Algebra und diskrete Mathematik

4. Auflage

Skriptum zur Vorlesung im
Sommersemester 2019

Franz Pauer

Institut für Mathematik
und
Institut für Fachdidaktik
Universität Innsbruck

Vorwort

Das vorliegende Skriptum soll den Hörerinnen und Hörern der Vorlesung „Algebra und diskrete Mathematik “ im Sommersemester 2019 das Mitschreiben und *Mitdenken* in der Vorlesung erleichtern. Das Skriptum enthält alle Definitionen und Sätze der Vorlesung, aber nur wenige Beispiele dazu. In der Vorlesung werden die Definitionen und Sätze motiviert, deren Beweise (und damit der Zusammenhang mit früheren Ergebnissen) erläutert und viele Beispiele vorgetragen.

Im ersten Teil der Vorlesung geht es vor allem um das Rechnen mit ganzen und rationalen Zahlen (Kapitel 1), sowie mit Polynomen, Polynomfunktionen und rationalen Funktionen (Kapitel 2). Kapitel 3 befasst sich mit dem rundungsfreien Rechnen mit algebraischen Zahlen (zum Beispiel Wurzeln). Kapitel 6 geht kurz auf Polynome in mehreren Variablen und algebraische Mengen ein. Die Kapitel 4 und 5 führen in die Graphentheorie ein, es werden Minimalgerüste bestimmt und das Problem des Briefträgers gelöst. Kapitel 7 führt in die Schaltalgebra ein.

Ich habe versucht, mit Begriffen möglichst sparsam umzugehen und nur jene einzuführen, die für die Resultate der Vorlesung von Bedeutung sind. Viele Sätze der Vorlesung könnten allgemeiner formuliert werden, ich habe jedoch darauf verzichtet, um den Blick der Studierenden nicht vom Wesentlichen abzulenken.

Der Inhalt der Vorlesung Lineare Algebra, VO4, wird als bekannt vorausgesetzt. Dieses Skriptum hat viel mit meinen Skripten Algebra (6. Auflage 2018) und Graphentheorie (5. Auflage 2007) gemeinsam.

Die erste Auflage (2016) dieses Skriptums ist in zwei Teilen erschienen. Diese wurden in dieser zweiten Auflage zusammengeführt. Florian Dreier hat viele Zeichnungen und Ergänzungen mit LaTeX erstellt und eingefügt.

Die vierte Auflage (2019) dieses Skriptums unterscheidet sich von der dritten nur durch kleine Korrekturen.

Innsbruck, Februar 2019

Inhaltsverzeichnis

KAPITEL 1

Rechnen mit ganzen und rationalen Zahlen

Es sei $\mathbb{N} := \{0,1,2,\ldots\}$ die Menge der natürlichen Zahlen. Wir setzen die Menge $\mathbb{Z} := \{\ldots,-2,-1,0,1,2,\ldots\}$ der ganzen Zahlen mit den *Rechenoperationen* Addition

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ (a,b) \longmapsto a+b,$$

und Multiplikation

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ (a,b) \longmapsto a \cdot b,$$

als bekannt voraus. Dabei gelten die folgenden Rechenregeln (kurz: $\mathbb{Z}$ mit $+$ und $\cdot$ ist ein kommutativer Ring):
Für alle ganzen Zahlen a,b,c ist

- $(a+b)+c = a+(b+c) =: a+b+c$ („Die Addition von ganzen Zahlen ist assoziativ“, das heißt: auf Klammern kann verzichtet werden).
- $0+a = a+0 = a$ („Die Zahl 0 ist das Nullelement von $\mathbb{Z}$“).
- $a+(-a) = (-a)+a = 0$ (dabei ist $-a := (-1)\cdot a$)
- $a+b = b+a$ („Die Addition ist kommutativ“).
- $(a \cdot b)\cdot c = a \cdot (b \cdot c) =: a \cdot b \cdot c$ („Die Multiplikation ist assoziativ“).
- $1 \cdot a = a \cdot 1 = a$ („Die Zahl 1 ist das Einselement von $\mathbb{Z}$“).
- $a \cdot b = b \cdot a$ („Die Multiplikation ist kommutativ“).
- $(a+b)\cdot c = (a\cdot c)+(b\cdot c) =: a\cdot c + b\cdot c$ („Distributivgesetz“)

Für $a,b \in \mathbb{Z}$ folgt aus $a \cdot b = 0$, dass $a = 0$ oder $b = 0$ ist.
Für $a,b,c \in \mathbb{Z}$ mit $c \neq 0$ folgt aus $a\cdot c = b\cdot c$, dass $(a-b)\cdot c = 0$ und daher $a-b = 0$. („In $\mathbb{Z}$ kann durch Zahlen $\neq 0$ gekürzt werden“).

Aus diesen grundlegenden Rechenregeln für ganze Zahlen können leicht weitere abgeleitet werden, zum Beispiel die „binomischen Formeln“:
Für alle ganzen Zahlen a und b ist

- $a^2 + 2ab + b^2 = (a+b)^2$
- $a^2 - 2ab + b^2 = (a-b)^2$
- $a^2 - b^2 = (a+b)\cdot(a-b)$

Beachte: Statt 3 bzw. 2 Multiplikationen auf der linken Seite muss auf der rechten Seite nur eine ausgeführt werden!
Die *Subtraktion* ist durch $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ (a,b) \longmapsto a+(-b) =: a-b$, gegeben.
Für ganze Zahlen a,b schreiben wir $a \leq b$ genau dann, wenn $b-a \in \mathbb{N}$ ist (Sprechweise: a ist kleiner oder gleich b). Wir schreiben $a < b$ für: $a \leq b$ und $a \neq b$ (Sprechweise: a ist kleiner als b).

Eine ganze Zahl ist *positiv* bzw. *negativ*, wenn sie größer bzw. kleiner als 0 ist. Es gilt:

$$\text{für } a,b,c \in \mathbb{Z} \text{ ist } a \leq b \text{ genau dann, wenn } a+c \leq b+c$$

und

$$\text{für } a,b,c \in \mathbb{Z} \text{ mit } c>0 \text{ ist } a \leq b \text{ genau dann, wenn } a \cdot c \leq b \cdot c \ .$$

Statt $a \cdot b$ schreibt man oft nur ab. Statt $(a \cdot b)+c$ schreibt man oft nur $a \cdot b+c$ („Punktrechnung kommt vor Strichrechnung“).

Das *Vorzeichen* $vz(a)$ einer ganzen Zahl a ist 1, wenn $a \in \mathbb{N}$, und -1, wenn $a \notin \mathbb{N}$. Der *Betrag* $|a|$ einer ganzen Zahl a ist $vz(a) \cdot a$. Für Zahlen $a,b \in \mathbb{Z}$ ist $|a \cdot b| = |a| \cdot |b|$ und $|a+b| \leq |a|+|b|$.

§1. Division mit Rest

Wenn Sie einen Sack mit a Euromünzen haben, die Sie an b Personen verteilen sollen (jede soll gleich viel bekommen), dann werden Sie wahrscheinlich zuerst jeder Person einen Euro geben und diesen Vorgang solange wiederholen, bis im Sack weniger als b Euromünzen sind. Sie haben dann *a mit Rest durch b dividiert*.
Der folgende Satz ist grundlegend für alle Rechenverfahren für ganze Zahlen. Seine Bedeutung liegt darin, dass er die Beziehung zwischen den drei „Strukturen“ $+, \cdot$ und $\leq$ beschreibt.

Satz 1 : (Division mit Rest von ganzen Zahlen)
Zu je zwei ganzen Zahlen a und b mit $b \neq 0$ *gibt es eindeutig bestimmte ganze Zahlen m und r mit den Eigenschaften*

$$a = m \cdot b + r \quad \textit{und} \quad 0 \leq r < |b| \ .$$

Die Zahlen m bzw. r heißen ganzzahliger Quotient von a und b *bzw.* Rest von a nach Division durch b. *Die Zahlen m und r können mit dem folgenden Verfahren (*Divisionsalgorithmus*) berechnet werden:*

- *Falls a und b natürliche Zahlen sind:*
  Setze $m := 0$ *und* $r := a$.
  Solange $r \geq b$ *ist, ersetze r durch* $r-b$ *und m durch* $m+1$.
  („Subtrahiere b solange von a, wie die Differenz noch nicht negativ ist. Der Rest ist dann die letzte Differenz und der ganzzahlige Quotient die Anzahl der ausgeführten Subtraktionen“.)
- *Falls* $a < 0$ *oder* $b < 0$ *ist:*
  Berechne wie oben n und s so, dass $|a| = n \cdot |b| + s$ *und* $0 \leq s < |b|$ *ist.*
  Wenn $a \geq 0$ *ist, dann setze* $m := -n$ *und* $r := s$.
  Wenn $a < 0$ *und* $s > 0$ *ist, dann setze* $m := -vz(b) \cdot (n+1)$ *und* $r := |b| - s$.
  Wenn $a < 0$ *und* $s = 0$ *ist, dann setze* $m := -vz(b) \cdot n$ *und* $r := 0$.

Beweis: Wenn a und b natürliche Zahlen sind, dann erhalten wir bei jedem Ersetzen von r durch $r-b$ eine um mindestens 1 kleinere Zahl. Also tritt nach höchstens a Schritten der Fall $r<b$ ein. Somit liefert das obige Verfahren nach endlich vielen Schritten ein Ergebnis m,r. Mit Induktion über a ist leicht nachzuprüfen, dass diese Zahlen die angegebenen Bedingungen erfüllen.
Wenn a oder b keine natürliche Zahl ist: $|a|$ mit Rest durch $|b|$ dividieren und dann daraus die gesuchten Zahlen ermitteln.
Es seien m_1,m_2,r_1,r_2 ganze Zahlen mit

$$a=m_1\cdot b+r_1=m_2\cdot b+r_2,\ 0\le r_1,r_2<|b|$$

und o.E.d.A. („ohne Einschränkung der Allgemeinheit“) $r_1\le r_2$. Dann ist

$$|b|>r_2-r_1=|m_1-m_2|\cdot|b|\ .$$

Daraus folgt $m_1=m_2$ und $r_1=r_2$, also sind der ganzzahlige Quotient von a und b und der Rest von a nach Division durch b eindeutig bestimmt.

Beispiel 2 :

$$\begin{aligned} 17&=3\cdot5+2, && 0\le2<5\\ -17&=(-4)\cdot5+3, && 0\le3<5\\ 17&=(-3)\cdot(-5)+2, && 0\le2<5\\ -17&=4\cdot(-5)+3, && 0\le3<5 \end{aligned}$$

§2. Zifferndarstellung von Zahlen

Nehmen wir an, Sie kommen mit einem Sack voller Euromünzen in eine Bank und wollen dieses Geld auf ihr Sparbuch einzahlen. Die Anzahl der Euromünzen im Sack ist eine eindeutig bestimmte natürliche Zahl a. Bevor diese Zahl in Ihr Sparbuch eingetragen werden kann, muss ihre *Zifferndarstellung* (zur Basis 10) berechnet werden. Eine Zahl ist also nicht immer schon in Zifferndarstellung gegeben, sondern diese ist eine „Zusatzinformation“ über die Zahl. Wie wird die Zifferndarstellung zur Basis 10 von a ermittelt? Man bildet aus den Euromünzen solange „Zehnerstapel“, bis nur noch weniger als zehn Münzen übrigbleiben, das heißt: a wird mit Rest durch 10 dividiert. Die Anzahl der übriggebliebenen Euromünzen ist dann die „Einerziffer“ von a. Macht man dasselbe nun mit den Zehnerstapeln statt mit den Münzen, dann erhält man die „Zehnerziffer“ von a, usw.

Satz 3 : (Darstellung von Zahlen durch Ziffern)
Es seien a und b natürliche Zahlen mit $a \neq 0$ und $b \geq 2$. Dann gibt es eindeutig bestimmte natürliche Zahlen $n, z_0, z_1, \ldots, z_n$ so, dass

$$z_n \neq 0,\ 0 \leq z_0, z_1, \ldots, z_n < b$$

und

$$a = z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0 = \sum_{i=0}^{n} z_i b^i$$

ist.
Wenn b fest gewählt ist, dann ist a durch die Zahlen $n, z_0, z_1, \ldots, z_n$ eindeutig bestimmt. Man wählt Zeichen für die Zahlen von 0 bis $b-1$ und schreibt

$$z_n z_{n-1} \ldots z_0 \quad \textit{statt} \quad \sum_{i=0}^{n} z_i b^i \quad .$$

Die Zahlen $z_0, z_1, \ldots, z_n$ heißen Ziffern von a zur Basis b *(für b=2 bzw. 10: „Binärziffern“ bzw. „Dezimalziffern“).*

Die Ziffern z_i von $a \neq 0$ zur Basis b können mit dem folgenden Verfahren berechnet werden:

- *Setze $i := 0$ und $z_0 :=$ Rest von a nach Division durch b.*
- *Solange a nicht 0 ist: Die i-te Ziffer z_i ist der Rest von a nach Division durch b. Ersetze a durch den ganzzahligen Quotienten von a und b. Ersetze i durch $i+1$.*

Beweis: Induktion über a:
Wenn $a = 1$ ist, ist $n = 0$ und $z_0 = 1$.
Für $a > 1$ seien m bzw. r der ganzzahlige Quotient von a und b bzw. der Rest von a nach Division durch b. Wegen $b > 1$ ist $m < a$, also gibt es nach Induktionsannahme eindeutig bestimmte Zahlen $k, y_0, y_1, \ldots, y_k$ so, dass $y_k \neq 0$, $0 \leq y_0, y_1, \ldots, y_k < b$ und

$$m = y_k b^k + y_{k-1} b^{k-1} + \ldots + y_1 b^1 + y_0$$

ist. Dann ist

$$a = m \cdot b + r = y_k b^{k+1} + y_{k-1} b^k + \ldots + y_1 b^2 + y_0 b + r\ ,$$

und $y_k, \ldots, y_0, r$ sind die Ziffern von a. Aus der Eindeutigkeit von m und r folgt aus der Induktionsannahme die Eindeutigkeit der Ziffern von a zur Basis b.

Beispiel 4 : Es sei $a :=$ sechsundzwanzig und $b :=$ zwei. Dann:
$a =$ dreizehn$\cdot b + 0$, also $z_0 = 0$
dreizehn = sechs$\cdot b + 1$, also $z_1 = 1$
sechs = drei$\cdot b + 0$, also $z_2 = 0$
drei = $1 \cdot b + 1$, also $z_3 = 1$

$1 = 0 \cdot b + 1$, also $z_4 = 1$
Die Zifferndarstellung von sechsundzwanzig zur Basis zwei ist daher 11010.

Beispiel 5 : Zeitangaben in Stunden, Minuten und Sekunden sind die Zifferndarstellung zur Basis 60 dieser Zeit in Sekunden.

Wird für die Zifferndarstellung einer Zahl die Basis b gewählt, dann können alle Zahlen durch Aneinanderreihen von b verschiedenen Symbolen angeschrieben werden. Eine kleine Basis (zum Beispiel 2) hat den Vorteil, dass man nur wenige Symbole braucht und dass das „kleine Einmaleins" sehr einfach ist. Allerdings braucht man dann für größere Zahlen sehr viele Ziffern.

Üblicherweise meint man mit „runden Zahlen" Zahlen mit der Eigenschaft, dass alle ihre Ziffern zur Basis zehn nach der (von links gelesen) ersten Ziffer Null sind. Rund zu sein ist also nicht eine Eigenschaft der Zahl allein, sondern ihrer Zifferndarstellung zur Basis 10. Man kann nicht annehmen, dass unsere Art, die Zahlen darzustellen, sich auf Naturphänomene auswirkt. Daher sind z.B. Wettervorhersagen nach dem „hundertjährigen Kalender" oder Weltuntergangsprophezeiungen anlässlich der Jahrtausendwende sehr fragwürdig.

Definition 6 : Es seien $v = (v_1, \ldots, v_n)$ und $w = (w_1, \ldots, w_n)$ zwei verschiedene n-Tupel von ganzen Zahlen und j die kleinste Zahl in $\{1, \ldots, n\}$ mit der Eigenschaft, dass $v_j \neq w_j$ ist.
Dann ist *v lexikographisch kleiner* als w (Schreibweise: $v <_{lex} w$), wenn $v_j < w_j$ ist.

Beispiel 7 : $(1,2,3,4) <_{lex} (1,2,4,3) <_{lex} (2,-7,-3,-5)$

Satz 8 : (Vergleich von zwei Zahlen, die durch Ziffern dargestellt sind) *Es seien b, x, y positive natürliche Zahlen, $b \geq 2$ und*

$$x_k, x_{k-1}, \ldots, x_0 \quad \textit{bzw.} \quad y_\ell, y_{\ell-1}, \ldots, y_0$$

die Ziffern von x bzw. y bezüglich b.
Dann ist x genau dann kleiner als y, wenn

$$k < \ell \quad \textit{oder} \quad (k = \ell \textit{ und } (x_k, x_{k-1}, \ldots, x_0) <_{lex} (y_\ell, y_{\ell-1}, \ldots, y_0)) \textit{ ist.}$$

Beweis: Wenn $k < \ell$ ist, dann ist

$$x = \sum_{i=0}^{k} x_i b^i \leq \sum_{i=0}^{k} (b-1) b^i = \sum_{i=1}^{k+1} b^i - \sum_{i=0}^{k} b^i = b^{k+1} - 1 < b^{k+1} \leq y \, .$$

Es seien $k = \ell$ und j die größte Zahl mit der Eigenschaft, dass $x_j \neq y_j$ ist. Wenn $x_j < y_j$ ist, dann ist

$$\sum_{i=0}^{j} x_i b^i \leq x_j b^j + (b^j - 1) < (x_j + 1) b^j \leq y_j b^j \leq \sum_{i=0}^{j} y_i b^i$$

und

$$x = \sum_{i=j+1}^{k} x_i b^i + \sum_{i=0}^{j} x_i b^i < \sum_{i=j+1}^{k} x_i b^i + \sum_{i=0}^{j} y_i b^i = y \, .$$

§3. Rechenverfahren für Zahlen in Zifferndarstellung

Es sei b eine natürliche Zahl mit $b \geq 2$. In diesem Abschnitt werden Verfahren angegeben, mit welchen die Zifferndarstellung zur Basis b der Summe, der Differenz, des Produktes, des ganzzahligen Quotienten und des Restes nach Divison zweier natürlicher Zahlen, die durch Ziffern zur Basis b gegeben sind, berechnet werden kann.

Es seien b, x, y, k, ℓ natürliche Zahlen, $b \geq 2$ und

$$x_k, x_{k-1}, \ldots, x_0 \quad \text{bzw.} \quad y_\ell, y_{\ell-1}, \ldots, y_0$$

die Ziffern von x bzw. y bezüglich b. O.E.d.A. sei $\ell \leq k$ und wir definieren $y_{\ell+1} := 0, \ldots, y_k := 0$.

Satz 9 : (Addition von zwei Zahlen, die durch Ziffern dargestellt sind) *Für je zwei Zahlen in $\{0, \ldots, b-1\}$ sei die Zifferndarstellung ihrer Summe („das kleine Eins plus Eins“) bekannt.*
Dann können die Ziffern von $x + y$ mit dem folgenden Verfahren berechnet werden:

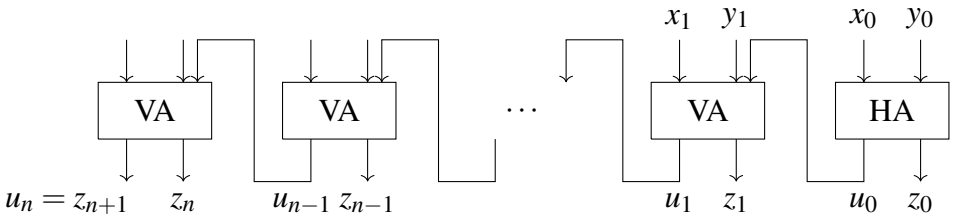
- *Ermittle die Ziffern $(x_0 + y_0)_1$ und $(x_0 + y_0)_0$ von $x_0 + y_0$.*
  Setze $(x+y)_0 := (x_0 + y_0)_0$, $u_0 := (x_0 + y_0)_1$ und $i := 0$.
- *Solange $i < k$ ist, setze $i := i + 1$ und ermittle die Ziffern*
  $(x_i + y_i + u_{i-1})_1$ und $(x_i + y_i + u_{i-1})_0$ von $x_i + y_i + u_{i-1}$.
  Setze $(x+y)_i := (x_i + y_i + u_{i-1})_0$ und $u_i := (x_i + y_i + u_{i-1})_1$ („i-ter Übertrag“).
- *Wenn $u_k \neq 0$ ist, setze $(x+y)_{k+1} := u_k$.*

Beweis: Wir zeigen durch Induktion über i, dass $u_{i-1} \leq 1$ und $(x_i + y_i + u_{i-1}) < 2b$ ist (daher hat $(x_i + y_i + u_{i-1})$ höchstens zwei Ziffern).
Für $i = 1$ folgt aus $x_0 < b$ und $y_0 < b$, dass
$x_0 + y_0 \leq (b-1) + (b-1) = 2b - 2$ ist. Somit ist $u_0 \leq 1$ und
$x_1 + y_1 + u_0 < 2b - 1$.
Für $i > 1$ folgt aus $u_{i-2} \leq 1$, $x_{i-1} < b$ und $y_{i-1} < b$, dass
$x_{i-1} + y_{i-1} + u_{i-2} \leq (b-1) + (b-1) + 1 = 2b - 1$ und $u_{i-1} \leq 1$ ist.

Beispiel 10 :

Basis 2	Basis 8	Basis 10
1 1 0 1 1	7 3 4	5 6 7
1 1 0 1	2 3 5	4 3 4
1 0 1 0 0 0	1 1 7 1	1 0 0 1

Beispiel 11 : Addierwerk:



VA... Volladdierer
HA... Halbaddierer

$0 \le x_0, \ldots, x_n, y_0, \ldots, y_n \le 1, \quad 0 \le u_1, \ldots, u_n, z_0, \ldots, z_{n+1} \le 1$

Satz 12 : (Subtraktion von zwei Zahlen, die durch Ziffern dargestellt sind)
Für je zwei Zahlen u, v in $\{0, \ldots, b-1\}$ sei die Zifferndarstellung von $u-v$, wenn $u \ge v$ ist, und von $(b+u)-v$, wenn $u < v$ ist, bekannt.
Dann können die Ziffern von $x-y$ mit dem folgenden Verfahren berechnet werden:

- *Sei $i := 0$. Wenn $x_0 \ge y_0$ ist, setze $(x-y)_0 := x_0 - y_0$ und $u_0 := 0$.*
  Wenn $x_0 < y_0$ ist, setze $(x-y)_0 := (b+x_0) - y_0$ und $u_0 := 1$.
- *Solange $i \le k$ ist, setze $i := i+1$.*
  Wenn $x_i \ge y_i + u_{i-1}$ ist, setze $(x-y)_i := x_i - y_i - u_{i-1}$ und $u_i := 0$.
  Wenn $x_i < y_i + u_{i-1}$ ist, setze $(x-y)_i := b + x_i - y_i - u_{i-1}$ und $u_i := 1$
  (u_i heißt der „i-te Übertrag“).

Beweis: Übung.

Beispiel 13 :

Basis 2	Basis 8	Basis 10
1 1 0 1 1	7 3 4	5 6 7
− 1 1 0 1	− 2 3 5	− 4 8 4
1 1 1 0	4 7 7	8 3

Satz 14 : (Multiplikation von zwei Zahlen, die durch Ziffern dargestellt sind) *Für je zwei Zahlen in* $\{0,\dots,b-1\}$ *sei die Zifferndarstellung ihres Produktes bekannt („das kleine Einmaleins").*
Sind $z_n,\dots,z_0$ *die Ziffern einer positiven ganzen Zahl* z *zur Basis* b*, dann sind* $z_{n+j},z_{n-1+j},\dots,z_j,0,\dots,0$ *die* $n+1+j$ *Ziffern von* $z\cdot b^j$*.*
Die Ziffern von $x\cdot y$ *können mit dem folgenden Verfahren berechnet werden:*

- *Für alle* j *mit* $0\le j\le k$ *ermittle die Ziffern* $(x_0\cdot y_j)_1$ *und* $(x_0\cdot y_j)_0$ *von* $x_0\cdot y_j$*. Setze* $(x\cdot y_j)_0:=(x_0\cdot y_j)_0$*,* $u_0:=(x_0\cdot y_j)_1$ *und* $i:=0$*.*
- *Solange* $i<k$ *ist, setze* $i:=i+1$ *und ermittle die Ziffern* $(x_i\cdot y_j+u_{i-1})_1$ *und* $(x_i\cdot y_j+u_{i-1})_0$ *von* $x_i\cdot y_j+u_{i-1}$*.*
  Setze $(x\cdot y_j)_i:=(x_i\cdot y_j+u_{i-1})_0$ *und* $u_i:=(x_i\cdot y_j+u_{i-1})_1$ *(„i-ter Übertrag").*
- *Wenn* $u_k\neq 0$ *ist, setze* $(x\cdot y)_{k+1}:=u_k$*.*
- *Berechne die Zifferndarstellung zur Basis* b *der Summe der Zahlen* $(x\cdot y_j)\cdot b^j$*,* $0\le j\le k$*.*

(In Worten: Multipliziere zuerst x *mit jeder Ziffer von* y*, multipliziere dann jedes Produkt* $x\cdot y_j$ *mit* b^j *und summiere schließlich alle Produkte* $(x\cdot y_j)\cdot b^j$ *auf).*

Beweis: Übung.

In Satz 1 wurde bereits ein Divisionsalgorithmus angegeben. Wenn eine Zifferndarstellung der gegebenen Zahlen bekannt ist, kann dieses Verfahren mit Hilfe dieser zusätzlichen Information verbessert werden.

Beispiel 15 : Wenn $x=2019$ und $y=7$ ist, dividiert man zunächst 20 mit Rest durch 7, subtrahiert also 7 zweimal und erhält $20=2\cdot 7+6$.
Daraus schließt man $2000=200\cdot 7+600$ und $2019=200\cdot 7+619$ (also hat man dank der Zifferndarstellung statt 200 Subtraktionen nur 2 ausführen müssen).
Der Rest von 2019 nach Division durch 7 ist derselbe wie der von 619 nach Division durch 7 und der ganzzahlige Quotient von 2019 und 7 ist die Summe von 200 und dem ganzzahligen Quotienten von 619 und 7.
Man dividiert jetzt noch 619 mit Rest durch 7, dazu geht man wieder gleich vor wie oben: $60=8\cdot 7+4$, also ist $600=80\cdot 7+40$, somit $619=80\cdot 7+59$ und $2019=280\cdot 7+59$.
Da 57 größer als 7 ist, ist noch ein weiteres „Durchlaufen der Schleife" nötig: $59=8\cdot 7+3$.
Der ganzzahlige Quotient von 2019 nach Division durch 7 ist daher $288=200+80+8$, der Rest ist 3.
Durch Ausnutzen der Zifferndarstellung der zwei Zahlen mussten anstatt 288 Subtraktionen nur $2+8+8=18$ Subtraktionen ausgeführt werden.

Satz 16 : (Division mit Rest von Zahlen, die durch Ziffern dargestellt sind)
Es seien x, y, k, ℓ natürliche Zahlen und

$$x_k, x_{k-1}, \ldots, x_0 \quad \textit{bzw.} \quad y_\ell, y_{\ell-1}, \ldots, y_0$$

die Ziffern von x bzw. y bezüglich b. O.E.d.A. sei $\ell \leq k$.
Für je zwei natürliche Zahlen u und v mit $u < b \cdot v$ sei die Zifferndarstellung des ganzzahligen Quotienten und des Restes von u nach Division durch v bekannt.
Dann können die Ziffern des ganzzahligen Quotienten m von x und y mit dem folgenden Verfahren berechnet werden:

- *Setze $j := k - \ell$, wenn $\sum_{i=0}^{\ell} x_{i+k-\ell} b^i \geq y$ ist, und $j := k - \ell - 1$, sonst. Dann ist $\sum_{i \geq 0} x_{i+j} b^i < b \cdot y$.*
- *Solange $j \geq 0$ ist, berechne den ganzzahligen Quotienten m_j von $\sum_{i \geq 0} x_{i+j} b^i$ und y. Dieser ist die j-te Ziffer von m.*
  Ersetze x durch $x - m_j \cdot y \cdot b^j$ und j durch $j - 1$.

Beweis: Übung.

Wichtig: Bei diesem Verfahren zur Division mit Rest von natürlichen Zahlen, deren Zifferndarstellung bekannt ist, werden beliebige Divisionen mit Rest auf mehrere Divisionen mit Rest zurückgeführt, deren *ganzzahliger Quotient mit nur einer Ziffer darstellbar ist*.
Die Division mit Rest (von ganzen Zahlen) darf nicht mit der Division (von rationalen oder reellen Zahlen) verwechselt werden.

§4. Rationale Zahlen

Es seien a und b ganze Zahlen, wobei $b \neq 0$ ist. Die Aufgabe „Finde eine Zahl z so, dass $b \cdot z = a$ ist“ bezeichnen wir als „Gleichung“ $b \cdot x = a$. Eine Zahl z mit $b \cdot z = a$ heißt *Lösung* von $b \cdot x = a$. Wenn $b > 1$ ist, dann hat zum Beispiel die Aufgabe $b \cdot x = 1$ in $\mathbb{Z}$ keine Lösung. Um Lösungen zu erhalten, müssen wir „den Zahlenbereich erweitern“.

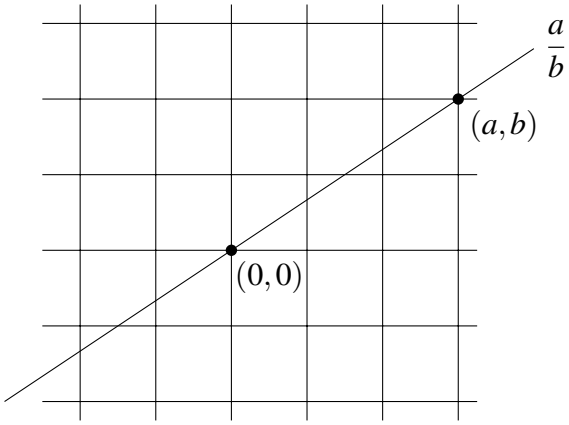
Ein Zahlenbereich wird durch eine *Zahlenmenge* und zwei darauf definierte *Rechenoperationen* („Addition“und „Multiplikation“) festgelegt. Dann kann untersucht werden, welche *Rechenregeln* für die zwei Rechenoperationen gelten.

Die Aufgabe $b \cdot x = a$ wird durch das Paar $(a, b) \in \mathbb{Z}^2$ eindeutig beschrieben, also liegt es nahe, die „neuen Zahlen“ durch Paare von ganzen Zahlen zu beschreiben. Allerdings sollten für $t \in \mathbb{Z}$, $t \neq 0$, die Gleichungen $b \cdot x = a$ und $t \cdot b \cdot x = t \cdot a$ dieselbe Lösung haben, daher sollen die Zahlenpaare (a, b) und $(t \cdot a, t \cdot b)$ dieselbe „neue Zahl“ beschreiben.

Definition 17 : Es seien a und b ganze Zahlen, wobei $b \neq 0$. Dann ist die Menge

$$\frac{a}{b} := \{(c,d) \mid c,d \in \mathbb{Z}, a \cdot d = b \cdot c, d \neq 0\}$$

die durch den „Zähler“ a und den „Nenner“ b gegebene *rationale Zahl* oder *Bruchzahl*. (Beachte: Eine Bruchzahl ist durch Vorgabe von Zähler und Nenner eindeutig bestimmt, aber umgekehrt sind Zähler und Nenner durch die Bruchzahl nicht eindeutig bestimmt). Wir schreiben $\mathbb{Q}$ für die Menge der rationalen Zahlen.
Für die Bruchzahl $\frac{a}{1}$ schreiben wir oft nur a und fassen so $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ auf. („Jede ganze Zahl ist eine rationale Zahl“).



Satz 18 : *Es seien a', b' ganze Zahlen und $b' \neq 0$. Dann sind die Bruchzahlen $\frac{a}{b}$ und $\frac{a'}{b'}$ genau dann gleich, wenn $a \cdot b' = a' \cdot b$ ist.*

Beweis: Wenn $\frac{a}{b} = \frac{a'}{b'}$ ist, dann ist insbesondere $(a',b') \in \frac{a}{b}$, also
$a \cdot b' = a' \cdot b$.
Sei umgekehrt $a \cdot b' = a' \cdot b$ und $(c,d) \in \frac{a}{b}$, also $b \cdot c = a \cdot d$. Dann ist zu zeigen, dass $(c,d) \in \frac{a'}{b'}$, also $b' \cdot c = a' \cdot d$ ist.
Es ist

$$a \cdot (b' \cdot c) = (a \cdot b') \cdot c = (a' \cdot b) \cdot c = a' \cdot (b \cdot c) = a' \cdot (a \cdot d) = a \cdot (a' \cdot d) \ .$$

Falls $a \neq 0$ ist, folgt daraus a$b' \cdot c = a' \cdot d$. Falls $a = 0$ ist, muss auch $a' = 0$ sein, also ist $\frac{a}{b} = 0 = \frac{a'}{b'}$

Satz 19 : *Für den Nenner einer Bruchzahl kann immer eine positive Zahl gewählt werden. Dann wird die totale Ordnung $\leq$ auf $\mathbb{Z}$ durch*

$$\frac{a}{b} \leq \frac{c}{d} :\Leftrightarrow a \cdot d \leq b \cdot c$$

zu einer totalen Ordnung auf $\mathbb{Q}$ erweitert.

Beweis: Zuerst ist zu zeigen, dass die Definition von $\leq$ nicht von der Wahl von Zähler und positivem Nenner abhängt.
Seien $a,a',c,c' \in \mathbb{Z}$ und b,b',d,d' positive ganze Zahlen so, dass $a\cdot b' = a'\cdot b$, $c\cdot d' = c'\cdot d$ und $a\cdot d \leq b\cdot c$ ist. Dann ist

$$a'\cdot d'\cdot b\cdot d = a\cdot d'\cdot b'\cdot d \leq b\cdot d'\cdot b'\cdot c = b'\cdot c'\cdot b\cdot d$$

und $a'\cdot d' \leq b'\cdot c'$.
Seien $a,c,e \in \mathbb{Z}$, b,d,f positive ganze Zahlen so, dass $\frac{a}{b} \leq \frac{c}{d}$ und $\frac{c}{d} \leq \frac{e}{f}$ ist. Es ist noch zu zeigen, dass dann auch $\frac{a}{b} \leq \frac{e}{f}$ ist. Aus $a\cdot d\cdot f \leq b\cdot c\cdot f \leq b\cdot d\cdot e$ folgt $a\cdot f \leq b\cdot e$ und daher die Behauptung.

Wir werden nun die Rechenoperationen von $\mathbb{Z}$ auf $\mathbb{Q}$ fortsetzen.

Satz 20 : *Die Funktionen*

$$+ : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}\ , \quad (\frac{a}{b},\frac{c}{d}) \longmapsto \frac{a}{b}+\frac{c}{d} := \frac{ad+bc}{bd}\ ,$$

und

$$\cdot : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}\ , \quad (\frac{a}{b},\frac{c}{d}) \longmapsto \frac{a}{b}\cdot\frac{c}{d} := \frac{ac}{bd}\ ,$$

sind wohldefiniert. Diese Rechenoperationen in $\mathbb{Q}$ erfüllen die gleichen Rechenregeln wie Addition und Multiplikation in $\mathbb{Z}$.

Die Einschränkungen von $+$ und $\cdot$ auf $\mathbb{Z}\times\mathbb{Z}$ stimmen mit der Addition und der Multiplikation auf $\mathbb{Z}$ überein.

Darüberhinaus hat jedes Element $\frac{a}{b} \in \mathbb{Q}\setminus\{0\}$ ein inverses Element *$(\frac{a}{b})^{-1}$ mit der Eigenschaft*

$$(\frac{a}{b})^{-1}\cdot\frac{a}{b} = 1\,,$$

und zwar ist

$$(\frac{a}{b})^{-1} = \frac{b}{a}\ .$$

(Kurz: $\mathbb{Q}$ mit den Rechenoperationen Addition und Multiplikation ist ein Körper).

Beweis: Wir müssen zuerst zeigen, dass die Funktionen $+$ und $\cdot$ wohldefiniert sind, das heißt: wenn $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$ ist, dann muss auch

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \quad \text{und} \quad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

sein.
Aus $a'b = ab'$ und $c'd = cd'$ folgt

$$(ad+bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = bd(a'd'+b'c')$$

und

$$(ac)b'd' = bd(a'c') \ .$$

Die Rechenregeln können leicht nachgeprüft werden.

§5. Zifferndarstellung von rationalen Zahlen

Satz 21 : (Zifferndarstellung von rationalen Zahlen)
Es seien b, c, d, p positive ganze Zahlen mit $b \geq 2$. Dann gibt es eindeutig bestimmte natürliche Zahlen $n, z_n, \ldots, z_0, z_{-1}, \ldots, z_{-p}$ so, dass

$$z_n \neq 0 \text{ oder } n = 0, \quad 0 \leq z_n, \ldots, z_0, z_{-1}, \ldots, z_{-p} < b$$

und

$$0 \leq \frac{c}{d} - (z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0 + z_{-1} b^{-1} + \ldots + z_{-p} b^{-p}) < b^{-p}$$

ist. Ist b fest gewählt, schreibt man

$$z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots z_{-p} \quad \textit{statt} \quad \sum_{i=-p}^{n} z_i b^i \ .$$

Die Zahlen $z_n, \ldots, z_0, z_{-1}, \ldots, z_{-p}$ heißen Ziffern von $\frac{c}{d}$ zur Basis b.
Diese können wie folgt berechnet werden:

- *Berechne die Ziffern $y_0, \ldots, y_k$ zur Basis b des ganzzahligen Quotienten m von $c \cdot b^p$ und d .*
- *Setze $z_i := y_{i+p}$, $-p \leq i \leq k - p =: n$.*

Beweis: Sei r der Rest von $c \cdot b^p$ nach Division durch d. Wegen $c \cdot b^p = m \cdot d + r$ ist dann

$$\frac{c \cdot b^p}{d \cdot b^p} = \frac{m \cdot d}{d \cdot b^p} + \frac{r}{d \cdot b^p} \ ,$$

also

$$\frac{c}{d} = \frac{m}{b^p} + \frac{r}{d} \cdot b^{-p} \quad \text{und} \quad \frac{r}{d} < 1 \ .$$

Rationale Zahlen können also „beliebig genau“ durch Zahlen der Form $z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots z_{-p}$ angenähert werden, aber es gibt rationale Zahlen, die für alle p von $z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots z_{-p}$ verschieden sind.

Eine rationale Zahl

$$z_0 . z_{-1} z_{-2} \ldots z_{-p} \, Ee \ := \ z_0 . z_{-1} z_{-2} \ldots z_{-p} \cdot b^e$$

mit $b \geq 2$ und $z_0 \neq 0$ ist in *Exponentialform* zur Basis b dargestellt. Die Zahlen e und $z_0 . z_{-1} z_{-2} \ldots z_{-p}$ heißen *Exponent* und *Mantisse*.

