Sur le nombre d'inégalités nécessaires pour définir un ouvert semi-algébrique, d'après Scheiderer et Bröcker

Hsuan-Yu Wang et Aurélien Fourré, encadré par Olivier Benoist

Juin 2024

Table des matières

1 Introduction

Dans ce mémoire, nous allons nous intéresser aux ouverts semi-algébriques basiques.

Définition 1.1 (*ouvert semi-algébrique basique*)

Une partie $\mathcal{U} \subset \mathbb{R}^n$ est dite ouvert semi-algébrique basique *quand il existe $k \in \mathbb{N}$ et $f_1, \dots, f_k \in \mathbb{R}[X_1, \dots, X_n]$ tels que*

$$\mathcal{U} = \{x \in \mathbb{R}^n \mid f_1(x) > 0, \dots, f_k(x) > 0\}.$$

Les polyèdres convexes sont des exemples d'ouverts semi-algébriques basiques, puisqu'ils sont définis comme une intersection finie de demi-espaces, et chaque demi-espaces est l'ensemble des points de $\mathbb{R}^n$ vérifiant une inégalité polynomiale de degré 1.

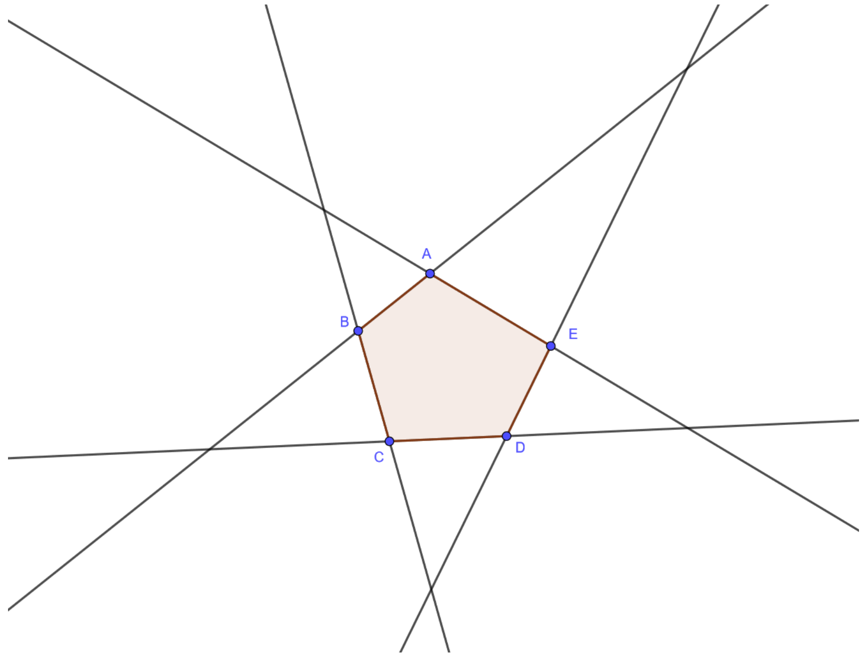

FIGURE 1 – Un exemple d'ouvert semi-algébrique basique, défini par 5 inéquations polynomiales strictes, les polynômes étant de degré 1 et s'annulant sur les droites tracées.

C'est un cas particulier d'ensemble semi-algébrique, c'est-à-dire d'ensemble défini par des équations et inéquations algébriques. Notons qu'un ouvert semi-algébrique n'est en général pas basique. Cependant, tout ouvert semi-algébrique s'écrit comme une union finie d'ouverts semi-algébriques basiques.

Si on s'autorise une seule inéquation, les ouverts obtenus sont les « intérieurs » de sous-variétés algébriques de $\mathbb{R}^n$. Si on s'autorise deux telles inéquations, on peut voir (cf. section « Optimalité du résultat ») qu'on peut construire plus d'ouverts. On pourrait imaginer qu'en s'autorisant à rajouter de plus en plus d'inégalités, on peut construire de plus en plus d'ouverts différents, mais il n'en est rien et c'est le théorème que nous souhaitons prouver.

Théorème 1.2 (*Scheiderer–Bröcker*)

Tout ouvert semi-algébrique basique de $\mathbb{R}^n$ est exprimable comme lieu des points vérifiant simultanément seulement n inéquations polynomiales strictes.

Ce théorème est démontré dans [Sch89]. Nous en présentons une version tirée de [BCR98]. Pour démontrer le théorème 1.2, il faut être capable d'exprimer un ouvert semi-algébrique en fonction de peu d'inégalités. Regardons ce que cela donne dans l'exemple de la figure 1. Le théorème affirme qu'il est possible d'obtenir le même pentagone avec seulement deux inéquations. On peut choisir comme premier polynôme le produit des cinq polynômes de degré 1 définissant le pentagone. Celui-ci est alors bien positif si les cinq polynômes étaient positifs, mais peut être positif également si deux (ou quatre) d'entre eux sont négatifs. Le lieu des points où ce polynôme est positif est en beige sur la figure 2. On rajoute donc une deuxième inéquation, définie par un autre polynôme (ici de degré 2, qui s'annule sur conique passant par les cinq points).

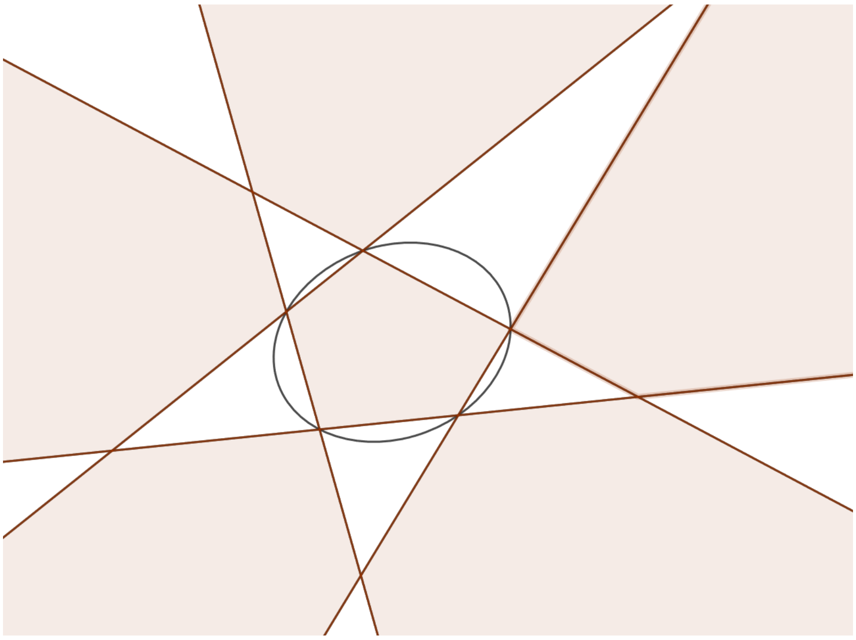

FIGURE 2 – Ré-expression de l'ouvert semi-algébrique basique de la figure 1 en fonction de seulement deux inéquations

Le théorème 1.2 est souvent présenté sous une forme plus générale. En effet, aucune forme d'analyse n'est utilisée et le corps $\mathbb{R}$ peut être remplacé par tout autre corps ayant les mêmes propriétés algébriques : les corps réels clos. Un corps R est dit réel clos quand -1 n'admet pas de racine carrée et que $R[\sqrt{-1}]$ est algébriquement clos. Un tel corps est alors muni naturellement d'un ordre dont les éléments positifs sont exactement les carrés.

Une autre généralisation standard consiste à remplacer R^n par une R-variété de dimension n générale. Il suffit en effet de savoir définir des polynômes et des fractions rationnelles sur cette variété. Nous rédigerons la preuve dans le cas de $\mathbb{R}^n$ mais nous invitons le lecteur frustré par ce manque de généralité à se convaincre par lui-même que chaque argument fonctionne de manière identique dans le cadre plus large mentionné.

Dans la section 2, nous décrirons de manière informelle les idées de la preuve. Dans la section 3, nous présenterons des résultats de la théorie des formes quadratiques, et de la théorie des formes de Pfister. La section 4 donne la preuve d'un théorème d'algèbre commutative. La section 5 utilise ce théorème pour prouver que certaines formes quadratiques représentent la valeur 1. La section 6 utilise ce résultat ainsi que les propriétés des formes de Pfister pour prouver le théorème. Dans la section 7, nous donnons un exemple simple d'ouvert semi-algébrique basique en dimension n demandant n inéquations polynomiales, montrant ainsi l'optimalité du résultat.

2 Idées générales de la preuve

2.1 Ouverts semi-algébriques et formes quadratiques sur $\mathbb{R}(X_1, \dots X_n)$

L'idée la plus importante de la preuve est de se servir de formes quadratiques. On ne regarde ici pas vraiment la relation entre des vecteurs et leur image par la forme, mais directement la forme comme objet algébrique. On considère notamment le plus souvent les formes quadratiques à équivalence près (cf. section suivante).

Nous allons utiliser une forme quadratique pour « représenter » un ouvert semi-algébrique basique. Plus précisément, à un ouvert semi-algébrique basique

$$\mathcal{U} = \{x \in \mathbb{R}^n \mid f_1(x) > 0, \dots, f_k(x) > 0\}$$

va être associée la forme quadratique $\langle f_1, \dots, f_k \rangle$. C'est une forme quadratique sur un espace vectoriel de dimension k sur le corps $\mathbb{R}(X_1, \dots X_n)$ dont la matrice est diagonale et dont les coefficients diagonaux sont les f_i.

