Développement 1

Théorème de Springer

Théorème. *Soit (V, q) un k-espace quadratique anisotrope et K/k une extension de corps vérifiant l'une des conditions suivantes :*

(i) K est transcendante pure.

(ii) K est algébrique de degré impair.

Alors V_K est anisotrope.

En se plaçant dans une base orthogonale, on se ramène au cas où q est de la forme $q(x) = a_1 x_1^2 + \cdots + a_n x_n^2$.

(i) Si V_K est isotrope, V devient déjà isotrope sur une extension transcendante pure de type fini de k. Par récurrence sur le degré de transcendance, on peut supposer $K = k(T)$. Si V_K est isotrope, il vient, en éliminant les dénominateurs éventuels, des polynômes $P_1, \ldots, P_n$ de $k[T]$ tels que :

$$a_1 P_1^2 + \cdots + a_n P_n^2 = 0$$

On peut de plus supposer les P_i premiers entre eux dans leur ensemble, et en particulier non tous divisibles par T. En évaluant alors en 0, il vient :

$$a_1 P_1(0)^2 + \cdots + a_n P_n(0)^2 = 0 \quad \text{avec } \big(P_1(0), \ldots, P_n(0)\big) \neq (0, \ldots, 0)$$

ce qui contredit l'anisotropie de V.

(ii) Comme précédemment, on peut supposer $K = k(\alpha)$ monogène, et l'on raisonne alors par récurrence sur le degré $d = [K : k]$. Soit $R \in k[T]$ le polynôme minimal de α. Si V_K est isotrope, il existe des polynômes $P_1, \ldots, P_n$ de degrés $< d$ tels que :

$$a_1 P_1^2 + \cdots + a_n P_n^2 = QR \quad \text{pour un certain } Q \in k[T]$$

On peut les supposer premiers entre eux dans leur ensemble. Posons alors $m = \max(\deg P_i)$. En considérant les coefficients dominants des polynômes qui interviennent dans l'équation précédente, on voit que $\deg Q = 2m - d$. En particulier, $\deg Q$ est impair et inférieur à $2(d-1) - d = d - 2$. Choisissons alors une racine β de Q dans une clôture algébrique de k. On a visiblement :

$$a_1 P_1(\beta)^2 + \cdots + a_n P_n(\beta)^2 = 0$$

et les $P_i(\beta)$ ne sont pas tous nuls par primalité. Par conséquent, $V_{k(\beta)}$ est isotrope, ce qui contredit l'hypothèse de récurrence.

Développement 2
Formes de Pfister

Théorème. *Soit $V \cong \langle\langle a_1, \ldots, a_n \rangle\rangle$ une forme de Pfister.*

(i) Si V est isotrope, alors V est hyperbolique.

(ii) $D(V)$ (l'ensemble des éléments de $k^\times$ représentés par V) est l'ensemble des $a \in k^\times$ tels que $\langle a \rangle \otimes V \cong V$. En particulier, c'est un sous-groupe de $k^\times$.

Montrons tout d'abord le résultat en admettant le lemme suivant :

Lemme. *Soit V une n-forme de Pfister, et $b \in D(V_p)$. Alors il existe $b_2, \ldots, b_n$ dans $k^\times$ tels que $V \cong \langle\langle b, b_2, \ldots, b_n \rangle\rangle$.*

(i) Si V est isotrope, elle contient un plan hyperbolique, et donc V_p représente -1. D'après le lemme, on a donc $V \cong \langle\langle -1, \ldots \rangle\rangle$, ce qui assure que V est hyperbolique.

