Seminar Quadratische Zahlringe
* Themenliste *

K. Halupczok

Math. Institut, WWU Münster, Sommersemester 2013

Inhaltsverzeichnis

Allgemeine Bemerkungen

Alle Literaturangaben, wenn nicht näher erläutert, beziehen sich auf das in der Seminarankündigung angegebene Skript von F. Lemmermeyer [1].

Ergänzungen finden Sie im Buch von O. Forster, Algorithmische Zahlentheorie [2], oder bei grundlegenden Fragen zur elementaren Zahlentheorie auch in meinem alten Skript [3].

Die Lösungen der Übungen, die im Vorbereitungstext vorkommen und wesentlich zum Verständnis des Themas sind, sollen im Vortrag vorgestellt werden. Ausdrücklich wird auch empfohlen, selbständig nach sinnvollen Ergänzungen in der Literatur zu suchen und vorzubereiten.

Themenliste

1 Quadratische Zahlringe

§ 1.4, S. 8–11 (als Einführung)

- quadratische Zahlkörper
- Norm, Spur und Diskriminante
- Galoisgruppe quadratischer Erweiterungen (von $\mathbb{Q}$)
- Ganzheitsring (Maximalordnung), Ganzheitsringe quadratischer Zahlkörper heißen quadratische Zahlringe
- Ganzheitsbasis

2 Teilbarkeit in Integritätsringen

§ 2.1, S. 12–16

- Einheiten, Assoziierte
- prime und irreduzible Elemente
- Teilbarkeit und Kongruenzen
- Primelemente sind irreduzibel
- Elemente mit Primnorm sind prim

3 ZPE-Ringe und Hauptidealringe

§ 2.2 und 2.3, S. 17–20

- in ZPE-Ringen gilt: irreduzible Elemente sind prim
- ZPE-Ringe $\supseteq$ Hauptidealringe $\supseteq$ euklidische Ringe
- In ZPE-Ringen existiert ein ggT, in Hauptidealringen existieren sogar Bezout-Elemente

4 Euklidische Ringe und Euklidischer Algorithmus

§ 2.4, S. 21–23, Zusatz: [2, § 4, S. 26–27]

Algorithmische Bestimmung des ggT und von Bezout-Elementen

- Der Berlekamp-Algorithmus
- Komplexitätsanalyse des Berlekamp-Algorithmus'

5 Bsp. quadr. ZR: Die Gaußschen Zahlen

§ 3.1, S. 27–32

- $\mathbb{Z}[i]$ ist ein normeuklidischer Ring
- Primelemente und Assoziierte in $\mathbb{Z}[i]$, Zerfall von Primzahlen
- Quadratische Reste in $\mathbb{Z}[i]$

6 Bsp. quadr. ZR: Die Eisensteinschen Zahlen

§ 3.2, S. 32–34 oben und S. 34–35 (Fermatglg. 3. Grades)

- $Z[\rho]$ ist ein normeuklidischer Ring
- Primelemente und Assoziierte in $\mathbb{Z}[\rho]$, Zerfall von Primzahlen
- Unlösbarkeit der Fermatgleichung 3. Grades in $\mathbb{Z}[\rho]$ und $\mathbb{Z}$

7 Die Pellsche Gleichung

§ 3.4, S. 38–40 und freiwillige Ergänzungen aus [2, § 25]

- Die Pellsche Gleichung $x^2 - my^2 = 1$ ist für jede quadratfreie natürliche Zahl nichttrivial lösbar
- Die Einheitengruppe reellquadratischer Zahlkörper ist $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$, Fundamentaleinheiten
- Freiwillig: Fundamentaleinheiten bzw. Lösungen der Pellschen Gleichung können mit einem Kettenbruchalgorithmus bestimmt werden

8 Idealarithmetik in quadratischen Zahlringen: I

§ 4.1, S. 49–51 und § 4.2, S. 51–53

- Motivation und Idealnorm
- Ideale in quadratischen Zahlringen bilden eine Halbgruppe mit Kürzungsregel

9 Idealarithmetik in quadratischen Zahlringen: II

§ 4.2, S. 53–56

- Eindeutige Primidealzerlegung in quadratischen Zahlringen
- Rationale Primzahlen sind in einem quadratischen Zahlring verzweigt, zerlegt oder träge, je nachdem ob $(d/p) = 0$, $+1$ oder -1 ist

10 Idealarithmetik in quadratischen Zahlringen: III

§ 4.3, S. 56–60

- Die Idealklassengruppe: Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen äquivalent, wenn es $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ gibt mit $\alpha\mathfrak{a} = \beta\mathfrak{b}$.
- Die Aquivalenzklassen von Idealen bilden eine Gruppe, die Idealklassengruppe.
- Die Idealklassengruppe eines quadratischen Zahlringes ist endlich.

Literatur

[1] F. Lemmermeyer, Quadratische Zahlkörper Schnupperkurs `http://www.rzuser.uni-heidelberg.de/~hb3/publ/qzk.pdf`

[2] O. Forster, Algorithmische Zahlentheorie, Vieweg Lehrbuch Mathematik, 1996

[3] K. Halupczok, Manuskript zur Vorlesung Elementare Zahlentheorie, Sommersemester 2009 (Freiburg), `http://wwwmath.uni-muenster.de/u/karin.halupczok/ElZthSS2009Skript.pdf`