Mathematisches Institut
der Universität München
Andreas Fackler

Sommersemester 2009
Lösungsvorschlag zu Übungsblatt 6

Klausurenkurs Algebra

Aufgabe 1 (Frühjahr 2005, Thema 3, Aufgabe 3)

Nach dem chinesischen Restsatz können wir $\varphi(x+1000\mathbb{Z}) = (x+8\mathbb{Z}, x+125\mathbb{Z})$ definieren. $\varphi^{-1}(a+8\mathbb{Z}, b+125\mathbb{Z})$ muss dann von der Form $x+1000\mathbb{Z}$ sein, wobei $x \equiv a \mod 8$ und $x \equiv b \mod 125$ ist. Es ist $125 \equiv 5 \mod 8$, also $125^2 \equiv 5^2 \equiv 1 \mod 8$. Umgekehrt wollen wir ein n mit $8^n \equiv 1 \mod 125$ finden. Da $(\mathbb{Z}/125\mathbb{Z})^\times$ genau $4 \cdot 5^2$ Elemente hat, ist $8^100 \equiv 1$ mod 125. Es ist also $\varphi^{-1}(a+8\mathbb{Z}, b+125\mathbb{Z}) = a \cdot 125^2 + b \cdot 8^{100} + 1000\mathbb{Z}$.

Aufgabe 2 (Frühjahr 2007, Thema 2, Aufgabe 2)

(a) Zunächst bestimmen wir die Einheiten in R. Da $\varphi(xy) = \varphi(x)\varphi(y)$ ist und immer $\varphi(x) \geq 1$ für $x \neq 0$ gilt, muss eine Einheit x die Eigenschaft $\varphi(x) = 1$ haben. Dies ist nur für 1 und -1 erfüllt, also sind diese Zahlen die einzigen Einheiten.

Ist p eine Primzahl in $\mathbb{Z}$, so ist $\varphi(p) = p^2$. Ist p also in $\mathbb{Z}[i\sqrt{2}]$ kein Primelement, so gibt es $x, y \in \mathbb{Z}[i\sqrt{2}]$ mit $\varphi(x) = p = \varphi(y)$ und $x \cdot y = p$. 5 und 7 sind Primelemente, da $\varphi(a + ib\sqrt{2}) = a^2 + 2b^2$ nie 5 oder 7 sein kann. Die anderen sind keine Primelemente: $2 = i\sqrt{2} \cdot (-i\sqrt{2})$, $3 = (1 + i\sqrt{2}) \cdot (1 - i\sqrt{2})$ und $11 = (3 + i\sqrt{2}) \cdot (3 - i\sqrt{2})$.

(b) Wir wenden den euklidischen Algorithmus an:

$$\begin{aligned} 6 &= 1 \cdot (4 + i\sqrt{2}) + (2 - i\sqrt{2}) \\ 4 + i\sqrt{2} &= (1 + i\sqrt{2}) \cdot (2 - i\sqrt{2}) \end{aligned}$$

Also ist $1 + i\sqrt{2}$ der größte gemeinsame Teiler von 6 und $4 + i\sqrt{2}$.

Aufgabe 3 (Frühjahr 2007, Thema 1, Aufgabe 4)

(a) Sei $P \neq \{0\}$ ein Primideal und sei $I \supset P$ ein echt größeres Ideal. Wir müssen zeigen, dass dann $I = R$ ist. Sei $I = Ra$ mit $a \in R$ und sei $P = Rp$. Dann gibt es ein $b \in R$ mit $p = ab$. Da P Primideal ist und $a \notin P$, muss dann $b \in P$ sein, also $b = cp$ für ein $c \in R$. Dann ist aber $p = ab = acp$, also $1 = ac$, also ist a eine Einheit und damit $I = R$.

(b) Es ist $R = R[X]/(X)$ und (X) ist ein Primideal. Ist also $R[X]$ ein Hauptidealring, so ist (X) ein maximales Ideal und damit $R[X]/(X)$ ein Körper.

Aufgabe 4 **(Herbst 2005, Thema 2, Aufgabe 3)**

Hauptidealringe sind faktorielle Ringe. Sei also $a = \epsilon p_1^{m_1} \cdots p_n^{m_n}$ eine (bis auf Einheiten) eindeutige Zerlegung von a in Primelemente. Dann gilt für jedes Ideal $Rb \supseteq Ra$, dass b ein Teiler von a ist, sich also als $b = \nu p_1^{k_1} \cdots p_n^{k_n}$ darstellen lässt. Dafür gibt es (bis auf Einheiten) nur endlich viele Möglichkeiten, da jeweils $k_i \leq m_i$ sein muss.