Nous baptiserons ainsi un théorème dont l'énoncé, d'une grande simplicité, est le suivant :

Théorème 1. *Si l'intérieur d'un carré du plan est recouvert par p triangles de même aire ne se chevauchant pas, alors p est pair.*

Nous le devons au mathématicien américain Paul Monsky, qui le démontra en utilisant les résultats, dus à Sperner, sur la triangulation des domaines plans.

Ce théorème est surprenant, et l'étrange simplicité de son énoncé ne devrait pas masquer sa complexité. En effet, il allie deux informations apparemment éloignées, l'une de nature topologique (le recouvrement du carré en triangles) et l'autre de nature métrique (les triangles ont la même aire), pour en déduire une conclusion de nature arithmétique : le nombre de triangles est pair ! On imagine alors la nécessité d'avoir recours à des arguments non triviaux, à l'intersection de trois domaines des mathématiques. Effectivement, nous verrons que la preuve combine des raisonnements combinatoires topologiques sur les coloriages des pavages du plan et des outils algébriques plutôt évolués, à savoir des éléments de la théorie des **valuations**.

Nous aurions pu admettre les pré-requis algébriques et aller directement à la cible, à savoir la démonstration des théorèmes de Sperner et de Monsky. Mais c'eût été refuser ce que nous offre aussi ce théorème, à savoir un bon prétexte pour faire un peu d'algèbre. Nous avons donc fait le choix inverse : nous donnerons tout ce qui est utile, avec les preuves les plus importantes, ceci avant d'aborder les questions géométriques. Les lecteurs à l'aise sur la théorie des valuations pourront omettre les pré-requis d'algèbre et commencer directement la lecture des très amusants résultats de Sperner sur les colorations des triangulations, et la merveilleuse application par Paul Monsky à la démonstration du théorème de Même aire, p pair .

1 Valuations et Anneaux de Valuations.

1.1 Les Valuations et le problème du prolongement.

Soit $(\Gamma, +)$ un groupe abélien. On suppose qu'il existe une partie non vide de Γ, notée ici Γ_+ telle que :

- Γ_+ est stable pour l'addition,
- Γ est union disjointe de Γ_+ de $\{0\}$ et de $-\Gamma_+$.

Cette dernière partie sera simplement notée Γ_- c'est l'ensemble des éléments négatifs du groupe. On définit alors une relation d'ordre total compatible avec l'addition en posant :

$$x > y \text{ si et seulement si } x - y \in \Gamma_+.$$

Par la suite on adjoindra aux groupes ordonnés un élément **maximal** pour la relation d'ordre et **absorbant** pour la loi $+$, qui sera noté ∞. Pour tout $x \in \Gamma$, $x < \infty$.

Cette notion permet de définir la notion de valuation sur un corps de la manière générale suivante :

Définition 2. *Soit K un corps, et Γ un groupe abélien totalement ordonné. On appelle* valuation *sur K à valeurs dans Γ une application $\nu : K \longrightarrow \Gamma \cup \{\infty\}$ vérifiant :*

- $\nu(x \cdot y) = \nu(x) + \nu(y)$
- $\nu(x + y) \geqslant \inf\{\nu(x); \nu(y)\}$
- $\nu(0) = \infty, \nu(1) = 0$

Par exemple, les valuations classiques sur le corps des rationnels $\mathbb{Q}$ sont les valuations p-adiques ν_p. Pour tout nombre premier p, elles sont définies de la manières suivante : $\nu_p(x) = n$ ssi le nombre rationnel non nul x s'écrit $x = p^n\, a/b$ où a et b sont des entiers relatifs premiers à p. Ici, le groupe abélien totalement ordonné Γ coïncide avec $\mathbb{Z}$ muni de son ordre naturel. Les valuations p-adiques mesurent l'ordre de factorisation par p d'un rationnel et satisfont aux conditions générales mentionnées plus haut. Outre son caractère illustratif, la valuation 2-adique ν_2 jouera dans la démonstration du Théorème de Sperner-Monsky un rôle majeur. Plus précisément, nous aurons besoin de l'existence d'un prolongement au corps des réels $\mathbb{R}$ de la valuation ν_2. Mathématiquement cela signifie l'existence d'une valuation $\nu\colon \mathbb{R} \to \Gamma$ avec une inclusion $\mathbb{Z} \to \Gamma$ compatible avec les ordres des deux groupes, tel que le diagramme suivant commute :

$$\begin{array}{rccc} \nu\colon & \mathbb{R} & \longrightarrow & \Gamma \\ & \uparrow & & \uparrow \\ \nu_2\colon & \mathbb{Q} & \longrightarrow & \mathbb{Z} \end{array}.$$

Il est important de remarquer que ce problème du prolongement n'a aucun caractère d'évidence. En effet, quand on regarde le développement en base 2 d'un nombre réel non nul :

$$x = \sum_{n \geqslant k} a_n \frac{1}{2^n} \text{ avec } a_n \in \{0;1\} \text{ et } a_k = 1,$$

une telle série converge pour la topologie réelle, mais elle est a priori totalement divergente pour la topologie 2-adique ! En effet, pour n grand , $1/2^n$ est grand pour la topologie 2-adique ! Il serait donc illusoire de songer à prolonger ν_2 à $\mathbb{R}$ en utilisant la densité naturelle des rationnels. De façon plus explicite, la suite $x_n = 1 + 1/2^n$ tend vers 1 dans $\mathbb{R}$, mais $\nu(x_n) = -n$ tend vers $-\infty$ alors que $\nu_2(1) = 0$! Par ailleurs, remarquons ce qui peut à priori choquer l'intuition à savoir, qu'ici le groupe des valeurs Γ doit contenir $\mathbb{Q}$. En effet pour tous n et k dans $\mathbb{N}$, on a $x^n = 2$ avec $x = \sqrt[n]{2}$ donc

$$\nu(x^k) = k/n.$$

Pour résoudre ce problème, il nous faudra donc avoir recours à d'autres arguments, à savoir la notion algébrique d'anneau de valuation que nous présentons maintenant dans un contexte algébrique général.