Ainsi, comme la positivité des termes diagonaux est un invariant des équivalences de formes quadratiques réelles, on peut avoir l'espoir de trouver une forme quadratique sur le même corps et le même espace sous-jacent, équivalente à la première, mais dont une des coordonnées soit 1 (ou un polynôme qui ne prend que des valeurs positives).

Imaginons que l'on puisse [1], pour chaque point x de $\mathbb{R}^n$, déduire de l'équivalence de deux formes quadratiques sur $\mathbb{R}(X_1, \dots X_n)$, l'équivalence des formes réelles obtenues en les coefficients en x. On obtiendrait ainsi l'équivalence entre le fait que les polynômes de départ soient tous positifs en x, c'est-à-dire que x soit dans l'ouvert, et que les $n-1$ autres termes diagonaux de la deuxième forme soient positifs en x. On aurait donc trouvé $n-1$ nouvelles inéquations polynomiales définissant le même ouvert semi-algébrique basique. Tant qu'on peut itérer cette construction, on peut diminuer le nombre d'inéquations nécessaires à définir l'ouvert semi-algébrique basique considéré.

2.2 Manipulations de formes de Pfister

L'autre idée importante de cette preuve et d'utiliser un outil classique de la théorie des formes quadratiques, les formes de Pfister.

La difficulté pour mettre en œuvre telle quelle l'idée du paragraphe précédent est de réussir à manipuler les formes $\langle f_1, \dots, f_k \rangle$. Nous allons donc faire le choix de ne pas prendre ces formes, mais plutôt les formes $\langle\langle f_1, \dots, f_k \rangle\rangle$. Cette notation sera détaillée dans la section 3 et désigne la forme quadratique de Pfister engendrée par les f_i. Ce choix est judicieux car les formes de Pfister possèdent des propriétés qui les rendent assez facilement manipulables. Ceci permet de découper la preuve en deux parties : démontrer dans un premier temps que 1 (ou un polynôme équivalent) est « représenté »par la forme quadratique [2] $\langle\langle f_1, \dots, f_k \rangle\rangle$, c'est-à-dire que c'est une valeur prise par la forme quadratique, puis dans un second temps montrer qu'on peut manipuler la forme pour la réécrire $\langle\langle 1, g_1, \dots, g_{k-1} \rangle\rangle$.

1. Cette implication est fausse en général, mais sera vraie dans notre cas.
2. En fait plutôt par sa sous-forme pure

3 Formes quadratiques et formes de Pfister

Soit F un corps de caractéristique différente de 2. Nous présentons la théorie des formes quadratiques et de Pfister. Une référence peut être trouvée dans [Kah09].

3.1 Formes quadratiques et théorème de simplification de Witt

Nous commençons par définir les formes quadratiques en général.

Définition 3.1 (*Forme quadratique*)

Une forme quadratique sur F est un F-espace vectoriel V de dimension finie muni d'une application $\varphi : V \to F$ telle que
- $\varphi(\lambda x) = \lambda^2 \varphi(x)$ pour tout $(\lambda, x) \in F \times V$;
- $B_\varphi : (x, y) \mapsto \frac{1}{2}(\varphi(x+y) - \varphi(x) - \varphi(y))$ est bilinéaire.

Nous noterons simplement la forme quadratique φ sans mentionner V. Nous appelons V l'espace sous-jacent à φ. La dimension de V est appelée la dimension de φ, et notée $\dim \varphi$.

Nous considérons la relation d'orthogonalité par analogie avec le produit scalaire usuel.

Définition 3.2 (*Orthogonalité*)

Si φ est une forme quadratique et V son espace sous-jacent, on dit que $x, y \in V$ sont orthogonaux si $B_\varphi(x, y) = 0$, et que $W_1, W_2 \subset V$ sont orthogonaux si pour tous $(x, y) \in W_1 \times W_2$, on a $B_\varphi(x, y) = 0$. Si $X \subset V$, son orthogonal $X^\perp$ est défini par :

$$X^\perp = \{x \in V \mid \forall y \in X, B_\varphi(x, y) = 0\}.$$

Définition 3.3 (*Non dégénérence*)

Le radical de φ est le sous-espace Rad $\varphi = V^\perp$. On dit que φ est non dégénérée si Rad $\varphi = \{0\}$.

Toutes les formes quadratiques considérées dans ce texte sont non dégénérées.

Définition 3.4 (*Équivalence entre les formes quadratiques*)

Deux formes quadratiques φ et ψ, d'espaces sous-jacents respectivement V et V', sont équivalentes (on note $\varphi \simeq \psi$) s'il existe $f : V \to V'$ un isomorphisme (d'espaces vectoriels) tel que $\varphi = \psi \circ f$.

Il est clair que $\simeq$ est une relation d'équivalence. Nous allons maintenant montrer dans le théorème 3.6 ci-dessous que toute forme quadratique φ est équivalente à une forme simple.

Lemme 3.5

Si $W \subset V$ est un sous-espace, on a Rad$(\varphi_{|W}) = W \cap W^\perp$. Si $\varphi_{|W}$ est non dégénérée, on a $V = W \oplus W^\perp$.

Démonstration : La première assertion est directe par définition. Pour la deuxième, choisissons une base $(e_1, \ldots, e_n)$ de W. Puisque W est non dégénéré, en utilisant l'algorithme de Gram–Schmidt (exactement comme dans le cas du produit scalaire), il existe une base $(f_1, \ldots, f_n)$ de W telle que $B_\varphi(f_i, f_j) = \delta_{ij}$ (symbole de Kronecker). Si $x \in V$ et $\lambda_i = B_\varphi(x, e_i)$, alors $x - \sum_i \lambda_i f_i \in W^\perp$. ■

Théorème 3.6

Toute forme quadratique non dégénérée φ possède une base orthogonale.

Démonstration : Raisonnons par récurrence sur $\dim \varphi$. Soit V l'espace vectoriel sous-jacent à φ. Puisque φ est non dégénérée, il existe $e_1 \in V$ tel que $\varphi(e_1) \neq 0$. Soit $W = \langle e_1 \rangle$. Alors $\varphi_{|W}$ est non dégénérée. En appliquant le lemme 3.5, on trouve $V = W \oplus W^\perp$. Par l'hypothèse de récurrence, $\varphi_{|W^\perp}$ possède une base orthogonale donc φ aussi (en ajoutant e_1 à cette base). ■

Ce théorème implique alors, en choisissons une base orthogonale $(e_1, \ldots, e_n)$ de V, que pour tout $x = \sum_i x_i e_i \in V$, on a $\varphi(x) = \sum_i a_i x_i^2$ avec $a_i = \varphi(e_i) \in F^*$. On note alors $\varphi \simeq \langle a_1, \ldots, a_n \rangle$ la forme φ. Cette forme est appelée la forme diagonale de coefficients a_i. Une forme diagonale $\langle a_1, \ldots, a_n \rangle$ est non dégénérée si et seulement si tous les a_i sont dans F^*.

Nous continuons à compléter les définitions.

Définition 3.7 (*Somme orthogonale et produit tensoriel*)

Pour deux formes quadratiques φ et ψ, d'espaces sous-jacents respectivement V et W, nous définissons :

- *La somme orthogonale (sur $V \oplus W$) : $\varphi \perp \psi(x \oplus y) = \varphi(x) + \psi(y)$.*
- *Le produit tensoriel (sur $V \otimes W$) : $B_{\varphi \otimes \psi}(x \otimes x', y \otimes y') = B_\varphi(x, x')B_\psi(y, y')$.*

Pour les formes diagonales, nous avons

$$\langle a_1, \ldots, a_m \rangle \perp \langle b_1, \ldots, b_n \rangle = \langle a_1, \ldots, a_m, b_1, \ldots, b_n \rangle$$

$$\langle a_1, \ldots, a_m \rangle \otimes \langle b_1, \ldots, b_n \rangle = \langle a_1 b_1, \ldots, a_m b_n \rangle.$$

Pour la suite nous considérons les formes quadratiques sur F^n et nous les appelons les formes quadratiques les formes quadratiques de dimension n sur F.

Introduisons quelques termes de vocabulaire :

Définition 3.8 (*Isotrope et Anisotrope*)

Soit φ une forme quadratique non dégénérée de dimension n sur F. La forme φ représente $b \in A$ sur A (où A est une F-algèbre) s'il existe $x \in A^n$ tel que $\varphi(x) = b$. Si $A = F$, on dit simplement que φ représente b. La forme φ est isotrope (sur F) s'il existe $x \neq 0$ dans F^n tel que $\varphi(x) = 0$, et anisotrope sinon.

Nous introduisons quelques propriétés fondamentales utiles pour la suite.

Proposition 3.9

Soit φ une forme quadratique non dégénérée de dimension n sur F.
(i) Si φ est isotrope, alors il existe $a_3, \ldots, a_n \in F^*$ tels que

$$\varphi \simeq \langle 1, -1, a_3, \ldots, a_n \rangle.$$

(ii) Si φ est isotrope, alors φ représente tout $b \in F^*$ (φ est universelle).
(iii) La forme φ représente $b \in F^*$ si et seulement si $\varphi \perp \langle -b \rangle$ est isotrope.

