ulm university universität
uulm

Prof. Dr. Stefan Wewers
Christian Steck
Wintersemester 2013/2014

Übungsblatt 2

Algebraische Zahlentheorie

Die Besprechung erfolgt am Mittwoch, dem 30.10.2013,
um 14:00 Uhr in O28 - 2003.

Aufgabe 1 (5+5)

Sei $p \geq 5$ eine Primzahl.

(a) Zeigen Sie:

$$\text{Es gibt } x, y \in \mathbb{N} \text{ mit } p = x^2 + 3y^2 \quad \Leftrightarrow \quad \left(\frac{-3}{p}\right) = 1$$

(b) Zeigen Sie:

$$\left(\frac{-3}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod 3$$

Bemerkung: Ersetzt man in obiger Aufgabe die Zahl 3 durch die Zahl 2, so erhält man mit einem ähnlichen Beweis die entsprechende Aussage aus Bemerkung 1.3.5 im Skript.

Aufgabe 2 (2+3+2+3)

In Aufgabe 1(a) gilt die Richtung „$\Leftarrow$“ im allgemeinen nicht, vergleiche Beispiel 1.3.9. Die folgenden Aussagen gelten jedoch für beliebiges $n \in \mathbb{N}$. Zur Vereinfachung nehmen wir an, dass n ungerade und quadratfrei ist, d.h. $n = q_1 \cdots q_r$ für ungerade Primzahlen $q_1, \ldots, q_r$. Im Folgenden sei stets p eine ungerade Primzahl.

(a) Zeigen Sie:

$$\text{Es gibt } x, y \in \mathbb{N} \text{ mit } p = x^2 + ny^2 \quad \Rightarrow \quad \left(\frac{-n}{p}\right) = 1$$

(b) Zeigen Sie:

$$\prod_{i=1}^{r} (-1)^{\frac{q_i - 1}{2}} = (-1)^{\frac{n-1}{2}}$$

Hinweis: Definieren Sie für a ungerade die Funktion $\varepsilon(a) = \frac{a-1}{2}$ und zeigen Sie die Gleichung $\varepsilon(ab) \equiv \varepsilon(a) + \varepsilon(b) \pmod 2$

(c) Zeigen Sie:

$$\left(\frac{-n}{p}\right) = 1 \quad \Leftrightarrow \quad \prod_{i=1}^{r} \left(\frac{p}{q_i}\right) = (-1)^{\frac{n+1}{2}\frac{p-1}{2}}$$

Bitte wenden!

(d) Zeigen Sie, dass es ganze Zahlen $a_1, \ldots, a_r$ gibt, so dass für alle bis auf endlich viele Primzahlen p die Äquivalenz

$$\left(\frac{-n}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv a_1, \ldots, a_r \pmod{N}$$

gilt, mit

$$N = \begin{cases} n, & \text{wenn } n \equiv 0,\, 3 \pmod 4 \\ 4n, & \text{wenn } n \equiv 1,\, 2 \pmod 4 \end{cases}$$

Aufgabe 3 (3+4+3)

(a) Berechnen Sie die Minimalpolynome von $\frac{1}{2} + \sqrt{3}$, $\frac{1}{2} - \frac{3}{2}\sqrt{5}$ und $1 + 2\sqrt[3]{7}$.

(b) Berechnen Sie jeweils den Grad der Körpererweiterung $K/\mathbb{Q}$ und eine Basis des $\mathbb{Q}$-Vektorraums K für

(i) $K = \mathbb{Q}\left(\sqrt{2}\right)$

(ii) $K = \mathbb{Q}\left(\frac{1}{2} + \sqrt{3}\right)$

(iii) $K = \mathbb{Q}\left(1 + 2\sqrt[3]{7}\right)$

(iv) $K = \mathbb{Q}\left(\sqrt{2},\, \sqrt[3]{3}\right)$

(c) Bestimmen Sie für die obigen Körpererweiterungen jeweils alle Einbettungen in $\mathbb{C}$.