1.2 Les Anneaux de Valuation.

Si ν est une valuation d'un corps commutatif K comme précédemment, nous lui associons les sous-ensembles de K suivants :

- $R_\nu = \{x \in K \,|\, \nu(x) \geqslant 0\}$;
- $m_\nu = \{x \in K \,|\, \nu(x) > 0\}$;
- $\mathcal{U}(R_\nu) = \{x \in K \,|\, \nu(x) = 0\}$.

Afin de préciser les propriétés de ces ensembles, nous rappelons brièvement quelques notions d'algèbre commutative. Soit $(A, +, \cdot)$ un anneau, I une partie de A. Dire que I est un **idéal** de A, c'est dire que I est un sous-groupe additif de A et qu'il est stable par la multiplication par tous les éléments de A. Ainsi, $\{0\}$ et A sont des idéaux. Si x est un élément de A, $A \cdot x$ (ensemble des produits $a \cdot x$, où a parcourt A) est un idéal, que nous noterons (x), appelé **idéal engendré par x**. Si x est inversible, on a $(x) = A$, donc si I est un idéal **strict** (c'est-à-dire distinct de A), I est inclus dans l'ensemble des éléments non inversibles de A.

Un idéal strict est dit **maximal** si le seul idéal qui le contienne est l'anneau A lui-même. Le lemme de Zorn assure que tout idéal strict est contenu dans un idéal maximal. A propos des idéaux maximaux, on appelle **anneau local**, un anneau vérifiant les conditions du résultat suivant :

Proposition 3. *Soit A un anneau. Il y a équivalence entre :*

i. A a un seul idéal maximal

ii. L'ensemble des éléments non inversibles de A est un idéal.

Démonstration. Comme tout idéal strict est contenu dans l'ensemble des éléments non inversibles, $(ii) \Rightarrow (i)$ est évident. L'implication inverse l'est à peine moins : en effet, comme tout élément non inversible est contenu dans un idéal maximal, et qu'un idéal strict ne peut contenir d'élément inversible, s'il n'y a qu'un idéal maximal, c'est que l'ensemble des éléments non inversibles en est un. □

Exemple 4. Un idéal I d'un anneau A est dit **premier** si : $x, y \in I \Rightarrow x \in I$ ou $y \in I$. Soit A un anneau et $\mathfrak{p}$ un idéal premier. Soit $S = A \backslash \mathfrak{p}$ le complémentaire de $\mathfrak{p}$ dans A, S est une partie stable pour la multiplication. Le **localisé** de l'anneau A en $\mathfrak{p}$ est l'anneau $S^{-1} \cdot A$, aussi noté $A_{\mathfrak{p}}$; on le construit exactement de la même manière que le corps des fractions de A en ce ne considérant cependant que les fractions à dénominateurs dans S. Cet anneau est local d'idéal maximal $S^{-1} \cdot \mathfrak{p} = \mathfrak{p} \cdot A_{\mathfrak{p}}$. (preuve très facile, laissée à titre d'exercice).

Avec ces notions, le lien entre les valuations et l'algèbre commutative est donné par :

Proposition 5. *Si ν: $K \to \Gamma$ est une valuation d'un corps K, alors R_ν, est un anneau local, d'idéal maximal m_ν possédant les propriétés suivantes.*

i. Pour tout $x \in K$, x ou $1/x$ appartient à R_ν.

ii. Un élément de R_ν est inversible dans R_ν ssi il appartient au groupe des unité $\mathcal{U}(R_\nu)$.

iii. l'application ν induit une bijection du groupe multiplicatif : $K^*/\mathcal{U}(R_\nu)$ sur le sous groupe des valeurs $\nu(K^*)$ de $(\Gamma, +)$.

Par ailleurs, pour tous x et y dans K, si $\nu(x) \neq \nu(y)$ alors, $\nu(x+y) = \inf\{\nu(x); \nu(y)\}$.

On dit que R_ν est **l'anneau de la valuation ν.**

Avant de démontrer ce résultat un peu formel, nous l'illustrons pour les valuations p-adiques $\nu = \nu_p$ de $\mathbb{Q}$. Ici $R_\nu = \mathbb{Z}_{(p)}$ est le localisé de $\mathbb{Z}$ en l'idéal premier $(p) = p\,\mathbb{Z}$. L'idéal maximal m_ν de R_ν est constitué des fractions factorisables par p au numérateur et de dénominateur premier à p. Quand au groupe des unités, c'est l'ensemble des fractions non nulles dont les numérateurs et dénominateurs sont premiers à p. Ainsi, chaque classe $\bar{x} \in \mathbb{Q}^*/\mathcal{U}(R_\nu)$ est-elle caractérisée par l'unique entier relatif $n \in \Gamma = \mathbb{Z}$, tel que $\bar{x}$ puisse être écrit $\bar{x} = \overline{(p^n)}$ modulo $\mathcal{U}(R_\nu)$.

Démonstration. Il est clair d'abord que $\forall x \in K^*$ $\nu(\frac{1}{x}) = -\nu(x)$. Donc si $x \notin R_\nu$ $\nu(x) < 0$, et alors $\nu(\frac{1}{x}) > 0$, donc $\frac{1}{x} \in R_\nu$. La réciproque est claire, ce qui démontre (i). Un élément $x \in R_\nu$ est inversible dans R_ν ssi $\nu(x) \geqslant 0$ et $\nu(\frac{1}{x}) = -\nu(x) \geqslant 0$ donc ssi $\nu(x) = 0$ ce qui prouve le deuxième point. Enfin, il est clair que 0 est le seul élément de K de valuation infinie, et que $\mathcal{U}(R_\nu)$ est le noyau de ν, laquelle est par définition un morphisme de groupes, ce qui prouve le troisième point. Démontrons maintenant la propriété donnée en dernier lieu. On a déjà, par définition,

$$\nu(x+y) \geqslant \inf\{\nu(x); \nu(y)\}.$$

Supposons $\nu(x) > \nu(y)$. On a alors $x = a \cdot y$ avec $\nu(a) = \nu(x/y) = \nu(x) - \nu(y) > 0$. Ainsi, $x + y = (1+a) \cdot y$, donc $\nu(x+y) = \nu(y) + \nu(1+a)$. Or $a \in m_\nu$ (car $\nu(a) > 0$) donc $1 + a \notin m_\nu$ car sinon on aurait $1 \in m_\nu$ ce qui est impossible. Puisque $1 + a \in A$, cet élément est inversible dans A et donc $\nu(1+a) = 0$. D'où l'égalité voulue. □