Am Computer kann eine Zahl dann durch die Ziffern des Exponenten und der Mantisse zur Basis 2 dargestellt werden. Die Anzahl dieser Ziffern

ist durch eine vorgegebene Zahl beschränkt. Die so am Computer verfügbaren Zahlen heißen *Maschinenzahlen*. Es gibt nur endlich viele Maschinenzahlen, alle Maschinenzahlen sind rationale Zahlen.

Beim Rechnen mit so dargestellten Zahlen gibt es im allgemeinen keine exakten Ergebnisse, sondern Rundungsfehler. Bei Rechenverfahren muss daher darauf geachtet werden, dass sich die Fehler nicht akkumulieren. Fehlerabschätzungen sind erforderlich.

Beispiel 22 : $p = 3, b = 10, \frac{c}{d} = \frac{2}{7}$

$$2000 = 285 \cdot 7 + 5$$

$$\frac{2}{7} = \frac{2000}{7 \cdot 10^3} = \frac{285 \cdot 7 + 5}{7 \cdot 10^3} = \underbrace{\frac{285}{10^3}}_{0.285} + \underbrace{\frac{5}{7} \cdot 10^{-3}}_{<10^{-3}}$$

Beispiel 23 : Die Zahl 0.1 (Dezimaldarstellung) auf der Tastatur wird vom Computer in Binärdarstellung $0.0001100110011001100\ldots$ umgewandelt und zum Beispiel als

$$1.10011001100110011001100110011001100110011001100\,E-4$$

gespeichert. Also ergibt schon die Eingabe von 0.1 einen Rundungsfehler!

Will man mit rationalen Zahlen am Computer exakt rechnen, kann man $\frac{a}{b}$ als Zahlenpaar (a,b) eingeben. Dann müssen für Zahlenpaare die Rechenoperationen

$$(a,b)+(c,d) := (ad+bc,bd) \quad \text{und} \quad (a,b)\cdot(c,d) := (ac,bd)$$

definiert werden.

§6. Der größte gemeinsame Teiler

Es seien a,b,c ganze Zahlen und $b \neq 0$, $c \neq 0$. Dann ist

$$\frac{a}{b} = \frac{a \cdot c}{b \cdot c} \in \mathbb{Q} \ .$$

Der Übergang von der Darstellung dieser rationalen Zahl durch das Zahlenpaar $(a \cdot c, b \cdot c)$ zu der durch (a,b) heißt *durch c kürzen*. Rechnet man mit rationalen Zahlen, dann ist es sehr empfehlenswert, alle auftretenden Brüche sofort durch möglichst große Zahlen zu kürzen. Dadurch werden die weiteren Rechnungen oft wesentlich vereinfacht. In diesem Abschnitt wird ein Verfahren zum „optimalen Kürzen“ angegeben.

Definition 24 : Es seien a und b ganze Zahlen mit $a \neq 0$ und $b \neq 0$. Dann heißt a *Teiler* von b (oder: a *teilt* b), wenn es eine ganze Zahl c gibt mit $b = ac$. Die Zahl b heißt dann ein *Vielfaches* von a.

Definition 25 : Der *größte gemeinsame Teiler* von zwei von Null verschiedenen ganzen Zahlen ist die größte ganze Zahl, die beide teilt. Das *kleinste gemeinsame Vielfache* von zwei von Null verschiedenen ganzen Zahlen ist die kleinste positive ganze Zahl, die Vielfaches von beiden ist.
Wir schreiben $ggT(a,b)$ bzw. $kgV(a,b)$ für den größten gemeinsamen Teiler bzw. das kleinste gemeinsame Vielfache zweier Zahlen a und b.

Satz 26 : *Es seien $a,b,c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ und $a \neq b$. Dann ist*

$$ggT(a,b) = ggT(|a|,|b|)$$

und

$$ggT(a,b) = ggT(a - c \cdot b, b) \ .$$

Beweis: Übung.

Satz 27 : (Euklidischer Algorithmus für ganze Zahlen)
Es seien $a,b \in \mathbb{Z}$, $a \neq 0$ und $b \neq 0$. Mit dem folgenden Verfahren kann der größte gemeinsame Teiler von a und b berechnet werden:

- *Ersetze a und b durch $|a|$ und $|b|$.*
- *Solange die zwei Zahlen verschieden sind, ersetze die größere durch die Differenz der größeren und der kleineren.*
- *Wenn die zwei Zahlen gleich sind, dann ist $ggT(a,b)$ gleich dieser Zahl.*

Ersetzt man mehrfaches Abziehen derselben Zahl durch eine Division mit Rest, dann hat dieses Verfahren die folgende Form:

- *Ersetze a und b durch $|a|$ und $|b|$.*
- *Solange keine der zwei Zahlen ein Teiler der anderen ist, ersetze die größere der zwei Zahlen durch ihren Rest nach Division durch die kleinere.*
- *Wenn eine der zwei Zahlen ein Teiler der anderen ist, dann ist sie der $ggT(a,b)$.*

Beweis: Nach Satz 26 können wir annehmen, dass a und b positive ganze Zahlen sind. Wenn sie verschieden sind, wird die größere der zwei Zahlen im nächsten Schritt durch eine kleiner positive ganze Zahl ersetzt. Also sind die zwei Zahlen nach höchstens $max(a,b) - 1$ Schritten gleich. Dabei ist $max(a,b)$ die größere der zwei Zahlen a und b. In jedem Schritt wird ein Zahlenpaar durch ein anderes ersetzt, nach Satz 26 aber so, dass die größten gemeinsamen Teiler der zwei Zahlenpaare gleich sind. Sobald man den größten gemeinsamen Teiler eines Zahlenpaares kennt (das ist spätestens dann der Fall, wenn die zwei Zahlen gleich sind), hat man $ggT(a,b)$ ermittelt.

Beispiel 28 : $ggT(301,215) = ggT(215,86) = ggT(129,86) =$
$= ggT(86,43) = ggT(43,43) = 43$

Im Euklidischen Algorithmus wird eine Strategie zur Lösung von Problemen verwendet, die wir schon bei linearen Gleichungssystemen kennengelernt haben: Wenn man die Lösung einer Aufgabe nicht sofort finden kann, ersetzt man diese Aufgabe durch eine einfachere, die aber dieselbe Lösungsmenge hat. Das wiederholt man solange, bis man bei einer Aufgabe landet, deren Lösung man kennt. Diese Lösung ist dann auch die Lösung der ursprünglichen Aufgabe.

Satz 29 : (Erweiterter Euklidischer Algorithmus)
Es seien $a,b \in \mathbb{Z}$, $a \neq 0$ und $b \neq 0$. Es gibt ganze Zahlen u,v so, dass $u \cdot a + v \cdot b = ggT(a,b)$ ist. Diese können mit dem folgenden Verfahren berechnet werden:

- *Setze $A := (A_1,A_2,A_3) := (|a|,1,0) \in \mathbb{Z}^3$ und*
  $B := (B_1,B_2,B_3) := (|b|,0,1) \in \mathbb{Z}^3$.
- *Solange B_1 die Zahl A_1 nicht teilt, berechne den ganzzahligen Quotienten m von A_1 und B_1 und setze $C := B$,*
  $B := A - m \cdot C := (A_1 - m \cdot C_1, A_2 - m \cdot C_2, A_3 - m \cdot C_3)$
  und dann $A := C$.
- *Wenn B_1 die Zahl A_1 teilt, dann ist $u := vz(a) \cdot B_2$ und $v := vz(b) \cdot B_3$*
  .

Beweis: Wenn zwei Zahlentripel S und T die Eigenschaft

$$S_1 = |a| \cdot S_2 + |b| \cdot S_3 \quad \text{bzw.} \quad T_1 = |a| \cdot T_2 + |b| \cdot T_3$$

haben, dann auch alle Tripel $S - m \cdot T$ mit $m \in \mathbb{Z}$. Die ersten zwei Tripel im Algorithmus haben diese Eigenschaft, daher auch alle anderen auftretenden Tripel. Für die ersten Komponenten der Tripel wird der euklidische Algorithmus durchgeführt, für das letzte Tripel B gilt daher $ggT(a,b) = |a| \cdot B_2 + |b| \cdot B_3 = vz(a) \cdot a \cdot B_2 + b \cdot vz(b) \cdot B_3$.

Satz 30 : (Berechnung von $kgV(a,b)$)
Es seien $a,b \in \mathbb{Z}$, $a \neq 0$ und $b \neq 0$. Dann ist

$$kgV(a,b) = \frac{|a|}{ggT(a,b)} \cdot |b| = \frac{|b|}{ggT(a,b)} \cdot |a| \ .$$

Beweis: Es ist klar, dass $\frac{|a|}{ggT(a,b)} \cdot |b| = \frac{|b|}{ggT(a,b)} \cdot |a|$ ein Vielfaches von a und von b ist. Sei z eine positive ganze Zahl, die Vielfaches von a und von b ist. Dann gibt es ganze Zahlen c,d mit $z = c \cdot a$ und $z = d \cdot b$. Nach Satz

29 gibt es Zahlen u, v so, dass $u \cdot a + v \cdot b = ggT(a,b)$ ist. Dann ist

$$z = \frac{u \cdot a + v \cdot b}{ggT(a,b)} \cdot z = \frac{u \cdot a}{ggT(a,b)} \cdot z + \frac{v \cdot b}{ggT(a,b)} \cdot z =$$
$$= \frac{u \cdot a \cdot d \cdot b}{ggT(a,b)} + \frac{v \cdot b \cdot c \cdot a}{ggT(a,b)} = \frac{a \cdot b}{ggT(a,b)} \cdot (u \cdot d + v \cdot c) =$$
$$= \frac{|a| \cdot |b|}{ggT(a,b)} \cdot vz(a \cdot b) \cdot (u \cdot d + v \cdot c)$$

ein Vielfaches von $\frac{|a|}{ggT(a,b)} \cdot |b|$.

Satz 31 : *(„Lösen einer ganzzahligen linearen Gleichung"). Es seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ und $b \in \mathbb{Z}$. Die größte ganze Zahl, die $a_1, \ldots, a_n$ teilt, heißt* größter gemeinsamer Teiler *von $a_1, \ldots, a_n$ und wird mit $ggT(a_1, \ldots, a_n)$ bezeichnet. Es ist*

$$ggT(a_1, \ldots, a_n) = ggT(a_1, ggT(a_2, ggT(a_3, ggT(\ldots, a_n) \ldots)) \ ,$$

also kann der größte gemeinsame Teiler von mehreren Zahlen durch sukzessives Berechnen des größten gemeinsamen Teilers von je zwei Zahlen berechnet werden.
Es gibt genau dann ein n-Tupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ mit

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n = b \ ,$$

wenn b ein Vielfaches von $g := ggT(a_1, \ldots, a_n)$ ist. In diesem Fall kann ein solches n-Tupel wie folgt berechnet werden:

- *Berechne mit Satz 29 Zahlen $u_1, \ldots, u_n$ so, dass $a_1 \cdot u_1 + \ldots + a_n \cdot u_n = g$ ist.*
- *Setze $x_i := u_i \cdot \frac{b}{g}$, $1 \leq i \leq n$.*

Beweis: Für jedes n-Tupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ wird $a_1 \cdot x_1 + \ldots + a_n \cdot x_n$ von g geteilt. Also ist die Bedingung, dass b ein Vielfaches von g ist, notwendig für die Existenz einer Lösung. Wenn diese Bedingung erfüllt ist, ist leicht nachzuprüfen, dass $(u_1 \cdot \frac{b}{g}, \ldots, u_n \cdot \frac{b}{g})$ eine Lösung ist.

Satz 32 : *(Partialbruchzerlegung von rationalen Zahlen) Es seien a, b, c positive ganze Zahlen so, dass $ggT(a,b) = 1$ und $c < a \cdot b$ ist. Dann gibt es ganze Zahlen u und v so, dass*

$$\frac{c}{a \cdot b} = \frac{v}{a} + \frac{u}{b}$$

ist. Die Zahlen u und v können wie folgt berechnet werden:

- *Berechne mit dem erweiterten Euklidischen Algorithmus ganze Zahlen s, t so, dass $s \cdot a + t \cdot b = 1$ ist.*
- *Dann ist $u = c \cdot s$ und $v = c \cdot t$.*

Beweis: Es ist

$$u \cdot a + v \cdot b = c$$

und somit

$$\frac{c}{a \cdot b} = \frac{u \cdot a + v \cdot b}{a \cdot b} = \frac{u}{b} + \frac{v}{a} .$$

Beispiel 33 : Die Partialbruchzerlegung von rationalen Zahlen kann zur Berechnung gewisser Summen verwendet werden. Zum Beispiel ist für alle positiven ganzen Zahlen i

$$\frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1} ,$$

daher ist

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \sum_{i=1}^{n} (\frac{1}{i} - \frac{1}{i+1}) = \sum_{i=1}^{n} \frac{1}{i} - \sum_{i=2}^{n+1} \frac{1}{i} = 1 - \frac{1}{n+1} .$$

§7. Primzahlen

Definition 34 : Eine ganze Zahl $p \in \mathbb{Z}$ heißt *Primzahl*, wenn $p \neq 0, p \neq 1, p \neq -1$ und $\{1, -1, p, -p\}$ die Menge der Teiler von p ist.

Satz 35 : *(„Lemma von Euklid") Es seien p eine Primzahl und $a, b \in \mathbb{Z}$. Wenn p die Zahl $a \cdot b$ teilt, dann teilt p auch a oder b.*

Beweis: Es gibt eine ganze Zahl c so, dass $c \cdot p = a \cdot b$ ist . Wenn p die Zahl a nicht teilt, dann ist $ggT(a, p) = 1$. Daher gibt es ganze Zahlen u und v so, dass $1 = u \cdot a + v \cdot p$ ist. Dann ist

$$b = b \cdot u \cdot a + b \cdot v \cdot p = u \cdot c \cdot p + b \cdot v \cdot p = (u \cdot c + b \cdot v) \cdot p ,$$

somit ist p ein Teiler von b.

Satz 36 : (Zerlegung in Primfaktoren)
Jede ganze Zahl , die größer als 1 *ist, kann als Produkt von positiven Primzahlen geschrieben werden. Diese Primzahlen heißen* Primfaktoren *der Zahl und sind bis auf die Reihenfolge eindeutig bestimmt.*

Beweis: Es sei a eine ganze Zahl, die größer als 1 ist. Wir beweisen die erste Aussage durch Induktion über a.
Wenn $a = 2$ ist, dann ist a eine Primzahl.
Wenn $a > 2$ ist, dann ist a entweder eine Primzahl oder es gibt ganze Zahlen b, c mit $0 < b, c < a$ so, dass $a = b \cdot c$ ist . Nach Induktionsannahme sind b und c Produkte von positiven Primzahlen, also auch a.

Wir beweisen noch die Eindeutigkeit der Primfaktorzerlegung. Es seien $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ und $a = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$ zwei Zerlegungen von a in Primfaktoren. Wir beweisen durch Induktion über $max(k,\ell)$, dass sie bis auf die Reihenfolge gleich sind. Weil p_1 das Produkt $q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$ teilt, gibt es nach Satz 35 eine Zahl $j \in \{1,\ldots,\ell\}$ so, dass $p_1 = q_j$. Weil $\mathbb{Z}$ ein Integritätsbereich ist, folgt

$$p_2 \cdot \ldots \cdot p_k = \prod_{1 \le i \le \ell, i \neq j} q_i \ ,$$

und die Behauptung folgt aus der Induktionsannahme.

Die Berechnung der Primfaktoren einer Zahl ist sehr aufwändig. Rechenverfahren, in denen Zahlen in Primfaktoren zerlegt werden müssen, sollten nach Möglichkeit vermieden werden.

Satz 37 : *Es gibt unendlich viele positive Primzahlen.*

Beweis: Wenn es nur endlich viele positive Primzahlen gäbe, dann wäre ihr Produkt q eine ganze Zahl und $q+1$ wäre größer als jede Primzahl. Insbesondere wäre $q+1$ keine Primzahl. Nach Satz 36 gibt es eine Primzahl p, die $q+1$ teilt. Da p auch q teilt, würde p dann auch 1 teilen, Widerspruch.

Satz 38 : (Berechnung von ggT und kgV zweier Zahlen, deren Primfaktoren bekannt sind).
Es seien $p_1,\ldots,p_n$ paarweise verschiedene positive Primzahlen und $e_1,\ldots,e_n,f_1,\ldots,f_n$ natürliche Zahlen. Dann ist

$$ggT(\prod_{i=1}^{n} p_i^{e_i}, \prod_{i=1}^{n} p_i^{f_i}) = \prod_{i=1}^{n} p_i^{min(e_i,f_i)}$$

und

$$kgV(\prod_{i=1}^{n} p_i^{e_i}, \prod_{i=1}^{n} p_i^{f_i}) = \prod_{i=1}^{n} p_i^{max(e_i,f_i)} \ .$$

Beweis: Es sei $g := \prod_{i=1}^{n} p_i^{min(e_i,f_i)}$. Es ist klar, dass g die Zahlen $a := \prod_{i=1}^{n} p_i^{e_i}$ und $b := \prod_{i=1}^{n} p_i^{f_i}$ teilt. Da nach Satz 36 die Zerlegung dieser zwei Zahlen in Primfaktoren eindeutig ist, kann ihr größter gemeinsamer Teiler keine anderen Primfaktoren als $p_1,\ldots,p_n$ enthalten. Aus demselben Grund darf p_i in $ggT(a,b)$ nur $min(e_i,f_i)$-mal auftreten. Daher ist $g = ggT(a,b)$. Die Behauptung für $kgV(a,b)$ folgt nun aus Satz 30.

§8. Restklassen

Definition 39 : Es sei n eine ganze Zahl mit $n > 1$. Für $a \in \mathbb{Z}$ heißt die Menge

$$\bar{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\}$$

Restklasse von a modulo n. Die Menge

$$\{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

wird mit

$$\mathbb{Z}_n \quad \text{oder} \quad \mathbb{Z}/n\mathbb{Z}$$

bezeichnet (Sprechweise: $\mathbb{Z}$ modulo n). Zwei ganze Zahlen a und b sind *zueinander kongruent modulo n* (Schreibweise: $a \equiv b \mod (n)$), wenn sie in derselben Restklasse modulo n liegen, das heißt: ihre Reste nach Division durch n sind gleich.

Satz 40 : *Es seien n eine ganze Zahl mit $n > 1$ und a, b ganze Zahlen. Die Restklassen $\bar{a}$ und $\bar{b}$ modulo n sind genau dann gleich, wenn $b - a$ ein Vielfaches von n ist.*

Beweis: Übung.

Wir wollen auf $\mathbb{Z}_n$ Rechenoperationen so definieren, dass $\mathbb{Z}_n$ ein kommutativer Ring wird.

Satz 41 : *Es sei n eine ganze Zahl mit $n > 1$. Die Funktionen*

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n , \quad (\bar{a}, \bar{b}) \longmapsto \bar{a} + \bar{b} := \overline{a+b}$$

und

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n , \quad (\bar{a}, \bar{b}) \longmapsto \bar{a} \cdot \bar{b} := \overline{ab}$$

sind wohldefiniert. Mit diesen Rechenoperationen ist $\mathbb{Z}_n$ ein (endlicher) kommutativer Ring (mit n Elementen). Er heißt Restklassenring $\mathbb{Z}_n$. *Das Nullelement bzw. Einselement von $\mathbb{Z}_n$ ist $\bar{0}$ bzw. $\bar{1}$.*

Beweis: Wir zeigen zuerst, dass $+$ und $\cdot$ wohldefiniert sind.
Es seien $a, c, b, d \in \mathbb{Z}$ so, dass $\bar{a} = \bar{c}$ und $\bar{b} = \bar{d}$ ist. Dann sind $a - c$ und $b - d$ Vielfache von n. Wegen

$$(a+b) - (c+d) = (a-c) + (b-d)$$

ist $\overline{a+b} = \overline{c+d}$. Wegen

$$ab - cd = a(b-d) + (a-c)d$$

ist $ab - cd$ ein Vielfaches von n, also $\overline{ab} = \overline{cd}$.
Nun kann leicht nachgeprüft werden, dass $+$ und $\cdot$ die Rechenregeln eines kommutativen Ringes erfüllen.

Beispiel 42 : Die Wohldefiniertheit von $+$ und $\cdot$ in $\mathbb{Z}_n$ bedeutet: aus

$$a \equiv c \mod (n),\ b \equiv d \mod (n)$$

folgt

$$a+b \equiv c+d \mod (n) \quad \text{und} \quad a \cdot b \equiv c \cdot d \mod (n)\ .$$

Am Computer können die Elemente von $\mathbb{Z}_n$ durch die Zahlen

$$0, 1, \ldots, n-1$$

dargestellt werden. Dann wird für $0 \leq a, b < n$ die Summe $\bar{a} + \bar{b}$ bzw. das Produkt $\bar{a} \cdot \bar{b}$ durch den Rest von $a+b$ bzw. $a \cdot b$ nach Division durch n dargestellt.
Eine andere Möglichkeit zur Darstellung der Restklassen modulo n ist die durch die Zahlen

$$-[\frac{n}{2}], -[\frac{n}{2}]+1, \ldots, [\frac{n-1}{2}]\ ,$$

wobei $[\frac{n}{2}]$ die größte ganze Zahl bezeichnet, die kleiner oder gleich $\frac{n}{2}$ ist.

In der Programmiersprache C bedeutet das Rechnen im Datentyp *unsigned int* das Rechnen im Restklassenring $\mathbb{Z}_n$ mit $n = 2^{32}$. Als Summe von $2^{32} - 1$ und 1 wird daher 0 ausgegeben.

Satz 43 : *Es seien $a \in \mathbb{N}$ und $a_n, a_{n-1}, \ldots, a_0$ die Dezimalziffern von a. Die Zahl* 9 *bzw.* 11 *teilt a genau dann, wenn* 9 *bzw.* 11 *die* Ziffernsumme *bzw.* alternierende Ziffernsumme

$$\sum_{i=0}^{n} a_i \quad \textit{bzw.} \quad \sum_{i=0}^{n} (-1)^i a_i$$

von a teilt.

Beweis: Die Zahl 9 bzw. 11 teilt $a = \sum_{i=0}^{n} a_i 10^i$ genau dann, wenn die Restklasse

$$\bar{a} = \overline{\sum_{i=0}^{n} a_i 10^i} = \sum_{i=0}^{n} \overline{a_i}\,\overline{10}^i$$

gleich $\bar{0}$ ist. Die Restklasse von 10 modulo 9 bzw. 11 ist $\bar{1}$ bzw. $\overline{-1}$. Daher ist die Restklasse von a modulo 9 bzw. 11 gleich der Restklasse der Ziffernsumme bzw. alternierenden Ziffernsumme von a.

Dieser Satz wurde früher zum Überprüfen der Richtigkeit (bis auf Vielfache von 9 bzw. 11) von Rechnungen mit ganzen Zahlen verwendet („Neunerprobe“ bzw. „Elferprobe“).

Definition 44 : Ein Element r eines kommutativen Ringes R mit Einselement 1 ist *invertierbar*, wenn es ein Element $s \in R$ mit

$$sr = 1$$

gibt. Das Element s heißt dann zu r *inverses Element* und wird mit r^{-1} bezeichnet.

Satz 45 : *Seien R ein kommutativer Ring und $r \in R$. Dann gibt es in R höchstens ein zu r inverses Element.*

Beweis: Es seien $s,t \in R$ mit $rs = 1 = rt$. Dann ist

$$t = t \cdot 1 = t \cdot (r \cdot s) = (t \cdot r) \cdot s = 1 \cdot s = s\,.$$

Satz 46 : *Es seien $a \neq 0$ und $n \geq 2$ ganze Zahlen.*

(1) *Die Restklasse $\bar{a} \in \mathbb{Z}_n$ ist genau dann invertierbar, wenn $ggT(a,n) = 1$ ist. In diesem Fall wird $\bar{a}^{-1}$ wie folgt berechnet:*
   - *Berechne mit dem erweiterten Euklidischen Algorithmus Zahlen $u,v \in \mathbb{Z}$ so, dass $u \cdot a + v \cdot n = 1$ ist.*
   - *Dann ist $\bar{a}^{-1} = \bar{u}$.*

(2) *$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis:

(1) Wenn $ggT(a,n) = 1$ und $u \cdot a + v \cdot n = 1$ ist, dann ist

$$\bar{1} = \bar{u} \cdot \bar{a} + \bar{v} \cdot \bar{n} = \bar{u} \cdot \bar{a}\,.$$

Wenn $\bar{a}$ invertierbar ist, dann gibt es eine ganze Zahl b so, dass n die Zahl $1 - a \cdot b$ teilt. Daher teilt $ggT(a,n)$ sowohl a als auch $1 - a \cdot b$, also muss $ggT(a,n)$ gleich 1 sein.

(2) folgt aus (1).

Ist p eine Primzahl, dann ist $\mathbb{Z}_p$ ein Körper, also kann mit den Restklassen in $\mathbb{Z}_p$ wie mit rationalen oder reellen Zahlen gerechnet werden. Insbesondere können Systeme linearer Gleichungen mit Gauß- Elimination gelöst werden.
Für eine positive ganze Zahl n ist $\mathbb{Z}_p^n$ (die Menge aller n-Tupel in $\mathbb{Z}_p$) ein n-dimensionaler Vektorraum über dem Körper $\mathbb{Z}_p$. Dieser Vektorraum

enthält p^n Elemente. Ein Unterrvektorraum dieses Vektorraums heißt *linearer Code*. Wird eine Nachricht als n-Tupel in $\mathbb{Z}_p^n$ dargestellt und wurde vereinbart, dass dieses Element eines linearen Codes $C \leq \mathbb{Z}_p^n$ ist, dann kann ein Empfänger überprüfen, ob die Nachricht bei der Übertragung verändert wurde: er prüft nach, ob das erhaltene n-Tupel ein Element von C ist. Wenn nicht, wurde die Nachricht verändert.

Definition 47 : Für natürliche Zahlen k und n mit $0 \leq k \leq n$ sei

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

der *Binomialkoeffizient n über k*. Dabei ist $0! := 1$.

Satz 48 : *Für* $0 \leq k < n$ *ist*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

„Pascal-Dreieck“ :

$$\begin{array}{ccccccccc} & & & & 1 & & & & n=0 \\ & & & 1 & & 1 & & & n=1 \\ & & 1 & & 2 & & 1 & & n=2 \\ & 1 & & 3 & & 3 & & 1 & n=3 \\ 1 & & 4 & & 6 & & 4 & & 1 \quad n=4 \\ 1 & & 5 & & 10 & & 10 & & 5 \quad 1 \quad n=5 \\ \multicolumn{9}{c}{\ldots\ldots\ldots\ldots\ldots\ldots} & \ldots\ldots \end{array}$$

Beweis:

$$\begin{aligned} \frac{n!}{k!(n-k)!} + \frac{n!}{(n-(k+1))!(k+1)!} &= \\ &= \frac{n!(k+1)+n!(n-k)}{(n-(k+1))!(k+1)!} = \\ &= \frac{(n+1)!}{(n-(k+1))!(k+1)!} \end{aligned}$$

Satz 49 : *Sind* a, b *Elemente eines kommutativen Ringes (zum Beispiel ganze Zahlen) und ist* n *eine natürliche Zahl, dann ist*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Beweis: Induktion über n und Satz 48.

Satz 50 : *Es seien $a, b \in \mathbb{Z}$ und p eine positive Primzahl.*

(1) *In $\mathbb{Z}_p$ ist*

$$(\bar{a}+\bar{b})^p = \bar{a}^p + \bar{b}^p \,.$$

(2) *(„Kleiner Satz von Fermat“) Es ist $\bar{a}^p = \bar{a} \in \mathbb{Z}_p$.*
Wenn $\bar{a} \neq 0$ ist, dann ist

$$\bar{a}^{p-1} = \bar{1} \quad \textit{und} \quad \bar{a}^{p-2} = \bar{a}^{-1} \,.$$

Insbesondere: Für alle ganzen Zahlen a ist der Rest von a^p nach Division durch p derselbe wie der von a.

Beweis: (1) Für $1 < k < p$ wird der Binomialkoeffizient

$$\binom{p}{k} = p \cdot \frac{(p-1)!}{k!(p-k)!}$$

von p geteilt. Daher ist

$$(\bar{a}+\bar{b})^p = \sum_{k=0}^{p} \overline{\binom{p}{k}} \bar{a}^k \bar{b}^{p-k} = \bar{a}^p + \bar{b}^p \,.$$

(2) Die Aussage $\bar{a}^p = \bar{a}$ beweisen wir durch Induktion über a (o.E.d.A. ist $a \geq 0$):
Für $a = 0$ ist nichts zu zeigen.
Sei $a > 0$. Nach Induktionsannahme ist dann

$$\bar{a}^p = (\overline{(a-1)} + \bar{1})^p = \overline{(a-1)}^p + \bar{1}^p = \overline{a-1} + \bar{1} = \bar{a} \,.$$

Beispiel 51 : Es seien p eine Primzahl, a eine ganze Zahl, die nicht von p geteilt wird und e eine „große“ natürliche Zahl. Mit Satz 50 kann der Rest von a^e nach Division durch p „schnell“ berechnet werden. Dividiere dazu e mit Rest durch $p-1$:

$$e = m \cdot (p-1) + r \,.$$

Dann ist

$$\overline{a^e} = (\bar{a}^{p-1})^m \bar{a}^r = \bar{a}^r \in \mathbb{Z}_p \,.$$

Sei zum Beispiel $p = 13$, $a = 7$ und $e = 10000$.
Dann ist $10000 = 833 \cdot 12 + 4$, also

$$\overline{7^{10000}} = \left(\bar{7}^{12}\right)^{833} \cdot \bar{7}^4 = \bar{7}^4 = \overline{49}^2 = \overline{-3}^2 = \bar{9} \in \mathbb{Z}_{13} \,.$$

Daher ist der gesuchte Rest gleich 9.

§9. Das RSA-Verfahren

Das 1978 von R. Rivest, A. Shamir und L. Adleman entwickelte RSA-Verfahren ermöglicht es, dass der Schlüssel zum Verschlüsseln von Nachrichten öffentlich bekanntgegeben, die verschlüsselte Nachricht aber trotzdem nur vom beabsichtigten Empfänger entschlüsselt werden kann. Wie funktioniert das?

- Der Empfänger gibt zwei sehr große natürliche Zahlen n und e öffentlich bekannt.
- Der Sender will dem Empfänger eine natürliche Zahl a, die kleiner als n ist, verschlüsselt mitteilen.
- Dazu berechnet er den Rest b von a^e nach Division durch n.
- Der Empfänger erhält die Zahl b und macht fast dasselbe wie der Sender: er potenziert und berechnet dann den Rest nach Division durch n. Der Exponent der Potenz ist aber nicht e, sondern eine geeignete andere natürliche Zahl d. So erhält er die ursprüngliche Nachricht a.

Das Zahlenpaar (e,n) heißt *Chiffrierschlüssel* und wird öffentlich bekannt gegeben. Das Paar (d,n) heißt *Dechiffrierschlüssel*, die Zahl d ist nur dem Empfänger bekannt.

Die Zahlen e, n und d werden vom Empfänger so gewählt bzw. berechnet:

- Der Empfänger wählt zwei sehr große, verschiedene Primzahlen p und q und berechnet die Produkte $n := p \cdot q$ und $m := (p-1)\cdot(q-1)$.
- Dann wählt er e so, dass
$$ggT(e,m) = 1$$
ist.
- Schließlich berechnet er ganze Zahlen c und d so, dass
$$m \cdot c + e \cdot d = 1$$
ist.

Wir werden im Satz 52 zeigen, dass für alle natürlichen Zahlen a, die kleiner als n sind, der Rest von
$$(a^e)^d = a^{e\cdot d} = a^{1-m\cdot c} = a \cdot (a^m)^{-c} = a \cdot (a^{(p-1)\cdot(q-1)})^{-c}$$
nach Division durch $n = p \cdot q$ gleich a ist.

Die Zahl n ist bekannt. Warum kann nicht jede/r ihre Primfaktoren p und q berechnen (und dann wie oben auch die Zahl d berechnen und die Nachricht entschlüsseln)? Die Berechnung der Primfaktoren ist auch für sehr große Zahlen theoretisch immer möglich, praktisch aber auch von den leistungsfähigsten Computern nicht in vernünftiger Zeit durchführbar. Der von 1991 bis 2007 laufende Wettbewerb *RSA Factoring Challenge* bot Preisgelder (bis zu 200.000 USD) für die Berechnung der Primfaktoren von speziellen natürlichen Zahlen mit 100 bis 617 Dezimalstellen. Von diesen sogenannten RSA-Zahlen konnten bisher nur die Primfaktoren der Zahlen mit

höchstens 232 Dezimalstellen berechnet werden. Die Berechnung für die Zahl RSA-768 mit 768 Binär- bzw. 232 Dezimalziffern gelang unter Verwendung von mehreren hundert Computern in rund zweieinhalb Jahren. Die Primfaktoren der Zahl RSA-1024

135066410865995223349603216278805969938881475605667027524485
143851526510604859533833940287150571909441798207282164471551
373680419703964191743046496589274256239341020864383202110372
958725762358509643110564073501508187510676594629205563685529
475213500852879416377328533906109750544334999811150056977236
890927563

mit 1024 Binärziffern bzw. 309 Dezimalziffern können mit heutigen Methoden nicht in diesem Jahrhundert berechnet werden.

Satz 52 : *Es seien p,q,d,e,m wie oben. Für alle natürlichen Zahlen a, die kleiner als n sind, ist der Rest von*

$$(a^e)^d = a^{e\cdot d} = a^{1-m\cdot c} = a\cdot(a^m)^{-c} = a\cdot(a^{(p-1)\cdot(q-1)})^{-c}$$

nach Division durch $n = p\cdot q$ gleich a .

Beweis: In $\mathbb{Z}_p$ ist

$$\bar{a}^{e\cdot d} = \bar{a}^{1-(p-1)(q-1)\cdot c} =$$
$$= \left.\begin{cases} \bar{a}\cdot(\underbrace{\bar{a}^{(p-1)}}_{=1\in\mathbb{Z}_p})^{-c\cdot(q-1)} = \bar{a} & \text{, wenn } \bar{a}\neq\bar{0} \text{ ist} \\ \bar{a}\cdot\bar{a}^{-(p-1)(q-1)\cdot c} = \bar{0} & \text{, wenn } \bar{a}=\bar{0} \text{ ist} \end{cases}\right\} = \bar{a}$$

und analog in $\mathbb{Z}_q$

$$\bar{a}^{e\cdot d} = \bar{a}^{1-(p-1)(q-1)\cdot c} =$$
$$= \left.\begin{cases} \bar{a}\cdot(\underbrace{\bar{a}^{(q-1)}}_{=1\in\mathbb{Z}_q})^{-c\cdot(p-1)} = \bar{a} & \text{, wenn } \bar{a}\neq\bar{0} \text{ ist} \\ \bar{a}\cdot\bar{a}^{-(p-1)(q-1)\cdot c} = \bar{0} & \text{, wenn } \bar{a}=\bar{0} \text{ ist} \end{cases}\right\} = \bar{a}\,.$$

Dies bedeutet, dass $a^{e\cdot d}-a$ sowohl von p als auch von q geteilt wird. Es gibt also ganze Zahlen s,t mit

$$s\cdot p = t\cdot q = a^{e\cdot d}-a\,.$$

Weil p und q verschieden sind und die Primzahl p das Produkt $t\cdot q$ teilt, muss p ein Teiler von t sein (Lemma von Euklid). Somit ist

$$t\cdot q = (p\cdot u)\cdot q = n\cdot u$$

für eine ganze Zahl u. Also teilt n die Zahl $t \cdot q = a^{e \cdot d} - a$ und

$$\bar{a}^{e \cdot d} = \bar{a} \text{ in } \mathbb{Z}_n .$$

KAPITEL 2

Polynomfunktionen und Polynome in einer Variablen

§1. Polynomfunktionen

In diesem Abschnitt sei R ein kommutativer Ring (zum Beispiel $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \ldots$).

Definition 53 : Seien $n \in \mathbb{N}$ und $a_0, a_1, \ldots, a_n \in R$. Dann ist die Funktion

$$f : R \to R, z \mapsto a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = \sum_{i=0}^{n} a_i z^i,$$

eine *Polynomfunktion* von R nach R. Die Elemente $a_0, \ldots, a_n$ heißen *Koeffizienten von* f. Für $i \in \mathbb{N}$ heißt die Polynomfunktion $R \to R, z \mapsto z^i$, die *i-te Potenzfunktion*.

Mit Polynomfunktionen sind mehrere grundlegende Aufgaben verbunden:

- *Auswerten* einer Polynomfunktion f mit Koeffizienten $a_0, \ldots, a_n$ in einem Element r von R: Berechne das Bild

  $$f(r) = \sum_{i=0}^{n} a_i r^i$$

  von r unter der Polynomfunktion f. Es ist klar, dass dieses Element von R immer durch Ausführen von Additionen und Multiplikationen in R berechnet werden kann. Darin liegt die „rechnerische Bedeutung“ der Polynomfunktionen.
- *Interpolation* durch eine Polynomfunktion: Gegeben sind eine endliche Teilmenge E von R und eine Funktion $g : E \longrightarrow R$. Gesucht ist eine Polynomfunktion von R nach R, deren Einschränkung auf E gleich g ist (siehe §5).
- *Überprüfe die Gleichheit* von zwei Polynomfunktionen: Zwei Polynomfunktionen seien durch ihre Koeffizienten gegeben. Wie kann man feststellen, ob diese zwei Funktionen gleich sind? Die Antwort ist nicht so leicht: zum Beispiel sind die Polynomfunktionen

  $$f : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \ , \ z \longmapsto z \ , \text{und } g : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \ , \ z \longmapsto z^2 \ ,$$

  gleich (siehe §4).

- *Berechnen der Nullstellen* einer Polynomfunktion f: Finde alle Elemente $r \in R$ mit der Eigenschaft, dass $f(r) = 0$ ist. Einfacher zu beantwortende Fragen sind: Gibt es solche Elemente? Wenn ja, wieviele? (Siehe §4 und §9).

Satz 54 : *Es seien $r \in R$ und f eine Polynomfunktion mit Koeffizienten $a_0, \ldots, a_n \in R$. Mit dem folgenden Verfahren kann $f(r)$ mit höchstens n Additionen und höchstens n Multiplikationen in R berechnet werden:*

- *Setze $i := n$ und $w := a_n$.*
- *Solange $i \neq 0$ ist, ersetze i durch $i-1$ und dann w durch $w \cdot r + a_i$.*
- *Wenn $i = 0$ ist, dann ist $f(r) = w$.*

Beweis:

$$\sum_{i=0}^{n} a_i r^i = (\ldots((a_n r + a_{n-1})r + a_{n-2})r + \ldots + a_1)r + a_0 \ .$$

§2. Moduln und Algebren

In diesem Abschnitt sei R ein Ring mit Einselement 1 (zum Beispiel $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{R}^{n\times n}, \ldots$).

Definition 55 : Es seien M eine Menge und

$$+ : M \times M \to M \ , \ (a,b) \longmapsto a+b \ , \quad \cdot : R \times M \to M \ , \ (r,b) \longmapsto r \cdot b \ ,$$

Funktionen. Das Tripel $(M, +, \cdot)$ ist ein *Modul über R* oder *R-Modul*, wenn die folgenden 3 Bedingungen erfüllt sind:

(1) $(M, +)$ ist eine abelsche Gruppe.
(2) Für alle $r, s \in R$ und für alle $a, b \in M$ ist $r \cdot (a+b) = (r \cdot a) + (r \cdot b)$ und $(r+s) \cdot a = (r \cdot a) + (s \cdot a)$.
(3) Für alle $r, s \in R$ und für alle $a \in M$ ist $(rs) \cdot a = r \cdot (s \cdot a)$ und $1 \cdot a = a$.

