

Musterlösung zur Serie 10

Algebra und Zahlentheorie und ihre Didaktik

Dr. Daniel Skodlerack

3. Juli 2017

Ab jetzt beinhaltet „unitärer Ring“, bzw. „Ring mit Eins“, immer die Forderung $1 \neq 0$.

Aufgabe 1. (5+5 Punkte)(Grad eines Polynoms) Es sei R ein unitärer Ring.

1. Zeigen Sie, dass für je zwei Elemente $P, Q \in R[X]$ die Ungleichung

$$\deg(PQ) \leq \deg(P) + \deg(Q) \quad (1)$$

gilt. Geben Sie ein Beispiel für R an, in dem in (1) für geeignete P und Q eine echte Ungleichung steht. Zeigen Sie, dass für alle Paare (P, Q) in (1) die Gleichheit gilt, falls R ein Integritätsbereich ist.

2. Gegeben seien $P, Q \in R[X]$, so dass der Leitkoeffizient von Q eine Einheit von R ist. Zeigen Sie, dass Polynome $S, T \in R[X]$ existieren, so dass der Grad von T kleiner als der Grad von Q ist und $P = QS + T$ gilt. Zeigen Sie, dass diese Darstellung eindeutig ist, also für Polynome $S', T' \in R[X]$, wobei T' einen kleineren Grad als Q hat, aus der Gleichung $P = QS' + T'$ die Gleichungen $S = S'$ und $T = T'$ folgen.

Lösung:

1. Wenn eines der beiden Polynome gleich dem Nullpolynom ist, dann steht auf beiden Seiten der Ungleichung (1) minus unendlich und wir erhalten sogar eine Gleichung. Es seien $P = \sum_{i=0}^l a_i x^i$ und $Q = \sum_{i=0}^k b_i x^i$ mit $a_l \neq 0$ und $b_k \neq 0$. Dann verschwindet in PQ der Koeffizient vor x^j für $j > l + k$. Also gilt $\deg(PQ) \leq l + k = \deg(P) + \deg(Q)$. In $\mathbb{Z}/4\mathbb{Z}[x]$ gilt:

$$-\infty = \deg(0) = \deg([2]_4 X \cdot [2]_4 X) < 2 = \deg([2]_4 X) + \deg([2]_4 X).$$

Wenn R nullteilerfrei ist, dann folgt aus dem Fakt, dass a_l und b_k ungleich null sind, dass auch $a_l b_k$ ungleich null ist, und deshalb steht dann in (1) sogar die umgekehrte Ungleichung, also eine Gleichung.

2. Wir zeigen zunächst die Existenz. Wir führen eine Induktion über den Grad von P . Im Fall $\deg(P) < \deg(Q)$ setzen wir einfach $S := 0$ und $T := P$. Wir betrachten nun den Fall $\deg(P) \geq \deg(Q)$. Es seien a der Leitkoeffizient von P und b der von Q . Dann hat $U := P - ab^{-1}X^{\deg(P)-\deg(Q)}Q$ einen kleineren Grad als P also nach Induktionsvoraussetzung existieren $S, T \in R[X]$, so dass $U = SQ + T$ und $\deg(T) < \deg(Q)$. Also erhalten wir für P :

$$P = (ab^{-1}X^{\deg(P)-\deg(Q)} + S)Q + T,$$

womit die Existenz durch vollständige Induktion bewiesen ist. Wir kommen nun zur Eindeutigkeit. Wir haben also $P = SQ + T = S'Q + T'$, wobei sowohl T als auch T' einen kleineren Grad als Q haben. Angenommen $S \neq S'$. Wir schreiben die Polynome S, S' und Q aus.

$$S = \sum_{i \geq 0} s_i X^i, \quad S' = \sum_{i \geq 0} s'_i X^i, \quad Q = \sum_{i \geq 0} q_i X^i.$$

Es sei i_0 das größte Element in $\mathbb{N}_0$, so dass sich die Koeffizienten s_{i_0} und s'_{i_0} unterscheiden. Dann unterscheiden sich die Koeffizienten von QS und QS' vor $X^{\deg(Q)+i_0}$, wie eine leichte Rechnung zeigt, wobei ausgenutzt wird, dass der Leitkoeffizient von Q eine Einheit ist. Wir bezeichnen den letzten Satz mit (*).

Der Koeffizient von P vor $X^{\deg(Q)+i_0}$ ist aber gerade der entsprechende Koeffizient von QS , da T aufgrund seines geringen Grades keinen Beitrag leistet. Analoges gilt für den Vergleich von P mit QS' . Also haben QS und QS' vor $X^{\deg(Q)+i_0}$ den gleichen Koeffizienten wie P . Das ist aber ein Widerspruch zur Aussage (*). Folglich ist die Annahme falsch, und S und S' müssen übereinstimmen. Daraus folgt aufgrund der Gleichungen, dass auch T und T' übereinstimmen.