Nous allons maintenant faire le chemin inverse, en montrant comment l'on peut, d'un anneau adéquat, remonter à une valuation. La clef de ce procédé réside dans le résultat suivant :

Proposition 6. *Soit V un anneau contenu dans un corps K. Les conditions suivantes sont équivalentes.*

i. Pour tout $x \in K$ si $x \notin V$ alors $1/x \in V$.

ii. K est le corps des fractions de V et l'ensemble des idéaux de V est totalement ordonné par la relation d'inclusion.

Dans ce contexte, V est un anneau local d'idéal maximal $m_V = V \backslash \mathcal{U}(V)$, le groupe multiplicatif $\Gamma = K^*/\mathcal{U}(V)$ est totalement ordonné par l'ordre $\bar{x} \leqslant \bar{y}$ ssi $y/x \in V$. Enfin, l'application naturelle $\nu : K^* \to K^*/\mathcal{U}(V)$ induit une valuation de K pour laquelle $R_\nu = V$.

On dit qu'un tel anneau est un **anneau de valuation** de K.

Démonstration. D'abord $(i) \Rightarrow (ii)$. Le lecteur montrera facilement l'identité de K et du corps des fractions de V. Soient maintenant deux idéaux stricts de V, I et J. Supposons l'existence de $x \in I, x \notin J$. Soit un y quelconque dans J. Supposons $x \cdot y^{-1} \in V$. Alors $x \cdot y^{-1} \cdot y \in J$ ce qui implique $x \in J$ ce qui est contraire à l'hypothèse. Donc $x^{-1} \cdot y \in V$ et alors $x \cdot x^{-1} \cdot y \in I$ et donc $y \in I$. On a donc $J \subset I$.

Montrons maintenant l'implication inverse. Le seul type d'élément du corps des fractions de V qui pose problème est de la forme $x = a/b$ avec a et b non inversibles dans V. Considérons les idéaux engendrés (a) et (b). Ces idéaux sont stricts puisque a et b sont non inversibles dans V. On a alors $(a) \subset (b)$ ou $(b) \subset (a)$. Dans le premier cas il existe $k \in V$ tel que $a = k \cdot b$ et alors

$$x = a/b = k \in V.$$

Dans le second cas, le même raisonnement conduit à $1/x \in V$. (Nous laissons le reste au lecteur, qui n'aura aucun mal à transporter dans les notations multiplicatives naturelles au groupe $K^*/\mathcal{U}(V)$ les définitions données plus haut dans des notations additives). □

C'est cette construction qui nous permettra de résoudre le problème du prolongement évoqué plus haut en le remplaçant par un problème d'extension d'anneaux de valuations. En convenant de dire que deux valuations sur un même corps K sont **équivalentes** ssi elles ont le même anneau de valuation, dans la quatrième partie de ce texte, nous démontrerons le résultat général suivant :

Théorème 7. *Soit ν une valuation sur K, et $K \hookrightarrow L$ une extension de K. Alors il existe une valuation sur L dont la restriction à K est équivalente à ν.*

2 Les Triangulations Colorées de Sperner

Définition 8. *Nous appellerons coloration de $\mathbb{R}^2$ en trois couleurs $\mathfrak{A}$, $\mathfrak{B}$, et $\mathfrak{C}$ une application $\mathbb{R}^2 \longrightarrow \{\mathfrak{A}, \mathfrak{B}, \mathfrak{C}\}$ telle que trois points alignés ne puissent être tricolores.*

Considérons alors une ligne polygonale fermée F. Nous appellerons **arête de type XY** une arête dont les extrémités sont de couleurs X et Y. On a alors le résultat suivant du à Sperner :

Théorème 9. *Si la ligne polygonale contient un nombre impair d'arêtes $\mathfrak{AB}$ alors, toute triangulation de la région délimitée par F contient au moins un triangle tricolore.*

Une arête de la triangulation sera dite **élémentaire** si entre ses extrémités il n'y a pas d'autres sommets de la triangulation. Le lemme suivant relie le nombre d'arêtes élémentaires aux emplacements des couleurs :

Lemme 10. *Dans une triangulation de la région polygonale F,*

i. Une arête de type $\mathfrak{AB}$ contient un nombre impair d'arêtes élémentaires de type $\mathfrak{AB}$. Les autres types d'arêtes contiennent un nombre pair d'arêtes élémentaires de type $\mathfrak{AB}$.

ii. Seuls les triangles tricolores contiennent un nombre impair d'arêtes élémentaires de type $\mathfrak{AB}$.

Démonstration. (i) Parmi les six types possibles d'arêtes : $\mathfrak{AB}$; $\mathfrak{AA}$; $\mathfrak{BB}$; $\mathfrak{AC}$; $\mathfrak{BC}$; $\mathfrak{CC}$, seuls les trois premiers types peuvent contenir des arêtes élémentaires de type $\mathfrak{AB}$ puisqu'il ne peut exister de points alignés de trois couleurs. Pour ces trois types nous raisonnons par récurrence sur le nombre n d'arêtes élémentaires constituant le segment. Pour $n = 1$ il n'y a rien à dire. Si $n \geqslant 2$, écrivons l'arête XY sous la forme $XZ\cdots Y$ où XZ est la première arête élémentaire succédant à X autrement dit, ZY est composée de $n-1$ arêtes élémentaires. Le tableau suivant où $f(UV)$ désigne le nombre d'arêtes élémentaires de type $\mathfrak{AB}$ dans le segment UV, résume la situation car à chaque fois $f(XZ) + f(ZY) = f(XY)$.