Ist $(M, +, \cdot)$ ein Modul, dann heißen die Funktionen $+$ „Addition“ und $\cdot$ „Skalarmultiplikation“. Statt $(M, +, \cdot)$ wird oft nur M geschrieben. Das neutrale Element von $(M, +)$ wird mit 0_M oder 0 bezeichnet.

Beispiel 56 : Wenn R ein Körper ist, dann stimmen die Begriffe R-Modul und R-Vektorraum überein.

Beispiel 57 : Es sei $0 \neq n \in \mathbb{N}$. Dann ist R^n mit

$$+ : R^n \times R^n \to R^n \ , \ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \longmapsto (a_1 + b_1, \ldots, a_n + b_n)$$

und

$$\cdot : R \times R^n \to R^n \ , \ (r,(a_1,\ldots,a_n)) \longmapsto (ra_1,\ldots,ra_n)$$

ein R-Modul.

Beispiel 58 : $R^{n\times 1}$ mit der Addition von Spalten und

$$R^{n\times n} \times R^{n\times 1} \to R^{n\times 1} \ , \ (A,x) \mapsto A \cdot x$$

ist ein $R^{n\times n}$-Modul.

Definition 59 : Es sei A ein Ring und ein R-Modul. Dann ist A eine *R-Algebra*, wenn für alle $r \in R$ und alle $a,b \in A$

$$r \cdot (ab) = a(r \cdot b) = (r \cdot a)b$$

ist. Eine Algebra ist *kommutativ*, wenn sie als Ring kommutativ ist.

Beispiel 60 : $\mathbb{R}$ ist eine $\mathbb{Q}$-Algebra (und auch $\mathbb{R}$-Algebra), $\mathbb{C}$ ist eine $\mathbb{R}$-Algebra, $\mathbb{Z}_n$ ist eine $\mathbb{Z}$-Algebra.

Beispiel 61 : Die Menge $R^{n\times n}$ aller $n \times n$-Matrizen mit Koeffizienten in einem kommutativen Ring R ist mit Addition, Skalarmultiplikation und Multiplikation von Matrizen eine R-Algebra. Diese ist nur dann kommutativ, wenn $n = 1$ ist.

Beispiel 62 : Jeder Ring R kann als Modul über R aufgefasst werden, dabei ist die Skalarmultiplikation die Multiplikation in R. Jeder kommutative Ring R ist eine R-Algebra.

Satz 63 : *Es seien X eine Menge, R ein kommutativer Ring und $A := \mathcal{F}(X,R)$ die Menge aller Funktionen von X nach R. Für $f,g \in A$, $x \in X$ und $r \in R$ sei*

$$(fg)(x) := f(x)g(x) \ , \ (f+g)(x) := f(x)+g(x) \text{ und } (r \cdot f)(x) := r(f(x)) \ .$$

Mit den Rechenoperationen

$$A \times A \longrightarrow A \ , \ (f,g) \longmapsto f+g \ ,$$
$$A \times A \longrightarrow A \ , \ (f,g) \longmapsto fg \ ,$$
$$R \times A \longrightarrow A \ , \ (r,g) \longmapsto r \cdot g \ ,$$

*(*punktweise Addition, Multiplikation, Skalarmultiplikation*) ist A eine kommutative R-Algebra.*

Beweis: Übung.

Definition 64 :

(1) Es seien M ein R-Modul und N eine nicht-leere Teilmenge von M. Dann ist N ein *Untermodul* von M, wenn für alle $a,b \in N$ und alle $r \in R$ auch
$$a+b \quad \text{und} \quad r \cdot a$$
in N enthalten sind.

(2) Es sei S eine nicht-leere Teilmenge von R. Dann ist S ein *Unterring* von R, wenn $1 \in S$ ist und für alle $a,b \in S$ auch die Elemente
$$a+b\ ,\ ab \quad \text{und} \quad -a$$
in S enthalten sind.

(3) Es seien A eine R-Algebra und B eine nicht-leere Teilmenge von A. Dann ist B eine *Unteralgebra* von A, wenn $1 \in B$ ist und für alle $a,b \in B,\ r \in R$ auch die Elemente
$$a+b\ ,\ ab \quad \text{und} \quad r \cdot a$$
in B enthalten sind.

Ein Unterring bzw. Untermodul bzw. eine Unteralgebra ist mit den auf diese Teilmenge eingeschränkten Rechenoperationen selbst ein Ring bzw. Modul bzw. eine Algebra.

Beispiel 65 : Die Menge $\{a(1,2)+b(-3,4) \mid a,b \in \mathbb{Z}\}$ ist ein $\mathbb{Z}$-Untermodul von $\mathbb{Z}^2$.

Beispiel 66 : Die Menge $\mathcal{C}^1(\mathbb{R}) := \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ differenzierbar}\}$ ist eine $\mathbb{R}$-Unteralgebra von $\mathcal{F}(\mathbb{R},\mathbb{R})$ (siehe Analysis 1).

Satz 67 : *Die Menge der Polynomfunktionen von einem kommutativen Ring R nach R ist eine R-Unteralgebra der Algebra $\mathcal{F}(R,R)$ aller Funktionen von R nach R.*

Beweis: Seien f und g Polynomfunktionen und $a_0,\dots,a_n$ bzw. $b_0,\dots,b_m$ ihre Koeffizienten. Für alle $z \in R$ ist dann $f(z) = \sum_{i=0}^{n} a_i z^i$ und $g(z) = \sum_{j=1}^{m} b_j z^j$. Daher ist für alle $z \in R$
$$\begin{aligned}(f \cdot g)(z) = f(z)g(z) &= \left(\sum_{i=0}^{n} a_i z^i\right)\left(\sum_{j=0}^{m} b_j z^j\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j z^{i+j} = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) z^k\,,\end{aligned}$$
also $f \cdot g$ eine Polynomfunktion. Die anderen Eigenschaften einer Unteralgebra sind leicht nachzuprüfen.

Definition 68 : Es seien M ein Modul über R und $(v_i)_{i\in I}$ eine Familie von Elementen in M, wobei I eine beliebige Indexmenge ist.
Eine Familie $(r_i)_{i\in I}$ von Elementen in R heißt *Koeffizienten-Familie*, wenn $r_i \neq 0$ für nur endlich viele $i \in I$ ist.
Ein Element $a \in M$ heißt eine *Linearkombination* von $(v_i)_{i\in I}$, wenn es eine Koeffizienten-Familie $(r_i)_{i\in I}$ gibt, sodass

$$a = \sum_{i\in I} r_i v_i$$

ist. Dabei ist im Fall einer unendlichen Indexmenge I die obige Summe als die endliche Summe über alle Indizes $i \in I$ mit $r_i \neq 0$ zu verstehen.

Satz 69 : *Es seien M ein Modul über R und $(v_i)_{i\in I}$ eine Familie in M. Dann ist die Menge aller Linearkombinationen von $(v_i)_{i\in I}$ der kleinste Untermodul von M, der alle Elemente v_i, $i \in I$, enthält. Er heißt der* von v_i, $i \in I$, erzeugte Untermodul von M *und wird mit*

$$_R\langle v_i \mid i \in I\rangle \qquad \textit{oder} \qquad \sum_{i\in I} Rv_i$$

bezeichnet.

Beweis: Übung.

Beispiel 70 : Jede Polynomfunktion ist eine Linearkombination von Potenzfunktionen. Der von der Familie aller Potenzfunktionen erzeugte Untermodul von $\mathcal{F}(R,R)$ ist der R-Modul aller Polynomfunktionen von R nach R.

Beispiel 71 : Sind $a_1,\ldots,a_n$ von Null verschiedene ganze Zahlen, dann ist

$$_{\mathbb{Z}}\langle a_1,\ldots,a_n\rangle = {}_{\mathbb{Z}}\langle ggT(a_1,\ldots,a_n)\rangle$$

(Beweis mit Hilfe des erweiterten euklidischen Algorithmus).

Definition 72 : Sei M ein Modul über R. Eine Familie $(v_i)_{i\in I}$ in M heißt ein *Erzeugendensystem* von M, wenn

$$_R\langle v_i \mid i \in I\rangle = M$$

ist.

Definition 73 : Seien M ein Modul über R und $(v_i)_{i\in I}$ eine Familie in M. Dann heißt $(v_i)_{i\in I}$ *linear unabhängig*, wenn für jede Koeffizienten-Familie

$(r_i)_{i\in I}$ aus

$$\sum_{i\in I} r_i v_i = 0$$

auch

$$r_i = 0 \quad \text{für alle } i \in I$$

folgt. Andernfalls heißt $(v_i)_{i\in I}$ *linear abhängig*.

Definition 74 : Sei M ein Modul über R. Ein linear unabhängiges Erzeugendensystem von M heißt eine *Basis* von M. Ein Modul heißt *frei*, wenn er eine Basis hat.

Beispiel 75 : Aus der Linearen Algebra ist bekannt: Wenn R ein Körper ist, ist jeder R-Modul frei.
Der R-Modul R^n ist frei. Die Familie $(e_i)_{1\le i\le n}$, wobei e_i das n-Tupel mit 1 in der i-ten und 0 in den anderen Komponenten ist, ist eine Basis von R^n und heißt *Standardbasis*.

Viele Definitionen und Sätze können direkt von Vektorräumen auf Moduln verallgemeinert werden. Ein wesentlicher Unterschied besteht aber darin, dass nicht alle Moduln frei sind. Zum Beispiel: $\mathbb{Z}_n$ mit $+$ und

$$\cdot : \mathbb{Z} \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \ , \ (a, \bar{b}) \longmapsto \overline{ab} \ ,$$

ist ein $\mathbb{Z}$-Modul. Für jedes Element $\bar{b}$ in $\mathbb{Z}_n$ ist $n \cdot \bar{b} = \overline{n \cdot b} = \bar{0}$, also gibt es in $\mathbb{Z}_n$ keine linear unabhängigen Familien.

§3. Polynome

In diesem Abschnitt sei R ein kommutativer Ring (zum Beispiel $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathcal{F}(\mathbb{R}, \mathbb{R}), \ldots$).

Definition 76 : Eine Folge $(r_i)_{i\in\mathbb{N}}$ in R ist eine *endliche Folge*, wenn es nur endlich viele Indizes i mit $r_i \neq 0$ gibt.

Durch jede endliche Folge wird eine Polynomfunktion definiert. Im Computer wird man daher diese Funktionen durch endliche Folgen darstellen. Allerdings können verschiedene endliche Folgen dieselbe Polynomfunktion definieren. Um den daraus entstehenden Problemen zunächst zu entgehen, betrachten wir statt der Funktionen die endlichen Folgen. Wir definieren für sie Rechenoperationen, die den punktweisen Rechenoperationen für Polynomfunktionen entsprechen.

Satz 77 : *Die Menge P aller endlichen Folgen in R mit den Funktionen*

$$+ : P \times P \longrightarrow P \qquad ,$$

$$((r_i)_{i\in\mathbb{N}},(s_i)_{i\in\mathbb{N}}) \longmapsto (r_i)_{i\in\mathbb{N}} + (s_i)_{i\in\mathbb{N}} := (r_i + s_i)_{i\in\mathbb{N}} \ ,$$

$$\cdot : P \times P \longrightarrow P \qquad ,$$

$$((r_i)_{i\in\mathbb{N}},(s_i)_{i\in\mathbb{N}}) \longmapsto (r_i)_{i\in\mathbb{N}} \cdot (s_i)_{i\in\mathbb{N}} := (\sum_{j=0}^{i} r_j s_{i-j})_{i\in\mathbb{N}} \ ,$$

und

$$\cdot : R \times P \longrightarrow P \ , \ (r,(s_i)_{i\in\mathbb{N}}) \longmapsto r \cdot (s_i)_{i\in\mathbb{N}} := (rs_i)_{i\in\mathbb{N}} \ ,$$

ist eine kommutative R-Algebra. Sie heißt Polynomring über *R oder* Algebra der Polynome mit Koeffizienten in *R. Ihre Elemente heißen* Polynome mit Koeffizienten in *R. Das Nullelement des Polynomringes ist die Folge* $0 := (0,0,0,\ldots)$*, das Einselement ist die Folge* $1 := (1,0,0,\ldots)$.

Beweis: Übung.

Definition 78 : Es sei $f = (r_0, r_1, r_2, \ldots) \neq 0$ ein Polynom mit Koeffizienten in R. Der *Grad* von f ist der größte Index i mit $r_i \neq 0$ und wird mit $\mathrm{gr}(f)$ bezeichnet. Das Element r_i heißt *i-ter Koeffizient* von f. Der Koeffizient $r_{\mathrm{gr}(f)}$ heißt *Leitkoeffizient* von f und wird mit $lk(f)$ bezeichnet. Das Polynom f heißt *normiert*, wenn $lk(f) = 1$ ist.
Die folgende Schreibweise ist zweckmäßig: Wir wählen irgendein Symbol, zum Beispiel x, und schreiben $1 := x^0 := (1,0,0,\ldots)$, $x := x^1 := (0,1,0,\ldots)$ und für $i \in \mathbb{N}$ $x^i := (0,\ldots,0,\underset{i}{1},0,\ldots)$. Dann ist

$$r_0 + r_1 x + r_2 x^2 + \ldots + r_{\mathrm{gr}(f)} x^{\mathrm{gr}(f)} = \sum_{i=0}^{\mathrm{gr}(f)} r_i x^i = (r_0, r_1, r_2, \ldots) \ .$$

Wir sprechen dann von einem *Polynom in der Variablen x mit Koeffizienten in R*. Für den Polynomring über R schreiben wir dann $R[x]$. Wir identifizieren Polynome vom Grad 0 mit ihrem nullten Koeffizienten und fassen R so als Teilmenge von $R[x]$ auf. Die „Variable x“ ist also ein Zeichen für die Folge $(0,1,0,\ldots)$.

Beispiel 79 : $\mathrm{gr}(1,2,3,4,5,0,\ldots) = \mathrm{gr}(\sum_{i=0}^{4}(i+1)x^i) = 4$ und

$lk(\sum_{i=0}^{4}(i+1)x^i) = 5.$

Definition 80 : Ein kommutativer Ring R heißt *Integritätsbereich*, wenn $R \neq \{0\}$ ist und

$$\text{für alle } a,b \in R \text{ aus } a \cdot b = 0 \text{ folgt, dass } a = 0 \text{ oder } b = 0$$

ist.

Beispiel 81 : $\mathbb{Z}$ ist ein Integritätsbereich. Jeder Körper ist ein Integritätsbereich. Der kommutative Ring aller Funktionen von $\mathbb{Q}$ nach $\mathbb{Q}$ (mit der punktweisen Addition und Multiplikation) ist kein Integritätsbereich.

Satz 82 : *Es seien $f \neq 0$, $g \neq 0$ Polynome mit Koeffizienten in R.*

(1) *Wenn $fg \neq 0$ ist, dann ist* $\mathrm{gr}(fg) \leq \mathrm{gr}(f) + \mathrm{gr}(g)$.
(2) *Wenn R ein Integritätsbereich ist, dann ist* $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$ *und* $lk(fg) = lk(f) \cdot lk(g)$.
(3) *Wenn $f + g \neq 0$, dann ist* $\mathrm{gr}(f+g) \leq \max(\mathrm{gr}(f), \mathrm{gr}(g))$.
Genau dann ist $\mathrm{gr}(f+g) < \max(\mathrm{gr}(f), \mathrm{gr}(g))$, *wenn* $\mathrm{gr}(f) = \mathrm{gr}(g)$ *und* $lk(f) = -lk(g)$ *ist.*

Beweis: (1) und (3) sind leicht nachzuprüfen.
Wenn R ein Integritätsbereich ist und $lk(f) \neq 0$, $lk(g) \neq 0$, ist auch $lk(f) \cdot lk(g)$ nicht 0. Daraus folgt (2).

Beispiel 83 : Es sei $f := \bar{2}x^2 + \bar{1}$ und $g := \bar{3}x \in \mathbb{Z}_6[x]$. Dann ist $f \cdot g = \bar{3}x$, also $\mathrm{gr}(f \cdot g) = 1$, aber $\mathrm{gr}(f) + \mathrm{gr}(g) = 3$.

Satz 84 : *Wenn R ein Integritätsbereich ist, dann ist auch $R[x]$ ein Integritätsbereich und alle invertierbaren Polynome haben den Grad* 0.

Beweis: Die Aussagen folgen aus Satz 82, (2).

Satz 85 : (Division mit Rest von Polynomen, vgl. Kap. 1, Satz 1)
Es seien f und g Polynome mit Koeffizienten in R. Der Leitkoeffizient von g sei in R invertierbar (wenn R ein Körper ist, bedeutet das: $g \neq 0$). Dann gibt es eindeutig bestimmte Polynome m und r mit den Eigenschaften

$$f = m \cdot g + r \quad \textit{und} \quad (r = 0 \textit{ oder } \mathrm{gr}(r) < \mathrm{gr}(g)) \quad .$$

Die Polynome m bzw. r heißen polynomialer Quotient von f und g *bzw.* Rest von f nach Division durch g. *Die Polynome m und r können mit dem folgenden Verfahren (*Divisionsalgorithmus*) berechnet werden:*

- *Setze $m := 0$ und $r := f$.*

- *Solange* $\mathrm{gr}(r) \geq \mathrm{gr}(g)$*, ersetze r durch*

$$r - lk(r) \cdot lk(g)^{-1} x^{gr(r)-gr(g)} g$$

und m durch

$$m + lk(r) \cdot lk(g)^{-1} x^{gr(r)-gr(g)}.$$

Beweis: Übung (analog dem Beweis des Satzes über die Division mit Rest von ganzen Zahlen).

Beispiel 86 : Es sei $f := 2x^4 - x + 3$ und $g := x^2 + 1 \in \mathbb{Z}[x]$. Dann:

$$\begin{array}{lll} m := 0, & r := f, & 4 = \mathrm{gr}(r) \geq \mathrm{gr}(g) = 2 \\ m := 0 + 2x^2, & r := r - 2x^2 \cdot g = -2x^2 - x + 3, & 2 = \mathrm{gr}(r) \geq \mathrm{gr}(g) \\ m := 2x^2 - 2, & r := r + 2g = -x + 5, & 1 = \mathrm{gr}(r) < \mathrm{gr}(g) = 2 \end{array}$$

und somit $f = (2x^2 - 2) \cdot g + (-x + 5)$.
Mit platzsparender Schreibweise:

$$\begin{array}{rrrl} 2x^4 & & -x & +3 \\ -(2x^4 & +2x^2) & & \\ & -2x^2 & -x & +3 \\ & -(-2x^2 & & -2) \\ & & -x & +5 \end{array} = (2x^2 - 2) \cdot (x^2 + 1) + (-x + 5)$$

Wenn R ein Körper ist, kann jedes Polynom durch jedes von Null verschiedene Polynom mit Rest dividiert werden. Daraus folgt, dass Polynomringe über Körpern und der Ring der ganzen Zahlen „algebraisch betrachtet“ einander sehr ähnlich sind.

Satz 87 : *Es seien* $(f_i)_{i \in \mathbb{N}}$ *eine Familie von Polynomen mit Koeffizienten in R so, dass für alle* $i \in \mathbb{N}$

$$\mathrm{gr}(f_i) = i \quad \textit{und} \quad lk(f_i) \textit{ in } R \textit{ invertierbar}$$

ist. Dann ist $(f_i)_{i \in \mathbb{N}}$ *eine R-Basis des Polynomrings über R. Insbesondere ist dieser ein freier R-Modul.*

Beweis: Sei $(r_i)_{i \in \mathbb{N}} \neq 0$ eine Koeffizientenfamilie in R. Sei k die größte Zahl so, dass $r_k \neq 0$. Wegen $\mathrm{gr}(f_k) = k$ und weil $lk(f_k)$ invertierbar ist, ist

$$lk(\sum_{i \in \mathbb{N}} r_i f_i) = r_k \cdot lk(f_k) \neq 0 \,,$$

also auch $\sum_{i\in\mathbb{N}} r_i f_i \neq 0$. Daher ist $(f_i)_{i\in\mathbb{N}}$ linear unabhängig.
Es sei $h \neq 0$ ein Polynom. Wir zeigen durch Induktion über $\mathrm{gr}(h)$, dass h eine R-Linearkombination von $(f_i)_{i\in\mathbb{N}}$ ist.
Wenn $\mathrm{gr}(h) = 0$ ist, dann ist $h = lk(h) \cdot lk(f_0)^{-1} \cdot f_0$.
Sei $j := \mathrm{gr}(h) > 0$. Division von h mit Rest durch f_j ergibt $h = m \cdot f_j + r$ mit $r = 0$ oder $\mathrm{gr}(r) < \mathrm{gr}(h)$. Dann ist

$$j = \mathrm{gr}(h) = \mathrm{gr}(m \cdot f_j) = \mathrm{gr}(m) + j \ ,$$

also $\mathrm{gr}(m) = 0$ und $m \in R$. Nach Induktionsannahme ist r eine R-Linearkombination von $(f_i)_{i\in\mathbb{N}}$, daher auch h.

Beispiel 88 : Die Familie $(x^i)_{i\in\mathbb{N}}$ ist eine R-Basis von $R[x]$.
Für jedes Element $a \in R$ ist $((x-a)^i)_{i\in\mathbb{N}}$ eine R-Basis von $R[x]$. Daher gibt es für jedes Polynom $h \in R[x]$ mit $n := \mathrm{gr}(h)$ eindeutig bestimmte Elemente $r_0, \ldots, r_n \in R$ so, dass

$$h = \sum_{i=0}^{n} r_i (x-a)^i$$

ist. Diese Darstellung von h kann wie im Satz oben durch mehrfache Division mit Rest durch $x-a$ ermittelt werden, oder indem in h statt x immer $(x-a)+a$ geschrieben wird („Taylorentwicklung“ von Polynomen).

Beispiel 89 : $3x^2+2x+1 = 3((x-a)+a)^2 + 2((x-a)+a)) + 1 =$
$= 3(x-a)^2 + (6a+2)(x-a) + (3a^2+2a+1)$.

§4. Nullstellen von Polynomen

In diesem Abschnitt sei R ein kommutativer Ring (zum Beispiel $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathcal{F}(\mathbb{R},\mathbb{R})$, …).

Definition 90 : Es sei $f = \sum_{i=0}^{n} c_i x^i \in R[x]$. Ein Element a einer R-Algebra A ist eine *Nullstelle von f in A*, wenn

$$f(a) := \sum_{i=0}^{n} c_i a^i = 0$$

ist. Dabei ist $a^0 := 1_A$, das Einselement von A. Man sagt: $f(a)$ ist das Element von A, das man durch „einsetzen von a in f“ erhält. es ist $x(a) = a$.
Ist $f = (c_0, c_1, \ldots, c_n, 0, \ldots) \in R[x]$, dann heißt

$$\tilde{f} : R \to R \ , \ a \mapsto f(a) = \sum_{i=0}^{n} c_i a^i$$

die durch f definierte Polynomfunktion. Es ist $\tilde{f}(a) = f(a)$, das heißt: Wertet man die Polynomfunktion $\tilde{f}$ in a aus, erhält man dasselbe Element von

R, wie wenn man a in das Polynom f einsetzt. Die durch x definierte Polynomfunktion $\tilde{x}$ ist die identische Funktion von R.
Man prüft nach, dass $\widetilde{f+g} = \tilde{f} + \tilde{g}$, $\widetilde{c \cdot f} = c \cdot \tilde{f}$ und $\widetilde{f \cdot g} = \tilde{f} \cdot \tilde{g}$ ist. Oft wird statt $\tilde{f}$ einfach wieder f geschrieben. Dann bedeutet x entweder das Zeichen, mit dem Polynome dargestellt werden, oder die identische Funktion von R nach R.

Satz 91 :

(1) *Der Rest von $f \in R[x]$ nach Division durch $x-a$ (mit $a \in R$) ist $f(a)$.*
(2) *Ein Element $a \in R$ ist genau dann Nullstelle eines Polynoms $f \in R[x]$, wenn das Polynom $x-a$ ein Teiler von f ist.*
(3) *Wenn R ein Integritätsbereich ist, dann hat jedes von Null verschiedene Polynom $f \in R[x]$ in R höchstens $\mathrm{gr}(f)$ Nullstellen.*
(4) *Es seien R ein Integritätsbereich, f, g Polynome über R und $f \neq g$. Dann haben die Graphen (in $R \times R$) der entsprechenden zwei Polynomfunktionen höchstens $\max(\mathrm{gr}(f), \mathrm{gr}(g))$ gemeinsame Elemente.*
(5) *Wenn R ein Integritätsbereich mit unendlich vielen Elementen ist, dann sind die Koeffizienten einer Polynomfunktion von R nach R eindeutig bestimmt. Insbesondere müssen in diesem Fall Polynome und Polynomfunktionen nicht unterschieden werden.*

Beweis:

(1) Division mit Rest von f durch $x-a$ ergibt $f = m \cdot (x-a) + r$, wobei $r = 0$ oder $\mathrm{gr}(r) = 0$, also $r \in R$ ist. Daher ist

$$f(a) = m(a) \cdot 0 + r = r.$$

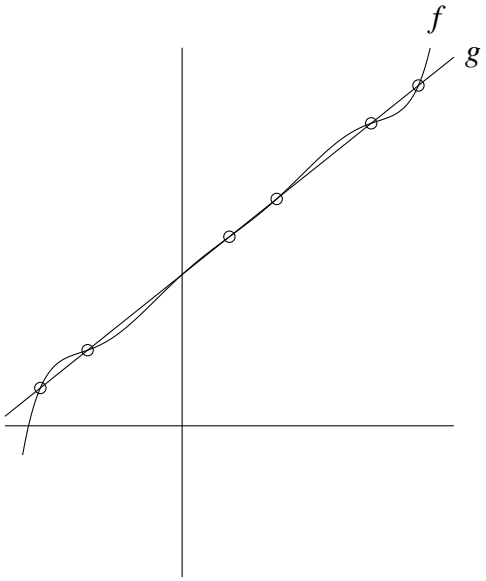
(2) folgt aus (1).
(3) Wir beweisen die Aussage durch Induktion über $n := \mathrm{gr}(f)$.
Wenn $n = 0$ ist, dann hat f wegen $f \neq 0$ keine Nullstellen.
Sei $n > 0$ und sei $a \in R$ eine Nullstelle von f. Nach (2) gibt es ein Polynom $h \in R[x]$ mit $f = (x-a) \cdot h$. Dann ist $\mathrm{gr}(h) = n-1$, nach Induktionsvoraussetzung hat h daher höchstens $n-1$ Nullstellen. Weil R ein Integritätsbereich ist, ist jede Nullstelle von $(x-a) \cdot h$ eine Nullstelle von h oder gleich a. Daraus folgt die Behauptung.
(4) Die Menge der gemeinsamen Elemente der Graphen von f und g ist

$$\{(a, f(a)) | f(a) = g(a)\},$$

ihre Anzahl ist daher die Anzahl der Nullstellen von $f-g$. Nach (3) ist diese höchstens $\max(\mathrm{gr}(f), \mathrm{gr}(g))$.
(5) Es seien f, g zwei Polynome mit Koeffizienten in R so, dass für alle $a \in R$ gilt: $f(a) = g(a)$. Da R unendlich ist, hat dann $f-g$ beliebig viele Nullstellen. Nach (3) ist daher $f = g$.

Beispiel 92 : Die Notwendigkeit der Voraussetzung „R Integritätsbereich“ in Satz 91, (3), zeigt das folgende Beispiel: Das Polynom $\bar{2}x \in \mathbb{Z}_4[x]$ hat Grad 1, aber in $\mathbb{Z}_4$ zwei Nullstellen, nämlich $\bar{0}$ und $\bar{2}$.

Beispiel 93 : Wenn



der Graph einer Polynomfunktion f ist, dann muss $\mathrm{gr}(f) \geq 6$ sein, weil $\mathrm{gr}(g) = 1$ und nach Satz 91, (4), $\mathrm{gr}(f) = \max(\mathrm{gr}(f), \mathrm{gr}(g)) \geq 6$ sein muss.

Nach Satz 91, können Polynome und Polynomfunktionen identifiziert werden, wenn der Koeffizientenring gleich $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ ist. Dann kann auch vom Grad einer Polynomfunktion gesprochen werden.

Beispiel 94 : Ist f ein Polynom mit $\mathrm{gr}(f) = 2$ und Koeffizienten in einem Körper K, dann hat f entweder keine Nullstelle in K oder $f = lk(f)(x-a)(x-b)$. Dabei sind a und b die Nullstellen von f (es kann auch $a = b$ sein).

§5. Interpolation

In diesem Abschnitt seien K ein Körper, $x_0, \ldots, x_n$ paarweise verschiedene Elemente von K und $y_0, \ldots, y_n$ Elemente von K. Wir suchen ein Polynom $f \in K[x]$ mit der Eigenschaft

$$f(x_i) = y_i \,, \quad 0 \leq i \leq n \,.$$

Ein solches Polynom heißt *interpolierendes Polynom*. Die Elemente $x_0, \ldots, x_n$ heißen *Stützstellen* und $y_0, \ldots, y_n$ *Werte* der Interpolationsaufgabe.

Satz 95 : *(Lagrange-Interpolation) Es gibt genau ein interpolierendes Polynom vom Grad $\leq n$. Dieses kann wie folgt berechnet werden:*

- *Berechne für $0 \leq i \leq n$ das Polynom*

$$f_i := \prod_{j \neq i} \frac{1}{x_i - x_j} \cdot (x - x_j) \in K[x] \ .$$

- *Das interpolierende Polynom ist*

$$\sum_{i=0}^{n} y_i \cdot f_i \ .$$

Beweis: Für $0 \leq i,k \leq n$ ist $f_i(x_k) = \delta_{ik}$. Daher ist für $0 \leq k \leq n$

$$(\sum_{i=0}^{n} y_i \cdot f_i)(x_k) = \sum_{i=0}^{n} y_i \delta_{ik} = y_k \ .$$

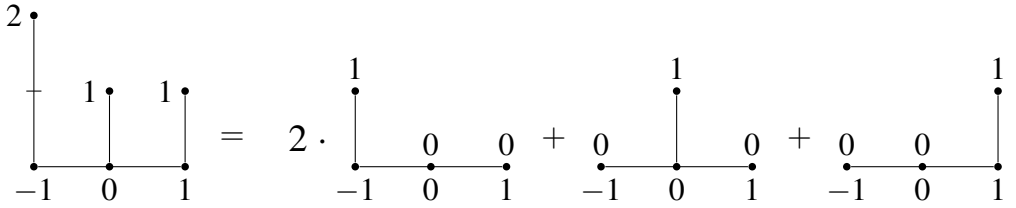
Der Grad von f_i ist n, also ist der Grad von $\sum_{i=0}^{n} y_i \cdot f_i$ kleiner oder gleich n.

Wenn f, g interpolierende Polynome vom Grad $\leq n$ sind, dann sind die Elemente $x_0, \ldots, x_n$ Nullstellen von $f - g$. Aus Satz 91 folgt daher $f = g$.

Die Strategie zur Lösung der Interpolationsaufgabe ist dieselbe wie die des erweiterten Euklidischen Algorithmus: Löse zuerst einfache Spezialfälle und konstruiere dann daraus die gesuchte Lösung.

Beispiel 96 : Es sei $x_0 = -1$, $x_1 = 0$, $x_2 = 1$ und $y_0 = 2$, $y_1 = 1$, $y_2 = 1$.

Interpolation nach Lagrange:



$$f_0 = \frac{1}{2}x(x-1) \quad f_1 = -(x+1)(x-1) \quad f_2 = \frac{1}{2}x(x+1)$$

$$f = 2f_0 + f_1 + f_2 = \frac{1}{2}x^2 - \frac{1}{2}x + 1$$

Interpolation nach Newton:

$$\begin{aligned} h_0 &= 2 \\ h_1 &= 2 + c_1(x+1) \\ 1 = h_1(0) &= 2 + c_1,\ c_1 = -1 \\ h_1 &= -x+1 \\ h_2 &= -x+1+c_2x(x+1) \\ 1 = h_2(1) &= c_2 \cdot 2,\ c_2 = \frac{1}{2} \\ f = h_2 &= -x+1+\frac{1}{2}x(x+1) = \frac{1}{2}x^2 - \frac{1}{2}x + 1 \end{aligned}$$

Satz 97: *(Newton-Interpolation) Das interpolierende Polynom kann induktiv wie folgt berechnet werden:*

- *Setze $k := 0$ und $h_0 := y_0$.*
- *Solange $k < n$ ist, ersetze k durch $k+1$, und setze*

$$c_k := \frac{y_k - h_{k-1}(x_k)}{\prod_{i=0}^{k-1}(x_k - x_i)}$$

und

$$h_k := h_{k-1} + c_k \prod_{i=0}^{k-1}(x - x_i)\ .$$

- *Das interpolierende Polynom ist dann h_n.*

Beweis: Übung.

Satz 98: *Es sei $f \in \mathbb{Q}[x]$ ein Polynom vom Grad $d \in \mathbb{N}$. Dann gibt es genau ein Polynom g vom Grad $d+1$ so, dass für alle $n \in \mathbb{N}$*

$$g(n) = \sum_{i=0}^{n} f(i)$$

ist.
Dieses Polynom kann wie folgt berechnet werden: Berechne durch Newton-Interpolation für die Stützstellen $0, 1, \ldots, d$ und die Funktionswerte $f(0), \ldots, f(d)$ Zahlen $c_0, \ldots, c_d \in \mathbb{Q}$ so, dass $f = c_0 + \sum_{i=1}^{d} c_i \prod_{j=0}^{i-1}(x-j)$ ist. Dann ist

$$g = c_0 + \sum_{i=1}^{d} \frac{c_i}{i+1} \prod_{j=-1}^{i-1}(x-j)\ .$$

Beweis: Es ist $g(0) = f(0)$. Für $0 \neq n \in \mathbb{N}$ ist

$$g(n)-g(n-1) = c_0 + \sum_{i=1}^{d} \frac{c_i}{i+1} \prod_{j=-1}^{i-1} (n-j) - c_0 - \sum_{i=1}^{d} \frac{c_i}{i+1} \prod_{j=-1}^{i-1} (n-j-1) =$$

$$= c_0 + \sum_{i=1}^{d} \frac{c_i}{i+1} (\prod_{j=0}^{i-1} (n-j))(i+1) = f(n) \ ,$$

also ist $g(n) =$

$$= (g(n)-g(n-1)) + (g(n-1)-g(n-2)) + \ldots + (g(1)-g(0)) + g(0) =$$

$$= \textstyle\sum_{i=0}^{n} f(i) \ .$$

Beispiel 99 : Es sei $f := x^3 \in \mathbb{Q}[x]$. Dann ist $f = x + 3x(x-1) + x(x-1)(x-2)$ und

$$\sum_{i=0}^{n} i^3 = \frac{1}{2} n(n+1) + n(n-1)(n+1) + \frac{1}{4} n(n-1)(n-2)(n+1) =$$

$$= \frac{1}{4} n^2 (n+1)^2 \ .$$

§6. Polynomringe über Körpern

In diesem Abschnitt sei K ein Körper. Statt „Polynom mit Koeffizienten in K“ schreiben wir nur „Polynom“.

Definition 100 : Es seien $f_1, \ldots, f_n$ von Null verschiedene Polynome. Das normierte Polynom größten Grades, das $f_1, \ldots, f_n$ teilt, heißt *größter gemeinsamer Teiler* von $f_1, \ldots, f_n$ und wird mit $ggT(f_1, \ldots, f_n)$ bezeichnet. Das normierte Polynom kleinsten Grades, das von $f_1, \ldots, f_n$ geteilt wird, heißt *kleinstes gemeinsames Vielfaches* von $f_1, \ldots, f_n$ und wird mit $kgV(f_1, \ldots, f_n)$ bezeichnet.

Satz 101 : *Es seien f, g, h Polynome, $f \neq 0$, $g \neq 0$ und $f \neq h \cdot g$. Dann ist*

$$ggT(f,g) = ggT(f - h \cdot g, g) \ .$$

Beweis: Wenn t ein Teiler von f und g ist, dann gibt es Polynome u, v so, dass $f = t \cdot u$ und $g = t \cdot v$ ist. Daher ist $f - h \cdot g = t \cdot u - h \cdot t \cdot v = t \cdot (u - h \cdot v)$, also t auch ein Teiler von $f - h \cdot g$.

Satz 102 : (Euklidischer Algorithmus für Polynome)
Es seien f,g Polynome, $f \neq 0$ und $g \neq 0$. Mit dem folgenden Verfahren kann der größte gemeinsame Teiler von f und g berechnet werden:

- *Solange keines der zwei Polynome ein Teiler der anderen ist, ersetze das Polynom größeren (oder gleichen) Grades durch seinen Rest nach Division durch das andere.*
- *Wenn h, eines der zwei Polynome, ein Teiler des anderen ist, dann ist $ggT(f,g) = lk(h)^{-1}h$.*

Beweis: Es seien a und b die Grade von f und g. Sei $a \geq b$. Wenn f und g verschieden sind, wird f im nächsten Schritt durch ein Polynom kleineren Grades ersetzt. Also liefert das Verfahren nach höchstens $max(a,b)$ Schritten ein Ergebnis. In jedem Schritt wird ein Paar von Polynomen durch ein anderes ersetzt, nach Satz 101 aber so, dass die größten gemeinsamen Teiler der zwei Polynompaare gleich sind. Sobald eines der zwei Polynome das andere teilt, ist dieses $c \cdot ggT(f,g)$, für ein $0 \neq c \in K$.

Beispiel 103 : Für $f := x^2+3x+2$ und $g := x^2+5x+6 \in \mathbb{Q}[x]$ ist $f = 1 \cdot g + (-2x-4)$ und $g = (-\frac{1}{2}x - \frac{3}{2})(-2x-4)+0$, also $ggT(f,g) = x+2$.

Satz 104 : (Erweiterter Euklidischer Algorithmus)
Es seien f,g Polynome, $f \neq 0$ und $g \neq 0$. Es gibt Polynome u,v so, dass $uf+vg = ggT(f,g)$ ist. Diese können mit dem folgenden Verfahren berechnet werden:

- *Setze $A := (A_1,A_2,A_3) := (f,1,0) \in K[x]^3$ und $B := (B_1,B_2,B_3) := (g,0,1) \in K[x]^3$.*
- *Solange B_1 das Polynom A_1 nicht teilt, berechne den polynomialen Quotienten m von A_1 und B_1 und setze $C := B$, $B := A - m \cdot C := (A_1 - m \cdot C_1, A_2 - m \cdot C_2, A_3 - m \cdot C_3)$ und dann $A := C$.*
- *Wenn B_1 das Polynom A_1 teilt, dann ist $u := lk(B_1)^{-1} \cdot B_2$ und $v := lk(B_1)^{-1} \cdot B_3$.*

Beweis: Wenn zwei Tripel von Polynomen S und T die Eigenschaft

$$S_1 = f \cdot S_2 + g \cdot S_3 \quad \text{bzw.} \quad T_1 = f \cdot T_2 + g \cdot T_3$$

haben, dann auch alle Tripel $S - hT$ mit $h \in K[x]$. Die ersten zwei Tripel im Algorithmus haben diese Eigenschaft, daher auch alle anderen auftretenden Tripel. Für die ersten Komponenten der Tripel wird der euklidische Algorithmus durchgeführt, für das letzte Tripel B gilt daher
$lk(B_1) \cdot ggT(f,g) = f \cdot B_2 + g \cdot B_3$.

