Ruprecht-Karls-Universität Heidelberg
Fakultät für Mathematik und Informatik
Mathematisches Institut
Sommersemester 2007

Seminar: Quadratische Formen über den rationalen Zahlen

# Die Sätze von Tsen und Chevalley-Warning

Leitung: Prof. Dr. Kay Wingberg

Nada Rožkova
nada_rozkova@yahoo.de

Rudolf Schenk
r.schenk@stud.uni-heidelberg.de

Heidelberg, 12. Juli 2007

# Inhaltsverzeichnis

**1 Der Satz von Chevalley-Warning für endliche Körper** **2**
1.1 Definitionen . . . 2
1.2 Wiederholung . . . 3
1.3 Vorbereitung . . . 4
1.4 Chevalley-Warning . . . 4
1.5 Ausblick . . . 5

**2 Der Satz von Tsen** **7**
2.1 Definitionen . . . 7
2.2 Tsen . . . 7
2.3 Tensorprodukt und Skalarerweiterung . . . 7
2.4 Galoissche Erweiterungen . . . 10

**Literatur** **12**

# Motivation

Über dem Körper der reellen Zahlen gibt es viele homogene Gleichungen, so wie

$$x_1^2 + x_2^2 + \ldots + x_n^2 = 0$$

welche nur die triviale Lösung $(0,0,\ldots,0)$ haben, hierbei kann $n$ jede positive ganze Zahl sein. Andererseits, gibt es andere Körper, für welche folgender bemerkenswerter Typ von Aussage gilt: Falls $f$ eine Form (homogenes Polynom) in $n$ Variablen, und $n$ hinreichend groß ist, verglichen mit dem Grad von $f$, dann hat $f$ eine nichttriviale Nullstelle.

Der erste Satz mit einer Aussage dieser Form wurde von Chiungtze C. Tsen bewiesen im Jahr 1933.

**(0.1) Satz:** *$K$ ein Funktionenkörper in einer Variablen über einem algebraisch abgeschlossenen Körper von Konstanten ist, dann gibt es keine zentralen Divisionsalgebren über $K$ (außer, natürlich, $K$ selbst).*

Eine Analyse seines Beweises zeigte, dass er tatsächlich ein stärkeres Resultat bewiesen hat:

**(0.2) Satz:** *Sei $f$ eine Form mit Koeffizienten in $K$ vom Grad $d$ in $n$ Variablen, und $n > d$, dann hat $f$ eine nicht-triviale Nullstelle in $K$.*

Wir werden zunächst (0.2) für endliche Körper $K$ beweisen und danach zeigen, wie (0.1) aus (0.2) folgt.

# 1 Der Satz von Chevalley-Warning für endliche Körper

## 1.1 Definitionen

**(1.1) Definition:** Sei $K$ ein Ring, $d < \infty$. Eine Abbildung $f : K^n \to K$ heißt (homogenes) Polynom vom Grad $d$ in $n$ Variablen, falls sie sich darstellen lässt als $K$-Linearkombination von Monomen des selben Gesamtgrades $d$: $f(x_1,\ldots,x_n) = \sum_{i=1}^{m} a_i (x_1^{d_{i_1}} \cdot \ldots \cdot x_n^{d_{i_n}})$, mit $d = \sum_{j=1}^{n} d_{i_j}, a_i \in K$ für alle $i \in \{1,\ldots,m\}, m < \infty$. Man nennt $f$ dann auch eine (algebraische) Form vom Grad $d$ in $n$ Variablen über $K$.

**(1.2) Definition:** Sei $K$ ein Körper. $K$ heißt $C_1$-Körper, falls jede Form $f$ vom Grad $d$ in $n$ Variablen mit $n > d$ über $K$ eine nicht-triviale Nullstelle hat.

und allgemeiner:

**(1.3) Definition:** Sei $K$ ein Körper und $i \geq 0$ eine ganze Zahl. $K$ heißt $C_i$-Körper, falls jede Form $f$ vom Grad $d$ in $n$ Variablen mit $n > d^i$ über $K$ eine nicht-triviale Nullstelle hat.

In diesem Sinne bedeutet $C_0$ nichts anderes als, dass ein Körper algebraisch abgeschlossen ist. $C_1$-Körper nennt man auch quasi-algebraisch abgeschlossen.

**(1.4) Definition:** Ein Körper $K$ heißt algebraisch abgeschlossen, wenn jedes Polynom $f \in K[X]$ von positivem Grad eine Nullstelle in $K$ hat.

## 1.2 Wiederholung

Sei $k$ ein endlicher Körper mit $q$ Elementen und $p$ die Charakteristik von $k$, $\mathrm{char}(k) = p$. Sei $k^* = k \backslash \{0\}$ die multiplikative Gruppe der Elemente von $k$ ungleich 0.