X	Z	Y	$f(XZ)$	$f(ZY)$	$f(XY)$
$\mathfrak{A}$	$\mathfrak{A}$	$\mathfrak{B}$	0	$2\mathbb{N}+1$	$2\mathbb{N}+1$
$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{B}$	1	$2\mathbb{N}$	$2\mathbb{N}+1$
$\mathfrak{A}$	$\mathfrak{A}$	$\mathfrak{A}$	0	$2\mathbb{N}$	$2\mathbb{N}$
$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{A}$	1	$2\mathbb{N}+1$	$2\mathbb{N}$
$\mathfrak{B}$	$\mathfrak{A}$	$\mathfrak{B}$	1	$2\mathbb{N}+1$	$2\mathbb{N}$
$\mathfrak{B}$	$\mathfrak{B}$	$\mathfrak{B}$	0	$2\mathbb{N}$	$2\mathbb{N}$

(ii) Si le triangle ABC est de couleur $\mathfrak{ABC}$, le nombre d'arêtes élémentaires qu'il contient est

$$f(AB) + f(BC) + f(CA) = f(AB).$$

D'après (i) ce nombre est impair. Les cas des triangles bi- et mono-colores se traite de la même façon. □

Nous pouvons maintenant donner la preuve du Théorème de Sperner.

Démonstration. Notons $\mathcal{B}$ le nombre d'arêtes élémentaires $\mathfrak{AB}$ de la triangulation qui sont inclues dans le bord de la ligne F, et $\mathcal{I}$ le nombre d'arêtes élémentaires de type $\mathfrak{AB}$ de la triangulation contenues dans l'intérieur du domaine délimité par F. En parcourant la triangulation en comptant chaque arête autant de fois qu'elle est le coté d'un triangle, le nombre total $\mathcal{T}$ d'arêtes élémentaires de type $\mathfrak{AB}$ est donné par la formule :

$$\mathcal{T} = \mathcal{B} + 2\mathcal{I}.$$

Et ceci, puisque chaque arête élémentaire intérieure au domaine est côté de deux triangles et donc comptée deux fois.

Par ailleurs, Chaque arête de type $\mathfrak{AB}$ du bord de F contient un nombre impair d'arêtes élémentaires du même type d'après le lemme. Ainsi puisque le bord contient un nombre impair d'arêtes de type $\mathfrak{AB}$, le nombre $\mathcal{B}$ est impair. (Une somme impaire d'entiers impairs est impaire). Ainsi $\mathcal{T}$ est impair.

Nous allons maintenant pouvoir conclure. $\mathcal{T}$ est la somme du nombre d'arêtes élémentaires $\mathfrak{AB}$ des triangles (toujours comptées autant de fois qu'elles sont arêtes d'un triangle, c'est-à-dire 1 ou 2). Si tous les triangles étaient bi- ou mono-colores, ils contiendraient tous un nombre **pair** d'arêtes élémentaires $\mathfrak{AB}$ donc $\mathcal{T}$ serait pair. Donc il y a au moins un (en fait, un nombre impair) de triangles tricolores. □

3 Le Théorème de Monsky

Rappelons son énoncé : on considère un carré du plan triangulé en p triangles de même aire. Alors p est pair. Pour le démontrer, l'idée est de définir ici un coloriage du plan satisfaisant aux conditions de Sperner. Ceci se fait en utilisant les valuations de la façon suivante : D'après le Théorème 7, soit ν une valuation de $\mathbb{R}$ qui prolonge la valuation 2-adique de $\mathbb{Q}$. Son groupe des valeurs Γ contient $\mathbb{Z}$ comme sous groupe ordonné.

Définition 11. *On construit un coloriage tricolore du plan de la manière suivante :*

$$\begin{array}{lcl} \{(x,y), \nu(x) > \nu(y) \text{ et } \nu(y) \leqslant 0\} & \longmapsto & \mathfrak{A} \\ \{(x,y), \nu(y) \geqslant \nu(x) \text{ et } \nu(x) \leqslant 0\} & \longmapsto & \mathfrak{B} \\ \{(x,y), \nu(x) > 0 \text{ et } \nu(y) > 0\} & \longmapsto & \mathfrak{C} \end{array}.$$

(Par la suite, nous confondrons par une même lettre les couleurs et les ensembles porteurs des couleurs).

Proposition 12. *Ce coloriage satisfait les conditions de la définition 8 en vertu des propriétés suivantes :*

i. Le sous ensemble $\mathfrak{C}$ *est un sous-groupe de* $(\mathbb{R}^2;+)$.

ii. On a les inclusions $\mathfrak{C}+\mathfrak{A}\subset\mathfrak{A}$ *et* $\mathfrak{C}+\mathfrak{B}\subset\mathfrak{B}$

iii. Trois points alignés ne peuvent être tricolores.

Démonstration. (*i*) En effet en notant $\mathfrak{m}=m_\nu$ l'idéal maximal de l'anneau de la valuation ν, on a par définition :

$$\mathfrak{C}=\mathfrak{m}\times\mathfrak{m}.$$

(*ii*) En utilisant la propriété si $\nu(x)\neq\nu(y)$, alors $\nu(x+y)=\inf\{\nu(x);\nu(y)\}$ démontrée à la Proposition 5, ceci est une conséquence des définitions.

(*iii*) Supposons A,B,C respectivement de couleurs $\mathfrak{A},\mathfrak{B},\mathfrak{C}$ et alignés. Par translation par $-C$ (qui respecte les couleurs, d'après (*ii*)), on se ramène au cas où $C=O$. Bien entendu, l'origine O est de couleur $\mathfrak{C}$ puisque $\nu(0)=\infty$. Il existe alors $\lambda\in\mathbb{R}^*$ tel que $x_B=\lambda.x_A$ et $y_B=\lambda.y_A$. Mais alors $\nu(x_B)=\nu(\lambda)+\nu(x_A)$ et $\nu(y_B)=\nu(\lambda)+\nu(y_A)$. Ainsi, $\nu(x_B)-\nu(y_B)=\nu(x_A)-\nu(y_A)$. Or $\nu(x_B)-\nu(y_B)\leqslant 0$ et $\nu(x_A)-\nu(y_A)>0$. On aboutit à une impossibilité. □

Proposition 13. *Le carré* $(0,0),(1,0),(1,1),(0,1)$ satisfait aux conditions de Sperner.

