ACTA ARITHMETICA
XXVI (1975)

Lineare Abhängigkeit von Wurzeln

von

MARTIN KNESER (Göttingen)

L/K sei eine separabel algebraische Körpererweiterung, $K^\times$ die multiplikative Gruppe von K, M eine Untergruppe von $L^\times$ mit endlicher Faktorgruppe $K^\times M/K^\times$. Wir setzen voraus, daß für ungerade Primzahlen p jede zu $K^\times M$ gehörige p-te Einheitswurzel schon in K liegt, und daß $i = \sqrt{-1}$ in K liegt falls $1 \pm i \in K^\times M$ ist. Dann gilt der

SATZ. *Der durch Adjunktion von M entstehende Körper $K(M)$ hat über K den* Grad $[K^\times M : K^\times]$.

Wenn K hinreichend viele Einheitswurzeln enthält, so handelt es sich um eine wohlbekannte Aussage über Kummersche Erweiterungen. Andere Spezialfälle, in denen L ausser ± 1 keine Einheitswurzeln enthält, wurden von Besicovitch [1], Mordell [2], Siegel [3] bewiesen.

Beweis. $K(M)$ besteht aus Linearkombinationen von Elementen aus $K^\times M$ mit Koeffizienten aus K, hat also über K höchstens den Grad $[K^\times M : K^\times]$ (1). Ist andererseits p eine Primzahl, p^t die höchste in $[K^\times M : K^\times]$ aufgehende Potenz von p, $N/K^\times$ die Untergruppe von $K^\times M/K^\times$ mit der Ordnung p^t, und weiß man, daß $[K(N):K] = p^t$ ist für alle p, so muß $[K(M):K]$ durch p^t teilbar und daher gleich $[K^\times M : K^\times]$ sein. Es genügt also, den Satz für den Fall zu beweisen, daß $[K^\times M : K^\times]$ Potenz einer Primzahl p ist.

In diesem Fall wählen wir Untergruppen $K^\times = N_0 \subset N_1 \subset \ldots \subset N_t = K^\times M$ mit $[N_s : N_{s-1}] = p$ und beweisen dann durch Induktion nach s, daß $K(N_s)$ über $K(N_{s-1})$ den Grad p hat, und daß ein Element aus $K(N_s)$ (bzw. aus $K(N_s) \cap K^\times M$, falls $p = 2$ und $i \in K(N_s)$ ist), dessen p-te Potenz in N_s liegt, schon selbst zu N_s gehört.

Wir nehmen die Behauptung für $s-1$ statt s als richtig an. Ein erzeugendes Element a von N_s über N_{s-1} ist Nullstelle des Polynoms $f(X) = X^p - a^p$ mit Koeffizienten in $K(N_{s-1})$. Die Gradrelation folgt,

(1) Wegen der bestehenden linearen Abhängigkeiten zwischen Einheitswurzeln sieht man auch sofort, daß der Grad sicher kleiner ist, wenn die eingangs gemachte Voraussetzung verletzt ist.

wenn f irreduzibel über $K(N_{s-1})$ ist. Wäre das Polynom reduzibel, so hätte es als Binom von Primzahlgrad in $K(N_{s-1})$ eine Nullstelle b, und es folgte $a = be$ mit einer p-ten Einheitswurzel e; weiter $b^p = a^p \in N_{s-1}$, also $b \in N_{s-1}$ nach Induktionsannahme, $e \in N_s$ und damit $e \in K^\times$ nach Voraussetzung; dann wäre aber $a \in N_{s-1}$, im Widerspruch zu $[N_s : N_{s-1}] = p > 1$.

