Thorie des nombres/ Number theory.

UN CONTRE-EXEMPLE AU PRINCIPE DE HASSE POUR LES SIMILITUDES DE FORMES BILINEAIRES

par Anne Cortella

Rsum Soient k un corps de nombres et V un k-espace vectoriel de dimension finie. On ramne le problme du principe de Hasse pour les similitudes de formes bilinaires sans symtrie sur V un problme de principe de Hasse reli des normes d'extensions finies particulires de k. Puis on donne un contre-exemple ce nouveau principe l'aide d'une extension galoisienne de $\mathbf{Q}$ de groupe de Galois le groupe des quaternions d'ordre 8.

A counterexample to the Hasse principle for similarities of bilinear forms

Abstract

Let k be a number field and V a vector space of finite dimension over k. We first translate the problem of the Hasse principle for similarities of non symetric bilinear forms to a problem of a Hasse principle related to norms for some special extensions of k. Then we give an explicit counterexample to this new principle coming from a Galois extension of $\mathbf{Q}$ with Galois group the quaternion group of order 8.

Introduction:

Deux formes bilinaires b et b' sur V sont dites similaires s'il existe $\lambda \in k$ tel que b' et λb soient isomorphes. Un tel isomorphisme est appel similitude et λ facteur de similitude.

Waterhouse [8] a montr que le principe de Hasse est vrai pour les formes bilinaires sans symtrie. Ono [4] a montr qu'il l'est aussi pour les similitudes de formes quadratiques (voir aussi [2]). Le problme est plus compliqu pour les similitudes de formes bilinaires sans symtrie.

1. Reformulation du problme

Soit $b : V \times V \to k$ une forme bilinaire. On lui associe la k-algbre

$$R = \{(e, f) \in \text{End } V \times \text{End } V \mid \forall (x, y) \in V,\ b(ex, y) = b(x, fy) \text{ et } b(x, ey) = b(fx, y)\}$$

comme le fait E.Bayer dans [1].

Le groupe A_b des automorphismes de b est alors isomorphe $U(R)$, le groupe unitaire de R pour l'involution $^- : R \to R$ dfinie par $\overline{(e, f)} = (f, e)$.

Le groupe GA_b des similitudes de b est isomorphe $GU(R) = \{r \in R \mid \overline{r}r \in k\}$; et le groupe des facteurs de similitude $G_b(R) = \{\lambda \in k \mid \exists r \in GU(R), \overline{r}r = \lambda\}$.

Supposons b non dgnre. Soit B la matrice de b dans une base de V; $B \in \mathbf{GL}_n(k)$. Alors

$$R = \{(E, F) \in \mathbf{M}_n(k) \times \mathbf{M}_n(k) \mid BE = F^t B \text{ et } E^t B = BF\}$$

$$= \{E \in \mathbf{M}_n(k) \mid EB^{-1}B^t = B^{-1}B^t E\}$$

Notons $A = B^{-1}B^t$. L'involution sur R s'crit maintenant: $\overline{E} = (BEB^{-1})^t$. En particulier, $\overline{A} = A^{-1}$.

Soit J le radical de R. Alors R/J est une algbre semi-simple et se dcompose en

$$R/J = R_1 \times ... \times R_r \times (R_{r+1} \times \overline{R}_{r+1}) \times ... \times (R_s \times \overline{R}_s)$$

o $R_i = \mathbf{M}_{n_i}(D_i)$, D_i corps gauche sur k, et $\overline{R}_i = R_i$ si $i \leq r$.

En fait les D_i sont des corps commutatifs K_i: ce sont les commutants des composantes irrductibles de A.

Considrons le cas o R est simple; alors $R = \mathbf{M}_n(K)$, et K est le commutant de chacune des composantes irrductibles de A. Soit Λ une de ces composantes, P son polynme minimal, $r =$deg P. Alors quitte changer de base, Λ est la matrice compagnon de P et:

$$K = \text{End}_K K = \{M \in \mathbf{M}_r(k) \mid M\Lambda = \Lambda M\} = k[\alpha]$$

o α est une racine de P. L'involution de R induit sur K la k-involution dfinie par $\overline{\alpha} = \alpha^{-1}$.

