INFORMATIONEN ZUR VERANSTALTUNG ALGORITHMISCHE ZAHLENTHEORIE WINTERSEMESTER 2014/15

STEFFEN MÜLLER
INSTITUT FÜR MATHEMATIK
CARL VON OSSIETZKY UNIVERSITÄT OLDENBURG

Zeit und Ort

- Die Vorlesung findet jede Woche Montags um 12 Uhr c.t. sowie alle 2 Wochen Dienstags um 12 Uhr c.t. statt.
- Die Übung findet alle 2 Wochen Dienstags um 12 Uhr c.t. statt.
- Veranstaltungsort ist der Raum W01 1-012.

Vorkenntnisse

Die Inhalte der Veranstaltungen Algebra I und II sowie des Vertiefungsmoduls Zahlentheorie und Computeralgebra werden vorausgesetzt. Falls Sie letzteres nicht besucht haben, aber dennoch an der Veranstaltung teilnehmen wollen, melden Sie sich bitte möglichst bald per E-Mail bei mir.

Inhalt

In dieser Vorlesung werden wir uns hauptsächlich mit der algorithmischen Invariantenberechnung von Zahlkörpern beschäftigen, d.h. mit algorithmischer algebraischer Zahlentheorie. Diese hat etliche Anwendungen, z.B. auf die explizite Lösung sog. *diophantischer Gleichungen*.

Ein *Zahlkörper* K ist eine endliche Körpererweiterung der rationalen Zahlen $\mathbb{Q}$. Diejenigen Elemente von K, deren Minimalpolynome ganzzahlige Koeffizienten haben, bilden einen Unterring von K; dieser wird *Ganzheitsring* oder *Maximalordnung* von K genannt und mit $\mathcal{O}_K$ bzw. $\mathbb{Z}_K$ bezeichnet. Dieser Ring hat endlich erzeugte Einheitengruppe und eine natürliche Struktur als freier $\mathbb{Z}$-Modul. Die Beziehung von $\mathcal{O}_K$ zu K verallgemeinert die Beziehung von $\mathbb{Z}$ zu $\mathbb{Q}$, insbesondere ist K der Quotientenkörper von $\mathcal{O}_K$. Allerdings ist $\mathcal{O}_K$ i.A. kein Hauptidealring und auch kein faktorieller Ring. In diesem Zusammenhang ist die *Klassengruppe* von K wichtig. Diese Gruppe ist stets endlich und ist z.B. trivial g.d.w. $\mathcal{O}_K$ ein Hauptidealring ist.

Beispiel 0.1. Sei i eine Nullstelle des Polynoms x^2+1. Dann ist $K = \mathbb{Q}(i)$ ein Zahlkörper. Sein Ganzheitsring ist $\mathbb{Z}[i]$, der Ring der Gaußschen Zahlen, dessen Einheitengruppe die Elemente $\pm 1, \pm i$ hat. Die Klassengruppe ist trivial, d.h. $\mathbb{Z}[i]$ ist ein Hauptidealring. Hiermit lässt sich z.B. zeigen, dass die einzige ganzzahlige Lösung der diophantischen Gleichung

$$y^2 = x^3 - 1$$

von der Form $(x, y) = (1, 0)$ ist. Der Ring $\mathbb{Z}[i]$ ist darüber hinaus ein euklidischer Ring, also insbesondere ein faktorieller Ring. Dies kann man z.B. benutzen, um zu zeigen, dass sich jede Primzahl $p \equiv 1 \pmod 4$ als Summe zweier ganzzahliger Quadrate schreiben lässt.

Wir werden die oben angeführten Aussagen beweisen und u.a. Algorithmen für folgende Probleme behandeln:

- Arithmetik in K

- Berechnung einer Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul
- Idealarithmetik in $\mathcal{O}_K$ (allgemeiner Arithmetik gebrochener Ideale)
- Berechnung von Erzeugern der Einheitengruppe $\mathcal{O}_K^\times$
- Berechnung der Klassengruppe von K
- Algorithmische Lösung gewisser diophantischer Gleichungen

Viele der in der Vorlesung behandelten Algorithmen lassen sich analog für *globale Funktionenkörper*, also Erweiterungen eines endlichen Körpers $\mathbb{F}_q$ vom Transzendenzgrad 1 verwenden. Wir werden auf die Invariantenberechnung dieser u.a. in Geometrie, Kodierungstheorie und Kryptographie wichtigen Körper gelegentlich eingehen, uns aus Zeitgründen aber hauptsächlich auf den Zahlkörperfall beschränken.

Übungen

Es wird insgesaamt 7 Aufgabenblätter geben, welche jeweils ca. 3–5 Aufgaben enthalten. Idealerweise bearbeiten Sie diese in Kleingruppen, ihre Lösungen geben Sie entweder alleine oder in Paaren ab. Diese werde ich zur nächsten Übung korrigiert zuückgeben.

In den Übungen sollen Lösungen der wichtigsten Aufgaben vorgestellt werden. Sollten sich für eine dieser Aufgaben keine Freiwilligen melden, werde ich versuchen, mit Ihnen gemeinsam zu einer Lösung zu gelangen oder Teilnehmer, die eine Lösung der betreffenden Aufgabe abgegeben haben, zur Präsentation auffordern. Die restliche Zeit werden wir uns entweder mit Präsenzaufgaben beschäftigen oder ich werde Inhalte, die wir in der Vorlesung nicht behandeln können, vorstellen.

