§ 9 RINGE

9.1 Motivation

- Häufig gibt es auf einer Menge zwei Verknüpfungen: eine „Addition" und eine „Multiplikation".
- Bsp.: $(\mathbb{Z}, +, \cdot)$
  Hier gibt es sogar noch eine Division mit Rest.
- Läßt sich dieses Konzept algebraisch abstrahieren?

9.2. Def.: Eine Menge R mit zwei Verknüpfungen $+, \cdot$ auf R heißt Ring, wenn gilt:

a) $(R, +)$ ist eine kommutative Gruppe.

b) $(R, \cdot)$ ist eine Halbgruppe

c) Distributivgesetze:

$$\left.\begin{aligned} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a \end{aligned}\right\} \quad \forall a,b,c \in R$$

Ist $(R, \cdot)$ sogar ein Monoid, so heißt $(R, +, \cdot)$ Ring mit Einselement. Gilt neben (a) – (c) noch

d) Kommutativgesetz der Multiplikation

$$a\cdot b = b\cdot a \qquad \forall a,b \in R$$

so heißt $(R, +, \cdot)$ kommutativer Ring.

9.3. Konventionen

In einem Ring $(R,+,\cdot)$ nennt man häufig

- das neutrale Element der Addition Nullelement (0)
- " " " " Multiplikation Einselement (1)
-
- das additive Inverse zu a: $-a$
- " multiplikative " " ": $\frac{1}{a}$

Um Klammern zu sparen, vereinbart man „Punkt vor Strich".

9.4. Beispiele

a) $(\mathbb{Z},+,\cdot)$ ist ein Ring, sogar ein kommutativer Ring mit Eins. Das Gleiche gilt für $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$.

b) Die Menge $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m bildet zusammen mit der modularen Addition und Multiplikation den Restklassenring $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$. Auch er ist kommutativ. Er besitzt das Einselement $[1]$. (vgl. §7).

Nachweis des ersten Distributivgesetzes:

$$
\begin{aligned}
[a]\cdot([b]+[c]) &= [a]\cdot[b+c] \\
&= [a(b+c)] \\
&= [ab+bc] \\
&= [ab]+[bc] \\
&= [a][b]+[b][c]
\end{aligned}
$$

Zweites Distributivgesetz folgt aus Kommutativität.

Beispiel für nichtkommutative Ringe folgt später (Matrizen)

9.5. <u>Satz (Unterringkriterium)</u>

Sei $(R,+,\cdot)$ ein Ring und $S \subset R$. Dann ist $(S,+,\cdot)$ genau dann ein Ring, falls

a) $(S,+)$ eine Untergruppe von $(R,+)$ ist (vgl. 8.5).

b) $(S,\cdot)$ ist abgeschlossen: $a,b \in S \Rightarrow a\cdot b \in S$.

Beweis wie Satz 8.5.

9.6. <u>Beispiel</u>

$(m\mathbb{Z},+,\cdot)$ ist Unterring von $(\mathbb{Z},+,\cdot)$, denn

a) $(m\mathbb{Z},+)$ ist Untergruppe von $(\mathbb{Z},+)$, und $(m\mathbb{Z},\cdot)$

b) $(m\mathbb{Z},\cdot)$ ist abgeschlossen:

Seien $a,b \in m\mathbb{Z}$: $\Rightarrow \exists q_1,q_2 \in \mathbb{Z}$:
$a = q_1 m, \quad b = q_2 m$

$$\Rightarrow ab = (q_1 m)(q_2 m) = (\underbrace{q_1 q_2 m}_{\in \mathbb{Z}})\, m \in m\mathbb{Z}.$$

9.7. <u>Polynomringe</u>

Sie sind die wichtigsten Ringe. Sei $(R,+,\cdot)$ ein Ring (z.B. $R=\mathbb{R}$) und $a_0, a_1, \ldots, a_n \in R$. Dann nennen wir die Abb.

$$p: R \to R, \quad x \mapsto \sum_{k=0}^{n} a_k x^k$$

<u>Polynom</u> (über R). Dabei ist $x^k := x\cdot x \cdot \ldots \cdot x$ (k Mal) Ist $a_n \neq 0$, so heißt n der <u>Grad</u> von p: $n = \deg(p)$.

(Bsp.: $p(x) = 5x^3 - 1.3x + 6$ ist ein Polynom vom Grad 3 über $\mathbb{R}$)

Die Menge aller Polynome über R nennen wir $R[x]$.

$a_0, \ldots, a_n$ heißen <u>Koeffizienten</u> von p.

