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

by A. SCHINZEL (Warszawa)

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

Abstract. Let $K$ be an algebraic number field and $f_1, \ldots, f_n$ ternary quadratic forms over $K$. If $f_1, \ldots, f_n$ 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 ($n \geq 3$) that represents 0 in every completion of $Q$ but not in $Q$.

Let $K \subset \mathbb{C}$ be an algebraic number field and $f_1, \ldots, f_n \in K[x, y, z]$ quadratic forms. Hase's principle asserts that if the forms $f_1, \ldots, f_n$ 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 $K = Q$, $k = 2$, $n \geq 4$ (see [2]). Thus it remains to consider the case $n = 3$.

We shall prove

Theorem 1. If quadratic forms $f_1, \ldots, f_n \in K[x, y, z]$ have a common non-trivial 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 Hase'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

$$\text{norm}(x + y \sqrt{5} + z \sqrt{-1}).$$

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 Hase's principle. The question is answered by
Theorem 2. The absolutely irreducible biquadratic form \( x^4 - 2y^4 - 16pqz^4 - 48r^4 \) represents \( 0 \) in every completion of \( Q \) but not in \( Q \); for all \( n \geq 4 \) the absolutely irreducible biquadratic form \( x^4 - 17a^2 - 2(a + \ldots + a)^2 \) 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 Fujiiwa [3].

Lemma 2. Let \( R(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k) \) be the resultant of \( \sum_{i=1}^k u_i f_i \), \( \sum_{i=1}^k v_i g_i \) with respect to \( x, (u_1, v_1) \) be determinants. If

\[
R(a, b; u_1, \ldots, u_l, v_1, \ldots, v_k) = 0, \quad a, b \in K, \langle a, b \rangle \neq \langle 0, 0 \rangle
\]

then either \( f_i \) have a common non-trivial zero in \( K \) or

\[
(bx - ay)^r | R(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k)
\]

and the forms \( f_i(a, b, c) \) differ from their highest common divisor by a constant factor.

Proof. If \( f_i \) are all of degree less than 2 with respect to \( x \) 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 \( x \) then both \( \sum_{i=1}^k u_i f_i \) and \( \sum_{i=1}^k v_i g_i \) are of degree 2 with respect to \( x \) with the leading coefficients independent of \( x, y \). Therefore (1) implies that

\[
\sum_{i=1}^k u_i f_i(a, b, c) = 0 \quad \text{and} \quad \sum_{i=1}^k v_i g_i(a, b, c) = 0
\]

have a common factor over the field \( K(a_1, \ldots, a_l, v_1, \ldots, v_k) \), hence also over the ring \( K[u_1, \ldots, u_l, v_1, \ldots, v_k] \). This factor must be independent of \( u_1, \ldots, u_l, v_1, \ldots, v_k \). If it is of degree 1 in \( x \) it has a zero \( c \in K \) and we have \( f_i(a, b, c) = 0 (1 \leq i \leq k) \). If it is of degree 2 in \( x \) we consider the Sylvester matrix \( S(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k) \) of the polynomials \( \sum_{i=1}^k u_i f_i \), \( \sum_{i=1}^k v_i g_i \). In virtue of a well-known theorem (see [7], Satz 114) the rank of the matrix \( S(a, b; u_1, \ldots, u_l, v_1, \ldots, v_k) \) must be 2. Hence all the minors of degree 3 of this matrix vanish. Hence all the minors of degree 3 of the matrix \( S(a, b; u_1, \ldots, u_l, v_1, \ldots, v_k) \) 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]

\[
R(a, b; u_1, \ldots, u_l, v_1, \ldots, v_k) = \sum_{i=1}^l u_i f_i(a, b, c) = 0 \quad (1 \leq i \leq k)
\]

and \( bx - ay \) divides \( R(a, b; u_1, \ldots, u_l, v_1, \ldots, v_k) \) if and only if \( \langle a, b \rangle \neq \langle 0, 0 \rangle \).

