4. Zahlentheorie und Algebraische Strukturen

#Mathe #Mathe1 #ZahlentheorieUndAlgebraischeStrukturen

Themen

Teilen und ggT

Definition

Sind $a, b \in \mathbb{Z}$, so heißt a durch b teilbar (b teilt a, in Zeichen $b|a$), wenn es eine Zahl q gibt, so dass $a = b \cdot q$ ist.

Definition

Sind $a, b, d \in \mathbb{Z}$ und gilt $d|a$ und $d|b$, so heißt d ein gemeinsamer Teiler von a und b. Der größte *positive* gemeinsame Teiler von a und b heißt *größter gemeinsamer Teiler* von a und b und wird mit $ggT(a, b)$ bezeichnet.

Hilfsatz >

Wichtig: Der ggT sowie ein nicht verschwindender Rest r bei der Division sind *positive* Zahlen!

Beispiele

1. $a = 54, b = 18 \rightarrow 54 = 18 \cdot 3 + 0 \rightarrow ggT(54, 18) = 3$
2. $a = 7, b = 5 \rightarrow 7 = 5 \cdot 1 + 2 \rightarrow q = 1, r = 2$

3. $a = -7, b = 5 \rightarrow -7 = 5 \cdot (-2) + 3 \rightarrow q = -2, r = 3$

Nach dem beschriebenen Hilfsatz lässt sich der ggT iterativ bestimmten, indem man bei jedem Schritt die betrachteten Zahlen betragsmäßig kleiner macht. Der 'Abstieg' endet, sobald bei der aktuell betrachteten Division der auftretende Rest den Wert 0 besitzt. Das hierfür verwendete Verfahren ist der sogenannte *Euklidische Algorithmus*, dessen Mechanik an den folgenden Beispielen dargestellt werden soll.

Euklidischer Algorithmus

**Beispiele:

1. $ggT(133, 42)$
   $133 = 42 \cdot 3 + 7$
   $42 = 7 \cdot 6 + 0$
   $\rightarrow ggT(133, 42) = 7$
2. $ggT(92, 64)$
   $92 = 64 \cdot 1 + 28$
   $64 = 28 \cdot 2 + 8$
   $28 = 8 \cdot 3 + 4$
   $8 = 4 \cdot 2 + 0$
   $\rightarrow ggT(92, 64) = 4$

Vielfachsummendarstellung

zu 1.: $7 = 1 \cdot 133 + (-3) \cdot 42$

zu 2.:
$$\begin{aligned} 4 &= 1 \cdot 28 + (-3) \cdot 8 \\ &= 1 \cdot 28 + (-3) \cdot (64 + (-2) \cdot 28) \\ &= 7 \cdot 28 + (-3) \cdot 64 \\ &= 7 \cdot (92 + (-1) \cdot 64) + (-3) \cdot 64 \\ &= 7 \cdot 92 + (-10) \cdot 64 \end{aligned}$$

Feststellungen

1. Der ggt zweier Zahlen a und b $(a > b)$ lässt sich berechnen mittels sukzessiver Durchführung der Division mit Rest. Startpunkt ist die Division mit Rest $a : b$.
   Der Endpunkt des Verfahrens ist erreicht, wenn kein Rest mehr auftritt. Der letzte nicht verschwindende Rest der gesuchte ggT.
2. Der ggT zweier Zahlen a und b $(a > b)$ lässt sich immer in der Form $ggT(a, b) = \alpha \cdot a + \beta \cdot b$ mit $(\alpha, \beta \in (Z))$ (sog. Vielfachsummendarstellung). Um diese *Vielfachsummendarstellung* zu ermitteln werden die Zwischenergebnisse aus den einzelnen Schritten des euklidischen Algorithmus verwendet.

Merke

Der ggT mehrerer Zahlen kann iterativ folgendermassen bestimmt werden:

$$ggT(a_1, a_2, \ldots, a_n) = ggT(a_1, ggT(a_2, \ldots, a_n))$$

Modulare Arithmetik / Modulares Rechnen

Definition

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Die Zahlen a, b heißen kongruent modulo n, wenn a-b durch n teilbar ist. In Zeichen $a \equiv b \bmod n$

Satz

Zu einem beliebigen aber fest vorgegebenen n stelle '$\equiv$' auf $\mathbb{Z} \times \mathbb{Z}$ eine Äquivalenzrelation dar. Für die Äquivalenzklasse einer ganzen Zahl a gilt $[a] = \{z \in \mathbb{Z} | z \equiv a \bmod n\} = \{z \in \mathbb{Z} | n | (z - a)\}$. Man schreibt auch $[a] = \{z \in \mathbb{Z} | z \bmod n = a \bmod n\}$. In der Äquivalenzklasse von a sind damit alle die ganzen Zahlen enthalten, die durch n geteilt den gleichen Rest ergeben, als wenn a durch n geteilt wird.

