Dr. J. M. Cerviño, Prof. G. Böckle 20. Mai 2008

Proseminar/Seminar im SS2008 (Mathematik, Diplom, Lehramt):

Quadratische Formen

Zeit und Ort: Fr. 10-12, Raum T03 R02 D26

Dieses Seminar dient als Einführung in die (arithmetische) Theorie der *quadratischen Formen*. Zunächst werde ich kurz erläutern, was ich mit "Einführung in die arithmetische Theorie der quadratischen Formen" meine.

Dass es eine "Einführung" ist, heißt nur, dass dieses Seminar nicht mehr, aber auch nicht weniger, voraussetzt, als Kenntnisse in der linearen Algebra (d.h. Themen der linearen Algebra I und II). An manchen Stellen sind weitere Kenntnisse in der Algebra/elementarer Zahlentheorie hilfreich, aber *nicht* notwendig.

Unser Musterproblem in der "Theorie der quadratischen Formen" stelle ich jetzt vor. Daran erläutere ich, worauf sich das Wort "arithmetisch" bezieht.
Sei

$$f(x_1, x_2, \ldots, x_n) := \sum_{1 \leq i,j \leq n} a_{i,j} x_i x_j$$

eine Funktion in n-Variablen, wobei alle $a_{i,j}$ ganze Zahlen sind (f heißt *(ganzzahlige) quadratische Form*). Unser Musterproblem ist Gleichungen der Form

$$f(x_1, \ldots, x_n) = t \tag{1}$$

zu untersuchen, mit t eine beliebige ganze Zahl.

Das Wort "arithmetisch" deutet auf eine interessante Einschränkung des obigen Problems hin; nämlich, man ist nur an *ganzzahligen Lösungen* von (1) interessiert - solche Gleichungen sind als *Diophantische Gleichungen* bekannt. Dieses Wort steht im ersten Satz zwischen Klammern, weil wir aus Zeitgründen nicht so weit kommen werden. Es soll auf eine wirklich interessante Fragestellung aufmerksam machen. Warum dies eine nicht triviale Einschränkung des Problems darstellt, zeigt folgendes Beispiel: sei

$$f(x_1, x_2) := 2x_1^2 + x_1 x_2 + 3x_2^2 = 1. \tag{2}$$

Diese Gleichung hat (mehr als) eine rationale Lösung, allerdings keine Ganzzahlige (zeigen Sie es durch eine quadratische Ergänzung; eine rationale Lösung haben Sie sicherlich schnell gefunden, oder?).

Das thematische **Ziel des Seminars** ist das sogenannte **Lokal-global-Prinzip** (auch Hasse-Prinzip genannt), ein in der modernen Mathematik zentrales Konzept. Grob gesagt, es ist nichts anderes als ein Algorithmus, der sagt, wann eine Zahl durch eine (reguläre) rationale quadratische Form *rational* darstellbar ist. Algorithmus heißt insbesondere, dass er aus endlich vielen Schritten besteht! Im letzten Vortrag werden alle im Seminar aufbauend gewonnenen Kenntnisse zusammengebündelt.

Als Literatur werden wir [Se], aber auch [BoSha], folgen.

Bemerkung 1: Auch wenn das nicht in jedem Vortrag explizit gesagt wird, sollte jeder Vortrag mindestens ein sinnvolles, motivierendes und **konkretes Beispiel** enthalten.

Bemerkung 2: Die Vorbereitung **soll/muss** eine Woche vor dem eigentlichen Vortrag zum größten Teil abgeschloßen sein. Um dies zu gewährleisten, und zugunsten aller Teilnehmer, wird jeder gebeten, sich eine Woche vor dem Vortrag mit einem *vollständigen* Entwurf bei mir zu melden, um den Vortrag durchzusprechen und eventuell Lücken zu schließen.