The last assertion of the lemma follows from the remark that if polynomials \( f_i(a, b, c) (1 \leq i \leq k) \) 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 \( R(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k) \) of \( \sum_{i=1}^k u_i f_i \), \( \sum_{i=1}^k v_i g_i \) with respect to \( x, y \). Viewed as a polynomial in \( x, y \) it is either 0 or a quartic form. In the first case \( f_i(1 \leq i \leq k) \) have a common factor, say \( d \). If \( d \) is of degree 2 then for each \( i \leq k \) we have \( f_i = c_i d, c_i \in K \). The solvability of \( f_i(1 \leq i \leq k) \) in a completion \( K \) of \( K \) implies the solvability of \( d(x, y) = 0 \) in \( K \), and if it holds for all but one completion then by the product formula and Hase’s principle for one quadratic form we get solvability in \( K \) of \( d(x, y) = 0 \) and hence of \( f_i(1 \leq i \leq k) \). If \( d \) is of degree 1 then it has again a non-trivial zero in \( K \) and the same conclusion holds.

If \( R(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k) \) is not identically 0, let \( r(x, y) \) be the highest common divisor of its coefficients when viewed as a form in \( u_1, \ldots, u_l, v_1, \ldots, v_k \). If \( f_i(1 \leq i \leq k) \) have a common non-trivial zero \( \langle a_i, b_i, c_i \rangle \) in \( K \), \( \sum_{i=1}^k u_i f_i \), \( \sum_{i=1}^k v_i g_i \) have it also, hence \( R(a_i, b_i; u_1, \ldots, u_l, v_1, \ldots, v_k) = 0 \), which implies

\[
r(a_i, b_i) = 0.
\]

(Here we use the fact that the coefficients of \( R \) are forms in \( x, y \). If \( a_i = b_i = 0 \) we have \( c_i = 0 \); hence the coefficient of \( x^2 \) in \( f_i \) is 0 for each \( i \leq k \) and the forms \( f_i(1 \leq i \leq k) \) have in \( K \) a common non-trivial zero \( \langle 0, 0, 1 \rangle \). If \( \langle a_i, b_i \rangle \neq \langle 0, 0 \rangle \) for each valuation \( v \) of \( K \) except at most one then by Lemma 1 \( v \) has in \( K \) a zero, say \( \langle a, b \rangle \neq \langle 0, 0 \rangle \). Thus \( bx - ay | r(x, y) \), \( bx - ay | R(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k) \) and by Lemma 2 either \( f_i \) have a common non-trivial zero in \( K \) or

\[
(bx - ay)^r | R(x, y; u_1, \ldots, u_l, v_1, \ldots, v_k)
\]

and the forms \( f_i(a, b, c) (1 \leq i \leq k) \) differ from their highest common divisor by a constant factor. In the latter case, by (3)
Let
\[ r(x, y) = (bx - ay)^2(x, y), \]
where \( x > 2 \), \( s(a, b) \neq 0 \), \( \deg r = \deg r - a \leq 2 \). 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 \( a_v = at_v, b_v = bt_v \) for an \( t \in K_v^* \); thus
\[ F(t, u) = s(t, u)b.c.d.f_i(at, bt, u) \]
has a non-trivial zero in \( K_v^* \); since by (4)
\[ \deg F - \deg s + 2 = \deg r = 2 + a \leq 4, \]
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 h.c.d.f_i(at, bt, u) then
\[ f_i(ac, bc, d) = 0 \quad (1 \leq i \leq k), \quad \langle ac, bc, d \rangle \neq \langle 0, 0, 0 \rangle. \]
If, on the other hand, \( s(c, d) = 0 \) then by (4) \( r(c, d) = 0 \); thus
\[ R(c, d; u_1, \ldots, u_n, v_1, \ldots, v_n) = 0 \]
and by Lemma 2 either \( f_i \) has a common non-trivial zero in \( K \) or
\[ (ds - cy)^2 | r(x, y) \]
and by (4)
\[ r(x, y) = c(bx - ay)^2(ds - cy)^2. \]
For every valuation \( v \) of \( K \) except at most one we have by (3)
\[ ba_v - ab_v = 0 \quad \text{or} \quad da_v - ec_v = 0; \]
thus for a suitable \( t \in K_v^* \) either \( a_v = at_v, b_v = bt_v \) or \( a_v = ct_v, b_v = dt_v \). It follows that the quartic form
\[ G(t, u) = \text{h.c.d.f}_i(at, bt, u), \quad \text{h.c.d.f}_i(ct, dt, u) \]
has a non-trivial zero in \( K_v^* \). By Lemma 1 \( G(t, u) \) has in \( K \) a zero, say \( \langle t_v, u_v \rangle \neq \langle 0, 0 \rangle \). If \( \langle t_v, u_v \rangle \) is a zero of the h.c.d.f_i(at, bt, u) then
\[ f_i(at_v, bt_v, u_v) = 0 \quad (1 \leq i \leq k), \quad \langle at_v, bt_v, u_v \rangle \neq \langle 0, 0, 0 \rangle; \]
if \( \langle t_v, u_v \rangle \) is a zero of the h.c.d.f_i(ct, dt, u) then
\[ f_i(ct_v, dt_v, u_v) = 0 \quad (1 \leq i \leq k), \quad \langle ct_v, dt_v, u_v \rangle \neq \langle 0, 0, 0 \rangle. \]
The proof is complete.

