STUDIA MATHEMATICA, T. LXXVII. (1983)

Hasse's principle for systems of ternary quadratic forms and for one biquadratic form

by

A. SCHINZEL (Warszawa)

To Professor Jan Mikusiński on the occasion of the 70th birthday

Abstract. Let K be an algebraic number field and $f_1, \ldots, f_k$ ternary quadratic forms over K. If $f_1, \ldots, f_k$ have a common non-trivial zero in every completion of K except at most one then — it is proved here — they have a common non-trivial zero in K. Besides an example is given of an absolutely irreducible n-ary biquadratic form ($n \geqslant 3$) that represents 0 in every completion of Q but not in Q.

Let K be an algebraic number field and $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ quadratic forms. *Hasse's principle* asserts that if the forms $f_1, \ldots, f_k$ have a common non-trivial zero in every completion of K they have a common non-trivial zero in K. The principle holds for $k = 1$, it trivially holds for $n = 1, 2$, and it fails for $K = Q$, $k = 2$, $n \geqslant 4$ (see [2]). Thus it remains to consider the case $n = 3$.

We shall prove

THEOREM 1. *If quadratic forms $f_1, \ldots, f_k \in K[x, y, z]$ have a common non-trival zero in every completion of K except at most one then they have a common non-trivial zero in K.*

As to biquadratic forms over Q it is easy to give an example of a reducible ternary form for which Hasse's principle fails (see [1], p. 72). An example of an irreducible ternary biquadratic form with the same property can be constructed by using results of Hilbert [4], namely

$$\operatorname{norm}(x+y\sqrt{5}+z\sqrt{-31}).$$

This form, however, is reducible in the complex field. Mordell [6] has left open the question whether there exists an absolutely irreducible ternary biquadratic form not fulfilling Hasse's principle. The question is answered by

THEOREM 2. *The absolutely irreducible biquadratic form* $x^4-2y^4-16y^2z^2-49z^4$ *represents* 0 *in every completion of* Q *but not in* Q; *for all* $n\geqslant 4$ *the absolutely irreducible biquadratic form* $x_1^4-17x_2^4-2(x_3^2+\ldots+x_n^2)^2$ *represents* 0 *in every completion of* Q *but not in* Q.

LEMMA 1. *If a binary form over* K *of degree not exceeding* 4 *represents* 0 *in all but finitely many completions of* K *it represents* 0 *in* K.

Proof. See Fujiwara [3].

LEMMA 2. *Let* $R(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$ *be the resultant of* $\sum_{i=1}^{k}u_if_i$, $\sum_{i=1}^{k}v_if_i$ *with respect to* z (u_i, v_i *are indeterminates*). *If*

$$(1)\qquad R(a,b;u_1,\ldots,u_k,v_1,\ldots,v_k)=0,\qquad a,b\in K,\ \langle a,b\rangle\neq\langle 0,0\rangle$$

then either f_i *have a common non-trivial zero in* K *or*

$$(bx-ay)^2\,|\,R(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$$

and the forms $f_i(at,bt,z)$ *differ from their highest common divisor by a constant factor.*

Proof. If f_i are all of degree less than 2 with respect to z then they have a common non-trivial zero, namely $\langle 0,0,1\rangle$. If at least one of the forms f_i is of degree 2 with respect to z then both $\sum_{i=1}^{k}u_if_i$ and $\sum_{i=1}^{k}v_if_i$ are of degree 2 with respect to z with the leading coefficients independent of x,y. Therefore (1) implies that

$$\sum_{i=1}^{k}u_if_i(a,b,z)\quad\text{and}\quad\sum_{i=1}^{k}v_if_i(a,b,z)$$

have a common factor over the field $K(u_1,\ldots,u_k,v_1,\ldots,v_k)$, hence also over the ring $K[u_1,\ldots,u_k,v_1,\ldots,v_k]$. This factor must be independent of $u_1,\ldots,u_k,v_1,\ldots,v_k$. If it is of degree 1 in z it has a zero $c\in K$ and we have $f_i(a,b,c)=0$ $(1\leqslant i\leqslant k)$. If it is of degree 2 in z we consider the Sylvester matrix $S(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$ of the polynomials $\sum_{i=1}^{k}u_if_i$, $\sum_{i=1}^{k}v_if_i$. In virtue of a well-known theorem (see [7], Satz 114) the rank of the matrix $S(a,b;u_1,\ldots,u_k,v_1,\ldots,v_k)$ must be 2. Hence all the minors of degree 3 of this matrix vanish and all the minors of degree 3 of the matrix $S(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$ are divisible by $bx-ay$. On the other hand, there are minors of degree 2 of the latter matrix not divisible by $bx-ay$,

in fact independent of x,y. Hence by a very special case of theorem of Rédei [8]

$$R(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)=\det S(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$$

is divisible by $(bx-ay)^2$.