En effet, en se souvenant que $\nu(1)=0<\nu(0)=\infty$, le coloriage des sommets du carré unité est tricolore en vertu du dessin suivant :

$$\begin{array}{ccc}\mathfrak{A} & — & \mathfrak{B}\\ | & & |\\ \mathfrak{C} & — & \mathfrak{B}\end{array}.$$

Proposition 14. *La surface du domaine délimité par un triangle tricolore est de valuation strictement négative.*

Démonstration. Par translation on se ramène encore au cas O, A, B avec la convention adoptée plus haut. Nommons T le domaine délimité par le triangle $O\,A\,B$ et $\mathcal{A}(T)$ son aire. Au signe près (ce qui n'a aucune importance car nous allons prendre la valuation) on a :

$$\mathcal{A}(T)=\frac{1}{2}\begin{vmatrix}x_A & x_B\\ y_A & y_B\end{vmatrix}=\frac{1}{2}\cdot(x_A.y_B-x_B.y_A).$$

Or $\nu(x_A)>\nu(y_A)$ et $\nu(y_B)\geqslant\nu(x_B)$. Ainsi,

$$\nu(x_A\cdot y_B)=\nu(x_A)+\nu(y_B)>\nu(y_A)+\nu(x_B)=\nu(y_A\cdot x_B).$$

Donc d'après la Proposition 5,

$$\begin{aligned}\nu(\mathcal{A}(T) &= \nu(1/2)+\inf\{\nu(x_A\cdot y_B);\nu(y_A\cdot x_B)\}\\ &= \nu(1/2)+\nu(y_A)+\nu(x_B).\end{aligned}$$

Ainsi, $\nu(\mathcal{A}(T))$ est strictement négatif puisque $\nu(1/2)=-1$, $\nu(y_A)\leqslant 0$ et $\nu(x_B)\leqslant 0$ dans Γ. □

Nous sommes enfin en mesure de terminer la :

Démonstration. du Théorème 1. On triangule le carré unité en p triangles d'aire commune :

$$\mathcal{A}=1/p.$$

D'après les Propositions 12 et 13 le coloriage de cette triangulation satisfait aux conditions du théorème de Sperner (Théorème 9). Donc il existe au moins un triangle tricolore. D'après la Proposition 14, on a donc

$$\nu(\mathcal{A})=\nu(1/p)=-\nu(p)<0$$

Donc $\nu_2(p) = \nu(p) > 0$ ce qui signifie que p est pair puisque la valuation ν coïncide avec la valuation 2-adique sur $\mathbb{Z}$. □

4 Prolongement des Valuations

Nous allons maintenant démontrer le Théorème 7. Si nous nous fixons pour règle de ne rien admettre, il nous faut accumuler pas mal de matériel.

4.1 Modules

La notion de module M sur un anneau commutatif A est une généralisation de la notion d'espace vectoriel sur un corps. Autrement dit, M est un groupe abélien constitué de vecteurs lesquels peuvent être multipliés selon les règles habituelles par les scalaires appartenant à A. En particulier, pour tout $m \in M$, $1 \cdot m = m$ et $0 \cdot m = 0$ l'élément neutre de M. Par analogie avec les espaces vectoriels, on définit de même les sous modules les modules quotients et les modules de type finis. Précisément, un module M est de type fini si et seulement si il existe une famille finie S de M telle que tout élément $m \in M$ puisse être calculé comme une combinaison linéaire à coefficients dans A des éléments de S.

Ce qui rend la théorie des modules plus complexe que celle des espaces vectoriels est l'absence à priori de base d'un module ! Et ceci même pour les modules de type finis. En effet, par exemple, prenons $A = \mathbb{Z}$ et $M = \mathbb{Z}/n\,\mathbb{Z}$, pour tout $x \in M$,

$$n \cdot x = \hat{0}.$$

Autrement dit M n'est pas fidèle conformément à la définition donnée plus bas. Par conséquent, bien que M soit engendré par la partie $S = \{\hat{1}\}$, cette famille n'est pas une base car aucun élément du module ne peut être écrit de manière unique sous la forme $m = k \cdot \hat{1}$ avec $k \in \mathbb{Z}$. Cependant il existe des modules admettant des bases. On dit alors que ce module est libre. Par exemple tout idéal d'un anneau principal est libre. Penser encore à $A = \mathbb{Z}$ et $I = n\,\mathbb{Z}$ par exemple.

4.2 Déterminants sur les modules

La théorie des déterminants des matrices à coefficients dans un corps commutatif se généralise pour les matrices à coefficients dans un anneau commutatif A de la façon suivante : En copiant les formules classiques, il existe une application déterminant :

$$\det : M_n(A) \longrightarrow A,$$

dont la valeur est 1 sur la matrice unité I_n. Pour toute matrice B de taille $n \times n$ à coefficients dans B, si $\tilde{B}$ est la transposée de la comatrice de B on a la relation de Cramer :

$$\tilde{B} \cdot B = \det(B) \cdot I_n.$$

On en déduit donc facilement le lemme suivant, important pour la suite :

Lemme 15. *Soit M un A-module; $w_1, ..., w_n$ des éléments de F; et $B = (b_{i,j})$ une matrice $n \times n$ à coefficient dans A. Supposons que pour tout $i \in 1, ...n$ $b_{i,1} \cdot w_1 + ... + b_{i,n} \cdot w_n = v_i$. Alors*

$$\det(B) \cdot \begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ w_n \end{pmatrix} = \tilde{B} \cdot \begin{pmatrix} v_1 \\ \cdot \\ \cdot \\ v_n \end{pmatrix}.$$

En particulier, si tous les v_i sont nuls, alors pour tout i, $\det(B).w_i = 0$. Si la famille des w_i engendre F, on a enfin : $\det(B) \cdot F = \{0\}$.