Auf $R[x]$ definieren wir eine Addition und eine Multiplikation „punktweise" durch

$$(p+q)(x) := p(x) + q(x)$$
$$(p\cdot q)(x) := p(x)\cdot q(x) \qquad \forall p, q \in R[X].$$

Dann ist $(R[x], +, \cdot)$ ein Ring, der Polynomring über R:

Der Nachweis der Ringeigenschaften ist arbeitsaufwändig.
Man verwendet: Mit $p(x) = \sum_{k=0}^{n} a_k x^k$, $q(x) = \sum_{k=0}^{n} b_k x^k$

gilt:

$$(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k)\, x^k$$

$$(p\cdot q)(x) = \sum_{k=0}^{n+n} \Big(\sum_{\substack{i+j=k \\ 0\le i,j\le n}} a_i b_j \Big)\, x^k$$

Dabei wurde $n := \max(\deg(p), \deg(q))$ gewählt (und entspr. Koeffizienten des Polynoms kleineren Grades Null gesetzt).

9.8. Das Horner-Schema

Oft müssen Funktionswerte von Polynomen effizient berechnet werden. Z.B. approximiert der Taschenrechner die Sinusfunktion durch ein Polynom.
Eine naive Auswertung eines Polynoms

$$p(x) = 5x^7 + 4x^6 - 3x^5 + 4x^4 + 6x^3 - 7x^2 + 4x - 1$$

erfordert 7 Additionen und $7+6+5+4+3+2+1 = 28$ Multiplikationen

Wesentlich effizienter ist das Horner-Schema, das eine geschickte Klammerung ausnutzt:

$$p(x) = ((((((5\cdot x + 4)\cdot x - 3)\, x + 4)\, x + 6)\, x - 7)\, x + 4)\, x - 1$$

Arbeitet man die Klammern von innen nach außen ab, benötigt man nur 7 Additionen und 7 Multiplikationen.

Allgemein benötigt man bei der naiven Auswertung eines Polynoms n-ten Grades n Additionen und $\sum_{k=1}^{n} k = \frac{1}{2} n(n+1)$ Multiplikationen. Das Horner-Schema reduziert den Multiplikationsaufwand auf n Operationen.

9.9 Polynomdivision

Im Ring $(\mathbb{Z}, +, \cdot)$ haben wir in §6 Division mit Rest betrachtet. Kann man Ähnliches auch im Polynomring $(\mathbb{R}[x], +, \cdot)$ tun? (Beachte: $R = \mathbb{R}$ hier)

Man kann zeigen:

Satz (Polynomdivision):

In $(\mathbb{R}[x], +, \cdot)$ kann man eine Division mit Rest durchführen:

Zu $a, b \in \mathbb{R}[x]$ mit $b \neq 0$ ex. eind. best. $q, r \in \mathbb{R}[x]$ mit

$$a = qb + r$$

und $\deg(r) < \deg(b)$.

9.10 Praktische Durchführung der Polynomdivision

Analog zur Division natürlicher Zahlen

$$\begin{array}{l} 365 : 7 = 52 \text{ Rest } 1 \\ -35 \\ \quad 15 \\ \; -14 \\ \quad\;\; 1 \end{array}$$

7 geht 5 Mal in 36

führt man die Polynomdivision durch:

$$\begin{array}{l} (x^4 + 2x^3 + 3x^2 + 4x + 5) : (x^2+1) = x^2 + 2x + 2 \text{ Rest } 2x+3 \\ -(x^4 \qquad\quad + x^2) \\ \qquad\quad 2x^3 + 2x^2 + 4x \\ \qquad -(2x^3 \qquad + 2x) \\ \qquad\qquad\quad 2x^2 + 2x + 5 \\ \qquad\qquad -(2x^2 \qquad + 2) \\ \qquad\qquad\qquad\quad 2x + 3 \end{array}$$

x^2+1 geht x^2 Mal in $x^4+2x^3+3x^2$

Satz 9.9 hat zwei wichtige Folgerungen

9.11. Satz (Abspaltung von Nullstellen)

Hat $p \in \mathbb{R}[x]$ die Nullstelle x_0 (d.h. $p(x_0) = 0$), so ist p durch das Polynom $x - x_0$ ohne Rest teilbar.

Beweis: Nach Satz 9.9 ex. für $p(x)$ und $b(x) = x - x_0$ eine Division mit Rest:

$$\exists\, q(x), r(x) \text{ mit } p(x) = q(x)\, b(x) + r(x)$$

In x_0 gilt dann $\quad 0 = p(x_0) = q(x_0) \underbrace{b(x_0)}_{0} + r(x_0) \qquad (*)$

Wegen $\deg(r) < \deg(b) = 1$ folgt $\deg(r) = 0$, d.h. $r(x) = a_0$.

Wegen $(*)$ ist $r(x) = a_0 = 0$.

$\square$

9.12. Satz (Zahl der Nullstellen)

Ein von 0 verschiedenes Polynom $p \in \mathbb{R}[x]$ vom Grad n hat höchstens n Nullstellen.

Beweis:

Ann.: $p(x)$ hat mehr als n Nullstellen.

