Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Martin Lüdtke

Grundlagen der Algebra

Sommersemester 2019

Übungsblatt 5 25. Juni 2019

Aufgabe 17. (3 Punkte)

Sei K ein Körper. Zeigen Sie, dass der Polynomring $K[X]$ unendlich viele normierte irreduzible Polynome enthält.
Hinweis: Folgen Sie dem Euklidischen Beweis für den Ring $\mathbb{Z}$.

Lösungsskizze zu Aufgabe 17:

Sei $p_1, \ldots, p_r$ eine endliche Liste von irreduziblen normierten Polynomen. Wir zeigen, dass es ein weiteres gibt, das noch nicht in der Liste enthalten ist. Wir können annehmen, dass $r \geq 1$ ist, indem wir etwa das Polynom X hinzunehmen. Betrachte das Polynom

$$f \coloneqq p_1 \cdots p_r + 1.$$

Dann ist f vom Grad $\sum \deg(p_i) \geq 1$. Sei p ein irreduzibler Teiler von f. Ein solcher existiert, da jedes Element eines Hauptidealrings eine Zerlegung als Produkt einer Einheit und irreduzibler Elemente besitzt. Alternativ kann man auch induktiv nach dem Grad argumentieren: Wenn f nicht selbst irreduzibel ist, gibt es einen nichtkonstanten Teiler $f_1 \mid f$ von kleinerem Grad. Wenn f_1 nicht irreduzibel ist, gibt es wiederum einen nichtkonstanten Teiler $f_2 \mid f_1$ von kleinerem Grad usw. Da der Grad der f_i von unten beschränkt ist, wird man irgendwann einen irreduziblen Teiler p von f erreichen.

Wir können annehmen, dass p normiert ist, indem wir durch den Leitkoeffizienten teilen, was eine Multiplikation mit einer Einheit ist. Dann ist p von $p_1, \ldots, p_r$ verschieden, denn die p_i sind wegen $f \equiv 1 \bmod p_i$ keine Teiler von f.

Bemerkung: Ist der Körper K unendlich, haben wir schon unendlich viele normierte Polynome der Form $X - a$ mit $a \in K$. Der obige Beweis gilt aber auch für endliche Körper.

Aufgabe 18. ($6 = 2{+}1{+}1{+}2$ Punkte)

(a) Sei K ein Körper und $f \in K[X]$ mit $\deg(f) \in \{2, 3\}$. Zeigen Sie: f ist genau dann irreduzibel, wenn f keine Nullstelle in K besitzt.

(b) Zeigen Sie, dass die Aussage in (a) für Polynome von Grad 4 im Allgemeinen falsch ist.

(c) Zeigen Sie, dass $f(X) = X^3 + 2X + 1$ in $\mathbb{F}_3[X]$ irreduzibel ist.

(d) Sei $\alpha \in \mathbb{F}_3[X]/(X^3 + 2X + 1)$ die Restklasse von X. Stellen Sie α^{-1} und α^5 als $\mathbb{F}_3$-Linearkombination von $1, \alpha, \alpha^2$ dar.

Lösungsskizze zu Aufgabe 18:

(a) Wenn f mit $\deg(f) \in \{2,3\}$ eine Nullstelle $a \in K$ besitzt, dann ist f durch den Linearfaktor $X-a$ teilbar, also $f = (X-a)g$ mit $\deg(g) = \deg(f)-1 \in \{1,2\}$. Da $X-a$ und g keine Einheiten sind, ist f nicht irreduzibel. Umgekehrt, angenommen f ist nicht irreduzibel, dann existiert eine Zerlegung $f = gh$, wobei g und h keine Einheiten sind, also nicht konstant. Wegen $\deg(g)+\deg(h) = \deg(f) \in \{2,3\}$ muss mindestens einer der beiden Faktoren den Grad 1 haben, etwa $h = aX + b$ mit $a \in K^\times$, $b \in K$. Dann ist $-b/a \in K$ eine Nullstelle von h, somit auch von f.

(b) Das Polynom $X^2 + 1 \in \mathbb{R}[X]$ hat keine Nullstellen in $\mathbb{R}$. Das Polynom

$$X^4 + 2X^2 + 1 = (X^2+1)^2$$

hat damit auch keine Nullstellen, dennoch ist es nicht irreduzibel.

(c) Gemäß (a) genügt es zu prüfen, dass $f(X) \coloneqq X^3 + 2X + 1$ keine Nullstelle in $\mathbb{F}_3$ besitzt. Wir prüfen dies einzeln für die drei Elemente von $\mathbb{F}_3$:

$$\begin{aligned} f(0) &= 0^3 + 2\cdot 0 + 1 = 1, \\ f(1) &= 1^3 + 2\cdot 1 + 1 = 4 = 1, \\ f(2) &= 2^3 + 2\cdot 2 + 1 = 13 = 1. \end{aligned}$$

(d) In $\mathbb{F}_3[X]/(f)$ gilt

$$\alpha^3 + 2\alpha + 1 = f(\alpha) = [f(X)] = 0.$$

Daraus folgt

$$\alpha(\alpha^2 + 2) = -1,$$

somit

$$\alpha^{-1} = -(\alpha^2+2) = 2\alpha^2 + 1.$$

Für α^5 berechnen wir durch Polynomdivision mit Rest:

$$X^5 = (X^2+1)f(X) + 2X^2 + X + 2.$$

Wegen $f(\alpha) = 0$ folgt

$$\alpha^5 = (\alpha^2+1)f(\alpha) + 2\alpha^2 + \alpha + 2 = 2\alpha^2 + \alpha + 2.$$