Démonstration : (i) Soit $x \in F^n \setminus \{0\}$ tel que $\varphi(x) = 0$. Comme φ est non dégénérée, il existe $y \in F^n$ tel que $B_\varphi(x, y) = 1$. Soit $z = y - \frac{\varphi(y)}{2}x$, on a $\varphi(z) = 0$ et $B_\varphi(x, z) = 1$. Soit W le sous-espace vectoriel engendré par x, z, alors avec $u = x + \frac{z}{2}, v = x - \frac{z}{2}$, on a $\varphi(u) = 1, \varphi(v) = -1$ et $B_\varphi(u, v) = 0$, donc $\varphi_{|W} \simeq \langle 1, -1 \rangle$. D'après le lemme 3.5, on a $F^n = W \oplus W^\perp$. Par le théorème 3.6, il existe $a_3, \ldots, a_n \in F^*$ tels que $\varphi_{|W^\perp} \simeq \langle a_3, \ldots, a_n \rangle$, alors on a

$$\varphi = \varphi_{|W} \oplus \varphi_{|W^\perp} \simeq \langle 1, -1, a_3, \ldots, a_n \rangle.$$

(ii) Par l'égalité $b = (\frac{b+1}{2})^2 - (\frac{b-1}{2})^2$ et (i), c'est immédiat.

(iii) S'il existe $x \in F^n$ tel que $\varphi(x) = b$, on a $\varphi \perp \langle -b \rangle (x \oplus 1) = 0$ donc $\varphi \perp \langle -b \rangle$ est isotrope. Réciproquement, supposons qu'il existe $x \in F^n$ et $y \in F$ tel que $\varphi \perp \langle -b \rangle (x \oplus y) = 0$, c'est à dire $\varphi(x) = by^2$. Si $y = 0$, alors φ est isotrope et on finit par (ii). Sinon $y \in F^*$ donc $\frac{x}{y} \in F^n$ est bien défini, et $\varphi(\frac{x}{y}) = b$. ■

Le lemme suivant sera utilisé dans la partie sur les formes de Pfister.

Lemme 3.10

Si la forme $\langle a, b \rangle$ représente $c \in F^*$, alors $\langle a, b \rangle \simeq c\langle 1, ab \rangle$.

Démonstration : Il existe $(u, v) \in F^2$ tel que $c = au^2 + bv^2 \neq 0$. En considérant la nouvelle base $((u, v), (-bv, au))$ orthogonale de F^2, on voit que $\langle a, b \rangle \simeq c\langle 1, ab \rangle$. ■

On termine cette partie par le théorème de simplification de Witt. Commençons par définir les réflexions au sens de la forme quadratiques φ.

Définition 3.11 (*Réflexion*)

Soit φ une forme quadratique et V son espace sous-jacent. Soit $x \in V$ tel que $\varphi(x) \neq 0$. Posons $u_x(y) = y - 2\frac{B_\varphi(x,y)}{q(x)}x$. Soit W la droite engendrée par x. L'application linéaire u_x est appelée réflexion d'axe W.

L'application u_x s'appelle réflexion car on a les deux propriétés suivantes. Nous omettons ici leurs preuves purement calculatoires.

— 1. $\varphi \circ u_x = \varphi$

— 2. $u_x^2 = Id$

On a aussi un lemme.

Lemme 3.12

Soit φ une forme quadratique d'espace vectoriel sous-jacent V, et soient $x, y \in V$ tels que $\varphi(x) = \varphi(y) \neq 0$. Alors il existe une réflexion u tel que $u(x) = y$ ou $u(x) = -y$.

Démonstration : Par calcul direct on a l'identité du parallélogramme :

$$\varphi(x+y) + \varphi(x-y) = 2\varphi(x) + 2\varphi(y).$$

On a donc $\varphi(x+y) \neq 0$ ou $\varphi(x-y) \neq 0$. Si $\varphi(x-y) \neq 0$. Posons $u = u_{x-y}$. On a $u(x-y) = -x+y$ et $u(x+y) = x+y$. Il en résulte que $u(x) = y$. Si $\varphi(x+y) \neq 0$, on remplace y avec $-y$ et on obtient $u(x) = -y$. ■

Alors on montre le théorème.

Théorème 3.13 (*Théorème de Simplification de Witt*)

Soient $\varphi, \varphi_1, \varphi_2$ trois formes quadratiques sur F non dégénérées. Si $\varphi \perp \varphi_1 \simeq \varphi \perp \varphi_2$, alors $\varphi_1 \simeq \varphi_2$.

Démonstration : En utilisant le théorème 3.6, il suffit qu'on montre le cas $\varphi = \langle a \rangle$ pour un $a \in F^*$ et puis précède la récurrence. Par transport de structure, on se ramène au cas où $\langle a \rangle \perp \varphi_1 = \langle a \rangle \perp \varphi_2$, on note Q cette forme quadratique. Soient V l'espace vectoriel sous-jacent à Q et W_1, W_2 les sous-espaces de V correspondant respectivement à φ_1 et φ_2. Le lemme 3.12 implique qu'il existe une réflexion u tel que, $u(W_1^\perp) = W_2^\perp$ comme u isomorphisme et préserve Q, on a $u(W_1) = W_2$. Donc on a $\varphi_1 \simeq \varphi_2$. ■

3.2 Formes quadratiques sur des corps de fractions rationnelles et sur des anneaux de polynômes.

Dans cette partie, nous étudions le comportement d'une forme quadratique (sur F) sur les F-algèbre de polynômes et de fractions rationnelles.

Proposition 3.14

Soit $f \in F[X]$. Soit φ une forme quadratique non dégénérée sur F. Si φ représente f sur le corps $F(X)$, alors φ représente f sur l'anneau $F[X]$.

Démonstration : Si φ est isotrope, en appliquant la proposition 3.9(i) et l'égalité $f = (\frac{f+1}{2})^2 - (\frac{f-1}{2})^2$, on a tous les $f \in F[X]$ sont représentés par φ sur $F[X]$.

Si φ est anisotrope, soit $f \neq 0$ (car le cas $f = 0$ est trivial). Considérons une représentation de f par φ sur $F(X)$:

$$f = \varphi(\frac{g_1}{g_0}, \dots, \frac{g_n}{g_0})$$

où $g_0, g_1, \dots, g_n \in F[X]$ et $g_0 \neq 0$. On introduit la forme quadratique $\psi = \langle -f \rangle \perp \varphi$ de dimension $n+1$ sur $F(X)$ i.e. $\psi(u) = -fu_0^2 + \varphi(u_1, \dots, u_n)$. En notant $g = (g_0, g_1, \dots, g_n) \in F[X]^{n+1}$. Par définition, on a $\psi(g) = 0$. Pour montrer la proposition, il suffit de construire un zéro de ψ de la forme $(1, p_1, \dots, p_n)$ avec $p_1, \dots, p_n \in F[X]$, car ceci implique $f = \psi(p_1, \dots, p_n)$.

Pour $i = 1, \dots, n$, on prend la division euclidienne $g_i = q_i g_0 + r_i$, avec $\deg(r_i) < \deg(g_0)$ ou $r_i = 0$. Si $q = (1, q_1, \dots, q_n)$ est un zéro de ψ, on est fini. Donc on suppose ensuite $\psi(q) \neq 0$. Alors

g et q sont linéairement indépendants sur $F(X)$, donc $h = \psi(q)g - 2B_\psi(g,q)q$ est non nul. Par construction, $h \in F[X]^{n+1}$, et h est un zéro de ψ :

$$\psi(h) = \psi(q)^2\psi(g) - 4\psi(q)(B_\psi(g,q))^2 + 4(B_\psi(g,q))^2\psi(q) = 0.$$

La première composante h_0 de h est

$$h_0 = \psi(q)g_0 - 2B_\psi(g,q) = \frac{1}{g_0}\varphi(r_1,\ldots,r_n),$$

et $r_1,\ldots,r_n$ ne sont pas tous nuls car sinon $g = g_0 q$. Comme φ est anisotrope sur F, $\varphi(r_1,\ldots,r_n) \neq 0$, et

$$\deg(h_0 g_0) = \deg(\varphi(r_1,\ldots,r_n)) = 2\max(\{\deg(r_i) \mid i = 1,\ldots,n\}) < 2\deg(g_0).$$

Donc on a construit un zéro h de ψ dans $F[X]^{n+1}$, avec $h_0 \neq 0$ et $\deg(h_0) < deg(g_0)$. Comme le degré décroît, on peut réitérer cette construction et finalement obtient un zéro de ψ dans $F[X]^{n+1}$ de la forme $(1, p_1, \ldots, p_n)$. Ceci termine la preuve. ■

Nous avons alors un corollaire direct.

Corollaire 3.15

Soit φ une forme quadratique sur F, et $f \in F[X_1,\ldots,X_m]$. Si φ représente f sur $F(X_1,\ldots,X_m)$, alors pour tout $a_1,\ldots,a_m \in F$, φ représente $f(a_1,\ldots,a_m)$ sur F.

Démonstration : Si φ représente f sur $F(X_1,\ldots,X_m) = F(X_1,\ldots,X_{m-1})(X_m)$, alors par la proposition 3.14, il existe des polynôme $A_1,\ldots,A_n$ à coefficients dans $F(X_1,\ldots,X_{m-1})$ tel que $f = \varphi(A_1(X_m),\ldots,A_n(X_m))$.

