NOMBRES p-ADIQUES

SERGE CANTAT

Attention, cette introduction aux nombres p-adiques a été rédigée bien rapidement, pour compléter un cours inachevé en période coronavirienne. N'hésitez pas à m'envoyer mes remarques et corrections par email.

Les deux références principales utilisées sont le livre de Neal Koblitz et celui d'Alain Robert,

- Neal Koblitz, *p-adic numbers, p-adic analysis, and Zeta functions*, Springer Verlag, Graduate Texts in Mathematics 58.
- Alain Robert, *A course in p-adic analysis*, Springer Verlag, Graduate Texts in Mathematics 198.

ainsi qu'un article de Bjorn Poonen (London Math. Society).

1. VALEUR ABSOLUE p-ADIQUE

1.1. Soit K un corps. Une **valeur absolue** sur K (à valeurs réelles) est une application $|\cdot|: K \to \mathbf{R}_+$ telle que

(a) $|xy| = |x||y|$ pour toute paire $(x,y) \in K^2$;
(b) $|x+y| \leq |x| + |y|$ pour toute paire $(x,y) \in K^2$;
(c) $|x| = 0$ si et seulement si $x = 0$.

Par exemple, la valeur absolue usuelle, qui sera notée $|\cdot|_\infty$, sur $\mathbf{Q}$ ou sur son complété $\mathbf{R}$, ou encore le module d'un nombre complexe, sont des valeurs absolues. Une valeur absolue est dite **ultramétrique**, ou **non-archimédienne** si l'inégalité triangulaire (b) peut être remplacée par l'inégalité plus forte suivante:

(b') $|x+y| \leq \max(|x|,|y|)$ pour toute paire $(x,y) \in K^2$.

Exercice 1.1. Montrer que $|-1|^2 = |1| = 1$.

La donnée d'une valeur absolue sur K munit K d'une distance et donc d'une topologie.

Date: 2020.

1.2. Soit $\mathcal{P} \subset \mathbf{N}$ l'ensemble des nombres premiers. Soit p un élément de $\mathcal{P}$.

Soit a un nombre rationnel non nul; écrivons $a = p^r a'$ avec $a' \wedge p = 1$, i.e. $a' = m/n$ et p n'apparait pas dans la décomposition en facteurs premiers de m et n. L'entier r est la **valuation p-adique** de a. On définit la **norme**, ou **valeur absolue**, p-adique de a par

$$|a|_p = p^{-r}. \tag{1.1}$$

Lorsque $a = 0$ on pose $|a|_p = 0$.

Théorème 1.2. *La valeur absolue p-adique est une valeur absolue ultramétrique; l'ensemble de ses valeurs $|\mathbf{Q}|_p$ est $p^{\mathbf{Z}} \cup \{0\}$. Ces valeurs absolues vérifient, avec la valeur absolue usuelle $|\cdot|_\infty$ la* **formule du produit***:*

$$\prod_{p \in \mathcal{P} \cup \{\infty\}} |a|_p = 1.$$

La démonstration est facile, le point principal étant de montrer que $|\cdot|_p$ est ultramétrique. Pour cela, on se donne deux nombres rationnels x et y de valuations respectives r et s; on suppose $r \leq s$ et l'on écrit $x = p^r m/n$, $y = p^s u/v$ où m, n, u, et v sont des entiers premiers à p. Alors

$$p^r \frac{m}{n} + p^s \frac{u}{v} = p^r \frac{mv + p^{s-r} un}{mv}$$

où l'on a mis en facteur la puissance de p la plus petite (i.e. $r \leq s$). Donc $|x+y|_p \leq \max(|x|_p + |y|_p)$ avec égalité dès que $r < s$: l'inégalité est stricte si et seulement si p divise $mv + p^{s-r}un$, si et seulement si $r = s$ et p divise $mv + un$.

La formule du produit correspond à la décomposition de tout nombre entier en produit de nombres premiers. □

Exemple 1.3. Si l'on prend $p = 3$, $x = 21$, $y = 12$, alors $|x|_p = 1/3$, $|y|_p = 1/3$, $|x+y|_p = |33|_p = 1/3$ et $|x-y|_p = 1/9$.

2. $\mathbf{Q}_p$ ET $\mathbf{Z}_p$

2.1. $\mathbf{Q}_p$ = complétion de $\mathbf{Q}$ par les suites de Cauchy (deux suites sont équivalentes si elles ont la même limite). C'est un corps muni d'une valeur absolue $|\cdot|_p$ ultramétrique qui étend celle de $\mathbf{Q}$; les opérations de corps $+$ et $\times$ sont continues pour la topologie induite. Le corps $\mathbf{Q}$ s'injecte dans $\mathbf{Q}_p$ et y est dense. On note $\mathbf{Z}_p$ l'adhérence de $\mathbf{Z}$ dans $\mathbf{Q}_p$; c'est un sous-anneau de $\mathbf{Q}_p$.

