Einführung in die Algebra
Blatt 7

Jendrik Stelzner

4. Dezember 2013

Aufgabe 7.1.

Aufgabe 7.2.

Für $x, y \in \mathbb{C}$ mit $xy = 21$ ist $|x||y| = 21$, also muss $|x| \leq \sqrt{21}$ oder $|y| \leq \sqrt{21}$. Es genügt daher die $a + \sqrt{5}bi = z \in \mathbb{Z}[\sqrt{-5}]$ mit $|z| \leq \sqrt{21}$, also $a^2 + 5b^2 \leq 21$ auf Teilbarkeit zu überprüfen. Da für jeden Teiler $z \in \mathbb{Z}[\sqrt{-5}]$ auch $-z, \bar{z}, -\bar{z} \in \mathbb{Z}[\sqrt{-5}]$ Teiler von 21 sind, genügt es auch die $a+\sqrt{5}bi \in \mathbb{Z}[\sqrt{-n}]$ mit $a, b \geq 0$ auf Teilbarkeit zu überprüfen.
Es ergeben sich mit diesen beiden Beschränkungen die möglichen Kandidaten

$$1, 2, 3, 4, 1 + \sqrt{5}i, 1 + 2\sqrt{5}i, 2 + \sqrt{5}i, 3 + \sqrt{5}i, 4 + \sqrt{5}i.$$

Einfaches Hinsehen und kurzes Nachrechnen ergibt, dass von diesen Zahlen nur

$$1, 3, 1 + 2\sqrt{5}i \text{ und } 4 + \sqrt{5}i$$

Teiler von 21 sind. Die Teiler von 21 in $\mathbb{Z}[i]$ sind also

$$\begin{gathered} 1, -1, 21, -21, 3, -3, 7, -7, \\ 1 + 2\sqrt{5}i, -1 - 2\sqrt{5}i, 1 - 2\sqrt{5}i, -1 + 2\sqrt{5}i, \\ 4 + \sqrt{5}i, -4 - \sqrt{5}i, 4 - \sqrt{5}i, -4 - \sqrt{5}i. \end{gathered}$$

Aufgabe 7.3.

Definition. *Für einen Ring R bezeichnet*

$$\operatorname{nil}(R) := \{x \in R : x^n = 0 \textit{ für ein } n \in \mathbb{N}\}$$

das Nilradikal von R.

Bemerkung 1. *Sei R ein kommutativer Ring. Dann gilt*

(i) $\operatorname{nil}(R)$ *ist ein Ideal von R.*

(ii) Für $e \in R^*$ und $a \in \operatorname{nil}(R)$ ist $e + a \in R^*$.

Beweis. **(i)**

Es ist $0 \in \operatorname{nil}(R)$, also $\operatorname{nil}(R)$ nicht leer. Für $a, b \in \operatorname{nil}(R)$ gibt es $n, m \in \mathbb{N}$ mit $a^n = b^m = 0$, also ist

$$(a+b)^{n+m} = \sum_{k=1}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k = 0$$

und daher $a + b \in \operatorname{nil}(R)$. Auch ist für alle $r \in R$

$$(ar)^n = a^n r^n = 0,$$

also $ar \in R$. Insbesondere ist daher für alle $a \in \operatorname{nil}(R)$ auch $-a = (-1) \cdot a \in R$.

(ii)

Für $e \in R^*$ und $a \in \operatorname{nil}(R)$ mit $a^n = 0$ ist $1 - ae^{-1} \in R^*$, da $\left(ae^{-1}\right)^n = 0$ und daher

$$\left(\sum_{k=0}^{n-1} \left(-ae^{-1}\right)^k\right) \left(1 + ae^{-1}\right) = 1 + (-1)^{n-1} \left(ae^{-1}\right)^n = 1.$$

Daher ist auch $e + a = e\left(1 + ae^{-1}\right) \in R^*$. □

Da $\operatorname{nil}(R) \subseteq \operatorname{nil}(R[X])$ ist auch $(\operatorname{nil}(R)) \subseteq \operatorname{nil}(R[X])$. Dabei ist, wie in einem früheren Übungsblatt gezeigt,

$$(\operatorname{nil}(R)) = \left\{ \sum_{i=0}^{n} a_i X^i : n \geq 0, a_i \in \operatorname{nil}(R) \text{ für alle } i \right\}.$$

Nach Bemerkung 1 ist also das Polynom $f = \sum_{i=0}^{n} a_i X^i$ mit $n \geq 0$, $a_0 \in R^*$ und $a_i \in \operatorname{nil}(R)$ für alle i invertierbar.
Sei andererseits $f = \sum_{i=0}^{n} a_i X^i \in R[X]$, mit $n \geq 0$ und $a_n \neq 0$, invertierbar, d.h. es gibt ein $g = \sum_{i=0}^{m} b_i X^i \in R[X]$, mit $m \geq 0$ und $b_m \neq 0$, so dass $fg = 1$. Da damit $a_0 b_0 = 1$ müssen a_0 und b_0 invertierbar sein. Ist $n > 0$, so bemerken wir:

Behauptung 2. *Es ist $a_n^{k+1} b_{m-k} = 0$ für $k = 0, \ldots, m$.*

Beweis. Der Beweis verläuft per Induktion über k.

