UE Einführung in die Algebra und Diskrete Mathematik
KV Algebra und Diskrete Mathematik

10. Übungszettel, 4. Juni 2013

Lösungen

1. Beweisen Sie den Vandermonde'schen Faltungssatz (Satz 17.6 im Skript).

2. Sei I die Menge aller Polynome über $\mathbb{Z}_3$, welche die Nullfunktion induzieren. Zeigen Sie, dass I ein Ideal von $\mathbb{Z}_3[x]$ ist.

   Lösung:
   Sei $p \in I$, d.h. $p \in \mathbb{Z}_3[x]$ und $p(a) = 0$, für alle $a \in \mathbb{Z}_3$. Sei q ein weiteres derartiges Polynom, dann gelten:

   - $0 \in I$,
   - $-p \in I$,
   - $p + q \in I$,

   wie wir durch kurzes Nachrechnen sofort sehen, z.B. $(p+q)(0) = p(0) + q(0) = 0 + 0 = 0$. Somit ist I eine additive Untergruppe. Sei nun r ein beliebiges Element von $\mathbb{Z}_3[x]$. Wir zeigen die Ideal-Eigenschaft, d.h. dass $rp \in I$ ist: $(r \cdot p)(0) = r(0) \cdot p(0) = r(0) \cdot 0 = 0$.

   Bestimmen Sie ein f, sodass $I = (f)$.

   Lösung:
   Ein Polynom $p \in \mathbb{Z}_3[x]$ ist genau dann im Ideal I, wenn alle Elemente von $\mathbb{Z}_3$ Nullstellen von p sind, also genau dann, wenn p ein Vielfaches von allen $(x - a)$, mit $a \in \mathbb{Z}_3$, ist. Wir wählen also

   $$f = x \cdot (x + 1) \cdot (x + 2).$$

   Ist $\mathbb{Z}_3[x]/I$ ein Körper?

   Lösung:
   Da $x \cdot (x + 1) \cdot (x + 2) \in I$, nicht aber die Faktoren, ist $\mathbb{Z}_3[x]/I$ nicht nullteilerfrei, also insbesondere kein Körper.

3. Sei $p = x^2 + 1$. Ist p über $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Q}$, $\mathbb{R}$ bzw. $\mathbb{C}$ irreduzibel?

   Lösung:
   Weil p Grad 2 hat, ist p genau dann reduzibel wenn es eine Nullstelle hat. Eine solche muss offensichtlich eine Wurzel von -1 sein. Es gelten:

   - $1^2 = 1 = -1$ *in* $\mathbb{Z}_2$;
   - $2^2 = 4 = -1$ *in* $\mathbb{Z}_5$;
   - $i^2 = -1$ *in* $\mathbb{C}$.

   p ist somit über diesen Koeffizientenbereichen reduzibel. Dagegen gelten:

   - $2^2 = 1 \neq -1$ *in* $\mathbb{Z}_3$;
   - $2^2 = 4 = 0 \neq -1$ *und* $3^2 = 1 \neq -1$ *in* $\mathbb{Z}_4$.

Über diesen Bereichen ist p daher ebenso irreduzibel wie bekanntermaßen über $\mathbb{Q}$ und $\mathbb{R}$.

Liegen die Polynome $x+1$, x^2+2, x^3+1, x^4+2, bzw. x^6+1 im Ideal (p)?

Lösung:
Wir testen für jedes dieser Polynome f, ob $f \equiv 0 \pmod{p}$. Dazu bestimmen wir den Rest bei der Division von f durch p bzw. reduzieren mit der Gleichung $p = 0$, also $x^2 = -1$.