Aufgabe 2. (5+5*+5)(Primfaktorzerlegung)

1. Zeigen Sie, dass das Ideal $(X - 3, 21)_{\mathbb{Z}[X]}$ kein Primideal von $\mathbb{Z}[X]$ ist.
- 2.* Es seien R ein unitärer Ring und a ein Element aus $R \setminus (R^\times \cup \{0\})$. Zeigen Sie, dass Ra genau dann ein Primideal von R ist, wenn a ein Primelement von R ist.
3. Finden Sie in $\mathbb{Q}[X]$ die Primfaktorzerlegung des folgenden Polynoms

$$X^5 - 2X^4 - 25X + 50,$$

wobei jeder Primfaktor normiert sein soll. (Ein Polynom heißt normiert, wenn der Leitkoeffizient gleich 1 ist.) Vergessen Sie nicht zu zeigen, dass die gefundenen Polynome auch Primelemente von $\mathbb{Q}[X]$ sind.

Lösung:

1. Wir setzen $I := (X - 3, 21)_{\mathbb{Z}[X]}$. Es ist I die Menge aller möglichen Linearkombinationen von $X - 3$ und 21 mit Koeffizienten in $\mathbb{Z}[X]$. Deshalb erfüllen alle Elemente von I : $3|P(0)$ und $7|P(3)$. Die konstanten Polynome 3 und 7 erfüllen jeweils nur eine der beiden Teilbarkeiten. Deshalb liegen 3 und 7 nicht in I . Das Element 21 liegt aber in I . Also ist I kein Primideal von $\mathbb{Z}[X]$.
2. Es ist aR genau dann ein Primideal von R , wenn für alle Paare $(b, c) \in R^2$ aus $bc \in aR$ folgt, dass b oder c ein Element von aR ist. Also genau dann, wenn für alle Paare $(b, c) \in R^2$ aus $a|bc$ (das ist äquivalent zu $bc \in aR$) folgt, dass b oder c durch a teilbar ist. Also genau dann, wenn a ein Primelement von R ist.

3. Es gilt:

$$X^5 - 2X^4 - 25X + 50 = (X^2 + 5)(X^2 - 5)(X - 2).$$

Die Polynome $X^2 + 5$ und $X^2 - 5$ sind irreduzibel, da sie den Grad 2 haben und keine Nullstelle in $\mathbb{Q}$ besitzen, und $X - 2$ ist irreduzibel, da bei einer Faktorisierung einer der Faktoren den Grad null haben muss. Nach Lemma 84 sind deshalb alle drei Polynome Primelemente in $\mathbb{Q}[X]$.

Aufgabe 3. (5+5 Punkte)(Nullteiler)

1. Finden Sie alle Nullteiler von $\mathbb{Z}/24\mathbb{Z}$. Es sei m eine natürliche Zahl größer als 1. Zeigen Sie, dass die Menge der Nullteiler von $\mathbb{Z}/m\mathbb{Z}$ mit $(\mathbb{Z}/m\mathbb{Z}) \setminus (\mathbb{Z}/m\mathbb{Z})^\times$ übereinstimmt.
2. Finden Sie einen unendlichen unitären Ring, in dem jedes Element ungleich Eins ein Nullteiler ist.

Lösung:

1. Aus der Vorlesung wissen wir, dass $(\mathbb{Z}/m\mathbb{Z}) \setminus (\mathbb{Z}/m\mathbb{Z})^\times$ genau aus den Resklassen $[a]_m$ besteht, für die a nicht teilerfremd zu m ist. Wir betrachten nun eine solche Resklasse $[a]_m$. Es sei t der größte gemeinsame Teiler von a und m . Nach der Wahl von a ist t größer als 1, und wir bezeichnen den Komplementärteiler von m zu t mit m' , d.h. $m't = m$. Insbesondere ist die natürliche Zahl m' kleiner als m , da t größer als 1 ist. Also ist $[m']_m \neq [0]_m$, und es ist m ein Teiler von am' und $[a]_m$ somit ein Nullteiler von $\mathbb{Z}/m\mathbb{Z}$. Andererseits ist jeder Nullteiler von $\mathbb{Z}/m\mathbb{Z}$ keine Einheit, denn das Produkt einer Einheit mit einem Element ungleich null ist wieder ein Element ungleich null. Damit ist der zweite Teil von 3.1 gezeigt. Die Nullteiler von $\mathbb{Z}/24\mathbb{Z}$ sind also nach obigem die Restklassen $[a]_{24}$, wobei a die Elemente in $\mathbb{N}^{\leq 24}$ durchläuft, die durch 2 oder 3 teilbar sind. Also erhalten wir genau die folgenden Nullteiler:

$$[2]_{24}, [3]_{24}, [4]_{24}, [6]_{24}, [8]_{24}, [9]_{24}, [10]_{24}, [12]_{24}, [14]_{24}, [15]_{24}, [16]_{24}, [18]_{24}, [20]_{24}, [21]_{24}, [22]_{24}, [24]_{24}.$$

2. Es sei M eine unendliche Menge. Dann gilt für alle Elemente N von $\mathfrak{P}(M) \setminus \{M\}$, dass der Schnitt von N mit $M \setminus N$ leer ist. In dem Ring $(\mathfrak{P}(M), \Delta, \cap)$ ist folglich jedes Element ungleich eins ein Nullteiler.

