Conspectus materiae tomi XXVIII, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de
la Rédaction
et de l'échange

Address of the
Editorial Board
and of the exchange

Die Adresse der
Schriftleitung und
des Austausches

Адрес редакции
и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

TA ARITHMETICA
XXVIII (1975)

Representability by certain norm forms over algebraic number fields

by

JOHN H. SMITH (Pasadena, Calif.)

In this note we show how the representability of a member of a number field K by a norm form over K can sometimes be reduced to local problems over a subfield. These are solved explicitly for some classes of examples.

The proof rests on the Hasse local to global principle for cyclic norm forms and the effect of inflation on local Brauer groups.

Terminology and notation are standard except that we use the same symbol for a field and its multiplicative group, relying on context for the distinction.

Let $[K:Q]$ be finite and let M/K be cyclic with basis $a_1, \ldots, a_n$. Let $f(X_1, \ldots, X_n) = N_{M/K}(X_1 a_1 + \ldots + X_n a_n)$ and let $0 \neq a \in K$. Let L be a subfield of M containing $a, a_1, \ldots, a_n$. Let $F = L \cap K$ and suppose that L/F is normal.

For each prime $\mathfrak{P}$ of M (including archimedean ones) let the restrictions of $\mathfrak{P}$ to L and K be denoted by $\mathfrak{P}$ and that to F by $\mathfrak{p}$, and let the corresponding completions be $M_{\mathfrak{P}}$, $K_{\mathfrak{P}}$, $L_{\mathfrak{P}}$, $F_{\mathfrak{p}}$ respectively. For each $\mathfrak{p}$ of F let $a^{n_{\mathfrak{p}}}$ be the smallest positive power of a which is in $N_{L_{\mathfrak{P}}/F_{\mathfrak{p}}}(L_{\mathfrak{P}})$. (Note that it is independent of $\mathfrak{P}|\mathfrak{p}$).

THEOREM 1. *Under the above hypotheses $f(X_1, \ldots, X_n) = a$ is solvable in K if and only if for all $\mathfrak{p}$ of F and all extensions $\mathfrak{P}$, $n_{\mathfrak{p}}$ divides $[K_{\mathfrak{P}}:F_{\mathfrak{p}}]$.*

Remark 1. For any M, K, a, $a_1, \ldots, a_n$ we may find such L, $L = M$ will do, though it gives no additional information about the equation. Presumably in most cases we will want to take L as small as possible.

Remark 2. The condition that K/F be finite is superfluous, provided that degree is taken in the sense of supernatural numbers [11]. This follows from the fact that for each $\mathfrak{p}$ if all finite subextensions of K/F could be embedded in extensions of $F_{\mathfrak{p}}$ of degree not divisible by $n_{\mathfrak{p}}$, so could K/F itself.

Proof. Let $H = G(M/K)$, $G = G(L/F)$. Since $F = L \cap K$ the natural map of H to G is an isomorphism. The solvability of the equation in K is equivalent to $\alpha \in N_{M/K}(M)$, solvability in F to $\alpha \in N_{L/F}(L)$ which in turn are equivalent respectively to $\alpha \in N_{M_{\mathfrak{P}}/K_{\mathfrak{P}}}(M_{\mathfrak{P}})$ and $\alpha \in N_{L_{\mathfrak{P}}/F_{\mathfrak{p}}}(L_{\mathfrak{P}})$ for all primes ([2], p. 185).

For each prime $\mathfrak{P}$ consider the diagram

$$\begin{tikzcd}
\widehat{H}^0(G_{\mathfrak{P}}, L_{\mathfrak{P}}) \arrow[r, "\varphi"] \arrow[d, "\varrho_0"'] & H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}) \arrow[r, "\inf"] \arrow[d, "\varrho_2"'] & H^2(\mathscr{G}, \Omega) \arrow[r, "\mathrm{inv}"] \arrow[d, "\varrho"'] & Q/Z \arrow[d, "\mu"'] \\
\widehat{H}^0(H_{\mathfrak{P}}, M_{\mathfrak{P}}) \arrow[r, "\varphi'"] & H^2(H_{\mathfrak{P}}, M_{\mathfrak{P}}) \arrow[r, "\inf"] & H^2(\mathscr{H}, \Omega) \arrow[r, "\mathrm{inv}"] & Q/Z.
\end{tikzcd}$$

Here Ω is an algebraic closure of $M_{\mathfrak{P}}$, $\mathscr{G} = G(\Omega/F_{\mathfrak{p}})$, $\mathscr{H} = G(\Omega/K_{\mathfrak{P}})$, $\widehat{H}^0$ and H^2 are Tate cohomology groups ([2]), ϱ_0, ϱ_2 are induced by the natural maps $H_{\mathfrak{P}} \to G_{\mathfrak{P}}$, $L_{\mathfrak{P}} \to M_{\mathfrak{P}}$, ϱ is the restriction map, φ and φ' are the natural isomorphisms of cohomology in the case of cyclic groups, inf and inv denote the inflation and invariant maps respectively, and μ is multiplication by the local degree $[K_{\mathfrak{P}}:F_{\mathfrak{P}}]$. Commutativity of the left two squares is routine, that of the right hand square is well known (e.g. [12], p. 201).