(ii) Comme une forme de Pfister représente toujours 1, si $\langle a \rangle \otimes V \cong V$, on a $a \in D(V)$. Réciproquement, soit $a \in D(V)$. Comme $V = \langle 1 \rangle \oplus V_p$, a s'écrit $t^2 + b$, avec $t \in k$ et $b \in D(V_p) \cup \{0\}$. Si $b = 0$, il n'y a rien à prouver. Sinon, d'après le lemme, $V \cong \langle\langle b, b_2, \ldots, b_n \rangle\rangle$. Ainsi :

$$\langle a \rangle \otimes V \cong \langle a \rangle \otimes \langle 1, b \rangle \otimes \langle\langle b_2, \ldots, b_n \rangle\rangle \cong \langle a, ab \rangle \otimes \langle\langle b_2, \ldots, b_n \rangle\rangle$$

Mais comme $a \in D(\langle 1, b \rangle)$, on a $\langle a, ab \rangle \cong \langle 1, b \rangle$, ce qui conclut.

Prouvons maintenant le lemme. On admettra les deux résultats suivants sur les 2-formes de Pfister (valables quand tout a un sens), qui sont des calculs simples :

$$\langle\langle u, v \rangle\rangle \cong \langle\langle u, (u + t^2)v \rangle\rangle \quad \text{et} \quad \langle\langle u, v \rangle\rangle \cong \langle\langle u + v, uv \rangle\rangle$$

On note $V = \langle\langle a_1, \ldots, a_n \rangle\rangle$ et l'on procède par récurrence sur n. Si $n = 1$ le résultat est clair. Sinon, posons $W = \langle\langle a_1, \ldots, a_{n-1} \rangle\rangle$. On a alors $V = W \oplus \langle a_n \rangle W$, et en particulier, $V_p = W_p \oplus \langle a_n \rangle W$. Le scalaire b s'écrit donc $a_n x + y$ avec $x \in D(W) \cup \{0\}$ et $y \in D(W_p) \cup \{0\}$, non simultanément nuls.

Premièrement, si $x = 0$, alors $b \in D(W_p)$ et par hypothèse de récurrence, il existe $b_2, \ldots, b_{n-1}$ tels que $W \cong \langle\langle b, b_2, \ldots, b_{n-1} \rangle\rangle$. Et alors $V \cong \langle\langle b, b_2, \ldots, b_{n-1}, a_n \rangle\rangle$, ce qui conclut.

Si maintenant $x \neq 0$, il se décompose sous la forme $x = x_0 + t^2$, avec $x_0 \in D(W_p) \cup \{0\}$ et $t \in k$ non tous deux nuls. On a alors $V \cong \langle\langle a_1, \ldots, a_{n-1}, x a_n \rangle\rangle$. En effet, si $x_0 = 0$ c'est clair, et sinon, il existe $c_2, \ldots, c_{n-1}$ tels que $W \cong \langle\langle x_0, c_2, \ldots, c_{n-1} \rangle\rangle$. Mais alors :

$$V \cong \langle\langle x_0, c_2, \ldots, c_{n-1}, a_n \rangle\rangle \cong \langle\langle x_0, c_2, \ldots, c_{n-1}, (x_0 + t^2) a_n \rangle\rangle \cong \langle\langle a_1, \ldots, a_{n-1}, x a_n \rangle\rangle$$

Si $y = 0$, $x a_n = b$ et on a terminé. Sinon, $y \in D(W_p)$, et alors $W \cong \langle\langle y, d_2, \ldots, d_{n-1} \rangle\rangle$. Il vient alors :

$$V \cong \langle\langle y, d_2, \ldots, d_{n-1}, x a_n \rangle\rangle \cong \langle\langle y + x a_n, d_2, \ldots, d_{n-1}, x y a_n \rangle\rangle \cong \langle\langle b, d_2, \ldots, d_{n-1}, x y a_n \rangle\rangle$$

ce qui conclut.

Développement 3

Algèbres de quaternions

Théorème. *Soit A et A' deux algèbres de quaternions. Les assertions suivantes sont équivalentes :*

(i) A et A' sont isomorphes comme algèbres.

(ii) A et A' sont isomorphes comme espaces quadratiques.

(iii) A_0 et A'_0 sont isomorphes comme espaces quadratiques.