Beispiel $n = 5$:
Es gilt
$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$
$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$
$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$
$[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$
$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$

Somit gelten z.B. die Identitäten $[0] = [15] = [675]$ oder auch $[29] = [9]$. Die Menge der ganzen Zahken ist somit auf 5 Äquivalenzklassen verteilt. Diese Menge der Äquivalenzklassen wird auch bezeichnet als $\mathbb{Z}/5\mathbb{Z}$ oder als $\mathbb{Z}_5$ gleich der Menge der Restklassen modulo 5. Es gilt also $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

Wichtiges zu Schreibweisen

- Die Schreibweise '$z \equiv a \bmod n$' bedeutet, dass z bei der Division durch n den gleichen Rest lässt wie a

- Die Schreibweise '$z \bmod n$' bezeichnet den Rest, der bei der Division von z durch n entsteht
- Die Schreibweise '$z \bmod n = a \bmod n$' drückt aus, dass bei der Division von z durch n der gleiche Rest entsteht wie bei der Division von a durch n

Definition

Es seien $a, b \in \mathbb{Z}$ und $[a], [b]$ die Restklassen modulo n von a und b.
Dann sind auf $\mathbb{Z}_n$ folgende Operationen $\oplus, \otimes$ definiert.

- $[a] \oplus [b] := [a + b]$ (Addition)
- $[a] \otimes [b] := [a \cdot b]$ (Multiplikation)

Statt nun mit den Restklassen zu rechene, wird der Einfachheit halber mit den ausgewählten Resten, d.h. mit den Elementen der Menge $\{0, 1, 2, \ldots, n-1\}$, die bei der Teilung durch n auftreten gerechnet, so dass sich für die Addition/Multiplikation von 2 Elementen $a, b \in \{0, 1, 2, \ldots, n-1\} = \mathbb{Z} + n\mathbb{Z} = \mathbb{Z}_n$ ergibt:

$$a \oplus b = (a + b) \bmod n \text{ bzw. } (a \otimes b) \bmod n$$

Aus dieser Definition ergeben sich am Beispiel von $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$ bzw. $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ somit folgende Verknüpfungstabellen:

Additionstabelle $n = 5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Additionstabelle $n = 6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2

+	0	1	2	3	4	5
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplikationstabelle $n = 5$

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

**Multiplikationstabelle $n = 6$

x	0	1	2	3	4	5
0	0	0	0	0	0	5
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Einsatzgebiete ggT und modilares Rechnen

text

Algebraische Strukturen

Gruppen / Gruppenaxiome

Definition

Gruppenaxiome auf $(G, \circ)$ — Eine Gruppe $(G, \circ)$ besteht aus einer Menge G und einer Verknüpfung '$\circ$' auf G mit den folgenden Eigenschaften:

1. Es gibt ein Element $e \in G$ mit der Eigenschaft $a \circ e = e \circ a = a$ für alle $a \in G$.
   e heißt neutrales Element von G
2. Zu jedem $a \in G$ gibt es ein *eindeutig bestimmtes Element* $a^{-1} \in G$ mit der Eigenschaft $a \circ a^{-1} = a^{-1} \circ a = e$.
   a^{-1} heißt inverses Element zu a
3. Für alle $a, b, c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$.
   G ist assoziativ bezüglich '$\circ$'

Eine Gruppe $(G, \circ)$ heißt *kommutative Gruppe* (abelsche Gruppe), wenn zusätzlich gilt: Für alle $a, b \in G$ ist $a \circ b = b \circ a$.

Beispiele:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sind (kommutative) Gruppen
- $(\mathbb{Q}\backslash\{0\}, \cdot), (\mathbb{R}\backslash\{0\}, \cdot)$ sind (kommutative) Gruppen
- $(\mathbb{Z}_5, +)$ und $(\mathbb{Z}_6, +)$ sind (kommutative) Gruppen

$(\mathbb{Z}, +)$:

1. Es gibt ein Element $0 \in \mathbb{Z}$ mit der Eigenschaft $a + 0 = 0 + a = a$ für alle $a \in \mathbb{Z}$. Die 0 ist also das neutrale Element in $\mathbb{Z}$
2. Zu jedem $a \in \mathbb{Z}$ gibt es ein eindeutig bestimmtes Element $-a \in \mathbb{Z}$ mit der Eigenschaft $a + (-a) = (-a) + a = 0$. $-a$ heißt inverses Element zu a.
3. Für alle $a, b, c \in \mathbb{Z}$ gilt $a + (b + c) = (a + b) + c$. $\mathbb{Z}$ ist assoziativ bezüglich '+'

$(\mathbb{Q}\backslash\{0\}, \cdot)$:

1. Es gibt ein Element $1 \in \mathbb{Q}$ mit der Eigenschaft $a \cdot 1 = 1 \cdot a = 1$ für alle $a \in \mathbb{Q}$. 1 heißt neutrales Element von $\mathbb{Q}$.
2. Zu jedem $a \in \mathbb{Q}$ gibt es ein eindeutig bestimmtes Element $a^{-1} \in \mathbb{Q}$ mit der Eigenschaft $a \cdot a^{-1} = a^{-1} \cdot a = 1$. a^{-1} heißt invereses Element zu a.
3. Für alle $a, b, c \in \mathbb{Q}$ gilt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. $\mathbb{Q}$ ist assoziativ bezüglich '$\cdot$'.