Bemerkung 3: *Jeder* Teilnehmer sollte folgendes als Ziel bei diesem Seminar haben:

- den Vortrag schön, klar strukturiert und verständlich halten, und
- an den anderen Vorträgen teilhaben und sich aktiv mitbeteiligen, damit wir alle zusammen die Vorträge bis zum Ende verstehen.

Den ersten Punkt erreicht man, indem man sich rechtzeitig mit dem Stoff des Vortrages befasst (mindestens drei Wochen vor dem Termin - nicht vergessen, dass eine Woche davor der Vortragsentwurf fertig sein soll), den Stoff versteht, die eine oder zwei wichtigsten Aussagen des Vortrages gut verstanden hat, und schließlich darüber für den Vortrag schreibt. Hier werde ich sie unterstützen: ich werde dafür wöchentlich zwei Sprechstunden anbieten (die Zeiten werden wir zusammen vereinbaren).

Beim zweiten Punkt kann ich nur in einer Seminarveranstaltung an Ehrlichkeit bzw. an Verantwortung mit sich selbst appellieren. Die Mühe zählt sich am Ende natürlich aus!

Bemerkung 4: Diese Veranstaltung gilt als Proseminar/Seminar. Die Proseminar- bzw. Seminarscheine werden nach folgenden Kriterien vergeben:

- für *Proseminarschein* wird ein Vortrag gehalten (wie? s.o.);
- für *Seminarschein* werden zwei Vorträge gehalten (wie? s.o.) und es wird eine Ausarbeitung derer (in LaTeX) abgegeben. Die Ausarbeitungen sind bis zum 03.08.08 abzugeben.

1 Endliche Körper

In diesem ersten Vortrag studieren wir endliche Körper. Man beweise, die multiplikative Gruppe eines solchen ist zyklisch, und den Satz von Chevalley-Warning mit seinen Folgerungen.

Literatur: [Se, Chapter I, §1 und §2]. Das erste Kapitel von [BoSha] ist hierfür auch sehr empfehlenswert.

Vortragender: Lars Adam, 11.04.08

2 Eulers Untersuchungen: $x^2 + ny^2$ für $n = 1, 2, 3$

Hier studieren wir für welche Primzahlen p ist die Gleichung $p = x^2 + ny^2$ mit ganzzahligen Koeffizienten lösbar (n gleich $1, 2$ oder 3 fest). Z.B. im Falle $n = 1$ ist die obige Gleichung ganzzahlig lösbar, genau dann, wenn $p \equiv 1 \pmod 4$ (d.h. nach der Division von p durch 4 bleibt 1 als Rest).
Man beweise die Aussagen (vgl. Literatur) für die Fälle $n = 1, 3$ vollständig. Die zwei Schritte der allgemeinen Strategie der Beweise, *Abstieg* und *Reziprozität* müssen gesprochen werden.

Literatur: [Cox, Theorem 1.2 und Exercises 1.4, 1.5].

Vortragende: Maren Kier, 18.04.08

3 $p = x^2 + ny^2$ und quadratische Reziprozität

Wir bringen den Reziprozitätsschritt und Legendres Symbol in Verbindung (vgl. [Cox, §1.C]). Konkret, man beweise die Aussage der Übung 1.9 op.cit. und bringe dies in Verbindung mit dem Reziprozitätsgesetz. Das muss auch bewiesen werden, siehe [Se, Chapter I, §3].

Literatur: [Cox] und [Se, Chapter I, §3].

Vortragende: Hélène Schenke, 25.04.08

4 Reduktionstheorie positiv definiter binärer quadratischer Formen

Dies ist [Bue, Chapter 2] bis Theorem 2.6, einschließlich vieler Beispiele. Theoreme 2.5 und 2.6 sind die Hauptaussagen. Am Ende sollte wenigstens der Fundamentalbereich von $\mathrm{SL}_2(\mathbb{Z})$ und die Bedeutung der Reduktionstheorie anhand dieses Bereiches [Bue, Proposition 2.7] erläutert werden.

Literatur: [Bue, Chapter 2].

