Ramifications Mathématiques

CONVEXITÉ, TIROIRS
et
COORDONNÉES ENTIÈRES

Par Gilbert LABELLE,
département de mathématiques
Université du Québec à Montréal

Cette chronique a pour but de présenter des sujets variés de l'arbre des mathématiques, sous forme d'exemples simples et de questions intégrées au texte, de façon à mettre en évidence des résultats mathématiques fondamentaux.

1. LE PRINCIPE DES TIROIRS.

Le lecteur connaît certainement le principe évident: *lorsque au moins* $n + 1$ *"objets" sont placés dans* n *"tiroirs"* $(n > 0)$*, alors l'un des tiroirs doit nécessairement contenir au moins deux objets.*

Sous une forme un peu plus mathématique, on peut l'énoncer comme suit:

PRINCIPE DES TIROIRS

Soit f*:* Ω — T *une fonction de l'ensemble* Ω *(non vide) dans un ensemble* T *(fixé et non vide). Alors*

$$\text{Card } \Omega > \text{Card T} \Rightarrow \text{f non injective} \tag{1.1}$$

Dans l'énoncé, Ω et T sont respectivement les ensembles d'objets et de tiroirs et Card X signifie la cardinalité (le nombre d'éléments) de X.

Comment généraliser ce principe de façon à obtenir des théorèmes "parallèles" à (1.1) ?

Voici une façon de le faire parmi, évidemment, une infinité d'autres! Considérons un ensemble préordonné X, soit un ensemble X muni d'une relation binaire $\leqslant$ satisfaisant aux propriétés

(i) $\forall\ x \in X,\ x \leqslant x$ (réflexivité)

(ii) $\forall\ x,y,z \in X,\ (x \leqslant y$ et $y \leqslant z) \Rightarrow x \leqslant z$ (transitivité).

Supposons maintenant donnée une propriété P, que chaque élément de X vérifie ou ne vérifie pas.

DÉFINITION

On dira qu'on a trouvé un "principe des tiroirs généralisé" sur l'ensemble X par rapport à la propriété P, si pour tout $x \in X$ on a un résultat du type

$$[x \text{ est assez grand} \Rightarrow X \text{ satisfait la propriété P}] \qquad (1.2)$$

et où "x est assez grand" est explicitement défini dans le contexte considéré.

REMARQUE. Pour retrouver à titre de cas particulier le principe initial des tiroirs, on peut prendre $X = \{f \mid f: \Omega — T, \Omega \neq \phi$ quelconque$\}$ et dire que $f_1 < f_2$ (où $f_i : \Omega_i — T$) ssi Card $\Omega_1 <$ Card Ω_2. On pose également que "f satisfait à P" si et seulement si f est injective et que "f est assez grand" si et seulement si $f > 1_T$, ou 1_T est la fonction identité sur T.

2. DEUX EXEMPLES SIMPLES.

Plaçons-nous par exemple sur une sphère de R^3: $S = \{(x, y, z) \mid x^2 + y^2 + z^2 = 1\}$ et soit X l'ensemble des parties de S ayant une aire (il est possible de montrer qu'il existe des parties de S qui ne possèdent pas d'aire). Posons que $U_1 \leqslant U_2$ (où $U_i \in X$) ssi aire $(U_1) \leqslant$ aire (U_2). Soit P la propriété de posséder deux points antipodaux. On a, comme analogue de (1.2),

$$\text{aire } (U) > 2\pi \Rightarrow U \text{ possède deux points antipodaux.} \qquad (2.1)$$

Comment démontrer ce résultat?

Supposons que U ne possède pas de points antipodaux. La fonction $\alpha: U \to S$ qui est définie par " $\alpha(x)$ = l'antipode de x" a une image $\alpha(U)$ nécessairement disjointe de U et l'on doit avoir

$$\begin{aligned} \text{aire } (U \cup \alpha(U)) &= \text{aire } (U) + \text{aire } (\alpha(U)) \\ &= \text{aire } (U) + \text{aire } (U) \qquad (2.2) \\ &= 2 \text{ aire } (U). \end{aligned}$$

Or $U \cup \alpha(U) \subset S$. Donc 2 aire $(U) \leqslant$ aire (S) i.e. 2 aire $(U) \leqslant 4\pi$, ce qui contredit l'hypothèse: aire $(U) > 2\pi$.

Le deuxième exemple est évident. Le lecteur est invité à en donner une preuve et à l'énoncer sous la forme (1.2) avec un choix approprié pour X et P.

Tout intervalle de R de longueur > 1 contient
deux nombres qui diffèrent par un entier. (2.3)

3. UN THÉORÈME DE MINKOWSKI.

G.D. Birkhoff [1] a généralisé (2.3) comme suit.

THÉORÈME 1. Si $A \subset R^n$ *possède une mesure* n*-dimensionnelle* (i.e. A *n'est pas trop pathologique, alors*

$$\text{mesure de } A > 1 \Longrightarrow \exists\, a \in A\ \exists\, a' \in A:\ a - a' \in Z^n \text{ et } a \neq a'. \tag{3.1}$$

Ce théorème revient à dire que lorsque la mesure d'un ensemble A dans R^n est "assez grande", alors l'ensemble contient deux points a et a' qui diffèrent, composante par composante, par des nombres entiers.