Let $\bar{\alpha}$ be the class of α in $\widehat{H}^0(G_{\mathfrak{P}}, L_{\mathfrak{P}})$; by assumption it is of order $n_{\mathfrak{p}}$. We wish to determine under what circumstances $\varrho_0(\bar{\alpha}) = 0$.

The maps inf and inv are known to be injective (see [11], p. I-15, [12], p. 200) so $\varrho_0(\bar{\alpha}) = 0$ iff $\mu\Big(\mathrm{inv}\big(\inf(\varphi(\bar{\alpha}))\big)\Big) = 0$. But $\mathrm{inv}\big(\inf(\varphi(\bar{\alpha}))\big)$ is of order $n_{\mathfrak{p}}$ so this is the case if and only if the local degree $[K_{\mathfrak{P}}:F_{\mathfrak{p}}]$ is a multiple of $n_{\mathfrak{p}}$. Q.E.D.

COROLLARY. *If $n = q$, a prime, then α is representable in K if and only if for each $\mathfrak{p}$ for which it is not representable in $F_{\mathfrak{p}}$, q divides $[K_{\mathfrak{P}}:F_{\mathfrak{p}}]$ for all extensions $\mathfrak{P}$ of $\mathfrak{p}$.*

Examples. We treat several cases of binary quadratic forms and one ternary cubic form. Binary (and some other) quadratic forms were treated by Hasse in [6], and our explicit answers can also be derived from the general results there.

If we wish to know whether a rational binary quadratic form of a given discriminant represents a given rational integer over a given number field K we may first transform the form to X^2+dY^2 where d, the discriminant, is a square-free integer. We may assume the number c to be represented is a square-free integer, and since the question is trivial if c/d is a rational square we may assume $cd \notin Z^2$. The answer is then contained in the following:

THEOREM 2. *The equation $X^2+dY^2 = c$ where d and c are non-zero square-free integers with $dc \notin Z^2$, is solvable in K $(-d \notin K^2)$, if and only if*

1. *K has no real imbeddings if $c < 0$, $d > 0$;*

2. *The degrees $[K_{\mathfrak{P}}:Q_p]$ are even for any prime $\mathfrak{P}$ extending an odd prime p of Q satisfying any of the following:*

(a) $\left(\dfrac{c}{p}\right) = 0, \left(\dfrac{-d}{p}\right) = -1,$

(b) $\left(\dfrac{d}{p}\right) = 0, \left(\dfrac{c}{p}\right) = -1,$

(c) $\left(\dfrac{c}{p}\right) = \left(\dfrac{d}{p}\right) = 0, \left(\dfrac{c/p}{p}\right) \neq \left(\dfrac{d/p}{p}\right);$

3. *If any of the following hold*

$$\begin{array}{ll}
d \equiv -3\ (8), & c \equiv 2, 3, 7\ (8), \\
d \equiv -5\ (8), & c\ \textit{even}, \\
d \equiv -7\ (8), & c \equiv 3, 6, 7\ (8), \\
d \equiv -6\ (16), & c \equiv 2, 5, 6, 7, 13, 15\ (16), \\
d \equiv -10\ (16), & c \equiv 2, 3, 5, 11, 13, 14\ (16), \\
d \equiv -14\ (16), & c \equiv 5, 6, 7, 10, 13, 15\ (16), \\
d \equiv -2\ (16), & c \equiv 3, 5, 6, 10, 11, 13\ (16),
\end{array}$$

then the local degrees $[K_{\mathfrak{P}}:Q_2]$ are even for the primes dividing 2.

Proof. Let $L = Q(\sqrt{-d})$, $M = KL$. For infinite primes the equation is locally solvable for complex imbeddings and solvable for real imbeddings unless $d > 0$, $c < 0$.

For odd primes dividing neither d nor c the extension L/Q is unramified and c a local unit, hence a local norm.

For odd primes with $\left(\dfrac{-d}{p}\right) = 1$ the local extension is trivial so there is no condition.

For odd primes dividing c but not d with $\left(\dfrac{-d}{p}\right) = -1$ the extension is unramified and the local norms are the local units by local class field theory [12]. Hence the equation is not solvable in Q_p.

For odd primes dividing d but not c, the extension is ramified, hence by local class field theory the local norms do not include the group generated by squares and local units. But c generates this group modulo squares unless it itself is a square. Hence if $\left(\dfrac{c}{p}\right) = -1$, c is not representable in Q_p.