Vortragender: Michael Matuschek, 02.05.08

5 p-adische Zahlen

Man erkläre die Konstruktion der p-adischen (ganzen) Zahlen erst einmal so, wie im letzten Absatz von [Se, Chapter II, §1.2] (vgl. [BoSha, Chapter I, §3]). Dann erläutere man die Konstruktion des projektiven Limes und seine Eigenschaften.
Das einfache Theorem 7 in [BoSha] und seine wichtige Folgerungen sollen gezeigt werden. Beispiele sind hier erwünscht, wo es klar wird, dass $\mathbb{Q}$ bzgl. der p-adischen Normen unvollständig ist - so, wie am Anfang des Paragraphes [BoSha, Chapter 1, §3] "gezeigt" wird, dass $\sqrt{2} \in \mathbb{Q}_7$ (einen kompletten Beweis dafür werden wir aber im nächsten Vortrag bekommen, mithilfe des Hensel-Lemmas).

Literatur: [Se, Chapter II, §1] und [BoSha, Chapter 1, §3].

Vortragender: wird von den Organisatoren übernommen, 09.05.08

6 Hensels Lemma

Wie aus letztem Vortrag klar wird, naïves Rechnen in $\mathbb{Q}_p$ ist nicht so trivial (beweise, dass $\sqrt{2} \in \mathbb{Q}_7$), da es im Prinzip unendlich viele Schritte bevorstehen. Hensels Lemma zeigt uns, dass man mit endlich vielen ans Ziel kommt (und zwar mit sehr wenigen...!).

Literatur: [Se, Chapter II, §2] oder/UND [BoSha, Chapter 1, §5.2].

Vortragender: Simon Zander, 16.05.08

7 Die Multiplikative Gruppe $\mathbb{Q}_p^\times$ und deren Quadrate

Man gebe eine explizite Beschreibung der Gruppen $\mathbb{Q}_p^\times$ und $\mathbb{Q}_p^{\times 2}$ und man berechne $\mathbb{Q}_p/\mathbb{Q}_p^{\times 2}$. Theorem 5 von [BoSha, Chapter 1, §6] ist eine nennenswerte unmittelbare Folgerung.

Literatur: [Se, Chapter II, §3] und [BoSha, Chapter 1, §6.1] (beide ergänzen sich sehr gut).

Vortragender: Oliver Schulte, 23.05.08

8 Hilbert-Symbol

Wir nehmen unser Hauptproblem über den p-adischen Zahlen wieder auf, und studieren es für kleinere Ränge ($m = 1, 2, 3$). Im wesentlichen haben wir schon Rang 1 und 2 gemacht, werden aber hier die Resultate zusammenfassen. Dann konzentrieren wir uns auf den Rang 3 Fall. Dafür definieren wir hier das Hilbert-Symbol [Se, Chapter III, §1.1] und rechnen es aus (§1.2 loc.cit). Der Beweis für Theorem 1 soll für den Fall $p \neq 2$ geführt werden (Fall $p = 2$ kommt im nächsten Vortrag).

Literatur: [Se, Chapter III, §1].

Vortragender: Benjamin Otto, 30.05.08

9 Produktformel

Man beende den Beweis vom letzten Vortrag ($p = 2$, s.o.) und beweise die Produktformel [Se, Chapter III, §2, Theorem 3].

Literatur: [Se, Chapter III, §2] und [BoSha, Seiten 66–67].