Pour tout $a_m \in F$, on obtient $f(X_1,\ldots,X_{m-1},a_m) = \varphi(A_1(a_m),\ldots,A_n(a_m))$, donc on a φ représente $f(X_1,\ldots,X_{m-1},a_m)$ sur $F(X_1,\ldots,X_{m-1})$. Le résultat est obtenu par récurrence sur m. ■

Nous avons une autre proposition qui est utile pour la suivante.

Proposition 3.16

Soit $a \in F, b_1,\ldots,b_n \in F^*, n > 1$ et $\varphi = \langle b_1,\ldots,b_n\rangle$. Alors les propriétés suivantes sont équivalentes :

(i) φ représente $b_1X^2 + a$ sur $F(X)$.

(ii) $\varphi' = \langle b_2,\ldots,b_n\rangle$ représente a, ou φ est isotrope.

Démonstration : (i) $\Rightarrow$ (ii) : D'après la proposition 3.14, φ représente $b_1X^2 + a$ sur $F[X]$:

$$b_1X^2 + a = \sum_{j=1}^{n} b_j f_j^2, f_j \in F[X].$$

Si φ est anisotrope sur F, on a

$$\deg(\sum_{j=1}^{n} b_j f_j^2) = 2\max(\{\deg(f_j) \mid j = 1,\ldots,n\}),$$

donc on a besoin que pour tout $j = 1,\ldots,n$, il existe $c_j, d_j \in F$, tel que $c_jX + d_j \in F$. Comme le polynôme $(c_1X + d_1)^2 - X^2 = ((c_1-1)X + d_1)((c_1+1)X + d_1)$ admet au moins une racine $e \in F$ (car $c_1 - 1$ et $c_1 + 1$ ne peut être simultanément nuls), avec $e^2 = c_1e^2 + d_1 = f_1(e)$, on a

$$b_1e^2 + a = b_1e^2 + \sum_{j=2}^{n} b_j f_j^2.$$

Donc φ' représente a sur F.

(ii) $\Rightarrow$ (i) : Si φ' représente a sur F, l'implication est immédiate par définition. If φ est isotrope, l'implication est immédiate par la proposition 3.9(ii). ■

Pour montrer la dernière proposition de la partie, nous présentons un lemme.

Lemme 3.17

Soit φ une forme quadratique anisotrope sur F. Alors φ est anisotrope sur $F(X)$.

Démonstration : Montrons par contraposé, supposons que φ est isotrope sur $F(X)$. Il existe $f_1, \dots, f_n \in F(X)$ non tous nuls tel que $\varphi(f_1, \dots, f_n) = 0$. En multipliant simultanément tous les f_i par X^n avec $n \in \mathbb{Z}$ spécifique, on peut supposer que les $f_1, \dots, f_n$ sont définis en 0 et les $f_1(0), \dots, f_n(0)$ sont non tous nuls, alors $\varphi(f_1(0), \dots, f_n(0)) = 0$, φ est isotrope sur F. ■

Nous finirons par notre dernière proposition.

Proposition 3.18

Soit $\varphi = \langle a_1, \dots, a_m\rangle, \psi = \langle b_1, \dots, b_n\rangle$ des formes quadratiques sur F, où $a_1, \dots, a_m, b_1, \dots, b_n \in F^*$. Supposons que φ est anisotrope sur F et φ représente $\psi(X_1, \dots, X_n) = \sum_{i=1}^n b_i X_i^2$ sur le corps $F(X_1, \dots, X_n)$. Alors il existe une forme quadratique θ sur F tel que $\varphi \simeq \psi \perp \theta$.

Démonstration : Nous procédons par récurrence sur $m = \dim \varphi$. Le cas $m = 1$ est trivial. Avec $m > 0$, supposons que le résultat est vrai pour $m - 1$. Par le corollaire 3.15, φ représente b_1 sur F, donc $\varphi \simeq \langle b_1\rangle \perp \rho$, en effet, nous prenons une base orthogonale de $\mathrm{Vect}(x)^\perp$ dans F^m où $\varphi(x) = b_1$. Comme φ est anisotrope sur $F(X_2, \dots, X_n)$ (une génération simple par récurrence du lemme 3.17), et elle représente $b_1 X_1^2 + (b_2 X_2^2 + \dots + b_n X_n^2)$ sur le corps $F(X_2, \dots, X_n)(X_1)$, on a d'après la proposition 3.16, ρ représente $b_2 X_2^2 + \dots + b_n X_n^2$ sur $F(X_2, \dots, X_n)$. La forme ρ est anisotrope sur F (car sinon φ est isotrope sur F). Donc, d'après l'hypothèse de la récurrence, nous avons $\rho \simeq \langle b_2, \dots, b_n\rangle \perp \theta$ et donc $\varphi \simeq \psi \perp \theta$. ■

3.3 Signature d'une forme quadratique réelle

Dans cette petite partie, nous introduisons une notion qui n'est utilisée que dans la partie 3.5 et la fin de la preuve de nos résultats principaux. On dit qu'une forme quadratique est réelle si elle est définie sur le corps $\mathbb{R}$

Définition 3.19 (*Signature*)

La signature d'une forme quadratique réelle non dégénérée φ est une paire (s^+, s^-) tel que, pour une forme diagonale $\langle a_1, a_2, \dots, a_n\rangle \simeq \varphi$, l'entier s^+(resp. s^-) est le nombre de valeurs strictement positives (resp. strictement négatives) dans $a_1, \dots, a_n$.

Par le théorème 3.6, toute forme quadratique réelle est équivalente à une forme diagonale. Pour montrer que la signature est bien définie, il nous suffit de montrer que deux formes diagonales équivalentes ont la même signature.

Prenons $\varphi_a = \langle a_1, \dots a_n\rangle \simeq \langle b_1, \dots, b_n\rangle = \varphi_b$, et soit (s_a^+, s_a^-) la signature de φ_a et (s_b^+, s_b^-) la signature de φ_b. Par un changement de base (avec des multiplications par des scalaires et une permutation des vecteurs de base), on a $\varphi_a \simeq \langle 1, \dots, 1, -1, \dots, -1\rangle$ (il y a s_a^+ fois 1 et s_a^- fois -1) et de même pour φ_b. Si les deux signatures sont différentes, en utilisant le théorème de simplification de Witt (théorème 3.13), on déduit $\langle 1, \dots, 1\rangle \simeq \langle -1, \dots, -1\rangle$ où ces formes ont dimension > 0, contradiction car l'une prend des valeurs positives et l'autre prend des valeurs négatives.

Comme deux formes diagonales ayant la même signature sont isométriques (on multiplie chaque vecteur de base par un bon scalaire), on en déduit le théorème suivant :

Théorème 3.20 (*Invariance de la signature*)

La signature est un invariant caractéristique pour l'isométrie de formes quadratiques réelles non dégénérées. Autrement dit, deux formes quadratiques réelles non dégénérées sont isométriques si et seulement si elles ont la même signature.

3.4 Formes de Pfister et multiplicativité.

Dans cette partie, nous introduisons la notion de forme de Pfister, c'est un cas particulier de forme quadratique.

Définition 3.21 (*Forme de Pfister*)

Une forme de Pfister φ sur F est une forme quadratique de dimension 2^n sur F, tel qu'il existe *des éléments $a_1, \dots, a_n \in F^*$, avec :*

$$\varphi = \langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \dots \otimes \langle 1, a_n \rangle$$

Notons alors $\varphi = \langle\langle a_1, \dots, a_n \rangle\rangle$. La forme φ' de dimension $2^n - 1$:

$$\varphi' = \langle a_1, \dots, a_n, a_1 a_2, \dots, a_1 a_2 \dots a_n \rangle$$

est appelée la sous-forme pure de la forme de Pfister φ. Nous avons $\varphi = \langle 1 \rangle \perp \varphi'$.

Une forme quadratique φ de dimension d sur F est dite multiplicative si elle vérifie la propriété suivante :

$$\forall x \in F^d, \varphi(x) \neq 0 \Rightarrow \varphi(x)\varphi \simeq \varphi$$

Théorème 3.22

Tous les formes de Pfister sont multiplicatives.

Soit φ une forme de Pfister de dimension 2^n. Montrons le théorème par récurrence sur n. Pour $n = 0$, on a $\varphi(X) = X^2$, qui est clairement multiplicative. Pour conclut, il suffit de prouver que si φ est multiplicative et $a \in F^*$, alors $\varphi \perp a\varphi = \langle 1, a \rangle \otimes \varphi$ est multiplicative. Soient $x, x' \in F^{2^n}$ tels que $\varphi(x) + a\varphi(x') \neq 0$. On distingue alors trois cas :

— Si $\varphi(x') = 0$, alors

$$\varphi(x)(\varphi \perp a\varphi) = (\varphi(x)\varphi) \perp (a\varphi(x)\varphi) \simeq \varphi \perp a\varphi.$$

— Si $\varphi(x) = 0$, alors

$$a\varphi(x')(\varphi \perp a\varphi) = (a\varphi(x')\varphi) \perp (a^2\varphi(x')\varphi) \simeq a\varphi \perp a^2\varphi \simeq a\langle 1, a \rangle \otimes \varphi \simeq \varphi \perp a\varphi.$$

Car $\langle 1, a \rangle \simeq a\langle 1, a \rangle$ par le lemme 3.10.

