Algebra Seminar SS05

Vortrag von Juan Carlos Matutat S.B.

May 17, 2005

Motivationsaufgabe

Sei k ein endlicher Körper der Charakteristik p mit q Elementen.
Sei $f(x,y,z) \in k[x,y,z]$ mit

$$f(x,y,z) = x^2 + y^2 + z^2.$$

Zeige nun,dass f eine nichttriviale Nullstelle besitzt.

LÖSUNG: Sei o.B.d.A. $x = 1$ so gilt es zu zeigen, dass $z^2 = -1 - y^2$ eine Lösung besitzt. Sei dazu $n := \#\{z^2 \mid z \in k\}$ und $m := \#\{-1 - y^2 \mid y \in k\}$.
Da $k^\times$ zyklisch ist und q-1 Elemente besitzt, gilt:

$$k^\times = \{x^1, x^2, ..., x^{q-1}\},\ \textit{wobei x ein erzeugendes Element ist.}$$

Nun besitzt $k^\times$ genau $\frac{q-1}{2}$ Quadrate, da
zum einen $k^\times$ mindestens $\frac{q-1}{2}$ Quadrate enthält, weil die Elemente $(x^k)^2 = x^{2k}$ für $k = 1, 2, ..., \frac{q-1}{2}$ verschieden sind und
zum anderen $k^\times$ höchstens $\frac{q-1}{2}$ Quadrate entält, wegen $\{z^2 \mid z \in k^\times\} = \{x^2, x^4, x^6, ..., x^{2(q-1)}\}$, aber $x^{2k} = x^{2k+(q-1)} = x^{q+2k-1}$ und $q+2k-1 \leq 2(q-1)$ für $k = 1, 2, ..., \frac{q-1}{2}$.
$\Rightarrow$ k besitzt $\frac{q-1}{2} + 1$ Quadrate wegen der 0.
$\Rightarrow n = m = \frac{q+1}{2}$
$\Rightarrow n + m = q + 1 > q$, d.h. $\exists\ z_0, y_0 \in k$ mit $z_0^2 = -1 - y_0^2$ und $(1, y_0, z_0) \neq 0$ ist eine nichtriviale Nullstelle.
$\Rightarrow$ Behauptung

Nun soll im folgenden diese Aussage ausgeweitet werden auf Polynome, die bestimmte Voraussetungen erfüllen.Hierzu sollten folgenden Konventionen für die Bezeichungen gelten.
Im folgenden sei k ein endlicher Körper mit q Elementen und der Charakteristik p, d.h. $q = p^n$,für ein $n \in N$. $k^\times$ sei die multiplikative Gruppe von k mit $(q-1)$ Elementen.$k^\times$ ist zyklisch (nach Vorlesung).
Im Ersten Teil der folgenden Ausführung zeigt man, dass für ein Polynom $f \in k[x_1, ..., x_n]$ mit $deg(f) = d$ und $d < n$ gilt, dass die Anzahl der Nullstellen kongruent 0 modulo p ist, d.h. insbesondere dass hiermit gezeigt ist,dass alle homogenen Polynome vom Grad grösser gleich 2 mindestens eine nicht-triviale Nullstelle besitzen,falls die Anzahl der Variablen echt grösser ist als der Grad von f (siehe z.B. Motivationsaufgabe).
Im Zweiten Teil zeigt man,dass die Anzahl der Nullstellen unter obigen Voraussetzungen sogar grösser gleich q^{n-d} ist.

Teil 1

LEMMA 1 Sei $m \geq 0$,$m \in N$, so gilt:

$$\sum_{x \in k} x^m = \begin{cases} -1 & , falls\ (q-1)\ teilt\ m \\ 0 & , sonst \end{cases}$$

BEWEIS: $x \longmapsto x^m$ ist ein Homomorphismus $k^\times \to k^\times$. Falls $(q-1) \mid m$ ist dieser trivial, da $k^\times$ zyklisch ist und $(q-1)$ Elemente besitzt. In diesem Falle gilt:

$$\sum_{x \in k} x^m = 0^m + \sum_{x \in k^\times} x^m = 0 + (q-1)1 \equiv -1 \ (mod\ p)$$

Falls $(q-1)$ jedoch nicht m teilt,folgt die Behauptung aus Lemma 2.