Induktionsanfang. Für $k = 0$ gilt: Wäre $a_n b_m \neq 0$, so wäre

$$0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g) = n + m \geq n > 0.$$

Induktionsschritt. Sei $1 \leq k \leq n$ und gelte die Aussage für $k - 1$. Da $fg = 1$ ist

$$0 = \sum_{\mu+\nu=n+m-k} a_\mu b_\nu.$$

Multiplikation der Gleichung mit a_n^k ergibt

$$0 = \sum_{\mu+\nu=n+m-k} a_n^k a_\mu b_\nu \underset{\text{IV.}}{=} a_n^{k+1} b_{m-k}.$$

□

Aus Behauptung 2 folgt insbesondere, dass $a_n^{m+1} b_0 = 0$. Da b_0 invertierbar ist, ist a_n daher nilpotent. Da nach Bemerkung 1 daher auch $f - a_n X^n$ invertierbar ist, ergibt sich durch Wiederholung der obigen Argumentation induktiv, dass a_i für alle $1 \leq i \leq n$ nilpotent ist.

Aufgabe 7.4.

Definition. *Sei R ein kommutativer Ring. Für $p = \sum_{i=0}^{\infty} a_i X^i \in R[\![x]\!]$ bezeichnet*

$$\operatorname{Deg}(p) := \begin{cases} \min\{i \in \mathbb{N} : a_i \neq 0\} & \textit{falls } f \neq 0, \\ \infty & \textit{sonst.} \end{cases}$$

den Grad von p.

Für einen kommutativen Ring R und $p, q \in R[\![x]\!]$ ist

$$\operatorname{Deg}(p+q) \geq \min\{\operatorname{Deg}(p), \operatorname{Deg}(q)\} \text{ und } \operatorname{Deg}(pq) \geq \operatorname{Deg}(p) + \operatorname{Deg}(q). \tag{1}$$

Ist R darüber hinaus nullteilerfrei, so gilt sogar

$$\operatorname{Deg}(pq) = \operatorname{Deg}(p) + \operatorname{Deg}(q). \tag{2}$$

Die Beweise der entsprechenden Aussage laufen analog zu den Beweisen der entsprechenden Aussagen für die Gradfunktion deg von $R[X]$.

(i)

Ist R kein Integritätsring, so ist auch $R[X] \subsetneq R[\![x]\!]$ kein Integritätsring, also auch $R[\![x]\!]$ nicht. Ist $R[\![x]\!]$ kein Integritätsring, so gibt es $p, q \in R[\![x]\!]$ mit $p, q \neq 0$, also $\operatorname{Deg}(p), \operatorname{Deg}(q) < \infty$, aber $pq = 0$, also $\operatorname{Deg}(pq) = \infty$. Mit (2) folgt, dass R kein Integritätsring ist.

(ii)

Ist $p = \sum_{i=0}^{\infty} a_i X^i \in R[\![x]\!]$ invertierbar, so gibt es $q = \sum_{i=0}^{\infty} b_i X^i \in R[\![x]\!]$ mit $pq = 1$. Insbesondere ist daher

$$1 = (pq)_1 = a_0 b_0,$$

also a_0 invertierbar.
Ist $p = \sum_{i=0}^{\infty} a_i X^i \in R[\![x]\!]$ mit a_0 invertierbar, so definieren wir eine Folge $(b_i)_{i \in \mathbb{N}}$ auf R rekursiv durch

$$b_0 := a_0^{-1} \text{ und } b_i := -a_0^{-1} \sum_{j=1}^{i} a_j b_{i-j},$$

und $q := \sum_{i=0}^{\infty} b_i X^i$ als die entsprechende Potenzreihe. Für $e = pq$ ergibt sich dann für alle $i \in \mathbb{N}$

$$e_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=1}^{i} a_j b_{i-j} + a_0 b_i = \sum_{j=1}^{i} a_j b_{i-j} - \sum_{j=1}^{i} a_j b_{i-j} = 0.$$