**(1.5) Wiederholung:** Vortrag 1, Satz 1. *Die Charakteristik p ist eine Primzahl.*

*Beweis.* $p = \mathrm{char}(k)$, das heißt, $p$ ist die kleinste natürliche Zahl mit $p \cdot 1 = 0$. $\lightning$-Annahme: Sei $p$ nicht prim, dann existieren $s, t \in \mathbb{N}$ mit $p = s \cdot t$, $s, t < p$. Dann gilt aber $0 = p \cdot 1 = (s \cdot t) \cdot 1 = (s \cdot 1)(t \cdot 1) \Rightarrow s \cdot 1 = 0$ oder $t \cdot 1 = 0$ $\lightning$, denn $s, t < p$, aber $p$ ist minimal mit der Eigenschaft $p \cdot 1 = 0$. *q.e.d.*

**(1.6) Wiederholung:** *Die Elemente* $0, 1, \ldots, (p-1) \cdot 1 \in k$ *bilden den kleinsten Teilkörper von k, den Primkörper.*

*Beweis.* Jeder Körper enthält 0, 1 und mit 1 auch alle additiven Vielfachen. Das heißt jeder Teilkörper von $k$ umfasst $\mathbb{F}_p \cong \{0, 1, \ldots, (p-1) \cdot 1\}$, da $\mathbb{F}_p$ selbst schon ein Körper ist, was man leicht durch die Isomorphie zu $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ einsieht, ist $\mathbb{F}_p$ schon der Primkörper, denn diesen erhält man durch Schnitt aller Teilkörper von $k$. *q.e.d.*

**(1.7) Wiederholung:** Vortrag 1, Satz 1. *Die Ordung von k ist eine Primzahlpotenz.*

*Beweis.* Der Primkörper $\mathbb{F}_p$ ist kanonisch isomorph zu dem Körper $\mathbb{Z}/p\mathbb{Z}$ der ganzen Zahlen modulo $p$. $k$ ist also eine Körpererweiterung von $\mathbb{F}_p$. Diese kann man als Vektorraum über $\mathbb{F}_p$ auffassen. Da $|k| < \infty$ ist $[k : \mathbb{F}_p] = \dim_{\mathbb{F}_p} k < \infty$. Sei $\nu \in \mathbb{N}$ die Dimension von $k$ als Vektorraum über $\mathbb{F}_p$, dann gilt: $q = |k| = p^\nu$, denn: $k \cong \mathbb{F}_p^\nu$; $q = |k| = |\mathbb{F}_p^\nu| = |\mathbb{F}_p|^\nu = p^\nu$. *q.e.d.*

Vergleiche: $\mathbb{R} \leq \mathbb{C} = \mathbb{R}(i) = \{x \cdot 1 + y \cdot i \mid x, y \in \mathbb{R}\}, \dim_{\mathbb{R}}(\mathbb{C}) = 2$.

**(1.8) Wiederholung:** Vortrag 1, Satz 2. $k^*$ *ist zyklisch von Ordnung* $q - 1$.

*Beweis.* $\lightning$-Annahme: $k^*$ ist nicht zyklisch. Die elementare Theorie der abelschen Gruppen sagt, dass das kleinste gemeinsame Vielfache $m$ aller Ordnungen der Elemente von $k^*$ ein echter Teiler von $q-1$ sein muss. Denn: Sei $k^* = \{a_1, \ldots, a_{q-1}\}$. Die von $a_1, \ldots, a_{q-1}$ erzeugte Untergruppe $\langle a_1, \ldots, a_{q-1} \rangle = k^*$ enthält ein Element $n$ der Ordnung $m := \mathrm{kgV}(\mathrm{ord}(a_1), \ldots, \mathrm{ord}(a_{q-1}))$. Für $\langle a_1, a_2 \rangle$ ist es in [Lorenz (1987)] bewiesen, der Rest geht induktiv, beginnend mit $\langle a_1, a_2 \rangle$, findet man ein Element $n_1$ mit $\mathrm{ord}(n_1) = \mathrm{kgV}(\mathrm{ord}(a_1), \mathrm{ord}(a_2))$. In $\langle n_1, a_3 \rangle$ gibt es ein Element $n_2$ mit $\mathrm{ord}(n_2) = \mathrm{kgV}(\mathrm{ord}(n_1), \mathrm{ord}(a_3)) = \mathrm{kgV}(\mathrm{ord}(a_1), \mathrm{ord}(a_2), \mathrm{ord}(a_3))$. kgV ist assoziativ. Die Ordnung der von $n$ erzeugten Untergruppe $\langle n \rangle$, teilt nach dem Satz von Lagrange die Gruppenordnung. Also $m \mid q - 1$. Nach Voraussetzung ist $k^*$

nicht zyklisch, also $q-1 = |k^*| > |\langle n\rangle| = m \Rightarrow (k^* : \langle n\rangle) \geq 2$. Also ist $m$ ein echter Teiler von $q-1$, denn $q-1 = (k^* : \langle n\rangle) \cdot m$. Aber dann hätte die Gleichung $X^m = 1 \Leftrightarrow X^m - 1 = 0$ mehr als $m$ verschieden Lösungen in $k$, nämlich alle Elemente von $k^*$ und das sind $q-1$ Stück. Denn für alle $x \in k^*$ gilt: $x^m - 1 = x^{\mathrm{ord}(x)\cdot \ell_x} - 1 = (x^{\mathrm{ord}(x)})^{\ell_x} - 1 = 1^{\ell_x} - 1 = 1 - 1 = 0$. Da $m$ ein echter Teiler von $q-1$ ist, ist also $m < q-1$.↯ Das kann nicht sein. Ein Polynom hat in jedem Körper maximal soviele Nullstellen wie sein Grad. Das Polynom $f = X^m - 1$ hat also über jedem Körper maximal $\mathrm{grad}(f) = m$ Nullstellen. Denn es ist maximal in $m$ verschiedene Linearfaktoren zerlegbar, deren Produkt ist genau dann Null, wenn mindestens ein Faktor Null ist, das kann aufgrund der Nullteilerfreiheit maximal $m$ mal passieren. Also ist $k^*$ doch zyklisch. *q.e.d.*