Sage

Da die Vorlesung eine starke algorithmische Komponente hat, werde ich auch Aufgaben stellen, die am Computer zu bearbeiten sind. Hierfür werden wir das Computeralgebrasystem `Sage` verwenden. Es ist keine lokale Installation erforderlich, da wir die Cloud-Lösung `SageMathCloud (SMC)` verwenden werden, siehe `http://cloud.sagemath.com`. Ich werde dort einen eigenen Bereich für den Kurs anlegen, für den Sie eine Einladung per E-Mail erhalten werden. Bitte richten Sie sich zunächst einen Account auf `SMC` ein, wobei Sie bitte Ihre Universitäts-E-Mail-Adresse verwenden. Unter `http://sagemath.org/pdf/de/tutorial/SageTutorial-de.pdf` finden Sie eine Einführung in `Sage`.

Es wird sowohl reine Anwendungsaufgaben, in denen Sie konkrete Fragestellungen mithilfe der in `Sage` implementierten Funktionalität lösen sollen, als auch Programmieraufgaben geben. `Sage` basiert auf der Programmiersprache `Python`, weshalb Sie sich für die Programmieraufgaben wenigstens rudimentäre Kenntnisse in `Python` aneignen sollten. Im Kursbereich auf `SMC` werde ich Links zu Einführungen in `Sage`, `SMC` und `Python` zur Verfügung stellen.

Prüfung

Die Prüfungsleistung besteht aus einer mündlichen Prüfung, welche ca. 30-40 Minuten dauern wird. Die Prüfungen werden zwischen dem 18.2.2015 und dem 27.2.2015 stattfinden, bitte melden Sie sich möglichst frühzeitig bei mir, falls Sie in diesem Zeitrahmen keinen Termin wahrnehmen können.

Sofern es unter den Teilnehmern keine Einwände gegen diese Regelung gibt, können Sie durch die Übungen Bonuspunkte für die mündliche Prüfung erwerben:

- 1 Notensprung: 50% der Punkte in den Hausübungen, 50% der Punkte in den `Sage`-Aufgaben, aktive Mitarbeit und mindestens 2-maliges Vorrechnen
- 2 Notensprünge: 75% der Punkte in den Hausübungen, 75% der Punkte in den `Sage`-Aufgaben, aktive Mitarbeit und mindestens 3-maliges Vorrechnen

Hierbei ist ein Notensprung die kleinste mögliche Verbesserung, also z.B. von 2.0 auf 1.7. Ich behalte mir vor, ggfs. die Präsentation einzelner abgegebener Aufgaben zu verlangen.

In der Prüfung werde ich Inhalte sowohl der Vorlesung als auch der Übung abfragen. Ich erwarte, dass Sie die Definitionen, Resultate und Algorithmen der Vorlesung beherrschen. Außerdem sollten Sie in der Lage sein, die Idee und grobe Struktur der Beweise der Sätze der Vorlesung wiederzugeben. Schließlich werde ich auch testen, ob Sie den in der Vorlesung und der Übung vermittelten Stoff auf konkrete Fragestellungen anwenden können.

Sprechstunde

Meine Sprechstunde ist Mittwochs von 11-12 Uhr. Sie können mir aber auch jederzeit per E-Mail oder i.d.R. nach den Vorlesungen Fragen stellen.

Skript

Ich werde ein Kurzskript zur Vorlesung erstellen, welches allerdings keine Beweise, Motivation o.ä. enthalten und zudem vermutlich nicht immer aktuell sein wird. Es ersetzt keinesfalls den Besuch der Vorlesung oder der Übung. Das Kurzskript wird sich in folgende Abschnitte gliedern:

(I) Moduln und Normalformen
(II) Zahlkörper und Ganzheit
(III) Berechnung der Maximalordnung
(IV) Gitter
(V) Einheiten
(VI) Dedekindringe, Klassengruppen und Primidealzerlegung in Erweiterungen
(VII) Berechnung von Klassengruppen
(VIII) Anwendungen auf diophantische Gleichungen

Literatur

Alle Quellen sind online verfügbar, wobei Sie für manche Quellen im Netzwerk der Universität angemeldet sein müssen. Auf meiner Profilseite bei Stud.IP finden Sie die Links. Wir werden uns für (I)–(VII) hauptsächlich an den Skripten von Fieker und Wildanger orientieren. Literatur für (VIII) wird noch nachgereicht.

- C. Fieker: *Algorithmic number theory*, Skript, TU Kaiserslautern (2014). Gut geschrieben und mit algorithmischem Fokus, aber z.Zt. noch etwas fehlerhaft. Die behandelten Themen decken sich stark mit denen der Vorlesung. Baut auf dem Skript von Wildanger auf.
- K. Wildanger: *Konstruktive Zahlentheorie*, Skript, Uni Düsseldorf (1993). Enthält (fast) alle in (I)–(VII) behandelten theoretischen und algorithmischen Ergebnisse.
- W. Stein: *Algebraic number theory, a computational approach* (2010). Kostenlos online verfügbares Lehrbuch, enthält die in (I)–(VII) vorgestellte Theorie, aber nicht alle Algorithmen, dafür viele `Sage`-Beispiele.
- H. Cohen: *A course in computational algebraic number theory*, Springer (1993). Enthält wohl alle von uns in (I)–(VII) behandelten Algorithmen, aber kaum Beweise oder Beispiele.
- D. Marcus, *Number fields*, Springer (1977). Recht elementare Einführung in die algebraische Zahlentheorie, ohne Algorithmen, dafür mit sehr vielen Beispielen.
- J. Neukirch: *Algebraische Zahlentheorie*, Springer (1992). Modernes Buch zur abstrakten algebraischen Zahlentheorie, sehr gut geschrieben, aber nicht leicht zu verdauen.