The last assertion of the lemma follows from the remark that if polynomials $f_i(a,b,z)$ $(1\leqslant i\leqslant k)$ have a common factor of degree 2 they differ from this common factor by a constant factor.

Proof of Theorem 1. Let us consider the resultant $R(x,y,u_1,\ldots,u_k,v_1,\ldots,v_k)$ of $\sum u_if_i$ and $\sum v_if_i$ with respect to z. Viewed as a polynomial in x,y it is either 0 or a quartic form. In the first case f_i $(1\leqslant i\leqslant k)$ have a common factor, say d. If d is of degree 2 then for each $i\leqslant k$ we have $f_i=c_id$, $c_i\in K$. The solvability of $f_i(x,y,z)=0$ $(i\leqslant k)$ in a completion K_v of K implies the solvability of $d(x,y,z)=0$ in K_v, and if it holds for all but one completion then by the product formula and Hasse's principle for one quadratic form we get solvability in K of $d(x,y,z)=0$ and hence of $f_i(x,y,z)=0$ $(1\leqslant i\leqslant k)$. If d is of degree 1 then it has again a non-trivial zero in K and the same conclusion holds.

If $R(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$ is not identically 0, let $r(x,y)$ be the highest common divisor of its coefficients when viewed as a form in $u_1,\ldots,u_k,v_1,\ldots,v_k$. If $f_i(x,y,z)$ $(1\leqslant i\leqslant k)$ have a common non-trivial zero $\langle a_v,b_v,c_v\rangle$ in K_v, $\sum u_if_i$ and $\sum v_if_i$ have it also, hence $R(a_v,b_v;u_1,\ldots,u_k,v_1,\ldots,v_k)=0$, which implies

$$(2)\qquad r(a_v,b_v)=0.$$

(Here we use the fact that the coefficients of R are forms in x,y). If $a_v=b_v=0$ we have $c_v\neq 0$; hence the coefficient of z^2 in f_i is 0 for each $i\leqslant k$ and the forms f_i $(1\leqslant i\leqslant k)$ have in K a common non-trivial zero $\langle 0,0,1\rangle$. If $\langle a_v,b_v\rangle\neq\langle 0,0\rangle$ for each valuation v of K except at most one then by Lemma 1 r has in K a zero, say $\langle a,b\rangle\neq\langle 0,0\rangle$. Thus $bx-ay\,|\,r(x,y)$,

$$bx-ay\,|\,R(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$$

and by Lemma 2 either f_i have a common non-trivial zero in K or

$$(3)\qquad (bx-ay)^2\,|\,R(x,y;u_1,\ldots,u_k,v_1,\ldots,v_k)$$

and the forms $f_i(at,bt,z)$ $(1\leqslant i\leqslant k)$ differ from their highest common divisor by a constant factor. In the latter case, by (3)

$$(bx-ay)^2\,|\,r(x,y).$$

Let

(4) $$r(x, y) = (bx-ay)^{a} s(x, y),$$

where $a \geqslant 2$, $s(a, b) \neq 0$, $\deg s = \deg r - a \leqslant 2$. For every valuation v of K except at most one we have by (2) and (4)

$$ba_v - ab_v = 0 \quad \text{or} \quad s(a_v, b_v) = 0.$$

The first equation implies $a_v = at$, $b_v = bt$ for a $t \in K_v^*$; thus

$$F(t, u) = s(t, u) \underset{1 \leqslant i \leqslant k}{\text{h.c.d.}} f_i(at, bt, u)$$

has a non-trivial zero in K_v. Since by (4)

$$\deg F = \deg s + 2 = \deg r + 2 - a \leqslant 4,$$

we infer from Lemma 1 that F has in K a zero, say $\langle c, d\rangle \neq \langle 0, 0\rangle$. If this is a zero of the $\underset{1 \leqslant i \leqslant k}{\text{h.c.d.}} f_i(at, bt, u)$, then

$$f_i(ac, bc, d) = 0 \quad (1 \leqslant i \leqslant k), \quad \langle ac, bc, d\rangle \neq \langle 0, 0, 0\rangle.$$