## 1.3 Vorbereitung

**(1.9) Lemma:** *Sei $\Omega$ ein Körper und sei $\varphi : k^* \to \Omega^*$ ein nicht-trivialer Homomorphismus der multiplikativen Gruppe von $k$ auf die multiplikative Gruppe von $\Omega$. Dann gilt:*

$$\sum_{x \in k^*} \varphi(x) = 0$$

*Beweis.* Nach Annahme ist $\varphi(y) \neq 1$ für ein $y \in k^*$, ansonsten wäre $\varphi$ trivial. Dann ist $\sum_{x\in k^*} \varphi(x) = \sum_{x\in k^*} \varphi(yx)$. Die Translation $\tau_y : k^* \to k^*; x \mapsto yx$ ist injektiv: $\tau_y(a) = \tau_y(b) \Rightarrow ya = yb \Rightarrow a = b$, da $k^*$ endlich, ist $\tau_y$ auch surjektiv. $\sum_{x\in k^*} \varphi(yx) = \varphi(y) \sum_{x\in k^*} \varphi(x)$. Dies kann aber nur für $\sum_{x\in k^*} \varphi(x) = 0$ gelten, da nach Voraussetzung $\varphi(y) \neq 1$. *q.e.d.*

**(1.10) Lemma:** Vortrag 1, Lemma 3. *Sei $m \in \mathbb{N}$, $m > 0$, so gilt:*

$$\sum_{x\in k} x^m = \begin{cases} -1 & \text{für } (q-1) \mid m \\ 0 & \text{für } (q-1) \nmid m \end{cases}$$

*Beweis.* Sei $\varphi : k^* \to k^*; x \mapsto x^m$. $\varphi$ ist ein (Gruppen-)Homomorphismus, da $\varphi(xy) = (xy)^m = x^m y^m = \varphi(x)\varphi(y)$, benötigt Kommutativität, und $\varphi(1) = 1^m = 1$. Da $k^*$ zyklisch von Ordnung $q-1$ ist, ist $\varphi$ nur trivial, das heißt: $\varphi(x) = 1$ für alle $x \in k^*$, falls $(q-1) \mid m$. In diesem Fall ist $\sum_{x\in k} x^m = 0 + (q-1)\cdot 1 \equiv -1 \mod p$. Denn: $(q-1) \mid m \Rightarrow m = \ell(q-1) \Rightarrow \varphi(x) = x^{\ell(q-1)} = (x^{q-1})^\ell = 1^\ell = 1$ für alle $x \in k^*$. Es folgt: $x^m = \begin{cases} 1 & ; x \in k^* \\ 0 & ; x = 0. \end{cases}$ Beachte $x^{\mathrm{ord}(k^*)} = 1$ für alle $x \in k^*$, Satz von Lagrange: Die Ordnung jedes Elements teilt die Gruppenordnung. Die letzte Gleicheit ergibt sich aus: $p \mid q \Rightarrow (q-1)\cdot 1 = q\cdot 1 - 1 = (\ell \cdot p)\cdot 1 - 1 \Rightarrow (q-1) \equiv -1 \mod p$. Falls $(q-1) \nmid m$, so folgt die Behauptung aus Lemma (1.9). *q.e.d.*

Unser Ziel ist zu zeigen, dass $k$ ein $C_1$-Körper ist, ohne Mehrarbeit können wir sogar ein stärkeres Resultat beweisen.

## 1.4 Chevalley-Warning

**(1.11) Satz:** Vortrag 1, Theorem von Chevalley-Warning. *Sei $f$ ein Polynom in $n$ Variablen mit Koeffizienten in einem endlichen Körper $k$ und sei $d$ sein Grad. Sei $N(f)$ die Anzahl der verschiedenen Nullstellen von $f$ in $k$. Falls $n > d$, so gilt:*

$$N(f) \equiv 0 \mod p$$

*Insbesondere, falls $f$ keinen konstanten Term hat, so hat $f$ eine nicht-triviale Nullstelle in $k$. Das bedeutet: $k$ ist $C_1$.*

*Beweis.* Sei $N := \{x \in k^n | f(x) = 0\}$. Für jedes $n$-Tupel $x \in k^n$ haben wir:

$$\mathbb{1}_N(x) := 1 - f(x)^{q-1} = \begin{cases} 1 & \text{falls } f(x) = 0 \\ 0 & \text{sonst} \end{cases}$$

