I
Les valeurs absolues des nombres rationnels

1. Valeurs absolues d'un corps

Soit K un corps. Une *valeur absolue* de K (au sens, par exemple, de Bourbaki, attention cette notion coïncide avec "valuation" en anglais) est une fonction non nulle $|.|$ définie sur K à valeurs dans les nombres réels positifs et vérifiant les trois conditions $((x, y) \in K^2)$:

(ι) $|x| = 0$ si et seulement si $x = 0$,
($\iota\iota$) $|xy| = |x|\,|y|$,
($\iota\iota\iota$) $|x + y| \leq |x| + |y|$.

La relation ($\iota\iota$) entraîne que $|.|$ induit un homomorphisme de groupes $K^* \longrightarrow \mathbf{R}_+^*$. La relation ($\iota\iota\iota$) s'appelle *l'inégalité triangulaire*.

Lorsque L est un sous-corps de K, une valeur absolue de K induit une valeur absolue de L. Toute valeur absolue d'un corps de caractéristique 0 prolonge donc une valeur absolue du corps des nombres rationnels $\mathbf{Q}$.

Exemples. — La valeur absolue triviale est égale à 1 sauf en 0. On l'exclut parfois implicitement.

Lorsqu'on a un plongement $i : K \longrightarrow \mathbf{C}$, les fonctions $x \mapsto |i(x)|_\infty^k = |\bar{i}(x)|_\infty^k$ sont des valeurs absolues de K (on a noté $|.|_\infty$ la valeur absolue habituelle de $\mathbf{C}$ et k est un nombre réel vérifiant $0 < k \leq 1$).

Une valeur absolue est dite *non-archimédienne* si la distance associée (qui associe à (x, y) le nombre $|x - y|$) est ultramétrique, c'est-à-dire si on a, pour tout $(x, y) \in K^2$, l'inégalité

$$|x + y| \leq \mathrm{Max}(|x|, |y|).$$

Cette distance associée définit une topologie sur K. Deux valeurs absolues sont dites *équivalentes* si elles se déduisent l'une de l'autre par élévation à la puissance d'un nombre réel > 0. Une valeur absolue est dite *archimédienne* si elle n'est pas équivalente à une valeur absolue non-archimédienne. Deux valeurs absolues équivalentes définissent des distances équivalentes (au sens usuel) donc la même topologie sur K.

Une place de K est une classe d'quivalence de valeur absolue non-triviale.

Soit x un élément non nul de K. Remarquons que pour la topologie définie par une valeur absolue $|.|$, les applications $K \longrightarrow K$ qui à y associe $x + y$, xy, $1/y$ (pour $y \neq 0$) et

$-y$ respectivement sont continues. De plus l'application $K \longrightarrow \mathbf{R}$ qui à y associe $|y|$ est continue.

On établit facilement que la valeur absolue d'une racine de l'unité est égale à 1 ; il en résulte que toute valeur absolue d'un corps fini est triviale (cela résulte de la propriété $(\iota\iota)$).

2. Valuations discrètes

Un *anneau de valuation discrète* A est par définition un anneau principal (et donc intègre) qui possède un unique idéal premier et non nul $\mathcal{M}_A$. Cet idéal est nécessairement maximal.

Lemme 1. — *Tout idéal non nul de A est de la forme $\mathcal{M}_A^n$.*
Démonstration. — Soit I un idéal de A. On a $I = xA$ avec $x \in A$ puisque A est principal. Comme I est non nul, on a $I \subset \mathcal{M}_A$ ou $I = A = \mathcal{M}_A^0$. Excluons ce dernier cas. Soit π un générateur de $\mathcal{M}_A$. L'idéal $\cap_{n\geq 0}\pi^n A$ est premier ; en effet, pour $(x, y) \in \pi^n A \times \pi^m A$, vérifiant $xy \in \cap_{n\geq 0}\pi^n A$, on a $(x/\pi^n)(y/\pi^m) \in \cap_{n\geq 0}\pi^n A \subset \mathcal{M}_A$ et donc $x/\pi^n \in \mathcal{M}_A$ ou $y/\pi^m \in \mathcal{M}_A$, c'est-à-dire $x \in \pi^{n+1}A$ ou $y \in \pi^{m+1}A$, et donc $x \in \cap_{n\geq 0}\pi^n A$ ou $y \in \cap_{n\geq 0}\pi^n A$ par un procédé inductif. L'idéal $\cap_{n\geq 0}\pi^n A$ n'est pas égal à $\mathcal{M}_A$ (car on aurait alors $\pi A = \pi^2 A$ et donc $A = \pi A$ par intégrité de A, ce qui est absurde). Il est donc nul.

