Mathematische Strukturen – Lösungen zu Übungsblatt 6

Hagen Knaf, SS 2016

1. Welche der folgenden Polynomfunktionen sind Primelemente im Ring $\mathrm{Pol}_{\mathbb{Z}}(\mathbb{R},\mathbb{R})$ der Polynomfunktionen mit ganzzahligen Koeffizienten:

   - $35x + 56$,
   - 13,
   - $3x^2 - 7x + 2$,
   - $8x^3 - 1$.

   Lösung:

   - Es gilt $35x+56 = 7(5x+8)$ und weder 7 noch $5x+8$ sind Einheiten in $\mathrm{Pol}_{\mathbb{Z}}(\mathbb{R},\mathbb{R})$, denn die Einheiten dieses Rings sind die konstanten Polynome $\{-1, 1\}$, wie in der Vorlesung gezeigt wurde. Folglich ist das Element $35x + 56$ nicht irreduzibel. Da jedes Primelement irreduzibel ist, ist $35x + 56$ also kein Primelement.
   - 13 kann als konstantes Polynom nur in konstante Faktoren zerlegt werden. Da 13 eine Primzahl ist, gibt es solche nicht, das heißt 13 ist irreduzibel. Da in $\mathrm{Pol}_{\mathbb{Z}}(\mathbb{R},\mathbb{R})$ *kein* euklidischer Ring ist, können irreduzible und Prrimelemente verschieden sein. Wir kommen hier also nicht weiter und müssen versuchen die Primelementeigenschaft direkt zu beweisen oder zu widerlegen.

     Es seien also f, g Polynome mit ganzzahligen Koeffizienten mit der Eigenschaft $13|(fg)$. Das bedeutet alle Koeffizienten von fg sind durch 13 teilbar. Falls 13 ein Primelement ist, muss dann $13|f$ oder $13|g$ gelten, dass heißt entweder sind alle Koeffizienten von f oder alle Koeffizienten von g durch 13 teilbar. Um ein Gefühl für die Situation zu bekommen, probiert man einige Fälle aus: Seien $f(x) = a_1x + a_0$ und $g(x) = b_1x + b_0$. Dann gilt

     $$fg = a_1b_1x^2 + (a_1b_0 + a_0b_1)x + a_0b_0.$$

     Aus $13|(fg)$ folgt dann $13|a_1b_1$, da 13 eine Primzahl ist, also $13|a_1$ oder $13|b_1$. Nehmen wir den ersten Fall an. Dann liest man an der Darstellung

     $$fg = a_1xg + a_0g$$

ab, dass $13|(a_1xg)$ gilt, folglich auch $13|(a_0g)$, das heißt $13|a_0b_0$ und $13|a_0b_1$. Aus der letzten Relation folgt $13|a_0$ oder 13 teilt a_0 nicht und $13|b_1$. Im ersten Fall ergibt sich $13|f$. Im zweiten Fall liefert $13|a_0b_0$ die Teilbarkeit $13|b_0$ also $13|g$. Insgesamt wurde die Vermutung bestätigt. Den Fall, dass $p|b_1$ gilt, behandelt man genauso.

Wir behaupten also allgemein: 13 ist ein Primelement von $\mathrm{Pol}_{\mathbb{Z}}(\mathbb{R},\mathbb{R})$, das heißt aus $13|(fg)$ folgt stets $13|f$ oder $13|g$.

Es ist naheliegend den Beweis dafür durch Induktion nach dem Grad n des Produkts fg zu führen.

Induktionsanfang $n = 0$: In diesem Fall sind auch f und g konstante Polynome und die Behauptung folgt aus der Tatsache, dass 13 eine Primzahl ist.

Induktionsschritt: Es gelte $n > 0$ und $f = a_sx^s + f_0$, $g = b_tx^t + g_0$ mit $s = \deg(f)$ und $t = \deg(g)$. Dann ist der Leitkoeffizient a_sb_t durch 13 teilbar, also kann man ohne Einschränkung $13|a_s$ annehmen.

Ist $s = 0$, so ist nichts mehr zu beweisen. Wie können also $s > 0$ annehmen. Es gilt

$$f = a_sx^sg + f_0g.$$

mit $13|(a_sx^sg)$ also $13|(f_0g)$. Der Grad des Produkts f_0g ist kleiner als n, es folgt also nach Induktionsannahme $13|f_0$ oder $13|g$. Im zweiten Fall ist der Induktionsschritt vollzogen. Im ersten Fall sind alle Koeffizienten von f_0, also alle bis auf a_s, durch 13 teilbar. Da a_s nach Voraussetzung durch 13 teilbar ist, folgt in diesem Fall $13|f$ und der Induktionsschritt ist ebenfalls abgeschlossen.

