Mathematik I für Studierende der Informatik und Wirtschaftsinformatik (Diskrete Mathematik) im Wintersemester 2017/2018

18. Januar 2018

Ringe und Körper

Definition 7.50

Eine Menge R zusammen mit zwei binären Operationen $+$ und $\cdot$ und zwei verschiedenen Konstanten 0 und 1 heißt ein *Ring* (mit 1), falls für alle $a, b, c \in R$ die folgenden Axiome (R1)–(R5) gelten:

(R1) Assoziativgesetze
- $a + (b + c) = (a + b) + c$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(R2) Kommutativgesetz der Addition:
- $a + b = b + a$

(R3) Distributivgesetze
- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

(R4) Existenz neutraler Elemente bezüglich der Addition und der Multiplikation
- $a + 0 = a$
- $1 \cdot a = a$

(R5) Existenz inverser Elemente bezüglich der Addition
- Es gibt ein Element $-a$ mit $a + (-a) = 0$.

Man beachte, dass der offizielle Name für hier definierten Strukturen “Ring mit 1” lautet.
Wir werden aber keine Ringe ohne 1 betrachten und sagen daher abkürzend einfach “Ring”, obwohl wir eigentlich “Ring mit 1” meinen.

Unter Verwendung der Begriffe Gruppe und Monoid können wir Ringe auch in der folgenden kompakten Form definieren.

Definition 7.51

Eine Menge R mit zwei binären Operationen $+$ und $\cdot$ ist ein *Ring* (mit 1) falls gilt:

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

(RII) $(R, \cdot)$ ist ein Monoid.

(RIII) Es gelten die Distributivgesetze, d.h., für alle $a, b, c \in R$ gilt:

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

Bei dieser Definition definieren wir 0 als das neutrale Element der Addition und 1 als das neutrale Element der Multiplikation.

Wie üblich schreiben wir $-a$ für das additive Inverse eines Ringelements a und a^{-1} für das multiplikative Inverse, falls es denn existiert.

Beispiel 7.52

a) Jeder Körper ist ein Ring.
Umgekehrt ist ein Ring $(R, +, \cdot)$ ein Körper, wenn das Kommutativgesetz für $\cdot$ gilt und jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.
b) Die ganzen Zahlen mit Addition, Multiplikation und den üblichen Konstanten 0 und 1 bilden einen Ring, aber bekanntlich keinen Körper.
c) Für jedes $m \geq 2$ ist $(\mathbb{Z}_m, +, \cdot)$ ein Ring.

Definition 7.53

Sei $(R, +, \cdot)$ ein Ring.
Die *Einheitengruppe* $E(R)$ von R ist die Menge derjenigen Elemente von R, die ein multiplikatives Inverses besitzen, zusammen mit der Multiplikation.

Wir hatten schon gesehen, dass die Einheitengruppe eines Ringes der Form $\mathbb{Z}_m$, $m \geq 2$, tatsächlich eine Gruppe ist.
Das gleiche Argument liefert die entsprechende Aussage für beliebige Ringe:

Satz 7.54

Für jeden Ring R ist $(E(R), \cdot)$ eine Gruppe.

Beispiel 7.55

a) Für jeden Körper K ist $E(K) = K \setminus \{0\}$.
Insbesondere ist $E(\mathbb{R}) = \mathbb{R} \setminus \{0\}$, $E(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$ und $E(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{[0]_p\}$ für jede Primzahl p.

b) Es gilt $E(\mathbb{Z}) = \{-1, 1\}$.

c) Es gilt $E(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ und
$E(\mathbb{Z}_{12}) = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

Polynome

Polynomfunktionen

Definition 8.1

Ist K ein Körper, so bezeichnen wir einen Ausdruck der Form $a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n$, wobei die Koeffizienten $a_0, \ldots, a_n$ aus K stammen und X eine Unbekannte ist, als *Polynom* (in der Unbestimmten X) über K.
Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
Polynome der Form a_0X^0 nennen wir *konstant*.
Die Elemente von K identifizieren wir mit den konstanten Polynomen und fassen so K als Teilmenge von $K[X]$ auf.