Falls $f(x) = 0 \Rightarrow 1 - f(x)^{(q-1)} = 1 - 0 = 1$, sonst $f(x) \in k^* \Rightarrow f(x)^{(q-1)} = 1$ Folgerung aus Lagrange $\Rightarrow 1 - f(x)^{(q-1)} = 1 - 1 = 0$, $\mathbb{1}_N$ ist eine Indikatorfunktion für die Nullstellenmenge $N$ von $f$: $\mathbb{1}_N(x) = \begin{cases} 1 & ; x \in N \Leftrightarrow f(x) = 0 \\ 0 & ; x \notin N \Leftrightarrow f(x) \neq 0 \end{cases}$

Summation über alle $x \in k^n$ ergibt:

$$\overline{N(f)} = \sum_{x \in k^n} \mathbb{1}_N(x) = \sum_{x \in k^n} (1 - f(x)^{q-1}) = -\sum_{x \in k^n} f(x)^{q-1}$$

wobei $\overline{N(f)}$ die Restklasse modulo $p$ von $N(f)$ ist, betrachtet als ein Element von $k$. Denn:$\sum_{x \in k^n} 1 - f(x)^{q-1} = \sum_{x \in k^n} 1 - \sum_{x \in k^n} f(x)^{q-1} = |k^n| 1 - \sum_{x \in k^n} f(x)^{q-1} = q^n \cdot 1 - \sum_{x \in k^n} f(x)^{q-1} = -\sum_{x \in k^n} f(x)^{q-1}$, da $p \mid q$. Daher müssen wir zeigen, dass für jedes Polynom mit $d < n$ gilt: $\sum_{x \in k^n} f(x)^{q-1} = 0$. Nun ist $f^{q-1}$, da es vom Grad $d(q-1)$ ist eine $k$-linear Kombination von Monomen vom Grad höchstens $d(q-1)$, dies ist ein einfaches Indiktionsargument. Falls $X^\mu = X_1^{\mu_1} \cdot X_2^{\mu_2} \cdot \ldots \cdot X_n^{\mu_n}$ so ein Monom ist, berechnen wir mit Hilfe des verallgemeinerten Distributivgesetzes: Eine Summe wird mit einer Summe multipliziert, indem man jeden Summanden der einen Summe mit allen Summanden der anderen Summe - unter Beachtung der Vorzeichen - multipliziert und die entstehenden Produkte addiert.

$$\sum_{x \in k^n} x^\mu = \sum_{x \in k^n} x_1^{\mu_1} \cdot \ldots \cdot x_n^{\mu_n} = \prod_{i=1}^{n} \sum_{x_i \in k} x_i^{\mu_i}$$

Da $d < n$, ist mindestens ein $\mu_i$ nicht teilbar durch $(q-1)$,nach Voraussetzung gilt $\sum_{i=1}^n \mu_i \leq d(q-1)$ mit $n > d$ folgt die Existenz eines $\mu_i < (q-1)$, denn ansonsten $\sum_{i=1}^n \mu_i \geq n(q-1) \geq d(q-1)$. Falls $\mu_i \neq 0$ folgt die Behauptung durch Lemma (1.10), da dann der $i$-te Term des obigen Produkts gleich 0 sein wird, falls $\mu_i = 0 \Rightarrow \sum_{x \in k} x^{\mu_i} = q \cdot 1 = 0$, da $p \mid q$. Die Folgerung ist leicht einzusehen: Falls $f$ keinen konstanten Term hat, ist $f(0, \ldots, 0) = 0$, gibt es keine nicht-triviale Nullstelle, so ist $1 = N(f) \equiv 0 \mod p$. Das ist aber in jedem Körper ein Widerspruch. *q.e.d.*

## 1.5 Ausblick

**(1.12) Bemerkung:** Die Bedingung $n > d$ ist scharf: Betrachtet man $k = \mathbb{F}_2$ und $f \in k[X_1, X_2]$ mit $f(X_1, X_2) = X_1^2 + X_1 X_2 + X_2^2$. Dann gilt:

- $f(0,0) = 0$
- $f(0,1) = f(1,0) = 1$
- $f(1,1) = 1$

$f$ hat also keine nicht-triviale Nullstelle.

**(1.13) Bemerkung:** Man kann mehr über die Anzahl der Nullen $N(f)$ aussagen. Ax zeigte, dass $N(f)$ durch $q$ nicht nur durch $p$ teilbar ist. Der Beweis benutzt Gauss-Summen. Die genaue Behauptung ist, dass falls $b$ die größte ganze Zahl echt kleiner als $\frac{n}{d}$ ist, dann teilt $q^b$ $N(f)$. Ax gibt auch ein Beispiel eines Polynoms $f$, so dass die höchste Potenz von $p$, die $N(f)$ teilt gerade $q^b$ ist. Somit ist sein Teilbarkeitsergebnis das Bestmögliche. Andererseits hat Warning gezeigt, dass falls $d < n$ und $f$ mindestens eine Null in $k$ hat, dann gilt, $N(f) \geq q^{n-d}$. Der Beweis benutzt nur Mittel der Linearen Algebra.

Allgemeine Sätze, die die Anzahl der Lösungen von Gleichungen auf endlichen Körpern abschätzen werden in der Arbeit von Lang und Weil gefunden. Die Beweise diese Arbeit fußen auf tieferen Resultaten der algebraischen Geometrie. Diese Fragen sind mit der Theorie der Zeta-Funktionen von algebraischen "Mannigfaltigkeiten"über endlichen Körpern verwandt.

