3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in $\mathbb{Z}$; ($\mathbb{Z} = \langle \mathbb{Z}, +, \cdot \rangle$ ist ein kommutativer Ring).

Definition 153

Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n.

Bemerkungen

1. Für $\ell, m \in \mathbb{Z}$ gilt:

$$m \in [\ell]_n \iff m \bmod n = \ell \bmod n\,.$$

   Gilt $m \in [\ell]_n$, so schreibt man auch $m \equiv \ell \bmod n$ oder $m = \ell \bmod n$ und spricht „m kongruent ℓ modulo n“.
2. Es gilt $[\ell]_n = \{\ell + kn : k \in \mathbb{Z}\} =: \ell + n\mathbb{Z} =: \ell + (n)$.
3. Da es genau n verschiedene Reste $0, 1, \ldots, n-1$ gibt, gibt es auch genau n verschiedene Restklassen $[0]_n, [1]_n, \ldots, [n-1]_n$.

Bemerkungen

4. Kongruenz modulo n definiert auf $\mathbb{Z}$ eine Äquivalenzrelation $\sim_n$: $m \sim_n \ell :\Longleftrightarrow\ n$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ.
5. Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren

$$[\ell]_n +_n [m]_n := [\ell + m]_n, \qquad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$

   und erhält einen kommutativen Ring; er heißt der Restklassenring $\mathbb{Z}$ modulo n und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}_n$ bezeichnet.
6. Die Abbildung $\langle \mathbb{Z}, +, \cdot \rangle \to \langle \mathbb{Z}_n, +_n, \cdot_n \rangle$, $\ell \mapsto$ „Rest der Division von ℓ durch n“ ist ein Ringhomomorphismus.

Restklassen können auch im Polynomring $K[x]$ (K ein Körper) gebildet werden.

Definition 154

Sei $g \in K[x]$ ein Polynom, $\mathrm{grad}(g) \geq 1$. Für jedes $f \in K[x]$ heißt die Menge

$$[f]_g := \{h \in K[x] : h - f \text{ ist durch } g \text{ teilbar}\}$$

die Restklasse von f modulo g.

Bemerkung: Wie in $\mathbb{Z}$ gilt nun auch im Polynomring $K[x]$:

1. $h \in [f]_g \iff h$ und f haben bei Polynomdivision durch g denselben Rest.
2. $[f]_g = \{f + hg \ : \ h \in K[x]\} =: f + (g)$ mit $(g) := \{hg : h \in K[x]\} =$ Menge aller Polynome, die durch g teilbar sind.

3. „Kongruenz modulo g“ definiert auf $K[x]$ eine Äquivalenzrelation $\sim_g$: $h \sim_g f \iff h - f$ ist durch g teilbar, und $[f]_g$ ist die Äquivalenzklasse von f.
4. Auf der Menge aller Restklassen $[f]_g$ kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \qquad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring $K[x]$ modulo g und wird mit $K[x]/(g)$ bezeichnet.

3.6.2 Eigenschaften von Restklassenringen

Teilt man Polynome durch ein fest gewähltes Polynom g, $\mathrm{grad}(g) \geq 1$, so treten als Reste sämtliche Polynome vom Grad $< d = \mathrm{grad}(g)$ auf. Deshalb setzen wir

$$K[x]_d := \{h \in K[x] : \mathrm{grad}(h) < d\},$$

und definieren auf $K[x]_d$ Addition $+_g$ und Multiplikation $\cdot_g$ wie folgt:

Mit $Rem(f)$ bezeichnen wir den Rest der Polynomdivision von f durch g.

$$f +_g h := f + h, \qquad f \cdot_g h := Rem(f \cdot h).$$

Man prüft leicht nach, dass $(K[x]_d, +_g, \cdot_g)$ ein kommutativer Ring ist.

Satz 155

Sei $g \in K[x]$ ein Polynom, $d = \mathrm{grad}(g) \geq 1$. Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \to (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto Rem(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch $r \mapsto [r]_g$.

Beweis:

Es gilt

1. $$[f]_g = [0]_g \iff g|f \iff Rem(f) = 0$$

2. $$[f]_g + [h]_g = [f+h]_g \mapsto Rem(f+h) = Rem(f) + Rem(h) = Rem(f) +_g Rem(h)$$

3. $$[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto Rem(f \cdot h) = Rem(Rem(f) \cdot Rem(h)) = Rem(f) \cdot_g Rem(h).$$

Aus (1) - (3) folgt, dass obige Abbildung wohldefiniert, injektiv und ein Ringhomomorphismus ist; sie ist auch surjektiv, denn für $f \in K[x]_d$ ist $Rem(f) = f$. □

Satz 156

Sei K ein Körper mit n Elementen, und sei $g \in K[x]$, $d = \mathrm{grad}(g) \geq 1$. Dann besitzt $K[x]/(g)$ genau n^d Elemente.