Bemerkung 8.2

In unserer Definition von Polynomen haben wir die verschiedenen Potenzen von X in aufsteigender Reihenfolge angegeben.
Oft werden die Potenzen jedoch in absteigender Reihenfolge angegeben.
Statt

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n$$

schreibt man also

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0X^0.$$

Die Potenz X^0 hat für alle möglichen Werte von X den Wert 1.
Deshalb lässt man den Term X^0 normalerweise weg.
Anstelle von X^1 schreibt man einfach X.
Mit diesen Konventionen lautet das Polynom also

$$a_n X^n + \cdots + a_1 X + a_0.$$

Ist für ein i der Koeffizient a_i gleich 0, so lässt man den Term $a_i X^i$ weg.
Bei negativen Koeffizienten zieht man das Minuszeichen mit dem vorhergehenden Pluszeichen zu einem Minuszeichen zusammen.
Koeffizienten, die den Wert 1 haben lässt man weg, falls es sich nicht um den Koeffizienten vor X^0 handelt.
Anstelle von

$$1X^0 + (-5)X^1 + 0X^2 + 1X^3$$

schreibt man also

$$X^3 - 5X + 1.$$

Beispiel 8.3

a) Aus der Schule sind Polynome mit reellen oder rationalen Koeffizienten bekannt, also Polynome über $\mathbb{R}$ oder $\mathbb{Q}$, wie das oben genannte Beispiel $X^3 - 5X + 1$.
Streng genommen sind die Koeffizienten dieses Polynoms sogar ganzzahlig, so dass man von einem Polynom über $\mathbb{Z}$ sprechen kann.
Wir werden jedoch nur Polynome über Körpern betrachten.

b) Wir kennen auch schon weitere Körper außer $\mathbb{R}$ und $\mathbb{Q}$, nämlich die endlichen Körper $\mathbb{Z}_p$ für Primzahlen p.
So können wir zum Beispiel $X^2 - X + 1$ als ein Polynom über $\mathbb{Z}_2$ auffassen, wenn wir 1 für das neutrale Element der Multiplikation in $\mathbb{Z}_2$ schreiben.
Wir könnten dieses Polynom auch $X^2 - X + [1]_2$ oder $[1]_2X^2 + [-1]_2X^1 + [1]_2$ schreiben.
Man beachte, dass für alle $a \in \mathbb{Z}_2$ die Gleichung $a = -a$ gilt.
Damit ist dieses Polynom identisch mit $X^2 + X + 1$.
Man sieht, dass es in diesem Falle (und vor allem bei der von uns gewählten Notation) wichtig ist, festzulegen, über welchem Körper man das Polynom betrachtet.

c) Wenn man Polynome über $\mathbb{Z}_p$ betrachtet, wird es schnell lästig, die Koeffizienten in der Form $[n]_p$ zu schreiben.
Deshalb schreiben wir in diesem Zusammenhang anstelle der Restklassen einfach die Standardrepräsentanten der Restklassen.
Für das Polynom $X^3 + [2]_3X^2 + [-2]_3X + [1]_3$ über $\mathbb{Z}_3$ schreiben wir also einfach $X^3 + 2X^2 + X + 1$.
Die Schreibweise $X^3 + 2X^2 - 2X + 1$ ist aber auch akzeptabel.

d) Spezielle Polynome sind die sogenannten *Monome* X^n, $n \in \mathbb{N}_0$.

Wir haben schon intuitiv zwei Polynome gleich genannt, wenn sie dieselben Koeffizienten haben.
An dieser Stelle müssen wir jedoch vorsichtig sein.
Was ist zu Beispiel mit den Polynomen $0X^2 + X - 1$ und $X - 1$?

Definition 8.4

Sei $p = a_0X^0 + \cdots + a_nX^n$ ein Polynom über einem Körper K.
Der *Grad* $\operatorname{grad}(p)$ von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$, falls solch ein i existiert.
Existiert kein i mit $a_i \neq 0$, so nennt man p das Nullpolynom und setzt $\operatorname{grad}(p) := -\infty$.
Polynome vom Grad ≤ 0 nennen wir *konstant*.

