définit par suite un élément du corps complété (qui est la “limite” de cette suite).

L’égalité de deux éléments est définie par :

$$\sum u_i p^i - \sum u'_i p^i \equiv 0 \pmod{p^n} \qquad \text{(pour tout } n > 0)$$

C’est encore dire qu’une somme est égale à une seule forme canonique :

$$\alpha = \sum a_i p^i \quad (i \text{ depuis } \omega(\alpha), 0 \leq a_i < p) \ .$$

L’ordre $\omega(\alpha)$ est l’exposant de p dans le premier terme de la suite.

Bibliographie

[1] Bourbaki (Nicolas). Topologie générale, Chapitres 1 et 2, 2e éd., Hermann, Paris, 1951 (Act. scient. et ind., 858-1142; Éléments de Mathématique, 2).

[2] Stoilow (S.). Leçons sur les principes topologiques de la théorie des fonctions analytiques., Paris, Gauthier-Villars, 1938.