Rien ne permet à ce point d'en déduire que $\det(B) = 0$. Cette observation motive la :

Définition 16. *On dit qu'un A-module F est* fidèle *si $(a \in A, a.F = \{0\}) \Rightarrow (a = 0)$. En particulier un anneau A considéré comme A-module est fidèle (il contient l'unité!).*

Théorème 17. *(Lemme de Nakayama) Soit A un anneau commutatif, $\mathfrak{b}$ un idéal de A contenu dans tous ses idéaux maximaux. Soit M un A-module de type fini. On note $\mathfrak{b}\cdot M$ l'ensemble des sommes $b_1\cdot x_1+....+b_n\cdot x_n$ avec les $b_i\in\mathfrak{b}$, et les $x_i\in M$. C'est un sous-module de M. Si $\mathfrak{b}\cdot M=M$ alors $M=\{0\}$*

Démonstration. Puisque M est de type fini, soient w_1, ..., w_n une famille génératrice de M. L'égalité $M=\mathfrak{b}\cdot M$ s'écrit encore

$$M=\mathfrak{b}\cdot w_1+\cdots+\mathfrak{b}\,w_n.$$

Ainsi en particulier chaque w_i peut-il s'écrire comme une combinaison linéaire des w_j à coefficients dans $\mathfrak{b}$. Il existe donc une matrice $B\in M_n(\mathfrak{b})$ telle que

$$\begin{pmatrix} w_1\\ .\\ .\\ w_n\end{pmatrix}=B\cdot\begin{pmatrix} w_1\\ .\\ .\\ w_n\end{pmatrix}\text{ c'est à dire }(\mathrm{Id}-B)\cdot\begin{pmatrix} w_1\\ .\\ .\\ w_n\end{pmatrix}=\begin{pmatrix} 0\\ .\\ .\\ 0\end{pmatrix}.$$

D'après le lemme 15, cette dernière formule implique

$$\det(\mathrm{Id}-B)\cdot M=\{0\}. \tag{1}$$

Mais en développant ce déterminant on a la relation :

$$\mathrm{Id}-B\equiv\mathrm{Id}\text{ modulo }(\mathfrak{b})\Rightarrow\det(\mathrm{Id}-B)\equiv 1\text{ modulo }(\mathfrak{b}).$$

Autrement dit il existe $b\in\mathfrak{b}$ tel que $\det(\mathrm{Id}-B)=1+b$. Puisque $\mathfrak{b}$ est contenu dans tous les idéaux maximaux de A, $\det(\mathrm{Id}-B)=1+b$ est inversible dans A. En multipliant à gauche l'égalité (1) par $(1+b)^{-1}$, on obtient $1\cdot M=M=\{0\}$. □

Le lecteur peu familier avec les arguments matriciels pourra démontrer le Lemme de Nakayama en raisonnant par récurrence sur le nombre n de générateurs du module.

4.3 Anneaux d'entiers

Proposition 18. *Soit B un anneau, A un sous-anneau de B, et $\alpha\in B$. Les propositions suivantes sont équivalentes :*

i. α est racine d'un polynôme unitaire p à coefficients dans A

ii. L'algèbre $A[\alpha]$ est un A-module de type fini

iii. Il existe un module fidèle M sur l'anneau $A[\alpha]$, qui est aussi un A-module de type fini.

Démonstration. $(i)\Rightarrow(ii)$ Le polynôme $p(X)$ étant unitaire, pour tout $f(X)\in A[X]$ la division Euclidienne de f par p :

$$f(X)=p(X).q(X)+r(X)\text{ avec }\deg(r)<\deg(p)=n,$$

se calcule dans $A[X]$. Cela signifie que $q(x)$ et $r(X)$ appartiennent à $A[X]$. Ainsi, $f(\alpha)=r(\alpha)$ et ceci prouve que l'algèbre $A[\alpha]$ coïncide avec le A-module engendré par $1,\alpha,\alpha^2,....,\alpha^{n-1}$.

$(ii)\Rightarrow(iii)$ $M=A[\alpha]$ lui-même convient.

$(iii)\Rightarrow(i)$ Soit M un module fidèle sur $A[\alpha]$, de type fini sur A. Soit w_1, ..., w_n une famille génératrice de M. De l'inclusion $\alpha.M\subset M$, il existe une matrice $B\in M_n(A)$ telle que

$$\begin{pmatrix}\alpha\,w_1\\ .\\ .\\ \alpha\,w_n\end{pmatrix}=B\cdot\begin{pmatrix} w_1\\ .\\ .\\ w_n\end{pmatrix}\text{ soit encore : }(\alpha\,\mathrm{Id}-B)\cdot\begin{pmatrix} w_1\\ .\\ .\\ w_n\end{pmatrix}=\begin{pmatrix} 0\\ .\\ .\\ 0\end{pmatrix} \tag{2}$$

Le polynôme $D(X)=\det(X\,\mathrm{Id}-B)$ est unitaire à coefficients dans A. D'après le Lemme 15 et l'équation (2), on a $D(\alpha)\cdot M=0$. Mais, comme M est fidèle, $D(\alpha)=0$. On a donc trouvé un polynôme unitaire annulant α. □

Dans les conditions de Proposition 18, α est dit **entier** sur A. Si tout élément de B est entier sur A, on dit que B est **entier** A. Cette notion généralise aux anneaux celle d'élément algébrique sur un corps. Le résultat suivant montre que cette généralisation est légitime.

Théorème 19. *Soit A un sous-anneau de l'anneau C. Les éléments de C entiers sur A forment un sous-anneau de C, dit la* clôture intégrale de $\boldsymbol{A}$ dans $\boldsymbol{C}$.