Démonstration. Soit $z = (z_1, \ldots, z_n) \in Z^n$ et considérons le "cube" $K = \{x \mid x = (x_1, \ldots, x_n) \text{ et } z_i \leqslant x_i < z_i + 1, \text{ pour } i = 1, \ldots, n\}$.

Considérons A^z défini comme suit:

$$A^z = A \cap K = \{x \in A \mid x = (x_1, \ldots, x_n) \text{ et } z_i \leqslant x_i < z_i + 1 \text{ pour } i = 1, \ldots, n\}.$$

Posons $A^z{}_{-z} = A^z - z = \{y \mid y = x - z \text{ pour un } x \in A^z\}$. Alors, évidemment, $A^z{}_{-z} \subset [0, 1)^n = \{x \mid 0 \leqslant x_i < 1 \text{ pour } i = 1, \ldots, n\}$. Soit M_z = mesure de $A^z{}_{-z}$ = mesure de A^z. On a $\sum_{z \in Z^n} M_z \neq$ mesure de $A > 1$ par hypothèse. Comme le cube unité $[0,1)^n$ a une mesure égale à 1, on en déduit que deux ensembles $A^z{}_{-z}$ et $A^{z'}{}_{-z'}$, se coupent lorsque z' et $z \neq z'$ sont à coordonnées entières. En d'autres termes, il existe des éléments $a \in A^z$ et $a' \in A^{z'}$ tels que $a - z = a' - z'$, ce qui revient à dire (puisque $A^z \subset A$ et $A^{z'} \subset A$) que

$$\exists\, a \in A \quad \exists\, a' \in A:\ a - a' = z - z' \in Z^n.$$

C.Q.F.D.

Rappelons ici deux définitions concernant les parties de R^n.

DÉFINITION. *Une partie* $A \subset R^n$ *est appelée convexe ssi* $(a \in A, a' \in A, t \in [0, 1]) \Longrightarrow (ta + (1 - t)\, a' \in A)$.

DÉFINITION *Une partie* $A \subset R^n$ *est appelée symétrique* (par rapport à O) *ssi* $a \in A \Rightarrow -a \in A$.

Un très élégant théorème de Minkowski [4] s'énonce alors comme suit:

THÉORÈME 2. (Minkowski). *Si* $A \subset R^n$ *est convexe et symétrique de mesure* $M > 2^n$, *alors* A *contient au moins un point de* Z^n *autre que* $(0, 0, \ldots, 0)$.

Démonstration. Considérons l'ensemble $\frac{1}{2}A = \{\frac{1}{2}x \mid x \in A\}$. On a alors évidemment: mesure de $\frac{1}{2}A = M/2^n > 1$. Le théorème 1 nous assure donc l'existence de deux points a et a' distincts éléments de $\frac{1}{2}A$ tels que $a - a' = w \in Z^n$. Comme $\frac{1}{2}A$ est convexe et symétrique (car A l'est), on déduit que $\frac{1}{2}a - \frac{1}{2}a' = \frac{1}{2}w \in \frac{1}{2}A$. Donc $w \in A$ et $w \neq 0$, car $a \neq a'$.

C.Q.F.D.

4. APPLICATIONS

Le théorème de Minkowski a plusieurs applications en théorie des nombres (voir [2], [3], et [5]). Nous donnerons ici une application immédiate (aux inégalités diophantiennes) dont la solution est laissée au lecteur qui connait l'algèbre linéaire. De toute façon on peut en trouver la démonstration dans [2, pp. 101-104].

Remarquons que la disposition des sièges à la Place des Arts a été résolue *en partie* par des solutions d'inégalités diophantiennes (inégalités dont les solutions sont des entiers).

DÉFINITION. *Soit* $L: R^n — R^n$ *une transformation linéaire non dégénérée* (i.e. $|L|$ = déterminant de $L \neq 0$). *L'ensemble* $\Lambda = L(Z^n)$ *des images des points à coordonnées entières est appelé RÉSEAU associé à L de déterminant* $|L|$.

THÉORÈME 3. Soit Λ *un réseau de* R^n *de déterminant* $|L| \neq 0$. *Alors tout ensemble convexe et symétrique* P *de mesure* $V > 2^n |L|$ *contient au moins un point de* Λ *différent de* $(0, 0, \ldots, 0)$.

Remarque. Il est facile de vérifier que si on suppose aussi P fermé, on peut restreindre la condition $V > 2^n |L|$ à $V \geqslant 2^n |L|$.

Bibliographie

[1] BLICHFELD, Trans. Amer. Math. Soc., 15 (1914), p. 230.

[2] CHANDRASEKHARAN, *Introduction to Analytic Number Theory,* Springer-Verlag, N.Y., 1968.

[3] G. H. HARDY and E. M. WRIGHT, *Introduction to the theory of numbers,* 4th ed., Clarendon Press, Oxford.

[4] H. MINKOWSKI, Gesammelte Abhanlungen, i, 264, 1891.

[5] P. SAMUEL, *Théorie algébrique des Nombres,* Collection Méthodes, Hermann, Paris.