If, on the other hand, $s(c, d) = 0$ then by (4) $r(c, d) = 0$; thus

$$R(c, d; u_1, \ldots, u_k, v_1, \ldots, v_k) = 0$$

and by Lemma 2 either f_i have a common non-trivial zero in K or

$$(dx-cy)^2 \mid R(x, y; u_1, \ldots, u_k, v_1, \ldots, v_k)$$

and $f_i(ct, dt, z)$ $(1 \leqslant i \leqslant k)$ differ by a constant factor from their highest common divisor. In the latter case

$$(dx-cy)^2 \mid r(x, y)$$

and by (4)

$$r(x, y) = e(bx-ay)^2(dx-cy)^2.$$

For every valuation v of K except at most one we have by (2)

$$ba_v - ab_v = 0 \quad \text{or} \quad da_v - ca_v = 0;$$

thus for a suitable $t \in K_v^*$ either $a_v = at$, $b_v = bt$ or $a_v = ct$, $b_v = dt$. It follows that the quartic form

$$G(t, u) = \underset{1 \leqslant i \leqslant k}{\text{h.c.d.}} f_i(at, bt, u) \cdot \underset{1 \leqslant i \leqslant k}{\text{h.c.d.}} f_i(ct, dt, u)$$

has a non-trivial zero in K_v. By Lemma 1 $G(t, u)$ has in K a zero, say $\langle t_0, u_0\rangle$

$\neq \langle 0, 0\rangle$. If $\langle t_0, u_0\rangle$ is a zero of the $\underset{1 \leqslant i \leqslant k}{\text{h.c.d.}} f_i(at, bt, u)$ then

$$f_i(at_0, bt_0, u_0) = 0 \quad (1 \leqslant i \leqslant k), \quad \langle at_0, bt_0, u_0\rangle \neq \langle 0, 0, 0\rangle;$$

if $\langle t_0, u_0\rangle$ is a zero of the $\underset{1 \leqslant i \leqslant k}{\text{h.c.d.}} f_i(ct, dt, u)$ then

$$f_i(ct, dt_0, u_0) = 0 \quad (1 \leqslant i \leqslant k), \quad \langle ct_0, dt_0, u_0\rangle \neq \langle 0, 0, 0\rangle.$$

The proof is complete.

For the proof of Theorem 2 we need three lemmata.

LEMMA 3. *The equation $u^4 - 17v^4 = 2w^2$ has no solutions in Q except $\langle 0, 0, 0\rangle$.*

Proof. See Lind [5] or Reichardt [10].

LEMMA 4. *Let $F(x_1, \ldots, x_n)$ be a polynomial with integer p-adic coefficients and $\gamma_1, \ldots, \gamma_n$ p-adic integers. If for an $i \leqslant n$ we have*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{2\delta+1}},$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{\delta}},$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$$

(δ a nonnegative integer) then there exist p-adic integers $\theta_1, \ldots, \theta_n$ such that

$$F(\theta_1, \ldots, \theta_n) = 0$$

and $\theta_1 \equiv \gamma_1 \pmod{p^{\delta+1}}, \ldots, \theta_n \equiv \gamma_n \pmod{p^{\delta+1}}$.

Proof. See [1], p. 42.

LEMMA 5. *$f(x, y, z) = x^4 - 2y^4 - 16y^2z^2 - 49z^4$ is irreducible in every field of characteristic different from 2 and 17.*

Proof. Let k be a field of this kind. It is enough to show that $f(x, y, z)$ is irreducible as a polynomial in x over $k(y, z)$. If it were not, then by Capelli's theorem (see [9], Satz 428) $\pm(2y^4 + 16y^2z^2 + 49z^4)$ would have to be a square in $k(y, z)$. This condition implies that

$$16^2 - 4 \cdot 2 \cdot 49 = -8 \cdot 17 = 0,$$

which is possible only if $\operatorname{char} k = 2$ or $\operatorname{char} k = 17$.