Il existe donc un plus petit entier $n \geq 0$ tel que $I \subset \mathcal{M}_A^n$. L'ensemble $\pi^{-n}I$ est alors un idéal de A non contenu dans $\mathcal{M}_A$. C'est donc A et on a $I = \pi^n A = \mathcal{M}_A^n$.

Un générateur de $\mathcal{M}_A$ comme A-module est une *uniformisante* de $\mathcal{M}_A$. Le corps $A/\mathcal{M}_A$ est le *corps résiduel* de A.

On a une suite décroissante de A-modules :

$$...\mathcal{M}_A^{n+1} \subset \mathcal{M}_A^n \subset ... \subset \mathcal{M}_A \subset A.$$

Soit $x \in A$ non nul. L'idéal de A engendré par x est égal à $\mathcal{M}_A^n$ où n est un entier ≥ 0. L'entier n est la *valuation* de x. Notons cette valuation $v(x)$.

L'application $v : A \longrightarrow \mathbf{N}$ est une *valuation* de A. Elle s'étend en une fonction surjective à valeurs dans $\mathbf{Z}$, encore notée v, sur le corps des fractions K de A, par la formule $v(\frac{x}{y}) = v(x) - v(y)$. La valuation est discrète car c'est un homomorphisme de groupes $K^* \longrightarrow \mathbf{Z}$ d'image un groupe discret.

(On pose souvent par convention $v(0) = +\infty$.)

Exemples. — Soit p un nombre premier. Notons $\mathbf{Z}_{(p)}$ l'ensemble des nombres rationnels dont le dénominateur est premier à p. C'est l'anneau obtenu en localisant $\mathbf{Z}$ relativement à l'idéal premier $p\mathbf{Z}$. Il est de valuation discrète d'idéal maximal égal à $p\mathbf{Z}_{(p)}$. On note v_p la valuation associée. Le corps résiduel est $\mathbf{F}_p$ le corps à p éléments.

L'anneau $\mathbf{Z}_p$ des entiers p-adiques est un cas éminent d'anneau de valuation discrète. On verra plus tard comment le construire à partir de $\mathbf{Z}_{(p)}$.

Soit k un corps. L'anneau $k[[T]]$ est un anneau de valuation discrète d'idéal maximal $Tk[[T]]$, de corps résiduel k et de corps des fractions $k((T))$.

PROPOSITION 1. — *Soit K un corps. Soit v un homomorphisme surjectif de groupes $K^* \longrightarrow \mathbf{Z}$. Supposons que v vérifie $v(x+y) \geq \min(v(x), v(y))$ pour tout $(x,y) \in K^{\times 2}$. Alors l'ensemble $A = \{x \in K^*/v(x) \geq 0\} \cup \{0\}$ est un sous-anneau de K de valuation discrète d'idéal maximal $\mathcal{M}_A = \{x \in K^*/v(x) > 0\} \cup \{0\}$.*
Démonstration. — Les ensembles A et $\mathcal{M}_A$ sont stables par l'addition interne et la multiplication par les éléments de A et contiennent 0 (De plus A contient 1). Ce sont donc un anneau et un idéal de A respectivement. Observons que les éléments inversibles de A sont ceux qui sont dans le noyau de v. Soit π un élément de A tel que $v(\pi) = 1$. Tout élément x de A est de la forme $\pi^n u$ avec n entier ≥ 0 et $v(u) = 0$. Tout idéal de A s'écrit donc sous la forme $\pi^n A$ avec $n \geq 0$. Il en résulte que A est principal et a pour unique idéal premier non nul $\pi A = \mathcal{M}_A$.

Soit a un nombre réel > 1. L'application $x \mapsto a^{-v(x)}$ est une valeur absolue de K dont la classe d'équivalence est indépendante de a.