# 2 Der Satz von Tsen

## 2.1 Definitionen

**(2.1) Definition:** Eine Algebra $A$ über einem Körper $K$ ist ein $K$-Vektorraum mit einer $K$-bilinearen Verknüpfung: $A \times A \to A$, Multiplikation genannt, die durch $x \cdot y$ oder $xy$ symbolisiert wird.

**(2.2) Definition:** Das Zentrum einer assoziativen Algebra $A$ ist die kommutative Unteralgebra

$$Z(A) := \{z \in A \mid za = az \text{ für alle } a \in A\}$$

**(2.3) Definition:** Eine endlich-dimensionale Algebra $D$ (über einem Körper $K$) mit 1, in der jedes von Null verschiedene Element ein Inverses hat und deren Zentrum genau $K$ ist, heißt zentrale (oder zentraleinfache) Divisionsalgebra über $K$.

## 2.2 Tsen

**(2.4) Satz:** Tsen. *Sei $K$ ein Funktionenkörper in einer Variablen über einem algebraisch abgeschlossenen Körper von Konstanten, dann gibt es keine zentralen Divisionsalgebren über $K$ (außer natürlich $K$ selbst.)*

Zunächst formulieren wir den Satz von Tsen in anderer Art und Weise: er zerfällt dann in zwei Teile:

**(2.5) Satz:** *Sei $K$ ein Funktionenkörper in einer Variablen über einem algebraisch abgeschlossenen Körper von Konstanten, dann ist $K$ ein $C_1$-Körper.*

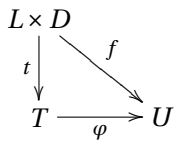
*Beweis.* Dieser Satz wird in größerer Allgemeinheit in Vortrag 12 bewiesen *q.e.d.*

**(2.6) Satz:** *Sei $K$ ein $C_1$-Körper, dann hat $K$ keine zentralen Divisionsalgebren.*

*Beweis.* Sei $D$ eine zentrale Divisionsalgebra (2.3) über $K$. Insbesondere ist also $D$ ein $K$-Vektorraum. Zu einem gegebenen Oberkörper $L$ über $K$, den man auch als Vektorraum über $K$ ansehen kann, betrachten folgende Konstruktion:

## 2.3 Tensorprodukt und Skalarerweiterung

**(2.7) Satz:** *Seien $L$ und $D$ Vektorräume über $K$. Dann gibt es einen bis auf Isomorphie eindeutig bestimmten $K$-Vektorraum $T$ zusammen mit einer bilinearen Abbildung $t : L \times D \to T$, die folgende universelle Abbildungseigenschaft haben: Zu jedem $K$-Vektorraum $U$ zusammen mit einer bilinearen Abbildung $f : L \times D \to U$ gibt es genau eine lineare Abbildung $\varphi : T \to U$ mit $f = \varphi \circ t$. Das kann man durch ein kommutatives Diagramm illustrieren:*




*Beweis.* Lorenz (1987)§ 3 *q.e.d.*

**(2.8) Bezeichnung:** Man nennt $T$ das Tensorprodukt von $L$ und $D$ über $K$ und schreibt $T =: L \otimes_K D$. Die Elemente von $L \otimes_K D$ heißen Tensoren.

**(2.9) Satz:** *Falls* $\dim_K L, \dim_K D < \infty$, *so ist* $\dim_K (L \otimes_K D) = \dim_K L \cdot \dim_K D$.

*Beweis.* Lorenz (1987)§ 3 *q.e.d.*

Im Folgenden sei $\dim_K L, \dim_K D < \infty$ vorausgesetzt.

**(2.10) Satz:** *Seien $\mathscr{B}_L = (\ell_i)_{i\in I}$ , $\mathscr{B}_D = (d_j)_{j\in J}$ Basen der Vektorräume $L$ beziehungsweise $D$. Dann ist $\mathscr{B}_L \otimes \mathscr{B}_D := (\ell_i \otimes d_j)_{(i,j)\in I\times J}$ eine Basis von $L \otimes_K D$ und ein Tensor $u \in L \otimes_K D$ ist stets von der Gestalt $u = \sum_{(i,j)\in I\times J} u_{i,j} \cdot \ell_i \otimes d_j$ , mit $u_{i,j} \in K$ für alle $(i,j) \in I \times J$.*

*Beweis.* Lorenz (1987)§ 3 *q.e.d.*

**(2.11) Bezeichnung:** Die Familie $(u_{i,j})_{(i,j)\in I\times J}$ wird als die Koordinatenfamilie von $u$ bezüglich der Basis $\mathscr{B}_L \otimes \mathscr{B}_D$ bezeichnet.