- *$x+1$ hat bereits Grad kleiner als p, stimmt also mit dem Rest überein, der somit nicht 0 ist.*
- $x^2 + 2 \equiv -1 + 2 \equiv 1 \pmod{p}$. *Also auch nicht im Ideal.*
- $x^3 + 1 = x^2 x + 1 \equiv -x + 1 \pmod{p}$. *Auch nicht im Ideal.*
- $x^4 + 2 = (x^2)^2 + 2 \equiv (-1)^2 + 2 \equiv 1 + 2 \pmod{p}$. *Dies ist genau dann 0, wenn $3 = 0$, also über $\mathbb{Z}_3$.*
- $x^6 + 1 = (x^2)^3 + 1 \equiv (-1)^3 + 1 \equiv -1 + 1 \equiv 0 \pmod{p}$. *Dieses ist also in allen Fällen im Ideal (p).*

4. Sei p wie zuvor. Bilden Sie den Ring $R := \mathbb{Z}_3[x]/(p)$ und berechnen Sie dessen Multiplikationstafel. Wir verwenden dabei vor allem: $x^2 = 2$ (genauer: $[x] \equiv [2]_3 \pmod{p}$; einfacher: $100 = 2$).

Lösung:

	0	1	2	10	11	12	20	21	22
0	0	0	0	0	0	0	0	0	0
1	0	1	2	10	11	12	20	21	22
2	0	2	1	20	22	21	10	12	11
10	0	10	20	2	12	22	1	11	21
11	0	11	22	12	20	1	21	2	10
12	0	12	21	22	1	10	11	20	2
20	0	20	10	1	21	11	2	22	12
21	0	21	12	11	2	20	22	10	1
22	0	22	11	21	10	2	12	1	20

Warum ist R ein Körper?

Lösung:
Dass es ein Ring ist, gilt schon wegen der Art der Konstruktion, auch die Kommutativität erbt R von $\mathbb{Z}_3[x]$. Auch das Einselement (eigentlich $[1]_{(p)}$, ganz genau sogar $[[1]_3]_{(p)}$, aber hier ebenfalls einfach durch 1 dargestellt). Weil in jeder Zeile (und auch Spalte), außer der mit 0, in der Multiplikationstafel das Einselement vorkommt, sehen wir sofort, dass es sich um einen Körper handelt.

Finden Sie in R ein Element e, sodass $\{e, e^2, e^3, e^4, ...\}$ alle Elemente von R enthält, außer das Nullelement.

Lösung:
x (bzw. 10) kommt nicht in Frage, weil $x^2 = -1$, und somit $x^4 = 1$ ist. Nächster Versuch: $e := x + 1$ (bzw. 11). Wegen $11^4 = 20^2 = 2$ gelingt dieser bessen. Alle Potenzen von 11, beginnend mit Exponent 0, sind:

$$1, 11, 20, 21, 2, 22, 10, 12; 1, 11, \ldots.$$

Suchen Sie ein Polymom m möglichst niedrigen Grades in $\mathbb{Z}_3[x]$ (aber nicht das Nullpolynom), sodass $m(e) = 0$.

Lösung:
$11^2 = 20 = 20 + 22 + 11 = 20 + 2 \cdot 11 + 11$, *also* $e^2 - 2e - 1 = 0$ *bzw.* $e^2 + e + 2 = 0$. *Dieses Polynom ist in unserer Tabelle irreduzibler Polynome gelistet, wo auch dessen Exponent* 8 *verzeichnet ist. Das Polynom* p *dagegen ist zwar irreduzibel (sonst würden wir keinen Körper bekommen) aber dessen Exponent ist nur* 4*; deshalb sind dessen Nullstellen keine primitiven Elemente.*

5. Sei p wie zuvor. Finden Sie einen Körper, über den p vollständig in Linearfaktoren zerfällt und bestimmen Sie diese.

Lösung:
Unser Ring R *von zuvor, der tatsächlich ein Körper ist, ist bereits dazu geeignet, denn* $10 \cdot 10 = 2 = -1$ *in* R*; dasselbe für* 20*. Genauer, ohne Kurznotation: Die Nullstellen von* $z^2 + 1$ *in* R *sind* $[x]_{(p)}$ *und* $[2x]_{(p)}$*. Oder andersrum: In* R *gilt*

$$z^2 + 1 = (z + [x]_{(p)})(z + [2x]_{(p)}).$$