H23-T3-A5

Seien $R \neq 0$ ein kommutativer Ring und $F, G \in R[X]$ Polynome, wobei G als normiert angenommen sei. Dann (das sollen Sie nicht beweisen) existieren eindeutig bestimmte $A, B \in R[X]$ so, dass gilt $F = AG + B$ und $\deg(B) < \deg(G)$ (hierbei ist $\deg(0) := -\infty$). (Das ist Division mit Rest durch ein normiertes Polynom).

a) Seien $f : R \to S \neq 0$ ein Ringhomomorphismus und $f[X] : R[X] \to S[X]$ der Ringhomomorphismus, der auf $R \subseteq R[X]$ mit f übereinstimmt und außerdem $f[X](X) = X$ erfüllt. Zeigen Sie, dass in $S[X]$ gilt $f[X](F) = f[X](A) \cdot F[X](G) + f[X](B)$, und dass diese Gleichung die Division mit Rest von $f[X](F)$ durch $f[X](G)$ ist.

b) Zeigen Sie, dass genau ein Ideal $I \subseteq R$ existiert, sodass für jeden Ringhomomorphismus $f : R \to S \neq 0$ äquivalent sind:

   i) $f[X](G)$ teilt $f[X](F)$ in $S[X]$.

   ii) $f(I) = 0$.

c) Bestimmen Sie das Ideal $I \subseteq R$ aus Teil b) in den beiden folgenden Fällen:

   i) $R := \mathbb{Z}, F := X^3 - 1, G := X^2 + 1 \in R[X]$.

   ii) $R := \mathbb{Z}[Y], F(X) := X^2 + Y, G(X) := X - 1 \in R[X]$.

Lösung

a) Aus $F = AG + B$ und der Tatsache, dass $F[X]$ ein Ringhomomorphismus ist, gilt

$$F[X](F) = F[X](A)F[X](G) + F[X](B) \tag{0.1}$$

und da $F[X](X) = X$ folgt $F[X](X^n) = X^n$. Hieraus erhält man das $\deg(F[X](P) \leq \deg(P)$ für alle $P \in R[X]$. Nimmt man an, dass $\text{def}(F[X](B) \leq \deg(F[X](G))$ dann erhält man $\deg(F[X](G) \leq \deg(G)$ das ist jedoch ein Widerspruch, da G normiert ist und daher der führende Koeffizient 1 ist und daher unter der Abbildung $f[X]$ nicht verschwindet. Dies zeigt, dass es sich bei (0.1) um Division mit Rest von $f[X](F)$ durch $f[X](G)$ handelt.

b) Wir betrachten wieder Gleichung (0.1), mit $B = \sum_{i=0}^{n} a_i X^i$. Definiere $I = (a_0, \dots, a_n)$. Man prüft leicht nach, dass für I die gefordete Äquivalenz gilt. Für die Eindeutigkeit überlegt man sich,

dass wenn für $J \lhd R$ ebenfalls die Äquivalenz gilt, dass dann aus „$\Rightarrow$“$J \subset I$ folgt und aus „$\Leftarrow$“$I \subset J$ folgt.

b) i) Wir führen Division mit Rest durch:

$$X^3 - 1 = X \cdot (X^2 + 1) - (X + 1).$$

Nach b) gilt also $I = (1) = \mathbb{Z}$.

b) Wiederum Division mit Rest:

$$X^2 + Y = X \cdot X + Y.$$

Wieder nach b) gilt $I = (Y)$.