Beispiel 105 : $f := x^2+1 \in \mathbb{Q}[x]$, $g := x+2 \in \mathbb{Q}[x]$

f	g		
1	0	x^2+1	$1\cdot f+0\cdot g = x^2+1$
0	1	$x+2$	$0\cdot f+1\cdot g = x+2$
1	$-x$	$-2x+1$	$1\cdot f+(-x)\cdot g = -2x+1$
$\frac{1}{2}$	$1-\frac{1}{2}x$	$\frac{5}{2}$	$\frac{1}{2}\cdot f+(1-\frac{1}{2}x)\cdot g = \frac{5}{2}$
$\frac{1}{5}$	$-\frac{1}{5}(x-2)$	1	$\frac{1}{5}f-\frac{1}{5}(x-2)\cdot g = 1$

Insbesondere ist $ggT(f,g) = 1$.

Satz 106 : (Berechnung von $kgV(f,g)$)
Es seien f,g Polynome, $f \neq 0$ und $g \neq 0$. Sei $z := lk(f)^{-1}lk(g)^{-1} \in K$. Dann ist

$$kgV(f,g) = \frac{z\cdot f}{ggT(f,g)}\cdot g = \frac{z\cdot g}{ggT(f,g)}\cdot f.$$

Beweis: Es ist klar, dass $\frac{z\cdot f}{ggT(f,g)}\cdot g = \frac{z\cdot g}{ggT(f,g)}\cdot f$ ein Vielfaches von f und von g ist. Sei h ein Polynom, das Vielfaches von f und von g ist. Dann gibt es Polynome c,d mit $h = c\cdot f$ und $h = d\cdot g$. Nach Satz 104 gibt es Polynome u,v so, dass $u\cdot f + v\cdot g = ggT(f,g)$. Dann ist

$$h = \frac{u\cdot f+v\cdot g}{ggT(f,g)}\cdot h = \frac{u\cdot f}{ggT(f,g)}\cdot h + \frac{v\cdot g}{ggT(f,g)}\cdot h =$$
$$= \frac{u\cdot f\cdot d\cdot g}{ggT(f,g)} + \frac{v\cdot g\cdot c\cdot f}{ggT(f,g)} = \frac{f\cdot g}{ggT(f,g)}\cdot(u\cdot d+v\cdot c) =$$
$$= \frac{z\cdot f\cdot g}{ggT(f,g)}\cdot z^{-1}\cdot(u\cdot d+v\cdot c)$$

ein Vielfaches von

$$\frac{z\cdot f\cdot g}{ggT(f,g)}.$$

Satz 107 : *Es seien $f_1,\ldots,f_n$ Polynome. Dann ist*

$$ggT(f_1,\ldots,f_n) = ggT(f_1,ggT(f_2,ggT(f_3,ggT(\ldots,f_n)\ldots)),$$

also kann der größte gemeinsame Teiler mehrerer Polynome durch sukzessives Berechnen des größten gemeinsamen Teilers von je zwei Polynomen berechnet werden.
Mit Satz 104 können Polynome $u_1,\ldots,u_n$ so berechnet werden, dass

$$f_1\cdot u_1+\ldots+f_n\cdot u_n = ggT(f_1,\ldots,f_n)$$

ist.

Beweis: Übung.

Satz 108 : *Es seien $f_1,\ldots,f_n$ von Null verschiedene Polynome ,*
$g := ggT(f_1,\ldots,f_n)$ und h ein Polynom. Es gibt genau dann ein n-Tupel $(x_1,\ldots,x_n)$ von Polynomen mit

$$f_1 \cdot x_1 + \ldots + f_n \cdot x_n = h \ ,$$

wenn h ein Vielfaches von g ist. In diesem Fall kann ein solches n-Tupel wie folgt berechnet werden:

- *Berechne Polynome $u_1,\ldots,u_n$ so, dass $f_1 \cdot u_1 + \ldots + f_n \cdot u_n = g$ ist.*
- *Setze $x_i := u_i \cdot \frac{h}{g},\ 1 \leq i \leq n$.*

Beweis: Für jedes n-Tupel $(x_1,\ldots,x_n)$ von Polynomen wird
$f_1 \cdot x_1 + \ldots + f_n \cdot x_n$ von g geteilt. Also ist die Bedingung, dass h ein Vielfaches von g ist, notwendig für die Existenz einer Lösung. Wenn diese Bedingung erfüllt ist, ist leicht nachzuprüfen, dass $(u_1 \cdot \frac{h}{g},\ldots,u_n \cdot \frac{h}{g})$ eine Lösung ist.

Definition 109 : Es seien R ein kommutativer Ring und I eine nicht-leere Teilmenge von R. Dann ist I genau dann ein *Ideal* von R, wenn für alle $a,b \in I$ und $r \in R$ gilt:

$$a+b \in I \quad \text{und} \quad ra \in I \ .$$

Die Schreibweise „$I \lhd R$“ bedeutet „I ist ein Ideal von R“.

Beispiel 110 : Die Teilmengen $\{0\}$ und R sind Ideale von R. Diese zwei Ideale heißen *triviale Ideale* von R. Für jedes Element $a \in R$ ist die Menge $aR := Ra := \{ra \mid r \in R\}$ ein Ideal von R. Diese Ideale heißen *Hauptideale* von R.

Beispiel 111 : Für $n \in \mathbb{Z}$ ist $\{t \cdot n \mid t \in \mathbb{Z}\}$ ein Hauptideal von $\mathbb{Z}$.
Für $f \in \mathbb{Q}[x]$ ist $\{s \cdot f \mid s \in \mathbb{Q}[x]\}$ ein Hauptideal von $\mathbb{Q}[x]$.

Satz 112 : *Alle Ideale in $\mathbb{Z}$ sind Hauptideale.*

Beweis: Sei I ein Ideal von $\mathbb{Z}$. Das Ideal $\{0\} = 0 \cdot \mathbb{Z}$ ist ein Hauptideal. Sei nun $I \neq \{0\}$. Dann enthält I eine Zahl $d \neq 0$. Da I ein Ideal ist, ist auch $vz(d) \cdot d \in I$, also enthält I eine positive Zahl. Sei b die kleinste positive Zahl in I. Wenn nun $a \in I$ ist, dann dividiere a mit Rest durch b. Es seien m bzw. r der entsprechende ganzzahlige Quotient bzw. Rest. Dann ist $a = m \cdot b + r$ und aus $a \in I,\ -m \cdot b \in I$ folgt $r = a - m \cdot b \in I$. Wegen der Minimalität von b kann r keine positive Zahl sein, somit ist $r = 0$ und a ein Vielfaches von b.

Satz 113 : *Alle Ideale in $K[x]$ sind Hauptideale. Wenn ein Ideal I von Polynomen $f_1 \neq 0, \ldots, f_n \neq 0$ erzeugt wird, dann auch vom größten gemeinsamen Teiler dieser Polynome.*

Beweis: Sei I ein Ideal von $K[x]$. Das Ideal $\{0\} = 0 \cdot K[x]$ ist ein Hauptideal. Sei nun $I \neq \{0\}$. Sei g ein Polynom kleinsten Grades in I. Wenn nun $f \in I$ ist, dann dividiere f mit Rest durch g. Es seien m bzw. r der entsprechende polynomiale Quotient bzw. Rest. Dann ist $f = m \cdot g + r$ und aus $f \in I,\ -m \cdot g \in I$ folgt $r = f - m \cdot g \in I$. Wegen der Minimalität des Grades von g muss $r = 0$ sein, somit f ein Vielfaches von g. Die zweite Behauptung folgt nun aus Satz 108 .

Satz 114 : *Es seien $(f_i)_{i \in M}$ eine Familie von Polynomen und I das von ihr erzeugte Ideal. Dann stimmen die Mengen*

$$\{a \in K \mid f_i(a) = 0, i \in M\} \quad \textit{und} \quad \{a \in K \mid g(a) = 0, g \in I\}$$

der gemeinsamen Nullstellen *der Familie $(f_i)_{i \in M}$ und des Ideals I überein. Insbesondere ist die Menge der gemeinsamen Nullstellen der Familie von Polynomen $(f_i)_{i \in M}$ gleich der Menge der Nullstellen des größten gemeinsamen Teilers dieser Polynome.*

Beweis: Es seien $g \in I$ und $a \in K$. Dann gibt es eine Koeffizientenfamilie $(c_i)_{i \in M}$ in $K[x]$ so, dass $g = \sum_{i \in M} c_i f_i$ ist. Wenn für alle $i \in M$ gilt: $f_i(a) = 0$, dann ist

$$g(a) = (\sum_{i \in M} c_i f_i)(a) = \sum_{i \in M} c_i(a) f_i(a) = 0 \, .$$

Die zweite Aussage folgt nun aus Satz 113.

Ein *System von polynomialen Gleichungen mit einer Unbekannten* ist die folgende Aufgabe: Gegeben sind Polynome $f_1, \ldots, f_k \in K[x]$. Gesucht sind alle Elemente a von K so, dass $f_1(a) = f_2(a) = \ldots = f_k(a) = 0$ ist. Das Element a ist dann eine *gemeinsame Nullstelle* von $f_1, \ldots, f_k$. Nach Satz 114 sind die gemeinsamen Nullstellen von $f_1, \ldots, f_k$ genau die Nullstellen von $ggT(f_1, \ldots, f_k)$. Systeme von polynomialen Gleichungen in einer Unbekannten können also auf eine polynomiale Gleichung zurückgeführt werden.

§7. Irreduzible Polynome

In diesem Abschnitt sei R ein Integritätsbereich.

Definition 115 : Zwei Elemente a und b von R heißen *assoziiert*, wenn es ein invertierbares Element c von R gibt so, dass $a = cb$ ist.

Beispiel 116 : Zwei ganze Zahlen sind genau dann assoziiert, wenn ihre Beträge gleich sind. Wenn zwei Polynome mit Koeffizienten in R assoziiert sind und den gleichen Leitkoeffizienten haben, dann sind sie gleich.

Definition 117 : Ein Element $f \in R$ ist *in R irreduzibel*, wenn die folgenden Bedingungen erfüllt sind:

(1) $f \neq 0$,
(2) f ist nicht invertierbar,
(3) jeder Teiler von f ist invertierbar oder zu f assoziiert („f hat nur triviale Teiler“).

Beispiel 118 : Eine ganze Zahl ist genau dann in $\mathbb{Z}$ irreduzibel, wenn sie eine Primzahl ist. In einem Körper gibt es keine irreduziblen Elemente. Ein Polynom f mit Koeffizienten in einem Körper K ist genau dann irreduzibel, wenn es in $K[x]$ keine Teiler hat, deren Grad größer als 0 und kleiner als $\mathrm{gr}(f)$ ist. Insbesondere sind alle Polynome mit Grad 1 in $K[x]$ irreduzibel.

Definition 119 : Ein Integritätsbereich R heißt *ZPE-Ring* („die **Z**erlegung in **P**rimfaktoren ist **e**indeutig“) oder *faktoriell*, wenn gilt:

(1) Für jedes von Null verschiedene und nicht invertierbare Element $f \in R$ gibt es irreduzible Elemente $p_1, \ldots, p_n \in R$ so, dass

$$f = p_1 p_2 \ldots p_n$$

ist.

(2) Wenn $q_1, \ldots, q_m \in R$ irreduzible Elemente sind so, dass

$$f = q_1 q_2 \ldots q_m$$

ist, dann ist $m = n$ und es gibt invertierbare Elemente $u_1, \ldots, u_n$ und eine Permutation $\sigma \in S_n$ so, dass $p_i = u_i q_{\sigma(i)}$, $1 \leq i \leq n$, ist.

Kurz formuliert: R ist faktoriell, wenn jedes von Null verschiedene und nicht invertierbare Element von R Produkt von irreduziblen Elementen ist und diese Faktoren bis auf die Reihenfolge und bis auf Assoziiertheit eindeutig bestimmt sind.

Beispiel 120 : $\mathbb{Z}$ ist faktoriell. Jeder Körper ist faktoriell.

Satz 121 : *Es sei $f \in K[x]$ ein irreduzibles Polynom mit Koeffizienten in einem Körper K. Wenn f das Produkt zweier Polynome teilt, dann auch eines dieser zwei Polynome.*

Beweis: Es seien $g,h \in K[x]$ so, dass f das Polynom gh teilt. Wir nehmen an, dass f das Polynom g nicht teilt. Weil f irreduzibel ist, ist dann $ggT(f,g) = 1$. Nach Satz 104 gibt es Polynome u,v mit $uf + vg = 1$. Weil f ein Teiler von ufh und vgh ist, teilt es auch $h = 1 \cdot h = ufh + vgh$.

Satz 122 : *Der Polynomring $K[x]$ mit Koeffizienten in einem Körper K ist faktoriell. Insbesondere gilt: Zu jedem Polynom $f \in K[x]$ mit positivem Grad gibt es bis auf die Reihenfolge eindeutig bestimmte normierte irreduzible Polynome $f_1, \ldots, f_n$ so, dass*

$$f = lk(f) \prod_{i=1}^{n} f_i$$

ist.

Beweis: Es sei $0 \neq f \in K[x]$ ein Polynom mit positivem Grad. Wir zeigen die Existenz einer Zerlegung in irreduzible Faktoren durch Induktion über $\mathrm{gr}(f)$.
Wenn $\mathrm{gr}(f) = 1$ ist, dann ist f irreduzibel.
Wenn $\mathrm{gr}(f) > 1$ ist, dann ist f entweder irreduzibel oder es gibt Polynome g,h mit positivem Grad so, dass $f = gh$ ist. Dann sind die Grade von g und h aber kleiner als der von f. Nach Induktionsannahme sind g und h Produkte von irreduziblen Elementen, also auch f.
Eindeutigkeit: Wenn $f = p_1 p_2 \ldots p_n$ und $f = q_1 q_2 \ldots q_m$ zwei Zerlegungen von f in irreduzible Elemente sind, dann gibt es nach Satz 121 einen Index j so, dass q_j das irreduzible Polynom p_n teilt. Es gibt also ein invertierbares Element u in $K[x]$ so, dass $p_n = uq_j$ ist. Daher ist

$$g := up_1 p_2 \ldots p_{n-1} = \prod_{1 \leq i \leq m,\, i \neq j} q_i \ .$$

Der Grad von g ist kleiner als der von f, daher folgt aus der Induktionsannahme die Eindeutigkeit der irreduziblen Faktoren von g bis auf die Reihenfolge und Assoziiertheit.

Satz 123 : *In jedem Polynomring über einem Körper gibt es unendlich viele normierte irreduzible Polynome.*

Wenn K ein Körper mit endlich vielen Elementen ist, gibt es zu jeder natürlichen Zahl n unendlich viele normierte irreduzible Polynome in $K[x]$, deren Grad größer als n ist.

Beweis: Wenn es nur endlich viele normierte irreduzible Polynome gäbe, dann wäre ihr Produkt q ein Polynom und der Grad von $q+1$ wäre größer (oder gleich, wenn es nur ein normiertes irreduzibles Polynom gibt) als der jedes irreduziblen Polynoms. Insbesondere wäre $q+1$ kein normiertes irreduzibles Polynom. Nach Satz 122 gibt es ein normiertes irreduzibles Polynom p, das $q+1$ teilt. Da p auch q teilt, würde p dann auch 1 teilen, Widerspruch.
Wenn K ein endlicher Körper und n eine natürliche Zahl ist, gibt es nur endlich viele Polynome, deren Grad kleiner oder gleich n ist. Daraus folgt die zweite Behauptung.

Beispiel 124 : Die irreduziblen Polynome in $\mathbb{Z}_2[x]$, deren Grad höchstens 3 ist, sind: x, $x+1$, x^2+x+1, x^3+x^2+1, x^3+x+1.

Satz 125 : *Ein Polynom mit komplexen Koeffizienten ist genau dann in $\mathbb{C}[x]$ irreduzibel, wenn sein Grad 1 ist.*
Insbesondere gilt: Wenn $f \in \mathbb{C}[x]$ positiven Grad hat und $z_1, \ldots, z_n$ die Nullstellen von f in $\mathbb{C}$ sind, dann gibt es eindeutig bestimmte positive ganze Zahlen $e_1, \ldots, e_n$ so, dass

$$f = lk(f) \prod_{i=1}^{n} (x - z_i)^{e_i}$$

ist.

Beweis: In der Analysis wird gezeigt, dass jedes Polynom in $\mathbb{C}[x]$ mit positivem Grad in $\mathbb{C}$ eine Nullstelle hat. Wenn z eine Nullstelle eines irreduziblen Polynoms f ist, dann wird f von $x-z$ geteilt. Daher muss
$f = lk(f)(x-z)$ sein.
Die zweite Aussage folgt nun aus Satz 122.

Satz 126 : *Wenn eine komplexe Zahl $z \in \mathbb{C}$ Nullstelle eines Polynoms mit reellen Koeffizienten ist, dann ist auch die zu z konjugierte komplexe Zahl $\bar{z}$ eine Nullstelle dieses Polynoms.*

Beweis: Es seien $f = \sum_{i=0}^{n} c_i x^i \in \mathbb{R}[x]$ und $z \in \mathbb{C}$ eine Nullstelle von f. Dann ist

$$f(\bar{z}) = \sum_{i=0}^{n} c_i \bar{z}^i = \overline{\sum_{i=0}^{n} c_i z^i} = \overline{f(z)} = \bar{0} = 0 .$$

Satz 127 : *Ein Polynom mit reellen Koeffizienten ist genau dann in* $\mathbb{R}[x]$ *irreduzibel, wenn*

- *sein Grad* 1 *ist oder*
- *sein Grad* 2 *ist und es in* $\mathbb{R}$ *keine Nullstellen hat.*

Beweis: Es sei f ein irreduzibles Polynom in $\mathbb{R}[x]$. Dann ist sein Grad eine positive Zahl, also hat f in $\mathbb{C}$ eine Nullstelle z.
Wenn z eine reelle Zahl ist, dann ist $x-z$ ein Teiler von f in $\mathbb{R}[x]$, also ist $f = lk(f)(x-z)$.
Wenn z nicht eine reelle Zahl ist, dann sind z und die dazu konjugierte komplexe Zahl $\bar{z}$ verschieden. Nach Satz 126 wird f in diesem Fall von $(x-z)(x-\bar{z})$ in $\mathbb{C}[x]$ geteilt. Alle Koeffizienten des Polynoms $(x-z)(x-\bar{z}) = x^2 - 2\mathrm{Re}(z) + |z|^2$ sind reell. Da f reelle Koeffizienten hat, muss das auch für den polynomialen Quotienten von f und $(x-z)(x-\bar{z})$ gelten. Daher wird f von $(x-z)(x-\bar{z})$ auch in $\mathbb{R}[x]$ geteilt, somit ist $f = lk(f)(x-z)(x-\bar{z})$.

§8. Polynomringe über faktoriellen Ringen

Das Polynom $2x$ ist in $\mathbb{Q}[x]$ irreduzibel, in $\mathbb{Z}[x]$ aber nicht. Das Polynom 2 ist in $\mathbb{Z}[x]$ irreduzibel, in $\mathbb{Q}[x]$ aber nicht. Im letzten Abschnitt haben wir gesehen, dass $\mathbb{Q}[x]$ faktoriell ist. Gilt das auch für $\mathbb{Z}[x]$?

In diesem Abschnitt ist R ein faktorieller Ring, zum Beispiel $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}[y], \ldots$.

Definition 128 : Ein Polynom in $R[x]$ heißt *primitiv*, wenn es nicht 0 ist und kein irreduzibles Element von R alle seine Koeffizienten teilt.

Beispiel 129 : $2x^2+3x+4 \in \mathbb{Z}[x]$ und $(y+1)x^2+(y^2-1)x+y \in (\mathbb{Q}[y])[x]$ sind primitiv, aber $2x^2+2x+4 \in \mathbb{Z}[x]$ ist nicht primitiv.

Beispiel 130 : Jedes normierte Polynom in $R[x]$ ist primitiv. Jedes irreduzible Polynom in $R[x]$ ist primitiv. Ein Polynom mit Koeffizienten in $\mathbb{Z}$ ist primitiv, wenn es nicht 0 ist und der größte gemeinsame Teiler seiner Koeffizienten 1 ist. Jedes von Null verschiedene Polynom mit Koeffizienten in einem Körper ist primitiv.

Satz 131 : („Lemma von Gauß“)
Das Produkt von zwei primitiven Polynomen in $R[x]$ ist primitiv.

Beweis: Es seien $f := \sum_i r_i x^i$ und $g := \sum_j s_j x^j$ zwei primitive Polynome in $R[x]$ und p ein irreduzibles Element von R. Seien m bzw. n der kleinste Index i so, dass p den Koeffizienten r_i bzw. s_i nicht teilt. Weil f und g primitiv sind, existieren diese Indizes. Der $(m+n)$-te Koeffizient c_{m+n} von fg ist

$$\sum_{\substack{i,j \\ i+j=m+n}} r_i s_j = r_m s_n + \sum_{\substack{i,j \\ i+j=m+n \\ i<m}} r_i s_j + \sum_{\substack{i,j \\ i+j=m+n \\ j<n}} r_i s_j \; .$$

Die Elemente

$$\sum_{\substack{i,j \\ i+j=m+n \\ i<m}} r_i s_j \quad \text{und} \quad \sum_{\substack{i,j \\ i+j=m+n \\ j<n}} r_i s_j$$

werden von p geteilt, also ist c_{m+n} die Summe von $r_m s_n$ und einem Vielfachen von p. Wenn p auch c_{m+n} teilte, wäre p auch ein Teiler und damit ein irreduzibler Faktor von $r_m s_n$. Weil p weder ein irreduzibler Faktor von r_m noch von s_n ist, folgt aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren, dass p den Koeffizienten c_{m+n} nicht teilt.

Definition 132 : Zwei Elemente a und b von R heißen *teilerfremd*, wenn sie keinen gemeinsamen irreduziblen Faktor haben, das heißt: es gibt kein irreduzibles Element von R, das sowohl a als auch b teilt.

Beispiel 133 : Im Ring der ganzen Zahlen oder im Polynomring über einem Körper sind zwei Elemente genau dann teilerfremd, wenn ihr größter gemeinsamer Teiler gleich 1 ist.

Satz 134 : *Es sei K der Quotientenkörper des faktoriellen Ringes R. Wir fassen $R[x]$ als Teilmenge von $K[x]$ auf.*

(1) *Es seien $f \in R[x]$ und $g,h \in K[x]$ so, dass $f = g \cdot h$ ist. Dann gibt es ein Element $0 \neq c \in K$ so, dass $c^{-1} \cdot g \in R[x]$, $c \cdot h \in R[x]$ und $c \cdot h$ primitiv ist.*
(2) *Die Menge der irreduziblen Polynome in $R[x]$ ist die Vereinigung der Menge der irreduziblen Elemente von R und der Menge der primitiven Polynome in $R[x]$, die in $K[x]$ irreduzibel sind.*
(3) *Der Polynomring mit Koeffizienten in R ist faktoriell.*

Beweis:

(1) Seien $a,b \in R \setminus \{0\}$ so, dass $a \cdot g \in R[x]$ und $b \cdot h \in R[x]$ ist. Seien g_1, h_1 primitive Polynome in $R[x]$ und $r,s \in R$ so, dass

$$a \cdot g = r \cdot g_1 \text{ und } b \cdot h = s \cdot h_1 .$$

Dann ist

$$a \cdot b \cdot f = r \cdot s \cdot g_1 \cdot h_1 .$$

Es seien $u,v,w \in R$ so, dass

$$a \cdot b = u \cdot v , \quad r \cdot s = u \cdot w$$

und dass v und w teilerfremd sind (u ist das Produkt der gemeinsamen irreduziblen Faktoren von $a \cdot b$ und $r \cdot s$). Dann ist

$$v \cdot f = w \cdot g_1 \cdot h_1 .$$

Wir nehmen an, es gäbe einen irreduziblen Faktor $p \in R$ von v. Dann teilt p alle Koeffizienten von $w \cdot g_1 \cdot h_1$. Nach Satz 131 ist $g_1 \cdot h_1$ primitiv, also wird ein Koeffizient von $g_1 \cdot h_1$ nicht von p geteilt. Somit wäre p ein irreduzibler Faktor von w, Widerspruch. Daher ist v in R invertierbar und

$$\frac{r \cdot s}{a \cdot b} = \frac{w}{v} \in R .$$

Sei $c := \frac{b}{s}$. Dann ist

$$c^{-1} \cdot g = \frac{r}{a} \cdot \frac{s}{b} \cdot g_1 \in R[x] \text{ und } c \cdot h = h_1 \in R[x] .$$

(2) Es ist klar, dass jedes irreduzible Polynom vom Grad 0 in R[x] ein irreduzibles Element von R ist und umgekehrt. Weiters ist jedes primitive Polynom in $R[x]$, das in $K[x]$ irreduzibel ist, auch in $R[x]$ irreduzibel. Seien nun f ein irreduzibles Polynom in $R[x]$ mit positivem Grad und g,h Polynome in $K[x]$ mit $f = g \cdot h$. Nach (1) ist dann $f = (c^{-1} \cdot g) \cdot (c \cdot h)$ mit $c \in K$, $c^{-1} \cdot g \in R[x]$ und $c \cdot h \in R[x]$. Da f in $R[x]$ irreduzibel ist, ist $c^{-1} \cdot g$ oder $c \cdot h$ in $R[x]$ (und damit auch in $K[x]$) invertierbar. Somit ist f auch in $K[x]$ irreduzibel.

(3) Es sei $0 \neq f \in R[x]$. Nach Satz 122 gibt es irreduzible Polynome $f_1, \ldots, f_n$ in $K[x]$ so, dass

$$f = \prod_{i=1}^{n} f_i$$

ist. Nach (1) gibt es $c_1, \ldots, c_n \in K$ mit $\prod_{i=1}^{n} c_i = 1$ und

$$c_1 \cdot f_1 \in R[x], \ldots, c_n \cdot f_n \in R[x] .$$

Seien $g_1, \ldots, g_n$ primitive Polynome in $R[x]$ und $r_1, \ldots, r_n \in R$ so, dass

$$r_i \cdot g_i = c_i \cdot f_i, 1 \leq i \leq n,$$

ist. Da R ein faktorieller Ring ist, ist $\prod_{i=1}^{n} r_i$ das Produkt von irreduziblen Elementen $s_1, \ldots, s_m \in R$. Mit (2) folgt nun, dass

$$f = s_1 \cdot \ldots \cdot s_m \cdot \prod_{i=1}^{n} g_i$$

eine Zerlegung von f in irreduzible Faktoren in $R[x]$ ist. Die Eindeutigkeit der Faktoren (bis auf die Reihenfolge und bis auf Assoziiertheit) folgt aus der der entsprechenden Elemente von $K[x]$ und R.

Satz 135: *Es seien K der Quotientenkörper von R und $f \in R[x]$ ein normiertes Polynom mit $f(0) \neq 0$. Dann ist jede Nullstelle von f in K ein Element von R, das $f(0) \in R$ teilt. Insbesondere: Jede Nullstelle in $\mathbb{Q}$ eines normierten Polynoms in $\mathbb{Z}[x]$ ist eine ganze Zahl.*

Beweis: Es sei $c := \frac{a}{b} \in K$ eine Nullstelle des normierten Polynoms $f \in R[x]$. Dabei können wir annehmen, dass die Elemente a und b in R teilerfremd sind. Dann ist das Polynom $bx - a$ primitiv und ein Teiler von f in $K[x]$. Nach Satz 134 (1) ist $bx - a$ auch in $R[x]$ ein Teiler von f. Daher gibt es ein Polynom $g \in R[x]$ so, dass $f = g \cdot (bx - a)$ ist. Somit ist b ein Teiler von $lk(f) = 1$ in R, also ist b in R invertierbar und $c \in R$. Weiters ist $0 \neq f(0) = g(0) \cdot (-a) = (-b \cdot g(0)) \cdot c$.

Beispiel 136: Es seien $n \geq 2$ eine ganze Zahl und p eine Primzahl. Dann hat $x^n - p$ in $\mathbb{Q}$ keine Nullstellen. Denn: Die Teiler $p, -p, 1, -1$ von p sind keine Nullstellen dieses Polynoms.
Insbesondere ist $\sqrt[n]{p}$ keine rationale Zahl.

§9. Die Anzahl der komplexen Nullstellen eines Polynoms

In diesem Abschnitt sei K ein Körper. Im Satz 91 wurde eine obere Schranke für die Anzahl der Nullstellen eines Polynoms angegeben, diese kann aber viel zu groß sein. Zum Beispiel hat das Polynom x^n für jedes $n \in \mathbb{N}$ in K nur eine Nullstelle.

Definition 137: Es seien $f \neq 0$ ein Polynom mit Koeffizienten in K und a eine Nullstelle von f in K. Die *Vielfachheit der Nullstelle a von f* ist die größte ganze Zahl n mit der Eigenschaft, dass $(x-a)^n$ ein Teiler von f ist. Eine Nullstelle ist *einfach*, wenn ihre Vielfachheit 1 ist, und *mehrfach*, wenn ihre Vielfachheit größer als 1 ist.

Beispiel 138 : 0 ist eine Nullstelle von x^{10} mit Vielfachheit 10.

Satz 139 : *Die Funktion*

$$D : K[x] \longrightarrow K[x] \quad , \quad \sum_{i=0}^{n} c_i x^i \longmapsto \sum_{i=1}^{n} i c_i x^{i-1}$$

heißt Differentiation *oder* Ableitung. *Sie ist K-linear und erfüllt die* Produktregel

$$\text{für alle Polynome } f,g \text{ ist } D(f \cdot g) = f \cdot D(g) + D(f) \cdot g \ .$$

Insbesondere ist für alle positiven ganzen Zahlen k und alle Polynome $f \in K[x]$

$$D(f^k) = k \cdot f^{k-1} \cdot D(f) \ .$$

Beweis: Übung.

Definition 140 : Es seien R ein Ring mit Einselement 1. Durch

$$a \cdot r := \underbrace{vz(a)r + \ldots + vz(a)r}_{|a| \text{ Summanden}}$$

für $a \in \mathbb{Z}$ und $r \in R$ wird R zu einem $\mathbb{Z}$-Modul. „Jeder Ring ist ein $\mathbb{Z}$-Modul."
Wenn für alle positiven ganzen Zahlen n gilt: $n \cdot 1 \neq 0$, dann ist R ein Ring der *Charakteristik* 0. Schreibweise: $char(R) = 0$.
Wenn es eine positive ganze Zahl n mit $n \cdot 1 = 0$ gibt und p die kleinste positive ganze Zahl mit dieser Eigenschaft ist, dann ist R ein Ring der *Charakteristik p*. Schreibweise: $char(R) = p$.

Beispiel 141 : Die Ringe $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben Charakteristik 0, der Ring $\mathbb{Z}_n$ hat Charakteristik n. Die Charakteristik des Polynomrings $R[x]$ ist die Charakteristik von R.

Satz 142 : *Es sei $f \neq 0$ ein Polynom mit Koeffizienten in K.*

(1) *Ein Element $a \in K$ ist genau dann eine mehrfache Nullstelle von f, wenn*

$$f(a) = 0 \quad \textit{und} \quad D(f)(a) = 0$$

ist.

(2) *Wenn $char(K) = 0$ ist, dann hat das Polynom*

$$\frac{f}{ggT(f, D(f))}$$

nur einfache Nullstellen und zwar genau die Nullstellen von f.

(3) *Wenn* $char(K) = 0$ *ist, dann hat das Polynom* f *höchstens*

$$\mathrm{gr}(f) - \mathrm{gr}(ggT(f, D(f)))$$

Nullstellen in K.

Beweis:

(1) Wenn a eine mehrfache Nullstelle von f ist, dann gibt es ein Polynom $h \in K[x]$ so, dass $f = (x-a)^2 \cdot h$ ist. Dann ist

$$D(f) = 2(x-a) \cdot h + (x-a)^2 \cdot D(h) =$$

$$= (x-a) \cdot (2h + (x-a) \cdot D(h)) \ ,$$

also a eine Nullstelle von $D(f)$.
Sei nun umgekehrt a eine Nullstelle von f und von $D(f)$. Wir dividieren f mit Rest durch $(x-a)^2$:

$$f = m \cdot (x-a)^2 + r \ , \ \mathrm{gr}(r) < 2 \ .$$

Dann ist

$$D(f) = D(m) \cdot (x-a)^2 + 2m \cdot (x-a) + D(r) \ .$$

Aus $f(a) = 0$ folgt $0 = r(a)$, also ist $r = 0$ oder $r = lk(r) \cdot (x-a)$. Aus $D(f)(a) = 0$ folgt $D(r) = 0$. Daher ist $r = 0$ und $(x-a)^2$ ein Teiler von f.

(2) Sei a eine Nullstelle von f und n ihre Vielfachheit. Dann gibt es ein Polynom h mit $f = (x-a)^n \cdot h$ und $h(a) \neq 0$. Wegen

$$D(f) = n \cdot (x-a)^{n-1} \cdot h + (x-a)^n \cdot D(h) =$$

$$= (x-a)^{n-1} \cdot (n \cdot h + (x-a) \cdot D(h))$$

wird $ggT(f, D(f))$ von $(x-a)^{n-1}$ geteilt. Wegen $h(a) \neq 0$ und weil $char(K) = 0$ ist, wird $n \cdot h + (x-a) \cdot D(h)$ nicht von $(x-a)$ geteilt. Somit werden $D(f)$ und $ggT(f, D(f))$ nicht von $(x-a)^n$ geteilt. Daher ist a eine einfache Nullstelle von $\frac{f}{ggT(f, D(f))}$.

(3) folgt aus (2).

Beispiel 143 : $f = (x-2)^2(x-3)^3 \in \mathbb{C}[x]$

$$\begin{aligned} D(f) &= 2(x-2)(x-3)^2 + 3(x-2)(x-3)^2 = \\ &= (x-2)(x-3)^2 \cdot (2(x-3) + 3(x-2)) = \\ &= (x-2)(x-3)^2 \cdot (5x-12) \\ ggT(f, D(f)) &= (x-2)(x-3)^2 \\ \frac{f}{ggT(f, D(f)} &= (x-2)(x-3) \end{aligned}$$

Satz 144 : *Die Anzahl der Nullstellen eines Polynoms* $0 \neq f \in \mathbb{C}[x]$ *in* $\mathbb{C}$ *ist*

$$\mathrm{gr}(f) - \mathrm{gr}(ggT(f, D(f))) \ .$$

Beweis: Folgt aus den Sätzen 125 und 142.

§10. Lineare Differenzengleichungen

In diesem Abschnitt sei K ein Körper und n eine positive ganze Zahl. Mit $\mathcal{F}(\mathbb{N}, K)$ bezeichnen wir die K-Algebra aller Funktionen von $\mathbb{N}$ nach K (bzw. Folgen in K).

Definition 145 : Eine *lineare Differenzengleichung (der Ordnung n)* ist die folgende Aufgabe:
Gegeben sind Elemente $c_0, c_1, \ldots, c_n \in K$ mit $c_n \neq 0$ und eine Funktion $h \in \mathcal{F}(\mathbb{N}, K)$.
Gesucht sind alle Funktionen $f \in \mathcal{F}(\mathbb{N}, K)$ so, dass für alle $k \in \mathbb{N}$

$$c_0 f(k) + c_1 f(k+1) + \ldots + c_n f(k+n) = h(k)$$

ist. Diese Funktionen f heißen Lösungen der Differenzengleichung. Wenn $h = 0$ ist, heißt die Differenzengleichung *homogen*.

Definition 146 : Für $\ell \in \mathbb{N}$ und $f \in \mathcal{F}(\mathbb{N}, K)$ sei $x^\ell \circ f \in \mathcal{F}(\mathbb{N}, K)$ durch

$$\text{für alle } k \in \mathbb{N} \text{ ist } (x^\ell \circ f)(k) := f(k+\ell)$$

definiert.
Für $p := \sum_{i=0}^{n} c_i x^i$ und $f \in \mathcal{F}(\mathbb{N}, K)$ sei

$$p \circ f := \sum_{i=0}^{n} c_i (x^i \circ f) \in \mathcal{F}(\mathbb{N}, K)$$

(also: für alle $k \in \mathbb{N}$ ist $(p \circ f)(k) = \sum_{i=0}^{n} c_i f(k+i)$).
Sprechweise: „die durch p und h gegebene lineare Differenzengleichung“ bedeutet „die durch $c_0, c_1, \ldots, c_n$ und h gegebene lineare Differenzengleichung“.

Satz 147 :

(1) *Durch* $K[x] \times \mathcal{F}(\mathbb{N}, K) \longrightarrow \mathcal{F}(\mathbb{N}, K)$, $(p, f) \longmapsto p \circ f$, *wird* $\mathcal{F}(\mathbb{N}, K)$ *ein* $K[x]-$*Modul.*

(2) *Für* $p \in K[x]$ *ist die Funktion*

$$p \circ (-) : \mathcal{F}(\mathbb{N}, K) \longrightarrow \mathcal{F}(\mathbb{N}, K), \ f \longmapsto p \circ f,$$

K-linear.

(3) *Sei $p \in K[x]$ und $h \in \mathcal{F}(\mathbb{N},K)$. Dann ist das Urbild von h unter $p \circ (-)$ die Menge der Lösungen der durch p und h gegebenen linearen Differenzengleichung.*
(4) *Die Menge der Lösungen einer homogenen linearen Differenzengleichung ist ein K-Untervektorraum von $\mathcal{F}(\mathbb{N},K)$.*
(5) *Wenn f (irgend)eine Lösung der durch p und h gegebenen linearen Differenzengleichung ist, dann erhält man alle Lösungen, indem man beliebige Lösungen der durch p gegebenen homogenen linearen Differenzengleichung zu f addiert.*

Beweis:

(1) Sei $f \in \mathcal{F}(\mathbb{N},K)$. Für $k,m \in \mathbb{N}$ ist
$$(x^\ell \circ (x^m \circ f))(k) = (x^m \circ f)(k+\ell) =$$
$$= f(k+\ell+m) = ((x^{\ell+m}) \circ f)(k),$$
daraus folgt für alle Polynome $p,q \in K[x]$ leicht
$$p \circ (q \circ f) = (pq) \circ f \ (= (qp) \circ f).$$
Die anderen Rechenregeln eines Moduls sind leicht nachzuprüfen.
(2) folgt aus (1).
(3) folgt aus der Definition von $p \circ f$.
(4) folgt aus (2) und (3).
(5) folgt aus (4).

Satz 148 : *Seien $p = \sum_{i=0}^{n} c_i x^i \in K[x]$, $\mathrm{gr}(p) = n$, $h \in \mathcal{F}(\mathbb{N},K)$ und $d_0,\ldots,d_{n-1} \in K$. Dann gibt es genau eine Lösung f der durch p und h gegebenen Differenzengleichung mit $f(i) = d_i$, $0 \le i \le n-1$. Insbesondere ist die K-Dimension des Lösungsraums dieser Differenzengleichung gleich n.*

Beweis: Wir definieren die Funktion f induktiv durch
$$f(0) := d_0, \ldots, f(n-1) := d_{n-1},$$
und für $k \ge n$:
$$f(k) := c_n^{-1} \cdot (h(k-n) - \sum_{i=0}^{n-1} c_i f(k-n+i)).$$
Dann ist f eine Lösung mit den vorgegebenen Funktionswerten $d_0,d_1,\ldots,d_{n-1}$ in $0,1,\ldots,n-1$.