Beweis:

Nach Satz 155 ist $|K[x]/(g)| = |K[x]_d|$, und offensichtlich gilt $|K[x]_d| = n^d$. □

Definition 157

Ein Polynom $g \in K[x]$ heißt irreduzibel, falls $\mathrm{grad}(g) \geq 1$ gilt und aus $g = g_1 \cdot g_2$ mit $g_1, g_2 \in K[x]$ stets $\mathrm{grad}(g_1) = 0$ oder $\mathrm{grad}(g_2) = 0$ folgt; ansonsten heißt g reduzibel.

Satz 158

Sei $g \in K[x]$, $\mathrm{grad}(g) \geq 1$. Dann gilt:

$$K[x]/(g) \text{ ist ein Körper } \Leftrightarrow g \text{ ist irreduzibel.}$$

Beweis:

"$\Rightarrow$" Sei $K[x]/(g)$ ein Körper. Angenommen, g ist nicht irreduzibel. Dann gibt es $g_1, g_2 \in K[x]$ mit $g = g_1 \cdot g_2$ und $\mathrm{grad}(g_1), \mathrm{grad}(g_2) \geq 1$.
Da $d := \mathrm{grad}(g) = \mathrm{grad}(g_1) + \mathrm{grad}(g_2)$, folgt $\mathrm{grad}(g_1) < d$ und $\mathrm{grad}(g_2) < d$. Also gilt $[g_1]_g \neq [0]_g$ und $[g_2]_g \neq [0]_g$.
Jedoch ist

$$[g_1]_g \cdot [g_2]_g = [g_1 g_2]_g = [g]_g = [0]_g \ ,$$

d.h. $[g_1]_g$ und $[g_2]_g$ sind Nullteiler. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 123).

Beweis (Forts.):

"$\Leftarrow$" Sei g irreduzibel, und sei $[f]_g \neq [0]_g$ gegeben.
$[f]_g \neq [0]_g$ bedeutet, dass f nicht durch g teilbar ist. Da g irreduzibel ist, sind f und g daher teilerfremd.
Somit existieren Polynome $p, q \in K[x]$ mit $pf + qg = 1$, und es folgt

$$\begin{aligned} [p]_g \cdot [f]_g &= [pf]_g = [1 - qg]_g = [1]_g - \underbrace{[qg]_g}_{=[0]_g} \\ &= [1]_g \ . \end{aligned}$$

Also ist $[p]_g = ([f]_g)^{-1}$.

□

3.7 Konstruktion endlicher Körper

Satz 159

*Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet ($GF =$ **G**alois **F**ield, nach Evariste Galois (1811–1832)).*

Beweis:

$n = 1$: $\mathbb{Z}_p = GF(p)$ ist ein Körper mit p Elementen.

$n > 1$: Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein *irreduzibles* Polynom vom Grad n (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).
Nach Satz 158 ist $K[x]/(g)$ ein Körper, und nach Satz 156 hat $K[x]/(g)$ genau p^n Elemente.

□

Satz 160

Je zwei endliche Körper mit p^n Elementen sind isomorph.

Beweis:

siehe geeignetes Textbuch zur Algebra oder Zahlentheorie,
ebenfalls bzgl. der Existenz irreduzibler Polynome! □

Beispiel 161

Wir betrachten den Fall $K = \mathbb{Z}_3 = GF(3)$ und $p(x) = x^2 + 1$.

Der Ring $\mathbb{Z}_3[x]/(p)$ besteht also aus allen Polynomen in $\mathbb{Z}_3[x]$ vom Grad ≤ 1:

$$\mathbb{Z}_3[x]/(p) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\} .$$

Bemerkung zur Notation: Wir schreiben hier (und auch sonst) das Polynom f statt der Restklasse $[f]_g$.

Das Polynom p ist irreduzibel. Wieso?

Beispiel 162

Für $K = \mathbb{Z}_2 = GF(2)$ und $p(x) = x^2 + x + 1$ gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x+1\} .$$

Für die Addition und Multiplikation modulo p ergibt sich

$+_p$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Aus diesen beiden Tabellen folgt, dass $\mathbb{Z}_2[x]/(p)$ mit den angegebenen Verknüpfungen $+_p$ und $\cdot_p$ einen Körper mit 4 Elementen bildet (den wir schon früher gesehen haben).

Beispiel 163

Für $K = \mathbb{Z}_2$ und $q(x) = x^2 + 1$ gilt wiederum

$$\mathbb{Z}_2[x]/(q) = \{0, 1, x, x+1\} .$$

Für die Addition und Multiplikation modulo q ergibt sich nunmehr jedoch

$+_q$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot_q$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Aus der zweiten Tabelle folgt, dass $\mathbb{Z}_2[x]/(q) \setminus \{0\}$ bzgl. $\cdot_q$ keine Gruppe bildet. Der Grund ist, dass q nicht irreduzibel ist.