LEMMA 2 Sei Ω ein Körper und h: $k^\times \to \Omega^\times$ ein nicht-trivialer Homomorphismus. So gilt:

$$\sum_{x \in k^\times} h(x) = 0$$

BEWEIS: o.B.d.A. sei $h(y) \neq 1$ für ein $y \in k^\times$. Da h ein Homomorphismus ist, gilt:

$$\sum_{x \in k^\times} h(x) = \sum_{x \in k^\times} h(xy) = h(y) \sum_{x \in k^\times} h(x)$$

Daher muss für die Gültigkeit der Gleichung gelten:

$$\sum_{x \in k^\times} h(x) = 0$$

BEMERKUNG: Nun folgt die Behauptung von Lemma 1 mit $h(x) := x^m$. Dieser erfüllt die Voraussetzungen von Lemma 2.

THEOREM *(Chevallay-Warning)*
$f \in k[x_1, ..., x_n]$ mit Koeffizienten aus k und $deg(f) = d$. Sei $N(f)$ die Anzahl der verschiedenen Nullstellen von f über k. Falls $n < d$, so ist

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

BEMERKUNG: Dies bedeutet insbesondere, dass falls f keinen konstanten Term besitzt, f auf jeden Fall mindestens eine nicht-triviale Null in k besitzt (d.h. C_1 ist).
Dies gilt, da wegen $f(0) = 0$ $N(f) \geq 1$ und wegen $N(f) \equiv 0 \ (mod\ p)$ existieren mindestens $(p-1)$ weitere Nullstellen von füber k. Und homogene Polynome vom Grad grösser 0 besitzen stets keine konstanten Terme.

BEWEIS: Im folgenden sei $x \in k^n$.Nun gilt:

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

Summiert man nun über alle $x \in k^n$, so gilt für die nullstellenzählende Funktion $N(f)$:

$$N(f) = \sum_{x \in k^n} (1 - f(x)^{q-1}) = -\sum_{x \in k^n} (f(x)^{q-1}) + \underbrace{q^n}_{\equiv 0 \ (mod\ p)} \equiv -\sum_{x \in k^n} f(x)^{q-1} \ (mod p)$$

Um die Behauptung zu zeigen, reicht es somit zu zeigen, dass

$$\sum_{x \in k^n} f(x)^{q-1} \equiv 0 \ (mod\ p).$$

Für alle f^{q-1} gilt, dass diese k-lineare Kombinationen von Monomen vom höchsten Grad $d(q-1)$ sind. Sei nun $x^\mu = x_1^{\mu_1} x_2^{\mu_2} \cdot ... \cdot x_n^{\mu_n}$ (1) ein solches Monom,so gilt:

$$\sum_{x \in k^n} x^\mu = \prod_{i=1}^{n} \sum_{x_i \in k} {x_i}^{\mu_i} \qquad (2)$$

Aus (1) folgt:

$$\sum_{i=1}^{n} \mu_i = \mu \leq d(q-1)$$

Da nun $d < n$ ist, muss ein Index $i \in (1, .., n)$ existieren mit μ_i ist nicht teilbar durch $(q-1)$.
$\overset{\text{Lemma2}}{\Rightarrow}$ Der i-te Faktor des Produkts (2) ist $\equiv 0 \ (mod\ p)$.
$\Rightarrow$ Das gesamte Produkt ist $\equiv 0 \ (mod\ p)$.
$\Rightarrow$ Alle Monome sind $\equiv 0 \ (mod\ p)$.

$$\Rightarrow \sum_{x \in k^n} f(x)^{q-1} \equiv 0 \ (mod\ p).$$

Teil 2

SATZ 1 $f(x) = f(x_1, ..., x_n)$ sei ein beliebiges Polynom in n Variablen über k vom Gesamtgrad $d < n$; $A_1, ..., A_r$ seien sämtliche verschiedenen Nullstellen von $f(x)$.
Dann gilt für jedes Polynom $\phi(x) = \phi(x_1, ..., x_n)$ über k, dessen Gesamtgrad $< (q-1)(n-d)$ ist

$$\sum_{i=1}^{r} \phi(A_i).$$

BEWEIS: Sei $F(x) := 1 - f(x)^{q-1}$ mit $deg(F) = (q-1)d$ so gilt:

$$F(x) = \begin{cases} 1 & , falls\ f(x) = 0 \\ 0 & , sonst \end{cases}$$

Sei $A \in k^n$ mit $A = (a_1, ..., a_n)$ und $a_i \in k$, so sei

$$F_A^*(x) := \prod_{k=1}^{n} (1 - (x_k - a_k)^{q-1})$$

und es gilt:

$$F_A^*(x) = \begin{cases} 1 & , falls\ x = A \\ 0 & , sonst \end{cases}$$

Seien nun $A_1, ..., A_r$ r verschiedene Punkte des k^n so ist

$$F^*(x) := \sum_{i=1}^{r} F^*_{A_i}(x) = (-1)^n \sum_{i=1}^{r} \prod_{k=1}^{n} ((x_k - a_{ik})^{q-1} - 1)$$

und es gilt:

$$F^*(x) = \begin{cases} 1 & , \quad falls\ x = A_i\ für\ ein\ i \in 1, .., r \\ 0 & , \quad falls\ x \neq A_i\ für\ alle\ i \in 1, .., r \end{cases}$$

In k gilt:

$$(x-a)^{q-1} = \frac{(x-a)^q}{x-a} = \frac{x^q - a^q}{x-a} = \sum_{\nu=0}^{q-1} x^{q-1-\nu} a^\nu$$

und dementsprechend

$$(x_k - a_{ik})^{q-1} - 1 = \sum_{\nu=0}^{q-1} {x_k}^{q-1-\nu} a_{ik}^\nu - 1 = \sum_{\nu=0}^{q-1} {x_k}^{q-1-\nu} c_{ik}^{(\nu)}$$

,wobei

$$c_{ik}^{(\nu)} = \begin{cases} a_{ik}^\nu & , \quad 0 \leq \nu < q-1 \\ a_{ik}^{q-1} - 1 & , \quad \nu = q-1 \end{cases}$$

Hieraus folgt die folgende Darstellung für $F^*(x)$

$$F^*(x) = (-1)^n \sum_{0 \leq \nu_k \leq q-1} x_1^{q-1-\nu_1} \cdot ... \cdot x_n^{q-1-\nu_n} \sum_{i=1}^{r} c_{i1}^{(\nu_1)} \cdot ... \cdot c_{in}^{(\nu_n)}$$

Seien nun $A_1, ..., A_r$ die r verschiedenen Nullstellen des Polynoms $f(x)$, so ist $F^*(x)$ das zu $F(x) = 1 - f^{q-1}(x)$ gehörige sogenannte reduzierte Polynom, denn für jeden Punkt x des k^n ist

$$F^*(x) = F(x) = \begin{cases} 1 & , \quad f(x) = 0, d.h.\ x = A_i\ für\ ein\ i \\ 0 & , \quad sonst \end{cases}$$

Es muss somit gelten:

$$deg(F(x)) \geq deg(F^*(x))$$

und damit müssen die Koeffizienten der Monome von F^* vom Grad grösser $(q-1) \cdot d$ verschwinden, d.h.

$$\sum_{i=1}^{r} c_{i1}^{(\nu_1)} \cdot .. \cdot c_{in}^{(\nu_n)} = 0$$

für alle $0 \leq \nu_k \leq q-1$ für die gilt:

$$(q-1)d = deg(F(x)) < deg(F^*(x)) = \sum_{k=1}^{n} (q - 1 - \nu_k) = (q-1)n - \sum_{k=1}^{n} \nu_k$$

Diese Ungleichung ist äquivalent zu

$$\sum_{k=1}^{n} \nu_k < (q-1)(n-d)$$

und somit gilt nach der Definition der c_{ik},dass

$$\sum_{i=1}^{r} a_{i1}^{\nu_1} \cdot ... \cdot a_{in}^{\nu_n} = 0$$

,falls alle $\nu_k < q-1$.
Für den Fall, dass $\nu_1 = q-1$ gilt:

$$\sum_{i=1}^{r} (a_{i1}^{q-1} - 1) a_{i2}^{\nu_2} \cdot ... \cdot a_{in}^{\nu_n} = 0$$

dies ist äquivalent zu

$$\sum_{i=1}^{r} a_{i1}^{q} a_{i2}^{\nu_2} \cdot ... \cdot a_{in}^{\nu_n} - \underbrace{\sum_{i=1}^{r} (a_{i1}^{0}) a_{i2}^{\nu_2} \cdot ... \cdot a_{in}^{\nu_n}}_{=0 \ ,da \ \nu_i < (q-1) \ für \ alle \ i} = 0$$

und daraus folgt:

$$\sum_{i=1}^{r} a_{i1}^{q-1} a_{i2}^{\nu_2} \cdot ... \cdot a_{in}^{\nu_n} = 0$$