— Si $\varphi(x)\varphi(x') \neq 0$, alors

$$\begin{aligned}(\varphi(x) + a\varphi(x'))(\varphi \perp a\varphi) &\simeq (\varphi(x) + a\varphi(x'))(\varphi \perp a\varphi(x)\varphi(x')\varphi) \\ &\simeq (\varphi(x) + a\varphi(x'))\langle 1, a\varphi(x)\varphi(x') \rangle \otimes \varphi \\ &\simeq \langle \varphi(x), a\varphi(x') \rangle \otimes \varphi \text{ (par le lemme 3.10)} \\ &\simeq \varphi(x)\varphi \perp a\varphi(x')\varphi \\ &\simeq \varphi \perp a\varphi.\end{aligned}$$

3.5 Propriétés des formes de Pfister

Dans cette section, on présente une série de lemmes qui concernent les formes de Pfister et qui sont directement utiles pour notre résultat principal. Il peut être pertinent de ne lire cette section en détail qu'après avoir lu la section « Preuve » de ce document, qui utilise et donne une motivation pour ces résultats.

Lemme 3.23

Soient $a_1, \dots, a_n \in F^*$. Pour $1 \leq i \leq n$, notons $\varphi_i = \langle\langle a_1, \dots, a_i \rangle\rangle$. Soit u_1 un carré dans F, et pour $1 < i \leq n$, soit $u_i \in F$ représenté par φ_{i-1}. Pour $1 \leq i \leq n$, définissons $b_i = \sum_{j=i}^{n} a_j u_j$. Si $b_1, \dots, b_n \in F^*$, alors on a

$$\varphi_n \simeq \langle\langle b_1, a_1 b_2, \dots, a_{n-1} b_n \rangle\rangle .$$

Les deux faits suivants sont utilisés dans notre preuve :

1. Si a, b et $a + b$ sont éléments de F^*, alors $\langle\langle a, b \rangle\rangle \simeq \langle\langle a + b, ab \rangle\rangle$. C'est une conséquence du lemme 3.10.
2. Si $b \in F^*$ est représenté par la forme de Pfister ψ, alors $\psi \otimes \langle\langle a \rangle\rangle \simeq \psi \otimes \langle\langle ab \rangle\rangle$. C'est parce que ψ est multiplicative (voir le théorème 3.22).

Démonstration : On montre par récurrence décroissante sur k que :

$$\varphi_n \simeq \varphi_k \otimes \langle\langle b_{k+1}, a_{k+1} b_{k+2}, \dots, a_{n-1} b_n \rangle\rangle .$$

Par (2), on a

$$\varphi_n = \varphi_{n-1} \otimes \langle\langle a_n \rangle\rangle \simeq \varphi_{n-1} \otimes \langle\langle a_n u_n \rangle\rangle = \varphi_{n-1} \otimes \langle\langle b_n \rangle\rangle$$

(on a $u_n \neq 0$, car $b_n \neq 0$). Donc il suffit de montrer que pour $0 < k < n$

$$\varphi_{k-1} \otimes \langle\langle a_k, b_{k+1} \rangle\rangle \simeq \varphi_{k-1} \otimes \langle\langle b_k, a_k b_{k+1} \rangle\rangle \ .$$

Si $u_k \neq 0$, on a par (1) et (2) :

$$\begin{aligned} \varphi_{k-1} \otimes \langle\langle a_k, b_{k+1} \rangle\rangle &\simeq \varphi_{k-1} \otimes \langle\langle a_k u_k, b_{k+1} \rangle\rangle \\ &\simeq \varphi_{k-1} \otimes \langle\langle a_k u_k + b_{k+1}, a_k u_k b_{k+1} \rangle\rangle \\ &\simeq \varphi_{k-1} \otimes \langle\langle b_k, a_k b_{k+1} \rangle\rangle \ . \end{aligned}$$

Si $u_k = 0$, on a $b_k = b_{k+1}$ donc par (2) :

$$\langle\langle a_k, b_{k+1} \rangle\rangle \simeq \langle\langle b_k, a_k \rangle\rangle \simeq \langle\langle b_k, a_k b_{k+1} \rangle\rangle \ .$$

■

En utilisant ce lemme, nous avons directement un autre lemme.

Lemme 3.24

Soit $\varphi = \langle\langle a_1, \ldots, a_n \rangle\rangle$, avec $a_1, \ldots, a_n \in F^*$. Soit $b_1 \in F^*$ un élément représenté par la sous-forme φ'. Alors il existe $c_2, \ldots, c_n \in F^*$ tel que $\varphi \simeq \langle\langle b_1, c_2, \ldots, c_n \rangle\rangle$.

Démonstration : Notons $\varphi_i = \langle\langle a_1, \ldots a_i \rangle\rangle$. Remarquons que pour $1 \leq r \leq n$, la forme pure $(\varphi_r)'$ est égale à $\langle a_1 \rangle \perp a_2 \varphi_1 \perp \cdots \perp a_r \varphi_{r-1}$.

Donc on a $b_1 = a_1 u_1 + a_2 u_2 + \cdots + a_n u_n$, où u_1 est un carré dans F et pour $1 < i \leq n$, $u_i \in F$ est représenté par φ_{i-1}. Supposons que $r \geq 1$ est le plus petit entier tel que $(\varphi_r)'$ représente b_1. Alors les $b_i^{(r)} = \sum_{j=i}^{r} a_j u_j$ sont non nuls. En appliquant le lemme 3.23 à φ_r on voit que $\varphi_r \simeq \langle\langle b_1, c_2, \ldots, c_r \rangle\rangle$ où $c_2, \ldots, c_r \in F^*$. Puis en notant $c_k = a_k \in F^*$ pour $k > r$, on a $\varphi \simeq \langle\langle b_1, c_2, \ldots, c_n \rangle\rangle$. ■

Comme celle nous sera utile dans la suite, nous introduisons la notion de la forme quadratique sur un anneau commutatif. On ne considère que les formes diagonales. Les notations pour les formes diagonales et les formes de Pfister restent valables dans ce cas (nous les définissons par les polynômes).

Définition 3.25 (*Faiblement représenté*)

Soit A un anneau, B une A-algèbre. Une forme quadratique $\varphi = \langle a_1, \ldots, a_m \rangle$ à coefficients dans A est non dégénérée sur B si l'image de $\prod_{i=1}^{m} a_i$ est inversible dans B. Un élément $b \in B$ est dit faiblement représenté par φ sur B s'il existe des éléments $u_1, \ldots, u_k \in B^m$, tels que $b = \varphi(u_1) + \cdots + \varphi(u_k)$.

Il est clair que cette définition de forme non dégénérée est compatible avec celle donnée dans le cas du corps.

Aussi, un élément est faiblement représenté par φ sur un corps réel clos R si et seulement s'il est représenté par φ sur R.

Soit $x \in \mathbb{R}^n$. Si $\varphi = \langle a_1, \ldots, a_m \rangle$ est une forme quadratique à coefficients dans $\mathbb{R}[X_1, \ldots, X_n]$, notons φ_x la forme quadratique $\langle a_1(x), \ldots, a_m(x) \rangle$ sur $\mathbb{R}$.

Lemme 3.26

Soient $g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$. Pour $i = 1, \ldots, m$, notons φ_i la forme de Pfister $\langle\langle g_1, \ldots, g_i \rangle\rangle$. Soit v_1 une somme de carrés dans $\mathbb{R}[X_1, \ldots, X_n]$. Pour $i = 1, \ldots, m-1$, soit v_{i+1} est un élément faiblement représenté par φ_i sur $\mathbb{R}[X_1, \ldots, X_n]$. Définissons pour $i = 1, \ldots, m-1$, $w_i = \sum_{j=i+1}^{n} g_j v_j$ et $\psi = \langle\langle w_0, g_1 w_1, \ldots, g_{m-1} w_{m-1} \rangle\rangle$. Soit $x \in \mathbb{R}^n$ tel que $(\varphi_m)_x$ et $(\psi)_x$ sont non dégénérées. Alors $(\varphi_m)_x \simeq (\psi)_x$, et les deux formes ont la même signature.

Démonstration : Notons que $v_1(x)$ est un carré dans $\mathbb{R}$, et que pour $i = 1, \ldots, m-1$, le réel $v_{i+1}(x)$ est représenté par $(\varphi_i)_x$ sur $\mathbb{R}$. Donc on applique le lemme 3.23 pour conclure. ■

4 Le théorème de Tsen–Lang

Le théorème de Tsen–Lang permet d'affirmer que certains corps vérifient une version faible du fait d'être algébriquement clos. On nomme cette propriété C_i, où C_0 est être algébriquement clos, et plus i est grand, moins cette propriété est forte.

Définition 4.1 (*Corps C_d*)

Un corps K est dit C_d quand tout polynôme homogène à coefficients dans K de degré n en N variables vérifiant $N > n^d$ a forcément un zéro non trivial.

On a immédiatement les propriétés suivantes :

Proposition 4.2

- *Un corps est C_0 si et seulement s'il est algébriquement clos.*
- *Un corps C_d est C_{d+1}*

Pour énoncer le théorème de Tsen–Lang, nous aurons besoin des définitions suivantes :

Définition 4.3 (*Partie algébriquement génératrice*)

Soit A un anneau ou corps et B un sous-anneau ou sous-corps. Une partie $\{a_1, \ldots a_d\}$ de A est dite B-algébriquement génératrice (ou simplement algébriquement génératrice) quand pour tout $x \in A$, il existe $P \in B[X_1, \ldots, X_{d+1}] \setminus \{0\}$ tel que $P(a_1, \ldots a_d, x) = 0$.