2.2. La distance entre deux entiers a et b de $\mathbf{Z}$ est $\leq p^{-k}$ si et seulement si $a \equiv b \mod (p^k)$.

Lemme 2.1. *Si q est un nombre entier (positif ou négatif) premier à p alors $1/q$ est une limite de nombres entiers positifs dans $\mathbf{Q}_p$.*

Démonstration. $q \wedge p = 1$ entraine $q \wedge p^k = 1$ pour tout $k \geq 1$ entraine l'existence de c_k entier positif $\leq p^k - 1$ tel que $c_k q \equiv 1 \mod p^k$). La suite c_k est une suite de Cauchy car $|c_k - c_\ell| \leq p^{-k}$ si $k \leq \ell$, donc converge vers un nombre p-adique qui est l'inverse de q. □

Par conséquent, -1 est dans l'adhérence de $\mathbf{Z}_+$ dans $\mathbf{Q}_p$. Ainsi, $\mathbf{Z}_p$, *l'adhérence de* $\mathbf{Z}$ *dans* $\mathbf{Q}_p$, *est aussi l'adhérence de* $\mathbf{Z}_+$.

Chaque entier positif a peut-être écrit de manière unique sous la forme $a_0 + a_1 p + a_2 p^2 + \ldots + a_p^k + \ldots$ où $a_i \in \{0, 1, \ldots, p-1\}$ pour tout i (et seul un nombre fini des a_i sont non nuls). C'est l'écriture de Teichmüller de a. Alors $|a-b|_p \leq p^{-k}$ si et seulement si $a_j = b_j$ pour tout $0 \leq j \leq k-1$. Les sommes partielles $\sum_{j=0}^{k-1} a_j p^j$ donnent les résidus de a modulo p^k: cette somme est l'unique entier compris entre 0 et $p^k - 1$ qui est égal à a modulo p^k.

Les séries de la forme $\sum_{j \geq 0} m_j p^j$ avec $m_j \in \mathbf{Z}$ convergent dans $\mathbf{Q}_p$. Elles sont toutes limites d'entiers. Les séries $\sum_{j \geq 0} m_j p^j$ avec $a_i \in \{0, 1, \ldots, p-1\}$ sont limites d'entiers positifs ; la valeur limite détermine les a_i, et réciproquement.

Théorème 2.2. *L'adhérence $\mathbf{Z}_p$ de $\mathbf{Z}$ dans $\mathbf{Q}_p$ vérifie les propriétés suivantes.*

(1) *$\mathbf{Z}_p$ est un sous-anneau de $\mathbf{Q}_p$. Il coïncide avec le disque unité (fermé)*

$$\{z \in \mathbf{Q}_p \ ; \ |z|_p \leq 1\}.$$

Le disque de rayon p^ℓ est égal à $p^{-\ell}\mathbf{Z}_p$.

(2) *Tout élément x de $\mathbf{Z}_p$ est égal à une unique somme de Teichmüller $\sum_j x_j p^j$ (avec $x_j \in \{0, \ldots, p-1\}$), finie ou infinie, et est la limite d'une unique suite de Cauchy $(y_k)_{k \geq 0}$ satisfaisant $y_k \in \{0, \ldots, p^{k+1} - 1\}$ et $y_{k+1} = y_k \mod p^{k+1}$) pour tout $k \geq 0$. Ces deux suites se correspondent par $y_k = \sum_{j=0}^{k} x_j p^j$.*

(3) *Cette écriture fournit des homéomorphismes entre $\mathbf{Z}_p$, $\{0, \ldots, p-1\}^{\mathbf{N}}$, et la limite projective des $\mathbf{Z}/p^k\mathbf{Z}$. Ce sont des isomorphismes d'anneaux (une fois transportée les opérations sur les sommes de Teichmüller).*

(4) *$\mathbf{Z}_p$ est un espace métrique compact homéomorphe à l'ensemble de Cantor.*

(5) *L'anneau $\mathbf{Z}_p$ est principal: tout idéal est de la forme $p^\ell \mathbf{Z}_p$ pour un $\ell \geq 0$; il contient un unique idéal maximal, à savoir*

$$\mathbf{Z}_p^o = \{x \in \mathbf{Z}_p \; ; \; |x|_p < 1\} = \{x \in \mathbf{Z}_p \; ; \; |x|_p \leq p^{-1}\}.$$

C'est un sous-ensemble ouvert et fermé de $\mathbf{Q}_p$.

(6) *Le quotient $\mathbf{Z}_p/\mathbf{Z}_p^o$ est le* **corps résiduel** $\mathbf{Z}/p\mathbf{Z}$*. Il y a p boules de rayon $1/p$ dans $\mathbf{Z}_p$, elles sont paramétrées par les résidus modulo p (i.e. les éléments de $\mathbf{Z}/p\mathbf{Z}$).*

Démonstration. Il faut voir qu'un nombre p-adique de norme ≤ 1 est dans $\mathbf{Z}_p$. Comme le groupe des valeurs est discret, c'est une limite de nombres rationnels de norme ≤ 1, et par le lemme c'est une limite d'entiers positifs.

Le disque de rayon p^ℓ est l'image du disque de rayon 1 par $z \mapsto p^{-\ell}\mathbf{Z}_p$.

Si $I \subset \mathbf{Z}_p$ est un sous-ensemble, le supremum des $|y|_p$ pour y dans I est un maximum, atteint par au moins un $y_0 \in I$, car l'ensemble des normes possibles est $p^{-\mathbf{N}}$; en particulier, $I \subset p^\ell \mathbf{Z}_p$ où $p^{-\ell} = |y_0|_p$. Si I est un idéal, alors $\mathbf{Z}_p \times y_0 \subset I$, mais $\mathbf{Z}_p y_0 = p^\ell \mathbf{Z}_p$ et donc $I = p^\ell \mathbf{Z}_p$. □

Exercice 2.3.