Aufgabe 4. (5+5* Punkte)(Primelemente und irreduzible Elemente)

1. Es sei R ein Integritätsbereich. Zeigen Sie, dass jedes Primelement von R irreduzibel ist.
- 2.* Es sei $P = \sum_{i=0}^l a_i X^i$ ein normiertes Polynom in X mit ganzzahligen Koeffizienten. Zeigen Sie, dass P genau dann ein Primelement von $\mathbb{Z}[X]$ ist, wenn es ein Primelement von $\mathbb{Q}[X]$ ist.

Lösung:

1. Es sei a ein Primelement von R , und es seien b und c zwei weitere Elemente des selbigen, so dass $a = bc$. Da a ein Primelement ist, folgt $a|b$ oder $a|c$. Ohne Einschränkung gelte ersteres. Dann gibt es ein Element d in R , so dass $da = b$ gilt. Dann folgt aber $adc = bc = a$ und folglich $a(dc - 1) = 0$. Aus der Nullteilerfreiheit von R und $a \neq 0$ (da prim) folgt: $dc - 1 = 0$, also $dc = 1$. Deshalb ist c eine Einheit. Außerdem ist a als Primelement kein Element von $R^\times \cup \{0\}$. Damit ist gezeigt, dass a irreduzibel ist.
2. Wir müssen hier zwei Richtungen zeigen. Wir beginnen mit der folgenden.

Wir zeigen, dass P ein Primelement von $\mathbb{Z}[X]$ ist, wenn es ein Primelement von $\mathbb{Q}[X]$ ist. Es sei als erstes erwähnt, dass aus $P \notin \mathbb{Q} = \mathbb{Q}[X]^\times \cup \{0\}$ folgt, dass P einen positiven Grad haben muss und deshalb weder eine Einheit von $\mathbb{Z}[X]$ noch gleich dem Nullelement sein kann. Es seien nun S, T Elemente von $\mathbb{Z}[X]$, so dass P das Produkt ST teilt. Aus der Primelementeigenschaft in $\mathbb{Q}[X]$ folgt, dass P einen der beiden Faktoren in $\mathbb{Q}[X]$ teilt. Ohne Einschränkung sei dies S , etwa $S = PR$ für ein Element $R \in \mathbb{Q}[X]$. Wir müssen zeigen, dass alle Koeffizienten von R ganzzahlig sind. Wir bezeichnen die Koeffizienten von R mit r_j und analog die Koeffizienten von S und P mit s_j bzw. p_j . Angenommen R ist kein Element $\mathbb{Z}[X]$, dann gibt es einen maximalen Index j_0 , so dass r_{j_0} keine ganze Zahl ist. Dann ist auch die folgende Summe keine ganze Zahl.

$$\sum_{j+i=j_0+\deg(P)} r_j p_i = r_{j_0} + r_{j_0+1} p_{\deg(P)-1} + \dots + r_{\deg(P)+j_0} p_0.$$

(Hier wurde verwendet, dass P normiert ist.) Diese Summe stimmt aber mit $s_{j_0+\deg(P)}$ überein, und muss deshalb ganzzahlig sein. Ein Widerspruch. Also sind doch alle Koeffizienten von R ganzzahlig, und P teilt S in $\mathbb{Z}[X]$. Damit ist gezeigt, dass P ein Primelement von $\mathbb{Z}[X]$ ist.

Wir zeigen nun die andere Richtung. Der Grad von P ist größer gleich eins, da P normiert ist, und P als Primelement von $\mathbb{Z}[X]$ ungleich eins sein muss. Also ist P auch keine Einheit von $\mathbb{Q}[X]$ und ungleich null. Es seien S und T zwei Elemente von $\mathbb{Q}[X]$, so dass dessen Produkt durch P teilbar ist. Es sei b ein gemeinsamer Nenner der Koeffizienten von S , und wir bilden $\tilde{S} := bS \in \mathbb{Z}[X]$. Analog bilden wir $\tilde{T} = cT \in \mathbb{Z}[X]$. Dann teilt P das Produkt $\tilde{S}\tilde{T}$ in $\mathbb{Q}[X]$ und mit dem selben Argument, wie in der vorangegangenen Richtung, folgt, dass es das Produkt in $\mathbb{Z}[X]$ teilt. Deshalb teilt P einen der Faktoren $\tilde{S}, \tilde{T}$, da P ein Primelement von $\mathbb{Z}[X]$ ist. Ohne Einschränkung teile P das Polynom $\tilde{S}$. Dann teilt P auch das Polynom $\tilde{S}$ in $\mathbb{Q}[X]$ und deshalb auch das Polynom S in $\mathbb{Q}[X]$. Damit ist der Beweis der Rückrichtung erbracht.