Also ist $e = 1$ und p daher invertierbar mit $p^{-1} = q$. Insbesondere ergibt sich das folgende Lemma:

Lemma 3. *Sei K ein Körper und seien $p, q \in K[\![x]\!]$. Dann gilt:*

(i) *p ist genau dann invertierbar, wenn $\operatorname{Deg} p = 0$.*

(ii) *Ist $\operatorname{Deg} p = \operatorname{Deg} q$, so sind p und q assoziiert. Ist $\operatorname{Deg} p = \operatorname{Deg} q < \infty$, so sind p und q assoziiert zu $X^{\operatorname{Deg} p}$.*

(iii) *Ist $\operatorname{Deg} p \geq \operatorname{Deg} q$, so ist $q \mid p$.*

Beweis. ***(i)***

$p = \sum_{i=0}^{\infty} a_i X^i$ ist genau dann invertierbar, wenn a_0 invertierbar ist, also genau dann wenn $a_0 \neq 0$, was wiederum äquivalent zu $\operatorname{Deg} a_0 = 0$ ist.

(ii)

Ist $p = q = 0$ so ist nichts zu zeigen. Ansonsten ist $p = \sum_{i=0}^{\infty} a_i X^i \neq 0$, also $p = X^{\operatorname{Deg} p} p'$ für $p' = \sum_{i=0}^{\infty} a_{i+\operatorname{Deg} p} X^i$ mit $a_{\operatorname{Deg} p} \neq 0$. Nach *(i)* ist p' invertierbar, also p assoziiert zu $X^{\operatorname{Deg} p}$. Analog ergibt sich, dass q assoziiert zu $X^{\operatorname{Deg} q}$ ist. Mit $\operatorname{Deg} p = \operatorname{Deg} q$ folgt damit auch die Assoziiertheit von p und q.

(iii)

Ist $\operatorname{Deg} p = \infty$, so ist $p = 0$ und nichts zu zeigen. Ansonsten ist $p = X^{\operatorname{Deg} p - \operatorname{Deg} q} p'$ wobei p' assozziert zu q ist, also $p = X^{\operatorname{Deg} p - \operatorname{Deg} q} cq$ für $c \in K^*$. □

(iii)

f ist in $\mathbb{Z}[X]$ nicht irreduzibel, da $f = (X+1)(X+2)$.
Seien $p, q \in \mathbb{Z}[\![x]\!]$ mit $p = \sum_{i=0}^{\infty} a_i X^i$ und $q = \sum_{j=0}^{\infty} b_i X^i$ so dass $pq = f$. Dann ergibt sich durch Koeffizientenvergleich, dass $a_0 b_0 = 2$. Da $a_0, b_0 \in \mathbb{Z}$, und $2 \in \mathbb{Z}$ irreduzibel ist, ist a_0 oder b_0 eine Einheit. Entsprechend ist p oder q eine Einheit. Also ist f irreduzibel in $\mathbb{Z}[\![x]\!]$.

Aufgabe 7.5.

Lemma 4. *$K[\![x]\!]$ bildet mit der Gradabbildung* Deg *einen euklidischen Ring.*

Beweis. Da K nullteilerfrei ist, ist $K[\![x]\!]$ ein Integritätsring. Seien $f, g \in K[\![x]\!]$ mit $g \neq 0$. Es gilt zu zeigen, dass es $q, r \in K[\![x]\!]$ gibt, so dass $f = qg + r$ mit $r = 0$ oder $\operatorname{Deg} r < \operatorname{Deg} g$. Ist $\operatorname{Deg} f < \operatorname{Deg} g$ so genügt es $q = 0$ und $r = f$ zu wählen. Ist $\operatorname{Deg} f \geq \operatorname{Deg} g$, so folgt aus 3, dass $g \mid f$, es kann also q mit $f = qg$ und $r = 0$ gewählt werden. □

Aus Lemma 4 folgt direkt, dass $K[\![x]\!]$ ein Hautidealring ist. Für jedes Ideal $(a) \neq 0$ von $K[\![x]\!]$ folgt mit Lemma 3, dass a assoziert zu $X^{\operatorname{Deg} a}$ ist, und da $K[\![x]\!]$ ein Integritätsring ist, daher $(a) = \left(X^{\operatorname{Deg} a}\right)$. Folglich sind die Ideale in $K[\![x]\!]$ gerade 0 und (X^n) für $n \in \mathbb{N}$. Insbesondere ist (X) das eindeutige maximale Ideal in $K[\![x]\!]$, weshalb $K[\![x]\!]$ lokal ist (dies lässt sich auch direkt aus Lemma 3 folgern).