A.– Se familiariser avec les opérations sur les séries de Teichmüller. Par exemple, avec $p = 5$, calculer la somme et le produit des nombres $a = 2 + 3 \times 5$ et $b = 2 + 4 \times 5 + 3 \times 5^2$ en écrivant le résultat sous forme de Teichmüller.

B.– Montrer que $1/(1-p) = \sum p^j$ et que $-1 = \sum (p-1)p^j$

2.3. Géométrie élémentaire. Les boules sont fermées et ouvertes. Deux boules sont disjointes ou emboitées. Tout point d'une boule est un centre.

La boule unité fermée contient p boules de rayon $1/p$ deux-à-deux disjointes, qui chacune contient p boules de rayon $1/p^2$, etc.

Exercice 2.4. Comprendre comment les relations d'inclusion entre ces boules forment un arbre donc les sommets correspondent à des résidus modulo p^m.

3. CORPS VALUÉS, NORMES APPROXIMATIVES, EXTENSIONS DE CORPS

Dans cette partie, nous expliquons comment trouver toutes les valeurs absolues sur $\mathbf{Q}$, et comment les étendre à sa clôture algébrique.

3.1. Corps valués: autres exemples. Nous avons déjà vu les exemples de $\mathbf{Q}$ avec les valeurs absolues $|\cdot|_p$, pour $p \in \mathcal{P} \cup \{\infty\}$.

Exemple 3.1. Soit $A = \mathbf{k}[t]$ l'anneau des polynômes à coefficients dans un corps $\mathbf{k}$; soit $K = \mathbf{k}(t)$ son corps des fractions. Si $P = \sum_{j\geq 0} a_j t^j$ appartient à A, on note $\mathrm{ord}(P)$ l'ordre d'annulation de P en 0, défini comme le plus petit indice $m \geq 0$ tel que a_m soit non nul. Ainsi $\mathrm{ord}(x^4 - 3x^2) = 2$ si la caractéristique de $\mathbf{k}$ n'est pas 3. Alors $|P| = \exp(-\mathrm{ord}(P))$ est une valuation ultramétrique; la complétion de A correspond aux séries formelles à coefficients dans $\mathbf{k}$; la complétion de K aux séries de Laurent.

Exemple 3.2. Considérons la fonction $P \in \mathbf{k}[t] \mapsto |P|$ définie par

$$|P| = \exp(\deg(P)). \tag{3.1}$$

Par exemple, $|x^3 - x + 1| = \exp(-3)$. Alors on a $|PQ| = |P||Q|$ et

$$\deg(P+Q) \leq \max(\deg(P), \deg(Q)) \tag{3.2}$$

donc $|P+Q| \leq \max(|P|, |Q|)$. C'est la même valeur absolue que dans l'exemple précédent, mais pour le point à l'infini (car $P(1/x) = x^{-d}Q(x)$ où l'ordre d'annulation de Q en 0 est nul).

3.2. Normes approximatives, caractérisation des normes.

Lemme 3.3. *Deux valeurs absolues (i) sont équivalentes (l'une puissance de l'autre) ssi (ii) elles définissent la même topologie ssi (iii) elles définissent la même boule unité (ouverte ou fermée).*

Exemple 3.4. $|\cdot|_\infty^2$ n'est pas une valeur absolue mais $|\cdot|_\infty^{1/2}$ en est une. Toute puissance d'une valeur absolue ultramétrique est une valeur absolue.

Démonstration. Si $|\cdot|_2 = |\cdot|_1^\alpha$ alors les boules sont les mêmes, donc on a (ii)

Avec (ii) on a les mêmes boules unité ouvertes car celles-ci correspondent aux points x pour lesquels x^n tend vers 0 lorsque n tend vers $+\infty$; les ensembles $\{|x|_j \geq 1\}$ coïncident donc aussi (passage au complémentaire) ainsi que les ensembles $\{|x|_j > 1\}$ (passage à $1/x$). On a donc aussi la même sphère unité et les mêmes boules unités fermées. Ainsi (ii) implique (iii).

Supposons (iii). Si les valeurs absolues ne sont pas triviales, on peut trouver x avec $|x|_1 > 1$; on prend $\alpha > 0$ tel que $|x|_2 = |x|_1^\alpha$. Alors pour $y \in K$ on regarde les rationnels $r = m/n$ tels que $|y|_j^r < |x|_j$; les deux intervalles de $\mathbf{Q}$ ainsi définis coïncident car il s'agit d'écrire $|y|_j^m < |x|_j^n$ i.e. $|y^m/x^n|_j < 1$. On en déduit $|y|_2 = |y|_1^\alpha$, donc (i). □

Lemme 3.5. *Soit $|\cdot|$ une valeur absolue sur un corps K. Les propriétés suivantes sont équivalentes*

(a) $|n| \leq 1$ *pour tout* $n \in \mathbf{N}$ *;*
(b) $|\mathbf{N}|$ *est un ensemble borné ;*
(c) $|1+x| \leq 1$ *dès que* $|x| \leq 1$ *;*
(d) $|\cdot|$ *est ultramétrique ;*
(e) *la boule unité fermée est un sous-anneau.*

Ainsi, toute valeur absolue sur un corps de caractéristique > 0 *est ultramétrique.*