Attention, la B-algèbre engendrée par les a_i, notée $B[a_1, \ldots a_d]$ n'est pas forcément A, par contre l'extension $A/B[a_1, \ldots a_d]$ doit être algébrique.

Définition 4.4 (*Degré de transcendance*)

Un anneau ou corps A a un degré de transcendance au plus d sur un sous-anneau ou sous-corps B, quand il existe une partie algébrique génératrice de cardinal d.

On a le théorème suivant :

Théorème 4.5 (*Tsen–Lang*)

Un corps de degré de transcendance (au plus) d sur un corps algébriquement clos est un corps C_d.

On pourrait montrer pour cela les deux propriétés suivantes, mais nous allons préférer une preuve directe du théorème.

Proposition 4.6

- *Si K est C_d et L/K est algébrique, alors L est C_d*
- *Si K est C_d, $K(t)$ est C_{d+1}*

Démonstration (Tsen–Lang) : Soient K un corps algébriquement clos, L un sur-corps de degré de transcendance au plus d et $\alpha_1, \ldots \alpha_d$ une partie algébriquement génératrice L de cardinal d. Introduisons également $\beta_1, \ldots \beta_r$ une $K(\alpha_1, \ldots \alpha_d)$-base de L. Grâce à ces notations, on peut exprimer chaque élément de L en fonction de r coordonnées dans $K(\alpha_1, \ldots \alpha_d)$, et chacune de ces coordonnées s'exprime en fonction de ses coefficients, qui sont dans K. Chaque point $x \in L$ s'écrit

$$x = \sum_{j=1}^{r} \beta_j F_{j,x}(\alpha_1, \ldots \alpha_d), \text{ où } F_{j,x} \in K(X_1, \ldots X_d).$$

On va donc réussir à passer d'une équation dans L à plusieurs équations dans K, et à utiliser l'hypothèse que K est algébriquement clos.

Cependant, on préférerait que les coordonnées $F_{j,x}$ ne soient pas seulement dans $K(\alpha_1, \ldots \alpha_d)$ mais même dans $K[\alpha_1, \ldots \alpha_d]$. Heureusement, une astuce nous permet de supposer exactement ceci. En effet, si on a un nombre fini d'éléments de L dont on veut que les β-coordonnées soient entières, il suffit de multiplier les vecteurs β_j par un scalaire (c'est-à-dire un élément de $K(\alpha_1, \ldots \alpha_d)$) adéquat.

Plus précisément ici, nous souhaitons que les coordonnées des produits $\beta_j \beta_k$ dans la base β, c'est-à-dire les $F_{i,\beta_j\beta_k}$ soient des polynômes (et non des fractions rationnelles). Pour cela, divisons chaque β_i par le produit sur j et k des dénominateurs de $F_{i,\beta_j\beta_k}$. Enfin, posons un polynôme arbitraire P homogène de degré d en $N > n^d$ variables à coefficients dans L et multiplions-le par un scalaire adéquat pour que chaque coordonnée de chaque coefficient soit dans $K[\alpha_1, \ldots \alpha_d]$. Le multiplier ainsi par un scalaire ne change pas ses racines. Nommons s le degré maximal de tous ces polynômes, cordonnées des $\beta_j\beta_k$ ou des coefficients de P.

Nous cherchons une racine (non triviale) pour P dans L, cherchons-la parmi les éléments de L dont les coordonnées sont des polynômes de degré inférieur strictement à M, où M est un entier qu'on posera à terme suffisamment grand. Notre racine potentielle $(x_1, \ldots, x_N)$ s'écrit

$$x_k = \sum_{j=1}^{r} \beta_j \sum_{I \in [\![0, M-1]\!]^d} \mu_{k,j,I} \alpha^I, \text{ où } \mu_{k,j,I} \in K.$$

Alors la donnée de x est équivalente à la donnée des $\mu_{k,j,I}$, c'est-à-dire de $N \cdot r \cdot M^d$ éléments de K.

Alors, on peut développer l'équation $P(x) = 0$ en une équation dans L en les variables μ. Cette équation se décompose dans la base β en n équations dans $K(\alpha_1, \ldots \alpha_d)$, mais nos hypothèses garantissent que ces équations sont en fait dans $K[\alpha_1, \ldots \alpha_d]$. De plus, il est possible de borner le degré en chaque variable α_i des polynômes qui constituent ces r équations : chaque terme comporte

— un coefficient de P, de degré au plus s

— un produit de d facteurs β_j qui se réécrit comme une combinaison linéaire de β_j où les coefficients sont de degrés inférieurs ou égaux à $s \cdot (d-1)$

— le produit de d termes α^I de degrés en chaque variable tous inférieurs strictement à M

Le degré en chaque variable est donc majoré strictement par $d(s+M)$. Le nombre total de termes dans ces polynômes est donc majoré par $(ds+dM)^i$. Chaque terme de ces polynômes donne une équation sur K, donc l'équation $P(x) = 0$ se traduit en $n \cdot (ds+dM)^i$ équations dans K.

Chacune de ces équations est polynomiale en les variables $\mu_{k,j,I}$, elles tracent donc une variété algébrique dans K^{NnM^i}. La théorie de la dimension, sur laquelle nous ne reviendrons pas ici, nous apprend que cette variété, si elle n'est pas vide, a pour dimension au moins $NnM^i - n(ds+dM)^i$. Or, comme $N > d^i$, pour M assez grand, $N^{1/i}M > ds + dM$ donc $NnM^i - n(ds+dM)^i > 0$. Or la variété considérée est non vide car elle contient le point 0 (tous les polynômes sont homogènes) et comme elle est de dimension strictement positive, elle contient d'autres points, qui correspondent à des racines non triviales de P. ■

5 La valeur 1 est représentée par les formes d'assez grande dimension

5.1 Le cas des corps

Nous allons montrer le théorème suivant.

Théorème 5.1

Soit K un corps de degré de transcendance au plus d sur $\mathbb{R}$. Soit $\varphi = \langle\!\langle a_1, \ldots, a_k \rangle\!\rangle$ une forme de Pfister à coefficients dans K avec $k > d$ et $k \geq 2$. Soit φ' la sous-forme pure (telle que $\varphi = \langle 1 \rangle \perp \varphi'$). Alors φ' représente 1 sur K.

Démonstration : Si φ est isotrope, alors elle contient la forme $\langle 1, -1 \rangle$. Alors φ' représente -1, donc par le lemme 3.24, on peut écrire $\varphi = \langle\!\langle -1, b_2 \ldots, b_k \rangle\!\rangle$ pour certains b_i. Comme $k \geq 2$, φ' contient la forme $\langle b_2, -b_2 \rangle$, qui représente 1. On peut donc maintenant supposer que φ est anisotrope.

La forme φ est de dimension 2^k donc par le théorème de Tsen–Lang (théorème 4.5), elle est isotrope sur $K[i]$, où i est une racine carrée de -1. En effet, si K est de degré de transcendance au plus d sur $\mathbb{R}$, alors $K[i]$ est une extension de $\mathbb{C}$ de degré de transcendance au plus d (on peut prendre la même partie génératrice). Par conséquent, $i \notin K$. La forme φ est isotrope sur $K[i]$, donc sur $K[i](X,Y)$, donc représente toutes les valeurs sur ce corps, en particulier $X + iY$. Alors il existe $h \in K[i](X,Y)^{2^k}$ tels que $\varphi(h) = X + iY$. Il existe $h = u + iv$ où $u, v \in K(X,Y)^{2^k}$. En notant $g = \frac{v}{Y}$ et $f = u - Xg$, on a $h = f + (X+iY)g$ et donc :

$$\varphi(f + (X+iY)g) = X + iY.$$

En nommant B_φ la forme bilinéaire associée à φ, on obtient

$$\varphi(g)(X+iY)^2 + (2B_\varphi(f,g) - 1)(X+iY) + \varphi(f) = 0.$$

D'après le lemme 3.17, φ est anisotrope sur $K(X,Y)$ donc $\varphi(g) \neq 0$, donc $(X+iY)$ est racine d'un polynôme de degré deux à coefficients dans $F(X,Y)$. Ce polynôme est donc multiple du polynôme minimal de $(X+iY)$ sur $F(X,Y)$, qui n'est autre que $P(T) = T^2 - 2XT + X^2 + Y^2$ car $i \notin F(X,Y)$. La relation de divisibilité entre les polynômes donne

$$\varphi(g)(X^2 + Y^2) = \varphi(f).$$

Comme $\varphi(g) \neq 0$ et φ est multiplicative (théorème 3.22), on a φ représente $X^2 + Y^2$ sur $F(X,Y)$. On peut appliquer la proposition 3.18 pour obtenir $\varphi \simeq \langle 1, 1\rangle \perp \theta$ pour une certaine forme θ. Par théorème d'annulation de Witt, $\varphi' \simeq \langle 1\rangle \perp \theta$, qui représente 1. ■

5.2 Le cas des anneaux

Nous allons maintenant généraliser le théorème précédent à des anneaux. Pour cela, nous introduisons une classe d'anneaux sur lequel une version faible du théorème sera vraie.

Définition 5.2 (*Anneau régulier de fonctions (ARF)*)

Un anneau régulier de fonctions (ARF) est un anneau de fractions d'une $\mathbb{R}$-algèbre de type finie tel que tous les éléments de la forme $1 + \sum_i a_i^2$ sont inversibles.