Nach Induktion nach den Exponenten ν_i gilt somit:

$$\sum_{i=1}^{r} a_{i1}^{\nu_1} a_{i2}^{\nu_2} \cdot ... \cdot a_{in}^{\nu_n} = 0 \qquad (*)$$

,falls

$$\sum_{k=1}^{n} \nu_k < (q-1)(n-d)$$

hieraus folgt somit die Behauptung, da sich jedes Monom von ϕ wie $(*)$ darstellen lässt.

LEMMA 3 Sei $N(a_1, ..., a_{n-d})$ die Anzahl derjenigen A_i,deren Koordinaten an $(n-d)$ Stellen die Werte $a_{ik} = a_k$ $(k = 1, ..., n-d)$ haben,wobei $a_1, ..., a_{n-d} \in k$ beliebig, so gilt $N(a_1, ..., a_{n-d})$ ist modulo p von den Werten a_k unabhängig.

BEWEIS: Es genügt zu zeigen, dass $N(a_1, ..., a_{n-d}) \equiv N(c_1, a_2, ..., a_{n-d}) (mod\ p)$ für ein $c_1 \in k$ mit $c_1 \neq a_1$.
Sei dazu

$$h(x) := x^{q-1} - 1 = \frac{x^q - x}{x - 0} = \prod_{\substack{\alpha \in k \\ \alpha \neq 0}} (x - \alpha)$$

und

$$\psi(x) := \frac{h(x_1 - a_1)}{x_1 - c_1} h(x_2 - a_2) \cdot ... \cdot h(x_{n-d} - a_{n-d})$$

und es gilt ferner

$$\frac{h(x_1 - a_1)}{x_1 - c_1} = \prod_{\substack{\alpha \in k \\ \alpha \neq a_1, c_1}} (x_1 - \alpha) = \frac{h(x_1 - c_1)}{x_1 - a_1}$$

,da $h(x_1 - a_1) = (x_1 - a_1)^{q-1} - 1 = \frac{(x_1-a_1)^q-(x_1-a_1)}{(x_1-a_1)} = \frac{x_1^q-a_1^q-x_1+a_1}{x_1-a_1} = \frac{x_1^q-a_1-x_1+a_1}{x_1-a_1} = \frac{x_1^q-x_1}{x_1-a_1} = \prod_{\substack{\alpha\in k\\ \alpha\neq a_1}} (x_1 - \alpha)$

Hieraus folgt für $x \in k^n$

$$\psi(x) = \frac{(-1)^{n-d}}{a_1 - c_1} \cdot \begin{cases} 1 & , \quad x_1 = a_1 \; und \; b_k = a_k \; , \; k = 2, .., n-d \\ -1 & , \quad x_1 = c_1 \; und \; b_k = a_k \; , \; k = 2, .., n-d \\ 0 & , \quad sonst \end{cases}$$

,da $h(0) = -1$, $\frac{h(a_1-c_1)}{a_1-c_1} = \frac{-1}{a_1-c_1}$ und $\frac{h(c_1-c_1)}{c_1-a_1} = \frac{1}{a_1-c_1}$.

Da $deg(\psi) = (q-1)(n-d) - 1 < (q-1)(n-d)$ folgt nach Satz 1:

$$0 = \sum_{i=1}^{r} \psi(A_i) = \frac{(-1)^{n-d}}{a_1 - c_1}(N(a_1, a_2, ..., a_{n-d}) - N(c_1, a_2, ..., a_{n-d}))$$

Daraus folgt die Behauptung, da $\frac{(-1)^{n-d}}{a_1-c_1} \neq 0$.

Satz 2 Für parallele d-dimensionale lineare Unterräume des k^n sind die Anzahlen der darin enthaltenen A_i kongruent (*modulo p*).