Démonstration. Supposons (b) vérifié. Alors

$$|1+x|^m \leq \sum_{k=0}^{m} |C_m^k||x|^k \leq B\sum_k |x| \leq (m+1)B \tag{3.3}$$

donc en prenant les racines m-èmes on obtient (c). Puis (c) entraine (d), qui entraine (e) qui entraine (a) car 1 est dans la boule unité. □

Théorème 3.6 (Ostrowski, I)**.** *Soit* $|\cdot|$ *une valeur absolue non triviale de* $\mathbf{Q}$*. Si elle est ultramétrique, elle est équivalente à une valeur absolue p-adique.*

Démonstration. Il existe un entier n de norme < 1, car sinon la valeur absolue est triviale. La multiplicativité montre que le plus petit entier avec cette propriété est un premier p. Le théorème de Bézout montre que la boule unité ouverte est constituée des multiples de p. On conclut grace au Lemme 3.3. □

Une fonction $f\colon K \to \mathbf{R}_+$ qui vérifie

(a) $f(x) = 0$ si et seulement si $x = 0$,
(b) $f(xy) = f(x)f(y)$,
(c) $f(x+y) \leq C\max(f(x), f(y))$ pour une constante uniforme C,

est appelé **norme approximative** (ou valeur absolue approximative).

Exemple 3.7. Une valeur absolue ultramétrique est une norme approximative. Si f est une norme approximative et $\alpha > 0$, alors f^α aussi. Si $|\cdot|$ est une valeur absolue c'est une norme approximative (prendre $C = 2$); donc $|\cdot|^\alpha$ est une norme approximative pour tout $\alpha > 0$.

Lemme 3.8. *Si* f *est une norme approximative avec* $C = 2$*, c'est une valeur absolue.*

Avant de démontrer ce lemme, itérons l'inégalité (c) : $f(x_1 + \cdots + x_4) \leq C^2\max(f(x_i))$, et plus généralement $f(x_1 + \cdots + x_{2^r}) \leq C^r\max(f(x_i))$. Si n

n'est pas une puissance de 2 on complète en ajoutant des zéros et on obtient

$$\begin{aligned} f(x_1+\cdots+x_n) &\leq C^{\log_2(n)+1}\max(f(x_i)) = (2n)^{\alpha}\max(f(x_i)) && (3.4)\\ &\leq (2n)^{\alpha}\sum_{i=1}^{n} f(x_i) && (3.5)\end{aligned}$$

où $C=2^{\alpha}$. En particulier $f(n)\leq(2n)^{\alpha}$.

En écrivant $f((a+b)^n)=f(\sum_j C_n^j a^j b^{n-j})$ on obtient

$$\begin{aligned} f((a+b)^n) &\leq 2^{\alpha}(n+1)^{\alpha}\sum_{j=0}^{n} f(C_n^j)f(a)^j f(b)^{n-j} && (3.6)\\ &\leq 4^{\alpha}(n+1)^{\alpha}\sum_{j=0}^{n} (C_n^j)^{\alpha} f(a)^j f(b)^{n-j} && (3.7)\end{aligned}$$

Démonstration du lemme 3.8. Comme $C=2$ on a $\alpha=1$ et

$$f((a+b)^n)\leq 4(n+1)(f(a)+f(b))^n. \tag{3.8}$$

On prend des racines n-èmes pour conclure. □

Lemme 3.9. *Si f est une norme approximative bornée sur les entiers positifs, c'est une valeur absolue ultramétrique.*

Démonstration. On a $f((1+x)^n)\leq(2(n+1))^{\alpha}\sum_{j=1}^{n} Bf(x)^j$ où B est une constante. Donc $f(1+x)\leq 1$ si $f(x)\leq 1$; ainsi $f(x+y)\leq\max(f(x),f(y))$ donc f est une valeur absolue ultramétrique. □

Théorème 3.10 (Ostrowski, II)**.** *Toute valeur absolue (approximative) non triviale sur le corps* $\mathbf{Q}$ *est équivalente à une des valeurs absolues $|\cdot|_p$ avec $p=\infty$ ou p premier.*

Démonstration. Montrons que

$$f(m)^{1/\log(m)}\leq\max\left(1,\ f(n)^{1/\log(n)}\right) \tag{3.9}$$

pour tout $n\geq 2$ et pour tout $m\geq 1$. Pour cela on écrit $m=\sum_{i=0}^{r} m_i n^i$ avec indice majoré par $r\leq\log(m)/\log(n)$. On pose $A(f;n)=\max\{f(q)\ ;\ 0\leq q\leq n-1\}$. Alors

$$\begin{aligned} f(m) &\leq (C)^{r+1}A(f;n)\max(1,f(n)^r) && (3.10)\\ &\leq C^{1+\log(m)/\log(n)}A(f;n)\max(1,f(n)^{\log(m)/\log(n)}). && (3.11)\end{aligned}$$

On change m en m^k et on prend les racines.[1]

[1] On pourrait aussi utiliser $\leq(2r)^{\alpha}A(f;n)\max(1,f(n)^r)$ avec une majoration $r\leq\log_2(m)/\log_2(n)$.

S'il existe un entier $n \neq 0$ avec $f(n) < 1$ alors $f(m) \leq 1$ pour tout entier ≥ 1, donc le lemme précédent montre que f est une valeur absolue ultramétrique et l'on conclut avec le premier théorème d'Ostrowski.

