

Algebra I Übungsblatt 9

Aufgabe 33:

- a) Sei N Normalteiler einer Gruppe G und $\pi: G \rightarrow G/N$ die kanonische Projektion. Zeigen Sie, dass die induzierte Abbildung π' mit $U \mapsto \pi(U)$ die Normalteiler $U \triangleleft G$, welche zwischen N und G liegen, bijektiv auf die Normalteiler von G/N abbildet.
- b) Sei I Ideal eines Rings R und $\pi: R \rightarrow R/I$ die kanonische Projektion. Zeigen Sie, dass die induzierte Abbildung π' mit $J \mapsto \pi(J)$ die Ideale J in R , welche zwischen I und R liegen, bijektiv auf die Ideale von R/I abbildet.

Aufgabe 34: Die Elemente der Menge $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ heißen *Gaußsche Zahlen*. Die ganze Zahl $N(a + bi) := a^2 + b^2$ heißt *Norm* von $a + bi$.

- a) Zeigen Sie, dass die Gaußschen Zahlen einen Unterring von \mathbb{C} bilden.
- b) Zeigen Sie, $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ für alle $\alpha, \beta \in \mathbb{Z}[i]$.
- c) Bestimmen Sie die Einheiten in $\mathbb{Z}[i]$. Ist $\mathbb{Z}[i]$ ein Körper?
- d) Bestimmen Sie, welche der Primzahlen $2, 3, \dots, 29$ eine nichttriviale Faktorisierung (d.h. kein Faktor ist Einheit) in $\mathbb{Z}[i]$ besitzen.

Aufgabe 35: Seien $a_0, a_1 \in \mathbb{Z} \setminus \{0\}$. Der folgende *Euklidische Algorithmus* berechnet einen ihrer größten gemeinsamen Teiler:

1. Setze $k := 1$.
2. Dividiere mit Rest $a_{k-1} = q_k a_k + a_{k+1}$, also $q_k \in \mathbb{Z}$ und $|a_{k+1}| < |a_k|$.
3. Ist $a_{k+1} = 0$, gebe a_k aus und stoppe.
4. Ist $a_{k+1} \neq 0$, erhöhe k um 1 und fahre mit Schritt 2 fort.

Wenden Sie den Euklidischen Algorithmus auf die Zahlenpaare $(2, 7)$, $(3, -5)$, $(13, 21)$ und $(164, 184)$ an. Bestimmen Sie für jedes Zahlenpaar durch Rückwärts einsetzen in die Gleichungen des Algorithmus $a_\ell = \dots, a_{\ell-1} = \dots$ bis $a_0 = q_1 a_1 + a_2$ eine Darstellung

$$\text{ggT}(a_0, a_1) = s \cdot a_0 + t \cdot a_1 \quad \text{mit } s, t \in \mathbb{Z}.$$

Aufgabe 36: Berechnen Sie eine ganze Zahl x , die die folgenden Kongruenzen simultan erfüllt:

$$x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 4 \pmod{7}.$$

Wie viele Lösungen gibt es? Wie unterscheiden sich zwei Lösungen?