Beispiel 149 : Die Lösung f der durch x^2-x-1 gegebenen homogenen linearen Differenzengleichung mit $f(0) = 0$ und $f(1) = 1$ heißt *Folge der Fibonacci-Zahlen*. Für $k \ge 2$ ist $f(k) = f(k-1) + f(k-2)$.

Definition 150 : Für $r, a \in K$ sei

$$r \cdot a^{(-)} : \mathbb{N} \longrightarrow K,\ m \longmapsto r \cdot a^m$$

die *geometrische Folge mit Anfangsglied r und Quotient a.*

Beispiel 151 : Sei $a \in K$. Dann ist $r \cdot a^{(-)}$ die Lösung der durch $x - a$ gegebenen homogenen linearen Differenzengleichung, deren Funktionswert in 0 gleich r ist.

Beispiel 152 : Seien $a_1, \ldots, a_n \in K$ paarweise verschieden und sei

$$p := \prod_{i=1}^{n} (x - a_i)\,.$$

Dann bilden die Funktionen $a_i^{(-)},\ 1 \leq i \leq n$ eine Basis des K-Untervektorraums von $\mathcal{F}(\mathbb{N}, K)$ aller Lösungen der durch p gegebenen homogenen linearen Differenzengleichung.
Denn: Für $1 \leq j \leq n$ ist

$$p \circ a_j^{(-)} = (\prod_{i \neq j} (x - a_i)) \circ ((x - a_j) \circ a_j^{(-)}) = 0\,.$$

Weil $a_1, \ldots, a_n \in K$ paarweise verschieden sind, sind die Funktionen $a_i^{(-)}$, $1 \leq i \leq n$, linear unabhängig, nach Satz 148 bilden sie daher eine Basis.

Die Lösungen von linearen Differenzengleichungen sind Folgen. Wie beschreibt man eine Folge durch endlich viele Daten? Eine Möglichkeit dazu ist: ein Verfahren angeben, mit dem man für jedes $k \in \mathbb{N}$ in endlich vielen Schritten $f(k)$ berechnen kann.

Satz 153 : *Seien $p = \sum_{i=0}^{n} c_i x^i \in K[x]$, $\mathrm{gr}(p) = n$, $h \in \mathcal{F}(\mathbb{N}, K)$ und $d_0, \ldots, d_{n-1} \in K$. Sei f die eindeutig bestimmte Lösung der durch p und h gegebenen linearen Differenzengleichung mit $f(i) = d_i$, $0 \leq i \leq n-1$. Für $k \geq n$ kann $f(k)$ wie folgt berechnet werden:*

Dividiere x^k mit Rest durch p:
$x^k = m_k \cdot p + r_k$ und ($r_k = 0$ oder $\mathrm{gr}(r_k) < n$).
Sei r_{ki} der Koeffizient von r_k bei x^i, $0 \leq i \leq n-1$.
Dann ist $f(k) = (m_k \circ h)(0) + \sum_{i=0}^{n-1} r_{ki} d_i$.

Beweis:

$$f(k) = (x^k \circ f)(0) = ((m_k \cdot p + r_k) \circ f)(0) =$$

$$= (m_k \circ (p \circ f))(0) + (r_k \circ f)(0) = (m_k \circ h)(0) + \sum_{i=0}^{n-1} r_{ki} d_i.$$

Beispiel 154 : Sei f die Fibonacci-Folge. Der Rest von x^{100} nach Division durch $x^2 - x - 1$ ist $354224848179261915075x + 218922995834555169026$, wegen $f(0) = 0$ und $f(1) = 1$ ist $f(100) = 354224848179261915075$.

Beispiel 155 : Homogene lineare Differenzengleichungen 1. Ordnung

Seien a und c reelle Zahlen. Berechne eine Folge f mit

$$(x - c) \circ f = 0 \quad \text{und} \quad f(0) = a \ !$$

Anders formuliert: Für alle $j \in \mathbb{N}$ sei

$$f(j+1) - c \cdot f(j) = 0 \quad \text{und} \quad f(0) = a\,.$$

Division mit Rest von x^j durch $x - c$ ergibt

$$x^j = m_j \cdot (x - c) + r_j \qquad \text{und} \qquad r_j \in \mathbb{R}\,.$$

Einsetzen von c für x ergibt

$$c^j = 0 + r_j\,,$$

also ist für alle $j \in \mathbb{N}$

$$f(j) = c^j \cdot a\,.$$

Beispiel 156 : Inhomogene lineare Differenzengleichungen 1. Ordnung

Seien a und c reelle Zahlen und h eine Folge in $\mathbb{R}$. Berechne eine Folge f mit

$$(x - c) \circ f = h \quad \text{und} \quad f(0) = a \ !$$

Anders formuliert: Für alle $j \in \mathbb{N}$ sei

$$f(j+1) - c \cdot f(j) = h(j) \quad \text{und} \quad f(0) = a\,.$$

Wie vorhin erhalten wir

$$x^j = m_j \cdot (x - c) + c^j\,.$$

Daher ist

$$m_j = \frac{x^j - c^j}{x - c} = \sum_{\ell=0}^{j-1} c^\ell \cdot x^{j-1-\ell}\,,$$

somit ist für alle $j \in \mathbb{N}$

$$f(j) = \sum_{\ell=0}^{j-1} c^\ell \cdot h(j-1-\ell) + c^j \cdot a\,.$$

Beispiel 157 : Homogene lineare Differenzengleichungen 2. Ordnung

Seien $a_0, a_1 \in \mathbb{R}$, $p := x^2 + c_1 x + c_0 \in \mathbb{R}[x]$ und x_1, x_2 Nullstellen von p. Berechne eine Folge f mit

$$p \circ f = 0, f(0) = a_0 \text{ und } f(1) = a_1 !$$

Sei $j \in \mathbb{N}$. Division mit Rest von x^j durch $p = (x - x_1)(x - x_2)$ ergibt

$$x^j = m_j \cdot (x - x_1)(x - x_2) + r_j \quad \text{und} \quad [r_j = 0 \text{ oder } grad(r_j) \leq 1].$$

Sei $r_j = r_{j_1} x + r_{j_0}$ mit $r_{j_0}, r_{j_1} \in \mathbb{R}$. Setzen wir x_1 bzw. x_2 für x ein, so erhalten wir

$$x_1^j = 0 + r_{j_1} x_1 + r_{j_0}$$

bzw.

$$x_2^j = 0 + r_{j_1} x_2 + r_{j_0}.$$

Falls $x_1 \neq x_2$ **ist**, folgt daraus

$$r_{j_1} = \frac{x_1^j - x_2^j}{x_1 - x_2}$$

und

$$r_{j_0} = \frac{x_1 x_2^j - x_1^j x_2}{x_1 - x_2}.$$

Das j - te Folgenglied $f(j)$ der Lösung f dieser Differenzengleichung ist also

$$f(j) = \frac{x_1^j - x_2^j}{x_1 - x_2} a_1 + \frac{x_1 x_2^j - x_1^j x_2}{x_1 - x_2} a_0 = \frac{a_1 - a_0 x_2}{x_1 - x_2} x_1^j + \frac{a_0 x_1 - a_1}{x_1 - x_2} x_2^j.$$

Falls $x_1 = x_2$ **ist**, gilt wie oben

$$x_1^j = 0 + r_{j_1} x_1 + r_{j_0}.$$

Eine zweite Bedingung für die Koeffizienten von r_j erhalten wir, indem wir $x^j = m_j \cdot (x - x_1)^2 + r$ nach x ableiten und dann für x die Zahl x_1 einsetzen:

$$j x_1^{j-1} = 0 + r_{j_1}.$$

In diesem Fall ist also

$$f(j) = j x_1^{j-1} a_1 + (1 - j) x_1^j a_0 = (1 - j) a_0 x_1^j + j a_1 x_1^{j-1}.$$

Beispiel 158 : Die Formel von Binet

Die Fibonacci-Folge f ist die Lösung einer homogenen linearen Differenzengleichung 2. Ordnung. Nach Beispiel 157 können wir daher ihre Folgenglieder mit Hilfe der Nullstellen von $x^2 - x - 1$ darstellen. Diese sind $\frac{1+\sqrt{5}}{2}$

und $\frac{1-\sqrt{5}}{2}$. Mit Beispiel 157 erhalten wir die *Formel von Binet*:

$$f(j) = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^j - \left(\frac{1-\sqrt{5}}{2} \right)^j \right].$$

Nach Beispiel 154 ist dann

$$354224848179261915075 = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{100} - \left(\frac{1-\sqrt{5}}{2} \right)^{100} \right].$$

§11. Quotientenkörper

Definition 159 : Eine *Äquivalenzrelation auf einer Menge M* ist eine Teilmenge $E \subseteq M \times M$ mit den folgenden Eigenschaften:

- Für alle $m \in M$ ist $(m,m) \in E$ (E ist *reflexiv*).
- Für alle $m,n \in M$ folgt aus $(m,n) \in E$, dass auch $(n,m) \in E$ ist (E ist *symmetrisch*).
- Für alle $m,n,p \in M$ folgt aus $(m,n) \in E$ und $(n,p) \in E$, dass auch $(m,p) \in E$ ist (E ist *transitiv*).

Statt $(m,n) \in E$ wird auch $m \sim n$ geschrieben (Sprechweise: m und n sind äquivalent). Für $m \in M$ heißt die Menge

$$\bar{m} := \{n \in M \mid m \sim n\} = \{n \in M \mid (m,n) \in E\}$$

die *Äquivalenzklasse* von m bezüglich E bzw. $\sim$.
Mit $M/\sim := \{\bar{m} \mid m \in M\}$ wird die Menge aller Äquivalenzklassen bezüglich $\sim$ bezeichnet.

Satz 160 : *Es sei $\sim$ eine Äquivalenzrelation auf M. Der Durchschnitt von zwei verschiedenen Äquivalenzklassen ist leer.*

Beweis: Es seien $\bar{m}$ und $\bar{n}$ zwei Äquivalenzklassen. Wenn es ein $k \in M$ mit $k \in \bar{m}$ und $k \in \bar{n}$ gibt, dann ist $m \sim k$ und $n \sim k$. Daraus folgt $m \sim n$, also $\bar{m} = \bar{n}$.

Beispiel 161 : Durch $(a,b) \sim (c,d) :\Leftrightarrow ad = bc$ wird eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definiert. Die Bruchzahl $\frac{a}{b}$ ist die Äquivalenzklasse von (a,b). $\mathbb{Q}$ ist die Menge der Äquivalenzklassen.

Beispiel 162 : Es seien $\underline{v}$ und $\underline{w}$ Basen eines reellen endlich-dimensionalen Vektorraums V. Durch

$\underline{v} \sim \underline{w}$ $:\Leftrightarrow$ es gibt eine invertierbare Matrix T, mit $\det(T) > 0$ so, dass $\underline{w} = \underline{v}T$ ist

wird eine Äquivalenzrelation auf der Menge aller Basen von V definiert. Es gibt genau zwei Äquivalenzklassen, diese sind die zwei Orientierungen von V.

Satz 163 : *R sei ein Integritätsbereich.*

(1) *Für $a,b,c \in R$ mit $c \neq 0$ folgt aus $ac = bc$, dass $a = b$ ist. („In Integritätsbereichen kann gekürzt werden").*
(2) *Durch $(a,b) \sim (c,d) :\Leftrightarrow ad = bc$ ist auf $R \times (R \setminus \{0\})$ eine Äquivalenzrelation definiert.*

Beweis:

(1) Aus $ac = bc$ folgt $0 = ac - bc = (a-b)c$, wegen $c \neq 0$ ist daher $a - b = 0$.
(2) Die Relation ist reflexiv und symmetrisch. Sind $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$, dann ist $ad = bc$ und $cf = de$, also $fad = fbc = bde$ und $d(af - be) = 0$. Wegen $d \neq 0$ folgt daraus $af = be$, daher ist $(a,b) \sim (e,f)$ und die Relation transitiv.

In einem Integritätsbereich kann addiert, subtrahiert, multipliziert, aber im allgemeinen nicht dividiert werden. Um diesen Nachteil zu beheben, konstruiert man einen Körper, der (bis auf Identifikation) den Integritätsbereich enthält und dessen Rechenoperationen unverändert lässt.

Definition 164 : Es seien R ein Integritätsbereich, $a \in R$ und $b \in R \setminus \{0\}$. Die Menge

$$\frac{a}{b} := \{(c,d) \mid c,d \in R, ad = bc, d \neq 0\}$$

heißt der durch den „Zähler" a und den „Nenner" b gegebene *Bruch* (oder *Quotient* von a und b). Wir schreiben $\mathrm{Quot}(R)$ für die Menge der Brüche von R, also für die Menge der Äquivalenzklassen der durch

$$(a,b) \sim (c,d) :\Leftrightarrow ad = bc$$

auf $R \times (R \setminus \{0\})$ definierten Äquivalenzrelation.
Für den Bruch $\frac{a}{1}$ schreiben wir oft nur a und fassen so R als Teilmenge von $\mathrm{Quot}(R)$ auf.

Satz 165 : (Quotientenkörper eines Integritätsbereiches)
Es seien R ein Integritätsbereich und $Quot(R)$ die Menge seiner Brüche. Die Funktionen

$$+ : Quot(R) \times Quot(R) \longrightarrow Quot(R) , \quad (\frac{a}{b}, \frac{c}{d}) \longmapsto \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} ,$$

und

$$\cdot : Quot(R) \times Quot(R) \longrightarrow Quot(R) \ , \quad (\frac{a}{b}, \frac{c}{d}) \longmapsto \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} \ ,$$

sind wohldefiniert. Mit diesen Rechenoperationen ist $Quot(R)$ ein Körper und heißt Quotientenkörper *von R. Wenn $\frac{a}{b} \neq 0$, dann ist*

$$(\frac{a}{b})^{-1} = \frac{b}{a} \ .$$

Die Einschränkungen von $+$ und $\cdot$ auf $R \times R$ stimmen mit der Addition und der Multiplikation auf R überein.

Beweis: Wir müssen zuerst zeigen, dass die Funktionen $+$ und $\cdot$ wohldefiniert sind, das heißt: wenn $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{c'}$ ist, dann muss auch

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \quad \text{und} \quad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

sein.
Aus $a'b = ab'$ und $c'd = cd'$ folgt

$$(ad+bc)b'd' = a'bdd' + bb'c'd = bd(a'd' + b'c')$$

und

$$(ac)b'd' = bd(a'c') \ .$$

Die Rechenregeln eines Körpers können leicht nachgeprüft werden.

Beispiel 166 : Der Quotientenkörper von $\mathbb{Z}$ ist der Körper der rationalen Zahlen.

§12. Rationale Funktionen

In diesem Abschnitt seien R ein Integritätsbereich und K sein Quotientenkörper.

Definition 167 : Der Quotientenkörper von $R[x]$ heißt *Körper der rationalen Funktionen* und wird mit $K(x)$ bezeichnet. Seine Elemente heißen *rationale Funktionen mit Koeffizienten in K*.

Es seien $a,b,c,d \in R$, $b \neq 0$, $c \neq 0$, $d \neq 0$ und $f,g \in R[x]$, $g \neq 0$. Dann ist

$$\frac{\frac{a}{b} \cdot f}{\frac{c}{d} \cdot g} = \frac{ad \cdot f}{bc \cdot g} \ ,$$

also können die Quotientenkörper von $R[x]$ und $K[x]$ als gleich aufgefasst werden.

Es seien $f,g \in K[x]$, $g \neq 0$ und m bzw. r der polynomiale Quotient bzw. Rest von f nach Division durch g. Dann ist

$$\frac{f}{g} = \frac{m}{1} + \frac{r}{g} = m + \frac{r}{g} ,$$

also kann jede rationale Funktion als Summe eines Polynoms und einer rationalen Funktion, deren Zähler einen kleineren Grad als der Nenner hat, geschrieben werden.

Es ist sehr empfehlenswert, jede rationale Funktion vor jeder Rechenoperation durch den größten gemeinsamen Teiler von Zähler und Nenner zu kürzen.

Im Gegensatz zu Polynomen kann rationalen Funktionen nicht eine Funktion von K nach K zugeordnet werden (obwohl der Name rationale *Funktion* das nahelegt). Wenn f,g Polynome sind, $g \neq 0$, und N die Menge der Nullstellen von g ist, dann wird durch die rationale Funktion $\frac{f}{g}$ die Funktion

$$K \setminus N \longrightarrow K \ , \ z \longmapsto \frac{f}{g}(z) := \frac{f(z)}{g(z)} ,$$

definiert.

Sind $\frac{f_1}{g_1} : K \setminus N_1 \to K$ und $\frac{f_2}{g_2} : K \setminus N_2 \to K$ rationale Funktionen, dann bezeichnen wir mit $\frac{f_1}{g_1} + \frac{f_2}{g_2}$ die rationale Funktion

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} : K \setminus (N_1 \cup N_2) \longrightarrow K \ , \ z \longmapsto \frac{f_1(z)}{g_1(z)} + \frac{f_2(z)}{g_2(z)} .$$

.

Satz 168 : *Es seien f,g,h von Null verschiedene Polynome mit Koeffizienten in K so, dass $\mathrm{gr}(g) > 0$, $\mathrm{gr}(h) > 0$, $ggT(g,h) = 1$ und $\mathrm{gr}(f) < \mathrm{gr}(gh)$ ist. Dann gibt es eindeutig bestimmte Polynome u und v so, dass*

$$\mathrm{gr}(u) < \mathrm{gr}(h) \ , \ \mathrm{gr}(v) < gr(g)$$

und

$$\frac{f}{gh} = \frac{u}{h} + \frac{v}{g}$$

ist. Die Polynome u und v können wie folgt berechnet werden:

- *Berechne mit dem erweiterten Euklidischen Algorithmus Polynome $s,t \in K[x]$ so, dass $sg + th = 1$ ist.*
- *Dann ist u bzw. v der Rest von fs bzw. ft nach Division durch h bzw. g.*

Beweis: Es sei p bzw. q der polynomiale Quotient von fs bzw. ft und h bzw. g. Dann ist $fs = ph + u$ und $ft = qg + v$. Aus $(fs)g + (ft)h = f$ folgt dann

$$(p+q)gh + ug + vh = f .$$

Wäre $p+q \neq 0$, dann würde wegen

$$\mathrm{gr}((p+q)gh) = \mathrm{gr}(p+q) + \mathrm{gr}(gh) > \mathrm{gr}(ug+vh)$$

auch

$$\mathrm{gr}(f) = \mathrm{gr}(p+q)gh \geq \mathrm{gr}(gh)$$

gelten, was im Widerspruch zur Annahme steht. Daher ist

$$ug+vh = f$$

und somit

$$\frac{f}{gh} = \frac{ug+vh}{gh} = \frac{u}{h} + \frac{v}{g} .$$

Wenn u' und v' Polynome mit $\mathrm{gr}(u') < \mathrm{gr}(h)$, $\mathrm{gr}(v') < gr(g)$ und

$$\frac{f}{gh} = \frac{u'}{h} + \frac{v'}{g}$$

sind, dann ist

$$\frac{u}{h} + \frac{v}{g} = \frac{u'}{h} + \frac{v'}{g} ,$$

also

$$(v-v')h = (u'-u)g .$$

Wenn $(v-v') = 0$ ist, dann ist $v = v'$ und $u = u'$.
Wäre $(v-v') \neq 0$, dann folgt aus $ggT(g,h) = 1$, dass g ein Teiler von $v-v'$ ist, also $\mathrm{gr}(g) \leq \mathrm{gr}(v-v') \leq \mathrm{gr}(v)$. Widerspruch zu $\mathrm{gr}(v) < gr(g)$.

Beispiel 169 :

$$\frac{1}{(x-1)(x^2-2)} = \frac{-(x^2-2)+(1+x)(x-1)}{(x-1)(x^2-2)} = \frac{-1}{x-1} + \frac{x+1}{x^2-2}$$

Satz 170 : *Es seien f,g Polynome mit Koeffizienten in K, $g \neq 0$ und n eine positive ganze Zahl. Dann gibt es eindeutig bestimmte Polynome $f_0, f_1, \ldots, f_n$ mit Koeffizienten in K so, dass*

$$\frac{f}{g^n} = \sum_{i=0}^{n} \frac{f_i}{g^i}$$

und

$$f_i = 0 \text{ oder } \mathrm{gr}(f_i) < \mathrm{gr}(g) \ , \ 1 \leq i \leq n,$$

ist. Diese Polynome können wie folgt berechnet werden:

- *Sei $i := 0$ und $h_0 := f$.*
- *Solange $i \neq n+1$: Dividiere h_i mit Rest durch g. Es seien h_{i+1} der polynomiale Quotient und r_i der Rest von h_i nach Division durch g. Setze*

$$f_{n-i} := r_i \text{ und } i := i+1 .$$

Beweis: Wir zeigen zuerst die Existenz dieser Zerlegung durch Induktion über n. Wenn $n = 1$, dann ist

$$\frac{f}{g} = h_1 + \frac{r_0}{g} = h_1 + \frac{f_1}{g} \ .$$

Wenn $n > 1$, dann ist

$$\frac{f}{g^n} = \frac{h_1}{g^{n-1}} + \frac{r_0}{g^n} = \frac{h_1}{g^{n-1}} + \frac{f_n}{g} \ .$$

Die Behauptung folgt nun nach Anwendung der Induktionsannahme auf

$$\frac{h_1}{g^{n-1}} \ .$$

Seien $f_0', f_1', \ldots, f_n'$ in $K[x]$ so, dass

$$\frac{f}{g^n} = \sum_{i=0}^{n} \frac{f_i'}{g^i}$$

und

$$f_i' = 0 \text{ oder } \operatorname{gr}(f_i') < \operatorname{gr}(f) \ , \ 1 \leq i \leq n,$$

ist.

Dann ist

$$\sum_{i=0}^{n} \frac{f_i}{g^i} = \sum_{i=0}^{n} \frac{f_i'}{g^i} \quad \text{und} \quad \sum_{i=0}^{n} f_i g^{n-i} = \sum_{i=0}^{n} f_i' g^{n-i} \ .$$

Wir nehmen an, es gäbe eine Zahl i mit $f_i \neq f_i'$. Sei j die größte Zahl Zahl mit dieser Eigenschaft. Dann ist

$$\sum_{i=0}^{j} f_i g^{n-i} = \sum_{i=0}^{j} f_i' g^{n-i}$$

und

$$f_j - f_j' = g \cdot \sum_{i=0}^{j-1} (f_i' - f_i) g^{j-i-1} \ ,$$

daher ist der Grad von f_j oder von f_j' nicht kleiner als der Grad von g. Widerspruch.

Satz 171 : (Partialbruchzerlegung rationaler Funktionen)
Es seien $f \in K[x]$, $g_1, \ldots, g_k$ paarweise nicht assoziierte irreduzible Polynome und

$$g := \prod_{i=1}^{k} g_i^{n_i} \ .$$

Dann gibt es eindeutig bestimmte Polynome f_0 und f_{ij}, $1 \leq i \leq k$, $1 \leq j \leq n_i$, sodass

$$\frac{f}{g} = f_0 + \sum_{i=1}^{k} \sum_{j=1}^{n_i} \frac{f_{ij}}{g_i^j}$$

und

$$f_{ij} = 0 \text{ oder } \operatorname{gr}(f_{ij}) < \operatorname{gr}(g_i)\ ,\ 1 \le i \le k\ ,\ 1 \le j \le n_i,$$

ist. Falls $K = \mathbb{C}$ *ist, kann die zweite Bedingung durch*

$$f_{ij} \in \mathbb{C}, 1 \le i \le k\ ,\ 1 \le j \le n_i$$

ersetzt werden.

Beweis: Folgt aus den Sätzen 168 und 170.

Beispiel 172 : Es seien $f \in K[x]$, $\operatorname{gr}(f) < k$ und $c_1, \ldots, c_k$ paarweise verschiedene Elemente von K. Nach Satz 171 gibt es Elemente $d_1, \ldots, d_k$ in K so, dass

$$\frac{f}{\prod_{i=1}^{k}(x-c_i)} = \sum_{j=1}^{k} \frac{d_j}{x-c_j}$$

ist. Multiplikation mit $\prod_{i=1}^{k}(x-c_i)$ ergibt

$$f = \sum_{j=1}^{k} d_j \prod_{i \ne j}(x-c_i)\ ,$$

daher ist

$$d_j = \frac{f(c_j)}{\prod_{i \ne j}(c_j - c_i)}\ .$$

Beispiel 173 :

$$\frac{1}{x(x+1)} = \frac{1}{x} - \frac{1}{x+1} \in K(x)\ .$$

Beispiel 174 : Es sei $\frac{f}{g}$ eine rationale Funktion mit Koeffizienten in $\mathbb{R}$ oder $\mathbb{C}$. Wenn die irreduziblen Faktoren des Zählers g bekannt sind, kann die Partialbruchzerlegung zur Berechnung des Integrals von $\frac{f}{g}$ verwendet werden. Zum Beispiel ist

$$\frac{x^4+x^2+x+1}{(x+1)^2(x-1)} = (x-1) + \frac{2}{x+1} - \frac{1}{(x+1)^2} + \frac{1}{x-1}\ ,$$

daher ist

$$\frac{1}{2}x^2 - x + \frac{1}{x+1} + \ln((x+1)^2 \cdot |x-1|)$$

das Integral dieser Funktion.

Da aber im allgemeinen die irreduziblen Faktoren des Zählers einer rationalen Funktion nicht bekannt sind, verwenden Computeralgebrasysteme andere Verfahren zur Berechnung des Integrals von rationalen Funktionen.

Statt der Zerlegung des Zählers in irreduzible Faktoren wird die leicht zu berechnende Zerlegung in *quadratfreie Faktoren* verwendet.

Definition 175 : Es seien $0 \neq f$ ein Polynom mit Koeffizienten in K. Dann ist f *quadratfrei*, wenn je zwei irreduzible Faktoren von f nicht assoziiert sind. Wenn K ein Unterring von $\mathbb{C}$ ist, ist f genau dann quadratfrei, wenn f in $\mathbb{C}$ keine mehrfachen Nullstellen hat.

Satz 176 : (Quadratfreie Zerlegung)
Es seien K ein Körper der Charakteristik 0 und $0 \neq f$ ein Polynom mit Koeffizienten in K. Dann gibt es eindeutig bestimmte normierte quadratfreie Polynome $f_1, \ldots, f_k$ so, dass

$$ggT(f_i, f_j) = 1 \ , \ 1 \leq i < j \leq k \qquad \textit{und} \qquad f = lk(f) \prod_{i=1}^{k} f_i^i$$

ist. Diese Zerlegung von f heißt quadratfreie Zerlegung *in die* quadratfreien Faktoren *$f_1, \ldots, f_k$ von f. Beachte: Auch 1 kann ein quadratfreier Faktor von f sein und nur dieser kann mehrfach auftreten.*
Die quadratfreien Faktoren von f können mit dem folgenden Verfahren berechnet werden:

- *Setze $i := 1$ und*
$$h_1 := \frac{f}{lk(f) \cdot ggT(f, D(f))} \ .$$
- *Solange $ggT(f, D(f)) \neq 1$ ist, ersetze f durch $ggT(f, D(f))$, i durch $i+1$, setze*
$$h_i := \frac{f}{ggT(f, D(f))} \quad \textit{und} \quad f_{i-1} := \frac{h_{i-1}}{h_i} \ .$$
- *Wenn $ggT(f, D(f)) = 1$ ist, setze $f_i := h_i$.*

Beweis: Es seien $u_1, \ldots, u_n$ paarweise verschiedene irreduzible Polynome und $e_1, \ldots, e_n$ positive ganze Zahlen so, dass

$$f = lk(f) \prod_{i=1}^{n} u_i^{e_i}$$

die Zerlegung von f in irreduzible Faktoren ist. Es sei k die größte der Zahlen $e_1, \ldots, e_n$. Für $1 \leq i \leq k$ sei f_i das Produkt aller Polynome in $\{u_j \mid 1 \leq j \leq n, e_j = i\}$. Dann sind $f_1, \ldots, f_k$ die quadratfreien Faktoren von f.
Nach Satz 142 ist

$$\frac{f}{ggT(f, D(f))} = lk(f) \prod_{i=1}^{n} u_i \ ,$$

damit ist leicht nachzuprüfen, dass das angegebene Verfahren die quadratfreien Faktoren von f berechnet.

Beispiel 177 :

$$x^9-18x^8+139x^7-604x^6+1627x^5-2818x^4+3141x^3-2176x^2+$$
$$+852x-144=$$
$$=(x-1)^4(x-2)^2(x-3)^2(x-4)=$$
$$=(x-1)^4[(x-2)(x-3)]^2(x-4)\cdot 1$$
$$f_4=x-1,\quad f_3=1,\quad f_2=(x-2)(x-3),\quad f_1=(x-4),\quad f_0=1\ .$$

Satz 178 : (Quadratfreie Partialbruchzerlegung rationaler Funktionen)
Es seien K ein Körper der Charakteristik 0, $0\neq f, 0\neq g$ Polynome mit Koeffizienten in K und $g_1,\ldots,g_k$ die quadratfreien Faktoren von g. Dann gibt es eindeutig bestimmte Polynome f_0 und f_{ij}, $1\leq i\leq k$, $1\leq j\leq n_i$, sodass

$$\frac{f}{g}=f_0+\sum_{i=0}^{k}\sum_{j=0}^{i}\frac{f_{ij}}{g_i^j}$$

und

$$f_{ij}=0 \text{ oder } \operatorname{gr}(f_{ij})<\operatorname{gr}(g_i)\ ,\ 1\leq j\leq i\leq k$$

ist. Falls $K=\mathbb{C}$ ist, kann die zweite Bedingung durch

$$f_{ij}\in\mathbb{C}, 1\leq j\leq i\leq k\ ,$$

ersetzt werden.

Beweis: Folgt aus den Sätzen 168 und 170.

KAPITEL 3

Rechnen mit algebraischen Zahlen

In diesem Kapitel sei K ein Körper.

§1. Algebraische Elemente und Minimalpolynome

In diesem Abschnitt sei A eine K-Algebra.

Definition 179 : Ein Element $a \in A$ ist *algebraisch über K*, wenn es Nullstelle eines Polynoms $f \neq 0$ in $K[x]$ ist. Elemente von A, die nicht algebraisch sind, sind *transzendent über K*. *Algebraische* bzw. *transzendente Zahlen* sind komplexe Zahlen, die über $\mathbb{Q}$ algebraisch bzw. transzendent sind.

Beispiel 180 : Die reellen Zahlen e und π sind transzendente Zahlen (Beweis in der Analysis). Die Matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$$

ist eine Nullstelle des Polynoms $x^2+1 \in \mathbb{Q}[x]$, also algebraisch über $\mathbb{Q}$. Die reelle Zahl $\sqrt[3]{5}$ ist eine Nullstelle von $x^3-5 \in \mathbb{Q}[x]$, also algebraisch über $\mathbb{Q}$. Die komplexe Zahl πi ist eine Nullstelle von $x^2+\pi^2 \in \mathbb{R}[x]$, also algebraisch über $\mathbb{R}$.

Satz 181 : *Es seien a ein über K algebraisches Element von A und I_a die Menge aller Polynome in $K[x]$, die a als Nullstelle haben. Dann ist I_a ein Ideal von $K[x]$. Es gibt genau ein normiertes Polynom kleinsten Grades in I_a. Dieses erzeugt das Ideal I_a und heißt* Minimalpolynom von a über K.

Beweis: Übung.

Satz 182 : *Es sei $a \in A$ algebraisch über K. Die Menge*

$$K[a] := \{h(a) \mid h \in K[x]\}$$

ist eine kommutative Unteralgebra von A. Diese ist genau dann ein Integritätsbereich, wenn das Minimalpolynom von a irreduzibel ist.

Beweis: Es ist klar, dass $K[a]$ eine kommutative Unteralgebra von A ist. Es seien $g,h \in K[x]$ und f das Minimalpolynom von a.
Es sei f irreduzibel. Wenn $g(a) \cdot h(a) = 0$ ist, dann ist $(gh)(a) = 0$, daher wird gh von f geteilt. Weil f irreduzibel ist, teilt f auch g oder h, also ist $g(a) = 0$ oder $h(a) = 0$.
Ist umgekehrt $K[a]$ ein Integritätsbereich und $f = gh$, dann folgt aus $0 = f(a) = (gh)(a) = g(a) \cdot h(a)$, dass a eine Nullstelle von g oder h ist. Also wird g oder h von f geteilt. Insbesondere hat eines dieser Polynome denselben Grad wie f und das andere den Grad 0. Somit ist f irreduzibel.

Satz 183 : *Es seien a ein über K algebraisches Element in A, dessen Minimalpolynom $f \in K[x]$ irreduzibel ist.*

(1) *Wenn $g \in K[x]$ ein irreduzibles normiertes Polynom mit $g(a) = 0$ ist, dann ist $f = g$.*
(2) *Es sei n der Grad von f. Dann ist*

$$(1, a, a^2, \ldots, a^{n-1})$$

eine K-Basis von $K[a]$. Wenn $r = \sum_{i=0}^{n-1} c_i x^i$ der Rest von $h \in K[x]$ nach Division durch f ist, dann ist $(c_0, \ldots, c_{n-1})$ das n-Tupel der Koordinaten von $h(a)$ bezüglich dieser Basis.
(3) *$K[a]$ ist ein Körper. Es seien $h \in K[x]$ und $h(a) \neq 0$. Die Koordinaten von $h(a)^{-1} \in K[a]$ bezüglich der Basis $(1, a, \ldots, a^{n-1})$ können wie folgt berechnet werden:*
   - *Berechne mit dem erweiterten Euklidischen Algorithmus Polynome $u, v \in K[x]$ so, dass $uf + vh = 1$ ist.*
   - *Berechne den Rest $\sum_{i=0}^{n-1} d_i x^i$ von v nach Division durch f.*
   - *Dann ist $(d_0, \ldots, d_{n-1})$ das gesuchte n-Tupel der Koordinaten von $h(a)^{-1}$.*

Beweis:

(1) Das irreduzible Polynom g wird nach Satz 181 von f geteilt, also ist es zu f assoziiert. Aus $lk(g) = 1 = lk(g)$ folgt daher $f = g$.
(2) Es seien $h \in K[x]$ und m bzw. r der polynomiale Quotient bzw. Rest von h nach Division durch f. Dann ist

$$h(a) = m(a) \cdot f(a) + r(a) = r(a) \ ,$$

also ist $h(a)$ eine K-Linearkombination von $(1, a, \ldots, a^{n-1})$. Wäre $(1, a, \ldots, a^{n-1})$ nicht linear unabhängig, dann gäbe es ein n-Tupel $0 \neq (d_0, \ldots, d_{n-1})$ in K^n mit $\sum_{i=0}^{n-1} d_i a^i = 0$. Dann wäre aber a die Nullstelle des Polynoms $0 \neq \sum_{i=0}^{n-1} d_i x^i$, dessen Grad kleiner als der von f ist. Widerspruch.

(3) Es seien $h \in K[x]$ und $h(a) \neq 0$. Dann wird h nicht von f geteilt, also ist $ggT(f,h) = 1$. Mit dem erweiterten Euklidischen Algorithmus können daher Polynome $u, v \in K[x]$ so berechnet werden, dass $uf + vh = 1$ ist. Dann ist $v(a) \in K[a]$ und

$$1 = u(a) \cdot f(a) + v(a) \cdot h(a) = 0 + v(a) \cdot h(a) \ ,$$

also $h(a)$ invertierbar und $h(a)^{-1} = v(a)$.

Wenn das Minimalpolynom eines algebraischen Elementes a bekannt ist, dann kann am Computer in $K[a]$ exakt gerechnet werden (wobei vorausgesetzt werden muss, dass man in K exakt rechnen kann). Die Elemente von $K[a]$ werden durch n-Tupel in K^n dargestellt, und die Rechenoperationen werden mit Hilfe der Aussagen (2) und (3) von Satz 183 ausgeführt.

Die erste Aussage von Satz 183 kann verwendet werden, um das Minimalpolynom zu finden: es muss zunächst irgendein normiertes Polynom f, dessen Nullstelle a ist, gegeben sein. Dann wird überprüft, ob f irreduzibel ist (siehe Abschnitt §4). Wenn es irreduzibel ist, dann ist f das Minimalpolynom von a . Wenn nicht, müssen wir einen Faktor g kleineren Grades mit $g(a) = 0$ finden und mit diesem von Neuem beginnen.

Beispiel 184 : Es sei $\sqrt[3]{2}$ die positive reelle Zahl, die Nullstelle von $x^3 - 2$ ist. Wenn das Polynom $x^3 - 2$ nicht irreduzibel über $\mathbb{Q}$ wäre, dann hätte es einen Faktor vom Grad 1. Nach Beispiel 136 hat $x^3 - 2$ aber keine Nullstelle in $\mathbb{Q}$, also auch keinen Faktor vom Grad 1. Daher ist $x^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ und $(1, \sqrt[3]{2}, \sqrt[3]{4})$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\sqrt[3]{2}]$. Um die Koordinaten von $(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4})^{-1}$ bezüglich dieser Basis zu berechnen, verwenden wir Satz 183. Es ist

$$(-3x - 50)(x^3 - 2) + (x^2 + 16x - 11)(3x^2 + 2x + 1) = 89 \ ,$$

also

$$(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4})^{-1} = \frac{-11}{89} + \frac{16}{89}\sqrt[3]{2} + \frac{1}{89}\sqrt[3]{4} \ .$$

Schreibt man dieses Ergebnis in der Form

$$\frac{1}{(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4})} = \frac{-11 + 16\sqrt[3]{2} + \sqrt[3]{4}}{89}$$

an, so wird diese Berechnung oft als „den Nenner wurzelfrei (oder rational) machen“ bezeichnet.

§2. Ring-, Modul- und Algebrenhomomorphismen

Definition 185 : Es seien R und R' Ringe mit Einselementen 1 und $1'$. Eine Funktion

$$f : R \to R'$$

heißt *Ringhomomorphismus*, wenn

$$f(1) = 1'$$

und für alle $s,t \in R$

$$f(s+t) = f(s)+f(t) \quad \text{und} \quad f(st) = f(s)f(t)$$

ist. („Das Bild des Einselementes ist das Einselement des Bildes, das Bild der Summe ist die Summe der Bilder und das Bild des Produktes ist das Produkt der Bilder“).
Ein bijektiver Ringhomomorphismus heißt *Ringisomorphismus* oder *Isomorphismus von Ringen*.

Satz 186 : *Es seien R und R' Ringe, 1 und $1'$ ihre Einselemente, 0 und $0'$ ihre Nullelemente und $f : R \to R'$ ein Ringhomomorphismus.*

(1) $f(0) = 0'$.
(2) *Für alle invertierbaren Elemente $r \in R$ ist auch $f(r)$ invertierbar und* $f(r^{-1}) = f(r)^{-1}$.
(3) $\text{Kern}(f) := \{r \in R \mid f(r) = 0'\}$ *ist ein Ideal von R und* $\text{Bild}(f)$ *ist ein Unterring von R'.*

Beweis:

(1) Es ist $0' + f(0) = f(0) = f(0+0) = f(0) + f(0)$, daher $0' = f(0)$.
(2) $f(r^{-1})f(r) = f(r^{-1}r) = f(1) = 1'$, also $f(r^{-1}) = f(r)^{-1}$.
(3) Aus $r \in R$, $s \in \text{Kern}(f)$ folgt $f(rs) = f(r)f(s) = f(r) \cdot 0' = 0'$, also $rs \in \text{Kern}(f)$. Die übrigen Aussagen können leicht nachgeprüft werden.

