Die Determinante dieses Gleichungssystems in $s_1, \ldots, s_n$ ist D. Nach Voraussetzung ist $D \not\equiv 0 \bmod p$, also hat das System (6) eine eindeutige Lösung $(s_1, \ldots, s_n) \bmod p$. Daraus folgt, daß das System (2) eine eindeutige Lösung k hat. Also ist der Satz in der einen Richtung gezeigt.

Sei nun umgekehrt $\mathfrak{h}$ ein Permutationsfunktionsvektor mod p^e. Dann ist $\mathfrak{h}$ auch einer mod p. Angenommen es sei $D \equiv 0 \bmod p$ für das Argument $(r_1, \ldots, r_n)$. Man setzt $k_i \equiv f_i(r_1, \ldots, r_n)/g_i(r_1, \ldots, r_n) \bmod p^e$ ein in die Kongruenz

$$(7) \quad \big(f_1(r_1, \ldots, r_n) - k_1 g_1(r_1, \ldots, r_n), \ldots, f_n(r_1, \ldots, r_n) - k_n g_n(r_1, \ldots, r_n)\big) \equiv (0, \ldots, 0) \bmod p^e.$$

Nach Voraussetzung ist $\mathfrak{h}$ ein Permutationsfunktionsvektor mod p^e, also auch einer mod p^{e-1}, d.h. (7) hat sowohl mod p^e als auch mod p^{e-1} genau eine Lösung $(r_1, \ldots, r_n)$. Alle Lösungen von (7) mod p^e bekommt man durch das Verfahren im Hinreichend-Beweis. Dort kommt man auf das System (6). Die Determinante dieses Systems ist aber jetzt $\equiv 0 \bmod p$. Daraus folgt: Es gibt mod p mehr als eine oder überhaupt keine Lösung $(s_1, \ldots, s_n)$. Daher ist (7) nicht eindeutig lösbar, im Widerspruch zur Voraussetzung. Also gilt $D \not\equiv 0 \bmod p$ und Satz 2 ist vollständig bewiesen.

Literatur

[1] L. Carlitz, *A note on permutation functions over a finite field*, Duke Math. Journ. 29 (1962), S. 325–332.

[2] R. Lidl, *Über Permutationspolynome in mehreren Unbestimmten*, Monatsh. Math. 75 (1971), S. 432–440.

[3] W. Nöbauer, *Gruppen von Restklassen nach Restpolynomidealen*, Monatsh. Math. 59 (1955), S. 118–145.

[4] — *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), S. 230–238.

[5] — *Zur Theorie der Polynomtransformationen und Permutationspolynome*, Math. Ann. 157 (1964), S. 332–342.

[6] — *Bemerkungen über die Darstellung von Abbildungen durch Polynome und rationale Funktionen*, Monatsh. Math. 68 (1964), S. 138–142.

[7] L. Redei, *Über eindeutig umkehrbare Polynome in endlichen Körpern*, Acta Scientiarium Math. 11 (1946–48), S. 85–92.

[8] — und T. Szele, *Algebraisch-zahlentheoretische Betrachtungen über Ringe I*, Acta Math. 79 (1947), S. 291–320.

IV. INSTITUT FÜR MATHEMATIK
Technische Hochschule, Wien

Eingegangen 18. 12. 1970 (128)

ACTA ARITHMETICA
XX (1972)

An application of Zassenhaus' unit theorem

by

HAROLD BROWN (Ohio)

In this note we present a direct application of Zassenhaus' generalized Dirichlet unit theorem [2] to the proof of an interesting result on orders with finite unit groups. This result is useful, e.g., in the determination of normalizers of finite unimodular groups [1].

THEOREM. *Let D be a finite dimensional division algebra over $\boldsymbol{Q}$, and let $\mathcal{O}$ be a maximal $\boldsymbol{Z}$-order in D. Then $U(\mathcal{O})$, the unit group of $\mathcal{O}$, is finite if and only if D is $\boldsymbol{Q}$-isomorphic to $\boldsymbol{Q}$, an imaginary quadratic extension of $\boldsymbol{Q}$, or a positive definite quaternion algebra over $\boldsymbol{Q}$.*

Proof. Let $\boldsymbol{R}\mathcal{O}$ denote the tensor product of $\boldsymbol{R}$ and $\mathcal{O}$. Since $\mathcal{O}$ contains a free $\boldsymbol{Q}$-basis for D, $\boldsymbol{R}\mathcal{O} \cong \boldsymbol{R} \otimes_{\boldsymbol{Q}} D$. We will show that if $U(\mathcal{O})$ is finite, then $\boldsymbol{R}\mathcal{O}$ is a division algebra over $\boldsymbol{R}$.