Beweis: Sei $x^{'} = \sigma_{i0} + \sum_{\nu=1}^{n} \sigma_{i\nu} x_\nu$ ($\sigma_{i\nu}$ beliebig aus k) eine beliebige affin lineare Transformation der Unbestimmten,so gilt für $A_i^{'} = \sigma(A_i)$ und für jedes Polynom $\phi(x)$ über k, dessen Grad $< (q-1)(n-d)$ ist, dass

$$\sum_{i=1}^{r} \phi(A_i^{'}) = 0$$

,da $\phi^{'}(x) = \phi(\sigma(x))$ ebenso die Voraussetungen von Satz1 erfüllt.
Sei nun L ein solcher d-dimensionaler affin-linearer Unterraum, so kann jeder hierzu parallele d-dimensionale affin-lineare Unterraum des k^n durch eine eindeutige Trafo σ angewendet auf L beschrieben werden.
z.B. $\begin{cases} x_\nu^{'} = a_\nu & für \; \nu = 1, ..., n-d \\ x_\nu^{'} & beliebig \; aus \; k \; für \; (n-d) < \nu \leq n \end{cases}$
Somit folgt nun die Behauptung mit dem Lemma 3.

Satz 3 Sei $f(x)$ ein Polynom das die Voraussetungen von Satz1 erfüllt.Falls nun $f(x)$ mindestens eine Nullstelle besitzt, so ist die Anzahl aller verschiedenen Nullstellen von $f(x)$ mindestens q^{n-d}.

Beweis: Sei nun r die Anzahl der Nullstellen von $f(x)$ und $r \neq 0$.

Fall 1: Sei $L \subset k^n$ ein d-dimensionaler affin-linearer Raum und r_L die Anzahl der darin enthaltenen Nullstellen A_i von $f(x)$.Weiter sei r_L nicht kongruent 0 (modulo p). Somit ist $r_L \geq 1$ und dies gilt nach Satz 2 ebenso für alle zu L parallelen d-dimensionalen affin-linearen Räume L_p. Durch jeden Punkt des k^n geht genau ein zu L paralleler d-dimensionaler Raum. Da jeder dieser Räume q^d Punkte enthält, stimmen je q^d der q^n Räume überein. Somit besteht der k^n aus genau q^{n-d} verschiedene zu L parallelen Räumen. $\Rightarrow r = q^{n-d} \cdot r_L \geq q^{n-d} \cdot 1$

Fall 2: Sei für jeden d-dimensionalen affin-lineare Raum r_L die Anzahl der darin enthaltenen Nullstellen A_i mit $r_L \equiv 0 \ (mod\ p)$. Da $r_L \neq 0 \ \exists s \in 1, ..., d$, so dass für jeden s-dimensionalen affin-linearen Raum die Anzahl der darin enthaltenen A_i kongruent Null modulo p ist, jedoch für einen gewissen (s-1)-dimensionalen affin-linearen Raum L_{s-1} die Anzahl r_{s-1} der enthaltenen A_i nicht kongruent modulo p.
Durch jeden der $q^n - q^{s-1}$ ausserhalb von L_{s-1} liegende Punkte des k^n, gibt es genau einen s-dimensionalen affin-linearen Raum, der L_{s-1} enthält. Dieser enthält $q^s - q^{s-1}$ nicht in L_{s-1} liegende Punkte. Daher gibt es genau $\frac{q^n - q^{s-1}}{q^s - q^{s-1}} = \frac{q^{n-s+1}-1}{q-1} = q^{n-s} + ... + q + 1$ verschiedene s-dimensionale lineare Räume L_s, welche zu je zweien L_{s-1} als Durchschnitt haben.
Sei nun $r_{s-1} \equiv a \ (mod\ p)$ mit $a \in 1, ..., p-1$, so gibt es also in jedem L_s mindestens $(p-a)$ A_i. Diese gehören nicht zu L_{s-1}. $\Rightarrow r \geq a + (p-a) \cdot \frac{q^{n-s+1}-1}{q-1} > \frac{q^{n-s+1}-1}{q-1} \geq \frac{q^{n-d+1}-1}{q-1} > q^{n-d}$

Somit ist der Satz bewiesen.

Literatur

Lütkebohmert, W., 'Vorlesungsmanuskript Algebra WS 2000/01'

Teil 1: Greenberg, Marvin J. 'Lectures on Forms in many variables', W.A. Benjamin Inc., New York

Teil 2: Warning, Ewald 'Bemerkungen zur vorstehenden Arbeit von Herrn Chevalley', Hamburg