Comme espaces quadratiques, on a $A = \langle 1\rangle \oplus A_0$ et $A' = \langle 1\rangle \oplus A'_0$, donc l'équivalence de (ii) et (iii) résulte du théorème de simplification de Witt. Supposons maintenant A et A' isomorphes comme algèbre, et soit $f : A \to A'$ un isomorphisme. Comme A_0 est caractérisé algébriquement comme l'ensemble des éléments de A non dans k et de carré dans k, et de même pour A'_0, f envoie A_0 sur A'_0 et préserve donc la conjugaison. Il en résulte que $Nf(x) = f(x)\overline{f(x)} = f(x)f(\bar{x}) = f(Nx) = Nx$ pour tout $x \in A$, et donc f est un isomorphisme d'espaces quadratiques.

Écrivons maintenant $A = \left(\frac{a,b}{k}\right)$, de générateurs i et j, et supposons qu'il existe un isomorphisme d'espaces quadratiques $f : A_0 \to A'_0$. Alors $Nf(i) = Ni = -a$. Mais par ailleurs $Nf(i) = f(i)\overline{f(i)} = -f(i)^2$. Donc $f(i)^2 = a$ et de même $f(j)^2 = b$. De plus, $f(i)$ et $f(j)$ sont orthogonaux, donc $f(i)f(j) = -f(j)f(i)$. Cela montre que $A' \cong \left(\frac{a,b}{k}\right) = A$, d'où le résultat.

Corollaire. *Soit A une algèbre de quaternions. Les assertions suivantes sont équivalentes : (i) $A \cong M_2(k)$. (ii) A isotrope. (iii) A_0 isotrope. (iv) A hyperbolique. (v) A n'est pas une algèbre à division. On dit alors que A est décomposée.*

Les propriétés (ii), (iii) et (iv) sont équivalentes d'après le théorème sur les formes de Pfister. Si A est isomorphe à $M_2(k)$, $A \cong \langle\langle 1, -1\rangle\rangle$ est bien hyperbolique, et comme il existe un seul espace hyperbolique de rang 4 à isomorphisme près, la réciproque est vraie. Enfin, $M_2(k)$ n'est pas une algèbre à division, et si, à l'inverse, A est un espace quadratique anisotrope, alors pour tout $x \in A\{0\}$, $\bar{x}/Nx$ est un inverse de x à gauche et à droite, donc A est une algèbre à division.

Corollaire. *Soit p un nombre premier congru à 3 modulo 8. Alors $A = \left(\frac{-p,-1}{\mathbf{Q}}\right)$ est une algèbre à division sur $\mathbf{Q}$ qui vérifie $A_{\mathbf{Q}_\ell} = M_2(\mathbf{Q}_\ell)$ pour tout $\ell \neq p$, $A_{\mathbf{Q}_p} \neq M_2(\mathbf{Q}_p)$ et $A_{\mathbf{R}} = \mathbf{H}$.*

En effet, comme espace quadratique, on a $A_0 \cong \langle 1, p, p\rangle$, donc A se décompose sur une extension K de $\mathbf{Q}$ si et seulement si la forme quadratique $q = x^2 + py^2 + pz^2$ y est isotrope. En particulier, $A_{\mathbf{R}} = \mathbf{H}$ et A est une algèbre à division. Par ailleurs, si ℓ est un nombre premier impair, q a un vecteur isotrope dans $\mathbf{F}_\ell$ et le lemme de Hensel permet de le relever à $\mathbf{Z}_\ell$, donc à $\mathbf{Q}_\ell$. De même, comme $q(1,1,2) \equiv 1 + 5p \equiv 0 \pmod 8$, q est isotrope dans $\mathbf{Q}_2$. Enfin, comme -1 n'est pas carré modulo p, q n'a visiblement pas de zéro non trivial dans $\mathbf{Z}/p^2\mathbf{Z}$, donc a fortiori pas non plus dans $\mathbf{Q}_p$.