Ist $\operatorname{grad}(p) \geq 0$, so nennt man den Koeffizienten $a_{\operatorname{grad}(p)}$ den *Leitkoeffizienten* von p.
Das Polynom p heißt normiert, falls der Leitkoeffizient 1 ist.

Wir nennen zwei Polynome $p = a_0X^0 + \cdots + a_nX^n$ und $q = b_0X^0 + \cdots + b_mX^m$ über demselben Körper K gleich, wenn sie denselben Grad k haben und für alle $i \in \{0, \ldots, k\}$ die Koeffizienten a_i und b_i gleich sind.

Insbesondere sind also die Polynome $0X^2 + X - 1$ und $X - 1$ gleich. Beide Polynome haben den Grad 1 und die Koeffizienten vor X^1 und X^0 sind jeweils dieselben.
Man beachte, dass es in diesem Beispiel egal ist, über welchem Körper man die Polynome betrachtet, solange es für beide Polynome derselbe Körper ist.

Als Nächstes definieren wir Summen und Produkte von Polynomen.

Definition 8.5

Seien $p = a_0X^0 + \cdots + a_nX^n$ und $q = b_0X^0 + \cdots + b_mX^m$ Polynome über demselben Körper K.
Sei $k = \max(m, n)$. Für alle $i \in \mathbb{Z}$ mit $n < i \leq k$ setzen wir $a_i := 0$.
Für alle $j \in \mathbb{Z}$ mit $m < j \leq k$ setzen wir $b_j := 0$.
Dann gilt $p = a_0X^0 + \cdots + a_kX^k$ und $q = b_0X^0 + \cdots + b_kX^k$.
Nun sei

$$p + q := (a_0 + b_0) + \cdots + (a_k + b_k)X^k.$$

Wir definieren die Summe zweier Polynome also "koeffizientenweise".

Das Produkt von p und q definieren wir durch Ausmultiplizieren.
Das Produkt $p \cdot q$ sei das Polynom $c_0 + \cdots + c_{n+m} X^{n+m}$ mit

$$c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0.$$

Beispiel 8.6

Addition und Multiplikation von Polynomen über $\mathbb{Q}$ und $\mathbb{R}$ setzen wir als bekannt voraus.

a) Wir betrachten Polynome über $\mathbb{Z}_5$.
Sei $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4$.
Dann ist

$$p + q = X^3 + (3+2)X^2 - X + (2+4) = X^3 + 4X + 1$$

und

$$\begin{aligned} p \cdot q &= (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) \\ &= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 2 \cdot 4 \\ &= 2X^5 + X^3 + X^2 + 3X + 3. \end{aligned}$$

Insbesondere ist

$$\operatorname{grad}(p \cdot q) = \operatorname{grad}(p) + \operatorname{grad}(q).$$

Wie man leicht nachrechnet, gilt diese Gleichung für je zwei Polynome über demselben Körper.

b) Wir betrachten wieder Polynome über $\mathbb{Z}_5$.
Sei $p = X^3 + 3X^2 + 2$ wie oben und $q = -X^3 + X^2 - 3$.
Dann gilt

$$p + q = (1-1)X^3 + (3+1)X^2 + (2-3) = 4X^2 - 1 = 4X^2 + 4.$$

Insbesondere ist

$$\text{grad}(p+q) < \text{grad}(p), \text{grad}(q).$$

Das ist aber ein Spezialfall.
Sind p und q Polynome von verschiedenem Grad, so ist

$$\text{grad}(p+q) = \max(\text{grad}(p), \text{grad}(q)).$$

Sind p und q Polynome vom selben Grad und ist der Leitkoeffizient von p nicht genau das additive Inverse des Leitkoeffizienten von q, so ist

$$\text{grad}(p+q) = \text{grad}(p) = \text{grad}(q).$$

Satz 8.7

Die Menge $K[X]$ zusammen mit den eben definierten Operationen $+$ und $\cdot$ für Polynome bildet einen Ring, in dem das Kommutativgesetz für $\cdot$ gilt.
(Damit ist $K[X]$ ein kommutativer Ring*.)*
Diesen Ring nennt man den Polynomring *(in der Unbestimmten X) über K.*

Beweis.

Die Axiome für Ringe und das Kommutativgesetz der Multiplikation rechnet man leicht nach. □