Leibniz Universität Hannover
Fakultät für Mathematik und Physik
Prof. Dr. M. Schütt
MSc. S. Brandhorst

21. April 2016

Einführung in die Algebraische Zahlentheorie
Sommersemester 2016
Blatt 3

1. Der n-te Potenzrestcharakter

   Für einen beliebigen Ring A setzen wir $\mu_n(A) := \{a \in A \mid a^n = 1\}$. Zur Erinnerung: Ein *(kommutatives) Monoid* ist eine Menge zusammen mit einer assoziativen und kommutativen Verknüpfung, die ein neutrales Element besitzt.

   Sei K ein Zahlkörper, A der zugehörige Ganzheitsring, und $\mathfrak{p}$ ein Primideal. Damit ist $k = A/\mathfrak{p}$ ein endlicher Körper mit $q = p^r$ Elementen. Im Folgenden wird eine zu p teilerfremde natürliche Zahl n betrachtet und es wird angenommen, dass das Polynom $f(x) = x^n - 1$ über K vollständig in Linearfaktoren zerfällt.

   (a) **Proposition** $A \setminus \mathfrak{p}$ ist ein kommutatives Monoid, und die Reduktionsabbildung $A \setminus \mathfrak{p} \to k^\times$ ist ein Monoidhomomorphismus.

   (b) **Proposition** In jedem Körper, dessen Charakteristik die Zahl n nicht teilt, sind die Nullstellen von f (die n-ten Einheitswurzeln) paarweise verschieden.

   (c) **Proposition** Die Abbildungen $\mu_n(K) \supset \mu_n(A) \to \mu_n(k)$ sind bijektiv.

   (d) **Korollar** Es gilt: $n \mid q - 1$.

   (e) **Proposition** Die Setzungen $\alpha(x) = x^n$ und $\beta(x) = x^{\frac{q-1}{n}}$ definieren eine exakte Sequenz wie folgt:
   $$k^\times \xrightarrow{\alpha} k^\times \xrightarrow{\beta} \mu_n(k) \to 1\,.$$

   (f) **Definition** Der n-te Potenzrestcharakter zum Primideal $\mathfrak{p}$, in Zeichen $\left(\frac{\cdot}{\mathfrak{p}}\right)$, ist gegeben durch die folgende Verkettung von Monoidhomomorphismen:
   $$A \setminus \mathfrak{p} \to k^\times \xrightarrow{\beta} \mu_n(k) \xleftarrow{\sim} \mu_n(A) \xrightarrow{\sim} \mu_n(K)\,.$$

   Gelegentlich wird eine feste Einbettung $K \subset \mathbb{C}$ gewählt und $\left(\frac{\cdot}{\mathfrak{p}}\right)$ wird als Monoidmorphismus $A \setminus \mathfrak{p} \to \mathbb{C}^\times$ bzw. als Gruppenhomomorphismus $k^\times \to \mathbb{C}^\times$ aufgefaßt. Für $a \in A \setminus \mathfrak{p}$ kann $\left(\frac{a}{\mathfrak{p}}\right)$ als Maß interpretiert werden, wie weit a davon entfernt ist, ein n-ter Potenzrest modulo $\mathfrak{p}$ zu sein.

2. Zeigen Sie, dass $x^4 - 16x^2 + 4$ irreduzibel über $\mathbb{Z}$, aber nicht über $\mathbb{F}_p$ für alle $p \in \mathbb{P}$ ist.