Nun sei $c \in K(N_s)$, $c^p \in N_s$ (und $c \in K^\times M$, falls $p = 2$ und $i \in K(N_s)$ ist), also $c^p = a^q d$ mit $0 \leqslant q < p$, $d \in N_{s-1}$. Wir nehmen zunächst $q > 0$, also prim zu p an und zeigen, daß das zu einem Widerspruch führt. Mit N bezeichnen wir die Norm von $K(N_s)$ nach $K(N_{s-1})$. Wegen $Na = (-1)^{p-1} a^p$ ergibt sich $\big((-1)^{p-1} a^p\big)^q = (Nc)^p d^{-p}$. Für ungerades p ist a^p demnach p-te Potenz eines Elements aus $K(N_{s-1})$, im Widerspruch zu

$$[K(N_s) : K(N_{s-1})] = p.$$

Im Fall $p = 2$ wird $-a^2 = f^2$ mit $f \in K(N_{s-1})$, also $i \in K(N_s)$, $i \notin K(N_{s-1})$, $c^2 = ad = \pm ifd$. Schreibt man $c = g + ih$ mit $g, h \in K(N_{s-1})$, so folgt $g^2 = h^2$, d.h. $c = (1 \pm i)g$. Daraus folgt $g^4 = -c^4/4 \in N_{s-1}$, weiter durch zweimalige Anwendung der Induktionsannahme $g \in N_{s-1}$ und damit $1 \pm i \in K^\times M$, was zusammen mit $i \notin K(N_{s-1})$ der anfangs gemachten Voraussetzung widerspricht.

Wir haben hiernach $c^p \in N_{s-1}$. Ist S ein Isomorphismus von $K(N_s)$ in einen Oberkörper, der alle Elemente aus $K(N_{s-1})$, nicht aber a fest lässt, also $Sa = ae$ mit einer primitiven p-ten Einheitswurzel e, so gilt $Sc^p = c^p$, also $Sc = ce^r$, und daraus folgt $c = a^r b$ mit $b \in K(N_{s-1})$; weiter $b^p \in N_{s-1}$ (und $b \in K^\times M$, falls $c \in K^\times M$), also $b \in N_{s-1}$, nach Induktionsannahme und damit $c \in N_s$.

Literaturverzeichnis

[1] A. S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15 (1940), S. 3–6.

[2] L. J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. 3 (1953), S. 625–630.

[3] C. L. Siegel, *Algebraische Abhängigkeit von Wurzeln*, Acta Arith. 21 (1972), S. 59–64.

Eingegangen 22. 12. 1973 (512)

ACTA ARITHMETICA
XXVI (1975)

One-class genera of positive quadratic forms in at least five variables

by

G. L. Watson (London)

1. Introduction. Let f be a positive-definite quadratic form, with integer coefficients, in any number n of variables; and denote by $c(f)$ the number of classes in the genus of f. I showed in [1] and [2] that there exists an f with $c(f) = 1$ if and only if $n \leqslant 10$. Now it would be of interest to find all the one-class genera of positive n-ary forms for any n with $2 \leqslant n \leqslant 10$ ($n = 1$ is trivial); especially for $n = 2$, which however seems hopeless.

Using a method based on the results of [3], I break the problem up into two parts. The second of these, which I defer to a later paper, involves a great deal of calculation, but is considerably simplified by using the results of [4]. The first part, done for $n = 3, 4$ in [5], [6], and for $5 \leqslant n \leqslant 10$ in this paper, consists in finding all the one-class positive genera that have certain simple arithmetic properties explained in the next section. The number of such genera is 1 for $n = 1$ and 20, 27, 14, 14, 7, 5, 1, 1 for $n = 3, \ldots, 10$; and considerably greater for $n = 2$.

On choosing reduced representatives of the $42 = 14 + \ldots + 1$ of these genera that have $n \geqslant 5$, and putting in $10 = 1 + 1 + 2 + 6$ forms with $n \leqslant 4$, we obtain a list of 52 forms $F_1, \ldots, F_{52}$ each of which, except $F_1 = x_1^2$, has one of the others as its leading $(n-1)$-ary section. This feature of the result shortens both the statement (see Table 1, below) and the proof of the main result.

2. Strongly primitive (SP) and square-free (SF) forms. We use the notation

$$\sum\{a_{ij} x_i x_j : 1 \leqslant i \leqslant j \leqslant n\} \tag{2.1}$$

for a quadratic form (with integer coefficients a_{ij}); and for $j < i$ we write $a_{ij} = a_{ji}$. For n-ary f and prime p we define $r_p(f)$ as the least of the