Über die Arfsche Invariante quadratischer Formen mod 2.

Von Wilhelm Klingenberg und Ernst Witt in Hamburg.

Über einem Körper K der Charakteristik 2 mit den Elementen $\alpha, \beta, \gamma, \dots$ betrachten wir die quadratische Form

$$(1) \quad F(x) = x'Ax = \sum \alpha_{ik}x_i x_k.$$

Durch die Form F ist die Matrix A bis auf Abänderungen $A \rightarrow A + B$ mit $\beta_{ik} = \beta_{ki}$ und $\beta_{ii} = 0$ eindeutig festgelegt. Daher ist die Matrix $I = A + A'$ der Form F eindeutig zugeordnet. Der simultane Übergang von A, B, I zu $A^* = S'AS, B^* = S'BS, I^* = S'IS$ entspricht einer Variablentransformation der Form F . Wir setzen voraus, daß F vollregulär ist, das heißt es soll $|I| \neq 0$ sein. In diesem Fall dürfen wir annehmen, daß I auf die Gestalt

$$(2) \quad I = \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix} \quad (e = \text{Einheitsmatrix})$$

transformiert ist. Wegen der Abänderungen $A \rightarrow A + B$ läßt sich A so normieren, daß in der linken unteren Teilmatrix nur Nullen auftreten. Wegen $I = A + A'$ hat A dann die Gestalt

$$(3) \quad A = \begin{pmatrix} p & e \\ 0 & q \end{pmatrix} \quad p = p'; \quad q = q'.$$

Das Ziel dieser Note ist der Beweis des Satzes:

Die Spur $\text{Sp}(pq)$ ist mod $\gamma^2 + \gamma$ eine Invariante der quadratischen Form F bezüglich Äquivalenz.

$\text{Sp}(pq)$ stimmt überein mit einer von Č. Arf¹⁾ in anderer Form angegebenen Invariante.

Durch die Normierung (2) von I sind nur noch Transformationen $A^* = S'AS$ mit einem S aus der symplektischen Gruppe $\mathfrak{S}$ möglich, die ja gerade definiert ist durch die Gleichung

$$(4) \quad S'IS = I.$$

Zum Beweis müssen wir also zeigen, daß

$$\text{Sp}(p^*q^*) = \text{Sp}(pq) \text{ mod } \gamma^2 + \gamma$$

ist, wenn p^*, q^* aus einem $A^* = S'AS$ mit $S \in \mathfrak{S}$ entnommen sind.

¹⁾ Č. Arf, Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. J. reine angew. Math. 183 (1941), 148–167. — Die vorliegende Note entstand in einer Diskussion über die voranstehende Arbeit von Witt; hier wird die Arfsche Invariante in allgemeiner Form angegeben.

Wir stellen Regeln für das Rechnen mit Spuren zusammen:

- (I) $\text{Sp}(srs^{-1}) = \text{Sp}(r)$
 (II) $\text{Sp}(r_1 r_2 \cdots r_n) = \text{Sp}(r_2 \cdots r_n r_1)$
 (III) $\text{Sp}(r + s) = \text{Sp}(r) + \text{Sp}(s)$
 (IV) $\text{Sp}(r^2) = (\text{Sp}(r))^2$.

Erster Beweis des Satzes. Wir benutzen, daß $\mathfrak{S}$ erzeugt wird von

$$(5) \quad S_1 = \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix}; \quad S_2 = \begin{pmatrix} r' & 0 \\ 0 & r^{-1} \end{pmatrix}; \quad S_3 = \begin{pmatrix} e & 0 \\ s & e \end{pmatrix} \quad (\text{mit } s = s').$$

Es genügt, die Invarianz gegenüber diesen Erzeugenden nachzuweisen. Man findet

für $S = S_1$: $\text{Sp}(p^* q^*) = \text{Sp}(qp) = \text{Sp}(pq)$ wegen (II),

für $S = S_2$: $\text{Sp}(p^* q^*) = \text{Sp}(r p q r^{-1}) = \text{Sp}(pq)$ wegen (I),

für $S = S_3$: $\text{Sp}(p^* q^*) = \text{Sp}(pq + sq + sqsq) = \text{Sp}(pq) + \text{Sp}(sq) + (\text{Sp}(sq))^2$

wegen (III) und (IV).

Zweiter Beweis des Satzes. Wir schreiben $S \in \mathfrak{S}$ in der Form

$$(6) \quad S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(4) schreiben wir in der Form $S^{-1} = IS'I$ oder, mit (6),

$$(7) \quad S^{-1} = \begin{pmatrix} d' & b' \\ c' & a' \end{pmatrix}.$$

$SS^{-1} = E$ liefert mit (6) und (7) die Gleichungen

$$(8) \quad ad' + bc' = cb' + da' = e; \quad ab' = ba'; \quad cd' = dc'.$$

Mit einem S in der Form (6) finden wir

$$(9) \quad \text{Sp}(p^* q^*) = \text{Sp}[(a'pa + a'c + c'qc)(b'pb + b'd + d'qd)].$$

Multiplizieren wir die rechte Seite aus, so finden wir unter anderem

$$(10) \quad \begin{aligned} & \text{Sp}(a'pab'pb + a'pab'd + a'cb'pb) \\ & = (\text{Sp}(a'pb))^2 + \text{Sp}(a'pba'd + a'(e + da')pb) = (\text{Sp}(a'pb))^2 + \text{Sp}(a'pb). \end{aligned}$$

Dabei wurden (8), (III), (IV) und (II) benutzt. Auf dieselbe Weise behandeln wir einen Ausdruck, der aus (10) durch die Ersetzung $p, a, b \rightarrow q, c, d$ entsteht.

Schließlich tritt in (9) noch auf

$$(11) \quad \begin{aligned} & \text{Sp}(a'pad'qd + c'qcb'pb + a'cb'd) \\ & = \text{Sp}[p(bc' + e)q(cb' + e) + pbc'qcb' + cb'(cb' + e)] \\ & = \text{Sp}(pq) + (\text{Sp}(cb'))^2 + \text{Sp}(cb') + \text{Sp}(qcb'p + pbc'q). \end{aligned}$$

Der letzte Term verschwindet aber wegen $pbc'q = (qcb'p)'$.