Prof. Dr. M. Rapoport
Dr. J. Ludwig

WS 2016/17

Algebra II

Bonusblatt

Das Ziel der folgenden Aufgaben ist der Beweis des folgenden Resultats:

Satz. *Sei p eine ungerade Primzahl und ζ eine primitive p-te Einheitswurzel. Wenn die Klassenzahl von $\mathbb{Q}(\zeta)$ nicht durch p teilbar ist, so besitzt die Gleichung*

$$x^p + y^p = z^p$$

keine Lösungen mit $x, y, z \in \mathbb{Z}$ und $p \nmid xyz$.

Aufgabe 1:

a) Der Satz ist richtig für $p = 3$.

b) Man kann zum Beweis des Satzes ohne Einschränkung voraussetzen, dass x, y und z paarweise teilerfremd sind.

Um den Satz zu beweisen, nehmen wir an, es wäre $x^p + y^p = z^p$, mit $p \nmid xyz$, x, y, z paarweise teilerfremd. Dann gilt

$$\prod_{k=0}^{p-1}(x + \zeta^k y) = z^p. \qquad (*)$$

Wir wollen dies in Aufgabe 4 mit Hilfe der Voraussetzung an die Klassenzahl zu einem Widerspruch führen. Dazu brauchen wir die Ergebnisse aus den Aufgaben 2 und 3. Wir bezeichnen mit R den Ring der ganzen Zahlen von $\mathbb{Q}(\zeta)$, d.h. $R = \mathbb{Z}[\zeta]$. In der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist p total verzweigt. Das einzige Primideal von R über p ist $\mathfrak{p} := (1 - \zeta)$.

Aufgabe 2:

Unter den obigen Voraussetzungen an x, y, z sind die $x+\zeta^k y$, $k = 0, \ldots, p-1$, paarweise teilerfremd in R, d.h.

$$(x + \zeta^k y, x + \zeta^m y) = R,$$

für $k, m \in \{0, \ldots, p-1\}$, $k \neq m$.

Aufgabe 3:

a) In R sind die $2p$-ten Einheitswurzeln enthalten, und keine weiteren.

b) Ist $a \in \mathbb{Z}$ in R durch $1 - \zeta$ teilbar, so ist a ein Vielfaches von p.

c) Jede Einheit in R läßt sich schreiben als Produkt einer Potenz von ζ und einer reellen Einheit.

Hinweis zu c): Zu einer Einheit $\varepsilon = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} =: r(\zeta)$, $a_i \in \mathbb{Z}$, betrachte die

komplexe Konjugierte $\bar{\varepsilon} = r(\zeta^{-1})$ und den Quotienten $\mu = \varepsilon/\bar{\varepsilon}$. Zeige, dass alle Konjugierten von μ Betrag 1 haben. Folglich ist μ eine Einheitswurzel, und nach a) gilt $\mu = \pm\zeta^a$. Wäre aber $\mu = -\zeta^a$, so folgte wegen

$$\varepsilon \equiv \bar{\varepsilon} \equiv \sum_{i=0}^{p-2} a_i =: M \mod (1-\zeta),$$

dass $M \equiv 0 \mod (1-\zeta)$ (verwende Teil b)). Dann wäre aber auch $\varepsilon \equiv 0 \mod (1-\zeta)$, was nicht möglich ist. Also ist $\varepsilon = \zeta^a\bar{\varepsilon}$. Wähle nun $s \in \mathbb{Z}$ mit $2s \equiv a \mod p$ und zeige, dass $\eta := \frac{\varepsilon}{\zeta^s}$ reell ist.

Aufgabe 4:

a) Wegen $(*)$ und Aufgabe 2 gilt $(x + \zeta^j y)R = \mathfrak{a}_j^p$ für alle j, wobei die $\mathfrak{a}_j$ Ideale in R sind. Die $\mathfrak{a}_j$ müssen dann Hauptideale sein, etwa $\mathfrak{a}_j = \alpha_j R$.

b) Wir schreiben $\alpha := \alpha_1$. Dann gilt $x + \zeta y = \alpha^p u$, $u \in R^\times$. Nach Aufgabe 3c) können wir u in der Form $u = \rho\eta$ schreiben, wobei ρ reell und η eine p-te Einheitswurzel ist. Nun gibt es $a \in \mathbb{Z}$ mit $\alpha \equiv a \mod \mathfrak{p}$. Folglich gilt $\zeta^j\alpha - a \in \mathfrak{p}$ für alle j, und damit

$$a^p - \alpha^p = \prod_{j=0}^{p-1}(a - \zeta^j\alpha) \in p\mathfrak{p}.$$

Wir schreiben $b = a^p$ und erhalten insgesamt

$$u^{-1}(x + \zeta y) \equiv b \mod p\mathfrak{p}. \qquad (**)$$

c) Führe $(**)$ zum Widerspruch, falls $\eta = 1$ oder $\eta \neq 1, \zeta\eta^{-1} = 1$. (Wende die komplexe Konjugation an und beachte, dass y und x nicht von p geteilt werden.)

d) Für $a_i \in \mathbb{Z}$ ist $\sum_{i=1}^{p-1} a_i\zeta^i$ genau dann ein Element von pR, wenn alle a_i von p geteilt werden.

e) Wir wollen jetzt $(**)$ in den verbleibenden Fällen zum Widerspruch führen. Zunächst muss

$$x\eta^{-1} + \zeta\eta^{-1}y - x\eta - \zeta^{-1}\eta y \equiv 0 \mod p\mathfrak{p}.$$

Es gelte nun $\eta \neq 1$, $\zeta \neq \eta$. Ferner ist $\zeta \neq 1$. Wende d) an auf die obige Gleichheit und folgere, dass $\eta = \zeta\eta^{-1}$. Zeige schließlich, dass das nicht möglich ist.

Abgabe: Montag, 16. Januar 2017.