Cette involution est triviale si et seulement si $\Lambda^{-1} = \Lambda$, c'est dire si $\Lambda^2 - Id = 0$, ce qui implique, Λ n'ayant pas de sous-espace stable, que $\Lambda = \pm Id$ donc $K = k$.

On voit donc que : ou bien $K = k$ et $^-$ est triviale, ou bien $[K : k]$ est pair et $K = k[X]/P$ o P est un polynme irrductible de type: $P = \sum_{i=1}^{n} a_i X^i$, avec pour tout i $a_{n-i} = \varepsilon a_i$, $\varepsilon = \pm 1$ (polynme "symtrique" ou "antisymtrique").

Les travaux de Riehm [5] et Waterhouse [8] conduisent aux memes rsultats.

Le cas $R = K$

Dans ce cas A est irrductible. Notons $K_0 = k[\alpha + \alpha^{-1}]$ le corps fixe de K par l'involution. Alors:
si $^-$ est triviale, $GU(K) = k^*$,
sinon $GU(K) = \{z \in K \mid z\overline{z} \in k^*\}$ est l'ensemble des k-similitudes de la forme hermitienne $< 1 >$ sur K.

Rappelons que $H^1(k, GA_b)$ est l'ensemble des classes de similitudes sur k des formes bilinaires de mme dimension que b, point par la classe de b. (cf [6,chX]).

Si $^-$ est triviale, alors $H^1(k, GA_b) = H^1(k, k^*) = 0$ par Hilbert 90; toutes les formes de mme dimension que b sont donc quivalentes.

Sinon, $H^1(k, GA_b)$ est l'ensemble des classes de k-similitudes de formes hermitiennes de dimension 1 sur K. Or une forme hermitienne $< a >$ sur K est k-similaire $< 1 >$ si et seulement si il existe $z \in K^*$ et $\lambda \in k^*$ tels que $a = \lambda N_{K/K_0}(z)$.

On obtient donc la reformulation suivante du problme de principe de Hasse pour les simi
-litudes de formes bilinaires:

Proposition: Toute forme bilinaire sur V similaire b sur tous les k_v l'est sur k si et seulement si tout lment de K de la forme $\lambda_v N_{K_v/K_{0,v}}(z_v)$ avec $z_v \in K_v$ et $\lambda_v \in k_v$ pour toute place v , est de la forme $\lambda N_{K/K_0}(z)$ avec $z \in K$ et $\lambda \in k$.

2. Un contre-exemple en dimension 8

Construisons un contre-exemple la proprit sur les normes donne dans le paragraphe prcdant.

Nous utilisons (d'aprs une suggestion de J-P. Serre [7]) l'extension suivante (Martinet [6]):

$k = \mathbf{Q}$, $K_0 = \mathbf{Q}(\sqrt{5}, \sqrt{41})$ et $K = K_0(\sqrt{M})$ avec $M = \frac{5+\sqrt{5}}{2}.\frac{41+\sqrt{41}\sqrt{5}}{2}$.

K est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois le groupe des quaternions d'ordre 8, dont tous les groupes de dcomposition sont cycliques (cf. [6]), et a les proprits suivantes:

(1): Il existe dans K un lment primitif α de polynme irrductible "symtrique": il suffit de prendre $\alpha = \frac{M+1}{M-1} + \frac{2\sqrt{M}}{M-1}$; son polynme irrductible sur $\mathbf{Q}$ est:

$$P = \frac{1}{189971}(189971X^8 + 1607507X^7 + 5858953X^6 + 12008589X^5 + 15134360X^4$$
$$+12008589X^3 + 5858953X^2 + 1607507X + 189971)$$

(2): Il existe dans K un lment a qui s'crit $a = \lambda_v N_{K_v/K_{0,v}}(z_v)$, $\lambda_v \in k_v$ et $z_v \in K_v$ pour toute place v de k mais n'est pas du type $\lambda N_{K/K_0}(z)$, $\lambda \in k$, $z \in K$.