Proof of Theorem 2. $f(x, y, z) = x^4 - 17z^4 - 2(y^2 + 4z^2)^2$; hence by Lemma 3 if $f(x, y, z) = 0$ and $x, y, z \in Q$ we have $x = y^2 + 4z^2 = 0$ and thus $x = y = z = 0$. Also $x_1^4 - 17x_2^4 - 2(x_3^2 + \ldots + x_n^2)^2 = 0$ implies $x_1 = x_2 = \ldots = x_n = 0$ for $x_i \in Q$.

It remains to show that $f(x, y, z)$ represents 0 in every field Q_p including $Q_\infty = R$. We verify this first using Lemma 3 for $p = \infty, 2, 5, 7, 13$ and 17.

For $p = \infty$ we take $x = \sqrt[4]{2}$, $y = 1$, $z = 0$.

For $p = 2$ we use Lemma 4 with $\gamma_1 = 3, \gamma_2 = 2, \gamma_3 = 1, \delta = 2, i = 1$.

For $p = 5$ we use Lemma 4 with $\gamma_1 = 0, \gamma_2 = 2, \gamma_3 = 1, \delta = 0, i = 2$.

For $p = 7$ we use Lemma 4 with $\gamma_1 = 2, \gamma_2 = 1, \gamma_3 = 0, \delta = 0, i = 1$.

For $p = 13$ we use Lemma 4 with $\gamma_1 = 1, \gamma_2 = 2, \gamma_3 = 3, \delta = 0, i = 1$.

For $p = 17$ we use Lemma 4 with $\gamma_1 = 0, \gamma_2 = 1, \gamma_3 = 2, \delta = 0, i = 2$.

For $p \neq 2, 5, 7, 13, 17$ we have either $p \geqslant 37$ or for a suitable $\operatorname{sign}(\pm 7|p) = 1$.

In the latter case the congruence

$$f(x, 0, z) = (x^2 - 7z^2)(x^2 + 7z^2) \equiv 0 \pmod{p}$$

is solvable nontrivially, and denoting its solution by γ_1, γ_3 we use Lemma 4 with $\gamma_2 = 0, \delta = 0, i = 1$.

It remains to consider primes $p \geqslant 37$. For such primes f is by Lemma 5 absolutely irreducible over F_p. Moreover, it has no singular zeros. Indeed, the equations

$$4x^3 = 0, \quad -8y^3 - 32yz^2 = 0, \quad -32y^2z - 196z^3 = 0$$

imply $x = 0$ and either $y = 0$, $196z^3 = 0$ or $y^2 + 4z^2 = 0$, $68z^2 = 0$; thus in any case $x = y = z = 0$. By the Riemann–Hurwitz formula the curve $f(x, y, z) = 0$ is over F_p of genus 3.

Therefore by Weil's theorem the number of points on this curve with coordinates in F_p is greater than $p + 1 - 6\sqrt{p}$, i.e., at least one. Since all points are non-singular, Lemma 4 applies with $\delta = 0$ and a suitable i.

Note added in proof. I have learned that already in 1981 A. Bremner, D. J. Lewis and P. Morton found the example $3x^4 + 4y^4 - 19z^4$ of a ternary biquadratic form for which Hasse's principle fails, but they did not publish it.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, New York and London 1966.

[2] J.-L. Colliot-Thélène, D. Coray, J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. Reine Angew. Math. 320 (1980), 150–191.

[3] M. Fujiwara, *Hasse principle in algebraic equations*, Acta Arith. 22 (1973) 267–276.

[4] D. Hilbert, *Über Diophantische Gleichungen*, Nachr. Königl. Gesell. Wiss. Göttingen 1897, 48–54.

[5] C. E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins* (Doctoral dissertation), Uppsala 1940.

[6] L. J. Mordell, *The diophantine equation $Ax^4 + By^4 + Cz^4 = 0$*, Proc. Cambridge Philos. Soc. 68 (1970), 125–128.

[7] O. Perron, *Algebra* I, Berlin 1951.

[8] L. Rédei, *Über die Determinantenteiler*, Acta Math. Acad. Sci. Hungar. 3 (1952), 143–149.

[9] — *Algebra* I, Leipzig 1959.

[10] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. 184 (1942), 12–18.

Received June 2, 1982 (1764)