

EINFÜHRUNG IN DIE ALGEBRA

BLATT 7

Jendrik Stelzner

23. Januar 2014

Aufgabe 7.1.

Für $x, y \in \mathbb{C}$ mit $xy = 1$ muss $|x||y| = 1$, also $|x| \leq 1$ oder $|y| \leq 1$. Die einzigen Elemente $z \in \mathbb{Z}[\sqrt{-n}]$ mit $|z| \leq 1$ sind $\{1, -1\}$ für $n > 1$ und $\{1, -1, i, -i\}$ für $n = 1$. Für $x, y \in \mathbb{Z}[\sqrt{-n}]$ mit $xy = 1$ ist also $x \in \{1, -1\}$ oder $y \in \{1, -1\}$ für $n > 1$ und $x \in \{1, -1, i, -i\}$ oder $y \in \{1, -1, i, -i\}$ für $n = 1$. Da all diese Elemente in $\mathbb{Z}[\sqrt{-n}]$ invertierbar sind, ist daher

$$(\mathbb{Z}[\sqrt{-n}])^* = \begin{cases} \{1, -1, i, -i\} & \text{für } n = 1, \\ \{1, -1\} & \text{für } n > 1. \end{cases}$$

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 zudem 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

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

Einfaches Hinsehen und gegebenenfalls 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 $\mathbb{Z}[\sqrt{-n}]$, die sich nun nach den obigen Zusammenhängen ergeben, sind also

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

Aufgabe 7.3.

Definition. Für einen Ring R bezeichnet

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

das Nilradikal von R .

Bemerkung 1. Sei R ein kommutativer Ring. Dann gilt

- (i) $\text{nil}(R)$ ist ein Ideal von R .
- (ii) Für $e \in R^*$ und $a \in \text{nil}(R)$ ist $e + a \in R^*$.

Beweis. (i)

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

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

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

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

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

(ii)

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

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

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

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

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

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 $a_i \in \text{nil}(R)$ für alle $i > 0$ 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 $g = \sum_{i=0}^m b_i X^i \in R[X]$, mit $m \geq 0$ und $b_m \neq 0$, so dass $fg = 1$. Da insbesondere $a_0 b_0 = 1$ müssen a_0 und b_0 in R invertierbar sein. Für $n = 0$ ist nichts weiter zu zeigen. Ist $n > 0$, so bemerken wir:

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

Beweis. Der Beweis verläuft per Induktion über k .

Induktionsanfang. Betrachte $k = 0$. Wäre $a_n b_m \neq 0$, so wäre

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

Induktionsschritt. Sei $1 \leq k \leq n$ und gelte die Aussage für $0, \dots, k-1$. Da $fg = 1$ ergibt sich für den $n+m-k$ -ten Koeffizienten des Produktes fg , dass

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

Multiplikation der Gleichung mit a_n^k ergibt

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

□

Aus Behauptung 2 folgt insbesondere, dass $a_n^{m+1} b_0 = 0$. Da b_0 invertierbar ist, ist $a_n^{m+1} = 0$, also a_n 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 $f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ bezeichnet

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

den Grad von f .

Bemerkung 3. Für einen kommutativen Ring R und $f, g \in R[[X]]$ ist

$$\begin{aligned} \text{Deg}(f+g) &\geq \min\{\text{Deg}(f), \text{Deg}(g)\} \text{ und} \\ \text{Deg}(fg) &\geq \text{Deg}(f) + \text{Deg}(g). \end{aligned}$$

Ist R darüber hinaus nullteilerfrei, so gilt sogar

$$\text{Deg}(fg) = \text{Deg}(f) + \text{Deg}(g).$$

Beweis. Der Beweis läuft analog zu dem der entsprechenden (Un)gleichungen der Gradfunktion \deg von $R[X]$. □

(i)

Ist R kein Integritätsring, so auch $R[[X]]$ nicht, da man R in kanonischer Weise als Unterring von $R[[X]]$ auffassen kann. Ist $R[[X]]$ kein Integritätsring, so gibt es $f, g \in R[[X]]$ mit $f, g \neq 0$, also $\text{Deg}(f), \text{Deg}(g) < \infty$, aber $fg = 0$, also $\text{Deg}(fg) = \infty$. Aus Bemerkung 3 folgt, dass R kein Integritätsring ist.

