Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. (Teil I.)

Von *Cahit Arf* in Istanbul.

Einleitung.

Witt [1]) hat eine Theorie der quadratischen Formen in beliebigen Körpern k aufgestellt. Er setzt dabei jedoch voraus, daß k nicht die Charakteristik 2 hat. Dann ist jede quadratische Form in eine Diagonalform $F = \sum_{i=1}^{n} a_i x_i^2$ transformierbar. Unter Heranziehung eines durch F metrisierten Vektorraumes wird in W. Q. bewiesen, daß die Algebra $\prod_{i \leqq j} (a_i, a_j)$ und die Zahlklasse $\prod_i a_i k^2$ Invarianten der Form F sind, und daß diese Invarianten zusammen mit n für spezielle Körper k die Form F bis auf äquivalente charakterisieren.

Wir wollen in diesem ersten Teil mittels ähnlicher Methoden wie in W. Q. den dort nicht betrachteten Fall untersuchen, daß k die Charakteristik 2 hat. Das Ergebnis dieser Untersuchung soll dann in einem zweiten Teil angewendet werden auf die Aufstellung der Invarianten für die arithmetische Äquivalenz der binären, ternären und quaternären Formen in einem Potenzreihenkörper mit Koeffizienten aus einem vollkommenem Körper der Charakteristik 2.

Die Anregung zu dieser Arbeit verdanke ich H. Hasse [2]).

I. Quadratische Formen in Körpern der Charakteristik 2.

Wir legen einen festen Körper k der Charakteristik 2 als Grundkörper zugrunde und betrachten quadratische Formen

$$F = \sum_{1 \leqq i \leqq j \leqq m} a_{ij} x_i x_j$$

mit Koeffizienten a_{ij} aus k.

Wie in W. Q. ordnen wir einer quadratischen Form F einen durch sie metrisierten Vektorraum

$$\mathfrak{R} = \sum_{i=1}^{m} k\,\mathfrak{u}_i = \langle \mathfrak{u}_1, \ldots, \mathfrak{u}_m \rangle$$

über k zu, indem wir das Längenquadrat eines Vektors

$$\mathfrak{x} = \sum_{i=1}^{m} x_i \mathfrak{u}_i$$

aus $\mathfrak{R}$ durch

---

[1]) E. Witt, Theorie der quadratischen Formen in beliebigen Körpern. Dieses Journal **176** (1937), 31—44; im folgenden mit W. Q. zitiert.

[2]) Anmerkung des Herausgebers: Im Einverständnis mit dem Verfasser habe ich dessen ursprüngliches Ms. überarbeitet.

$$|\mathfrak{x}|^2 = F(\mathfrak{x})$$

definieren. Eine Äquivalenz $F \simeq F'$ zwischen zwei Formen F und F' drückt sich dann durch die Isomorphie $\mathfrak{R} \simeq \mathfrak{R}'$ der zugeordneten metrischen Räume aus, also durch eine umkehrbar eindeutige lineare längentreue Zuordnung zwischen $\mathfrak{R}$ und $\mathfrak{R}'$. Die verschiedenen zu F äquivalenten Formen entsprechen umkehrbar eindeutig den verschiedenen Basen von $\mathfrak{R}$.

Für zwei Vektoren

$$\mathfrak{x} = \sum_{i=1}^{m} x_i \mathfrak{u}_i, \quad \mathfrak{y} = \sum_{i=1}^{m} y_i \mathfrak{u}_i$$

aus $\mathfrak{R}$ definieren wir das skalare Produkt durch die Beziehung

$$|\mathfrak{x} + \mathfrak{y}|^2 = |\mathfrak{x}|^2 + |\mathfrak{y}|^2 + \mathfrak{x}\mathfrak{y},$$

also als die Bilinearform

$$\mathfrak{x}\mathfrak{y} = F(\mathfrak{x}, \mathfrak{y}) = \sum_{1 \leq i < j \leq m} a_{ij}(x_i y_j + x_j y_i).$$