Lorsque le corps résiduel est d'ordre fini $|k|$, on choisit comme représentant canonique $a = |k|$. Lorsque $A = \mathbf{Z}_{(p)}$, on pose $|x|_p = p^{-v_p(x)}$. C'est la valeur absolue *p-adique* du corps des nombres rationnels $\mathbf{Q}$.

3. Valeurs absolues de Q

Ce qui suit est connu comme le théorème d'Ostrowski.

THÉORÈME 1. — *Soit $|.|$ une valeur absolue non triviale de $\mathbf{Q}$. Alors $|.|$ est équivalente à $|.|_p$ pour un nombre premier p ou à $|.|_\infty$.*
Démonstration. — Supposons d'abord qu'il existe $x_0 \in \mathbf{Z}$ tel que $|x_0| > 1$. Puisqu'on a $|-1| = 1$, quitte à remplacer x_0 par $-x_0$ on peut supposer que x_0 est un entier positif. Soit x un entier strictement positif. Ecrivons x_0^n en base x :

$$x_0^n = \alpha_k x^k + ... + \alpha_1 x + \alpha_0.$$

Rappelons qu'on a l'inégalité $0 \leq \alpha_i < x$ $(i = 0, 1, ..., k)$. Posons

$$C_x = \mathrm{Max}(|1|, ..., |x-1|).$$

En appliquant l'inégalité triangulaire on obtient

$$|x_0|^n \leq C_x(1+k)\mathrm{Max}(1, |x|^k).$$

De plus on a

$$k \leq \log_x(x_0^n),$$

où $\log_x$ est le logarithme en base x. Cela donne

$$|x_0|^n \leq C_x(1+\log_x(x_0^n))\mathrm{Max}(1, |x|^{\log_x(x_0^n)}).$$

En prenant les racines n-ièmes et en faisant tendre n vers l'infini on obtient

$$|x_0| \leq \mathrm{Max}(1, |x|^{\log_x(x_0)}),$$

et donc, puisque $|x_0| > 1$,

$$|x_0|^{\frac{1}{\log x_0}} \leq |x|^{\frac{1}{\log x}}.$$

Cela donne $|x| > 1$ et par échange des rôles de x et x_0

$$|x_0|^{\frac{1}{\log x_0}} = |x|^{\frac{1}{\log x}}.$$

Cette égalité s'étend immédiatement à l'égalité suivante pour deux nombres rationnels non nuls x et x_0 quelconques

$$|x_0|^{\frac{1}{\log |x_0|_\infty}} = |x|^{\frac{1}{\log |x|_\infty}}.$$

Par passage aux logarithmes, cela entraîne que la valeur absolue $|.|$ est équivalente à la valeur absolue archimédienne.

Abandonnons notre hypothèse de départ. On peut donc supposer que sur $\mathbf{Z}$ la valeur absolue $|.|$ est à valeurs dans les nombres réels ≤ 1. On va la supposer non triviale. Cela entraîne que $|.|$ est non constante égale à 1 sur les entiers non nuls par multiplicativité de la valeur absolue et en raison du fait que tout nombre rationnel est quotient de deux nombres entiers. Pour tout $x \in \mathbf{Z}$ on a donc $|x| \leq 1$.

Lemme 2. — *La valeur absolue* $|.|$ *est non archimédienne.*
Démonstration. — Soit x et y deux nombres rationnels. On a, utilisant le fait que le coefficient binomial $\binom{n}{k}$ est un entier et donc vérifie $|\binom{n}{k}| \leq 1$ et l'inégalité triangulaire, les inégalités

$$|x+y|^n = |(x+y)^n| \leq \sum_{k=0}^{n} \binom{n}{k} |x|^k |y|^{n-k} \leq (n+1)\mathrm{Max}(|x|^n, |y|^n).$$

Par passage à la limite sur n après avoir extrait les racines n-ièmes, on obtient l'inégalité cherchée.