Démonstration. Soient α et β éléments de C entiers sur A. Soient les A-modules $M = A[\alpha]$ et $N = A[\beta]$. Ces modules sont de type fini (Proposition 18 (*ii*)). Supposons M engendré par une famille $\{v_i\}$, N par une famille $\{w_j\}$. Considérons un élément de $M \cdot N = A[\alpha, \beta]$, soit $\sum x_{i,j} \cdot \alpha^i \cdot \beta^j$. Il suffit de décomposer chaque α^i et chaque β^j sur la famille génératrice correspondante pour voir que la famille des $v_i \cdot w_j$ engendre $A[\alpha, \beta]$, lequel est donc de type fini sur A; par ailleurs, en tant que $A[\alpha.\beta]$-module il est fidèle (il contient l'unité). $\alpha.\beta$ est donc entier sur A, d'après la Proposition 18 (*iii*). Que $\alpha + \beta$ soit entier se vérifie de même. □

Définition 20. *Si A est un anneau intègre identique à sa clôture intégrale dans son corps de fractions, on dit que A est* intégralement clos. *C'est en particulier le cas si A est intègre et factoriel. (comme $\mathbb{Z}$). On a en outre le résultat suivant, qui exprime le fait que la clôture intégrale commute à la localisation :*

Proposition 21. *Soit A un anneau, S une partie multiplicative de A ne contenant pas 0. Si A est intégralement clos, $S^{-1} \cdot A$ aussi.*

Démonstration. Soit α un élément du corps des fractions de A, entier sur $S^{-1} \cdot A$. En appelant $s \in S$ le produit des dénominateurs intervenant dans une relation de dépendance intégrale, on voit que $s \cdot \alpha$ est entier sur A. Or A est intégralement clos, donc $s \cdot \alpha \in A$, donc $\alpha \in S^{-1} \cdot A$. □

Étant donné un anneau A, une $\boldsymbol{A}$**-algèbre** est un anneau qui est aussi un A-module. Exemple : l'anneau des polynômes à n variables sur un anneau A est une A-algèbre. Une sous-algèbre d'une A-algèbre est un sous-anneau stable pour le produit par les éléments de A (donc une partie qui est à la fois un sous-anneau et un sous-module). Une A-algèbre est de type fini quand elle est identique à l'algèbre engendrée par une partie finie.

Proposition 22. *Soit deux anneaux $A \subset B$, B entier sur A et de type fini en tant que A-algèbre (c'est-à-dire $B = A[x_1, ..., x_n]$ pour $x_1, ..., x_n \in B$ fixés). Alors B est de type fini en tant que A-module.*

Démonstration. C'est vrai si $B = A[\alpha]$ par définition d'un élément entier. On termine par récurrence sur le nombre des générateurs $x_1, ..., x_n \in B$ sur A, en se souvenant que $A[x_1, ..., x_n] = A[x_1, ..., x_{n-1}][x_n]$ et que si x_n est entier sur A, il l'est sur $A[x_1, ..., x_{n-1}]$. □

4.4 Le Going − up de Cohen − Seidenberg

Soit un anneau B et A un sous-anneau de B. Soit $\mathfrak{p}$ un idéal premier de A, $\mathfrak{P}$ un idéal premier de B. On dit que $\mathfrak{P}$ **domine** $\mathfrak{p}$ ssi $\mathfrak{P} \cap A = \mathfrak{p}$.

Théorème 23. *(Going-up de Cohen-Seidenberg) Soit un anneau B et A un sous-anneau de B, B entier sur A. Soit $\mathfrak{p}$ un idéal premier de A. Il existe un idéal premier de B qui domine $\mathfrak{p}$.*

Nous avons besoin d'un lemme :

Lemme 24. *Soit A un anneau local, B une extension entière de A, $\mathfrak{p}$ un idéal premier de A. Alors $\mathfrak{p}.B \neq B$*

Démonstration. D'abord il est clair que $\mathfrak{p} \cdot B = B \Leftrightarrow 1 \in \mathfrak{p} \cdot B$. Supposons que $1 \in \mathfrak{p} \cdot B$. On a alors une relation $1 = a_1 \cdot b_1 + ... + a_n \cdot b_n$ avec les a_i dans $\mathfrak{p}$ et les b_i dans B. Considérons alors le sous-anneau de B défini par $B_0 = A[b_1, ..., b_n]$. En tant que A-algèbre, il est de type fini; mais comme tous les b_i sont entiers sur A, il est de type fini en tant que A-module. Or, comme $1 \in \mathfrak{p} \cdot B_0$, $\mathfrak{p} \cdot B_0 = B_0$. Le lemme de Nakayama entraîne que $B_0 = 0$, ce qui est impossible (A étant local, $\mathfrak{p}$ est contenu dans l'unique idéal maximal de A). □

Démonstration. du Théorème du Going-up de Cohen-Seidenberg

Revenons à la démonstration, qui va faire intervenir les localisés de A et B en $\mathfrak{p}$, notés $A_\mathfrak{p}$ et $B_\mathfrak{p}$. Ces anneaux satisfont aux hypothèses du lemme, en particulier $A_\mathfrak{p}$ est local, et son idéal maximal est $m_\mathfrak{p} = \left\{\frac{p}{s}, p \in \mathfrak{p}, s \in A - \mathfrak{p}\right\}$. Il est clair que $\mathfrak{p} \cdot B_\mathfrak{p} = m_\mathfrak{p} \cdot B_\mathfrak{p}$. On a donc, en vertu du lemme, $m_\mathfrak{p} \cdot B_\mathfrak{p} \neq B_\mathfrak{p}$. L'idéal strict $m_\mathfrak{p} \cdot B_\mathfrak{p}$ est donc contenu dans un idéal maximal $\mathfrak{M}$ de $B_\mathfrak{p}$. Considérons le diagramme suivant, où les flèches sont pour les injections canoniques, et pour l'inclusion de A dans B.

$$\begin{array}{ccc} B & \to & B_\mathfrak{p} \\ \uparrow & & \uparrow \\ A & \to & A_\mathfrak{p} \end{array}$$

Comme l'image réciproque d'un idéal maximal par un morphisme est un idéal premier, l'image réciproque de $\mathfrak{M}$ dans B est un idéal premier de B, soit $\mathfrak{P}$. L'image réciproque de $\mathfrak{P}$ dans A est simplement $\mathfrak{P} \cap A$. De l'autre côté, l'image réciproque de $\mathfrak{M}$ dans $A_\mathfrak{p}$ est un idéal contenant $m_\mathfrak{p}$, donc $m_\mathfrak{p}$, puisque celui-ci est maximal. Il est clair enfin que l'image réciproque de $m_\mathfrak{p}$ dans $A_\mathfrak{p}$ est $\mathfrak{p}$. En conclusion, nous avons bien $\mathfrak{P} \cap A = \mathfrak{p}$. □