(ii)

Ist $f = \sum_{i=0}^{\infty} a_i X^i \in R[[x]]$ invertierbar, so gibt es $g = \sum_{i=0}^{\infty} b_i X^i \in R[[x]]$ mit $fg = 1$. Insbesondere ergibt sich für den 0-ten Koeffizienten von fg , dass $1 = a_0 b_0$. Also ist a_0 invertierbar in R .

Ist $f = \sum_{i=0}^{\infty} a_i X^i \in R[[x]]$ 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 definieren $g := \sum_{i=0}^{\infty} b_i X^i$ als die entsprechende Potenzreihe. Es ergibt sich für $fg =: e = \sum_{i=0}^{\infty} e_i X^i$, dass $e_0 = a_0 b_0 = 1$ und für alle $i \geq 1$

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

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

Lemma 4. Sei K ein Körper und seien $f, g \in K[[x]]$. Dann gilt:

(i) f ist genau dann invertierbar, wenn $\text{Deg } f = 0$.

(ii) Ist $\text{Deg } f = \text{Deg } g$, so sind f und g assoziiert. Genauer: Ist $\text{Deg } f < \infty$, so ist f assoziiert zu $X^{\text{Deg } f}$.

(iii) Ist $\text{Deg } f \leq \text{Deg } g$, so ist $f \mid g$.

Beweis. (i)

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

(ii)

Ist $f = g = 0$ so ist nichts zu zeigen. Ansonsten ist $f = \sum_{i=0}^{\infty} a_i X^i \neq 0$, also $f = X^{\text{Deg } f} f'$ mit $f' = \sum_{i=0}^{\infty} a_{i+\text{Deg } f} X^i$ und $a_{\text{Deg } f} \neq 0$. Nach (i) ist f' invertierbar, also f assoziiert zu $X^{\text{Deg } f}$.

(iii)

Ist $\text{Deg } g = \infty$, so ist $g = 0$ und nichts zu zeigen. Ansonsten ist $g = X^{\text{Deg } g - \text{Deg } f} g'$, wobei g' wegen $\text{Deg } g' = \text{Deg } f$ assoziiert zu f ist, also $g = X^{\text{Deg } g - \text{Deg } f} c f$ für $c \in K^*$. \square

(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 $q = \sum_{j=0}^{\infty} b_j X^j$ so dass $pq = f$. Dann ist $a_0 b_0 = 2$. Da $a_0, b_0 \in \mathbb{Z}$, und 2 in \mathbb{Z} irreduzibel ist, ist a_0 oder b_0 eine Einheit in \mathbb{Z} . Entsprechend ist p oder q nach dem vorherigen Aufgabenteil eine Einheit. Also ist f irreduzibel in $\mathbb{Z}[[x]]$.

Aufgabe 7.5.

Lemma 5. $K[[x]]$ 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 $\text{Deg } r < \text{Deg } g$.

Ist $\text{Deg } f < \text{Deg } g$ so genügt es $q = 0$ und $r = f$ zu wählen. Ist $\text{Deg } f \geq \text{Deg } g$, so folgt aus Lemma 4, dass $g \mid f$, es kann also q mit $f = qg$ und $r = 0$ gewählt werden. \square

Aus Lemma 5 folgt direkt, dass $K[[x]]$ ein Hauptidealring ist. Für jedes Ideal $(a) \neq 0$ von $K[[x]]$ folgt mit Lemma 4, dass a assoziiert zu $X^{\text{Deg } a}$ ist, und da $K[[x]]$ ein Integritätsring ist, daher $(a) = (X^{\text{Deg } a})$. 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 4 folgern).