Ist $\mathfrak{x}\mathfrak{y} = 0$, so sagen wir, $\mathfrak{x}$ und $\mathfrak{y}$ sind senkrecht zueinander. Ist $\mathfrak{r}$ ein Teilraum von $\mathfrak{R}$, und ist $\mathfrak{y}$ senkrecht zu allen $\mathfrak{x}$ aus $\mathfrak{r}$, so nennen wir $\mathfrak{y}$ senkrecht zu $\mathfrak{r}$. Mit $\mathfrak{r}^*$ bezeichnen wir den Teilraum aller zu $\mathfrak{r}$ senkrechten Vektoren aus $\mathfrak{R}$. Ist $\mathfrak{s}$ ein weiterer Teilraum von $\mathfrak{R}$, und sind alle $\mathfrak{y}$ aus $\mathfrak{s}$ senkrecht zu $\mathfrak{r}$, so sagen wir, $\mathfrak{r}$ und $\mathfrak{s}$ sind senkrecht zueinander. Unter einer *direkten Zerlegung* $\mathfrak{R} = \mathfrak{r} + \mathfrak{s}$ verstehen wir eine Zerlegung von $\mathfrak{R}$ in zwei zueinander fremde und zueinander senkrechte Teilräume $\mathfrak{r}$ und $\mathfrak{s}$. Ihr entspricht eine Darstellung $F = f + g$ als Summe zweier Formen f und g in untereinander verschiedenen Variablen. Wir verwenden das Pluszeichen bei Räumen und Formen nur im Sinne dieser direkten Zerlegung.

Durch $\mathfrak{R}$ ist invariant der Teilraum $\mathfrak{R}^*$ aller zu dem vollen Raum $\mathfrak{R}$ senkrechten Vektoren aus $\mathfrak{R}$ bestimmt. Er zerfällt direkt in eindimensionale Teilräume:

$$\mathfrak{R}^* = \sum_{j=1}^{n^*} \langle \mathfrak{w}_j \rangle.$$

Ist $\mathfrak{R}^* = 0$, so nennen wir $\mathfrak{R}$ und die zugehörigen Formen *vollregulär*. Es gilt nun weiter:

Satz 1. *Der Raum $\mathfrak{R}$ zerfällt direkt in zweidimensionale vollreguläre Teilräume und $\mathfrak{R}^*$:*

$$\mathfrak{R} = \sum_{i=1}^{n} \langle \mathfrak{u}_i, \mathfrak{v}_i \rangle + \mathfrak{R}^* \quad \textit{mit} \quad \mathfrak{u}_i \mathfrak{v}_i \neq 0.$$

Beweis. Ist $\mathfrak{u}_1$ ein nicht zu $\mathfrak{R}^*$ gehöriger Vektor aus $\mathfrak{R}$, so gibt es in $\mathfrak{R}$ einen Vektor $\mathfrak{v}_1$ mit $\mathfrak{u}_1\mathfrak{v}_1 \neq 0$. Da $\mathfrak{u}_1\mathfrak{u}_1 = 0$, $\mathfrak{v}_1\mathfrak{v}_1 = 0$, sind dann $\mathfrak{u}_1$ und $\mathfrak{v}_1$ linear unabhängig, und jeder Vektor $\mathfrak{x}$ aus $\mathfrak{R}$ besitzt eine eindeutige Zerlegung

$$\mathfrak{x} = (\alpha_1 \mathfrak{u}_1 + \beta_1 \mathfrak{v}_1) + \mathfrak{x}_1, \quad \mathfrak{x}_1 \text{ in } \langle \mathfrak{u}_1\ \mathfrak{v}_1 \rangle^*,$$

nämlich mit

$$\alpha_1 = \frac{\mathfrak{x}\mathfrak{v}_1}{\mathfrak{u}_1\mathfrak{v}_1}, \quad \beta_1 = \frac{\mathfrak{x}\mathfrak{u}_1}{\mathfrak{u}_1\mathfrak{v}_1}.$$

