Prérequis. Aucun.

Théorème 0.0.1. *Soient* $\mathbf{L}/\mathbf{K}$ *une extension finie de degré impair et* q *une forme quadratique sur* $\mathbf{K}^n$*. Si* q *admet un vecteur isotrope dans* $\mathbf{L}^n$ *alors elle en admet un dans* $\mathbf{K}^n$*.*

Démonstration. On démontre le résultat par récurrence sur le degré $m = [\mathbf{L} : \mathbf{K}]$. Le cas $m = 1$ ne demande aucune démonstration, supposons le résultat vrai jusqu'à $m - 2$.

Remarquons d'abord que $\mathbf{L}$ est de la forme $\mathbf{K}[\alpha_1, \ldots, \alpha_k]$, et que chaque extension $\mathbf{K}[\alpha_1, \ldots, \alpha_{s+1}]/\mathbf{K}[\alpha_1, \ldots, \alpha_s]$ est de degré impair. Par hypothèse de récurrence, on peut alors supposer que $k = 1$, c'est-à-dire que $\mathbf{L} = \mathbf{K}[\alpha]$. On notera μ le polynôme minimal de α (qui est donc de degré m).

Soit donc $v \in \mathbf{L}^n$ un vecteur isotrope. On écrit alors $v_i = g_i(\alpha)$ avec $g_i \in \mathbf{K}[X]$ de degré au plus $m - 1$. De l'égalité :

$$0 = q(g_1(\alpha), \ldots, g_n(\alpha)) \in \mathbf{K}[\alpha] \cong \mathbf{K}[X]/\mu,$$

on déduit que le reste de la division euclidienne de $q(g_1, \ldots, g_n)$ par μ est nul. On peut alors écrire $q(g_1, \ldots, g_n) = \mu h$ avec $h \in \mathbf{K}[X]$.

Montrons que l'on peut prendre les g_i premiers entre eux. Soit δ leur pgcd. Alors comme q est une forme quadratique :

$$\delta^2 q(g_1/\delta, \ldots, g_n/\delta) = \mu h,$$

et comme $\deg \delta < m$, il est impossible que μ divise δ. Comme μ est irréductible, ces deux polynômes sont premiers entre eux, donc δ^2 divise h. On peut alors écrire :

$$q(g_1/\delta, \ldots, g_n/\delta) = \mu \tilde{h}$$

avec $\tilde{h}$ de degré plus petit que h et cette fois-ci, les g_i/δ premiers entre eux.

Si $h = 0$, alors par coprimalité des g_i, pour $x \in \mathbf{K}$ il existe i tel que $g_i(x) \neq 0$ donc le vecteur $(g_1(x), \ldots, g_n(x)) \in \mathbf{K}^n$ n'est pas nul et est isotrope.

Supposons alors $h \neq 0$. Comme $q(g_1, \ldots, g_n)$ est de degré pair $< 2m$ (chaque g_i est de degré $< m$) et μ de degré m impair, le degré de h doit être impair et $< m$. Ainsi, h admet un facteur irréductible de degré impair h_0.

On pose alors $\mathbf{L}_0 = \mathbf{K}[X]/h_0 \cong \mathbf{K}[\beta]$ avec β la classe de X. Comme $\deg h_0 \leqslant \deg h < m$, on a $[\mathbf{L}_0 : \mathbf{K}] < [\mathbf{L} : \mathbf{K}]$. Et comme $h_0(\beta) = 0$, on a aussi :

$$q(g_1(\beta), \ldots, g_n(\beta)) = 0.$$

Si tous les $g_i(\beta)$ sont nuls alors h_0 divise g_i ce qui est impossible. Donc le vecteur $(g_1(\beta), \ldots, g_n(\beta))$ est isotrope dans une extension de degré impair $< m$: l'hypothèse de récurrence conclut. □

Remarques.

— Pour éclaircir, le schéma de la preuve est le suivant : on fait une récurrence sur le degré (impair) de $\mathbf{L}/\mathbf{K}$, l'initialisation étant évidente et l'hérédité se faisant en construisant une extension de $\mathbf{K}$ de degré impair et plus petit que celui de $\mathbf{L}/\mathbf{K}$ dans laquelle on a un vecteur isotrope. En fait, on obtient en quelque sorte un algorithme pour passer d'un vecteur isotrope sur $\mathbf{L}$ à un vecteur isotrope sur $\mathbf{K}$, sous réserve de savoir calculer α, son polynôme minimal μ, et l'isomorphisme entre $\mathbf{K}[\alpha]$ et $\mathbf{K}[X]/\mu$. Si l'on sait faire ça, on calcule facilement les polynômes g_i puis les facteur irréductibles de $q(g_1, \dots, g_n)/\mu$. On calcule alors le vecteur isotrope $(g_1(\beta), \dots, g_n(\beta))$ et l'on recommence jusqu'à ce que l'extension soit triviale.

— Il est important d'avoir les idées claires sur l'endroit où l'on utilise le fait que l'extension est de degré impair. C'est quand on dit que h a un facteur irréductible de degré impair, ce qui peut être faux si h est de degré pair. Il faut absolument un contre-exemple dans le cas pair. On peut prendre $\mathbf{K} = \mathbf{R}$ et $\mathbf{L} = \mathbf{C}$, la forme quadratique $x^2 + y^2$ n'a aucun vecteur isotrope sur $\mathbf{R}$ pourtant le vecteur $(1, i)$ est isotrope sur $\mathbf{C}$.

— Ce théorème est important mais au niveau de l'agrégation c'est difficile de donner une motivation compréhensible. Il démontre par exemple l'injectivité du morphisme $W(\mathbf{K} \to \mathbf{L}) : W(\mathbf{K}) \to W(\mathbf{L})$ entre les anneaux de vecteurs de Witt correspondants, ou bien est utile dans l'étude des algèbres de Jordan.

Recasages.

— 125 : C'est en plein dans le mille. On utilise des théorèmes usuels sur les extensions de corps, et on fait un pont avec d'autres leçons (puisque d'habitude, c'est rare de parler de formes quadratiques dans cette leçon).

— 141 : Un peu limite, mais ça passe parce que l'on utilise plusieurs fois l'irréductibilité de μ de manières différentes. Une fois comme polynôme minimal, une fois avec le lemme de Gauss/Euclide, on choisit une fois un facteur irréductible de h, ... Attention alors à bien motiver le théorème en tant que conséquence de quelque chose dans le sujet.

— 144 : C'est borderline. Le théorème s'inscrit dans la même famille que les propriétés du résultant ou le théorème de Gauss-Wantzel ; ici, on obtient des racines dans un petit corps à partir de racines dans un grand corps. Attention par contre à ne pas faire de hors-sujet parce que la leçon doit surtout parler de polynômes à une seule indéterminée.

— 170 : Parfait. En plus, le jury n'aime pas que l'isotropie soit oubliée : ce développement est un cadeau du ciel pour eux (et probablement que ça leur plaira assez pour qu'ils choisissent ce développement à coup sûr, rendant l'autre presque inutile à réviser pendant la préparation).