Nous pouvons maintenant énoncer le théorème :

Théorème 5.3

*Soit A un ARF de degré de transcendance au plus d sur $\mathbb{R}$. Soit $\varphi = \langle\langle a_1, \ldots, a_k\rangle\rangle$ une forme de Pfister à coefficients dans A avec $k > d$ et $k \geq 2$. Soit φ' la sous-forme pure (telle que $\varphi = \langle 1\rangle \perp \varphi'$). Alors φ' représente **faiblement** 1 sur A.*

Pour la preuve, nous allons utiliser le résultat suivant, vrai sur des anneaux plus généraux et conséquence du théorème 8.7 dans [AM94].

Lemme 5.4

L'anneau de fractions total d'un ARF sans élément nilpotent non nul, obtenu en inversant tous les éléments n'étant pas des diviseurs de 0, est un produit d'un nombre fini de corps.

Démonstration du théorème 5.3 : On raisonne par récurrence sur d. L'initialisation et l'hérédité commencent de la même manière, donc fixons un $d \geq 0$ et si $d > 0$, supposons le théorème vrai pour tous les ARFs de degré de transcendance au plus $d - 1$.

On veut appliquer le lemme 5.4 et donc la première étape est de se ramener au cas où il n'y a pas d'éléments nilpotents non nuls. Soit $N \subset A$ l'idéal des éléments nilpotents. On vérifie que A/N est un ARF de degré de transcendance au plus d. Si 1 est faiblement représenté sur A/N on a $b \in N$ et $a_i \in A$ tels que $1 + b = \sum_i \varphi(a_i)$. Comme b est nilpotent, on peut définir $s = (1+b)^{-1/2}$ par le développement limité de $x \mapsto (1+x)^{-1/2}$ arrêté au degré de nilpotence de b. Alors on a $s^2(1+b) = 1$. Donc $1 = \sum_i \varphi(s \cdot a_i)$. On peut donc remplacer A par A/N et supposer que $N = 0$.

Maintenant, considérons B l'anneau de fraction total de A. En vertu du lemme, on a $B = \prod_i K_i$ pour un nombre fini de corps K_i. Ces corps sont de degré de transcendance au plus d car la partie algébriquement génératrice de cardinal d de A justifie que B soit de degré de transcendance au plus d sur $\mathbb{R}$, et donc K_i aussi.

Si $d = 0$, le corps K_i est une extension algébrique de $\mathbb{R}$, donc $\mathbb{R}$ ou $\mathbb{C}$. Mais si un K_i, disons K_1, est égal à $\mathbb{C}$, alors $1 + (i, 0, 0, \ldots, 0)^2 = 0$ n'est pas inversible. Donc B est un produit de copies de $\mathbb{R}$. Comme A est une sous-$\mathbb{R}$-algèbre de B, c'est elle-même un produit de copies de $\mathbb{R}$. On a $\varphi' = \langle a_1, a_2, a_1a_2\rangle \perp \theta$ où θ est une forme quadratique. Sur chacune de ces copies de $\mathbb{R}$, a_1, a_2 et a_1a_2 se projettent en 3 réels ne pouvant être tous les trois négatifs, donc 1 est représenté sur chacune des copies, donc sur A.

Si $d > 0$, par le théorème 5.1, la valeur 1 est représenté par φ' sur chacun de ces K_i, donc 1 est représenté par φ' sur B, disons par u/f où $u, f \in A$ et f n'est pas un diviseur de 0 dans A. Si f est inversible dans A, la valeur 1 est représentée par φ' dans A. Supposons donc que f n'est pas inversible dans A. On a $f^2 = \varphi'(u)$. Nous allons maintenant utiliser le lemme suivant :

Sous-Lemme 5.5

Si f n'est pas un diviseur de 0 dans un ARF A de degré de transcendance inférieur à d, alors A/f est un ARF de degré de transcendance inférieur à $d - 1$.

Démonstration : Il est clair que A/f est un ARF.

Considérons $u_1, \ldots, u_d$ une base de transcendance de A. Alors f et les u_i sont algébriquement liés par un polynôme non nul à coefficients dans A : $P(f, u_1, \ldots u_d) = 0$. Comme

f n'est pas un diviseur de 0, P ne peut pas être constant en chacun des u_i, supposons le non-constant en u_d. Alors $\mathbb{R}[f, u_1, \dots u_d]/\mathbb{R}[f, u_1, \dots u_{d-1}]$ est une extension algébrique. Or $A/\mathbb{R}[u_1, \dots u_d]$ est une extension algébrique, donc $A/\mathbb{R}[f, u_1, \dots u_d]$ aussi. La composée de deux extensions algébriques est algébrique, donc $A/\mathbb{R}[f, u_1, \dots u_{d-1}]$ est algébrique.

Il reste à prouver que $(A/f)/\mathbb{R}[u_1, \dots u_{d-1}]/f$ est alors également algébrique. Pour cela, prenons $x \in A$. On a un polynôme non nul $P(x, f, u_1, \dots, u_{d-1}) = 0$. Si ce polynôme est multiple de sa deuxième variable, comme f n'est pas un diviseur de 0, on peut diviser cette équation polynomiale par f. Recommençons jusqu'à ce qu'il y ait un terme constant en f. Ce terme constant en f est un polynôme Q non nul tel que $Q(x, u_1, u_2, \dots u_{d-1})$ est multiple de f. Donc $Q(x, u_1, u_2, \dots u_{d-1}) = 0$ dans A/f. Ceci conclut. ■

Le lemme nous permet d'utiliser notre hypothèse de récurrence sur A/f. On obtient

$$1 + bf = \sum_i \varphi'(v_i).$$

En passant le 1 de l'autre côté avant de mettre au carré et en utilisant $f^2 = \varphi'(u)$, on obtient

$$\left(1 - \sum_i \varphi'(v_i)\right)^2 = b^2 f^2 = \varphi'(bu).$$

On développe partiellement le carré et on pose $w_i = \sqrt{2} v_i$ ainsi que $s = \sum_i \varphi'(v_i)$ pour obtenir

$$1 + s^2 = \varphi'(bu) + \sum_i \varphi'(w_i).$$

Par définition d'un ARF, $1 + s^2$ est inversible donc on peut écrire

$$1 = \varphi'\left(\frac{bu}{1+s^2}\right) + \varphi'\left(\frac{s \cdot bu}{1+s^2}\right) + \sum_i \varphi'\left(\frac{w_i}{1+s^2}\right) + \sum_i \varphi'\left(\frac{s \cdot w_i}{1+s^2}\right),$$

ce qui conclut. ■

6 Preuve du théorème 1.2

On rappelle l'énoncé du théorème :

Théorème 6.1 (*Scheiderer–Bröcker*)

Tout ouvert semi-algébrique basique $\mathcal{U} = \{x \in \mathbb{R}^n \mid g_1(x) > 0, \dots, g_k(x) > 0\}$ *de* $\mathbb{R}^n$ *est exprimable sous la forme* $\mathcal{U} = \{x \in \mathbb{R}^n \mid f_1(x) > 0, \dots, f_n(x) > 0\}$ *pour des* $f_i \in \mathbb{R}[X_1, \dots X_n]$ *bien choisis.*

Démonstration : Dans la suite, on supposera $k = n + 1$. En effet, si on sait éliminer une inéquation d'un groupe de $n + 1$, on peut itérer cette construction pour enlever toutes les inéquations sauf n.

Considérons la forme de Pfister sur le corps $\mathbb{R}(X_1 \dots X_n)$, de dimension $n+1$: $\varphi = \langle\langle g_1, \dots, g_{n+1}\rangle\rangle$. C'est cette forme que nous allons essayer de réécrire $\varphi \simeq \langle\langle 1, h_2 \dots, h_{n+1}\rangle\rangle$ pour réécrire $\mathcal{U}$ avec seulement n polynômes, $h_2, \dots h_{n+1}$. Nommons φ' la sous-forme pure de φ, telle que $\varphi = \langle 1\rangle \perp \varphi'$.

Considérons $\Sigma\mathcal{U}$ la partie de $\mathbb{R}[X_1 \dots X_n]$ constituée des polynômes prenant sur $\mathcal{U}$ uniquement des valeurs strictement positives. Par hypothèse, $g_1, \dots g_{n+1} \Sigma\mathcal{U}$. Comme $1 \in \Sigma\mathcal{U}$ et comme $\Sigma\mathcal{U}$ est stable par multiplication, on peut considérer l'anneau localisé $(\Sigma\mathcal{U})^{-1}\mathbb{R}[X_1 \dots X_n]$. Cet anneau est défini comme l'anneau où l'on a inversé tous les éléments de $\Sigma\mathcal{U}$. Comme $\mathbb{R}[X_1 \dots X_n]$ est intègre, ce localisé est le sous-anneau du corps de fractions de $\mathbb{R}(X_1, \dots, X_n)$ engendré par $X_1 \dots X_n$ ainsi que les inverses des éléments de $\Sigma\mathcal{U}$.