Si $f(n) > 1$ pour tout $n \geq 2$, l'inégalité (3.9) fournit $f(m)^{1/\log(m)} = f(n)^{1/\log(n)}$ par symétrie, ceci pour tous les entiers m et $n \geq 2$. Posant $f(2) = 2^{\beta}$, nous obtenons $f(m) = m^{\beta}$ pour tout $m \geq 2$, et donc $f(m) = m^{\beta}$ pour tout m car $f(-1) = 1$ par multiplicativité. □

3.3. Construction de la norme p-adique sur les extensions finies de $\mathbf{Q}_p$. Soit K une extension finie du corps $\mathbf{Q}_p$: c'est un $\mathbf{Q}_p$-espace vectoriel de dimension finie, notée d. Par définition, une norme de $\mathbf{Q}_p$-espace vectoriel $\| \cdot \| : K \to \mathbf{R}_+$ est compatible avec $|\cdot|_p$ si $\| ax \| = |a|_p \, \| x \|$ pour tout $a \in \mathbf{Q}_p$ et tout $x \in K$. Deux telles normes sont toujours équivalentes: il existe deux réels c et $C > 0$ tels que $c \, \| x \| \leq \| x \|' \leq C \, \| x \|$ pour tout $x \in K$. Donc *si la valeur absolue de $\mathbf{Q}_p$ peut-être étendue à K, cette extension est unique*, comme on le voit à partir de $c|x^n| \leq |x^n|' \leq C|x^n|$ en prenant des racines n-èmes.

Soit x un élément de K. Les puissances de x sont liées sur $\mathbf{Q}_p$, donc on peut écrire $P_x(x) = 0$ pour un polynôme unitaire à coefficients dans $\mathbf{Q}_p$. Si l'on choisit P_x de degré minimal, alors P_x est unique: c'est le **polynôme minimal** de x (sur $\mathbf{Q}_p$); plus précisément, l'idéal des polynômes s'annulant en x est principal et P_x est l'unique polynôme unitaire tel que cet idéal soit égal à $\mathbf{Q}_p[t]P_x(t)$.

Remarque 3.11. L'application $Q \in \mathbf{Q}_p[t] \mapsto Q(x)$ est un homomorphisme d'anneaux dont le noyau est $\langle P_x \rangle := \mathbf{Q}_p[t]P_x(t)$; cet idéal principal est maximal. Le quotient $\mathbf{Q}_p[t]/\langle P_x \rangle$ est donc un corps, qui s'identifie au sous-corps $\mathbf{Q}_p(x) \subset K$ engendré par x.

En notant d_x le degré de P_x, $(1, x, x^2, \ldots, x^{d_x - 1})$ est une base de $\mathbf{Q}_p(x) \subset K$, sous-corps de K de dimension d_x. On pose alors

$$N_{\mathbf{Q}_p(x):\mathbf{Q}_p}(x) = \det(\ell_x) = P_x(0) = \prod y_i \tag{3.12}$$

où les y_i sont les autres racines de P_x (calculées dans une clôture algébrique de $\mathbf{Q}_p$) et ℓ_x est l'opérateur $\mathbf{Q}_p$-linéaire $\ell_x : y \mapsto xy$ sur l'espace vectoriel $\mathbf{Q}_p(x)$. Cet opérateur envoie 1 sur x, x sur x^2, …, $x^{d_x - 1}$, puis sur x^{d_x} qui s'exprime en fonction des autres x^i et des coefficients de P_x.

Plus généralement, on peut définir

$$N_{K:\mathbf{Q}_p}(x) = \det(\ell_{K,x}) = N_{\mathbf{Q}_p(x):\mathbf{Q}_p}(x)^{d/d_x} \tag{3.13}$$

où maintenant on prend l'opérateur de multiplication par x sur K. On pose alors

$$|x|_p = |N_{K:\mathbf{Q}_p}(x)|_p^{1/d} \tag{3.14}$$

où d est le degré de l'extension dans laquelle on calcule la norme.

Théorème 3.12. *Soit K une extension finie de $\mathbf{Q}_p$. La valeur absolue p-adique s'étend à K de façon unique : l'extension est donnée par $|x|_p = |N_{K:\mathbf{Q}_p}(x)|_p^{1/d}$.*

Démonstration. Cela étend $|\cdot|_p$ en une application multiplicative car le déterminant l'est. Soit (z_i) une base de K comme $\mathbf{Q}_p$-espace vectoriel. Munissons K de la norme du supremum dans cette base. Notons $N(x)$ au lieu de $N_{K:\mathbf{Q}_p}(x)$ pour simplifier. La fonction $|N(x)|_p$ ne s'annule pas sur la boule unité et est continue (car polynomiale, c'est un déterminant), donc il existe a et $A > 0$ avec

$$a \parallel x \parallel \leq |N(x)|^{1/d} \leq A \parallel x \parallel \tag{3.15}$$

pour tout x de norme 1, donc pour tout x par multiplicativité. Alors

$$\begin{aligned} N(x+y)^{1/d} &\leq A \parallel x+y \parallel && (3.16)\\ &\leq A(\parallel x \parallel + \parallel y \parallel) && (3.17)\\ &\leq 2(A/a)\max(N(x)^{1/d}, N(y)^{1/d}) && (3.18) \end{aligned}$$

si bien que $N^{1/d}$ est une norme approximative sur le corps K. Comme $N^{1/d}$ est bornée sur les entiers, c'est une valeur absolue. □

Exemple 3.13. Prenons $p = 3$. Le polynôme $t^2 - 3$ a deux racines dont le produit vaut -3; puisque $|-3|_p = 1/3$, les deux racines de ce polynôme ont une valeur absolue égale à $1/\sqrt{3}$. Si l'on note ces racines $x = \sqrt{3}$ et $x' = -\sqrt{3}$, on obtient $|\sqrt{3}|_p = 1/\sqrt{3}$ pour $p = 3$. Pour p distinct de 3 nous obtenons $|\sqrt{3}|_p = 1$ car $|-3|_p = 1$.

