Universität Karlsruhe
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein
Petra Forster

25.06.2008

Elementare Zahlentheorie – Übungsblatt 11

Aufgabe 1 (4 Punkte)

Sei $d < 0$ quadratfrei, $d \equiv 1 \mod 4$, $K = \mathbb{Q}(\sqrt{d})$. Sei weiter $-d \notin \mathbb{P}$ und p ein Primteiler von d. Zeigen Sie:

(a) p ist nicht die Norm eines Elementes aus O_K.

(b) O_K ist kein Hauptidealring.

Aufgabe 2 (4 Punkte)

Sei $A \in \mathbb{Z}^{2\times 2}$, $A^2 = dI_2$, $d \in \mathbb{Z}$ kein Quadrat.

(a) Zeigen Sie:
$\mathrm{Spur}(A) = 0$ und $\det(A) = -d$.

(b) Sei $A = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \in \mathbb{Z}^{2\times 2}$ mit $a^2 + bc = d$.
Zeigen Sie, dass $\mathbb{Z}c + \mathbb{Z}(\sqrt{d} - a)$ ein Ideal in $\mathbb{Z}[\sqrt{d}]$ ist und die Multiplikation mit $\sqrt{d}$ bezüglich einer geeigneten Basis durch A beschrieben wird.

Aufgabe 3 (4 Punkte)

Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 1$, $K = \mathbb{Q}(\sqrt{d})$ mit Diskriminante D_K. Weiter sei O_K der Ganzheitsring von K und $I \subseteq O_K$ ein Ideal mit $\mathrm{ggT}(N(I), D_K) = 1$. Zeigen Sie:

$$[\exists g \in \mathbb{Z} : I = gO_K] \Longleftrightarrow I = \kappa(I)$$

wobei κ der Automorphismus aus der Vorlesung ist.

Aufgabe 4 (4 Punkte)

Sei $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$, $\epsilon = 2 + \sqrt{3}$ und $r_k := \epsilon^{2^{k-1}} + \kappa(\epsilon)^{2^{k-1}}$. Zeigen Sie:

(1) Es gilt $r_1 = 4$ und $r_{k+1} = r_k^2 - 2$.

(2) Sei nun p eine ungerade Primzahl und $M_p = 2^p - 1$. Es soll gezeigt werden, dass M_p eine Primzahl ist, falls $M_p \mid r_{p-1}$. Dies ist der *Lucas-Lehmer-Test* für Mersenne-Primzahlen. Schreibe dazu $\epsilon^{2^{p-2}} + \kappa(\epsilon)^{2^{p-2}} = M_p \cdot n$ mit $n \in \mathbb{N}$.

   (a) Es gilt $\epsilon^{2^{p-1}} = n \cdot M_p \epsilon^{2^{p-2}} - 1$ und $\epsilon^{2^p} = (n \cdot M_p \epsilon^{2^{p-2}} - 1)^2$.
   (b) Hat M_p einen Primteiler $l \leq \sqrt{M_p}$, so hat ϵ die Ordnung 2^p in $(\mathcal{O}/l\mathcal{O})^\times$.
   (c) Führen Sie (b) zu einem Widerspruch.

Abgabe: Bis Mittwoch, den 02.07.2008, vor Beginn der Übung in den Kasten neben Zimmer 308 des Mathematikgebäudes.