Somit ist

$$\mathfrak{R} = \langle \mathfrak{u}_1, \mathfrak{v}_1) + \langle \mathfrak{u}_1, \mathfrak{v}_1 \rangle^*.$$

Ist $\langle \mathfrak{u}_1, \mathfrak{v}_1 \rangle^*$ noch umfassender als $\mathfrak{R}^*$, so kann man auf $\langle \mathfrak{u}_1, \mathfrak{v}_1 \rangle^*$ statt $\mathfrak{R}$ dieselbe Schlußweise anwenden. So ergibt sich schließlich die Behauptung.

Zusatz. *Ist $\mathfrak{r}$ ein vollregulärer Teilraum von $\mathfrak{R}$, so ist*

$$\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^*.$$

Nach dem Verfahren des eben geführten Beweises kann man nämlich eine direkte Zerlegung

$$\mathfrak{r} = \sum_{i=1}^{r} \langle \mathfrak{u}_i, \mathfrak{v}_i \rangle \quad \text{mit} \quad \mathfrak{u}_i \mathfrak{v}_i \neq 0$$

zu einer direkten Zerlegung der obigen Form von $\mathfrak{R}$ ausbauen, und dabei erzeugen die hinzukommenden Teilräume gerade $\mathfrak{r}^*$.

Aus Satz 1 und der Bemerkung davor folgt unmittelbar:

Satz 2. *Jede quadratische Form ist in die Gestalt*

$$F = \sum_{i=1}^{n} (a_i x_i^2 + b_i x_i y_i + c_i y_i^2) + \sum_{j=1}^{n^*} d_j z_j^2 \quad \textit{mit} \quad b_i \neq 0$$

transformierbar. Dabei ist die Form

$$F^* = \sum_{j=1}^{n^*} d_j z_j^2$$

durch F bis auf äquivalente eindeutig bestimmt.

Der Zusammenhang der Normalform von Satz 2 mit der Zerlegung von Satz 1 wird durch die Formeln

$$|\mathfrak{u}_i|^2 = a_i, \quad \mathfrak{u}_i \mathfrak{v}_i = b_i, \quad |\mathfrak{v}_i|^2 = c_i; \quad |\mathfrak{w}_j|^2 = d_j$$

gegeben. Wir nennen eine Form F von dieser Gestalt *quasidiagonal.* Die Quasidiagonalformen übernehmen hier die Rolle der Diagonalformen in W. Q. Die invariante Teilform F^* nennen wir den *quasilinearen Teil* von F; er ist das Längenquadrat im invarianten Teilraum $\mathfrak{R}^*$ von $\mathfrak{R}$. Der vollreguläre Teil von F ist nicht invariant, wohl aber seine Variablenanzahl $2n$. Bei vollregulären Formen fehlt der quasilineare Teil, und die Variablenanzahl $2n$ ist gerade.

Die Vektoren vom Längenquadrat 0 aus $\mathfrak{R}^*$ bilden einen Teilraum $\mathfrak{R}_0^*$ von $\mathfrak{R}^*$. Ist $\mathfrak{R}_0^* = 0$, so nennen wir $\mathfrak{R}$ und die zugehörigen Formen *regulär.* Wählt man eine Basis von $\mathfrak{R}$ so, daß darin eine Basis von $\mathfrak{R}_0^*$ enthalten ist, so erkennt man, daß jede quadratische Form in eine reguläre Form von ev. kleinerer Variablenanzahl transformierbar ist. Wir können daher im folgenden durchweg ohne Einschränkung die zu betrachtenden Formen als regulär voraussetzen. In der Quasidiagonalform sind dann die $d_j \neq 0$ und bilden eine Basis des Moduls $\sum_{j=1}^{n^*} d_j k^2$. Dieser Modul ist ein durch Quadratbildung entstehendes isomorphes Bild von $\mathfrak{R}^* = \sum_{j=1}^{n^*} k\mathfrak{w}_j$, er besteht aus den durch die Form F^* darstellbaren Elementen aus k. Die Beschränkung auf reguläre Formen tritt an die Stelle der Beschränkung auf Formen von Null verschiedener Diskriminante in W. Q.