Let $\varphi\colon \boldsymbol{R}\mathcal{O} \to \mathrm{Hom}(\boldsymbol{R}\mathcal{O}, \boldsymbol{R}\mathcal{O})$ be the left regular representation of $\boldsymbol{R}\mathcal{O}$, and for any $x \in \boldsymbol{R}\mathcal{O}$ and any $\boldsymbol{R}$-basis B for $\boldsymbol{R}\mathcal{O}$, let $\hat{\varphi}_B(x)$ be the matrix of $\varphi(x)$ with respect to B. For $x \in \boldsymbol{R}\mathcal{O}$, let $\|x\|$ denote the regular norm of x, i.e. $\|x\| = \det \hat{\varphi}_B(x)$.

Consider $L(\mathcal{O}) = \{x \in \boldsymbol{R}\mathcal{O} \mid \|x\| = \pm 1\}$. $L(\mathcal{O})$ is clearly closed under multiplication, and for any $x \in L(\mathcal{O})$, $\|x\| = \det \hat{\varphi}_B(x) \neq 0$ implies x is not a left zero divisor in $\boldsymbol{R}\mathcal{O}$. Since $\boldsymbol{R}\mathcal{O}$ is finite dimensional over $\boldsymbol{R}$, there exists $y \in \boldsymbol{R}\mathcal{O}$ such that $xy = 1$. Therefore, $\hat{\varphi}_B(y) = \hat{\varphi}_B(x)^{-1}$ and $\hat{\varphi}_B(y)\hat{\varphi}_B(x) = I_n$. Since the regular representation is faithful, we have $yx = 1$, i.e. $y = x^{-1}$. Thus $L(\mathcal{O})$ is a subgroup of the unit group of $\boldsymbol{R}\mathcal{O}$. Also, $L(\mathcal{O})$ contains $U(\mathcal{O})$. For if we choose B as an integral basis for $\mathcal{O}$, then $x \in U(\mathcal{O})$ implies $\hat{\varphi}_B(x)$ and $\hat{\varphi}_B(x^{-1}) = \hat{\varphi}_B(x)^{-1}$ are integral matrices. Thus $\|x\| = \pm 1$.

Let $t = \dim_{\boldsymbol{R}} \boldsymbol{R}\mathcal{O} = \operatorname{rank} \mathcal{O}$, and let $L(\mathcal{O})$ have the topology induced by the usual Euclidean topology on $M_{t\times t}(\boldsymbol{R})$. $L(\mathcal{O})$ is a Lie group with respect to this topology[1]. By Zassenhaus' theorem $U(\mathcal{O})$ is a discrete subspace of $L(\mathcal{O})$ with compact factor space. Thus, if $U(\mathcal{O})$ is finite, $L(\mathcal{O})$ must be compact, i.e. closed and bounded.

[1] Note that we could equivalently use the topology of $\boldsymbol{R}\mathcal{O}$ as a t-dimensional real manifold as $\hat{\varphi}_B$ is a topological isomorphism.

$\boldsymbol{R}\mathcal{O}$ is a semi-simple algebra over $\boldsymbol{R}$. By Wedderburn's structure theorems, $\boldsymbol{R}\mathcal{O} = \bigoplus_1^k T_i$ where each T_i is $\boldsymbol{R}$-isomorphic to some $M_{n_i \times n_i}(B_i)$, B_i a finite dimensional division algebra over $\boldsymbol{R}$. Choose an $\boldsymbol{R}$-basis B for $\boldsymbol{R}\mathcal{O}$ by selecting an $\boldsymbol{R}$-basis for each T_i. Then for $x \in \boldsymbol{R}\mathcal{O}$, say $x = \bigoplus_1^k x_i$, $x_i \in T_i$, we have $x \in L(\mathcal{O})$ if and only if $\prod_{i=1}^k \|x_i\|_i = \pm 1$ where $\|x_i\|_i$ is the regular norm of x_i in T_i.

We claim that if $U(\mathcal{O})$ is finite, then k must be 1. For if $k > 1$, say $\dim_{\boldsymbol{R}} T_1 = k_1$ and $\dim_{\boldsymbol{R}} T_2 = k_2$, let $x = 2 \oplus 2^{-k_1/k_2} \oplus 1 \oplus \ldots \oplus 1$. Then x, and thus all of its integral powers, are in $L(\mathcal{O})$. But $\{x^s \mid s \in \boldsymbol{Z}\}$ is unbounded, which is a contridiction. Hence if $U(\mathcal{O})$ is finite, $\boldsymbol{R}\mathcal{O} \underset{\boldsymbol{R}}{\cong} M_{n\times n}(C)$ where C is a finite dimensional division algebra over $\boldsymbol{R}$. We will show that in this case n must be 1.

