Fachbereich Mathematik und Statistik
Prof. Dr. Salma Kuhlmann
Michele Serra
Simon Müller
SS 2017

Algebraische Zahlentheorie - Übungsblatt 1

Abgabe. Donnerstag, 4 Mai 2017, 10:00 Uhr, Briefkasten n. 19.

Aufgabe 1 (4 Punkte)**.** Sei B ein kommutativer Ring mit Eins und A ein Unterring von B. Ein Element $b \in B$ heißt *ganz* über A, wenn es ein normiertes Polynom $p \in A[X]$ gibt, so dass $p(b) = 0$ ist.
Sei R ein faktorieller Ring und sei Q der Quotientenkörper von R. Ferner, sei K eine Körpererweiterung von Q und $\alpha \in K$ algebraisch über Q.
Zeigen Sie, dass α genau dann ganz über R ist, wenn das Minimalpolynom von α über Q in $R[X]$ ist.
Folgern Sie, dass $\beta \in Q$ genau dann ganz über R ist, wenn $\beta \in R$ ist.

Aufgabe 2 (4 Punkte)**.** Sei $\mathcal{P}$ die Menge der Primzahlen. Zeigen Sie, dass

$$\{\text{Unterringe von } \mathbb{Q}\} \longrightarrow \{\text{Teilmengen von } \mathcal{P}\},\ R \longmapsto R^\times \cap \mathcal{P}$$

eine Bijektion zwischen den Unterringen von $\mathbb{Q}$ und den Teilmengen von $\mathcal{P}$ definiert.
Hinweise:

(a) Sei $\emptyset \neq P \subseteq \mathcal{P}$. Sei S_P das *von P erzeugte multiplikative System*, d.h., S_P ist die Menge aller endlichen Produkte von Elementen aus P. Nach Algebra (B3), ist

$$S_P^{-1}\mathbb{Z} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in S_P\},$$

die Lokalisierung von $\mathbb{Z}$ nach S_P, ein Unterring von $\mathbb{Q}$.

Zeigen Sie, dass $(S_P^{-1}\mathbb{Z})^\times \cap \mathcal{P} = P$.

(b) Sei R ein Unterring von $\mathbb{Q}$. Sei $P = R^\times \cap \mathcal{P}$, d.h., P ist die Menge der Primzahlen deren multiplikatives Inverses zu R gehört. Dann ist es klar, dass $S_P^{-1}\mathbb{Z} \subseteq R$.

Zeigen Sie, dass tatsächlich $S_P^{-1}\mathbb{Z} = R$ gilt.

Aufgabe 3 (4 Punkte, ohne (e))**.** Sei $D \in \mathbb{Z}$ quadratfrei. Wir definieren die (Körper)Norm als die folgende Abbildung:

$$N\colon \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q},\ N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D \in \mathbb{Q}.$$

Wir bemerken dass $N(a + b\sqrt{D}) \neq 0$ wenn $a + b\sqrt{D} \neq 0$.

(a) Zeigen Sie, dass die Norm *multiplikativ* ist, d.h., für alle $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$ gilt $N(\alpha\beta) = N(\alpha)N(\beta)$.

Sei $\mathcal{O} = \mathbb{Z}[\omega]$ der Ring der ganzen Zahlen, wobei

$$\omega = \begin{cases} \sqrt{D}, & D \equiv 2,3 \mod 4; \\ \frac{1+\sqrt{D}}{2}, & D \equiv 1 \mod 4. \end{cases}$$

(b) Folgern Sie, dass $N(\alpha) \in \mathbb{Z}$ für jedes $\alpha \in \mathcal{O}$.

(c) Zeigen Sie, dass ein Element $\alpha \in \mathcal{O}$ genau dann eine Einheit ist wenn $N(\alpha) = \pm 1$.

(d) Finden Sie alle Einheiten in den Ringen $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ und $\mathbb{Z}[\sqrt{-3}]$.

(e) (2 Bonus Punkte) Für $D > 0$ ist die Einheitengruppe von $\mathbb{Z}[\sqrt{D}]$ unendlich.
Hinweis: betrachten Sie z.B. $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Aufgabe 4 (4 Punkte)**.** In dieser Übung zeigen wir dass die Gaußschen Zahlen $\mathbb{Z}[i]$ mit der Norm $N(a+ib) = a^2 + b^2$ einen Euklidischen Ring bilden, d.h., für alle $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$ existieren ρ, σ so dass $\alpha = \rho\beta + \sigma$ und $\sigma = 0$ oder $N(\sigma) < N(\beta)$.

(a) Zeigen Sie, dass $r, s \in \mathbb{Q}$ existieren, so dass, im Körper $\mathbb{Q}(i)$, $\frac{\alpha}{\beta} = r + si$.

(b) Zeigen Sie, dass $p, q \in \mathbb{Z}$ existieren, so dass $|r-p|, |s-q| \leq \frac{1}{2}$ gilt.

(c) Sei $\rho = (p+qi)$. Zeigen Sie, dass es $\sigma \in \mathbb{Z}[i]$ gibt, so dass $\alpha = \rho\beta + \sigma$ mit $N(\sigma) \leq \frac{1}{2}N(\beta)$.
Hinweis: betrachten Sie $\beta[(r-p) + (s-q)i]$.

Zusatzaufgabe für Interessierte (2 Punkte)**.** Sei K eine algebraische Erweiterung von $\mathbb{Q}$ und $R \subseteq K$ ein Unterring. Zeigen Sie, dass wenn I ein nichttriviales Ideal von R ist, dann ist $I \cap \mathbb{Z}$ ein nichttriviales Ideal von $\mathbb{Z}$.