Die Nulldarstellungen durch F entsprechen den Vektoren $\neq 0$ vom Längenquadrat 0 aus $\mathfrak{R}$. Stellt eine reguläre Form die Null dar, so sind dabei nicht alle Variablen des vollregulären Teils Null.

Um zu weiteren Invarianten zu gelangen, betrachten wir wie in W. Q. das der Form

$$F = \sum_{1 \leq i \leq j \leq m} a_{ij} x_i x_j$$

invariant zugeordnete Cliffordsche System

$$C(F) = \sum_{e_1, \ldots, e_m = 0, 1} k u_1^{e_1} \cdots u_m^{e_m}$$

mit der Multiplikationstafel

$$u_i^2 = a_{ii}, \quad u_i u_j + u_j u_i = a_{ij} \qquad (i < j).$$

$C(F)$ ist eine Algebra vom Rang 2^m über k. Es ist

$$F = \left(\sum_{i=1}^{m} x_i u_i\right)^2.$$

Um zu einer direkten Zerlegung in normale einfache Algebren vom Rang 4 zu gelangen, mußte Witt in W. Q. der Form F anstelle von $C(F)$ die Algebra $C\left(F - \sum_{i=1}^{m} y_i^2\right)$ zuordnen. Das ist in unserem Falle nicht nötig. Vielmehr entspricht hier jeder quasidiagonalen Darstellung

$$F \simeq \sum_{i=1}^{n} f_i + F^*,$$

$$f_i = a_i x_i^2 + b_i x_i y_i + c_i y_i^2, \quad F^* = \sum_{j=1}^{n^*} d_j z_j^2$$

eine direkte Zerlegung von $C(F)$ selbst:

$$C(F) = \prod_{i=1}^{n} C(f_i) \cdot C(F^*).$$

Dabei ist

$$C(F^*) = \prod_{j=1}^{n^*} C(d_j z_j^2)$$

das Zentrum von $C(F)$.

$C(F^*)$ wird durch n^* Elemente w_j mit $w_j^2 = d_j$ erzeugt. Kommt in dem Modul $\sum_{j=1}^{n^*} d_j k^2$ der durch F^* darstellbaren Elemente aus k die 1 nicht vor, so ist $C(F^*)$ das direkte Produkt der n^* unabhängigen inseparablen quadratischen Körper $k(\sqrt{d_j})$, oder also, invariant beschrieben, der Körper $k(\sqrt{F^*})$ vom Grade 2^{n^*}, der durch Adjunktion der Quadratwurzeln aus den durch F^* darstellbaren Elementen aus k erzeugt wird. Dann ist also

$$C(F) = \prod_{i=1}^{n^*} C(f_i) \cdot k(\sqrt{F^*}).$$

Gibt es aber eine Darstellung $\sum_{j=1}^{n^*} d_j \gamma_j^2 = 1$, so entspricht ihr ein Element $w = 1 + \sum_{j=1}^{n^*} \gamma_j w_j$ aus $C(F^*)$ mit $w^2 = 0$. Dann ist $C(F^*)$ das direkte Produkt des Körpers $k(\sqrt{F^*})$, der jetzt nur den Grad 2^{n^*-1} hat, mit der durch w erzeugten Algebra $k + kw$ vom Rang 2. Dabei erzeugt w das Radikal $C(F^*)w = k(\sqrt{F^*})w$ von $C(F^*)$, und da die $C(f_i)$, wie wir gleich sehen werden, normale einfache Algebren sind, auch das Radikal $C(F)w = \prod_{i=1}^{n} C(f_i) \cdot k(\sqrt{F^*})w$ von $C(F)$. Läßt man den Fakter $k + kw$ aus dem direkten Produkt $C(F)$ fort, so entspricht das also der Reduktion der Algebra $C(F)$ auf die Restklassenalgebra nach ihrem Radikal. Da dies ein invarianter Prozeß ist, ist in dem betrachteten Falle auch die so entstehende Algebra

$$C_0(F) = \prod_{i=1}^{n} C(f_i) \cdot k(\sqrt{F^*})$$

eine Invariante der Form F.

