RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 2 / 15.–17. April 2013

AUFGABE 1:

(a) Sei R zunächst ein beliebiger Ring und $N : R \to \mathbb{Z}$ eine Funktion mit $N(ab) = N(a) \cdot N(b)$ und $N(1) = 1$.
Zeigen Sie, dass für alle Einheiten $x \in R^*$ gilt: $N(x) \in \{-1, +1\}$

(b) Sei nun $R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ für $d \in \mathbb{Z}$ mit d kein Quadrat.
Wir betrachten die Funktion $\sigma : R \to R$, gegeben durch $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. (Für $d < 0$ ist σ die komplexe Konjugation!). Weiterhein betrachten wir die Normfunktion $N : R \to \mathbb{Z}$, gegeben durch $N(a + b\sqrt{d}) = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}) = (a + b\sqrt{d}) \cdot \sigma(a + b\sqrt{d})$.
Zeigen Sie, dass für $x, y \in R$ gilt: $\sigma(x + y) = \sigma(x) + \sigma(y)$ sowie $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$.
Folgern Sie, dass $N(xy) = N(x)N(y)$ für alle $x, y \in R$ gilt und dass $N(1) = 1$ ist.

(c) Zeigen Sie, dass $x \in R$ invertierbar ist *genau dann* wenn $N(x) \in \{-1, +1\}$ ist, wobei $R = \mathbb{Z}[\sqrt{d}]$ und N wie in (b) definiert sind.

(d) Zeigen Sie, dass die Einheiten von $\mathbb{Z}[i]$ genau $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ sind.

AUFGABE 2:
Sei nun $K = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ und $R = \mathbb{Z}[\sqrt{3}] \subset K \subset \mathbb{R}$.
Wie in Aufgabe 2 betrachten wie die Normfunktion $N : K \to \mathbb{Q}, N(a + b\sqrt{d}) = a^2 - 3b^2$, wobei $N(x) \in \mathbb{Z}$ für $x \in R$. Zeigen Sie, dass $R = \mathbb{Z}[\sqrt{3}]$ ein euklidischer Ring ist mit dem Betrag der Normfunktion N als Bewertungsfunktion.

Bemerkung: Die Ergebnisse von 1(b) gelten auch für Koeffizienten aus $\mathbb{Q}$. Der Körper (warum ist das einer?) K dient hier nur dem Zweck, eventuell mit Zwischenergebnissen mit rationalen Koeffizienten rechnen zu können.

AUFGABE 3:
Faktorisieren Sie 30 in $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$.

AUFGABE 4:
Sei R ein Integritätsring und $I_1 \subset I_2 \subset \cdots$ eine (unendliche) Kette aufsteigender Ideale in R. Zeige Sie, dass dann auch $I = \bigcup I_i$ ein Ideal ist.

AUFGABE 5:

Sei R ein euklidischer Ring mit Bewertungsfunktion $\delta : R \setminus \{0\} \to \mathbb{N}$. Zeigen Sie, dass dann auch $\widetilde{\delta}(x) = A\delta(x) + C$ eine Bewertungsfunktion ist, wobei $A, C \in \mathbb{N}$ mit $A > 0$, $C \geq -\frac{\min\{\delta(x) | x \in R \setminus \{0\}\}}{A}$.

AUFGABE 6:

Zeigen Sie, dass das Ideal $(2, 3X) \subset \mathbb{Z}[X]$ kein Hauptideal ist.