ACTA ARITHMETICA
LIX.2 (1991)

A note on the Hasse principle. Addenda

by

NGUYEN QUOC THANG (Waterloo)

In [2] we have discussed a method of giving counter-examples to the Hasse principle for systems of many quadratic forms in many variables. Here we would like to give some more details, making Lemma 10 in [2] and its proof more precise, and also to correct Example 2 there.

1. Let D be a quaternion division algebra over a field k of characteristic $\neq 2$, Φ be a nondegenerate skew-hermitian form of rank n w.r. to the standard involution J of D. Further we keep the notation in [2]. Denote by $M(\Phi) = m(\mathrm{GU}(\Phi)(k))$ the group of multiplicators of Φ. Let $\mathrm{GU}^+(\Phi) = \mathrm{SU}(\Phi)\cdot G_m$ (the almost direct product, where $\mathrm{SU}(\Phi)$ is the special unitary k-group of Φ) and let $M^+(\Phi) = m(\mathrm{GU}^+(\Phi)(k))$. The correct formulation of Lemma 10 in [2] is as follows.

LEMMA 10. *Let k be any field of characteristic $\neq 2$ and D be a non-trivial quaternion division algebra. For any natural number n, there is a skew-hermitian form Φ w.r. to J of rank n such that*

$$\mathrm{PGU}(\Phi)(k) \neq \mathrm{PGU}(\Phi)_0(k).$$

Proof. It is well known and easy to see that for any skew-hermitian form Φ, the group $\mathrm{GU}^+(\Phi)$ is just the connected component of the group $\mathrm{GU}(\Phi)$. Since D is non-trivial, $\mathrm{U}(\Phi)(k) = \mathrm{SU}(\Phi)(k)$, and $\mathrm{PGU}(\Phi)(k) \neq \mathrm{PGU}(\Phi)_0(k)$ is equivalent to $M(\Phi) \neq M^+(\Phi)$.

Let $g \in \mathrm{GU}(\Phi)(k)$, $\lambda = m(g)$. Then we know that, if $n = \operatorname{rank} \Phi$, $\mathrm{Nrd}(g)^2 = \lambda^{2n}$, hence $\mathrm{Nrd}(g) = \lambda^n$ or $-\lambda^n$, and that $g \in \mathrm{GU}^+(\Phi)(k)$ (i.e. $\lambda \in M^+(\Phi)$) if and only if $\mathrm{Nrd}(g) = \lambda^n$. Now assume that $(1, i, j, ij)$ is a canonical basis of D over k, $i^2 = \theta, j^2 = \eta, ij = -ji$, θ and η belong to $k^\times$. We consider in D the equation

$$X^J \cdot i \cdot X = \lambda \cdot i.$$

For $x = x_0 + x_1 i + x_2 j + x_3 ij$, it follows by easy calculations (see [2], Example 1 for details) that this equation is equivalent to the following two systems of equations:

$$\begin{cases} x_0 = x_1 = 0, \\ \eta x_2^2 - \theta\eta x_3^2 = \lambda; \end{cases} \qquad \begin{cases} x_2 = x_3 = 0, \\ x_0^2 - \theta x_1^2 = \lambda. \end{cases}$$

Since D is non-trivial, these two systems never have solutions simultaneously. Now we take $\lambda = \eta x_2^2 - \theta\eta x_3^2$ for some x_2 and x_3 (not all zero). Then the equation

$$X^J \cdot i \cdot X = \lambda \cdot i$$

has a solution X with $\mathrm{Nrd}(X) = -\lambda$.

For any odd natural number n we put $\Phi = \mathrm{diag}\,(i, \ldots, i)$ (n entries i). Then for X above we put $Y = \mathrm{diag}\,(X, \ldots, X)$. Then Y is a similitude of Φ and clearly $Y \notin \mathrm{GU}^+(\Phi)(k)$.

If n is even then using similar arguments to the above, it is not hard to choose skew-quaternions $\alpha, \beta \in D$ such that for the form $\Phi_0 = \mathrm{diag}(\alpha, \beta)$, we have $M(\Phi_0) \neq M^+(\Phi_0)$. We then put $\Phi = \mathrm{diag}(\alpha, \beta, \ldots, \beta)$ ($n-1$ entries β) and we have again $M(\Phi) \neq M^+(\Phi)$. ∎

2. From the above it follows that Example 2 in [2] is not correct. Here we should take, for the two-dimensional case, the form Φ_0 of the previous part, and for the three-dimensional case, the form $\Phi = \mathrm{diag}\,(i, i, i)$ in order to write the systems of quadratic forms of small size, after having made some complicated computations.

3. Denote by $M'(\Phi) = \bigcap_v \big(M(\Phi_v) \cap k^\times\big)$ the group of all elements of k which are multiplicators of the form Φ locally everywhere, where k is assumed to be a global field of characteristic $\neq 2$ and v runs over all valuations of k. Then by [2], if $M(\Phi) \neq M^+(\Phi)$, then $\mathrm{Card}\,\big(M'(\Phi)/M(\Phi)\big) = 2^{s-2}$. Therefore, we can describe briefly our general method as follows:

(a) Choose the algebra D and the form Φ s.t. $s > 2$ and $M(\Phi) \neq M^+(\Phi)$.

(b) Choose $\lambda \in M'(\Phi) \backslash M(\Phi)$.

(c) Write the system according to the value λ obtained.

Practically, after having done step (a), to do step (b), we can proceed as follows. Take the decomposition of $M'(\Phi)$ into cosets modulo $M^+(\Phi)$:

$$M'(\Phi) = \bigcup_i M^+(\Phi) \cdot \lambda_i.$$

Since $M'(\Phi) \neq M(\Phi)$, there are λ_i such that $\lambda_i \notin M(\Phi)$. From this we can write the system of quadratic forms as required.

I would like to thank B. E. Kuniavski for valuable comments on the results of [2]. In particular, he has pointed out that our examples provide a lower bound $N = O(r)$, where the Hasse principle fails for systems of r quadratic forms in N variables. It is still an open question if it is so if $N = O(r^2)$ (cf. [1], Problem 9, pp. 106–107).

References

[1] D. J. Lewis, *Diophantine problems: solved and unsolved*, in: *Number Theory and Applications*, R. A. Mollin (ed.), Kluwer Academic Publishers, 1989, 103–121.

[2] Nguyen Quoc Thang, *A note on the Hasse principle*, Acta Arith. 54 (1990), 171–184.

INSTITUTE OF MATHEMATICS
P. O. Box 631, Bo Ho
Ha noi, Viet Nam

Received on 2.5.1990 (2037)