Ruprecht-Karls-Universität Heidelberg
Mathematisches Institut
Seminar: Quadratische Formen über den rationalen Zahlen
Sommersemester 2007
Dozent: Prof. Dr. Kay Wingberg
Assistent: Johannes Bartels

Kapitel 1: Endliche Körper

1 Allgemeines

2 Gleichungen über einem endlichen Körper

Referentinnen:
Katrin Dollinger
Anja Schäfer

Endliche Körper

1 Allgemeines

Alle Körper werden als kommutativ betrachtet

1.1 Endliche Körper

Sei K ein Körper. Das Bild von $\mathbb{Z}$ in K ist ein Integritätsbereich, daher isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/p\mathbb{Z}$, wobei p eine Primzahl ist. Sein Quotientenkörper ist isomorph zu $\mathbb{Q}$ oder $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Im ersten Fall kann man sagen, K hat die Charakteristik 0; im zweiten die Charakteristik p.
Die Charakteristik von K wird geschrieben als $char(K)$. Wenn gilt, dass $char(K) = p \neq 0$, dann ist p auch die kleinste ganze Zahl $n > 0$, so dass $n \cdot 1 = 0$ (kurze Erinnerung: Die Charakteristik eines Körpers ist definiert durch:

$$char(K) = \begin{cases} \min\left\{k \mid \underbrace{1 + \cdots + 1}_{k} = 0\right\} & \text{falls } \neq 0 \\ 0 & \text{sonst} \end{cases}$$

Lemma
Wenn $char(K) = p$, ist die Abbildung $\sigma : x \mapsto x^p$ ein Isomorphismus von K auf einen seiner Unterkörper K^p

Beweis: Homomorphismus:

- Wir haben: $\sigma(xy) = \sigma(x)\sigma(y)$. Denn $(xy) \mapsto (xy)^p = x^p y^p \checkmark$

zz.: $\sigma(xy) = \sigma(x) + \sigma(y)$, d.h. $(x+y)^p = x^p + y^p$

- Für:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

mit $k \in \{1, 2, ..., p-1\}$ gilt:

$$p \mid \binom{p}{k}$$

denn

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}, \text{ p prim } \Rightarrow p|p!, p \nmid k!, p \nmid (p-k)! \Rightarrow \binom{p}{k} = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}$$

d.h. der Binomialkoeffizient $\binom{p}{k} \equiv 0 (mod\, p)$, wenn $0 < k < p$

$$\begin{aligned}\Rightarrow (x+y)^p &= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \\ &= \binom{p}{0} x^0 y^p + \underbrace{\sum_{k=1}^{p-1} \binom{p-1}{k} x^k y^{p-k}}_{=0} + \binom{p}{p} x^p y^0 \\ &= x^p + y^p\end{aligned}$$

daher ist σ ein Homomorphismus.

zz.: Bijektivität

- injektiv: klar, denn $ker(\sigma)$ enthält nur die 0
- surjektiv: folgt aus Definition $K^p = \{y^p | y \in K\} = \{x \in K | \exists y \in K : y^p = x\}$ $\square$

Satz 1

(i) Die Charakteristik eines endlichen Körpers K ist eine Primzahl $p \neq 0$. Wenn $f = [K : \mathbb{F}_p]$(d.h. f ist die Dimension von K als $\mathbb{F}_p$-Vektorraum), ist die Anzahl der Elemente von K $q = p^f$.

(ii) Sei p eine Primzahl und sei $q = p^f (f \geq 1)$ eine Potenz von p. Sei Ω ein algebraisch abgeschlossener Körper der Charakteristik p. Es existiert ein eindeutiger Unterkörper $\mathbb{F}_q$ von Ω der q Elemente besitzt. Es ist die Menge der Nullstellen des Polynoms $X^q - X$

(iii) Alle endlichen Körper mit $q = p^f$ Elementen sind isomorph zu $\mathbb{F}_q$

Beweis:

