Übungen zur Vorlesung Algebraische Zahlentheorie

Sommersemester 2007 Blatt 2

W.Knapp Tübingen, den 5. April 2007

4. Es bezeichne $R = \mathbb{Z}[i]$ den Ring der Gaußschen Zahlen. Sei π ein Primelement von R. Beweisen Sie:
   (a) Es gibt genau eine Primzahl p in $\mathbb{Z}$ mit $\pi R \cap \mathbb{Z} = p\mathbb{Z}$.
   (b) Falls π zu $1+i$ assoziiert ist, gilt $R = \pi R + \mathbb{Z}$, $\pi R \cap \mathbb{Z} = 2\mathbb{Z}$ und $R/\pi R \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. Hierbei gilt $2\mathbb{Z} \subsetneqq 2R = \pi^2 R \subsetneqq \pi R$.
   (c) Falls π zu einer Primzahl p in $\mathbb{Z}$ assoziiert ist mit $p \equiv 3 \pmod 4$, so gilt $R/\pi R \cong \mathbb{F}_{p^2}$.
   (d) Falls π zu $a+bi$ assoziiert ist, wobei $a, b \in \mathbb{Z}$, $0 < |b| < a$ und $p = a^2 + b^2$ eine ganzrationale Primzahl ist mit $p \equiv 1 \pmod 4$, gilt $\pi R \cap \mathbb{Z} = p\mathbb{Z}$, $R = \pi R + \mathbb{Z}$ und $R/\pi R \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

(12 Punkte)

5. Es sei $K := \mathbb{Q}(\sqrt{5}) \subset \mathbb{R}$ und $\theta = \frac{1}{2}(1+\sqrt{5})$. Setze $R := \mathbb{Z}[\theta]$ und $S := \mathbb{Z}[\sqrt{5}]$ als Teilringe von K. Wir betrachten die Ringe R und S als $\mathbb{Z}$-Moduln.
   (a) Beweisen Sie, dass $X^2 - X - 1$ das Minimalpolynom von θ über $\mathbb{Q}$ ist.
   (b) Beweisen Sie, dass R ein freier $\mathbb{Z}$-Modul vom Rang 2 ist und S ein Untermodul von R.
   (c) Bestimmen Sie eine $\mathbb{Z}$-Basis (b_0, b_1) von R und ein Paar ganzrationaler Zahlen (a_0, a_1) derart, dass $(a_0 b_0, a_1 b_1)$ eine $\mathbb{Z}$-Basis von S ist mit $a_0 | a_1$. Was ist der Index $|R : S|$ im Sinne der Gruppentheorie?

(8 Punkte)

6. Bestimmen Sie Primitivwurzeln (d.h. Erzeugende der multiplikativen Gruppe) für die endlichen Körper $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_8$, $\mathbb{F}_9$ und $\mathbb{F}_{16}$.

7. Über welchen endlichen Körpern $\mathbb{F}_{p^m}$ ist das Polynom $X^2 + 1$ irreduzibel, über welchen reduzibel?
   (Geben Sie notwendige und hinreichende Anforderungen an die Primzahl p und den Ordnungsexponenten m an.)

Die Übungsaufgaben 4 und 5 sind schriftlich zu bearbeiten und vor der Vorlesung am Mittwoch, dem 2. Mai 2007, abzugeben.