Recasages possibles : 125, 141, 170.
Référence : Carnet de voyage en algébrie, Caldero, Perronier, (p. 131-133)

Développement

Théorème 1 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps de degré m impair. Soit q une forme quadratique sur $\mathbb{K}^n$ que l'on prolonge naturellement à $\mathbb{L}^n$. Si q admet un vecteur isotrope non nul dans $\mathbb{L}^n$, alors q admet un vecteur isotrope non nul dans $\mathbb{K}^n$.

- *Étape 1* : On se ramène au cas d'une extension monogène. Puisque $\mathbb{L}/\mathbb{K}$ est une extension finie, elle est en particulier de type fini donc il existe $\alpha_1, \dots, \alpha_r \in \mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_r]$. On a donc la tour d'extensions monogènes suivante

$$\mathbb{K} \subset \mathbb{K}[\alpha_1] \subset \mathbb{K}[\alpha_1][\alpha_2] \subset \cdots \subset \mathbb{K}[\alpha_1, \dots, \alpha_{r-1}][\alpha_r] = \mathbb{L}.$$

  Par le théorème de la base télescopique, pour tout $i \in [\![0, r-1]\!]$,

$$\big[\mathbb{K}[\alpha_1, \dots, \alpha_i][\alpha_{i+1}] : \mathbb{K}[\alpha_1, \dots, \alpha_i]\big] \mid [\mathbb{L} : \mathbb{K}] = m.$$

  Ainsi, par imparité de m, toutes les extensions monogènes intervenant dans la tour ci-dessus sont de degré impair. Par conséquent, si on parvient à montrer le théorème dans le cas d'une extension monogène, alors par récurrence sur le nombre r de générateurs de $\mathbb{L}/\mathbb{K}$, on aura montré le théorème dans le cadre général annoncé.

- *Étape 2* : On montre le **Théorème 1** sur les extensions monogènes par récurrence sur $m = [\mathbb{L} : \mathbb{K}] \in 2\mathbb{N} + 1$.
  - Si $m = 1$, alors $\mathbb{L} = \mathbb{K}$ donc tout vecteur isotrope non nul dans $\mathbb{L}^n$ est un vecteur isotrope non nul dans $\mathbb{K}^n$.
  - Soit $m \geqslant 3$ impair. Supposons que pour toute extension monogène de $\mathbb{K}$ de degré $k \leqslant m-2$ impair, et que pour toute forme quadratique sur $\mathbb{K}^n$, le **Théorème 1** est vrai. Soit $\mathbb{L}/\mathbb{K}$ une extension monogène de degré m et q une forme quadratique sur $\mathbb{K}^n$ admettant un vecteur isotrope non nul $x \in \mathbb{L}^n$.

    Par hypothèse, il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$. Notons $\mu \in \mathbb{K}[X]$ le polynôme minimal de α sur $\mathbb{K}$ et remarquons que le polynôme μ est de degré m. Écrivons $x = (x_1, \dots, x_n) \in \mathbb{L}^n$, de sorte que pour tout $i \in [\![1, n]\!]$, $x_i \in \mathbb{L} = \mathbb{K}[\alpha]$ donc il existe $P_i \in \mathbb{K}[X]$ de degré $\leqslant m-1$ tel que $x_i = P_i(\alpha)$. De plus, le n-uplet $\big(P_1(\alpha), \dots, P_n(\alpha)\big) = x$ est non nul, donc les P_i sont non tous nuls. Comme q est une forme quadratique sur $\mathbb{K}^n$, on peut voir q comme un polynôme homogène de degré 2 dans $\mathbb{K}[X_1, \dots, X_n]$. Notons alors

$$Q(X) = q\big(P_1(X), \dots, P_r(X)\big) \in \mathbb{K}[X].$$

On a par construction $Q(\alpha) = q(x) = 0$, donc $\mu \mid Q$ dans $\mathbb{K}[X]$, c'est-à-dire qu'il existe $A \in \mathbb{K}[X]$ tel que $Q = \mu A$. Posons $D = \operatorname{pgcd}(P_1, \dots, P_n)$ et notons $\Pi_1, \dots, \Pi_n$ les polynômes de $\mathbb{K}[X]$ premiers entre eux dans leur ensemble tels que $\forall i \in [\![1, n]\!]$, $P_i = D\Pi_i$. Comme q est un polynôme homogène de degré 2, on a

$$D^2 q(\Pi_1, \dots, \Pi_n) = q(D\Pi_1, \dots, D\Pi_n) = q(P_1, \dots, P_n) = Q = \mu A.$$