(i) Wenn K endlich ist, enthält es nicht den Körper $\mathbb{Q}$, denn dieser ist abzählbar. Daher ist seine Charakteristik eine Zahl n. Aufgrund der Definition der Charakteristik von K ist n die kleinste natürliche Zahl für die gilt:

$$n \cdot 1 = \underbrace{1 + 1 + ... + 1}_{n-mal} = 0$$

Angenommen, $n = m \cdot l$. Dann ist $0 = n \cdot 1 = (m \cdot 1) \cdot (l \cdot 1)$. Also $m \cdot 1 = 0$ oder $l \cdot 1 = 0$. Wegen der Minimalität von n und der Nullteilerfreiheit des Körpers folgt daraus, dass n eine Primzahl ist, also $n = p$.
Sei f der Grad des Körpererweiterung $K/\mathbb{F}_p$. K als $\mathbb{F}_p$-Vektorraum aufgefasst und mit K endlich, dann folgt daraus, dass $\mathbb{F}_p$ ein endlich-dimensionaler Vektorraum ist. Sei $\{k_1, ..., k_f\}$ eine Basis. Dann lässt sich jedes Element auf genau eine Weise als Linearkombination [s. LA I] $\sum a_i k_i$ mit $a_i \in \mathbb{F}_p$ schreiben. $\Rightarrow$ es gibt genau $|\mathbb{F}_p|^f = p^f$ Elemente in K.

(ii) Da Ω algebraisch abgeschlossen ist mit Charakteristik p, ist $\sigma' : x \mapsto x^q$ ein Automorphismus von Ω, nämlich die f-te Iteration von $\sigma : x \mapsto x^p$. Die Invarianten von σ' formen den Unterkörper $\mathbb{F}_q$ von Ω. Die Ableitung des Polynoms $X^q - X$ ist:

$$qX^{q-1} - 1 = \underbrace{p \cdot p^{f-1} X^{q-1}}_{=0, \text{ da } p=0} - 1 = -1$$

und ist nicht 0. Dies impliziert (da Ω algebraisch abgeschlossen ist), dass $X^q - X$ q paarweise verschiedene Wurzeln hat, daher $Card(\mathbb{F}_q) = q$.
Umgekehrt, wenn K ein Unterkörper von Ω ist mit q Elementen, hat die multiplikative Gruppe $K^* = K \backslash \{0\} q - 1$ Elemente. Dann ist $x^{q-1} = 1$, für $x \in K^*$ und $x^q = x$, für $x \in K$. Dies beweist, dass K in $\mathbb{F}_q$ enthalten ist. Weil $Card(K) = Card(\mathbb{F}_q)$ haben wir $K = \mathbb{F}_q$, was den Beweis zu ii) vervollständigt.

(iii) Aussage iii) folgt aus ii) und aus der Tatsache, dass alle Körper mit p^f Elementen in Ω eingeschlossen werden können, da Ω algebraisch abgeschlossen ist.

1.2 Die multiplikative Gruppe eines endlichen Körpers

Sei p eine Primzahl und f eine natürliche Zahl ≥ 1 und sei $q = p^f$

Satz 2

Die multiplikative Gruppe $\mathbb{F}_q^*$ eines endlichen Körpers $\mathbb{F}_q$ ist zyklisch mit Ordnung $q - 1$

Beweis: $\Phi(d)$ bezeichnet die Eulerfunktion: $\Phi(d) = \sharp\{1 \leq a \leq m | (a,m) = 1\}$. Sei $d \in \mathbb{N}$. Dann ist $\Phi(d)$ die Anzahl der Erzeuger der zyklischen Gruppe, der Ordnung d. $\square$

Um den Beweis zu vervollständigen werden die folgenden beiden Lemmata benötigt.

Lemma 1

Wenn n eine natürliche Zahl ≥ 1 ist, dann gilt

$$n = \sum_{d|n} \Phi(d)$$

(Erinnerung: die Schreibweise $d|n$ bedeutet: d teilt n)

Beweis: Wenn $d|n$; sei C_d die eindeutige Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ mit der Ordnung d und sei Φ_d die Menge der Erzeuger von C_d. Da alle Elemente von $\mathbb{Z}/n\mathbb{Z}$ eines der C_d erzeugen, ist die Gruppe $\mathbb{Z}/n\mathbb{Z}$ die disjunkte Vereinigung von Φ_d und wir erhalten:

$$n = Card(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} Card(\Phi_d) = \sum_{d|n} \Phi(d) \quad \square$$

Lemma 2

Sei H eine endliche Gruppe der Ordnung n. Es sei angenommen, dass für alle Teiler d von n, die Menge $\{x \in H | x^d = 1\}$ höchstens d Elemente besitzt. Dann ist H zyklisch.