Vortragender: Benjamin Otto, 06.06.08

10 Symmetrische Bilinearformen, Quadratische Formen

Bisher haben wir außer $\mathbb{Z}$ und $\mathbb{Q}$ noch $\mathbb{Z}_p$, dessen Quotientenkörper $\mathbb{Q}_p$ und den Restklassenkörper $\mathbb{F}_p$ (und endliche Erweiterungen davon) kennengelernt.
In diesem Vortrag geben wir die grundlegenden Definitionen, Beispiele und beweisen wir einen Satz [Kneser, Satz (1.20)] über die Zerlegung von symmetrischen Bilinearformen bzw. quadratischen Formen (da wir uns für Charakteristik ungleich 2 interessieren, entsprechen sich die symmetrischen Bilinearformen mit den quadratischen Formen eins zu eins - das muss auch angegeben werden). Hier lernen wir aber auch, dass über Körpern der Charakteristik 2, die quadratischen Formen i.A. nicht diagonalisiert werden können.
In dem Buch soll R als ein Körper verstanden werden und demnach ist der Begriff *Modul* durch *Vektorraum* (endlicher Dimension, versteht sich) zu ersetzen.

Literatur: [Kneser, Kapitel I, §§1 und 2], [Se, Chapter IV, §§1.1–1.4].

Vortragender: Patrick Elfert, 13.06.08

11 Die orthogonale Gruppe und der Satz von Witt

Das ist [Kneser, Kapitel I, §3] - setze durchweg voraus, dass die Charakteristik ungleich 2 ist. Man beachte, dass diese Einschränkung den Paragraph §3 wesentlich kürzer macht. Außerdem beweise man den Satz von Cartan-Dieudonné [Dieu, Proposition 8].

Literatur: [Kneser, Kapitel I, §3] und [Dieu].

Vortragende: Felicia Kalhoff, 20.06.08

12 Folgerungen. Quadratische Formen über $\mathbb{F}_q$

Man ziehe Folgerungen aus den vorherigen Resultaten und studiere quadratische Formen über endlichen Körpern.

Literatur: [Se, Chapter IV, §§1.6 und 1.7].

Vortragende: Matthias Austrup, 27.06.08

13 Quadratische Formen über $\mathbb{Q}_p$: Teil I

Ziel des Vortrages ist es, die Invariante ε zu definieren und ein notwendiges und hinreichendes Kriterium anzugeben, wann eine beliebige quadratische Form über $\mathbb{Q}_p$ die Null nicht trivial darstellt [Se, Chapter IV, §2.2, Theorem 6].

Literatur: [Se, Chapter IV, §§2.1 und 2.2].

Vortragender: Lars Adam, 04.07.08

14 Quadratische Formen über $\mathbb{Q}_p$: Teil II

Man beweise das endgültige Klassifikationstheorem für quadratische Formen über den p-adischen Zahlen (damit auch über den Reellen).

Literatur: [Se, Chapter IV, §§2.3 und 2.4].

Vortragender: Marius Jähme, 11.07.08

15 Minkowski-Hasse: das Lokal-global-Prinzip für rationale quadratische Formen

Das ist der Höhepunkt unseres Seminars [Se, Chapter IV, §3.2, Theorem 8]. Eine Formulierung ([Kneser, Kapitel VI, §19]):

Sie (V, q) eine rationale reguläre quadratische Form, und t eine rationale Zahl (ungleich Null). Dann gilt $t \in q(V)$, genau wenn $t \in q(V_p)$ für alle Stellen p (d.h. alle Primzahlen und $p = \infty$).

Literatur: [Se, Chapter IV, §§3.1 und 3.2] (vgl. auch [BoSha, Chapter 1, §§7.1–7.4] und [Kneser, Kapitel VI, §19]!).

Vortragender: Oliver Schulte, 18.07.08

Literatur

[BoSha] Z.I. Borevitch und I.R. Shafarevich, *Number theory*, Academic Press 1966.

[Bue] D.A. Buell, *Binary quadratic forms*, Springer Verlag 1989.

[Cox] David Cox, *Primes of the form* $x^2 + ny^2$, John Wiley and Sons 1989.

[Dieu] Jean Dieudonné, *Sur les groupes classiques*, Actualités Scientifiques et Industrielles 1040, Hermann 1958.

[Kneser] Martin Kneser, *Quadratische Formen*, Springer Verlag 2002.

[Se] J.-P. Serre, *A course in arithmetic*, Springer 1996.