Beispiel 187 : Es sei R ein Ring mit Einselement 1_R. Die Funktion

$$\mathbb{Z} \longrightarrow R \ , \ z \longmapsto z \cdot 1_R \ ,$$

ist der einzige Ringhomomorphismus von $\mathbb{Z}$ nach R.
Ihr Kern ist $n\mathbb{Z} := \{\, k \cdot n \,|\, k \in \mathbb{Z} \,\}$, wobei n die Charakteristik von R ist.

Beispiel 188 : Es sei $n \geq 2$ eine natürliche Zahl. Die Funktion

$$kan : \mathbb{Z} \longrightarrow \mathbb{Z}_n, r \longmapsto \bar{r}$$

ist ein Ringhomomorphismus und heißt *kanonische Projektion*. Ihr Kern ist $n\mathbb{Z}$ und ihr Bild ist $\mathbb{Z}_n$.

Definition 189 : Es seien R ein Ring und M und M' Moduln über R. Eine Funktion

$$f : M \to M'$$

heißt *R-Modulhomomorphismus* oder *R-linear*, wenn für alle $r \in R$ und alle $v, w \in M$

$$f(v+w) = f(v) + f(w) \quad \text{und} \quad f(r \cdot v) = r \cdot f(v)$$

ist. Ein bijektiver R-Modulhomomorphismus heißt *Isomorphismus von R-Moduln*.

Satz 190 : *Es seien R ein Ring, M und M' Moduln über R und f eine R-lineare Funktion von M nach M'.*
Dann ist $\text{Kern}(f) := \{r \in M \mid f(r) = 0'\}$ *ein Untermodul von M und* $\text{Bild}(f)$ *ist ein Untermodul von M'.*

Beweis: Übung.

Definition 191 : Es seien R ein Ring und A und A' Algebren über R. Eine Funktion

$$f : A \to A'$$

heißt *R-Algebrenhomomorphismus*, wenn sie ein Ringhomomorphismus und R-linear ist.
Ein bijektiver R-Algebrenhomomorphismus heißt *Isomorphismus von R-Algebren*.

Satz 192 : *Es seien R ein Ring, A und A' Algebren über R und f ein Algebrenhomomorphismus von A nach A'.*
Dann ist $\text{Kern}(f) := \{r \in A \mid f(r) = 0'\}$ *ein Ideal von A und* $\text{Bild}(f)$ *ist eine Unteralgebra von A'.*

Beweis: Übung.

Beispiel 193 : Es seien R ein kommutativer Ring, A eine R-Algebra und $a \in A$. Die Funktion

$$R[x] \longrightarrow A \ , \ g \longmapsto g(a) \ ,$$

ist ein R-Algebrenhomomorphismus und heißt *Einsetzungshomomorphismus*.

Beispiel 194 : Es seien R ein kommutativer Ring und A die R-Algebra der Polynomfunktionen von R nach R. Dann ist die Funktion

$$\varphi : R[x] \longrightarrow A \ , \ f \longmapsto [r \mapsto f(r)] = f(Id_R) \ ,$$

die jedem Polynom die entsprechende Polynomfunktion zuordnet, ein Algebrenhomomorphismus. Wenn R ein unendlicher Integritätsbereich ist, dann ist φ ein Algebrenisomorphismus.

Beispiel 195 : Es seien V ein n-dimensionaler Vektorraum über einem Körper K und $\underline{v}$ eine Basis von V. Dann ist die Funktion von $\mathrm{Lin}_K(V,V)$, der Algebra aller linearen Funktionen von V nach V, nach $K^{n\times n}$, der Algebra der $n \times n$-Matrizen, die jeder linearen Funktion ihre Matrix bezüglich $\underline{v}$ zuordnet, ein K-Algebrenisomorphismus.

Satz 196 : *Wenn f ein Ringisomorphismus bzw. Modulisomorphismus bzw. Algebrenisomorphismus ist, dann auch die Umkehrfunktion f^{-1}.*

Beweis: Übung

§3. Existenz von Nullstellen

In diesem Abschnitt sei $f \in K[x]$ ein irreduzibles normiertes Polynom.

Definition 197 : Eine Körper L, der K als Unterring enthält, heißt *Körpererweiterung* von K. Eine Körpererweiterung $K \subseteq L$ ist *endlich*, wenn L als K-Vektorraum endlichdimensional ist. Die Dimension dieses Vektorraums heißt *Grad* der Körpererweiterung. Schreibweise: $\mathrm{gr}(L/K)$.

Ein irreduzibles Polynom hat in K keine Nullstellen, daher sucht man eine endliche Körpererweiterung $K \subseteq L$ von möglichst kleinem Grad, sodass das Polynom in L eine Nullstelle hat. Dazu gibt es zwei Möglichkeiten:

(1) Man sucht in einer bereits bekannten K-Algebra A nach einer Nullstelle a von f. Wenn man sie findet, dann ist $K \subseteq K[a]$ die gesuchte Körpererweiterung.
(2) Man *konstruiert* eine endliche Körpererweiterung, in der f eine Nullstelle haben muss.

Beispiel 198 : (Komplexe Zahlen, erste Vorgangsweise)
Wenn $K = \mathbb{R}$ und $f = x^2 + 1$ ist, dann hat f in der $\mathbb{R}$-Algebra $\mathbb{R}^{2\times 2}$ die

Nullstelle

$$i := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} .$$

Also ist $\mathbb{R} \subseteq \mathbb{R}[i] := \{aI_2 + bi = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{R}\} =: \mathbb{C}$ eine Körpererweiterung von $\mathbb{R}$ vom Grad 2.

Beispiel 199 : Wenn $K = \mathbb{Q}$ und $f = x^2 - 2$ ist, dann hat f in der $\mathbb{Q}$-Algebra $\mathbb{Q}^{2\times 2}$ die Nullstelle

$$\sqrt{2} := \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} .$$

Also ist $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] := \{aI_2 + b\sqrt{2} = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{Q}\}$ eine Körpererweiterung von $\mathbb{Q}$ vom Grad 2, in der „eine Wurzel aus 2 existiert".

Beispiel 200 : Wenn $K = \mathbb{Q}$ und $f := x^2 - 2$ ist, dann hat f in der $\mathbb{Q}$-Algebra $\mathbb{R}$ die Nullstelle $\sqrt{2}$, das ist die eindeutig bestimmte positive reelle Zahl mit $(\sqrt{2})^2 = 2$. Die Existenz einer solchen reellen Zahl folgt aus dem Zwischenwertsatz (cf. Analysis 1). Also ist

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \in \mathbb{R} \mid a,b \in \mathbb{Q}\}$$

eine Körpererweiterung von $\mathbb{Q}$ vom Grad 2.

Satz 201 : *Wenn $K \subseteq L$ und $L \subseteq M$ endliche Körpererweiterungen sind, dann ist auch $K \subseteq M$ eine endliche Körpererweiterung und*

$$gr(M/K) = gr(M/L) \cdot gr(L/K) .$$

Beweis: Es sei $(a_1, \ldots, a_d)$ eine K-Basis von L und $(b_1, \ldots, b_e)$ eine L-Basis von M. Dann ist $(a_i b_j)_{1\le i\le d, 1\le j\le e}$ eine K-Basis von M (nachprüfen).

Satz 202 : *Es seien $K \subseteq L$ eine endliche Körpererweiterung und $a \in L$ eine Nullstelle von f. Dann ist der Grad dieser Körpererweiterung ein Vielfaches von* $\mathrm{gr}(f)$.

Beweis: Da f irreduzibel ist, ist f das Minimalpolynom von a. Nach Satz 183 ist die K-Algebra $K[a]$ ($\subseteq L$) ein Körper und hat den Grad $\mathrm{gr}(f)$. Nach Satz 201 ist $\mathrm{gr}(L/K) = \mathrm{gr}(L/K[a]) \cdot \mathrm{gr}(K[a]/K)$.

Eine allgemeine Methode zur Konstruktion einer endlichen Körpererweiterung von kleinstmöglichem Grad, in der f eine Nullstelle hat, liefert der folgende

Satz 203: *Es seien $n := \mathrm{gr}(f)$ und V der von $1, x, x^2, \ldots, x^{n-1}$ erzeugte Untervektorraum von $K[x]$. Mit der Multiplikation*

$$\cdot : V \times V \longrightarrow V \ , \ (g,h) \longmapsto \textit{ Rest von } gh \textit{ nach Division durch } f \ ,$$

wird V zu einer K-Algebra, die sogar eine Körpererweiterung von K (vom Grad n) ist. Das Element $x \in V$ ist eine Nullstelle von f in V.
Das zu $h \in V$ inverse Element kann wie folgt berechnet werden:

- *Berechne mit dem erweiterten Euklidischen Algorithmus Polynome $u, v \in K[x]$ so, dass $uf + vh = 1$ ist.*
- *Der Rest von v nach Division durch f ist das zu h inverse Element.*

Beweis: Übung.

Beispiel 204: Seien $K = \mathbb{R}$, $f = x^2 + 1$ und $V := {}_{\mathbb{R}}\langle 1, x \rangle$ der von 1 und x erzeugte Untervektorraum von $\mathbb{R}[x]$. Wir betrachten V wie in Satz 203 als zweidimensionale Körpererweiterung von $\mathbb{R}$. Dann hat f in V die Nullstelle $i := x$.

Beispiel 205: Seien $K = \mathbb{Q}$, $f = x^2 - 2$ und $V := {}_{\mathbb{R}}\langle 1, x \rangle$. Wir betrachten V wie in Satz 203 als zweidimensionale Körpererweiterung von $\mathbb{Q}$. Dann hat f in V die Nullstelle $\sqrt{2} := x$.

Beispiel 206: Das Polynom $x^2 + x + 1$ ist über $\mathbb{Z}_2$ irreduzibel, also ist ${}_{\mathbb{Z}_2}\langle 1, x \rangle$ mit der in Satz 203 definierten Multiplikation ein Körper der Charakteristik 2 mit 4 Elementen. Seine Elemente sind $0, 1, x$ und $x + 1$. Es ist $x \cdot (1 + x) = 1$, $x^2 = x + 1$ und $(x + 1)^2 = x$.

§4. Irreduzibilitätskriterien

Im vorangegangenen Abschnitt haben wir immer angenommen, dass das Polynom, das in dem in Satz 203 angegebenen Körper eine Nullstelle hat, irreduzibel ist. In diesem Abschnitt überlegen wir uns, wie man nachprüfen kann, ob ein Polynom irreduzibel ist.

Definition 207 : Es sei $n \geq 2$ und k natürliche Zahlen und $f = \sum_{i=0}^{k} c_i x^i \in \mathbb{Z}[x]$ ein Polynom mit ganzzahligen Koeffizienten. Dann heißt

$$\bar{f} = \sum_{i=0}^{k} \overline{c_i} x^i \in \mathbb{Z}_n[x]$$

die Restklasse von f in $\mathbb{Z}_n[x]$.

Satz 208 : *Es sei* $n \geq 2$. *Die Funktion*

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_n[x], f \longmapsto \bar{f},$$

ist ein $\mathbb{Z}$*-Algebrenhomomorphismus.*
Wenn n *den Leitkoeffizienten von* f *nicht teilt, dann ist* $gr(\bar{f}) = gr(f)$.

Beweis: Nachprüfen.

Satz 209 : *Es seien* $f \neq 0$ *ein primitives Polynom mit Koeffizienten in* $\mathbb{Z}$ *und* p *eine positive Primzahl, die* $lk(f)$ *nicht teilt. Wenn die Restklasse* $\bar{f}$ *von* f *in* $\mathbb{Z}_p[x]$ *irreduzibel ist, dann ist auch* f *in* $\mathbb{Z}[x]$ *(und* $\mathbb{Q}[x]$*) irreduzibel.*

Beweis: Wenn f das Produkt von zwei Polynomen $g, h \in \mathbb{Z}[x]$ ist, dann ist $\bar{f} = \bar{g} \cdot \bar{h}$ und $\mathrm{gr}(\bar{f}) = \mathrm{gr}(\bar{g}) + \mathrm{gr}(\bar{h})$. Weil $\bar{f}$ irreduzibel ist, ist $\mathrm{gr}(\bar{g}) = 0$ oder $\mathrm{gr}(\bar{h}) = 0$. Da p den Leitkoeffizienten von f nicht teilt, ist $\mathrm{gr}(f) = \mathrm{gr}(\bar{f})$ und daher auch $\mathrm{gr}(g) = \mathrm{gr}(\bar{g})$ und $\mathrm{gr}(h) = \mathrm{gr}(\bar{h})$. Somit ist $\mathrm{gr}(g) = 0$ oder $\mathrm{gr}(h) = 0$. Weil f primitiv ist, folgt daraus die Behauptung.

Beispiel 210 : Es sei

$$h = x^5 + 3456x^4 + 7890x^3 - 12345x^2 + 987654321 \in \mathbb{Z}[x] .$$

Die Restklasse von h in $\mathbb{Z}_2[x]$ ist $f := x^5 + x^2 + \bar{1}$. Wenn f reduzibel ist, dann wird f von einem Polynom vom Grad 1 oder vom Grad 2 geteilt, also von x, $x+1$ oder x^2+x+1. Man prüft durch Division mit Rest nach, dass das nicht der Fall ist. Daher ist f in $\mathbb{Z}_2[x]$ irreduzibel. Aus Satz 209 folgt nun, dass auch h irreduzibel ist.

Satz 211 : (Kriterium von Eisenstein)
Es sei $f \neq 0$ ein primitives Polynom in $\mathbb{Z}[x]$. Wenn es eine Primzahl p gibt, die

den Leitkoeffizienten von f nicht teilt, aber
alle anderen Koeffizienten von f teilt, und
deren Quadrat die Zahl $f(0)$ nicht teilt,

dann ist f irreduzibel.

Beweis: Es seien n der Grad von f, c der Leitkoeffizient von f und p eine Primzahl mit den angegebenen Eigenschaften. Die Restklasse von f in $\mathbb{Z}_p[x]$ ist dann $\bar{c}x^n \neq \bar{0}$. Seien $g,h \in \mathbb{Z}[x]$ so, dass $f = gh$ ist. Dann ist $\bar{f} = \bar{g}\bar{h} = \bar{c}x^n$. Weil $\mathbb{Z}_p[x]$ faktoriell ist, gibt es natürliche Zahlen k,ℓ und ganze Zahlen $a \neq 0$, $b \neq 0$ so, dass $k+\ell = n$, $\bar{g} = \bar{a}x^k$ und $\bar{h} = \bar{b}x^\ell$ ist. Wenn sowohl g als auch h positiven Grad hätten, würden $g(0)$ und $h(0)$ von p und

$$g(0) \cdot h(0) = f(0)$$

von p^2 geteilt werden. Widerspruch. Daher ist entweder g oder h zu f assoziiert und f irreduzibel.

Beispiel 212 : Es seien p eine positive Primzahl und n eine positive ganze Zahl. Dann ist das Polynom

$$x^n + px^{n-1} + px^{n-2} + \ldots + px + p \in \mathbb{Z}[x]$$

irreduzibel.

Beispiel 213 : Die Polynome

$$x^{10} - 6, x^{11} - 15, x^2 - 2, x^4 + 3x + 3 \in \mathbb{Z}[x]$$

sind irreduzibel.

§5. Der Körper der algebraischen Zahlen

Satz 214 : *Es seien $K \subseteq L$ eine Körpererweiterung und $a \in L$. Dann ist a genau dann algebraisch über K, wenn $K[a]$ ein endlichdimensionaler K-Vektorraum ist.*

Beweis: Wenn a algebraisch ist, dann ist die K-Dimension von $K[a]$ nach Satz 183 endlich.
Ist umgekehrt $K[a]$ ein endlichdimensionaler K-Vektorraum, dann ist die Familie $(a^i)_{i\in\mathbb{N}}$ nicht linear unabhängig. Also gibt es Elemente $c_0,\ldots,c_n$ so, dass $\sum_{i=0}^n c_i a^i = 0$ ist. Daher ist a eine Nullstelle von $\sum_{i=0}^n c_i x^i$.

Definition 215 : Ein Körper K ist *algebraisch abgeschlossen*, wenn jedes Polynom in $K[x]$ mit positivem Grad eine Nullstelle in K hat.

Beispiel 216 : Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

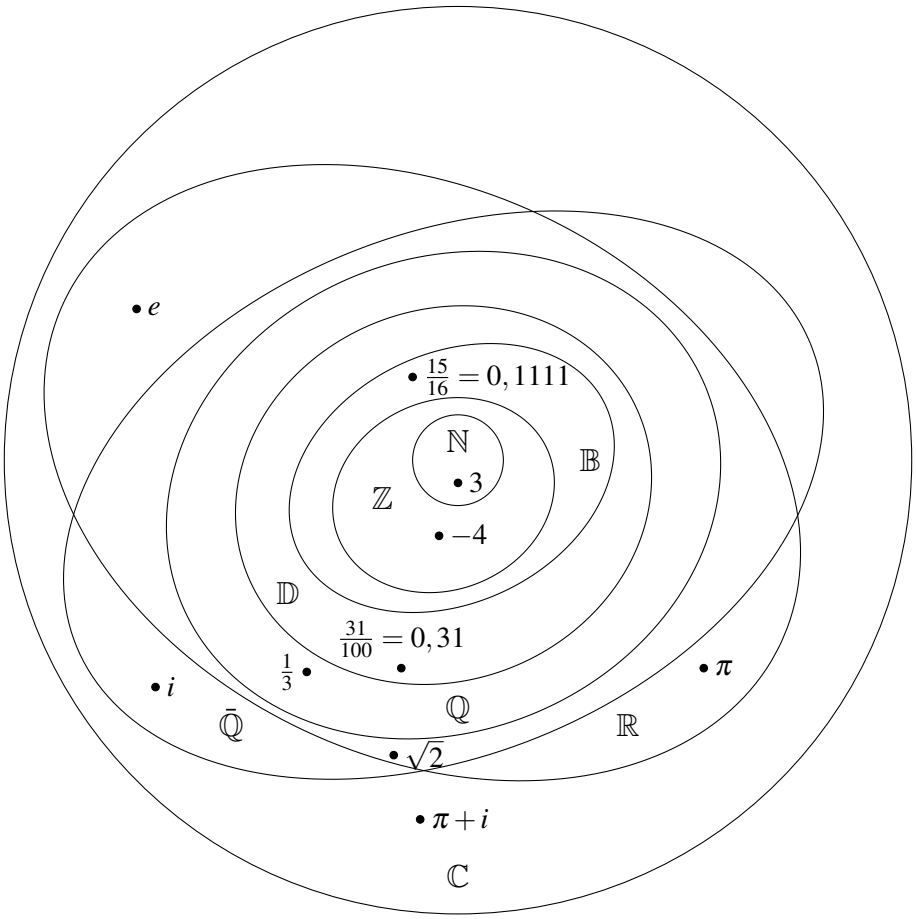
Satz 217 : *Die Summe und das Produkt von algebraischen Zahlen ist wieder eine algebraische Zahl. Die zu einer algebraischen Zahl inverse Zahl ist wieder algebraisch. Jedes Polynom mit positivem Grad, dessen Koeffizienten algebraische Zahlen sind, hat eine algebraische Zahl als Nullstelle. Kurz formuliert: Die Menge $\bar{\mathbb{Q}}$ aller algebraischen Zahlen ist ein Unterkörper von $\mathbb{C}$ und algebraisch abgeschlossen.*

Beweis: Es seien a und b algebraische Zahlen. Dann sind die Körpererweiterungen $\mathbb{Q} \subseteq \mathbb{Q}[a]$ und $\mathbb{Q}[a] \subseteq (\mathbb{Q}[a])[b] =: \mathbb{Q}[a,b]$ endlich, nach Satz 201 auch $\mathbb{Q} \subseteq \mathbb{Q}[a,b]$. Nach Satz 214 ist jedes Element von $\mathbb{Q}[a,b]$ eine algebraische Zahl, insbesondere $a+b$, $a \cdot b$ und a^{-1}.
Es sei $f := \sum_{i=0}^{n} c_i x^i \in \bar{\mathbb{Q}}[x]$ ein Polynom mit positivem Grad. Dann gibt es eine komplexe Zahl $a \in \mathbb{C}$ mit $f(a) = 0$. Die Koeffizienten von f sind in $\mathbb{Q}[c_0, c_1, \ldots, c_n]$ enthalten, also ist a algebraisch über diesem Körper. Daher sind die Körpererweiterungen $\mathbb{Q} \subseteq \mathbb{Q}[c_0, c_1, \ldots, c_n]$ und
$\mathbb{Q}[c_0, c_1, \ldots, c_n] \subseteq \mathbb{Q}[c_0, c_1, \ldots, c_n, a]$ endlich, somit nach Satz 201 auch

$$\mathbb{Q} \subseteq \mathbb{Q}[c_0, c_1, \ldots, c_n, a] \; .$$

Nun folgt aus Satz 214, dass a eine algebraische Zahl ist.

Zahlbereiche:



$\mathbb{B}$ ... Binärzahlen, $\mathbb{D}$ ... Dezimalzahlen
Nicht unter den Rechenoperationen abgeschlossen sind die Menge $\mathbb{C} \setminus \bar{\mathbb{Q}}$ der transzendenten Zahlen, die Menge $\mathbb{R} \setminus \mathbb{Q}$ der irrationalen Zahlen, die Menge $\mathbb{Z} \setminus \mathbb{N}$ der negativen Zahlen und die Menge der Maschinenzahlen.

KAPITEL 4

Graphentheorie

§1. Graphen und Digraphen

Definition 218 : Ein *Graph* ist ein Paar (E,K) von endlichen Mengen, wobei E nicht leer und K eine Menge von zweielementigen Teilmengen von E ist. Die Elemente von E heißen *Ecken* (engl.: vertices), die Elemente von K heißen *Kanten* (engl.: edges) des Graphen (E,K).

Wenn $k := \{a,b\}$ eine Kante des Graphen (E,K) ist, dann heißen die Ecken a und b die *Eckpunkte (oder Ecken) von* k. In diesem Fall sind die Ecken a und b *benachbart*.

Ein Graph (E,K) heißt *vollständig*, wenn K die Menge aller zweielementigen Teilmengen von E ist. Ein Graph (E,K) heißt *trivial*, wenn K die leere Menge ist.

In der Literatur wird der Begriff Graph manchmal allgemeiner definiert. Dann wird ein Graph im Sinne von Definition 218 als *einfacher Graph* oder *schlichter Graph* bezeichnet.

Beispiel 219 : Seien $E := \{1,2,3,4,5,6,7\}$ und

$$K := \big\{\{1,2\},\{1,3\},\{1,4\},\{5,6\},\{5,7\},\{6,7\}\big\},$$

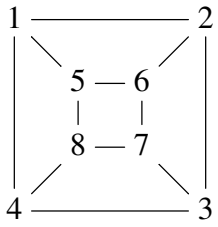
Dann ist (E,K) ein Graph, der nicht vollständig ist. Die Zahlen 5 und 7 sind die Eckpunkte der Kante $\{5,7\}$.

Zeichnerische Darstellung von Graphen:
Zeichne die Ecken als Punkte der Ebene und die Kanten als Strecken zwischen ihren Eckpunkten.

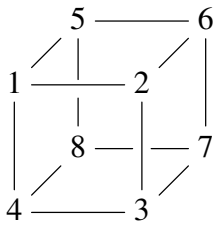
Zum Beispiel: Der Graph

$$\big(\{1,2,3,4,5,6,7,8\},\big\{\{1,2\},\{2,3\},\{3,4\},\{4,1\},\{5,6\},\{6,7\},\{7,8\},\{8,5\},\{1,5\},\{2,6\},\{3,7\},\{4,8\}\big\}\big)$$

kann (in der Zeichenebene) durch



oder



dargestellt werden.

Bemerkung: Ein vollständiger Graph mit n Ecken hat $\binom{n}{2} = \frac{n(n-1)}{2}$ Kanten.

Definition 220 : Ein *gerichteter Graph* oder *Digraph* ist ein Paar (E,K) von endlichen Mengen, wobei E nicht leer und K eine Teilmenge von

$$(E \times E) \setminus \{(a,a) \mid a \in E\}$$

ist. Die Elemente von E heißen *Ecken*, die Elemente von K heißen *gerichtete Kanten* oder *Pfeile* des Digraphen (E,K). Wenn $k := (a,b)$ eine gerichtete Kante des Digraphen (E,K) ist, dann heißt a *Anfangsecke* und b *Endecke* von k. Die Ecke a ist dann ein *Vorgänger* von b und die Ecke b ist ein *Nachfolger* von a.

Beispiel 221 : E sei die Menge aller Straßenkreuzungen einer Stadt. K sei die Menge aller Paare $(a,b) \in E \times E$ mit den Eigenschaften: $a \neq b$ und man kann mit dem Auto von a nach b fahren, ohne eine andere Straßenkreuzung zu passieren (Einbahnregelungen sind dabei zu beachten!). Dann ist (E,K) ein gerichteter Graph.

Bemerkung: Ist (E,K) ein Graph, dann ist das Paar

$$\big(E, K_g) := \big\{(a,b) \mid \{a,b\} \in K\big\}\big)$$

ein gerichteter Graph. Beachte, dass dann $\#(K_g) = 2 \cdot \#(K)$ ist. Ist umgekehrt (E', K'_g) ein gerichteter Graph, dann ist das Paar

$$\big(E', \big\{\{a,b\} \mid (a,b) \in K'_g \text{ oder } (b,a) \in K'_g\big\}\big)$$

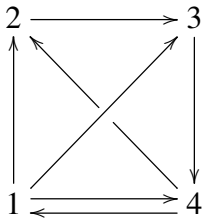
ein Graph. Graphen können daher als Spezialfälle von gerichteten Graphen, nämlich als jene gerichtete Graphen, für die mit jeder gerichteten Kante (a,b) auch (b,a) eine gerichtete Kante ist, aufgefasst werden.

Zeichnerische Darstellung von Digraphen:
Zeichne die Ecken als Punkte der Ebene und die gerichtete Kanten als Pfeile.

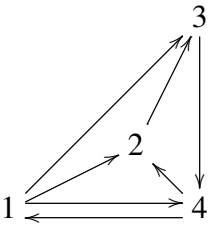
Der Digraph

$$\big(\{1,2,3,4\},\{(1,2),(2,3),(3,4),(4,1),(1,4),(1,3),(4,2)\}\big)$$

kann durch



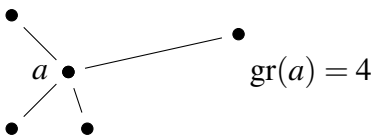
oder



dargestellt werden.

§2. Grad von Ecken, Untergraphen

Definition 222 : Seien (E,K) ein Graph und $a \in E$.
Der *Grad von a* (Schreibweise $\mathrm{gr}(a)$) ist die Anzahl aller Kanten von (E,K), die a als Eckpunkt haben. Die Ecke a ist *gerade* bzw. *ungerade*, wenn $\mathrm{gr}(a)$ eine gerade bzw. ungerade Zahl ist.



Beispiel 223 : In einem vollständigen Graphen mit n Ecken ist der Grad jeder Ecke gleich $n-1$.

Satz 224 : *(E,K) sei ein Graph. Dann ist*

$$\sum_{a\in E} \mathrm{gr}(a) = 2\cdot\#(K)\ ,$$

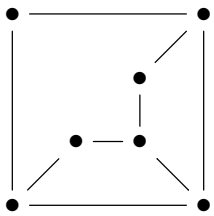
insbesondere ist die Anzahl der ungeraden Ecken in (E,K) eine gerade Zahl.

Beweis: Jede Kante hat zwei Eckpunkte, daher ist die Summe der Grade aller Ecken gleich $2\cdot\#(K)$. Eine Summe von ganzen Zahlen ist genau dann gerade, wenn die Anzahl der ungeraden Summanden gerade ist.

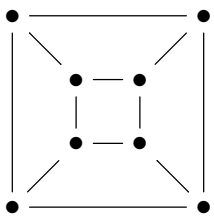
Definition 225 : $G := (E,K)$ und $G' := (E',K')$ seien Graphen (oder Digraphen). G ist genau dann ein *Untergraph* von G' (Schreibweise: $G \subseteq G'$), wenn $E \subseteq E'$ und $K \subseteq K'$ ist.

Ein Untergraph (E,K) von G' ist der *von E induzierte Untergraph*, wenn K alle (gerichteten) Kanten in K', deren Ecken in E liegen, enthält. Ein Untergraph (E,K) von G' heißt *aufspannend*, wenn $E = E'$ ist. Seien $a \in E'$ und $k \in K'$. Der Untergraph $(E',K' \setminus \{k\})$ heißt der *Untergraph von G', der durch Weglassen der Kante k entsteht*. Der Untergraph von G', der von $E \setminus \{a\}$ induziert wird, heißt der *Untergraph von G', der durch Weglassen einer Ecke entsteht.*

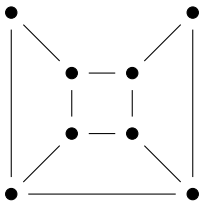
Beispiel 226 : Der Graph



ist ein Untergraph von



der durch Weglassen einer Ecke entsteht. Der Graph

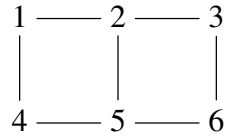


ist aus diesem durch Weglassen einer Kante entstanden.

§3. Wege, Kreise und Zusammenhang

Definition 227 : Seien $G := (E,K)$ ein Graph und n eine positive ganze Zahl. Eine endliche Folge $a_0, a_1, \ldots, a_n$ in E heißt *Kantenfolge der Länge n* in G, wenn für $1 \leq i \leq n$ gilt: $\{a_{i-1}, a_i\} \in K$. Schreibweise: $[a_0, a_1, \ldots, a_n]$. Ist $a_0 = a_n$, dann ist die Kantenfolge *geschlossen*.
Eine Kantenfolge $[a_0, \ldots, a_n]$ heißt *Weg* von a_0 nach a_n, wenn $a_0, a_1, \ldots, a_n$ paarweise verschieden sind. Eine geschlossene Kantenfolge $[a_0, \ldots, a_n]$ der Länge ≥ 3 heißt *Kreis*, wenn die Ecken $a_1, a_2, \ldots, a_n$ paarweise verschieden sind.

Beispiel 228 : Im Graphen



ist

$[1,2,3,5,4]$	keine Kantenfolge,
$[1,2,5,6,3,2,1]$	eine geschlossene Kantenfolge, aber kein Kreis,
$[2,3,6,5,2]$	ein Kreis und
$[1,2,5,6]$	ein Weg.

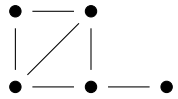
Definition 229 : Ein Graph G ist *zusammenhängend*, wenn es von jeder Ecke von G zu jeder anderen Ecke einen Weg gibt. Ein Digraph (E,K) ist *zusammenhängend*, wenn der Graph

$$\big(E, \big\{\{a,b\} \mid (a,b) \in K\big\}\big)$$

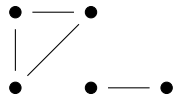
zusammenhängend ist.

Ein Untergraph H eines Graphen bzw. Digraphen G ist eine *Zusammenhangskomponente* von G, wenn er zusammenhängend ist und wenn es keinen von H verschiedenen zusammenhängenden Untergraphen von G gibt, der H enthält.

Beispiel 230 : Der Graph



ist zusammenhängend, der Graph

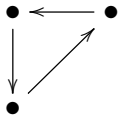


ist nicht zusammenhängend und hat zwei Zusammenhangskomponenten.

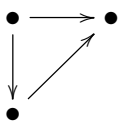
Beispiel 231 : Jeder vollständige Graph ist zusammenhängend. Ein trivialer Graph ist genau dann zusammenhängend, wenn er nur eine Ecke hat.

Definition 232 : Seien $G := (E,K)$ ein Digraph und n eine positive ganze Zahl. Eine endliche Folge $a_0,a_1,\ldots,a_n$ in E heißt *gerichtete Kantenfolge der Länge n in G*, wenn für $1 \leq i \leq n$ gilt: $(a_{i-1},a_i) \in K$. Schreibweise: $[a_0,a_1,\ldots,a_n]$. Ist $a_0 = a_n$, dann ist die gerichtete Kantenfolge *geschlossen*. Eine gerichtete Kantenfolge $[a_0,a_1,\ldots,a_n]$ heißt *gerichteter Weg von* a_0 *nach* a_n, wenn $a_0,a_1,\ldots,a_n$ paarweise verschieden sind. Eine Ecke $b \in E$ ist *von* $a \in E$ *aus erreichbar*, wenn es einen gerichteten Weg von a nach b gibt. Der Digraph G ist *stark zusammenhängend*, wenn jede Ecke von G von jeder anderen Ecke aus erreichbar ist.

Beispiel 233 : Der Digraph



ist stark zusammenhängend, der Digraph

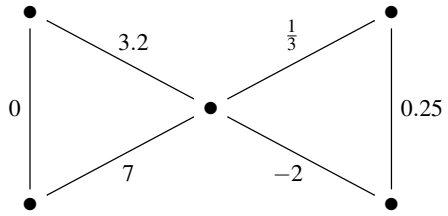


ist zusammenhängend, aber nicht stark zusammenhängend.

§4. Bewertete Graphen und Netzwerke

Definition 234 : $G := (E,K)$ sei ein Graph oder Digraph. Eine Abbildung $w : K \to \mathbb{R}$ heißt *Bewertungsfunktion* von G. Für $k \in K$ heißt die Zahl $w(k)$ die *Bewertung der Kante k*. Das Paar (G,w) heißt dann *bewerteter Graph bzw. Digraph*.

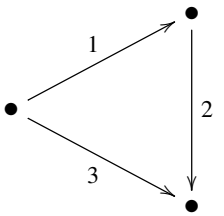
Zeichnerisch kann ein bewerteter Graph oder Digraph dargestellt werden, indem $w(k)$ über (oder unter oder neben) die Kante k geschrieben wird.



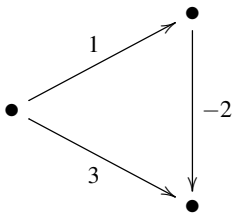
Beispiel 235 : E sei die Menge der Bushaltestellen einer Stadt, K sei die Menge aller Paare (a,b) von Haltestellen mit der Eigenschaft, dass ein Bus ohne Halt von a nach b fährt. Die Bewertung $w\big((a,b)\big)$ der Kante (a,b) sei die durchschnittliche Dauer (in Minuten) der Fahrt von a nach b. Dann ist $\big((E,K),w\big)$ ein bewerteter Digraph.

Definition 236 : Ein bewerteter Digraph heißt *Netzwerk*, wenn er zusammenhängend ist und die Bewertung jeder Kante eine positive Zahl ist. In diesem Fall heißt die Bewertung einer Kante k auch *Kapazität* von k.

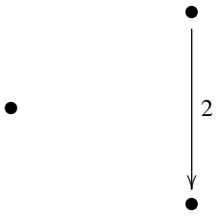
Beispiel 237 : Der bewertete Digraph



ist ein Netzwerk, die bewerteten Digraphen



und



aber nicht.

§5. Speicherung von Graphen

$G = (E,K)$ sei ein Graph oder Digraph. Die Ecken seien geordnet: $E = \{a_1, \ldots, a_n\}$.

Definition 238 : Die ganzzahlige $n \times n$-Matrix
$A := A(G) := (A_{ij})_{1 \le i,j \le n}$ mit

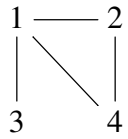
$$A_{ij} := \begin{cases} 1 & \text{wenn } \{a_i, a_j\} \in K \text{ bzw. } (a_i, a_j) \in K \\ 0 & \text{sonst} \end{cases}$$

heißt *Adjazenzmatrix* oder *Nachbarmatrix* von G.

In der Diagonale von $A(G)$ stehen nur Nullen.

Wenn G ein Graph ist, dann ist die Matrix $A(G)$ symmetrisch, d.h.: $A_{ij} = A_{ji}$ für $1 \le i, j \le n$.

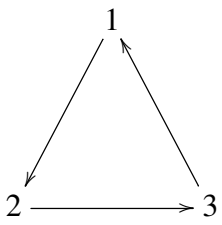
Beispiel 239 : Die Adjazenzmatrix von



ist

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Beispiel 240 : Die Adjazenzmatrix von



ist

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Satz 241 : *Es seien A die Nachbarmatrix von G und p eine positive ganze Zahl. Dann ist $(A^p)_{ij}$ die Anzahl der (gerichteten) Kantenfolgen der Länge p von a_i nach a_j. Insbesondere ist ein Graph bzw. Digraph G genau dann zusammenhängend bzw. stark zusammenhängend, wenn alle Koeffizienten außerhalb der Diagonale von*

$$A + A^2 + \cdots + A^{n-1}$$

positiv sind.

Beweis: Induktion über p.

$p = 1$: nach Definition von A.

$p > 1$: Sei $B := A^{p-1}$. Nach Induktionsannahme ist B_{ir} die Anzahl der (gerichteten) Kantenfolgen der Länge $p-1$ von a_i nach a_r. Eine Kantenfolge der Länge p von a_i nach a_j erhält man, indem man an eine Kantenfolge der Länge $p-1$ von a_i nach $a_r \in E$ eine (gerichtete) Kante von a_r nach a_j anfügt. Daher ist

$$(A^p)_{ij} = \sum_{r=1}^{n} B_{ir} A_{rj} =$$

$$= \sum_{r=1}^{n} (\text{Anzahl der Kantenfolgen der Länge } p-1 \text{ von } a_i \text{ nach } a_r) \cdot$$

$$\cdot (\text{Anzahl der Kanten von } a_r \text{ nach } a_j)$$

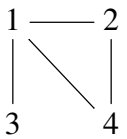
die Anzahl aller Kantenfolgen der Länge p von a_i nach a_j.

Definition 242 : Das n-Tupel

$$\Big(\big(a_i, \{ a_j \mid \{a_i, a_j\} \in K \text{ bzw. } (a_i, a_j) \in K \} \big) \Big)_{1 \le i \le n}$$

heißt Adjazenzliste von G.

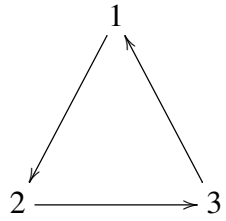
Beispiel 243 : Die Adjazenzliste von



ist

$$\big((1, \{2,3,4\}), (2, \{1,4\}), (3, \{1\}), (4, \{1,2\}) \big).$$

Beispiel 244 : Die Adjazenzliste von



ist

$$\big((1,\{2\}),(2,\{3\}),(3,\{1\})\big).$$

Definition 245 : (G,w) sei ein bewerteter Graph bzw. Digraph.
Sei $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$. Die $n \times n$-Matrix mit Koeffizienten in $\overline{\mathbb{R}}$

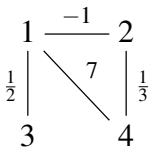
$$A(G,w) := (A_{ij})_{1 \le i,j \le n}$$

mit

$$A_{ij} := \begin{cases} w(\{a_i,a_j\}) \text{ bzw. } w\big((a_i,a_j)\big), & \text{wenn } \{a_i,a_j\} \in K \text{ bzw. } (a_i,a_j) \in K \\ \infty & \text{sonst} \end{cases}$$

heißt *Matrix des bewerteten Graphen* bzw. *Digraphen* (G,w).