For odd primes dividing d and c let r be any element with $\left(\frac{r}{p}\right) = -1$. Then L/Q is ramified, hence is either $Q_p(\sqrt{p})$ or $Q_p(\sqrt{rp})$ according as $\left(\frac{-d/p}{p}\right) = \pm 1$ and the norm group is $Q_p^2(-p)$ or $Q_p^2(-rp)$ respectively. The element c is in the first if $\left(\frac{-c/p}{p}\right) = 1$, and the second if $\left(\frac{-c/p}{p}\right) = -1$, hence locally a norm iff $\left(\frac{c/p}{p}\right) = \left(\frac{d/p}{p}\right)$.

For primes dividing 2 the proof is similar, if $d \equiv 1\ (8)$ noting that the local extension is trivial and otherwise computing the local norm groups. Q.E.D.

Corollary 1. *$X^2+dY^2 = c$ is solvable in $Q(\sqrt{b})$, (b, c, d square-free integers, cd, $-bd \notin Z^2$) if and only if*

1. *If $c < 0$, $d > 0$ then $b < 0$;*
2. *For any p for which any of the conditions of 2 above hold, $\left(\frac{b}{p}\right) = 0$ or -1;*
3. *If any of the conditions of 3 above hold then $b \not\equiv 1\ (8)$.*

Remark. N. Plotkin [10] has shown that this condition is equivalent to the solvability of

$$dt^2 - dcu^2 - cv^2 = -b \text{ in } Q.$$

Corollary 2. *$X^2+dY^2 = c$ is solvable in $Q(\zeta_n)$ (c, d square-free integers, $cd \notin Z^2$, n odd, $\sqrt{-d} \notin Q(\zeta_n)$) if and only if*

1. *$n \neq 1$ if $d > 0$, $c < 0$;*
2. *For all p for which any of the conditions of 2 of Theorem 2 hold, either p divides n or p has even order* mod$n$;
3. *If any of the conditions of 3 of Theorem 2 hold then 2 has even order* mod n.

Remark. If $d = 1$, $c = -1$ the above corollaries give the stufe of quadratic and cyclotomic fields ([1], [3], [4], [5], [7], [8], [9], [10]).

We close with an example of a cubic norm form. Let $\zeta = e^{2\pi i/7}$, $L = Q(\zeta+\zeta^{-1})$,

$$\begin{aligned} f(X, Y, Z) &= N_{L/Q}\big(X+(\zeta+\zeta^{-1})Y+(\zeta^2+\zeta^{-2})Z\big) \\ &= X^3+Y^3+Z^3-X^2Y-X^2Z-2XY^2-2XZ^2+3Y^2Z-4YZ^2-4XYZ. \end{aligned}$$

Then for any cube free integer a in Z, the local conditions for representability in Q are that primes other than 7 dividing a split completely in L, hence are congruent to $\pm 1 \bmod 7$, and for the prime 7 that the 7-free part of a is congruent to $\pm 1 \bmod 7$. (Note that this follows from the other conditions, a reflection of the fact that the sum of local invariants is 0). For primes not satisfying this, the local degrees must be divisible by 3. Hence a is represented by f in K if and only if

1. For all primes $\mathfrak{P}$ extending a prime divisor p of a congruent 2, 3, 4 or $5 \bmod 7$, $[K_{\mathfrak{P}}:Q_p]$ is divisible by 3;
2. If a', the result of removing any 7's in a, is not $\equiv \pm 1 \bmod 7$ then for any $\mathfrak{P}$ of K extending 7, $[K_{\mathfrak{P}}:Q_7]$ is divisible by 3.

References

[1] F. W. Barnes, *On the stufe of an algebraic number field*, J. Number Theory, 4 (1972), pp. 474–476.

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Washington, D. C., 1967.

[3] P. Chowla, *On the representation of -1 as a sum of squares in a cyclotomic field*, J. Number Theory 1 (1969), pp. 208–210.

[4] — and S. Chowla, *Determination of the stufe of certain cyclotomic fields*, J. Number Theory 2 (1970), pp. 271–272.

[5] B. Fein, B. Gordon and J. Smith, *On the representation of -1 as a sum of two squares in an algebraic number field*, J. Number Theory 3 (1971), pp. 310–315.

[6] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. 153 (1924), pp. 113–130.

[7] C. Moser, *Représentation de -1 par une somme de carrés dans certains corps locaux et globaux et dans certains anneaux d'entiers algébriques*, C. R. Acad. Sci. Paris, Ser. A-B 271 (1970), pp. A1200–A1203.

[8] — *Représentation de -1 comme somme de carrés dans un corps cyclotomique quelconque*, J. Number Theory 5 (1973), pp. 139–141.

[9] T. Nagell, *Sur la résolubilité de l'équation $x^2+y^2+z^2 = 0$ dans un corps quadratique*, Acta Arith. 21 (1972), pp. 35–43.

[10] N. Plotkin, *The solvability of the equation $ax^2+by^2 = c$ in quadratic fields*, Proc. Amer. Math. Soc. 34 (1972), pp. 337–339.

[11] J. P. Serre, *Cohomologie Galoisienne*, 4th ed., Berlin 1973.

[12] — *Corps Locaux*, Paris 1962.

Received on 10.12.1973
and in revised form on 10.5.1974 (516)