Körper / Körperaxiome

Definition

Eine Menge G mit den Operatoren $+$ und $\times$, also eine Struktur $(G, +, \times)$ wird *Körper* genannt, wenn

- $(G, +)$ eine kommutative Gruppe mit neutralem Element 0 darstellt
- $(G\backslash\{0\}, \times)$ eine kommutative Gruppe mit neutralem Element 1 darstellt

- $\forall a, b, c \in G : a \times (b + c) = a \times b + a \times c$ (Distributiv-Gesetz)

Beispiele:

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_5, +, \cdot)$ sind Körper
- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_6, +, \cdot)$ sind keine Körper

Bemerkungen:

- Es gibt unendliche Körper wie $(\mathbb{Q}, +\cdot)$ oder $(\mathbb{R}, +, \cdot)$
- Es gibt endliche Körper wie $(\mathbb{Z}_5, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$ ist im Allgemeinen kein Körper, außer genau dann wenn n eine Primzahl ist

Ringe / Ringaxiome

Definition

Ein Ring $(R, \oplus, \otimes)$ besteht aus einer Menge R und zwei Verknüpfungen $\oplus, \otimes$ auf R mit den folgenden Eigenschaften:

1. $(R, \otimes)$ ist eine kommutative Gruppe
2. Für alle $a, b, c \in R$ gilt $a \otimes (b \otimes c) = (a \otimes b) \otimes c$. R ist assoziativ bezüglich $\otimes$
3. Für alle $a, b, c \in R$ gilt $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$. R ist distributiv

---

Ein Ring $(R, \oplus, \otimes)$ heißt kommutativ, wenn zusätzlich gilt: Für alle $a, b \in G$ ist $a \otimes b = b \otimes a$. Ein Ring heißt 'Ring mit Eins', wenn in R ein Einselement bezüglich der Operation $\otimes$ enthalten ist.

Beispiele:

- *Ringe:*
  $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sind allesamt kommutative Ringe

- *Ringe mit Eins:*
  $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sind allesamt kommutative Ringe mit Eins

- *Ringe mit Eins, die Körper sind:*
  $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ (n ist eine Primzahl)

- *Ringe mit Eins, die keine Körper sind:*
  $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ (n ist keine Primzahl)

In Ringen wie bspw. $(\mathbb{Z}, +, \cdot)$ kann man definieren und durchführen:

- Division mit Rest und Resklassen (im Sinne von Äquivalenzklassen)
- euklidischen Algorithmus
- ggT-Bestimmung

Polynome und Polynomringe

Definition

Sei K ein beliebiger Körper (z.B. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_5$). Eine Abbildung $p : K \implies K$ der Form $p(x) = \sum_{i=0}^{n} a_i \cdot x^i + a_{n-1} \cdot x^{n-1} + \cdots + a^1 \cdot x + a_0$ (mit $n \in \mathbb{N} \cup 0$) heißt **Polynom über dem Körper K**. Die Zahlen $a_i \in K$ werden Koeffizienten des Polynoms genannt.

Damit gilt: $K[x] = \{p(x) = \sum_{i=0}^{n} a_i \cdot x^i | a_n \neq 0, a_i \in K(i \in 0, \ldots, n), n \in \mathbb{N} \cup 0$

Unter der Voraussetzung $a_n \neq 0$ nenn man $n = deg(p)$ den Grad des Polynoms. Der **Grad eines Polynoms** ist also der *höchste vorkommende Exponent*. Ein Polynom, bei dem der *Koeffizient der höchsten x-Potenz* $a_n \neq 0$ den *Wert 1* hat, nennt man **normiert**.

Beispiele:

- *Polynome aus $\mathbb{R}[x]$:* $\pi x^5 + 2x^3 - 34$, $\sqrt{2x^2} - x + 3$, $x^3 + 1$ (nicht normiert)
- *Polynome aus $\mathbb{Q}[x]$:* $\frac{1}{4}x^5 + 1,1x^3 - 34$, $-0,34x^2 - x + 3$, $x^3 + 1$ (nicht normiert)
- *Polynome aus $\mathbb{Z}_2[x]$:* $x^5 + x^3 + x + 1$, $x^2 + x + 1$ (normiert)
- *Polynome aus $\mathbb{Z}_5[x]$:* $4x^5 + 3x^3 + 2x^2 + 4$, $3x^3 + 2x4$ (nicht nomiert)

Grundrechenarten

$(K[x], +, \cdot)$ stellt bezüglich der in K definierten Addition und Multiplikation einen *kommutativen Ring mit 1* dar.