3.4. Les corps $\mathbf{C}_p$ et Ω_p. Le théorème précédent montre que la valeur absolue $|\cdot|_p$ s'étend de manière unique à $\overline{\mathbf{Q}_p}$, clôture algébrique de $\mathbf{Q}_p$. Cependant, $\overline{\mathbf{Q}_p}$ n'est pas complet pour cette valeur absolue et l'on doit compléter pour obtenir un nouveau corps $\mathbf{C}_p$; ce corps est à la fois complet et algébriquement clos. Voir les livres de Koblitz et Robert mentionnés en introduction pour des compléments.

4. Découpages triangulaires du carré

Nous allons illustrer l'usage de la valeur absolue p-adique (avec ici $p = 2$) pour démontrer le théorème suivant.

Théorème 4.1 (Monsky)**.** *Il n'existe aucun découpage du carré en un nombre impair de triangles de mêmes aires.*

Autrement dit, si le nombre de triangles est P, on a : même aire implique P pair, ce que l'on peut lire "*si mémère alors pépère*". Nous renvoyons au livre *Proofs from the Book, Sixth Edition*, par Martin Aigner et Günter M. Ziegler (voir le chapitre 22, page 155, intitulé "One square and an odd number of triangles") pour les détails de la démonstration.

4.1. Démonstration (cas particulier). Nous considèrerons le carré $[0,1] \times [0,1]$ (on peut toujours se ramener à ce cas par déplacement euclidien). Nous verrons ce carré soit comme sous-ensemble du plan, soit comme sous-ensemble de $\mathbf{R}^3$ situé à l'altitude $z = 1$: les points du carrés sont donc de la forme $(x,y,1)$ avec $0 \leq x,y \leq 1$.

Nous allons démontrer ce théorème en supposant que les coordonnées des sommets de la triangulation sont dans $\mathbf{Q}$.

Remarquons que si un tel découpage existait, alors tous les triangles auraient une aire égale à $1/N$, où N est le nombre de triangles. Si N est impair, *tous les triangles ont donc une aire de norme 2-adique égale à* 1.

Considérons trois points du carré $[0,1] \times [0,1]$ de coordonnées (x_i, y_i), $i = 1,2,3$. En plaçant l'origine au point (x_3, y_3) dans le plan du carré, on trouve une aire orientée

$$Aire = \frac{1}{2}((x_1 - x_3)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_3)); \tag{4.1}$$

en retranchant la dernière ligne aux deux premières, on en déduit

$$Aire = \frac{1}{2} \det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix}. \tag{4.2}$$

Colorions les points $(x,y,1)$ du carré (vu à l'altitude 1) qui sont à coordonnées rationnelles en trois couleurs : bleu rouge vert. Un sommet est bleu si x maximise la norme 2-adique des coordonnées; il est rouge si $|x|_2 < |y|_2 \geq 1$; il est vert si x et y ont une norme < 1. Par exemple, $(1/3, 1/2, 1)$ est rouge. Si x et y sont dans un sous-corps de $\mathbf{R}$ auquel on sait étendre la valeur absolue 2-adique, par exemple $\overline{\mathbf{Q}}$, alors le même raisonnement s'appliquera (voir plus bas).

La **remarque cruciale** est la suivante: *le déterminant (resp. l'aire) d'un triangle tricolore a une valeur absolue 2-adique* ≥ 1 *(resp.* ≥ 2*); cette valeur*

absolue est celle de $x_b \times y_r \times 1_v$. Ceci résulte directement du calcul du déterminant ci-dessus. L'aire d'un triangle tricolore ne peut donc pas être $1/N$ avec N impair. On en déduit : *sur un même segment, on ne peut voir apparaître que deux couleurs de sommets* (car l'aire d'un triplet tricolore ne peut être nulle).

Maintenant, il s'agit de montrer qu'il existe au moins un triangle tricolore pour terminer la démonstration, ce qui résulte du lemme suivant.

Lemme 4.2 (Sperner)**.** *Le nombre de triangles tricolores est impair.*

Démonstration. Le sommet $(0,0,1)$ est vert, le sommet $(1,0,1)$ est bleu; sur le côté du carré les reliant on ne voit que du bleu et du rouge, avec un nombre impair de segments (bleu, rouge). Le sommet $(0,1,1)$ est rouge, $(1,1,1)$ est bleu, et tous les sommets sur $[(1,0,1),(1,1,1)]$ sont bleus ou rouges. Donc il n'y a pas de segment (bleu, rouge) sur les trois autres côtés.

Un triangle tricolore a un côté de chaque type bicolore. Notons T le nombre de triangles tricolores.