Beispiel 246 : Die Matrix von



ist

$$\begin{pmatrix} \infty & -1 & \frac{1}{2} & 7 \\ -1 & \infty & \infty & \frac{1}{3} \\ \frac{1}{2} & \infty & \infty & \infty \\ 7 & \frac{1}{3} & \infty & \infty \end{pmatrix}.$$

§6. Verbindungsprobleme

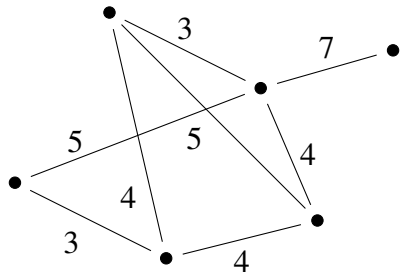
Beispiel 247 : Einige Dörfer sollen mit einer Wasserleitung versorgt werden. Für je zwei Dörfer, die direkt mit einer Wasserleitung verbunden werden können, sind die Kosten dafür bekannt. Bestimme ein Leitungsnetz, das möglichst wenig kostet!

Dieses Problem kann durch einen bewerteten Graphen $\big((E,K),w\big)$ modelliert werden: Die Ecken sind die Dörfer, die Kanten entsprechen den direkten Leitungsverbindungen zwischen zwei Dörfern und die Bewertung einer Kante entspricht den Kosten für diese Leitung. Gesucht ist ein aufspannender Untergraph (E,K') von (E,K) so, dass (E,K') zusammenhängend

ist, keine Kreise enthält und

$$\sum_{k \in K'} w(k)$$

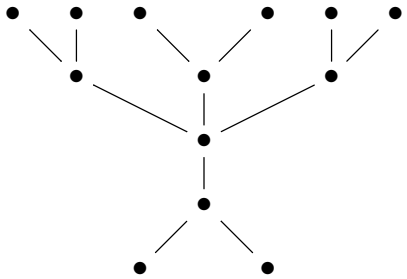
möglichst klein ist.
Zum Beispiel:



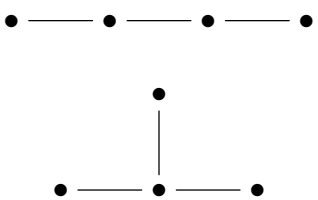
§7. Bäume

Definition 248 : Ein *Wald* ist ein Graph, der keinen Kreis enthält. Ein *Baum* ist ein zusammenhängender Wald. Ein *Blatt* ist eine Ecke eines Baumes, deren Grad 1 ist.

Beispiel 249 :



Beispiel 250 : Es gibt (bis auf Umbenennung der Ecken) nur zwei Bäume mit 4 Ecken:



Der eine Baum hat zwei, der andere drei Blätter.

Satz 251 : *Jeder Wald mit mindestens einer Kante hat mindestens zwei Blätter.*

Beweis: Da die Eckenmenge endlich ist und es in einem Wald keine Kreise gibt, enthält ein Wald Kantenfolgen maximaler Länge. Deren erste und letzte Ecke haben Grad 1.

Satz 252 : *$G := (E,K)$ sei ein Graph. Die folgenden Aussagen sind äquivalent:*

1. *G ist ein Baum.*
2. *Für je zwei Ecken a,b von G gibt es genau einen Weg von a nach b.*
3. *G ist zusammenhängend und hat eine Ecke mehr als Kanten.*
4. *G enthält keine Kreise und hat eine Ecke mehr als Kanten.*

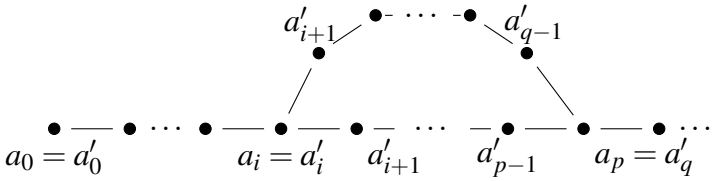
Beweis:

(1) $\Rightarrow$ (2): Jeder Baum ist zusammenhängend, daher gibt es einen Weg $[a = a_0, a_1, \ldots, a_m = b]$ von a nach b.

Sei $[a = a'_0, a'_1, \ldots, a'_n = b]$ ein weiterer Weg von a nach b. Wir nehmen an, dass diese zwei Wege verschieden sind. Wegen $a_0 = a'_0$ gibt es Indizes k mit $a_k = a'_k$ und $a_{k+1} \neq a'_{k+1}$. Sei i die kleinste dieser Zahlen. Wegen $a_m = a'_n$ gibt es Indizes k,l mit $k > i$, $l > i$, $a_{k-1} \neq a'_{l-1}$ und $a_k = a'_l$. Seien p,q die kleinsten dieser Zahlen. Dann ist

$$[a_i, a_{i+1}, \ldots, a_{p-1}, a_p = a'_q, a'_{q-1}, \ldots, a'_{i+1}, a'_i]$$

ein Kreis. In G gibt es aber keine Kreise. Widerspruch.



(2) $\Rightarrow$ (3): G ist nach Definition zusammenhängend. Wir zeigen durch Induktion über $\#(K)$, dass $\#(E) = \#(K) + 1$ ist:
Für $\#(K) = 0$ ist $\#(E) = 1$.
Sei $\#(K) > 0$. Sei $G' = (E,K')$ der Graph, der durch Weglassen einer Kante entsteht. Nach (2) hat G' genau zwei Zusammenhangskomponenten, diese sind Bäume. Nach Induktionsannahme hat jede Zusammenhangskomponente eine Ecke mehr als Kanten. Daher ist
$\#(K) = \#(K') + 1 = \big(\#(E) - 2\big) + 1 = \#(E) - 1$.

(3) $\Rightarrow$ (4): Wir nehmen an, dass G einen Kreis der Länge n (≥ 3) enthält. Für jede Ecke a von G, die nicht zu diesem Kreis gehört, wählen wir einen Weg kürzester Länge zu einer Ecke des Kreises. Sei $k(a)$ die Kante dieses Weges, die a enthält. Die Kanten $k(a)$, $k(b)$ sind für je zwei Ecken a und b, die nicht zum gewählten Kreis gehören,

verschieden. Aus

$$\{k \mid k \text{ Kante des Kreises}\} \dot\cup \\ \dot\cup \{k(a) \mid a \in E,\ a \text{ gehört nicht zum Kreis}\} \subseteq K$$

folgt

$$\#(K) \geq n + \big(\#(E) - n\big) = \#(E),$$

Widerspruch zu (3).

(4) $\Rightarrow$ (1): Nach (4) ist G ein Wald. Wir zeigen noch durch Induktion über $\#(E)$, dass G zusammenhängend ist. Wenn $\#(E) = 1$ ist, ist G zusammenhängend. Sei $\#(E) > 1$. Dann ist
$\#(K) \geq 1$. Nach Satz 251 gibt es in G ein Blatt a. Sei k die Kante die a enthält. Dann ist $G' := \big(E \setminus \{a\}, K \setminus \{k\}\big)$ ein Wald, der eine Ecke mehr als Kanten hat. Nach Induktionsannahme ist G' zusammenhängend, also auch G.

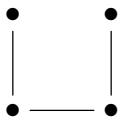
§8. Der Algorithmus von Prim

$(G,w) := \big((E,K),w\big)$ sei ein zusammenhängender bewerteter Graph.

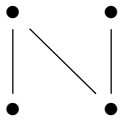
Definition 253 : Ein *Minimalgerüst* von (G,w) ist ein aufspannender Untergraph (E,K') von G mit den Eigenschaften:

- (E,K') ist ein Baum und
- $\sum_{k\in K'} w(k)$ ist möglichst klein.

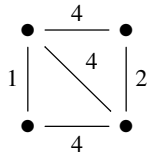
Beispiel 254 : Die Graphen



und

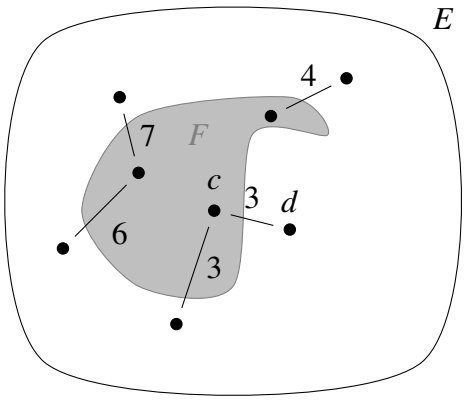


sind Minimalgerüste von



Satz 255: *Mit dem folgenden Algorithmus wird ein Minimalgerüst von (G,w) berechnet:*

- *Wähle eine Ecke a von G. Wähle unter den Nachbarn von a eine Ecke b so, dass $w\big(\{a,b\}\big)$ möglichst klein ist. Setze $F := \{a,b\}$ und $K' := \big\{\{a,b\}\big\}$.*
- *Solange $F \neq E$ ist, wähle $c \in F$, $d \in E \setminus F$ so, dass $\{c,d\} \in K$ und $w(\{c,d\})$ möglichst klein ist. Ersetze F durch $F \cup \{d\}$ und K' durch $K' \cup \big\{\{c,d\}\big\}$.*
- *Dann ist (E,K') ein Minimalgerüst von (G,w).*

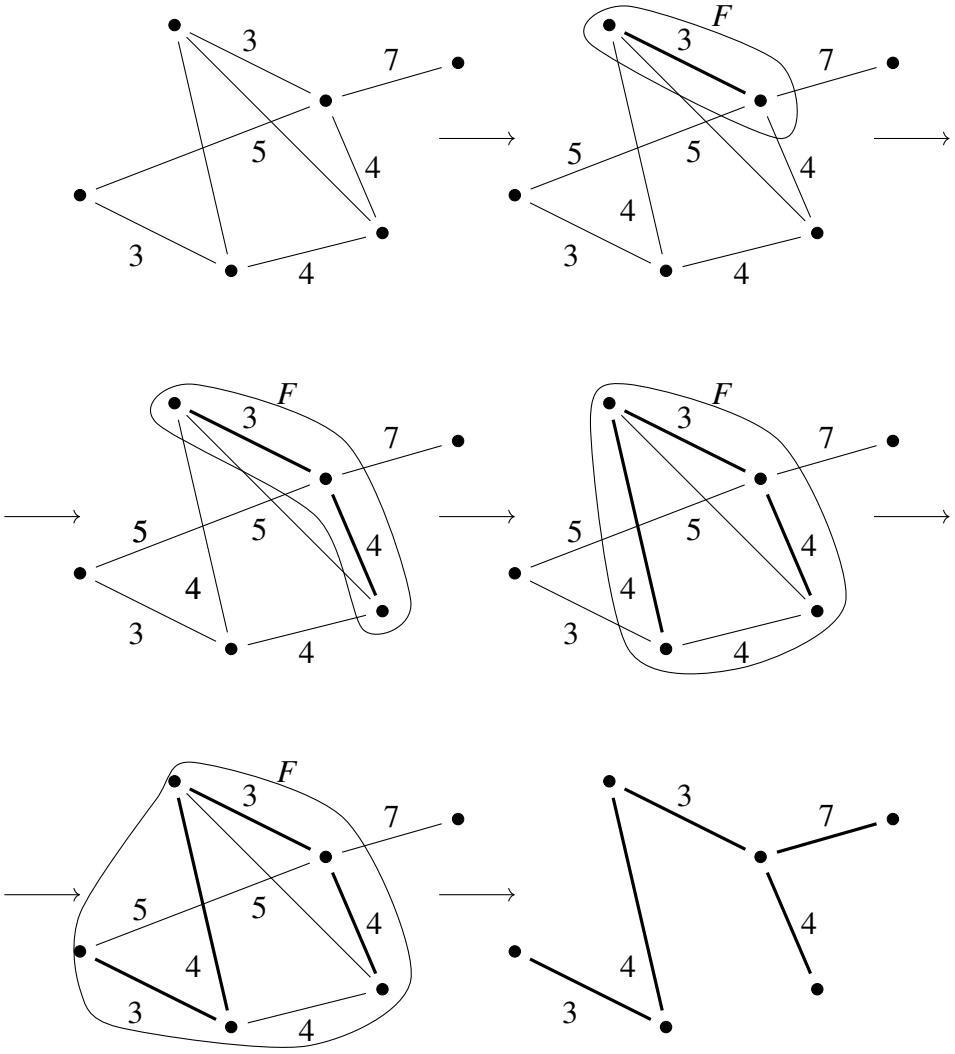


$w(\{c,d\})$ minimal

Beweis: Da G zusammenhängend ist, gibt es immer $c \in F$ und $d \in E \setminus F$ so, dass $\{c,d\} \in K$ ist. In jedem Schritt des Verfahrens wird die Menge F um ein Element vergrößert. Der Algorithmus liefert also nach $\#(E)-2$ Schritten ein Ergebnis (E,K'). Nach Konstruktion ist (E,K') aufspannend und ein Baum. Sei (E,L) ein Minimalgerüst von (G,w) so, dass $\#(K' \cap L)$ möglichst groß ist. Zeige: $L = K'$.

Wir nehmen an, dass $L \neq K'$ ist. Dann gibt es eine Kante $k \in K'$, die nicht in L liegt. Sei F wie in dem Schritt im Verfahren, in dem die Kante k gewählt wird. Dann liegt eine Ecke (a) von k in F, die andere (b) in $E \setminus F$ und $w(k)$ ist minimal mit dieser Eigenschaft. Da (E,L) ein Baum ist, gibt es genau einen Weg in L von a nach b. Auf diesem Weg gibt es eine Kante ℓ, deren eine Ecke in F und deren andere Ecke in $E \setminus F$ liegt. Nach Wahl von k muss $w(k) \leq w(\ell)$ sein. Sei $M := \big(L \setminus \{\ell\}\big) \cup \{k\}$. Weil (E,L) ein Baum ist und ℓ und k in einem Kreis in G liegen, ist (E,M) auch ein Baum. Wegen $w(k) \leq w(\ell)$ ist $\sum_{m \in M} w(m) \leq \sum_{m \in L} w(m)$, also auch (E,M) ein Minimalgerüst. Aber $\#(K' \cap M) > \#(K' \cap L)$, das ist ein Widerspruch zur Wahl von (E,L).

Beispiel 256 :



Summe der Bewertungen der Kanten des Minimalgerüstes: 21.

Bemerkung: Ein *Maximalgerüst* eines bewerteten Graphen (G,w) ist ein aufspannender Untergraph (E,K') von G mit den Eigenschaften:

- (E,K') ist ein Baum und
- $\sum_{k\in K'} w(k)$ ist möglichst groß.

Ein Maximalgerüst von (G,w) ist ein Minimalgerüst von $(G,-w)$ und kann daher auch mit den Algorithmen von Prim berechnet werden.

Bemerkung: Im Algorithmus von Prim werden "lokal richtige" Entscheidungen getroffen, die sich dann auch als "global richtig" erweisen. Bei vielen anderen Problemen der Graphentheorie ist das nicht so.

KAPITEL 5

Das Problem des Briefträgers

Beispiel 257 : Ein Briefträger geht vom Postamt los, durch alle Straßen seines Zustellbereichs und kehrt wieder zum Postamt zurück. Wie muss er gehen, damit die insgesamt zurückgelegte Strecke möglichst kurz ist?

Graphentheoretische Modellierung: Wir betrachten einen bewerteten Graphen, dessen Ecken das Postamt und die Straßenkreuzungen im Zustellbereich sind. Die Kanten entsprechen den Straßenabschnitten zwischen zwei Kreuzungen. Nach Wahl einer Längeneinheit wird jede Kante mit der Entfernung zwischen den zwei Eckpunkten bewertet. Gesucht wird eine geschlossene Kantenfolge $[a_0, a_1, \ldots, a_j = a_0]$ so, dass $\big\{\{a_i, a_{i+1}\} \mid 0 \leq i < j\big\}$ die Menge aller Kanten ist und

$$\sum_{i=0}^{j-1} w(\{a_i, a_{i+1}\})$$

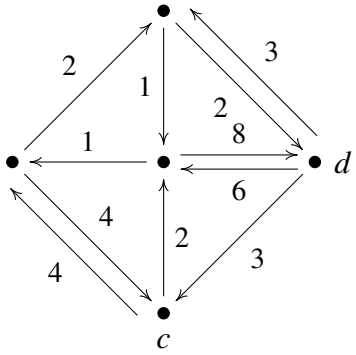
möglichst klein ist.

§1. Kürzeste Wege

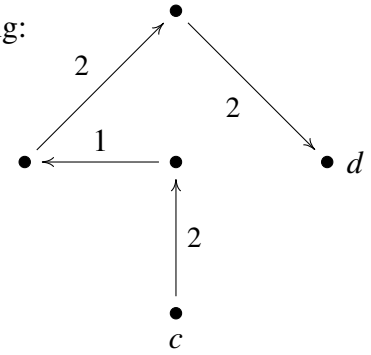
Beispiel 258 : Es seien E eine Menge von Flughäfen, K die Menge aller Paare (a,b) von Flughäfen so, dass es von a nach b einen Direktflug gibt. Für $(a,b) \in K$ sei $w\big((a,b)\big)$ die Zeit für einen Flug von a nach b. Dann ist $\big((E,K),w\big)$ ein bewerteter Digraph. Seien c,d zwei Flughäfen so, dass es einen gerichteten Weg von c nach d gibt. Finde einen gerichteten Weg $[c = a_0, \ldots, a_j = d]$ so, dass die gesamte Flugzeit, also

$$\sum_{i=0}^{j-1} w\big((a_i, a_{i+1})\big) \ ,$$

möglichst klein ist!



Lösung:



Definition 259 : Sei $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$. Wir erweitern die Ordnung $\leq$ von $\mathbb{R}$ auf $\overline{\mathbb{R}}$ durch:

$$\text{für alle } z \in \mathbb{R} \text{ ist } z < \infty.$$

Für alle $z \in \overline{\mathbb{R}}$ sei $z + \infty := \infty$.

Im weiteren sei $\big(G := (E,K), w\big)$ ein bewerteter Graph bzw. Digraph. Für $a,b \in E$ mit $\ell := \{a,b\} \notin K$ bzw. $\ell := (a,b) \notin K$ setzen wir $w(\ell) := \infty$.

Definition 260 : Die *Länge eines Weges* bzw. *eines gerichteten Weges* ist die Summe der Bewertungen seiner Kanten. Der *Abstand* $d_G(a,b)$ von einer Ecke a zu einer Ecke b in G ist die kleinste Länge eines Weges bzw. gerichteten Weges von a nach b, falls ein solcher existiert, und ∞ sonst. Ein Weg bzw. gerichteter Weg $[a = a_0, \ldots, a_j = b]$ ist ein *kürzester Weg* von a nach b, wenn

$$\sum_{i=0}^{j-1} w(\{a_i, a_{i+1}\}) = d_G(a,b) \quad \text{bzw.} \quad \sum_{i=0}^{j-1} w((a_i, a_{i+1})) = d_G(a,b)$$

ist.

Im weiteren nehmen wir ohne Einschränkung der Allgemeinheit an, dass G ein gerichteter Graph ist. (Falls nicht, ersetzen wir jede Kante $k := \{a,b\}$ durch die zwei gerichteten Kanten (a,b) und (b,a) und bewerten beide mit $w(k)$).

Satz 261 : *Seien $A \subsetneq E$, $a \in A$ und $w(k) > 0$ für alle $k \in K$. Sei $b \in E \setminus A$ so, dass*

$$s(b) := \min_{d \in A} \big(d_G(a,d) + w((d,b))\big)$$

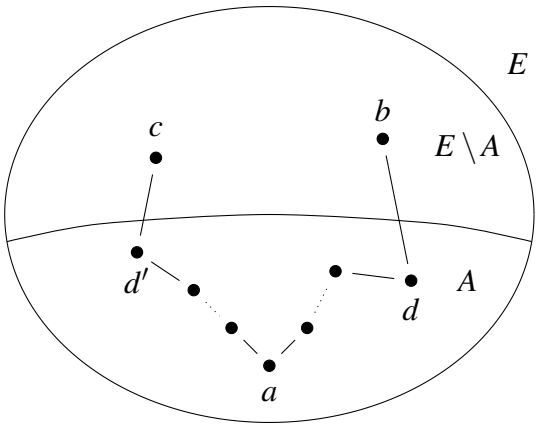
möglichst klein (also $s(b) = \min_{c \in E \setminus A} \min_{d \in A} \left(d_G(a,d) + w((d,c)) \right)$ *ist. Dann ist*

$$s(b) = d_G(a,b)$$

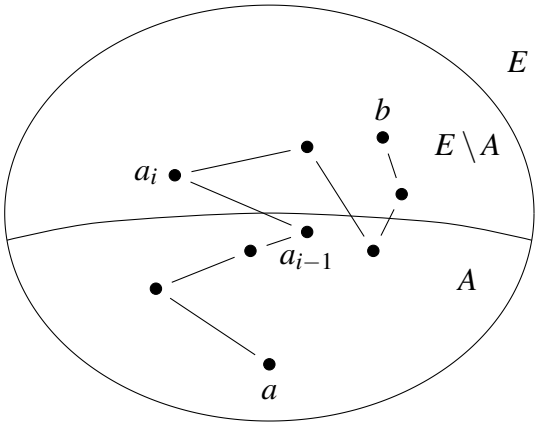
und

$$d_G(a,b) = \min_{c \in E \setminus A} d_G(a,c) \ ,$$

also: alle Ecken außer b eines kürzesten Weges von a nach b sind Elemente von A und b ist jene Ecke in $E \setminus A$*, die von a den kleinsten Abstand hat.*



Beweis: Wenn es keinen gerichteten Weg von a zu einer Ecke in $E \setminus A$ gibt, ist die Behauptung leicht nachzuprüfen. Wir können daher annehmen, dass es einen Weg von a nach b gibt. Sei $[a = a_0, a_1, \ldots, a_j = b]$ ein kürzester Weg von a nach b. Sei i der kleinste Index so, dass $a_i \notin A$ ist.



Es ist $d_G(a,a_{i-1}) + w((a_{i-1},a_i)) + d_G(a_i,b) = d_G(a,b)$. Wäre $i \neq j$, dann wäre $d_G(a_i,b) > 0$ (weil die Bewertungen aller Kanten positiv sind) und daher $d_G(a,a_{i-1}) + w((a_{i-1},a_i)) < d_G(a,b)$.
Wegen

$$s(a_i) := \min_{d \in A} \left(d_G(a,d) + w((d,a_i)) \right) \leq d_G(a,a_{i-1}) + w((a_{i-1},a_i))$$

und

$$d_G(a,b) \leq s(b)$$

wäre dann $s(a_i) < s(b)$. Widerspruch zur Wahl von b. Also ist $i = j$ und

$$d_G(a,b) = d_G(a,a_{i-1}) + w((a_{i-1},b)) = \min_{d\in A}\left(d_G(a,d) + w((d,b))\right) .$$

Satz 261 liefert die Idee für ein Verfahren zur Berechnung eines kürzesten Weges von einer Ecke a zu einer Ecke b in G:

Wenn die kürzesten Wege von a zu allen Elementen einer Teilmenge $A \subsetneq E$ mit $a \in A$ bereits bestimmt sind, dann können mit Satz 261 eine Ecke $c \in E \setminus A$, deren Abstand von a kleinstmöglich ist, und ein kürzester Weg von a nach c ermittelt werden. Ersetze dann A durch $A \cup \{c\}$. Wiederhole das solange, bis $c = b$ ist.

Satz 262 (Algorithmus von Dijkstra)**:** *Seien $a \in E$, $a \neq b \in E$ und $w(k) > 0$ für alle $k \in K$. Mit dem folgenden Algorithmus werden der Abstand $d_G(a,b)$ von a nach b und, falls $d_G(a,b) < \infty$ ist, ein kürzester Weg von a nach b berechnet:*

- *Setze $i := 0$, $a_0 := a$, $A_0 := \{a_0\}$ und definiere die Abbildung $f_0 : E \to \overline{\mathbb{R}}$ durch*

$$f_0(a_0) := 0 \text{ und } f_0(c) := \infty \text{ für } c \in E \setminus A_0.$$

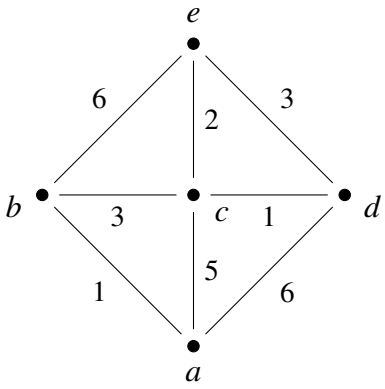
(⋆) • *Definiere die Abbildung $f_{i+1} : E \to \overline{\mathbb{R}}$ durch*

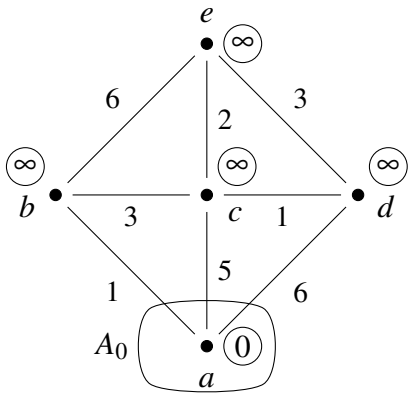
$$f_{i+1}(c) := \begin{cases} f_i(c), & \text{falls } c \in A_i \text{ ist,} \\ \min\{f_i(c), f_i(a_i) + w((a_i,c))\}, & \text{falls } c \in E \setminus A_i \text{ ist.} \end{cases}$$

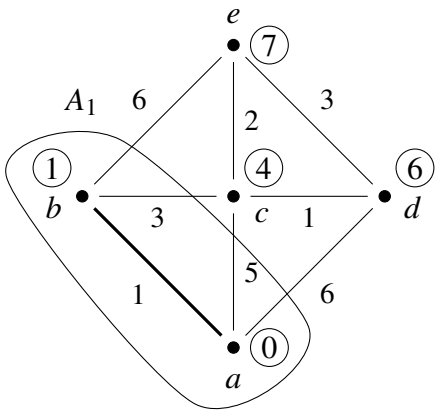
- *Wähle $c \in E \setminus A_i$ so, dass $f_{i+1}(c)$ möglichst klein ist. Setze $a_{i+1} := c$, $A_{i+1} := A_i \cup \{a_{i+1}\}$ und dann $i := i+1$.*
- *Wenn $a_i \neq b$ ist, gehe zurück zu (⋆). Sonst ist $d_G(a,b) = f_i(b)$ (und auch $d_G(a,x) = f_i(x)$ für alle $x \in A_i$).*
- *Wenn $d_G(a,b) = \infty$ ist, gibt es keinen gerichteten Weg von a nach b. Sonst sei $j_0 := i$ und $p := 0$.*
- *Solange $j_p \neq 0$ ist, setze*

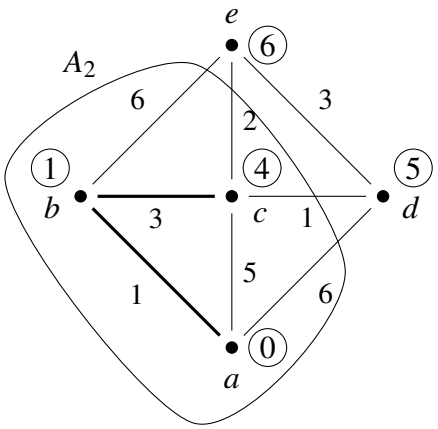
$$j_{p+1} := \min\{r \mid f_{r+1}(a_{j_p}) = f_{j_p}(a_{j_p})\} \quad \text{und}$$
$$p := p+1.$$

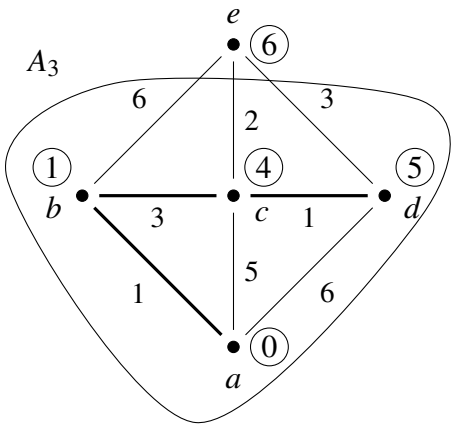
Dann ist $[a = a_0, \ldots, a_{j_2}, a_{j_1}, a_{j_0} = b]$ ein kürzester Weg von a nach b.

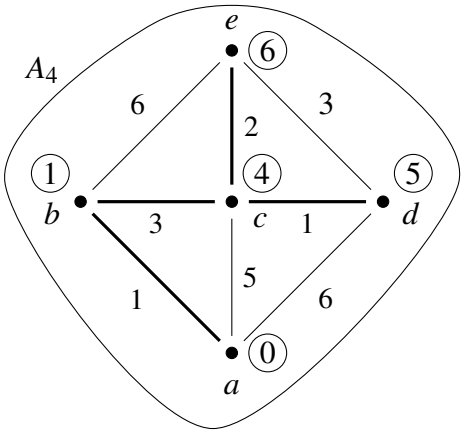












Somit: $d_G(a,e) = 6$, kürzester Weg von a nach e: $[a,b,c,e]$. Weiters ist $d_G(a,d) = 5$.

Beweis: Zeige durch Induktion über i, dass $f_i(a_i) = d_G(a, a_i)$, $0 \leq i < n$, ist.

$i = 0$: $f_0(a_0) = 0 = d_G(a_0, a_0)$.
$i > 0$: Die Ecken $a_0, a_1, \ldots, a_{i-1}$ wurden so gewählt, dass für alle $c \in E \setminus A_{i-1}$ gilt:

$$f_i(c) = \min_{0 \leq j < i} \big(f_j(a_j) + w((a_j, c)) \big).$$

Nach Induktionsannahme ist

$$f_j(a_j) = d_G(a, a_j), \quad 1 \leq j < i,$$

daher ist

$$f_i(c) = \min_{d \in A_{i-1}} \big(d_G(a, d) + w((d, c)) \big).$$

Also gilt für a_i:

$$\min_{d \in A_{i-1}} \big(d_G(a, d) + w((d, a_i)) \big) = f_i(a_i) =$$
$$= \min_{c \in E \setminus A_{i-1}} f_i(c) = \min_{c \in E \setminus A_{i-1}} \min_{d \in A_{i-1}} \big(d_G(a, d) + w((d, c)) \big).$$

Nach Satz 261 ist daher $f_i(a_i) = d_G(a, a_i)$.

Beispiel 263 : Sei G der bewertete Graph mit Eckenmenge $\{1, 2, 3, \ldots, 8\}$, dessen Matrix

$$\begin{pmatrix} \infty & 1 & \infty & 2 & 7 & 8 & 5 & 9 \\ 1 & \infty & 3 & 1 & \infty & \infty & \infty & 8 \\ \infty & 3 & \infty & \infty & \infty & 1 & 3 & 7 \\ 2 & 1 & \infty & \infty & 6 & 5 & 9 & 6 \\ 7 & \infty & \infty & 6 & \infty & 4 & 9 & 5 \\ 8 & \infty & 1 & 5 & 4 & \infty & \infty & 4 \\ 5 & \infty & 3 & 9 & 9 & \infty & \infty & 3 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & \infty \end{pmatrix}$$

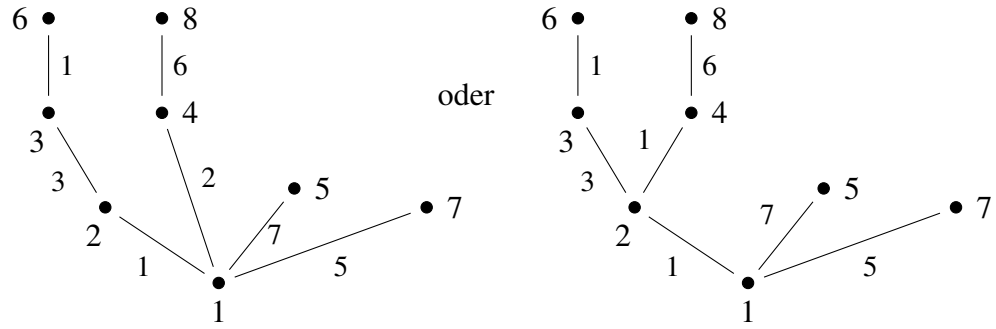
ist. Gesucht ist ein kürzester Weg von 1 nach 8 und von 1 nach 6. Wir schreiben die Abbildung $f_i : E \to \overline{\mathbb{R}}$ als 8-Tupel

$$f_i = \big(f_i(1), f_i(2), \ldots, f_i(8) \big)$$

an.

$$
\begin{aligned}
f_0 &= (\underline{0},\infty,\infty,\infty,\infty,\infty,\infty,\infty)\\
a_0 &= 1\\
f_1 &= (0,\underline{1},\infty,2,7,8,5,9)\\
a_1 &= 2\\
f_2 &= (0,1,4,\underline{2},7,8,5,9)\\
a_2 &= 4\\
f_3 &= (0,1,\underline{4},2,7,7,5,8)\\
a_3 &= 3\\
f_4 &= (0,1,4,2,7,\underline{5},5,8)\\
a_4 &= 6\\
f_5 &= (0,1,4,2,7,5,\underline{5},8)\\
a_5 &= 7\\
f_6 &= (0,1,4,2,\underline{7},5,5,8)\\
a_6 &= 5\\
f_7 &= (0,1,4,2,7,5,5,\underline{8})\\
a_7 &= 8
\end{aligned}
$$

Baum der kürzesten Wege:



$d_G(1,8) = 8$, kürzester Weg: $[1,4,8]$ oder $[1,2,4,8]$.
$d_G(1,6) = 5$, kürzester Weg: $[1,2,3,6]$.

§2. Eulersche Touren

In diesem Abschnitt sei $G = (E,K)$ ein Graph, in dem keine Ecke den Grad 0 hat.

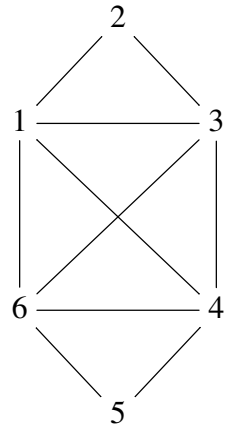
Definition 264 : Ein *Kantenzug* in G ist eine Kantenfolge $[a_0,a_1,\ldots,a_n]$ so, dass die Kanten $\{a_i,a_{i+1}\}$, $0 \leq i < n$, paarweise verschieden sind. ("In einem Kantenzug kommt jede Kante höchstens einmal vor").

Ein *Eulerscher Kantenzug* in G ist ein Kantenzug $[a_0,a_1,\ldots,a_n]$ so, dass $K = \big\{\{a_i,a_{i+1}\} \mid 0 \leq i < n\big\}$ ist. ("In einem Eulerschen Kantenzug kommt jede Kante von G genau einmal vor").

Eine *Eulersche Tour* in G ist ein geschlossener Eulerscher Kantenzug.

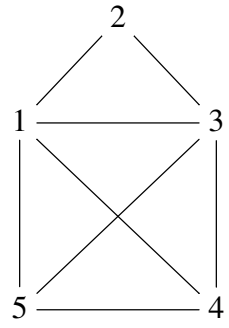
G ist ein *Eulerscher Graph*, wenn es in G eine Eulersche Tour gibt.

Beispiel 265 : Der Graph



ist Eulersch, $[1,2,3,1,4,3,6,4,5,6,1]$ ist ein Eulersche Tour.

Beispiel 266 : Der Graph



ist nicht Eulersch, $[5,1,2,3,1,4,3,5,4]$ ist ein Eulerscher Kantenzug.

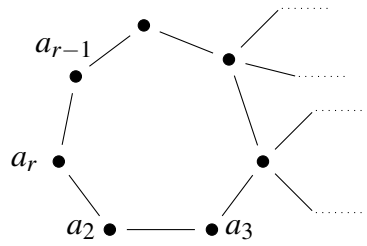
Satz 267 : *G ist genau dann Eulersch, wenn G zusammenhängend und der Grad jeder Ecke gerade ist. In diesem Fall kann mit dem folgenden Algorithmus (von Hierholzer) eine Eulersche Tour bestimmt werden:*

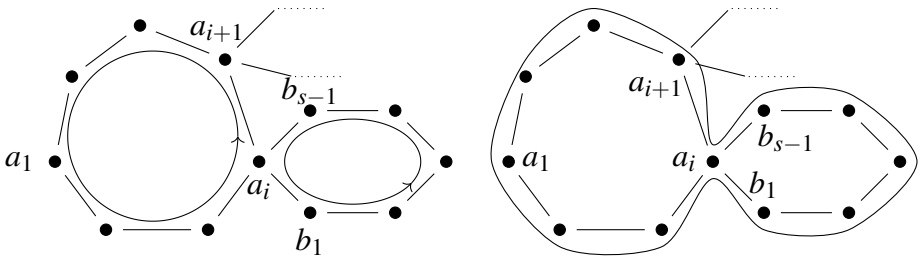
- *Wähle $a_1 \in E$ und einen Kantenzug $X := [a_1, \ldots, a_r]$ in G, der nicht mehr fortgesetzt werden kann. (Jede Ecke ist gerade, also muss $a_1 = a_r$ sein).*

($\star$) • *Falls X eine Eulersche Tour ist: Ende.*
Sonst sei $K' := K \setminus \{\{a_i, a_{i+1}\} \mid 1 \leq i < r\}$ und $G' := (E, K')$. Wähle $i \in \{1, \ldots, r-1\}$ so, dass a_i Eckpunkt einer Kante in K' ist (eine solche Ecke existiert, weil $K' \neq \emptyset$ und G zusammenhängend ist). Wähle einen Kantenzug $Y := [a_i, b_1, \ldots, b_s]$ in G', der nicht mehr fortgesetzt werden kann. (Da auch jede Ecke von G' gerade ist, muss $a_i = b_s$ sein). Setze X und Y zum geschlossenen Kantenzug

$$Z := [a_1, \ldots, a_i, b_1, \ldots, b_s = a_i, a_{i+1}, \ldots, a_r]$$

zusammen. Ersetze X durch Z und gehe zurück zu ($\star$).



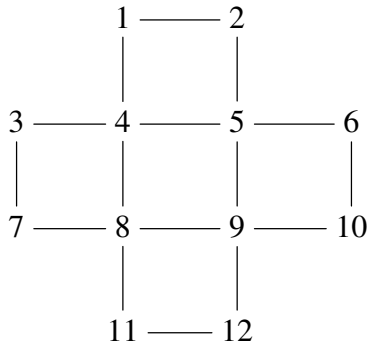


Beweis: Wir nehmen zuerst an, dass es in G eine Eulersche Tour gibt. Wird bei dieser eine Ecke a über eine Kante erreicht, dann wird sie über eine *andere* Kante wieder verlassen. Also muss der Grad von a gerade sein.

Sei nun G zusammenhängend und der Grad jeder Ecke von G gerade. Dann ist der Algorithmus von Hierholzer korrekt, denn: bei jedem Durchlauf von ($\star$) wird die Anzahl der Kanten in der Kantenfolge X vergrößert,

also ist X nach höchstens $\#(K)$ Schritten eine Eulersche Tour. Insbesondere ist G Eulersch.