Ainsi, $D^2 \mid \mu A$. Or, si μ divisait D, alors μ diviserait $P_1, \dots, P_n$ donc le vecteur $x = \big(P_1(\alpha), \dots, P_n(\alpha)\big)$ serait nul, ce qui est exclu. Ainsi $\mu \nmid D$ et par irréductibilité de μ, μ et D sont premiers entre eux, et donc μ et D^2 sont premiers entre eux (D^2 ayant les mêmes facteurs irréductibles que D dans l'anneau factoriel $\mathbb{K}[X]$). Ainsi, d'après le lemme de Gauss, $D^2 \mid A$ et en notant $\widetilde{A}$ le polynôme de $\mathbb{K}[X]$ tel que $A = D^2\widetilde{A}$, on obtient

$$\widetilde{Q} := q(\Pi_1, \dots, \Pi_n) = \mu\widetilde{A}. \qquad (*)$$

Remarquons que si l'on note $k = \max\limits_{i \in [\![1,n]\!]} \big(\deg(\Pi_i)\big)$, alors q étant homogène de degré 2, on a $\deg\big(\widetilde{Q}\big) \leqslant 2k$. Distinguons alors selon le degré de $\widetilde{Q}$:

  - Supposons que $\deg\big(\widetilde{Q}\big) < 2k$. Pour tout $i \in [\![1, n]\!]$, notons a_i le coefficient de Π_i devant X^k. Remarquons que $(a_1, \dots, a_n) \in \mathbb{K}^n \setminus \{0\}$. Or, $q(a_1, \dots, a_n)$ est exactement le coefficient devant X^{2k} dans $\widetilde{Q}$, donc comme ce dernier est de degré $< 2k$, on a $q(a_1, \dots, a_n) = 0$, ce qui fournit un vecteur isotrope non nul dans $\mathbb{K}^n$, et conclut donc ce cas.

  - Supposons alors que $\deg\big(\widetilde{Q}\big) = 2k$. Alors, comme μ est de degré m impair, $\widetilde{A}$ qui est non nul (sinon $\widetilde{Q}$ le serait) est nécessairement de degré impair. En particulier, $\widetilde{A}$ n'est pas constant, et donc possède des diviseurs irréductibles dans $\mathbb{K}[X]$. S'ils étaient tous de degré pair, alors $\widetilde{A}$ le serait aussi ce qui est faux, donc il en existe au moins un de degré impair. Notons le Π. On remarque que comme pour tout $i \in [\![1, n]\!]$, $\deg(P_i) < m$, on a

$$\deg(\Pi) \leqslant \deg(\widetilde{A}) \leqslant \deg(A) = \deg(Q) - \deg(\mu) < 2m - m = m.$$

On considère alors $\widetilde{\mathbb{L}} = \mathbb{K}[\beta]$ un corps de rupture de Π sur $\mathbb{K}$, avec donc $\Pi(\beta) = 0$. On a $\left[\widetilde{\mathbb{L}} : \mathbb{K}\right] = \deg(\Pi)$ qui est impair et $< m$. Ainsi, il suffit de trouver un vecteur non nul dans $\widetilde{\mathbb{L}}^n$ isotrope pour q. Par construction, Π est le polynôme minimal de β sur $\mathbb{K}$. En particulier, comme $\Pi \mid \widetilde{A}$, on a $\widetilde{A}(\beta) = 0$, puis d'après $(*)$,

$$\widetilde{Q}(\beta) = q\big(\Pi_1(\beta), \dots, \Pi_n(\beta)\big) = 0.$$

Or, $\beta \in \widetilde{\mathbb{L}}$ et $\forall i \in [\![1, n]\!]$, $\Pi_i \in \mathbb{K}[X] \subset \widetilde{\mathbb{L}}[X]$ donc

$$\big(\Pi_1(\beta), \dots, \Pi_n(\beta)\big) \in \widetilde{\mathbb{L}}^n.$$

Si ce vecteur était nul, alors β serait une racine commune à tous les Π_i dans $\mathbb{K}$, donc le polynôme minimal de β sur $\mathbb{K}$, qui est Π diviserait tous les Π_i, ce qui serait absurde puisque les Π_i sont premiers entre eux. Ainsi $\big(\Pi_1(\beta), \dots, \Pi_n(\beta)\big) \neq 0$ et on a trouvé un vecteur de $\widetilde{\mathbb{L}}^n$ non nul isotrope pour q. Par hypothèse de récurrence, il existe un vecteur non nul dans $\mathbb{K}^n$ isotrope pour q, ce qui conclut la récurrence et prouve le **Théorème 1**.

2 Remarque : Une question naturelle est de trouver un contre-exemple dans le cas d'une extension de degré pair. Le plus simple est de considérer l'extension quadratique $\mathbb{C}/\mathbb{R}$, et de prendre la forme quadratique définie-positive

$$q : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x, y) & \longmapsto & x^2 + y^2 \end{array} \right.$$

Cette forme quadratique n'admet clairement pas de vecteur isotrope non nul dans $\mathbb{R}^2$, mais en revanche $(1, i)$ en est un dans $\mathbb{C}^2$, ce qui montre la nécessité de l'imparité de $\left[\mathbb{L} : \mathbb{K}\right]$ dans le **Théorème 1**.