Beispiel für Addition in $\mathbb{R}[x]$:
$(x^3 - 4x^2 + 5x + 24) + (-x^4 - 2x^3 + 16) = -x^4 - x^3 - 4x^2 + 5x + 40$

Beispiel für Multiplikation in $\mathbb{R}[x]$:
$(x^2 + 2x2) \cdot (x^2 - 3x - 3) = x^4 - x^3 - 7x^2 - 12x - 6$

Beispiel für Addition in $\mathbb{Z}_2[x]$:
$(x^3 + x^2 + x + 1) + (x^4 + x^3 + x^2) = x^4 + x + 1$

Beispiel für Multiplikation in $\mathbb{Z}_5[x]$:
$(2x^2 + 4x + 3) \cdot (3x + 4) = x^3 + 2$

Zur Begründung, dass bspw. $(\mathbb{R}[x], +, \cdot)$ einen Ring mit 1 darställt, lässt sich feststellen:

1. $(\mathbb{R}[x], +)$ ist eine kommutative Gruppe. Das Nullpolynom ist das Nullelement, zu $p(x)$ ist $-p(x)$ das inverse Element.
2. Für alle $p_1(x), p_2(x), p_3(x) \in \mathbb{R}[x]$ gilt $p_1(x) \cdot (p_2(x) \cdot p_3(x)) = (p_1(x) \cdot p_2(x)) \cdot p_3(x)$.
3. Für alle $p_1(x), p_2(x), p_3(x) \in \mathbb{R}[x]$ gilt
   $p_1(x) \cdot (p_2(x) + p_3(x)) = p_1(x) \cdot p_2(x) + p_1(x) \cdot p_3(x)$.
4. Das Einselement ist das Polynom $p(x) = 1 \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + \cdots = 1$.

Division und ggT

Über die mittels Addition und Multiplikation definierten 'normalen' Operatoren in $(K[x], +, \cdot)$ hinausgehend, kann wie auf der Struktur $(\mathbb{Z}, +, \cdot)$ eine *Division mit Rest*, ein *Euklidischer Algorithmus* und eine *ggT-Bestimmung* definiert werden.

Satz zur Polynomdivision

Sind $p(x)$ und $q(x)$ Polynome aus $K[x]$ mit $deg(q) \leq deg(p)$, dann gibt es Polynome $s(x)$ und $r(x)$, so dass gilt: $p(x) = s(x) \cdot q(x) + r(x)$. Der Grad von $s(x)$ ist gleich der Differenz $deg(p) - deg(q)$, der Grad des Restpolynoms r(x) ist kleiner als der des Polynoms $q(x)$, das heißt es gilt $deg(r) < deg(q)$.

Satz zum Euklidischen Algorithmus für Polynome

Auch zu 2 Polynomen $p(x)$ und $q(x)$ kann der ggT bestimmt werden. Aus der Gleichung $p(x) = s(x) \cdot q(x) + r(x)$ ergibt sich sofot die Erkenntnis $ggT(p(x), q(x)) = ggT(q(x), r(x))$, so dass sich analog zum Vorgehen bei der Bestimmung des ggT von zwei ganzen Zahlen nach endlich vielen Schritten ein Divisionsrest 0 ergibt. Der im Iterationsschritt davor sich ergebende, nicht verschwindende Rest ist (ggf. nach Durchführung einer Normierung) der $ggT(p(x), q(x))$.

Der ggT von zwei Polynomen $p(x)$ und $q(x)$ ist das **normierte** Polynom höchsten Grades, das beide Polynome teilt.

Zusätzliche Informationen

1. Der ggT zweier Polynome kann analog der ggT-Darstellunf bei Zahlen, d.h. analog zum Vorgehen in der Struktur $(\mathbb{Z}, +, \cdot)$ als Vielfachsumme der beiden Polynome dargestellt werden. Die Vielfachen sind Elemente $K[x]$.
2. Der ggT von mehr als zwei Polynomen ist iterativ wie bei Zahlen zu ermitteln
3. Analog zu Restklassen $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ im Ring der ganzen Zahlen $\mathbb{Z}$ kann man auch Restklassen im Ring $K[x]$ definieren und betrachten. Diese Restklassen können dann zusammen mit geeigneten Operationen $+$ und $\cdot$ zu Körpern werden. Bei $\mathbb{Z}_n$ war das dann der Fall, wenn n eine Primzahl war.