**(2.12) Satz:** Rechenregeln für Tensoren. *Für $\ell, \ell' \in L$, $d, d' \in D$, $k \in K$ gilt:*

1. $(\ell + \ell') \otimes d = \ell \otimes d + \ell' \otimes d$
2. $\ell \otimes (d + d') = \ell \otimes d + \ell \otimes d'$
3. $(k \cdot \ell) \otimes d = k \cdot (\ell \otimes d) = \ell \otimes (k \cdot d)$

*Beweis.* Lorenz (1987)§ 3 *q.e.d.*

Für jedes $\lambda \in L$ induziert die $K$-bilineare Abbildung:

$$f_\lambda : L \times D \to L \otimes_K D$$
$$\ell \times d \mapsto (\lambda \cdot \ell) \otimes d$$

eine eindeutig bestimmte lineare Abbildung:

$$\varphi_\lambda (=: \lambda\cdot) : L \otimes_K D \to L \otimes_K D$$
$$\ell \otimes d \mapsto (\lambda \cdot \ell) \otimes d$$

**(2.13) Satz:** *$L \otimes_K D$ ist ein $L$-Vektorraum, der seine Addition durch die Struktur als $K$-Vektorraum erhält und auf dem zusätzlich eine Multiplikation mit einem Skalar aus $L$ erklärt ist durch: $\lambda \cdot v := \varphi_\lambda(v)$ für $\lambda \in L$ und $v \in L \otimes_K D$.*

*Beweis.* $L \otimes_K D$ ist ein $K$-Vektorraum. Das heißt $(L \otimes_K D, +)$ ist eine abelsche Gruppe, und $1_L \cdot v = 1_K \cdot v = v$ für alle $v \in L \otimes_K W$, da $1_K = 1_L$. Zu prüfen bleibt die Assoziativität und die Distributivgesetze, diese folgen aus der Linearität von $\varphi_\lambda$ was man durch einfaches Nachrechnen verifizieren kann.
Assoziativität:

Seien $a, b \in L$, $u \in L \otimes_K D$

$$
\begin{aligned}
a \cdot (b \cdot u) &= a \cdot \left( \varphi_b \left( \sum_{i \in I, j \in J} u_{i,j} \cdot \ell_i \otimes d_j \right) \right) && u_{i,j} \in K, \ell_i \in L, d_j \in D \text{ geeignet} \\
&= \varphi_a \left( \sum_{(i,j) \in I \times J} \varphi_b \left( \left( u_{i,j} \cdot \ell_i \right) \otimes d_j \right) \right) && \varphi_b \text{ ist linear} \\
&= \sum_{(i,j) \in I \times J} \varphi_a \left( \left( b \cdot u_{i,j} \cdot \ell_i \right) \otimes d_j \right) && \varphi_a \text{ ist linear, Definition von } \varphi_b \\
&= \sum_{(i,j) \in I \times J} \left( a \cdot \left( b \cdot u_{i,j} \cdot \ell_i \right) \right) \otimes d_j && \text{Definition von } \varphi_a \\
&= \sum_{(i,j) \in I \times J} \left( (a \cdot b) \cdot \left( u_{i,j} \cdot \ell_i \right) \right) \otimes d_j && \text{Assoziativität in } L \\
&= \sum_{(i,j) \in I \times J} \varphi_{(a \cdot b)} \left( \left( u_{i,j} \cdot \ell_i \right) \otimes d_j \right) && \text{Definition von } \varphi_{(a \cdot b)} \\
&= \varphi_{(a \cdot b)} \left( \sum_{(i,j) \in I \times J} \left( u_{i,j} \cdot \ell_i \right) \otimes d_j \right) && \varphi_{(a \cdot b)} \text{ ist linear} \\
&= (a \cdot b) \cdot u
\end{aligned}
$$

Distributivgesetze
Seien $a, b \in L$, $u \in L \otimes_K W$

$$
\begin{aligned}
(a+b) \cdot u &= \varphi_{(a+b)} \left( \sum_{(i,j) \in I \times J} u_{i,j} \cdot \ell_i \otimes d_j \right) && \text{mit } u_{i,j} \in K, \ell_i \in L, d_j \in W \text{ geeignet} \\
&= \sum_{(i,j) \in I \times J} \varphi_{(a+b)} \left( u_{i,j} \cdot \ell_i \otimes d_j \right) && \text{Linearität} \\
&= \sum_{(i,j) \in I \times J} \left( (a+b)\, u_{i,j} \cdot \ell_i \right) \otimes d_j && \text{Definition, RR für Tensor} \\
&= \sum_{(i,j) \in I \times J} \left( a u_{i,j} \cdot \ell_i + b u_{i,j} \cdot \ell_i \right) \otimes d_j && \text{Assoziativität in } L \\
&= \sum_{(i,j) \in I \times J} a u_{i,j} \cdot \ell_i \otimes d_j + b u_{i,j} \cdot \ell_i \otimes d_j && \text{RR für Tensor} \\
&= \sum_{(i,j) \in I \times J} a u_{i,j} \cdot \ell_i \otimes d_j + \sum_{(i,j) \in I \times J} b u_{i,j} \cdot \ell_i \otimes d_j \\
&= \varphi_a \left( \sum_{(i,j) \in I \times J} u_{i,j} \cdot \ell_i \otimes d_j \right) + \varphi_b \left( \sum_{(i,j) \in I \times J} u_{i,j} \cdot \ell_i \otimes d_j \right) && \text{Definition} \\
&= a \cdot u + b \cdot u
\end{aligned}
$$

Seien $a \in L$, $u, v \in L \otimes_K W$

$$
\begin{aligned}
a \cdot (u+v) &= \varphi_a (u+v) \\
&= \varphi_a (u) + \varphi_a (v) && \text{Linearität} \\
&= a \cdot u + b \cdot v
\end{aligned}
$$

*q.e.d.*

**(2.14) Bezeichnung:** Man nennt $D_L := L \otimes_K D$ den aus $D$ durch Skalarerweiterung mit $L$ entstandenen Vektorraum.