Sukzessives Abspalten der n Nullstellen $x_1, \ldots, x_n$ ergibt

$$\exists\, q \in \mathbb{R}[x]: \quad p(x) = (x-x_1)\cdot(x-x_2)\cdot\ldots\cdot(x-x_n)q(x)$$

$q(x)$ hat Grad 0, sonst wäre $\deg(p) > n$.

d.h. $q(x) = a_0$

Sei nun x_{n+1} eine weitere Nullstelle, d.h.

$$0 = p(x_{n+1}) = (x_{n+1}-x_n)\cdot\ldots\cdot(x_{n+1}-x_1)\cdot a_0$$

Also ist einer der Faktoren $(x_{n+1}-x_n), \ldots, (x_{n+1}-x_1), a_0$ Null.

$a_0 = 0$ geht nicht, da $p(x) \neq 0$.

$\Rightarrow$ x_{n+1} stimmt mit einem der $x_1, \ldots, x_n$ überein $\square$

Im Ring $(\mathbb{Z}, +, \cdot)$ haben wir Teilbarkeit und ggT studiert (vgl. §6). Geht das auch im Polynomring $(\mathbb{R}[x], +, \cdot)$?

9.13. Def.: Seien $a, b \in \mathbb{R}[x]$. Dann ist a durch b teilbar, wenn es ein $q \in \mathbb{R}[x]$ gibt mit $a(x) = q(x)\, b(x)$.
Ein Polynom $p \in \mathbb{R}[x]$ ist gemeinsamer Teiler von a und b, falls p sowohl a als auch b teilt.
p heißt größter gemeinsamer Teiler von a und b, falls p durch jeden gemeinsamen Teiler von a und b teilbar ist.

9.14 Euklidischer Algorithmus für Polynome

Analog zu 6.11 bestimmt man den ggT zweier Polynome $a, b \in \mathbb{R}[x]$ mit $\deg(a) \geq \deg(b)$ mit dem Euklidischen Algorithmus.

Beispiel: $a(x) = x^4 + x^3 - x^2 + x + 2$

$b(x) = x^3 + 2x^2 + 2x + 1$

Polynomdivision ergibt

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

$$(x^3 + 2x^2 + 2x + 1) = (-x-4)(-x^2 + 2x + 3) + (13x + 13)$$

$$(-x^2 + 2x + 3) = \left(-\frac{1}{13}x + \frac{3}{13}\right)(13x + 13)$$

Also ist $\text{ggT}(a(x), b(x)) = 13x + 13$

(ebenso wie jedes andere Polynom $c(13x+13)$ mit einer Konstanten $c \neq 0$).

Gibt es „Primfaktoren" in Polynomringen?

9.15. Def.: Sei $(R, +, \cdot)$ ein kommutativer Ring mit 1.
Ein Polynom $p \in R[x]$ heißt reduzibel über R, wenn es nichtkonstante Polynome $a, b \in R[x]$ gibt mit $p = a \cdot b$. Andernfalls heißt p irreduzibel über R.

9.16. Beispiele

a) $x^2 - 4$ ist reduzibel über $\mathbb{Z}$:

$x^2 - 4 = (x+2)(x-2)$

b) $x^2 - 3$ ist irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$, aber reduzibel über $\mathbb{R}$:

$x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3})$

c) $x^2 + 1$ ist irreduzibel über $\mathbb{R}$.

9.17. Irreduzible Polynome als „Primfaktoren" in $(\mathbb{R}[x], +, \cdot)$

Irreduzible Polynome in $(\mathbb{R}[x], +, \cdot)$ haben ähnliche Eigenschaften wie Primfaktoren in $(\mathbb{Z}, +, \cdot)$. So existiert z.B. eine „Primfaktorzerlegung":

Jedes nichtkonstante Polynom $p \in \mathbb{R}[x]$ läßt sich als Produkt irreduzibler Polynome aus $\mathbb{R}[x]$ darstellen. Die Darstellung ist bis auf die Reihenfolge der irreduziblen Polynome und bis auf Multiplikation mit konstanten Polynomen eindeutig. (vgl. Satz 6.6)

9.18. Beispiel

$p(x) = x^3 - x^2 + x - 1$ hat in $\mathbb{R}[x]$ die folgende Zerlegung in irreduzible Polynome:

$p(x) = (x^2 + 1)(x - 1)$

Äquivalent hierzu sind z.B.

$p(x) = (x - 1)(x^2 + 1) = (4x - 4)\left(\frac{1}{4}x^2 + \frac{1}{4}\right)$

Generell kann man zeigen, dass es über $\mathbb{R}$ nur 2 Typen von irreduziblen Polynomen gibt:

a) lineare Polynome

b) quadratische Polynome $ax^2 + bx + c$ mit $b^2 - 4ac < 0$.