Universität Heidelberg
Mathematisches Institut

Prof. Dr. Otmar Venjakob
Dr. Andreas Riedel
Christian Rüschoff

Algebraische Zahlentheorie 1

Wintersemester 2015/2016

Aufgabenblatt 1 16. Oktober 2015

Aufgabe 1. *(4 Punkte)*
Zeigen Sie: $z \in \mathbb{Z}[i]$ ist genau dann eine Einheit, wenn $N(z) = 1$.

Aufgabe 2. *(4 Punkte)*
Es sei p eine Primzahl und ζ_p eine p-te primitive Einheitswurzel. Zeigen Sie:

a) $\alpha \in \mathbb{Z}[\zeta_p] \quad \Rightarrow \quad \alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta_p]$

b) Es sei $\alpha = a_0 + a_1\zeta_p + ... + a_{p-1}\zeta_p^{p-1} \in \mathbb{Z}[\zeta_p]$ mit $a_i \in \mathbb{Z}$ und mindestens einem $a_i = 0$.
Falls $\alpha \in n\mathbb{Z}[\zeta_p]$, für ein $n \in \mathbb{Z}$, so ist auch $a_i \in n\mathbb{Z}$, für alle $0 \leq i \leq p-1$.

Aufgabe 3. *(8 Punkte)*
In dieser Aufgabe beweisen wir in Teilschritten folgenden Satz von Kummer:
Für eine ungerade Primzahl p gelte folgende Bedingung, für alle $a, b, c \in \mathbb{Z}[\zeta_p]$:

$(*)$ $ab = c^p,\ (a, b) = \mathbb{Z}[\zeta_p] \quad \Rightarrow \quad a, b$ sind p-te Potenzen (modulo Einheiten).

Dann besitzt die Gleichung $x^p + y^p = z^p$ keine Lösung $x, y, z \in \mathbb{Z}$ mit $(xyz, p) = \mathbb{Z}$ und $xyz \neq 0$.

Wir nehmen an, es gäbe eine solche Lösung $x, y, z \in \mathbb{Z}$ und führen dies zum Widerspruch. Zeigen Sie:

a) Die Behauptung gilt für $p = 3$ (Betrachten Sie das Problem modulo 9).

b) $z^p = x^p + y^p = \prod_{0 \leq i \leq p-1} (x + \zeta_p^i y)$.

c) $(x + \zeta_p^i y, x + \zeta_p^j y) = \mathbb{Z}[\zeta_p]$, für $i \neq j$ und $(x, y) = \mathbb{Z}$.
Hinweis: Für jedes Primideal $(x + \zeta_p^i y, x + \zeta_p^j y) \subset \mathfrak{p} \lhd \mathbb{Z}[\zeta_p]$ gilt $x + y \in \mathbb{Z} \cap \mathfrak{p} = (p)$. Warum?

d) $x + \zeta_p^i y \equiv a_i z_i \mod p$, für gewisse $a_i \in \mathbb{Z}$, $z_i \in \mathbb{Z}[\zeta_p]^\times$.

e) $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \mod p$, für ein $r \in \mathbb{N}$.
Hinweis: Verwenden Sie (ohne Beweis) ein späteres Resultat aus der Vorlesung:

$$u \in \mathbb{Q}[\zeta_p]^\times \quad \Rightarrow \quad u = \zeta_p^j \cdot v, \qquad \text{für gewisse } j \in \mathbb{N}, \quad v \in \mathbb{Q}[\zeta_p + \zeta_p^{-1}]^\times.$$

f) Vervollständigen Sie den Beweis. Benutzen Sie $p \geq 5$ und 2b) um folgende Fälle zum Widerspruch zu führen:

(a) $1, \zeta_p, \zeta_p^{2r-1}, \zeta_p^{2r}$ sind paarweise verschieden.
(b) $1 = \zeta_p^{2r}$.
(c) $1 = \zeta_p^{2r-1}$.
(d) $\zeta_p = \zeta_p^{2r-1}$.

Homepage zur Vorlesung: `www.mathi.uni-heidelberg.de/~rueschoff/ws15azt1/`
Abgabe bis spätestens 23. Oktober 2015 vor der Vorlesung.