Un triangle monocolore n'a pas de côté bicolore.

Un triangle bicolore a un côté monocolore et deux côtés bicolores 'identiquement colorés'. Par exemple deux côtes (bleu, rouge) et un côté (bleu,bleu). Notons B le nombre de triangles bicolores (bleu, rouge)

Donc si on compte le nombre de côtés (bleu, rouge) avec multiplicité (un côté intérieur comptant double) on obtient un nombre impair (à cause du bord du carré); et si l'on somme sur les triangles on obtient un $2 \times B + 1 \times T$. En égalisant on voit que T est impair. □

4.2. Démonstration, cas général. Pour démontrer le théorème en toute généralité, il s'agit d'étendre la valeur absolue 2-adique de $\mathbf{Z}$ à $\mathbf{Z}(x_i, y_i)$ où les nombres réels x_i et y_i que l'on adjoint sont les coordonnées des sommets de la triangulation. Pour cela, on peut consulter le livre de Robert, ou celui de Aigner et Ziegler (dans cette seconde référence, les auteurs utilisent une astuce consistant à adapter le groupe des valeurs de la valeur absolue).

5. LE LEMME DE HENSEL

Soit $P \in \mathbf{Z}_p[t]$ un polynôme d'une variable dont les coefficients sont des entiers p-adiques. Soit $P'(t)$ son polynôme dérivé; c'est aussi un élément de $\mathbf{Z}_p[t]$. Soit a_0 un élément de $\mathbf{Z}_p$. Supposons que $P(a_0) = 0 \mod (p)$ (c'est-à-dire que $|P(a_0)|_p < 1$, ou encore $P(a_0) \in p\mathbf{Z}_p$) et que $P'(a_0) \neq 0 \mod (p)$ (c'est-à-dire $|P'(a_0)| = 1$). Il existe alors un élément a de $\mathbf{Z}_p$ tel que $P(a) = 0$ et $a = a_0 \mod (p)$ (c'est-à-dire $|a - a_0| \leq 1/p$).

Démonstration. Ecrivons $P(t) = c_0 + c_1 t + c_2 t^2 + \cdots + c_d t^d$ où d est le degré de P. Par hypothèse, $P(a_0) = 0 \mod (p)$. Nous allons montrer qu'il existe une suite de nombres entiers $a_1, a_2, \cdots$, telle que

(i) $P(a_n) = 0 \mod (p^{n+1})$
(ii) $a_n = a_{n-1} \mod (p^n)$
(iii) $0 \leq a_n < p^{n+1}$

ceci pour tout $n \geq 1$. Ceci est suffisant pour conclure la démonstration en posant $a = \lim_n (a_n)$.

Commençons avec $n = 1$. Notons a_0' l'unique nombre entier compris entre 0 et $p-1$ tel que $a_0 = a_0' \mod (p)$. Nous cherchons a_1 sous la forme $a_1 = a_0' + pb_1$ avec $0 \leq b_1 < p$; les propriétés (ii) et (iii) seront alors automatiques. Pour (i), nous voulons que $P(a_0' + pb_1) = 0 \mod (p^2)$; mais

$$P(a_0' + pb_1) = P(a_0') + P'(a_0')pb_1 \mod (p^2). \tag{5.1}$$

Puisque $P(a_0) = 0 \mod (p)$ nous obtenons $P(a_0') = 0 \mod (p)$ et donc $P(a_0') = p\alpha \mod (p^2)$ pour un unique $\alpha \in \{0, \ldots, p-1\}$. Puisque $P'(a_0) \neq 0 \mod (p)$ nous obtenons $P'(a_0') \neq 0 \mod (p)$. Il existe donc un unique $b_1 \in \{0, \ldots, p-1\}$ tel que $\alpha = P'(a_0')b_1 \mod (p)$ et ce b_1 est l'unique choix assurant (i).

Pour passer de a_{n-1} à a_n l'argument est le même : puisque $P'(a_0)$ n'est pas nul modulo p, $P'(a_{n-1})$ est également inversible modulo p, et l'on peut trouver b_n avec $a_n = a_{n-1} + b_n p^n$. □

Exemple 5.1. Prenons $p = 3$. Si le polynôme $P(t) = t^2 - 3$ avait une racine dans $\mathbf{Q}_3$ celle-ci vérifierait $|a|_3^2 = 1/3$, une contradiction. Le lemme de Hensel ne peut donc pas s'appliquer ; d'ailleurs, $P(0) = 0$, $P(1) = 1$ et $P(2) = 1$ tandis que $P'(0) = 0$ modulo 3.

Exemple 5.2. Les carrés modulo 5 sont 0, 1, 4, donc il n'y a pas de a_0 dans $\mathbf{Z}_5$ tel que $P(a_0) = 0 \mod (5)$. A nouveau, il n'y a pas de racine de 3 dans $\mathbf{Z}_5$, ni dans $\mathbf{Q}_5$ d'ailleurs (mais l'argument de norme est insuffisant pour obtenir cette conclusion). Un argument similaire fonctionne si $p = 7$.

Exemple 5.3. Modulo 2 les carrés sont 0 et 1, donc 3 est le carré de 1. Mais $P'(t) = 2t = 0$ modulo 2 donc le lemme de Hensel ne s'applique pas. Si l'on cherche une racine carrée sous la forme $1 + pb_1 + p^2 b_2 + \cdots$ ceci donne

$$(1 + 2b_1)^2 = 3 \mod (4)$$

et l'on voit qu'il n'y a pas de solution.

