Prof. Dr. K. Wingberg, Dr. O. Venjakob

Seminar: Quadratische Formen über den rationalen Zahlen

Sommersemenster 2004

Donnerstags, 14-16 MHS 3 (INF 288) Beginn: 22.04.2004

Anmeldung: ab sofort bei Otmar Venjakob, Zi. 107, INF 288,
otmar@mathi.uni-heidelberg.de

Text: J.P. Serre *A Course in Arithmetic* Ch.I - Ch. IV

Programm:
Seien n, ν positive ganze Zahlen.
Man sagt:

> "n ist Summe von ν Quadraten", falls n über $\mathbb{Z}$ darstellbar ist durch die quadratische Form $x_1^2 + \cdots + x_\nu^2$, d.h. es gibt $n_1, \ldots, n_\nu \in \mathbb{Z}$ derart, da"s $n = n_1^2 + \cdots + n_\nu^2$.

Lagrange: Jede positive ganze Zahl ist Summe von 4 Quadraten.

Ch.I Endliche Körper

Vortrag 1: §1, §2

Satz: Sei K ein endlicher Körper. Dann gibt es eine Primzahl p und ein $r \in \mathbb{N}$, so dass K genau $q = p^r$ Elemente besitzt. Zu jedem $q = p^r$ gibt es (bis auf Isomorphie) genau einen Körper mit q Elementen. Diesen Körper bezeichnet man mit $\mathbb{F}_q$.
Satz: $\mathbb{F}_q^\times$ ist eine zyklische Gruppe, d.h. es gibt ein $x \in \mathbb{F}_q^\times$, so dass $\mathbb{F}_q^\times = \{x, x^2, \ldots, x^{q-1}\}$.
Weiter werden Gleichungen über endlichen Körpern behandelt.

Vortrag 2: §3 Das quadratische Reziprozitätsgesetz.

Satz: a) Ist $p = 2$, so sind alle Elemente von $\mathbb{F}_q$ Quadrate.
b)Ist $p \neq 2$, so gilt:

$$\#\{x \in \mathbb{F}_q^\times \,|\, \exists y \in \mathbb{F}_q : y^2 = x\} = \frac{q-1}{2}$$

Definition: Sei $p \neq 2$, $x \in \mathbb{F}_p^\times$. Das Legendre Symbol $\left(\frac{x}{p}\right)$ ist definiert durch

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & x \text{ ist Quadrat} \\ -1 & \text{sonst.} \end{cases}$$

Es gilt:

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

Satz: Seien $l, p \neq 2$ Primzahlen. Dann gilt:

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\frac{l-1}{2}\frac{p-1}{2}}.$$

Zusatz:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Beispiel:

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1,$$

also ist 29 kein Quadrat mod 43.

Ch II
Vortrag 3 §1 §2: p-adische Zahlkörper
Sei p eine Primzahl. Betrachte die formalen Potenzreihen

$$\sum_{i=0}^{\infty} a_i \, p^i.$$

Diese bilden einen Ring $\mathbb{Z}_p$. Der Quotientenkörper

$$\mathbb{Q}_p = \{\frac{x}{y} | x, y \in \mathbb{Z}_p, y \neq 0\}$$

heißt Körper der p-adischen Zahlen.

Vortrag 4: §3
Die multiplikative Gruppe von $\mathbb{Q}_p$. Quadrate in $\mathbb{Q}_p^\times$.

Ch III
Vortrag 5: §1 Das lokale Hilbertsymbol
Sei $k = \mathbb{Q}_p$ oder $\mathbb{R}$.
Für $a, b \in k^\times$ setze:

$$(a, b) = \begin{cases} +1, & \text{falls } z^2 - ax^2 - by^2 = 0 \text{ eine Lösung } \neq (0,0,0) \text{ in } k^3 \text{ hat.} \\ -1, & \text{sonst.} \end{cases}$$

Eigenschaften. Berechnung in Termen des Legendre-Symbols.

Vortrag 6: §2 Das globale Hilbert-Symbol
Sei $k = \mathbb{Q}$. Es gibt Einbettungen $\mathbb{Q} \xrightarrow{i_p} \mathbb{Q}_p \, \forall \, p$, $\mathbb{Q} \xrightarrow{i_\infty} \mathbb{R}$.
Seien $a, b \in \mathbb{Q}^\times$. Setze $(a, b)_\nu = (i_\nu(a), i_\nu(b))$ für $\nu = p$ oder ∞.
Satz: $(a, b)_\nu = 1$ für fast alle ν. $\prod_\nu (a, b)_\nu = 1$.

Ch IV
Vortrag 7 §1:
Quadratische Formen (Wiederholung aus der lin. Algebra)
Quadratische Formen über $\mathbb{F}_q$

Vortrag 8: §2
Quadratische Formen über $\mathbb{Q}_p$, Klassifikation

Vortrag 9 §3
Quadratische Formen über $\mathbb{Q}$.(3.1,3.2)
Satz von Hasse-Minkowski: Sei $f = a_1 x_1^2 + \cdots a_n x_n^2$, $a_i \in \mathbb{Q}^\times$ eine quadratische Form und f_ν ($\nu = p, \infty$) die entsprechende Form, wenn man a_i unter i_ν als Element von $\mathbb{Q}_\nu$ bzw. $\mathbb{R}$ auffaßt. Dann gilt:
f stellt 0 dar $\Longleftrightarrow$ f_ν stellt 0 dar für alle $\nu = p, \infty$.

Vortrag 10 §3.3
Klassifikation, Summe von 3 Quadraten, Satz von Lagrange.

Die letzten beiden Vorträge behandeln Formen in vielen Variablen von beliebigem Grad. Literatur: M. J. Greenberg, "' Lectures on Forms in many variables"'

Vortrag 11: aus der Einleitung (Ch. 1) die Definition einer Form in n Variablen vom Grad d, S. 1 (und alles was sonst interessant erscheint aus der Einleitung) zur Motivation erzählen, Definition 1.1, Def. von zentralen Divisionsalgebren und Beweis von Theorem 1.3, Def. 1.4., Ziel des Vortrags ist der Beweis des Satzes 2.3 von Chevalley-Warning, der besagt, dass endliche Körper C_1 sind.

Vortrag 12: Chapter 3 aus obigem Buch: Ziel ist der Beweis einer Verallgemeinerung von Tsen's Theorem: Ist k C_i und K ein Funktionenkörper über k in j Variablen, dann ist K C_{i+j}, Thm. 3.6.