Revenons à la démonstration du théorème. L'ensemble des entiers x tels que $|x| < 1$ constitue un idéal premier non nul de $\mathbf{Z}$. (Cela résulte de l'inégalité ultramétrique établie par le lemme de façon analogue à la démonstration de la proposition 1.) Il est donc de la forme $p\mathbf{Z}$ où p est un nombre premier. Soit $a \in \mathbf{Q}$. Posons $a = a_0 p^n$, avec a_0 quotient de deux nombres entiers premiers à p et $n \in \mathbf{Z}$. On a $|a| = |a_0||p|^n = |p|^{v_p(a)}$. La norme $|.|$ est donc équivalente à la valeur absolue p-adique $|.|_p$. Cela achève la démonstration du théorème d'Ostrowski.

Remarque . — On verra que le théorème d'Ostrowski détermine les valeurs absolues des extensions finies de $\mathbf{Q}$ et que dans ce cas on a plus d'une valeur absolue non-archimédienne.

La formule suivante est connue sous le nom de *formule du produit.*

PROPOSITION 2. — *Soit x un nombre rationnel non nul. On a*

$$(\prod_{p \text{ premier}} |x|_p)|x|_\infty = 1.$$

Démonstration. — Par multiplicativité des valeurs absolues, il suffit de vérifier la formule pour les nombres premiers et pour -1. Soit q un nombre premier. Lorsque p est un nombre premier différent de q on a $|q|_p = 1$. De plus on a $|q|_q = 1/q$ et $|q|_\infty = q$.

On ne s'étendra ici sur la notion de place qui ne nous sera pas vraiment utile. Une *place* d'un corps K dans un corps L est une application $K \cup \{\infty\} \longrightarrow L \cup \{\infty\}$ qui respecte l'addition et la multiplication prolongées partiellement des corps K et L à $K \cup \{\infty\}$ et $L \cup \{\infty\}$ par $x + \infty = \infty$ (x élément du corps), $x\infty = \infty$ (x non nul) et $\infty + \infty = \infty$ (0∞ n'est pas défini). Une telle place est dite *finie* (resp. *infinie*) lorsque L est fini (resp. infini).

Pour p nombre premier, la réduction modulo p fournit un place de $\mathbf{Q}$ dans le corps $\mathbf{F}_p$ à p éléments (en convenant que la réduction modulo p d'un nombre rationnel non p-entier est ∞). Il s'agit d'une place finie. Ces places coïncident naturellement avec les valeurs absolues non-archimédiennes de $\mathbf{Q}$. La place triviale de $\mathbf{Q}$ dans $\mathbf{Q}$ peut être vue comme correspondant à la valeur absolue archimédienne. Un homomorphisme de corps $K \longrightarrow L$, qui est nécessairement injectif, fournit par un prolongement trivial une place de K dans L.

Signalons que toutes les places de $\mathbf{Q}$ sont obtenues en composant celle mentionnées ci-dessus avec des places déduites d'homomorphismes injectifs de corps comme ci-dessus. A un homomorohisme de corps près, les places de $\mathbf{Q}$ correspondent donc aux valeurs absolues de $\mathbf{Q}$ à équivalence près. Cette remarque trouve son intérêt dans le fait que la notion de place est plus intrinsèque que la notion de valeur absolue : Elle ne recourt pas au corps des nombres réels.

Exercice 1. — Soit k un corps. Soit P un polynôme irréductible de k. Soit $Q = P^n \frac{u}{v} \in k(T)$, où u et v sont deux polynômes premiers entre eux et premiers à P et $n \in \mathbf{Z}$. Soit $\delta \in \mathbf{R}$, $0 < \delta < 1$. Posons

$$|Q|_P = \delta^n.$$

1. Démontrer que l'application qui à Q associe le nombre réel $|Q|_P$ est une valeur absolue de $k(T)$.
2. Démontrer que l'application qui à $Q = \frac{u}{v} \in k(T)$ associe $\delta^{\mathrm{d}^0 v - \mathrm{d}^0 u}$ est une valeur absolue de $k(T)$.
3. Démontrer que les valeurs absolues de $k(T)$ qui sont triviales sur k sont à équivalence près de l'un des deux types précédents.
4. En déduire que les valeurs absolues de $\mathbf{F}(T)$ sont de l'un des deux types ci-dessus lorsque $\mathbf{F}$ est un corps fini.

Exercice 2. — Soit K un corps. Soit $|.|_1$, $|.|_2$, ..., $|.|_n$ des valeurs absolues non triviales.