Exemple 5.4. Les carrés modulo 11 sont 0, 1, 4, 9, 5, 3. Ainsi, $5^2 = 25 = 3+2\times 11$ si bien que 3 est bien un carré. De plus, $P'(5) = 2\times 5 = 10$ qui n'est pas nul modulo 11. Le lemme de Hensel s'applique, et l'algorithme donne les approximations suivantes pour la racine de P: $5+11b_1$ avec

$$25+2\times 5\times 11b_1+b_1^2\times 11^2-3=(2-b_1)\times 11 \mod (11^2)$$

soit $2+2\times 5\times b_1=0 \mod (11)$ soit $b_1=2 \mod (11)$, i.e. $b_1=2$. Ainsi $\sqrt{3}=5+2\times 11+\cdots$ dans $\mathbf{Z}_{11}$. Ensuite on cherche b_2 tel que $(27+11^2b_2)^2-3=0 \mod (11^3)$. On obtient $11^2\times 6+2\times 11^2\times 27\times b_2=0 \mod (11^3)$ ce qui donne $6+2\times 5\times b_2=0 \mod (11)$ et $b_2=6$. D'où

$$5+2\times 11+6\times 11^2.$$

Si l'on démarre avec 6 au lieu de 5 modulo 11 on trouve l'autre racine.

6. La suite

Vous êtes maintenant armés pour comprendre les deux applications suivantes.

6.1. Dynamique p-adique. Certains phénomènes qui font la richesse des systèmes dynamiques holomorphes, par exemple l'existence de points de Cremer, deviennent plus simples lorsqu'on les transpose du *côté p-adique*. Un bon exemple est donné par le lemme de Jason Bell décrit dans le texte *Un lemme d'interpolation*. Voici une conséquence de ce théorème.

Soit $f\colon \mathbf{C}^k\to\mathbf{C}^k$ une transformation polynomiale; ceci signifie qu'il existe des polynômes $f_i(x_1,\ldots,x_k)\in\mathbf{C}[x_1,\ldots,x_k]$ tels que

$$f(x_1,\ldots,x_k)=(f_1(x_1,\cdots,x_k),\ldots,f_k(x_1,\ldots,x_k)). \tag{6.1}$$

On dit que f est un automorphisme de l'espace $\mathbf{C}^k$, et l'on note $f\in\mathsf{Aut}(\mathbf{C}^k)$ si f est inversible et l'inverse $f^{-1}\colon \mathbf{C}^k\to\mathbf{C}^k$ est également une transformation polynomiale. C'est le cas, par exemple, de toutes les transformations affines, ou de $f(x_1,x_2)=(x_2,x_1+x_2^3+3)$. Dans l'énoncé suivant, f^n désigne la composition $f\circ f\circ\cdots\circ f$ (n fois); plus précisément, les itérés de f définissent un homomorphisme de groupe $n\in\mathbf{Z}\mapsto f^n\in\mathsf{Aut}(\mathbf{C}^k)$ (les automorphismes forment un groupe pour la composition).

Théorème 6.1. *Soit f un élément de $\mathsf{Aut}(\mathbf{C}^k)$. Soit V un sous-ensemble de $\mathbf{C}^k$ défini par un sytème d'équations polynomiales. Si $x\in\mathbf{C}^k$, alors l'ensemble des temps de passage*

$$Pas_f(x;V)=\{m\in\mathbf{Z}\,;\ f^m(x)\in V\}$$

est une union finie de progression arithmétiques.

Autrement dit, $Pas_f(x;V)$ est une union finie d'ensembles de la forme $\{a\ell + b\ ;\ \ell \in \mathbf{Z}\}$ où la raison a de la progression arithmétique $a\ell + b$ peut être nulle. En particulier, si $Pas_f(x;V)$ est infini, il contient une suite $\ell \in \mathbf{Z} \mapsto a\ell + b$ avec $a \neq 0$. Ce théorème est dû à Bell, Ghioca et Tucker. Lorsque f est linéaire et V est un sous-espace linéaire de $\mathbf{C}^k$, c'est le théorème de Skolem, Mahler et Lech: *l'ensemble des indices n en lesquels une suite (u_n) définie par une relation de récurrence linéaire s'annule est une union finie de progressions arithmétiques.*

6.2. Alternative de Tits. Plus difficile, voici un énoncé démontré par Jacques Tits, dont la démonstration utilise aussi un passage aux nombres p-adiques. Soit G un sous-groupe de $\mathsf{GL}_k(\mathbf{C})$ engendré par un nombre fini de matrices A_1, $\ldots$, A_s. Alors, ou bien G contient un sous-groupe H d'indice fini qui est résoluble, ou bien G contient deux matrices A et B qui engendrent un groupe libre de rang 2. Ceci signifie qu'il n'y a pas de relations non-triviale entre A et B : si les entiers relatifs m_j et n_j sont tous non nuls, alors $A^{m_1}B^{n_1}A^{m_2}B^{n_2}\cdots A^{m_\ell}B^{n_\ell} \neq \mathsf{Id}$. Voir le texte d'Yves Benoist intitulé *Sous-groupes discrets des groupes de Lie*, Chapitre 3.

UNIV RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE
E-mail address: serge.cantat@univ-rennes1.fr