4.5 Retour aux Anneaux de Valuation

Soit K un corps, A et B deux sous-anneaux de K supposés locaux d'idéaux maximaux respectifs m_A et m_B. Si $A \subset B$ l'ensemble $m_B \cap A$ est un idéal de A. Il est donc contenu dans m_A. On dira que B **domine** A ssi cette inclusion est une égalité. C'est à dire ssi :

$$A \subset B \text{ et } m_A = m_B \cap A.$$

La relation de domination est une relation d'ordre partielle pour les anneaux locaux d'un corps donné. Les éléments maximaux pour cet ordre les anneaux de valuation conformément au :

Théorème 25. *Soit K un corps et A un sous-anneau de K. Il y a équivalence entre (i) et (ii) :*

i. A est l'anneau d'une valuation sur K.

ii. A est un anneau local maximal dans K pour la relation de domination.

Démonstration. $(i) \Rightarrow (ii)$ On sait d'emblée que A est local. Soit B un sous-anneau de K local et dominant A. Soit $x \in B - A$. Alors $x^{-1} \in A$, donc $x^{-1} \in B$. x^{-1} est donc inversible dans B, donc $x^{-1} \notin m_B$. Donc $x^{-1} \notin m_A$. Cela signifie que x^{-1} est donc inversible dans A. Donc

$$x = (x^{-1})^{-1} \in A.$$

Ceci est contradictoire avec l'hypothèse initiale donc $B = A$.

$(ii) \Rightarrow (i)$ Nous allons prouver que, pour tout x de K, $x \in A$ ou $x^{-1} \in A$ ce qui permettra de conclure. Soit donc $x \in K$ (que l'on peut évidemment considérer non nul). Deux cas se présentent :

- Si x entier sur A. Alors $A[x]$ est entier sur A, et on a vu que tout idéal premier de A se relève en un idéal premier de $A[x]$ qui le domine au sens du Théorème 23. Soit donc $\mathfrak{p}$ un idéal premier de $A[x]$ tel que $m_A \subset \mathfrak{p}$. Alors l'anneau localisé $A[x]_\mathfrak{p}$ est un anneau local, son idéal maximal est $\mathfrak{p}$, donc il domine A. Donc $A[x]_\mathfrak{p} = A$ donc $x \in A$.
- Si x n'est pas entier sur A. Alors x^{-1} n'est pas inversible dans le sous-anneau $A\left[x^{-1}\right]$ de K. En effet, sinon, on aurait une égalité de la forme $x = a_0 + a_1.x^{-1} + ... + a_n.x^{-n}$, et en multipliant par x^n on obtiendrait une relation de dépendance intégrale rendant x entier sur A. Donc x^{-1} appartient à un idéal maximal de $A\left[x^{-1}\right]$, soit m. Considérons le morphisme canonique $A \longrightarrow A\left[x^{-1}\right]/m$. Il est surjectif, et donc son noyau $m \cap A$ est un idéal maximal de A, c'est donc m_A. Si nous considérons maintenant l'anneau local $A\left[x^{-1}\right]_m$, dont l'idéal maximal n'est autre que m, nous voyons qu'il domine A. Il est donc égal à A. Or x^{-1} est élément de cet anneau. Donc $x^{-1} \in A$.

Remarquons au passage que nous avons démontré qu'un anneau de valuation était intégralement clos. □

Nous allons enfin pouvoir conclure.

Démonstration. du Théorème 7. Soit A l'anneau de v. A est local et inclus dans L. On vérifie que l'ensemble des anneaux locaux inclus dans L dominant A est inductif pour la relation de domination. Le lemme de Zorn assure de l'existence d'un anneau local B maximal, dominant A. B est alors un anneau de valuation sur L. Soit w une valuation d'anneau B. w restreinte à K est évidemment une valuation sur K, d'anneau $B \cap K$. Mais $B \cap K$ est local et domine A, donc $B \cap K = A$. □

Nous indiquons enfin quelques lectures supplémentaires. L'article original de Paul Monsky est [4]. Le théorème de Sperner connu sous la dénomination de Sperner's Lemma en langue anglaise, peut être lu dans [5] page 151. Une magnifique introduction à la théorie des pavages du plan dans la direction des travaux de Boloai et des invariants de Dehn-Hatzwinger est accessible dans [1]. Robin Hartshorne ne manquant pas d'humour, y donne le théorème de Monsky à titre d'exercice. Par ailleurs sur la base des mêmes idées que le présent texte, Kasimatis dans [2], généralise le théorème de Monsky à tous les polygones réguliers à plus de quatre cotés. Précisément son résultat est le :

Théorème 26. *Si un polygone régulier à n cotés avec $n \geqslant 5$ est recouvert par des triangles de même aire alors, le nombre de triangles est un multiple du nombre de cotés n.*

En ce qui concerne la théorie algébrique des valuations, le texte fondateur est [7]. Des référence plus accessibles au lecteur contemporain sont [6] et [3] dont il existe maintenant une version française parue chez Dunot.

Bibliographie

[1] Robin Hartshorne. Geometry: Euclid and beyond. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2000.

[2] E. A. Kasimatis. Dissections of regular polygons into triangles of equal areas. Discrete Comput. Geom., 4(4):375--381, 1989.

[3] Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.

[4] Paul Monsky. On dividing a square into triangles. Amer. Math. Monthly, 77:161--164, 1970.

[5] Edwin H. Spanier. Algebraic topology. McGraw-Hill Book Co., New York, 1966.

[6] M. Vaquié. Valuations. In Resolution of Singularities, number 181 in Progress in Mathematics, pages 439--590. Birkhauser, Basel, 2000.

[7] O. Zariski and P. Samuel. Commutative Algebra, volume II of The University Series in Higher Mathematics. D. Van Nostrand Company, INC., 1960.