Beweis: Sei d ein Teiler von n. Wenn ein $x \in H$ mit der Ordnung d existiert, ist die durch x erzeugte Untergruppe $(x) = \{1, x, ..., x^{d-1}\}$ zyklisch mit Ordnung d. Im Hinblick auf die These gilt, dass alle Elemente $y \in H$ mit $y^d = 1$ zu (x) gehören. Besonders sind alle Elemente von H mit Ordnung d Erzeuger von (x) und dies sind $\Phi(d)$ Stück.
$\Rightarrow$ Es gibt nur 0 oder $\Phi(d)$ Elemente der Ordnung d in H. Wäre es 0 für einen Wert von d, würde aus Lemma 1 folgen, dass die Anzahl der Elemente von $H < n$ ist, im Widerspruch zur Annahme. Insbesondere existiert ein $x \in H$ mit Ordnung d und H fällt mit der zyklischen Gruppe (x) zusammen.
Satz 2 folgt aus Lemma 2 für $H = \mathbb{F}_q*$ und $n = q - 1$; es ist auch offensichtlich,

dass die Gleichung $x^d = 1$ mit Grad d nur höchstens d Lösungen in $\mathbb{F}_q$ hat. $\square$

Bemerkung

Der obige Beweis zeigt allgemeiner, dass alle endlichen Untergruppen der multiplikativen Gruppe eines Körpers zyklisch sind.

2 Gleichungen über einem endlichen Körper

2.1 Potenzsummen

Lemma

Sei u eine natürliche Zahl ≥ 0. Wir einigen uns auf $x^u = 1$, wenn $u = 0$, auch wenn $x = 0$.

$$S(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \begin{cases} 0 & \text{falls } u = 0 \\ -1 & \text{falls } u \geq 1 \wedge (q-1)|u \\ 0 & \text{falls } u \geq 1 \wedge (q-1) \nmid u \end{cases}$$

ist äquivalent zu -1 wenn $u \geq 1$ ist und teilbar durch $q-1$; sie ist äquivalent zu 0 sonst.

Beweis:

- 1. Fall: $u = 0$

  $$S(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q} x^0 = q \cdot 1 = 0$$

  weil $\mathbb{F}_q$ die Charakteristik p hat.

- 2. Fall: $u \geq 1, (q-1)|u, x \in \mathbb{F}_q \backslash \{0\}$
  $\Rightarrow u = (q-1)a$ mit $a \geq 1$

  $$\sum_{x \in \mathbb{F}_q^*} x^u = \sum_{x \in \mathbb{F}_q^*} \underbrace{x^{(q-1)a}}_{=1} = \sum_{i=1}^{q-1} 1^i = (q-1) \cdot 1 = q-1$$

Damit gilt:

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} x^u &= 0^u + \sum_{x\in\mathbb{F}_q*} x^u \\ &= 0^u + (q-1) \\ &= 0 + (p^f - 1) \\ &= -1\end{aligned}$$

- 3. Fall: $u \geq 1 \wedge (q-1) \nmid u$
  Da $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ zyklisch mit Ordnung $q-1$ ist, existiert ein $y \in F_q^*$ mit $y^u \neq 1$.
  Multiplikation von $\sum_{x\in\mathbb{F}_q^*} x^u$ mit y^u ergibt:

$$\begin{aligned}y^u(\sum_{x\in\mathbb{F}_q^*} x^u) = \sum_{x\in\mathbb{F}_q^*}(y\cdot x)^u = \sum_{x\in\mathbb{F}_q^*} x^u \\ \Leftrightarrow y^u(\sum_{x\in\mathbb{F}_q^*} x^u) - (\sum_{x\in\mathbb{F}_q^*} x^u) = 0 \\ \Leftrightarrow (\sum_{x\in\mathbb{F}_q^*} x^u)\underbrace{(y^u - 1)}_{\neq 0} = 0 \Rightarrow \sum_{x\in\mathbb{F}_q^*} x^u = 0 \qquad \square\end{aligned}$$

