WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

11-28-2003

Restklassen in Polynomringen

Einführung und Definition

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

Definition

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:

   $m \in [\ell]_m \iff m$ und ℓ haben bei Division durch n denselben Rest

   Gilt $m \in [\ell]_n$, so schreibt man auch $m \equiv \ell \bmod n$ 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. a es genau n verschiedene Reste $0, 1, \ldots, n-1$ gibt, gibt es auch genau n verschiedene Restklassen $[0]_n, [1]_n, \ldots, [n-1]_n$.

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 Äquivalenzklasse von ℓ.
5. Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren

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

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

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

Definition

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.*

Bem.: 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.

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

Definition

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.*

Bem.: 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.

4. "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 Äquivalenzklasse von f.
5. 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.

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 $R(f)$ bezeichnen wir den Rest der Polynomdivision von f durch g (g sei im folgenden fest gewählt).

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

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

Satz

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

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

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

Beweis.

Es gilt

1. $[f]_g = 0 \iff g|f \iff R(f) = 0$
2. $[f]_g + [h]_g = [f+h]_g \mapsto R(f+h) = R(f) + R(h) = R(f) +_g R(h)$
3. $[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto R(f \cdot h) = R(R(f) \cdot R(h)) = R(f) \cdot_g R(h)$.

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 $R(f) = f$. □

Beweis.

Es gilt

1. $[f]_g = 0 \iff g|f \iff R(f) = 0$
2. $[f]_g + [h]_g = [f+h]_g \mapsto R(f+h) = R(f) + R(h) = R(f) +_g R(h)$
3. $[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto R(f \cdot h) = R(R(f) \cdot R(h)) = R(f) \cdot_g R(h)$.

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 $R(f) = f$. □

Satz

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

Definition

Ein Polynom $g \in K[x]$ heißt *irreduzibel*, wenn $\mathrm{grad}(g) \geq 1$ 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

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

Definition

Ein Polynom $g \in K[x]$ heißt *irreduzibel*, wenn $\mathrm{grad}(g) \geq 1$ 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*.