Hierdurch wird man auf die Betrachtung der Invariante $C(F)$ für vollreguläre

$$F \simeq \sum_{i=1}^{n} f_i$$

zurückgeführt. Dann ist

$$C(F) = \prod_{i=1}^{n} C(f_i).$$

Für eine vollreguläre binäre Form

$$f = ax^2 + bxy + cy^2$$

ist $C(f)$ eine normale einfache Algebra vom Rang 4, erzeugt durch zwei Elemente u, v mit den Relationen

$$u^2 = a, \quad uv + vu = b, \quad v^2 = c.$$

Um $C(f)$ als verschränktes Produkt darzustellen, setze man ohne Einschränkung $a \neq 0$ voraus, was ja durch eine der beiden Transformationen $x' = y$, $y' = x$ oder $x' = x$, $y' = x + y$ erreichbar ist. Dann kann man als Erzeugende auch

$$\omega = \frac{uv}{b}, \quad \theta = u$$

nehmen, mit den Relationen

$$\wp\omega = \frac{ac}{b^2}, \quad \theta\omega\theta^{-1} = \omega + 1, \quad \theta^2 = a.$$

Dabei ist zur Abkürzung $\wp\omega = \omega^2 + \omega$ gesetzt; wir schreiben ferner umgekehrt $\omega = \frac{ac}{b^2}/\wp$ für eine Wurzel von $\wp\omega = \frac{ac}{b^2}$. Hiernach ist $C(f)$ ein verschränktes Produkt mit dem separablen Körper $k\left(\frac{ac}{b^2}/\wp\right)$ als Zerfällungskörper. Die für diesen Zerfällungskörper charakteristische additive Klasse $\frac{ac}{b^2} + \wp\alpha$, wo α die Elemente aus k durchläuft, bezeichnen wir mit $\Delta(f)$ und schreiben auch kurz

$$\Delta(f) \equiv \frac{ac}{b^2} \quad \text{mod. } \wp k.$$

Ferner setzen wir zunächst formal

$$\Delta(F) \equiv \sum_{i=1}^{n} \Delta(f_i) \equiv \sum_{i=1}^{n} \frac{a_i c_i}{b_i^2} \quad \text{mod. } \wp k.$$

Wir werden beweisen, daß $\Delta(F)$ eine Invariante von F ist. Schließlich schreiben wir

$$N(x + y\omega) = (x + y\omega)(x + y(\omega + 1)) = x^2 + xy + \frac{ac}{b^2} y^2.$$

Es ist das die Norm im Zerfällungskörper $k\left(\frac{ac}{b^2}/\wp\right)$ von $C(f)$, wobei dieser aber, auch falls $\frac{ac}{b^2}/\wp$ in k liegt, als die Algebra $k + k\omega$, also dann als die direkte Summe zweier Exemplare von k aufgefaßt wird.

Satz 3. *Zwei vollreguläre binäre Formen*

$$F = ax^2 + bxy + cy^2, \quad F' = a'x'^2 + b'x'y' + c'y'^2$$

sind dann und nur dann äquivalent, wenn

$$C(F) \simeq C(F')$$

und

$$\Delta(F) \equiv \Delta(F') \quad \text{mod. } \wp k$$

ist.

Beweis. Man kann ohne Einschränkung $a \neq 0$, $a' \neq 0$ voraussetzen. Dann hat man