2.2 Satz von Chevalley

Satz von Chevalley-Warning

Seien $f_\alpha \in \mathbb{F}_q[X_1, ..., X_n]$ Polynome mit n Variablen mit $\alpha = 1, ..., n$. Bezeichne G das Gleichungssystem

$$f_\alpha(X_1, ..., X_n) = 0$$

$V = L(G)$ sei die Lösungsmenge dieses Systems. V ist eine Teilmenge von $\mathbb{F}_q^n$. Dann gilt:

$$0 \leq Card(v) \leq q^n$$

Ist

$$\sum_\alpha deg f_\alpha < n$$

dann gilt:

$$Card(V) \equiv 0 (mod\, p)$$

Beweis: Setze $P := \prod_\alpha (1 - f_\alpha^{q-1})$ und sei $x \in \mathbb{F}_q^n$. Wenn $x \in V$, dann sind alle $f_\alpha(x) = 0$ und

$$P(x) = 1$$

Ist $f_\alpha(x) \neq 0$ für ein α, also $x \notin V$, so ist

$$f_\alpha^{q-1}(x) = 1$$

also

$$1 - f_\alpha^{q-1}(x) = 0$$

damit ist

$$P(x) = 0$$

Daher ist P die charakteristische Funktion von V.
Daher gilt

$$S(P) \equiv Card(V)(mod\, p)$$

da

$$\begin{aligned} S(P) &= \sum_{x \in \mathbb{F}_q^n} P(x) \\ &= \sum_{x \in V} \overbrace{P(x)}^{=1} + \sum_{x \notin V} \overbrace{P(x)}^{=0} \\ &= Card(V) \cdot 1 + 0 \end{aligned}$$

Es bleibt noch zu zeigen, dass

$$\sum_{x \in \mathbb{F}_q^n} P(x) = 0$$

gilt.
Es ist

$$deg(1 - f_\alpha^{q-1}) \leq (q-1) \cdot (deg f_\alpha)$$

P ist nach Voraussetzung ein Polynom mit

$$\begin{aligned} degP &= \sum_{\alpha} deg(1 - f_{\alpha}^{q-1}) \\ &= \sum_{\alpha} (q-1)(deg\, f_{\alpha}) \\ &= (q-1) \cdot n \end{aligned}$$

Wir können daher P als Linearkombination von Monomen der Form

$$X^u = X_1^{\mu_1} \cdot ... \cdot X_n^{\mu_n} \quad \text{mit} \quad \mu_1 + ... + \mu_n < (q-1)n$$

schreiben.
Es ist in jedem dieser Monome mindestens ein $\mu_i < (q-1)$.
Nach Distributivgesetz gilt:

$$\sum_{x \in \mathbb{F}_q^n} X_1^{\mu_1} \cdot ... \cdot X_n^{\mu_n} = \Big(\sum_{x \in \mathbb{F}_q^n} X_1^{\mu_1} \Big) \cdot ... \cdot \Big(\sum_{x \in \mathbb{F}_q^n} X_n^{\mu_n} \Big)$$

Nach vorherigem Lemma ist mindestens einer dieser Faktoren gleich 0 und damit auch das Produkt. Und daher gilt:

$$\sum_{x \in \mathbb{F}_q^n} P(x) = 0 \quad \square$$

Korollar 1

Wenn $\sum_{\alpha} deg f_{\alpha} < n$ und wenn die f_{α} keinen konstanten Term haben, dann haben die f_{α} eine nichttriviale gemeinsame Null.

Beweis: Tatsächlich, wenn V auf $\{0\}$ reduziert wäre, wäre $Card(V)$ nicht teilbar durch p. Korollar 1 ist besonders dann anwendbar, wenn die f_{α} homogen sind.

Korollar 2

Alle quadratischen Formen mit mindestens drei Variablen über K haben eine nichttriviale gemeinsame Nullstelle.