Let $\psi\colon \boldsymbol{R}\mathcal{O} \to M_{n\times n}(C)$ be an $\boldsymbol{R}$-isomorphism and let $b_1, \ldots, b_s$ be an $\boldsymbol{R}$-basis for C. Then $\{e_{ij} b_q \mid 1 \leqslant i, j \leqslant n;\ 1 \leqslant q \leqslant s\}$ ordered lexicographically is an ordered $\boldsymbol{R}$-basis for $M_{n\times n}(C)$. Here the e_{ij} denote the usual matrix units. Since ψ is a $\boldsymbol{R}$-isomorphism, $B = \{\psi^{-1}(e_{ij} b_q)\}$ is an $\boldsymbol{R}$-basis for $\boldsymbol{R}\mathcal{O}$. Let $\psi(x) = I_n + e_{1n}$. Then $\hat{\varphi}_B(x)$ is of the form

$$\begin{bmatrix} 1 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & . & . & . & . & . & . & 0 & 1 \\ 0 & . & . & . & . & . & . & 0 & 1 \end{bmatrix}.$$

Now $\|x\| = 1$, i.e. $x \in L(\mathcal{O})$, but $\{x^q \mid q \in \boldsymbol{Z}\}$ is unbounded if $n > 1$.

Thus we have that if $U(\mathcal{O})$ is finite, $\boldsymbol{R}\mathcal{O}$ is a finite dimensional division algebra over $\boldsymbol{R}$. Hence, since $\boldsymbol{R}\mathcal{O} \cong \boldsymbol{R} \otimes_{\boldsymbol{Q}} D$, D must be $\boldsymbol{Q}$-isomorphic to either $\boldsymbol{Q}$, an imaginary quadratic extension of $\boldsymbol{Q}$ or a positive definite quaternion algebra over $\boldsymbol{Q}$. This condition is clearly also sufficient to assure that $U(\mathcal{O})$ is finite.

References

[1] H. Brown, J. Neubuser and H. Zassenhaus, *On integral groups III*, to appear.

[2] H. Zassenhaus, *On the units of orders*, to appear.

THE OHIO STATE UNIVERSITY

Received on 8. 4. 1971 (155)

ACTA ARITHMETICA
XX (1972)

Solvability of a Diophantine inequality in algebraic number fields

by

S. Raghavan and K. G. Ramanathan (Bombay)

1. Introduction. Let K be a totally real algebraic number field of finite degree h over the field $\boldsymbol{Q}$ of rational numbers and $\bar{K} = K \otimes_{\boldsymbol{Q}} \boldsymbol{R}$ the tensor product of K with the field $\boldsymbol{R}$ of real numbers. Any element α in $\bar{K}$ is represented as

$$\alpha = \begin{pmatrix} \alpha^{(1)} & & 0 \\ & \ddots & \\ 0 & & \alpha^{(h)} \end{pmatrix}$$

where $\alpha^{(1)}, \ldots, \alpha^{(h)}$ are the 'conjugates' of α. Put

$$\|\alpha\| = \max_{1 \leqslant k \leqslant h} |\alpha^{(k)}|. \tag{1}$$

Let $m \geqslant 2$ be a rational integer and

$$f(x_1, \ldots, x_s) = \sum_{r=1}^{s} a_r x_r^m \tag{2}$$

be a polynomial with coefficients a_r in $\bar{K}^*$, the group of non-singular elements of $\bar{K}$. We say that $f(x_1, \ldots, x_s)$ is *totally indefinite*, if, for every k, $1 \leqslant k \leqslant h$,

$$f^{(k)}(x_1, \ldots, x_s) = \sum_{r=1}^{s} a_r^{(k)} x_r^m = 0$$

has a real solution with all $x_1, \ldots, x_s$ *not* equal to zero.

Let $\mathfrak{O}$ denote the ring of integers of K. The object of this paper is to prove the following

Theorem. *Let $f(x_1, \ldots, x_s)$ be a totally indefinite polynomial over $\bar{K}^*$ given by* (2). *Let*

$$f \neq \lambda \varphi(x_1, \ldots, x_s)$$

where $\lambda \in \bar{K}^*$ and $\varphi(x_1, \ldots, x_s)$ is a polynomial with coefficients in K. Let $mh \geqslant 4$ and

$$s \geqslant \max\left(2^m + 2,\ h 2^{m-1}(m-1) + h^2 + h\right). \tag{3}$$