(3): Il existe a dans K telque: $(a, M)_{\mathfrak{p}_3} = (a, M)_{\mathfrak{q}_3} = -1$ et $(a, M)_w = 1$ partout ailleurs, o $\mathfrak{p}_3$ et $\mathfrak{q}_3$ sont les deux idaux audessus de 3 dans K et o $(x, y)_w$ est l'algbre de quaternions sur K_w associe x et y.

En effet il suffit de prendre $a = 3.\frac{1+\sqrt{5}}{2}$ pour (3). Alors a convient aussi pour (2): a a la bonne forme sur K_v pour toutes les places, et on montre qu'il ne l'a pas sur K grce :

(4) Si $\lambda_v N_{K_v/K_{0,v}}(z_v) = 1$, $\lambda_v \in k_v$, $z_v \in K_v$, alors $(\lambda_v, 5)_v = 1$ (cf. [7]).

preuve: Si 5 est un carr dans k_v, c'est clair. Sinon, v est tel que E_v est un corps, o $E = k(\sqrt{5})$. Alors $K_{0,v} = K_{0,w} \times K_{0,w'}$ et $K_v = K_w \times K_{w'}$ o w et w' sont les places au-dessus de v et $K_{0,w} = K_{0,w'} = E_v$. $K_w \supset E_v \supset k_v$ donne une extension cyclique d'ordre 4.

Par hypothse, $z_w \in K_w^*$ est tel que $\lambda_v^{-1} = N_{K_w/K_{0,w}}(z_w)$. Or on a:

(5): Soit $E_4 \supset E_2 \supset E_1$ une extension cyclique de degr 4 de corps locaux. L'homomorphisme dfini par l'inclusion: $E_1^*/N_{E_2/E_1}E_2^* \longrightarrow E_2^*/N_{E_4/E_2}E_4^*$ est un isomorphisme.

Via l'isomorphisme du corps de classes local cela rsulte de ce que, si C est un groupe cyclique et C' un sous-groupe de C, le tranfert $C \longrightarrow C'$ est surjectif.

On applique le sous-lemme $K_w \supset E_v \supset Q_v$ et l'lment λ_v. L'image de cet lment dans $E_v^*/N_{K_w/E_v}K_w^*$ est 1 donc son image dans $Q_v^*/N_{E_v/Q_v}E_v$ est 1, ce qui signifie que $(\lambda_v, 5)_v = 1$.

La mthode du paragraphe 1 permet d'obtenir une bijection entre formes hermitiennes de dimension 1 sur K et formes bilinaires de mme dimension que b sur k et de trouver les formes bilinaires b et $\beta : K \times K \to k$ correspondant aux formes hermitiennes $< 1 >$ et $< a >$ sur K. Vu la taille des cefficients du polynme P, j'ai utilis le systme PARI. On obtient:

$a = U(\alpha)$ avec:

$$U(X) = \frac{94795529}{820}X^7 + \frac{2231284717}{2460}X^6 + \frac{614344038}{205}X^5 + \frac{16195852}{3}X^4$$
$$+\frac{70364504}{123}X^3 + \frac{8764206073}{2460}X^2 + \frac{989524041}{820}X + \frac{105449371}{615}$$

On en dduit les matrices (b_{ij}) et(β_{ij}) de b et β dans la base $(1, \alpha, ..., \alpha^7)$ de K sur k: pour $1 \leq i, j \leq 8$,

