Aufgabe F13T2A3 (6 Punkte)

Sei R ein Integritätsbereich, und seien $x_1, ..., x_n$ und a Elemente von R. Zeigen Sie: Ist R faktoriell und d ein größter gemeinsamer Teiler von $x_1, ..., x_n$, so ist ad ein größter gemeinsamer Teiler von $ax_1, ..., ax_n$.

Lösung:

Weil d ein gemeinsamer Teiler von $x_1, ..., x_n$ ist, gibt es Elemente $r_1, ..., r_n \in R$ mit $x_j = r_j d$ für $1 \leq j \leq n$. Die Gleichungen $ax_j = a(r_j d) = r_j(ad)$ zeigen, dass ad ein gemeinsamer Teiler von $ax_1, ..., ax_n$ ist. Weil R faktoriell ist, besitzen die Elemente $ax_1, ..., ax_n$ auch einen größten gemeinsamen Teiler $t \in R$. Nehmen wir nun an, dass ad kein größter gemeinsamer Teiler dieser Elemente ist. Dann gilt zwar $(ad) \mid t$, aber die Elemente ad und t sind nicht assoziiert, d.h. es gilt $t \nmid ad$. Für das Element $\alpha = \frac{t}{ad}$ im Quotientenkörper von R bedeutet dies, dass α in R liegt, aber keine Einheit in R ist. Da R faktoriell ist, folgt daraus, dass ein Primelement $p \in R$ mit $p \mid \alpha$ existiert. Es gibt also ein $r \in R$ mit $pr = \alpha = \frac{t}{ad} \Leftrightarrow prad = t$.

Weil t ein gemeinsamer Teiler von $ax_1, ..., ax_n$ ist, gibt es Elemente $s_1, ..., s_n \in R$ mit $ax_j = s_j t$ für $1 \leq j \leq n$. Es folgt $ax_j = s_j prad \Rightarrow x_j = s_j prd$ für $1 \leq j \leq n$. Also ist pd ein gemeinsamer Teiler von $x_1, ..., x_n$. Weil d ein größter gemeinsamer Teiler dieser Elemente ist, folgt $pd \mid d$, also $d = spd$ für ein $s \in R$. Daraus folgt $sp = 1$, somit wäre p in R eine Einheit. Aber dies steht im Widerspruch dazu, dass p in R ein Primelement ist. Also war die Annahme, dass ad kein größter gemeinsamer Teiler von $ax_1, ..., ax_n$ ist, falsch.

Hinweis:

Aus der Vorlesung ist bekannt, dass jedes Element in einem faktoriellen Ring R eine Darstellung als Produkt von Primelementen besitzt, die eindeutig bis auf Reihenfolge wird, sobald man ein Repräsentantensystem der Primelemente von R fixiert. Genauer gilt: Ist $P \subseteq R$ ein Repräsentantensystem der Primemelemente in R, dann gibt es für das Element $a \in R$ aus der Aufgabe eine eindeutig bestimmte Familie $(e_p)_{p \in P}$ in $\mathbb{N}_0$ und eine eindeutig bestimmte Einheit $\varepsilon \in R^\times$, so dass

$$a = \varepsilon \prod_{p \in P} p^{e_p}$$

und $e_p = 0$ für alle bis auf endlich viele $p \in P$ gilt. (Nur auf Grund dieser letzten Bedingung ist das Produkt $\prod_{p \in P} p^{e_p}$ in R überhaupt definiert.) Genauso besitzen die Elemente $x_1, ..., x_n$ eindeutige Darstellungen dieser Form, und mit Hilfe dieser Darstellungen lässt sich auch ein ggT von $x_1, ..., x_n$ hinschreiben. Man kann auch auf diesem Wege die Aufgabe lösen, wenn man zusätzlich berücksichtigt, dass je zwei ggT's derselben Elemente in einem Ring jeweils zueinander assoziiert sind. Die Ausarbeitung der Details ist eine sinnvolle Übungsaufgabe.