**(2.15) Satz:** $\dim_K D = \dim_L D_L$

*Beweis.* Einerseits gilt:
$\dim_K D_L = \dim_K L \cdot \dim_L D_L$ und andererseits gilt:
$\dim_K D_L = \dim_K L \otimes_K D = \dim_K L \cdot \dim_K D$. Es folgt:
$\dim_K L \cdot \dim_L D_L = \dim_K L \cdot \dim_K D$. Durch kürzen folgt die Behauptung. *q.e.d.*

**(2.16) Satz:** *Jede zentraleinfache $K$-Algebra $D$ besitzt Zerfällungskörper $L/K$. Dabei heißt $L/K$ ein Zerfällungskörper von $D$, wenn es einen Isomorphismus zwischen $L \otimes_K D$ und $M_{n\times n}(L)$ gibt, wobei mit $n^2 = [D:K]$ und $n = [L/K]$.*

*Beweis.* Lorenz (1990), § 29, Satz 17 *q.e.d.*

Wählt man eine lineare Basis von $D$ über $K$ fest, sieht man, dass jedes Element $d \in D$ festgelegt wird von $n^2$ Einträgen in $L$. Da $D$ auf natürliche Weise in $D_L$ eingebettet ist (identifiziere $d \in D$ mit $1 \otimes d \in D_L$), können wir, indem wir einen Isomorphismus $\psi$ von $D_L$ mit $M_{n\times n}(L)$ wählen, $d$ als $n \times n$-Matrix mit Einträgen in $L$ ansehen. Zunächst beschäftigen wir uns daher etwas näher mit den Körpererweiterungen von $K$.

## 2.4 Galoissche Erweiterungen

**(2.17) Definition:** *algebraisch.* Eine Erweiterung $L$ ist eine algebraische Erweiterung über $K$, wenn jedes Element aus $L$ algebraisch über $K$ ist.

**(2.18) Definition:** *algebraisch.* Ein Element $\alpha \in L$ heißt algebraisch über $K$, falls es ein Polynom $f \in K[X]$ gibt, mit $f(\alpha) = 0$.

**(2.19) Definition:** *Automorpismengruppe.* Die Menge der Automorphismen von $L$, zusammen mit der Verkettung von Abbildungen als Verknüpfung wird die Automorphismengruppe von $L/K$ genannt und mit $G(L/K) = G(L)$ bezeichnet.

**(2.20) Definition:** *Fixkörper.* Sei $L$ ein Körper, und $G(L)$ die Automorphismengruppe von $L$. Die Menge

$$L^{G(L)} := \{\ell \in L | \forall \sigma \in G(L) : \sigma(\ell) = \ell\}$$

wird der Fixkörper von $G(L)$ genannt.

**(2.21) Definition:** *galoisch.* Eine algebraische Körpererweiterung $L$ über $K$ heißt galoisch, wenn gilt

$$K = L^{G(L/K)}.$$

Die Gruppe $G(L/K)$ heißt dann die Galoisgruppe von $L/K$ und wird mit $\mathrm{Gal}(L/K)$ bezeichnet.

**(2.22) Satz:** *Jede zentraleinfache $K$-Algebra $D$ besitzt Zerfällungskörper $L/K$, welche über $K$ galoissch sind.*

*Beweis.* Lorenz (1990), § 29, F22 *q.e.d.*

**(2.23) Definition:** *operiert.* Sei $G$ eine Gruppe, $D$ eine nicht-leere Menge und $S(D)$ die Gruppe der Bijektionen von $D$ auf sich, zusammen mit der Verkettung von Abbildungen als Verknüpfung. Man sagt $G$ operiert auf $D$, wenn es einen Homomorphismus von Gruppen

$$\phi : G \to S(D)$$

$$\sigma \mapsto \phi(\sigma) = \phi_\sigma$$

von $G$ in die Gruppe aller Bijektionen von $D$ gibt. Die Anwendung eines $\sigma \in G$ auf ein $d \in D$ notieren wir dann auch in der Form

$$\sigma d = d^\sigma = \phi_\sigma(d)$$

Man erhält so eine Abbildung

$$G \times D \to D$$

$$(\sigma, d) \mapsto \sigma d = d^\sigma$$

mit

1. $1d = d^1 = d$
2. $(\sigma\tau)d = \sigma(\tau d)$, beziehungsweise $d^{(\sigma\tau)} = (d^\tau)^\sigma$

**(2.24) Beispiel:** Sei $L/K$ eine galoissche Körpererweiterung mit Galoisgruppe $\mathrm{Gal}(L/K)$. Vermöge $(\sigma, \ell) \mapsto \sigma(\ell) = \ell^\sigma$ operiert $\mathrm{Gal}(L/K)$ auf $L$.

