ALGEBRA I
9. ÜBUNGSBLATT

HENNING KRAUSE
MARTIN KALCK

Aufgabe 1. (2+2 Punkte)

Sei R ein *kommutativer* Ring. Zeigen Sie, dass

(a) $p \in R$ genau dann prim ist, wenn das Hauptideal $(p) \subseteq R$ ein *Primideal*[1] ist.
(b) $\mathfrak{p} \subseteq R$ genau dann ein Primideal ist, wenn der Faktorring $R/\mathfrak{p}$ ein Integritätsring ist.

Aufgabe 2. (3+1 Punkte)

(a) Sei R ein *faktorieller* Ring. Zeigen Sie, dass ein Element $x \in R$ genau dann *prim* ist, wenn es *irreduzibel* ist.
(b) Beweisen oder widerlegen Sie:
Sei R ein faktorieller Ring und $I \subseteq R$ ein Ideal. Dann ist der Faktorring R/I faktoriell.

Aufgabe 3. (2+2 Punkte)

(a) Beweisen Sie den chinesischen Restsatz:
Sei R ein kommutativer Ring mit paarweise *koprimen*[2] Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq R$ und sei $\pi_i \colon R \to R/\mathfrak{a}_i$ die kanonische Projektion. Dann induziert die Abbildung

$$R \longrightarrow R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n, \quad x \longmapsto (\pi_1(x), \ldots, \pi_n(x))$$

einen Isomorphismus von Ringen

$$R/\bigcap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$$

(b) Folgern Sie den chinesischen Restsatz aus der Zahlentheorie:
Seien $m_1, \ldots, m_t$ paarweise teilerfremde natürliche Zahlen und $a_1, \ldots, a_t$ ganze Zahlen. Dann besitzt das System von Kongruenzen

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_t \pmod{m_t} \end{cases}$$

eine *eindeutige* Lösung x modulo $m := m_1 \cdot \ldots \cdot m_t$.

Abgabe: Montag, 10. Juni 2013, bis 14 Uhr in die Postfächer der Tutoren in V3-126.

[1] Ein Ideal $\mathfrak{p} \subsetneq R$ heißt *Primideal*, falls für Elemente $a, b \in R$ aus $a \cdot b \in \mathfrak{p}$ folgt, dass $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ gilt.
[2] Zwei Ideale I und J von R heißen *koprim*, falls $I + J = R$ gilt.

Aufgabe 4. (4 Punkte)

Sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie, dass das Polynom $f = X^{p-1} + X^{p-2} + \ldots + X + 1$ ein Primelement in $\mathbb{Q}[X]$ ist.

(*Hinweis: Wenden Sie das Eisenstein-Kriterium auf eine geeignete Modifikation von f an!*)