- Die Lösungformel für quadratische Gleichungen liefert

$$x_{1,2} = \frac{7}{6} \overset{+}{-} \sqrt{(\frac{7}{6})^2 - \frac{2}{3}} = \frac{7}{6} \overset{+}{-} \sqrt{\frac{49-24}{36}} = \frac{5}{6},$$

also die rationalen Nullstellen $x_1 = 2$ und $x_2 = \frac{1}{3}$. Es folgt

$$3x^2 - 7x + 2 = (x-2)(3x-1),$$

womit das Polynom nicht irreduzibel und daher kein Primelement ist.

- Da die Koeffizienten von $8x^3 - 1$ keinen gemeinsamen Teiler haben, kann man dieses Element nicht in der Form $c \cdot p$ zerlegen,

wobei $c \in \mathbb{Z} \setminus \{-1, 1\}$ gilt. Das Polynom besitzt als einzige reelle Nullstelle $x = \frac{1}{2}$, eine Zerlegung in nichtkonstante Polynome muss also so aussehen: $(2x - 1)q$. Polynomdivision liefert

$$(8x^3 - 1) : (2x - 1) = 4x^2 + 2x + 1,$$

womit $8x^3 - 1$ nicht irreduzibel also keine Primelement ist.

2. Bestimmen Sie mit dem Verfahren von Kronecker alle rationalen Nullstellen $q \in \mathbb{Q}$ des Polynoms

$$p(x) := x^4 + \frac{183}{77}x^3 + \frac{236}{77}x^2 - \frac{255}{77}x - \frac{25}{77}$$

und führen Sie eine Polynomdivision durch die zu den Nullstellen gehörenden Faktoren $x - q$ durch.

3. Zeigen Sie, dass im Ring $\mathbb{Z}[i]$ die Zahl 5 kein Primelement ist, wohl aber die Zahl 3. Verwenden Sie dabei wie in der Vorlesung bei der Bestimmung der Einheiten von $\mathbb{Z}[i]$ die komplexe Betragsfunktion.

   LÖSUNG: Aus der Vorlesung ist bekannt: $\alpha \in \mathbb{Z}[i]$ ist genau dann eine Einheit, wenn $|\alpha|^2 = 1$ gilt, wobei $|\alpha|$ der Betrag der Zahl α ist.

   Sei nun α *keine* Einheit und $\alpha = \beta\gamma$. Dann gilt $|\alpha|^2 = |\beta|^2|\gamma|^2$, das heißt das Quadrat des Betrags jedes Teilers von α in $\mathbb{Z}[i]$ ist ein Teiler von $|\alpha|^2$ in $\mathbb{Z}$. Man beachte dabei, dass für $\alpha \in \mathbb{Z}[i]$ stets $|\alpha|^2 \in \mathbb{Z}$ gilt.

   Es gilt $|3|^2 = 9$. Ein *echter* Teiler $d \in \mathbb{Z}[i]$ von 3, also $d \neq 3$ und d keine Einheit, muss die Eigenschaft $|d|^2 = 3$ besitzen. Sei $d = z + wi$. Dann gilt also $3 = |d|^2 = z^2 + w^2$ mit gewissen $z, w \in \mathbb{Z}$. Solche Zahlen gibt es nicht.

   Dagegen muss für einen echten Teiler $d = z + wi$ von 5 die Gleichung $5 = z^2 + w^2$ gelten, also zum Beispiel $z = 2$ und $w = 1$. Tatsächlich gilt

$$5 = (2 + i)(2 - i),$$

   womit 5 nicht irreduzibel also kein Primelement ist. Man beachte dabei, dass $2 + i$ und $2 - i$ keine Einheiten sind.

4. Es seien

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ und } B := \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}.$$

Zeigen Sie, dass die Menge R aller Matrizen $C \in \mathbb{R}^{2\times 2}$, die sich als Summe $M_1 + M_2 + \ldots + M_r$ einer beliebigen Zahl $r \in \mathbb{N}$ von Matrizen der Form

$$zE \cdot A^k \cdot B^\ell,\ z \in \mathbb{Z},\ E \text{ die Einheitsmatrix},$$

schreiben lassen, bezüglich Matrixaddition und -multiplikation einen kommutativen Ring bilden.

Gibt es in diesem Ring Nullteiler? Gibt es von 0 verschiedene nilpotente Elemente?

Lösungsskizze:

- Die Matrizen A und B sind vertauschbar: $AB = BA$.
- Damit sind zwei beliebige Matrizen der Form $zE \cdot A^k \cdot B^\ell$ vertauschbar.
- Nach dem Distributivgesetz sind dann alle Matrizen in R vertauschbar, woraus sich ergibt, dass R ein kommutativer Ring ist.
- Die Matrix $B - A$ ist nilpotent.