1. Supposons-les deux à deux non équivalentes. Soit $(\alpha_1, \alpha_2, ..., \alpha_n) \in K^n$. Pour tout nombre réel $\epsilon > 0$, montrer qu'il existe $\beta \in K$ tel que pour tout $i \in \{1, 2, ..., n\}$ on ait $|\beta - \alpha_i|_i < \epsilon$. (On pourra commencer par $n = 2$ et procéder par récurrence.) C'est essentiellement le théorème d'approximation faible, qui sera vu plus tard.
2. Montrer que, si $|.|_1$ et $|.|_2$ sont équivalentes, elles définissent la même topologie sur K.
3. Montrer que, si elles définissent la même topologie, elles sont équivalentes.

Exercice 3. — Soit K un corps de caractéristique 0. Supposons K muni d'une valeur absolue $|.|$ archimédienne pour laquelle il est complet.
1. Montrer que K contient un sous-corps isomorphe à $\mathbf{R}$ et que la restriction de la valeur absolue à ce sous-corps est équivalente à la valeur absolue habituelle de $\mathbf{R}$.
2. Montrer que la valeur absolue complexe est, équivalence près, la seule extension à $\mathbf{C}$ de la valeur absolue de $\mathbf{R}$.
3. On pourra admettre le théorème de Gelfand-Mazur suivant. Soit A une algèbre commutative sur $\mathbf{R}$. Supposons que A admette un élément i tel que $i^2 = -1$. Supposons que l'espace vectoriel réel A admette une norme $||.||$ et que, pour tout x, y dans A on a $||xy|| \leq ||x||\,||y||$. Pout tout $z \in A$, $z \neq 0$, il existe u, $v \in \mathbf{R}$ tels que $z - (u + iv)$ n'est pas inversible dans A.
4. En déduire que K est isomorphe à $\mathbf{R}$ ou $\mathbf{C}$, et que $|.|$ est équivalente aux valeurs absolues usuelles de ces corps. On appelle aussi ce résultat théorème de Gelfand-Mazur.

4. Commentaires sur les analogies en arithmétique

Les extensions finies des corps $\mathbf{Q}$ et $\mathbf{F}(T)$ sont respectivement les *corps de nombres* et les *corps de fonctions*. Les propriétés arithmétiques de ces corps sont très analogues, mais généralement plus difficiles à établir pour les corps de nombres. D'un point de vue technique, l'étude des corps de fonctions revient à l'étude des courbes algébriques sur les corps finis, ce qui est du ressort de la géométrie algébrique.

Prenons note de quelques différences entre $\mathbf{Q}$ et $\mathbf{F}(T)$:

– Le corps $\mathbf{Q}$ possède une valeur absolue archimédienne contrairement à $\mathbf{F}(T)$. Dans l'esprit qui prévaut en théorie des nombres, cette valeur absolue doit être prise en compte et, éventuellement, placée à égalité avec les valeurs absolues non archimédiennes.

– Les anneaux de valuation discrète associés aux valeurs absolues de $\mathbf{F}(T)$ (resp. $\mathbf{Q}$) ont des corps résiduels qui ont tous même caractéristique (resp. ont des caractéristiques toutes différentes).

– Le corps $\mathbf{F}(T)$ possède des extensions finies obtenues en considérant les extensions de $\mathbf{F}$ (on s'accorde toutefois à penser que certaines extensions de $\mathbf{Q}$ obtenues en ajoutant des racines de l'unité seraient les analogues de ces extensions).

– On peut faire sur l'anneau $\mathbf{F}[T]$ (qui est l'anneau des entiers de $\mathbf{F}(T)$) l'opération suivante $\mathbf{F}[T] \otimes_{\mathbf{F}} \mathbf{F}[T] \simeq \mathbf{F}[T_1, T_2]$. On ne voit pas comment donner un sens à une telle opération pour le corps $\mathbf{Q}$ (*i.e.* on a $\mathbf{Z} \otimes \mathbf{Z} \simeq \mathbf{Z}$, ce qui n'est pas très intéressant).

– Le corps $\mathbf{F}(T)$ est muni d'une application $\mathbf{F}$-linéaire donnée par la dérivation. C'est parfois un outil très commode dont on aimerait bien disposer pour étudier les nombres.