Aufgabe 19. (3 Punkte)

Sei R ein Hauptidealring und $x, y \in R$. Zeigen Sie, dass für $n \in \mathbb{N}$ gilt:

$$x^n \mid y^n \;\Rightarrow\; x \mid y.$$

Lösungsskizze zu Aufgabe 19:

Wir schreiben x und y jeweils als Produkt einer Einheit und endlich vieler Primelemente:

$$\begin{aligned} x &= u p_1^{e_1} \cdots p_r^{e_r}, \\ y &= v p_1^{f_1} \cdots p_r^{f_r} \end{aligned}$$

mit $u, v \in R^\times$, $e_i, f_i \in \mathbb{N}_0$ und paarweise nicht-assoziierten Primelementen $p_1, \ldots, p_r$. Hierbei können wir für x und y die gleichen p_i benutzen, indem wir nötigenfalls Faktoren

der Form p_i^0 hinzufügen. Aufgrund der eindeutigen Primfaktorzerlegung in Hauptidealringen gilt:

$$x \mid y \;\Leftrightarrow\; e_i \leq f_i \;\text{ für } i = 1, \ldots, r.$$

Für x^n und y^n haben wir die Darstellungen

$$x^n = u^n p_1^{ne_1} \cdots p_r^{ne_r},$$
$$y^n = v^n p_1^{nf_1} \cdots p_r^{nf_r},$$

wobei u^n und v^n Einheiten sind. Nun gilt:

$$\begin{aligned} x^n \mid y^n &\Leftrightarrow ne_i \leq nf_i \quad \text{für } i = 1, \ldots, r \\ &\Leftrightarrow e_i \leq f_i \quad \text{für } i = 1, \ldots, r \\ &\Leftrightarrow x \mid y. \end{aligned}$$

Aufgabe 20. (4 = 3+1 Punkte)

(a) Bestimmen Sie mit dem Euklidischen Algorithmus ganze Zahlen $a, b \in \mathbb{Z}$, so dass gilt:

$$2019a + 130b = 1.$$

(b) Bestimmen Sie eine ganze Zahl $x \in \mathbb{Z}$, so dass gilt:

$$x \equiv 1 \bmod 2019,$$
$$x \equiv 2 \bmod 130.$$

Lösungsskizze zu Aufgabe 20:

(a) Wir folgen dem euklidischen Algorithmus aus der Vorlesung. Wir setzen $r_0 \coloneqq 2019$, $r_1 \coloneqq 130$ und berechnen $r_2, r_3, \ldots$ durch wiederholte Division mit Rest (schriftliche Division):

$$r_{i-1} = q_i r_i + r_{i+1} \quad \text{mit } q_i, r_i \in \mathbb{Z},\ 0 \leq r_{i+1} < r_i,$$

bis wir $r_i = 0$ erreichen.

$$\begin{aligned} 2019 &= 15 \cdot 130 + 69, \\ 130 &= 1 \cdot 69 + 61, \\ 69 &= 1 \cdot 61 + 8, \\ 61 &= 7 \cdot 8 + 5, \\ 8 &= 1 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Wir tragen die so berechneten r_i und q_i in eine Tabelle ein und berechnen s_i und t_i rekursiv durch

$$\begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und für $i \geq 1$:

$$s_{i+1} \coloneqq s_{i-1} - q_i s_i,$$
$$t_{i+1} \coloneqq t_{i-1} - q_i t_i.$$

Das liefert:

i	r_i	q_i	s_i	t_i
0	2019	–	1	0
1	130	15	0	1
2	96	1	1	-15
3	61	1	-1	16
4	8	7	2	-31
5	5	1	-15	233
6	3	1	17	-264
7	2	1	-32	497
8	1	2	49	-761
9	0			

Aus der Zeile $i = 8$ lesen wir ab:

$$1 = 2019 \cdot 49 - 130 \cdot 761, \qquad (\star)$$

somit erfüllt $(a, b) \coloneqq (49, -761)$ die Anforderung.

(b) Wir setzen

$$e_1 \coloneqq -130 \cdot 761 = -98930,$$
$$e_2 \coloneqq 2019 \cdot 49 = 1 - e_1 = 98931.$$

Betrachten wir die Gleichung $(\star)$ modulo 2019 bzw. 130, sehen wir

$$e_1 \equiv 1 \bmod 2019, \quad e_1 \equiv 0 \bmod 130,$$
$$e_2 \equiv 0 \bmod 2019, \quad e_2 \equiv 1 \bmod 130,$$

d.h. e_1 und e_2 sind Urbilder von $(1, 0)$ bzw. $(0, 1)$ unter dem Isomorphismus aus dem chinesischen Restsatz

$$\mathbb{Z}/(2019 \cdot 130)\mathbb{Z} \cong \mathbb{Z}/2019\mathbb{Z} \times \mathbb{Z}/130\mathbb{Z}, \quad x \mapsto (x \bmod 2019, x \bmod 130).$$

Ein Urbild x von $(1, 2)$ wie gesucht ist somit

$$1 \cdot e_1 + 2 \cdot e_2 = e_1 + 2(1 - e_1) = 2 - e_1 = 98932.$$

Man überprüft, dass in der Tat gilt:

$$98932 \equiv 1 \bmod 2019,$$
$$98932 \equiv 2 \bmod 130.$$

Abgabe: Am kommenden Dienstag, den **2. Juli 2019**, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6–8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/76786679/Grundlagen_der_Algebra`