For the proof of Theorem 2 we need three lemmata.

**Lemma 3.** The equation \( x^4 - 17y^4 = 2w^4 \) 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 \( \gamma_1, \ldots, \gamma_n \) \( p \)-adic integers. If for an \( i \leq n \) we have
\[ F(\gamma_1, \ldots, \gamma_n) = 0 \mod p^{a_i+1}, \]
and by \( \frac{\partial F}{\partial x_i} (\gamma_1, \ldots, \gamma_n) = 0 \mod p^{a_i} \)
\[ \frac{\partial F}{\partial x_i} (\gamma_1, \ldots, \gamma_n) 
eq 0 \mod p^{a_i+1} \]
\( (a \text{ a nonnegative integer}) \) then there exist \( p \)-adic integers \( \theta_1, \ldots, \theta_n \) such that
\[ F(\theta_1, \ldots, \theta_n) = 0 \]
and \( \theta_i = \gamma_i \mod p^{a_i+1}, \ldots, \theta_n = \gamma_n \mod p^{a_n+1} \).

**Proof.** See [1], p. 42.

**Lemma 5.** \( f(x, y, z) = x^4 - 2y^4 - 16y^2z^2 - 49x^4 \) 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 Capel's theorem (see [9], Satz 428) \( f \) would have to be a square in \( k(y, z) \). This condition implies that
\[ 16z^4 + 4z^2 - 49x^4 = 0, \]
which is possible only if \( \text{char} k = 2 \) or \( \text{char} k = 17 \).

**Proof of Theorem 2.** \( f(x, y, z) = x^4 - 17z^4 - 2(y^4 + 49x^4) \); hence by Lemma 3 if \( f(x, y, z) = 0 \) and \( x, y, z \in Q \) we have \( x^4 + 49z^4 = 0 \) and thus \( x = y = z = 0 \). Also \( x_1^4 - 17x_2^4 - 2(x_3^4 + \ldots + x_n^4) = 0 \) 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 $Q_m = R$. We verify this first using Lemma 3 for $p = \infty$, 2, 5, 7, 13 and 17.

For $p = \infty$ we take $x = \sqrt{2}$, $y = 1$, $z = 0$.
For $p = 2$ we use Lemma 4 with $v_1 = 3$, $v_2 = 2$, $v_3 = 1$, $\delta = 2$, $i = 1$.
For $p = 5$ we use Lemma 4 with $v_1 = 0$, $v_2 = 2$, $v_3 = 1$, $\delta = 0$, $i = 2$.
For $p = 7$ we use Lemma 4 with $v_1 = 2$, $v_2 = 1$, $v_3 = 0$, $\delta = 0$, $i = 1$.
For $p = 13$ we use Lemma 4 with $v_1 = 1$, $v_2 = 2$, $v_3 = 3$, $\delta = 0$, $i = 1$.
For $p = 17$ we use Lemma 4 with $v_1 = 0$, $v_2 = 1$, $v_3 = 2$, $\delta = 0$, $i = 2$.
For $p \neq 2, 5, 7, 13, 17$ we have either $p \geq 37$ or for a suitable sign $\pm r(p) = 1$.

In the latter case the congruence

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

is solvable nontrivially, and denoting its solution by $v_1, v_2$ we use Lemma 4 with $v_3 = 0$, $\delta = 0$, $i = 1$.

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

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

imply $x = 0$ and either $y = 0$, $196z^2 = 0$ 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 of 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. Brauner, D. J. Lewis and P. Morton found the example $3a^4 + 4g^4 - 16e^4$ of a ternary bi-quadratic form for which Hasse's principle fails, but they did not publish it.

References