$$\begin{pmatrix} 0 & 0 & 0 & -1 & b_{1,5} & b_{1,6} & b_{1,7} & b_{1,8} \\ 0 & 0 & 0 & 0 & -1 & b_{1,5} & b_{1,6} & b_{1,7} \\ 0 & 0 & 0 & 0 & 0 & -1 & b_{1,5} & b_{1,6} \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & b_{1,5} \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ b_{1,5} & -1 & 0 & 0 & 0 & 0 & 0 & \\ b_{1,6} & b_{1,5} & -1 & 0 & 0 & 0 & 0 & 0 \\ b_{1,7} & b_{1,6} & b_{1,5} & -1 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} & \beta_{1,5} & \beta_{1,6} & \beta_{1,7} & \beta_{1,8} \\ \beta_{1,1} & \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} & \beta_{1,5} & \beta_{1,6} & \beta_{1,7} \\ \beta_{1,2} & \beta_{1,1} & \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} & \beta_{1,5} & \beta_{1,6} \\ \beta_{1,3} & \beta_{1,2} & \beta_{1,1} & \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} & \beta_{1,5} \\ \beta_{1,4} & \beta_{1,3} & \beta_{1,2} & \beta_{1,1} & \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} \\ \beta_{1,5} & \beta_{1,4} & \beta_{1,3} & \beta_{1,2} & \beta_{1,1} & \beta_{1,1} & \beta_{1,2} & \beta_{1,3} \\ \beta_{1,6} & \beta_{1,5} & \beta_{1,4} & \beta_{1,3} & \beta_{1,2} & \beta_{1,1} & \beta_{1,1} & \beta_{1,2} \\ \beta_{1,7} & \beta_{1,6} & \beta_{1,5} & \beta_{1,4} & \beta_{1,3} & \beta_{1,2} & \beta_{1,1} & \beta_{1,1} \end{pmatrix}$$

avec :

$$\begin{cases} b_{ij} = 0 \; sij = i+2, i+1, i \; ou \; i = j+1, j+2, j+3 \\ b_{ij} = -1 \; si \; j = i+3 \; ou \; i = j+4 \\ b_{ij} = 1797478/189971 \; si \; j = i+4 \; ou \; i = j+5 \\ b_{ij} = -1776427306983/36088980841 \; si \; j = i+5 \; ou \; i = j+6 \\ b_{ij} = 1288348045247800216/6855859779345611 \; si \; j = i+6 \; ou \; i = j+7 \\ b_{ij} = -769037454741294091886545/1302414538142065067281 \; si \; j = 8, i = 0 \end{cases}$$

$$\begin{cases} \beta_{ij} = 83397269/2460 \; si \; i = j, j+1 \\ \beta_{ij} = -258550531/2460 \; si \; j = i+1 \; ou \; i = j+2 \\ \beta_{ij} = 11208289/60 \; si \; j = i+2 \; ou \; i = j+3 \\ \beta_{ij} = -706184071/2460 \; si \; j = i+3 \; ou \; i = j+4 \\ \beta_{ij} = 194229083166919/467328660 \; si \; j = i+4 \; ou \; i = j+5 \\ \beta_{ij} = -51909390322689686191/88778892868860 \; si \; j = i+5 \; ou \; i = j+6 \\ \beta_{ij} = 13663658396321170597347199/16865415057190203060 \; si \; j = i+6 \; ou \; i = j+7 \\ \beta_{ij} = -3565006060789271260797393731/32039397638294800655112 60 \; si \; j = 8, i = 0 \end{cases}$$

Ce travail a t ralis sous la direction de E.Bayer.

Bibliographie

[1] E.BAYER-FLUCKIGER: "Principe de Hasse pour les systmes de formes quadratiques". J.reine.angew.Math 378(1987) pp 55-59.

[2] A.CORTELLA: "Principe de Hasse pour les similitudes de formes quadratiques". Pub. Math.Besanon (1993).

[3] J.MARTINET: "Modules sur l'algbre du groupe quaternionien". Annales scient.E.N.S. t 4(1971) pp 399-408.

[4] T.ONO: "Arithmetic of orthogonal groups".J.Math.Soc.Japan 7(1955) pp79-91.

[5] C.RIEHM: "The equivalence of bilinear forms". J.Algebra 31(1974) pp 45-66.

[6] J-P.SERRE: "Corps locaux". Hermann.(Paris 1962).

[7] J-P.SERRE: lettre E.Bayer du 8/02/1993

[8] W.C.WATERHOUSE: "A non symmetric Hasse-Minkovski theorem". Amer.J.Math. 99 (1977) pp755-759.