Par le théorème précédent, comme $(\Sigma\mathcal{U})^{-1}\mathbb{R}[X_1 \dots X_n]$ est un anneau régulier (voir la définition 5.2) de fonctions de degré de transcendance au plus n sur $\mathbb{R}$, le nombre 1 est faiblement représenté par φ' sur $(\Sigma\mathcal{U})^{-1}\mathbb{R}[X_1 \dots X_n]$. Par conséquent, le carré $(1 - g_{d+1} + g_{d+1}^2)^2$ est aussi faiblement représenté. On va vouloir appliquer le lemme 3.26, dont on reprend les notations : $\varphi_i = \langle\langle g_1, \dots, g_i\rangle\rangle$, $\varphi_0 = \langle 1\rangle$. On a alors

$$\varphi' = g_1\varphi_0 \perp g_2\varphi_1 \perp g_3\varphi_2 \perp \dots \perp g_{n+1}\varphi_n.$$

La représentation faible de $(1 - g_{d+1} + g_{d+1}^2)^2$ donne l'égalité suivante :

$$(1 - g_{d+1} + g_{d+1}^2)^2 = g_1u_1 + g_2u_2 + \dots + g_du_d + g_{d+1}u_{d+1},$$

où u_{i+1} est faiblement représenté par φ_i pour $0 \leq i \leq n$. Cela se réécrit

$$(1+g_{d+1}^2)^2 = g_1u_1 + g_2u_2 + \ldots + g_du_d + g_{d+1}(u_{d+1} + 2 + 2g_{d+1}^2 - g_{d+1}).$$

Or les coefficients diagonaux de φ_n sont strictement positifs sur $\mathcal{U}$ donc u_{d+1} est positif sur $\mathcal{U}$ donc $u_{d+1} + 2 + 2g_{d+1}^2 - g_{d+1}$ est strictement positif sur $\mathcal{U}$. De plus, les u_i sont dans $(\Sigma\mathcal{U})^{-1}\mathbb{R}[X_1 \ldots X_n]$ donc on peut multiplier cette égalité par le carré de son dénominateur, strictement positif sur $\mathcal{U}$. On obtient une égalité de la forme

$$w_0^2 = g_1v_1 + g_2v_2 + \ldots + g_dv_d + g_{d+1}v_{d+1},$$

où v_{i+1} est faiblement représenté par φ_i et où v_{d+1} est strictement positif sur $\mathcal{U}$. On peut appliquer le lemme 3.26 : définissons $w_i = \sum_{j=i+1}^n g_jv_j$, $f_i = g_iw_i$ et $\psi = \langle\langle w_0, f_1, \ldots, f_n \rangle\rangle$. Alors pour tout $x \in \mathbb{R}^n$ tel que $(\varphi_m)_x$ et $(\psi)_x$ soient non dégénérées, on a $(\varphi_m)_x \simeq (\psi)_x$, et ces deux formes ont donc la même signature.

Il reste à montrer que $f_1, \ldots f_n$ définissent le même ouvert semi-algébrique basique que $g_1, \ldots g_{n+1}$, c'est-à-dire que les points de $\mathbb{R}^n$ où tous les f_i sont strictement positifs sont exactement ceux de $\mathcal{U}$. Si on prend un point $x \in \mathcal{U}$, par construction de f_i, celui-ci est strictement positif. Réciproquement, si tous les f_i sont strictement positifs en $x \in \mathbb{R}^n$, alors $(\psi)_x$ est non dégénéré, et comme les g_i divisent les f_i ils ne peuvent pas être nuls non plus, donc $(\varphi)_x$ est également non dégénérée. Donc $(\varphi_m)_x \simeq (\psi)_x$, et les deux formes ont la même signature (théorème 3.20). Comme $(\psi)_x$ a tous ses termes diagonaux positifs par hypothèse, on deduit que $(\varphi)_x$ aussi, et donc que $x \in \mathcal{U}$. ∎

7 Optimalité du résultat

Dans cette section, nous montrons que le théorème est optimal même avec la condition "génériquement égaux" moins fort que la condition égaux. Cette généralisation permet d'effectuer une récurrence.

Définition 7.1

Deux parties semi-algébrique S et T d'un ensemble algébrique irréductible V sont génériquement égaux dans V si

$$\dim((S \setminus T) \cup (T \setminus S)) < \dim(V) .$$

Dans cette définition, la dimension est au sens de la $\mathcal{C}^\infty$-variété. Ceci revient à dire que S et T sont denses l'un dans l'autre.

Théorème 7.2

Il n'existe pas des polynômes $f_1, \ldots, f_{n-1} \in \mathbb{R}[X_1, \ldots, X_n]$ tel que

$$\mathcal{U}(f_1, \ldots, f_{n-1}) = \{x \in \mathbb{R}^n \mid f_1(x) > 0, \ldots, f_{n-1}(x) > 0\}$$

est génériquement égal à $A_n = \{x \in \mathbb{R}^n \mid x_1 > 0, \ldots, x_n > 0\}$.

Démonstration : Procédons par récurrence sur n. Le théorème est vrai pour $n = 2$, car sinon le degré de $P_{y_0}(X) = f_1(X, y_0)$ doit être impair si $y_0 > 0$ et pair si $y_0 < 0$, mais pour tous les y_0 sauf un nombre fini, le degré de P_{y_0} est le degré en la première variable de f_1, qui ne peut pas être simultanément pair et impair.

Supposons par l'absurde que, il existe $n > 2$ et $f_1, \ldots, f_{n-1} \in \mathbb{R}[x_1, \ldots, x_n]$ tel que A_n et $\mathcal{U}(f_1, \ldots, f_{n-1})$ sont génériquement égaux, on suppose pour la suite que n soit minimum. A_n et $\mathcal{U}(f_1, \ldots, f_{n-1})$ génériquement égaux implique que A_n est dans l'adhérence de $\mathcal{U}(f_1, \ldots, f_{n-1})$, donc que les f_i sont positives sur A_n. Soit $X_n^{e_i}$ la puissance plus grande de X_n qui divise f_i. On a alors $f_i = X_n^{e_i}g_i$ où $g_i(X', 0) \neq 0$ dans $\mathbb{R}[X'] = \mathbb{R}[X_1, \ldots, X_{n-1}]\cdot$ On ne peut pas avoir que tous les e_i sont pairs car pour chaque $X' \in \mathbb{R}^{n-1}$, au moins un de f_i doit changer de signe en $X_n = 0$, donc un des f_i change de signe en $X_n = 0$ quel que soit X', donc un e_i est impair.

Donc on peut supposer par exemple que, pour $i = 1, \ldots, r-1, e_i$ est impair et pour $i = r, \ldots, n-1, e_i$ est pair $(1 < r \leq n-1)$. Définissons :

$$B = \{x' \in \mathbb{R}^{n-1} \mid g_1(x', 0)g_i(x', 0) > 0 \text{ pour } 1 < i \leq r-1, g_j(x', 0) > 0 \text{ pour } r \leq j \leq n-1\}.$$

Observons que B est défini par $n-2$ inégalités. Donc il suffit de montrer que B et A_{n-1} sont génériquement égaux pour trouver une contradiction avec notre hypothèse.

Comme les f_l sont positives sur A_n, on a les g_l sont aussi positives sur A_n, donc :

$$A_{n-1} \setminus \{x' \in \mathbb{R}^{n-1} \mid \prod_{i=1}^{n} g_i(x', 0) = 0\} \subset B.$$

Donc

$$A_{n-1} \setminus B \subset \{x' \in R_{n-1} \mid \prod_{i=1}^{n} g_i(x', 0) = 0\}$$

et on a $\dim(A_{n-1} \setminus B) < n - 1$.

Considérons $b' \in B$ tel que $g_1(b', 0) \neq 0$. Notons que sauf si $r = 2$, c'est forcément le cas. Il existe une boule ouverte $\Gamma \in \mathbb{R}^n$ centrée au $(b', 0)$ tel que pour $i = 1, \ldots, r-1$ les $g_i(x)$ sont de même signe que $g_1(b', 0)$ sur Γ et que pour $j = r, \ldots, n-1, g_j(x) > 0$ sur Γ.

Donc il existe une demi-boule découpée par $X_n = 0$, celle où $X_n > 0$ si $g_1(b', 0) > 0$ et celle où $X_n < 0$ si $g_1(b', 0) < 0$ sur laquelle tous les f_l sont positifs pour $l = 1, \ldots, n-1$. Cette demi-boule est incluse dans $\mathcal{U}(f_1, \ldots, f_{n-1})$, donc $(b', 0) \in \overline{A_n}$, et donc $b' \in \overline{A_{n-1}}$. On a alors

$$B \setminus \{x' \in \mathbb{R}^{n-1} \mid g_1(x', 0) = 0\} \subset \overline{A_{n-1}}.$$

Donc

$$B \setminus \overline{A_{n-1}} \subset \{x' \in \mathbb{R}^{n-1} \mid g_1(x', 0) = 0\}.$$

Donc

$$B \setminus A_{n-1} \subset \{x' \in \mathbb{R}^{n-1} \mid g_1(x', 0) = 0\} \cup \overline{A_{n-1}} \setminus A_{n-1}$$

et on a $\dim(B \setminus A_{n-1}) < n - 1$. Ceci complète la démonstration. ■

Bibliographie

[Sch89] C. Scheiderer. “Stability index of real varieties”. In : *Inventiones mathematicae* (1989), p. 115-127.

[AM94] M. F. Atiyah et I. G. MacDonald. Addison-Wesley, 1994, p. 90.

[BCR98] J. Bochnak, M. Coste et M-F. Roy. *Real Algebraic Geometry*. Springer, 1998.

[Kah09] B. Kahn. *Forme quadratique sur un corps*. Société Mathématique de France, 2009, p. 1-28.