**(2.25) Beispiel:** Sei $L/K$ eine galoissche Körpererweiterung mit Galoisgruppe $\mathrm{Gal}(L/K)$ und $D$ eine zentraleinfache Divisionsalgera über $K$. Die Galoisgruppe $\mathrm{Gal}(L/K)$ operiert auf $D_L := L \otimes_K D$ vermöge

$$\phi : \mathrm{Gal}(L/K) \times D_L \to D_L$$

$$(\sigma, \ell \otimes d) \mapsto (\sigma(\ell)) \otimes d = \ell^\sigma \otimes d$$

Die zu $\sigma$ gehörige Bijektion von $D_L$ sei mit $\phi_\sigma$ bezeichnet.

**(2.26) Satz:** *Nach Basiswahl induziert $\phi_\sigma$ eine Abbildung $\varphi_\sigma$ von $M_{n\times n}(L)$ auf sich:*

$$\begin{array}{ccc} D_L & \xrightarrow{\psi} & M_{n\times n}(L) \\ {\scriptstyle \phi_\sigma}\downarrow & & \downarrow{\scriptstyle \varphi_\sigma} \\ D_L & \xrightarrow[\psi]{} & M_{n\times n}(L) \end{array}$$

*mit $\varphi_\sigma = \psi^{-1}\phi_\sigma\psi$, diese hat für $d = \left(d_{i,j}\right)_{1\le i,j\le n}$ die Form:*

$$\varphi_\sigma(d) = \left(d_{i,j}^\sigma\right)_{1\le i,j\le n}$$

$\mathrm{Gal}(L/K)$ *operiert auf $M_{n\times n}(L)$ also durch Operation auf den Matrixeinträgen.*

*Beweis.* Lorenz (1990), § 30, Lemma 2 *q.e.d.*

**(2.27) Satz:** *Sei $d \in D$, $\sigma \in \mathrm{Gal}(L/K)$ so gilt $d^\sigma = d$.*

*Beweis.*

$$d^\sigma = \sigma(1 \otimes d) = (\sigma(1)) \otimes d = 1 \otimes d = d$$

*q.e.d.*

**(2.28) Satz:** *Sei $d^\sigma = d$ für alle $\sigma \in \mathrm{Gal}(L/K)$, dann ist $d \in M_{n\times n}(K)$*

*Beweis.*

$$d^\sigma = \left(\left(d_{i,j}\right)_{1\le i,j\le n}\right)^\sigma = \left(\left(d_{i,j}^\sigma\right)_{1\le i,j\le n}\right) = \left(\left(d_{i,j}\right)_{1\le i,j\le n}\right) = d$$

$\Rightarrow \forall 1 \le i,j \le n : a_{i,j}^\sigma = a_{i,j}$

$\Rightarrow \forall 1 \le i,j \le n : a_{i,j} \in K$, denn $L/K$ ist galoisch und daher $K = L^{G(L/K)}$ *q.e.d.*

Tatsächlich können wir $d \in D$ als eine Matrix mit Einträgen in $K$ ansehen. Nun können wir die Determinate dieser Matrix betrachten. Als eine Funktion der Einträge von $d$, ist diese Determinante eine Form in $n^2$ Variablen vom Grad $n$, genannt die reduzierte Norm $N_{\text{red}}(d)$ von $d$ mit Koeffizienten in $K$. Die Multiplikativität der Determinanten impliziert $N_{\text{red}}(x) \cdot N_{\text{red}}(y) = N_{\text{red}}(x \cdot y)$ für alle $x, y \in D$. Da die Determinante der Einheitsmatrix 1 ist, impliziert dies: $N_{\text{red}}(d) \cdot N_{\text{red}}(d^{-1}) = 1$ für $d \neq 0$ in $D$. Daher ist $N_{\text{red}}(d) \neq 0$ für $d \neq 0$ und die einzige Nullstelle dieser Form in $K$ ist die triviale. Nach unserer Annahme, dass K ein $C_1$-Körper ist, kann dies nur für $n = 1$ sein, das bedeutet $D = K$. Somit gibt es keine zentalen Divisionsalgebren über $K$, außer $K$ selbst. *q.e.d.*

## Literatur


[Böge 2006] BÖGE, Sigrid: *Vorlesungsmanuskript Algebra 1.* 2006

[Greenberg 1969] GREENBERG, Marvin J.: *Lectures on forms in many variables.* New York-Amsterdam : W.A. Benjamin Inc., 1969. – MathSciNet review: 39 #2698

[Lorenz 1987] LORENZ, Falko: *Einführung in die Algebra, Teil I.* Mannheim : Bibliographisches Institut, 1987. – MathSciNet review: 89j:12001

[Lorenz 1990] LORENZ, Falko: *Einführung in die Algebra, Teil II.* Mannheim : Bibliographisches Institut, 1990. – MathSciNet review: 92j:00006

[Warning 1936] WARNING, Ewald: Bemerkungen zur vorstehenden Arbeit von Herrn Chevalley. In: *Abh. Math. Sem. Univ. Hamburg* 11 (1936), S. 76–83