URA 741 CNRS
Laboratoire de mathmatiques
UFR Sciences et Techniques
16, route de Gray
25030 Besanon cedex

Si de plus $n = 1$, alors $R = K$ qui est muni d'une involution *.Soit K_0 le corps fixe pour *.On a $[K : K_0] = 1$ ou 2, et:

$$\begin{cases} U(K) = \{x \in K / x^2 = 1\} \\ GU(K) = \{x \in K / x^2 \in K\} \\ MS(K) = k^* \bigcap K^{*2} \end{cases} \text{ si } ^* \text{ est triviale, } \begin{cases} U(K) = ker N_{K/K_0} \\ GU(K) = N^{-1}_{K/K_0}(k^*) \\ MS(K) = k^* \cap N_{K/K_0}(K^*) \end{cases} \text{ sinon.}$$

les corps K pouvant intervenir

Waterhouse [3] donne une autre approche du problme: il y a correspondance bijective entre les formes bilinaires sur k et les formes $(-X)$-hermitiennes de $M \times M$ dans E, o $A = k[X, 1/X]$ est muni de l'involution $X^J = 1/X$, F est son corps des fractions, $E = F/A$ et M dcrit les A-modules de type fini.

Cette correspondance donne un systme d'invariants des formes bilinaires b sur k.

- Les R_i, $i > r$ sont dans ce systme les composantes P_i-primaires de M pour P_i premier et $P_i^J A \neq P_i A$;
- les R_i, $i \leq r$ tels que $^*_{|K_i} \neq Id_{K_i}$ sont relis des formes hermitiennes sur A/P_iA pour P_i premier, $P_i^J A = P_i A$ et J non trivial sur A/P_iA. K_i est alors exactement A/P_iA;
- les R_i, $i \leq r$ tels que $^*_{|K_i} = Id_{K_i}$ sont relis des formes bilinaires symtriques ou antisymtriques sur A/P_iA pour P_i premier et $P_i^J A = P_i A$ avec J trivial sur A/P_iA qui est exactement K_i, et comme $P_i = X - 1$ ou $X + 1$, $K_i = k$.

On voit donc que si $R = K$, ou bien $K = k$ et * est triviale, ou bien $[K : k]$ est pair et $K = k[X]/P$ ou P est un polynome irrductible de type: $P = \sum_{i=1}^{n} a_i X^i$, avec $\forall i \ a_{n-i} = \varepsilon a_i, \varepsilon = \pm 1$ polynome "symtrique" ou "antisymtrique".

Le principe sur les normes correspondant

Le principe de Hasse pour les similitudes quivaut en termes de cohomologie galoisienne l'injectivit du morphisme naturel d'ensembles points:

$$H^1(k, GA_b(k^s)) \longrightarrow \prod_v H^1(k_v, GA_b(k_v^s))$$

o v dcrit l'ensemble des places de k, k_v est le complt de k en v, et k^s (resp. k_v^s) est une cloture sparable de k (k_v).

On voit donc qu'il n'y aura pas de contre exemple pour $K = k$ ni pour $[K : k] = 2$ (d'aprs la forme de GU), et on se restraint maintenant $[K : k] > 2$ et $^* \neq Id$. En fait $K = k[\alpha]$ est alors muni de l'involution non triviale

$\alpha \mapsto \alpha^{-1}$ et $K_0 = k[\alpha + \alpha^{-1}]$. Les suites exactes:

$$1 \longrightarrow U(K) \longrightarrow GU(K) \longrightarrow MS(K) \longrightarrow 1$$
$$1 \longrightarrow U(K^s) \longrightarrow GU(K^s) \longrightarrow MS(K^s) \longrightarrow 1$$

donnent la suite exacte de cohomologie):

$$1 \longrightarrow k^*/MS(K) \longrightarrow H^1(k, U) \longrightarrow H^1(k, GU) \longrightarrow 1$$

(tronque droite grce Hilbert 90)

En faisant la mme chose avec tous les complts de k, et avec les morphismes naturels verticaux, on obtient le diagramme commutatif:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^*/MS(K) & \longrightarrow & H^1(k,U) & \longrightarrow & H^1(k,GU) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \prod_v k_v^*/MS(K_v) & \longrightarrow & \prod_v H^1(k_v,U) & \longrightarrow & \prod_v H^1(k_v,GU) & \longrightarrow & 1 \end{array}$$

Le principe de Hasse pour les similitudes de formes bilinaires sur V s'crit:φ est injective.