Beispiel 268 : Der Graph



ist zusammenhängend und alle Ecken sind gerade. Der Kantenzug

$$X := [1,4,8,11,12,9,5,2,1]$$

kann nicht mehr fortgesetzt werden. Sei

$$Y := [4,3,7,8,9,10,6,5,4],$$

dann ist

$$Z := [1,4,3,7,8,9,10,6,5,4,8,11,12,9,5,2,1]$$

eine Eulersche Tour.

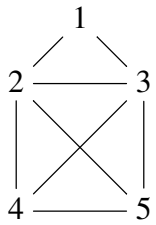
Wenn es im Zustellbereich eines Briefträgers nur Kreuzungen mit einer geraden Anzahl einmündender Straßen gibt, dann kann das Problem des Briefträgers mit dem Algorithmus von Hierholzer gelöst werden.

Satz 269 : *In G gibt es genau dann einen Eulerschen Kantenzug, wenn G zusammenhängend ist und höchstens zwei ungerade Ecken enthält.*

Beweis:

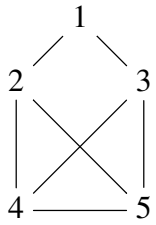
- $\Rightarrow$: Nur die Anfangs- und Endecke eine Eulerschen Kantenzuges können ungerade Ecken sein.
- $\Leftarrow$: Nach Satz 1 gibt es entweder keine oder genau zwei ungerade Ecken. Wenn alle Ecken gerade sind, folgt die Behauptung aus Satz 267. Seien a und b zwei ungerade Ecken in G. Sei $c \notin E$ und $H := \big(E \cup \{c\}, K \cup \big\{\{a,c\},\{b,c\}\big\}\big)$. Dann sind alle Ecken von H gerade und H ist zusammenhängend. Nach Satz 267 gibt es eine Eulersche Tour $[c, a = d_1, \ldots, d_r = b, c]$ in H. Dann ist $[a = d_1, \ldots, d_r = b]$ ein Eulerscher Kantenzug in G.

Beispiel 270 : Im Graphen



gibt es einen Eulerschen Kantenzug, zum Beispiel $[4,2,1,3,2,5,3,4,5]$.

Im Graphen



sind 4 Ecken ungerade, also gibt es keinen Eulerschen Kantenzug.

§3. Optimale Touren

In diesem Abschnitt sei $(G,w) := \big((E,K),w\big)$ ein zusammenhängender bewerteter Graph und für alle $k \in K$ sei $w(k) > 0$.

Definition 271 : Eine *Tour* in G ist eine geschlossene Kantenfolge $T := [a_0, a_1, \ldots, a_n]$ so, dass

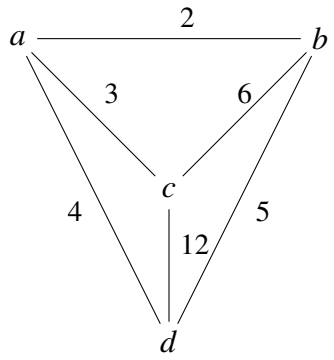
$$K = \big\{\{a_i, a_{i+1}\} \mid 0 \leq i < n\big\}$$

ist. Die Zahl

$$w(T) := \sum_{i=0}^{n-1} w(\{a_i, a_{i+1}\})$$

heißt *Bewertung* der Tour T. Eine Tour T ist *optimal*, wenn ihr Bewertung möglichst klein ist, das heißt: für jede Tour S in G ist $w(S) \geq w(T)$.

Beispiel 272 : G sei der vollständige Graph mit Eckenmenge $\{a,b,c,d\}$ und den folgenden Bewertungen der Kanten:



Dann sind die geschlossenen Kantenfolgen

$$T_1 := [a,b,c,d,a,c,d,b,a] \quad \text{und}$$
$$T_2 := [a,b,d,c,b,d,a,c,a]$$

Touren, ihre Bewertungen sind $w(T_1) = 49$ und $w(T_2) = 46$.

Beispiel 273 : Wenn G ein Eulerscher Graph ist, dann ist eine Tour genau dann optimal, wenn sie eine Eulersche Tour ist.

Satz 274 : *In einer optimalen Tour in G wird jede Kante höchstens zweimal durchlaufen.*

Beweis: Sei T eine optimale Tour. Wir nehmen an, die Kante $\{a,b\}$ werde mehr als zweimal durchlaufen, o. E. d. A. zuerst in der Reihenfolge a,b. Dann sind vier Fälle zu unterscheiden:

$$T = [\ldots,a,b,\ldots,a,b,\ldots,a,b,\ldots] \quad \text{oder}$$
$$T = [\ldots,a,b,\ldots,a,b,\ldots,b,a,\ldots] \quad \text{oder}$$
$$T = [\ldots,a,b,\ldots,b,a,\ldots,a,b,\ldots] \quad \text{oder}$$
$$T = [\ldots,a,b,\ldots,b,a,\ldots,b,a,\ldots].$$

Im ersten Fall

$$T = [\ldots,a,b,\ldots,a,b,c_1,\ldots,c_r,a,b,\ldots]$$

wäre

$$T' := [\ldots,a,b,\ldots,a,c_r,c_{r-1},\ldots,c_1,b,\ldots]$$

ebenfalls eine Tour und $w(T') + w(\{a,b\}) = w(T)$, Widerspruch zur Optimalität von T. Die anderen drei Fälle werden analog ausgeschlossen.

Satz 275 : *Mit dem folgenden Verfahren wird eine optimale Tour in (G,w) ermittelt:*

- *Falls G Eulersch ist, bestimme mit Satz 267 eine Eulersche Tour, diese ist optimal. Ende.*
- *Seien $a_1,\ldots,a_{2m}$ die ungeraden Ecken in G (ihre Anzahl ist immer gerade). Berechne mit Satz 262 alle Abstände $d_G(a_i,a_j)$, $1 \le i < j \le 2m$.*
- *Wähle $b_1,\ldots,b_m,c_1,\ldots,c_m$ so, dass*

$$\{b_1,\ldots,b_m,c_1,\ldots,c_m\} = \{a_1,\ldots a_{2m}\}$$

und

$$\sum_{i=1}^{m} d_G(b_i,c_i)$$

möglichst klein ist, das heißt: sind $b'_1,\ldots,b'_m,c'_1,\ldots,c'_m$ so, dass

$$\{b'_1,\ldots,b'_m,c'_1,\ldots,c'_m\} = \{a_1,\ldots a_{2m}\}$$

ist, dann ist

$$\sum_{i=1}^{m} d_G(b_i,c_i) \le \sum_{i=1}^{m} d_G(b'_i,c'_i).$$

Berechne kürzeste Wege W_i von b_i nach c_i, $1 \le i \le m$. Sei $\overline{W}_i$ der entsprechende Weg von c_i nach b_i, $1 \le i \le m$.
- *Seien $x_1,\ldots,x_m$ paarweise verschiedene Elemente, die nicht in E enthalten sind. Sei*

$$H := \big(E \cup \{x_1,\ldots,x_m\}, K \cup \big\{\{b_i,x_i\},\{x_i,c_i\} \mid 1 \le i \le m\big\}\big).$$

(Dann ist G ein Untergraph von H und H ist Eulersch).
- *Bestimme mit Satz 267 eine Eulersche Tour in H. Ersetze in dieser Tour $\ldots,b_i,x_i,c_i,\ldots$ durch $\ldots W_i \ldots$ und $\ldots,c_i,x_i,b_i,\ldots$ durch $\ldots \overline{W}_i \ldots$. Die so konstruierte Folge von Ecken ist eine optimale Tour in G. Die Bewertung dieser Tour ist*

$$\sum_{k \in K} w(k) + \sum_{i=1}^{m} d_G(b_i,c_i).$$

Beispiel 276 : Im bewerteten Graphen im Beispiel 272 sind alle 4 Ecken ungerade. Die Abstände zwischen diesen Ecken sind in der folgenden Tabelle dargestellt. Zum Beispiel: Der Abstand zwischen b und d ist 6 (Eintrag in der zweiten Zeile und dritten Spalte).

	a	b	c	d
a	0	2	3	4
b	2	0	5	5
c	3	5	0	7
d	4	5	7	0

Daher ist

$$d_G(a,d)+d_G(b,c)=4+5=9$$
$$d_G(a,b)+d_G(c,d)=2+7=9$$

und

$$d_G(a,c)+d_G(b,d)=3+5=8.$$

Eine optimale Tour ist $[b,a,c,d,b,c,a,d,b]$, ihre Bewertung ist 40.

Beweis: Es ist leicht nachzuprüfen, dass die konstruierte Folge von Ecken eine Tour in G ist. Wir zeigen noch, dass die Bewertung einer optimalen Tour größer oder gleich

$$\sum_{k\in K} w(k)+\sum_{i=1}^{m} d_G(b_i,c_i)$$

ist. Sei $[v_0,v_1,\ldots,v_s=v_0]$ eine optimale Tour in G und $k_i:=\{v_i,v_{i+1}\}$, $0\le i<s$. Sei

$$J:=\{j \mid 0\le j<s, \text{ es gibt ein } i<j \text{ mit } k_i=k_j\}.$$

Seien y_j, $j\in J$, paarweise verschiedene Elemente, die nicht in E enthalten sind. Sei G_1 der Graph mit Eckenmenge $E\cup\{y_j \mid j\in J\}$ und Kantenmenge $K\cup\big\{\{v_j,y_j\},\{y_j,v_{j+1}\} \mid j\in J\big\}$. Sei T die Folge von Ecken in G_1, die man durch Einfügen von y_j zwischen v_j und v_{j+1}, für alle $j\in J$, erhält:

$$T=[v_0,v_1,\ldots,v_j,y_j,v_{j+1},\ldots,v_s=v_0].$$

Nach Satz 274 ist T eine Eulersche Tour im Graphen G_1. Entfernt man aus T alle Kanten in K, dann verbleibt, eine Vereinigung von Kantenzügen $Z_1,\ldots,Z_r$, wobei $Z_i=[v_j,y_j,v_{j+1},y_{j+1},v_{j+2},\ldots]$ ist für ein $j\in J$. Die Grade (in G) der Anfangs- und Endecken von Z_i, $1\le i\le r$, sind ungerade, die aller anderen Ecken sind gerade. Also ist die Menge dieser Anfangs- und Endpunkte gleich der Menge $\{a_1,a_2,\ldots,a_{2m}\}$ der ungeraden Ecken von G, insbesondere ist $m=r$. Sei u_{2i-1} bzw. u_{2i} die Anfangs- bzw. Endecke von Z_i, $1\le i\le m$. Dann ist

$$\begin{aligned} w([v_0,v_1,\ldots,v_s=v_0]) &= \sum_{i=0}^{s-1} w(\{v_i,v_{i+1}\}) \ge \\ &\ge \sum_{k\in K} w(k)+\sum_{i=0}^{m} d_G(u_{2i-1},u_{2i}) \ge \\ &\ge \sum_{k\in K} w(k)+\sum_{i=0}^{m} d_G(b_i,c_i). \end{aligned}$$

KAPITEL 6

Polynomfunktionen und Polynome in mehreren Variablen

§1. Polynome in mehreren Variablen

In diesem Abschnitt seien R ein kommutativer Ring und n eine positive ganze Zahl. Der *Betrag* eines Elementes $i \in \mathbb{N}^n$ ist die Zahl

$$|i| := |(i_1, \ldots, i_n)| := i_1 + i_2 + \ldots + i_n \ .$$

Auf $\mathbb{N}^n$ betrachten wir die *komponentenweise Addition*:
für $i, j \in \mathbb{N}^n$ ist

$$i + j := (i_1, \ldots, i_n) + (j_1, \ldots, j_n) := (i_1 + j_1, \ldots, i_n + j_n) \ .$$

Dann ist

$$|i + j| = |i| + |j| \ .$$

Für jedes $k \in \mathbb{N}^n$ gibt es nur endliche viele Paare $(i, j) \in \mathbb{N}^n \times \mathbb{N}^n$ mit der Eigenschaft $i + j = k$.

Definition 277 : Eine Familie $(r_i)_{i \in \mathbb{N}^n}$ in R ist eine *endliche Familie* mit Indexmenge $\mathbb{N}^n$, wenn es nur endlich viele Indizes $i \in \mathbb{N}^n$ mit $r_i \neq 0$ gibt.

Satz 278 : *Die Menge P_n aller endlichen Familien mit Indexmenge $\mathbb{N}^n$ in R mit den Funktionen*

$$+ : P_n \times P_n \longrightarrow P_n \qquad ,$$

$$((r_i)_{i \in \mathbb{N}^n}, (s_i)_{i \in \mathbb{N}^n}) \longmapsto (r_i)_{i \in \mathbb{N}^n} + (s_i)_{i \in \mathbb{N}^n} := (r_i + s_i)_{i \in \mathbb{N}^n} \ ,$$

$$\cdot : P_n \times P_n \longrightarrow P_n \qquad ,$$

$$((r_i)_{i \in \mathbb{N}^n}, (s_i)_{i \in \mathbb{N}^n}) \longmapsto (r_i)_{i \in \mathbb{N}^n} \cdot (s_i)_{i \in \mathbb{N}^n} := (\sum_{i,j \in \mathbb{N}^n,\ i+j=k} r_i s_j)_{k \in \mathbb{N}^n} \ ,$$

und

$$\cdot : R \times P_n \longrightarrow P_n \ , \ (r, (s_i)_{i \in \mathbb{N}^n}) \longmapsto r \cdot (s_i)_{i \in \mathbb{N}^n} := (r s_i)_{i \in \mathbb{N}^n} \ ,$$

ist eine kommutative R-Algebra. Sie heißt Polynomring (in n Variablen) über R *oder* Algebra der Polynome (in n Variablen) mit Koeffizienten in R. *Ihre Elemente heißen* Polynome in n Variablen mit Koeffizienten in R. *Das Nullelement des Polynomringes in n Variablen ist die Familie $0 := (0)_{i \in \mathbb{N}^n}$, das Einselement ist die Familie $1 := (\delta_{i0})_{i \in \mathbb{N}^n}$, wobei δ_{i0} gleich 1 ist, wenn $i = 0$, und 0 sonst.*

Beweis: Übung.

Definition 279 : Es sei $f = (r_i)_{i\in\mathbb{N}^n} \neq 0$ ein Polynom mit Koeffizienten in R. Der *Grad* von f oder *Totalgrad* von f ist die größte Zahl in

$$\{\,|i| \mid i \in \mathbb{N}^n, r_i \neq 0\}$$

und wird mit $\mathrm{gr}(f)$ bezeichnet. Das Polynom f heißt *homogen vom Grad* $d \in \mathbb{N}$, wenn für alle $i \in \mathbb{N}^n$ mit $r_i \neq 0$ gilt: $|i| = d$. Homogene Polynome vom Grad 1 bzw. 2 heißen *Linearformen* bzw. *quadratische Formen*.
Die folgende Schreibweise ist zweckmäßig: Wir wählen n Symbole, zum Beispiel $x_1,\ldots,x_n$, und schreiben

$$\sum_{i\in\mathbb{N}^n} r_i x^i \quad \text{oder} \quad \sum_{i_1,\ldots,i_n} r_{i_1\ldots i_n} x_1^{i_1} x_2^{i_2}\ldots x_n^{i_n} \quad \text{statt} \quad (r_i)_{i\in\mathbb{N}^n}\ .$$

Wir sprechen dann von einem *Polynom in den Variablen* $x_1,\ldots,x_n$ *mit Koeffizienten in* R. Für den Polynomring über R schreiben wir dann $R[x_1,\ldots,x_n]$ oder, wenn n fest gewählt ist, $R[x]$. Wir identifizieren Polynome vom Grad 0 mit ihren nullten Koeffizienten und fassen R so als Teilmenge von $R[x_1,\ldots,x_n]$ auf. Die Polynome

$$x^j := (\delta_{ij})_{i\in\mathbb{N}^n}\ , \quad j \in \mathbb{N}^n\ ,$$

wobei δ_{ij} gleich 1 ist, wenn $i = j$, und 0 sonst, heißen *Potenzprodukte in n Variablen*.

Satz 280 : *Die Familie der Potenzprodukte* $(x^i)_{i\in\mathbb{N}^n}$ *ist eine R-Basis von* $R[x_1,\ldots,x_n]$.

Beweis: Übung.

Der Polynomring $R[x_1,\ldots,x_n]$ in n Variablen mit Koeffizienten in R kann durch

$$\sum_{i\in\mathbb{N}^n} r_i x^i = \sum_{i_n}\Big(\sum_{i_1,\ldots,i_{n-1}} r_i x_1^{i_1} x_2^{i_2}\ldots x_{n-1}^{i_{n-1}}\Big)x^{i_n}$$

als Polynomring $R[x_1,\ldots,x_{n-1}][x_n]$ in einer Variablen mit Koeffizienten in $R[x_1,\ldots,x_{n-1}]$ oder durch

$$\sum_{i\in\mathbb{N}^n} r_i x^i = \sum_{i_2,\ldots,i_n}\Big(\sum_{i_1} r_i x_1^{i_1}\Big)x_2^{i_2}\ldots x_{n-1}^{i_{n-1}} x^{i_n}$$

als Polynomring $R[x_1][x_2,\ldots,x_n]$ in $n-1$ Variablen mit Koeffizienten in $R[x_1]$ aufgefasst werden.

Satz 281 :

(1) *Wenn R ein Integritätsbereich ist, dann auch* $R[x_1,\ldots,x_n]$ *und jedes invertierbare Polynom in* $R[x_1,\ldots,x_n]$ *hat Grad* 0.
(2) *Wenn R faktoriell ist, dann auch* $R[x_1,\ldots,x_n]$.

Beweis: Induktion über n.

n =1: Satz 84 und Satz 134.
n >1: $R[x_1,x_2,\ldots,x_n] = R[x_1,\ldots,x_{n-1}][x_n]$, also folgt die Behauptung nach Induktionsannahme aus den Sätzen 84 und 134.

Beispiel 282 : Polynome vom Grad 1 in $R[x_1,x_2,\ldots,x_n]$ sind irreduzibel.
Das Polynom $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) \in \mathbb{Z}[x_1,x_2]$ ist reduzibel.
Das Polynom $x_1^2 + x_2^2 \in \mathbb{R}[x_1,x_2]$ ist irreduzibel in $\mathbb{R}[x_1,x_2]$, aber in $\mathbb{C}[x_1,x_2]$ reduzibel: $x_1^2 + x_2^2 = (x_1 - i\cdot x_2)(x_1 + i\cdot x_2)$.

Definition 283 : Es seien

$$f := \sum_{i_1,\ldots,i_n} r_{i_1\ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \in R[x_1,x_2,\ldots,x_n]$$

ein Polynom und $a := (a_1,\ldots,a_n)$ ein n-Tupel von Elementen einer kommutativen R-Algebra A. Dann ist

$$f(a) := \sum_{i_1,\ldots,i_n} r_{i_1\ldots i_n} a_1^{i_1} a_2^{i_2} \ldots a_n^{i_n}$$

ein Element von A. Das n-Tupel a ist eine *Nullstelle von* f *in* A^n, wenn

$$f(a) = 0$$

ist.
Die Funktion

$$\psi(f) : R^n \longrightarrow R \ , \ r \longmapsto f(r) \ ,$$

heißt die durch f definierte *Polynomfunktion* und wird häufig wieder mit f bezeichnet.

Satz 284 : *Es seien A eine kommutative R-Algebra,* $\mathcal{F}(R^n,R)$ *die R-Algebra aller Funktionen von* R^n *nach R und* $a \in A^n$.

(1) *Die Funktionen*

$$R[x_1,x_2,\ldots,x_n] \longrightarrow A \ , \ f \longmapsto f(a) \ ,$$

und

$$\psi : R[x_1,x_2,\ldots,x_n] \longrightarrow \mathcal{F}(R^n,R) \ , \ f \longmapsto \psi(f) = [b \mapsto f(b)] \ ,$$

sind R-Algebrenhomomorphismen.

(2) *Wenn R ein unendlicher Integritätsbereich ist, dann hat jedes Element von $\mathcal{F}(R^n,R)$ höchstens ein Urbild unter ψ. In diesem Fall müssen ein Polynom und die durch sie definierte Polynomfunktion nicht unterschieden werden.*

Beweis:

(1) Übung.

(2) Induktion über n.

n =1: Satz 91, (4).

n >1: Es sei $f \in R[x_1,x_2,\ldots,x_n]$ so, dass für alle $r \in R^n$

$$f(r) = 0$$

ist. Wir zeigen, dass dann $f = 0$ ist.
Seien $g_k \in R[x_1,x_2,\ldots,x_{n-1}]$ so, dass

$$f = \sum_{k\in\mathbb{N}} g_k x_n^k \in R[x_1,\ldots,x_{n-1}][x_n]$$

ist. Für $b \in R^{n-1}$ sei

$$f_b := \sum_{k\in\mathbb{N}} g_k(b) x_n^k \in R[x_n] \ .$$

Dann ist für alle $c \in R$ und $b \in R^{n-1}$

$$f_b(c) = f(b_1,\ldots,b_{n-1},c) = 0 \ ,$$

also folgt aus dem Fall $n = 1$, dass $f_b = 0$ ist. Das bedeutet aber, dass für alle $k \in \mathbb{N}$ und $b \in R^{n-1}$

$$g_k(b) = 0$$

ist. Nach Induktionsannahme sind dann für alle k die Polynome g_k gleich Null, also auch $f = 0$.

Wenn R ein unendlicher Integritätsbereich ist, dann ist der *Grad* einer Polynomfunktion von R^n nach R der Grad des sie definierenden Polynoms. Polynomfunktionen vom Grad 0 bzw. 1 bzw. 2 sind dann *konstante* bzw. *affine* bzw. *quadratische* Funktionen.

§2. Algebraische Mengen

In diesem Abschnitt seien R ein kommutativer Ring und n eine positive ganze Zahl.

Definition 285 : Ein *System von polynomialen Gleichungen* über R ist gegeben durch eine Teilmenge $M \subseteq R[x_1,x_2,\ldots,x_n]$. Gesucht ist die Menge

$$\mathcal{N}_{R^n}(M) := \{r \in R^n \mid \text{ für alle } \ f \in M \text{ ist } f(r) = 0\}$$

aller gemeinsamen Nullstellen der Polynome in M. Diese heißt *Nullstellenmenge von M* oder *Lösungsmenge des Systems*. Eine Teilmenge $\mathcal{N}$ von R^n ist eine *algebraische Menge*, wenn sie die Nullstellenmenge einer Teilmenge von $R[x_1, x_2, \ldots, x_n]$ ist.

Satz 286 : *Wenn zwei Teilmengen von $R[x_1, x_2, \ldots, x_n]$ dasselbe Ideal erzeugen, dann sind ihre Nullstellenmengen gleich.*

Beweis: Übung.

Satz 287 : *Beliebige Durchschnitte und endliche Vereinigungen von algebraischen Mengen sind wieder algebraisch.*
Genauer formuliert: Wenn $\mathcal{N}_1, \mathcal{N}_2, \ldots \subseteq R^n$ die Nullstellenmengen von $M_1, M_2, \ldots \subseteq R[x_1, \ldots, x_n]$ sind, dann ist

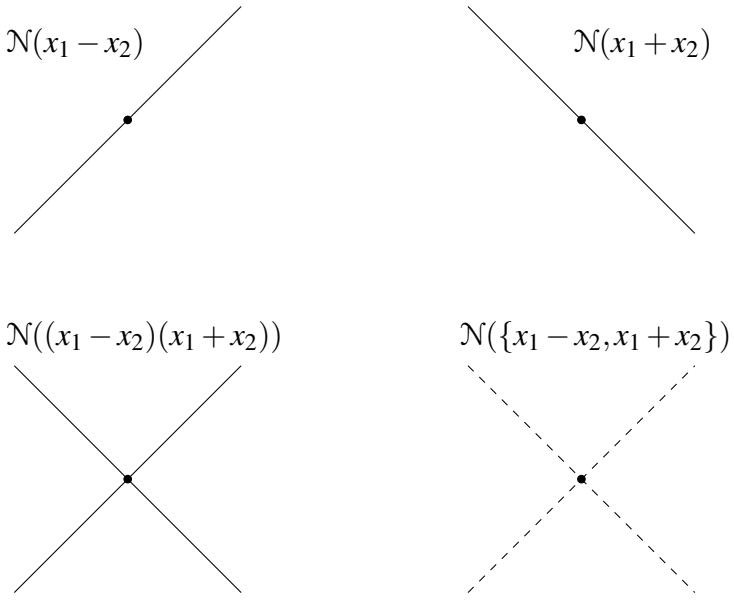
$$\bigcap_{i \in \mathbb{N}} \mathcal{N}_i = \mathcal{N}(\bigcup_{i \in \mathbb{N}} M_i)$$

und

$$\bigcup_{i=1}^{k} \mathcal{N}_i = \mathcal{N}(\{f_1 \cdot f_2 \cdot \ldots \cdot f_k \mid f_i \in M_i,\, 1 \leq i \leq k\}) \; .$$

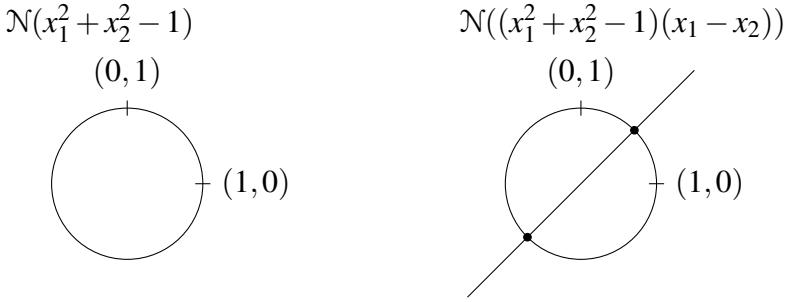
Beweis: Übung.

Beispiel 288 : $n = 2$, $R = \mathbb{R}$



Die Nullstellenmenge von $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$ in $\mathbb{R}^2$ ist die Vereinigung der zwei Geraden $\mathcal{N}(x_1 + x_2)$ und $\mathcal{N}(x_1 - x_2)$. Die Nullstellenmenge von $\{x_1 + x_2, x_1 - x_2\}$ ist der Punkt $(0,0)$, der Durchschnitt dieser zwei Geraden.

Beispiel 289 : $\mathcal{N}((x_1^2 + x_2^2 - 1)$ ist der Kreis mit Mittelpunkt $(0,0)$ und Radius 1.



Definition 290 : Das *Radikal* oder die *Wurzel* eines Ideals I von $R[x_1, \ldots, x_n]$ ist das Ideal $Rad(I) :=$

$$= \{f \in R[x_1, \ldots, x_n] \mid \text{ es gibt eine positive ganze Zahl } e \text{ mit } f^e \in I\} \ .$$

Beispiel 291 : Es seien $n = 1$, R ein Körper der Charakteristik 0 und $0 \neq f \in R[x]$. Dann ist

$$Rad(R[x] \cdot f) = R[x] \cdot \frac{f}{ggT(f, D(f))} \ .$$

Satz 292 : *(Hilbert'scher Nullstellensatz) Es seien K ein algebraisch abgeschlossener Körper und I ein Ideal in $K[x_1, \ldots, x_n]$. Die Nullstellenmenge von I in K^n ist genau dann leer, wenn $1 \in I$ ist. Das Radikal von I ist die Menge aller Polynome in $K[x_1, \ldots, x_n]$, deren Nullstellenmenge die Nullstellenmenge von I enthält.*

Beweis: wird weggelassen.

Zwei durch Teilmengen M_1 und M_2 von $K[x_1, \ldots, x_n]$ gegebene Systeme von polynomialen Gleichungen haben also genau dann dieselben Lösungsmengen, wenn die Radikale der von M_1 und M_2 erzeugten Ideale gleich sind.

§3. Quadratische Funktionen und Quadriken

In diesem Abschnitt betrachten wir Polynomfunktionen von $\mathbb{R}^n$ nach $\mathbb{R}$. Nach Satz 284 können wir dann Polynomfunktionen und Polynome identifizieren und daher auch vom Grad einer Polynomfunktion sprechen. Eine *quadratische Funktion* ist eine Polynomfunktion vom Grad 2. Nullstellenmengen von quadratischen Funktionen von $\mathbb{R}^n$ nach $\mathbb{R}$ heißen *Quadriken* in $\mathbb{R}^n$.

Satz 293 : *(Scheitelform)*
Es sei $f : \mathbb{R} \longrightarrow \mathbb{R}\,, z \longmapsto az^2+bz+c,$ *eine quadratische Funktion.*

(1) *Es gibt eindeutig bestimmte reelle Zahlen s und t so, dass für alle reellen Zahlen z*

$$f(z) = a(z-s)^2+t$$

ist. Diese Darstellung von f heißt Scheitelform *von f.*
Es ist $s = -\frac{b}{2a}$ *und* $t = c-\frac{b^2}{4a}$.

(2) *Wenn* $\frac{t}{a} > 0$ *ist, gibt es keine (reelle) Nullstelle von f. Wenn* $\frac{t}{a} = 0$ *ist, ist s die einzige Nullstelle von f. Wenn* $\frac{t}{a} < 0$ *ist, hat f zwei Nullstellen, und zwar* $s+\sqrt{-\frac{t}{a}}$ *und* $s-\sqrt{-\frac{t}{a}}$.

(3) *Der Punkt* $(s,t) \in \mathbb{R}^2$ *ist ein Element des Graphen von f und heißt* Scheitelpunkt von f. *Wenn* $a < 0$ *ist, dann ist* $f(s) = t$ *der größte Funktionswert von f. Wenn* $a > 0$ *ist, dann ist* $f(s) = t$ *der kleinste Funktionswert von f.*
(„Extremwertaufgaben“ für quadratische Funktionen können daher durch Berechnen der Scheitelform gelöst werden).

(4) *Ist P der Graph der Funktion* $g : \mathbb{R} \longrightarrow \mathbb{R}\,, z \longmapsto az^2$, *dann ist*

$$Graph(f) = \{\,(s,t)+p \,|\, p \in P\,\}.$$

„Man erhält den Graphen von f, indem man P um (s,t) verschiebt.“

Beweis:

(1) Übung.
(2) Übung.
(3) Das Quadrat einer reellen Zahl ist immer ≥ 0. Wenn $a < 0$ ist, ist daher $a(z-s)^2 \leq 0$. Somit kann $f(z) = a(z-s)^2+t$ nicht größer als $t = f(s)$ werden. Analog für $a > 0$.
(4) $Graph(f) = \{\,(z, a(z-s)^2+t) \,|\, z \in \mathbb{R}\,\} = \{\,(z+s, az^2+t) \,|\, z \in \mathbb{R}\,\} =$
$= \{\,(s,t)+(z,az^2) \,|\, z \in \mathbb{R}\,\}$.

Definition 294 : Die quadratischen Funktionen $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ mit

$$f(x,y) = \pm(x^2+y^2)+c \text{ oder } f(x,y) = x^2-y^2+c \text{ oder}$$

$$f(x,y) = \pm x^2 + c \text{ oder } f(x,y) = \pm x^2 - 2y$$

mit $c \in \mathbb{R}$ heißen *affine Normalformen* von quadratischen Funktionen von $\mathbb{R}^2$ nach $\mathbb{R}$.

Satz 295 :

(1) *Zu jeder quadratischen Funktion $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ gibt es eine bijektive affine Funktion (das ist die Hintereinanderausführung einer Translation mit einer linearen Funktion) $h : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ und eine quadratische Funktion g in Normalform so, dass $g \circ h = f$ ist.*
„In Koordinatenform" formuliert: Es gibt eine invertierbare Matrix $T \in \mathbb{R}^{2\times 2}$, eine Spalte $u \in \mathbb{R}^{2\times 1}$ und eine quadratische Funktion g in Normalform so, dass für alle $(x,y) \in \mathbb{R}^2$

$$f(x,y) = g(T_{11}x + T_{12}y + u_1, T_{21}x + T_{22}y + u_2)$$

ist.

(2) *Die Nullstellenmenge von f ist das Bild der Nullstellenmenge der quadratischen Funktion g unter der affinen Funktion h^{-1}, dh.*

$$\{(x,y) \in \mathbb{R}^2 \,|\, f(x,y) = 0\} = \{h^{-1}(x,y) \in \mathbb{R}^2 \,|\, g(x,y) = 0\}.$$

„In Koordinatenform" formuliert: Mit den Bezeichnungen von (1) ist die Nullstellenmenge von f gleich

$$\{((T^{-1})_{11}(x-u_1) + (T^{-1})_{12}(y-u_2), (T^{-1})_{21}(x-u_1) + (T^{-1})_{22}(y-u_2)) \\ | (x,y) \in \mathbb{R}^2, g(x,y) = 0\}.$$

Beweis: Es seien $a,b,c,d,e,k \in \mathbb{R}$ so, dass für alle $(x,y) \in \mathbb{R}^2$

$$f(x,y) = ax^2 + bxy + cy^2 + dx + ey + k$$

ist.

(1) Fall 1: $a > 0$.
$ax^2 + bxy + cy^2 + dx + ey + k = a(x^2 + \frac{b}{a}xy) + cy^2 + dx + ey + k =$
$= a(x + \frac{b}{2a}y)^2 + (c - \frac{b^2}{4a})y^2 + d(x + \frac{b}{2a}y) + (e - \frac{bd}{2a})y + k =$
$= a(x + \frac{b}{2a}y + \frac{d}{2a})^2 + (c - \frac{b^2}{4a})y^2 + (e - \frac{bd}{2a})y + k - \frac{d^2}{4a} =$
$= (\sqrt{a}x + \frac{\sqrt{a}b}{2a}y + \frac{\sqrt{a}d}{2a})^2 + (c - \frac{b^2}{4a})y^2 + (e - \frac{bd}{2a})y + k - \frac{d^2}{4a}$
Setze $T_{11} := \sqrt{a}, T_{12} := \frac{\sqrt{a}b}{2a}, u_1 := \frac{\sqrt{a}d}{2a}$.
Fall 1.1: $c - \frac{b^2}{4a} = 0$.
$f(x,y) = (T_{11}x + T_{12}y + u_1)^2 - 2((-\frac{1}{2}e + \frac{bd}{4a})y - \frac{1}{2}(k - \frac{d^2}{4a}))$.
Setze $T_{21} := 0, T_{22} := (-\frac{1}{2}e + \frac{bd}{4a}), u_2 := -\frac{1}{2}(k - \frac{d^2}{4a})$.
Fall 1.2: $c - \frac{b^2}{4a} \neq 0$.
Bestimme wie in (1) T_{22}, u_2 und $\ell \in \mathbb{R}$ so, dass
$(c - \frac{b^2}{4a})y^2 + (e - \frac{bd}{2a})y + (k - \frac{d^2}{4a}) = (T_{22}y + u_2)^2 + \ell$ ist.

Dann ist $f(x,y) = (T_{11}x + T_{12}y + u_1)^2 + (T_{22}y + u_2)^2 + \ell$.
Fall 2: $a < 0$. Analog Fall 1.
Fall 3: $a = 0, c \neq 0$. Analog Fall 1.
Fall 4: $a = 0, c = 0$. Dann ist $b \neq 0$ und $bxy + dx + ey + k =$
$= \frac{1}{4}b(x+y)^2 - \frac{1}{4}b(x-y)^2 + \frac{d+e}{2}(x+y) + \frac{d-e}{2}(x-y) + k$.
Weiter wie in Fall 1 mit $x+y$ statt x und $x-y$ statt y.

(2) Nachrechnen.

Beispiel 296 : Finde eine Nullstelle der quadratischen Funktion $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ mit $f(x,y) = x^2 + 2xy + 3y^2 - 2x + 2y - 6$!
Es ist

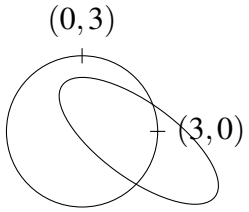
$$x^2 + 2xy + 3y^2 - 2x + 2y - 6 = (x+y)^2 + 2y^2 - 2(x+y) + 4y - 6 =$$

$$= (x+y-1)^2 + (\sqrt{2}y + \sqrt{2})^2 - 9 = (T_{11}x + T_{12}y + u_1)^2 + (T_{22}y + u_2)^2 - 9$$

mit

$$T := \begin{pmatrix} 1 & 1 \\ 0 & \sqrt{2} \end{pmatrix},\ T^{-1} := \frac{\sqrt{2}}{2}\begin{pmatrix} \sqrt{2} & -1 \\ 0 & 1 \end{pmatrix} \text{ und } u := \begin{pmatrix} -1 \\ \sqrt{2} \end{pmatrix}.$$

Die Nullstellenmenge von $g : \mathbb{R}^2 \longrightarrow \mathbb{R}$ mit $g(x,y) = x^2 + y^2 - 9$ ist $K_3 := \{\,(x,y) \,|\, \|(x,y)\| = 3\,\}$, also ein Kreis mit Radius 3 und Mittelpunkt $(0,0)$.
Die Nullstellenmenge von f ist somit $\{\,(x - \frac{\sqrt{2}}{2}y + 2, \frac{\sqrt{2}}{2}y - 1) \,|\, (x,y) \in K_3\,\}$.
Zum Beispiel ist $(3,0) \in K_3$, also $f(5,-1) = 0$.



§4. Die Anzahl der Potenzprodukte in n Variablen vom Grad d

Satz 297 : *Es seien k und n natürliche Zahlen mit $k \leq n$.*
Eine Menge mit n Elementen hat genau $\binom{n}{k}$ Teilmengen mit k Elementen.

Beweis: Sei M eine Menge mit n Elementen. Wir beweisen die Behauptung durch Induktion über n:
Eine Menge mit 1 Element hat $\binom{1}{0} = 1$ Teilmenge mit 0 Elementen und $\binom{1}{1} = 1$ Teilmenge mit 1 Element.
Wir nehmen an, dass wir die Behauptung für $n - 1 \geq 0$ schon bewiesen haben. Wenn $k = n$ ist, dann ist M die einzige Teilmenge von M mit k Elementen und $\binom{n}{n} = 1$. Wir können daher annehmen, dass $k \leq n - 1$ ist. Ist $m \in M$, dann ist die Anzahl der Teilmengen von $M \setminus \{m\}$ mit k Elementen nach Induktionsannahme gleich $\binom{n-1}{k}$. Die Anzahl der Teilmengen mit

k Elementen von M, die m enthalten, ist gleich der Anzahl der Teilmengen von $M \setminus \{m\}$ mit $k-1$ Elementen (weil jede solche durch Hinzunahme von m zu einer Teilmenge von M mit k Elementen ergänzt werden kann), nach Induktionsannahme also $\binom{n-1}{k-1}$. Daher ist $\binom{n-1}{k-1} + \binom{n-1}{k}$ die Anzahl der Teilmengen mit k Elementen von M. Nach Satz 48 ist $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.

Satz 298 : *Es seien n und d positive ganze Zahlen, R ein kommutativer Ring und $R[x_1,\ldots,x_n]$ der Polynomring in n Variablen mit Koeffizienten in R. Die Produkte $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ heißen* Potenzprodukte *in n Variablen.*

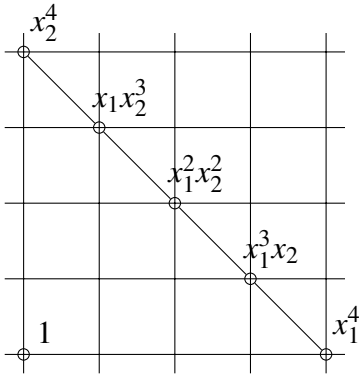
(1) *Die Anzahl der Potenzprodukte in n Variablen vom Grad d ist $\binom{d+n-1}{n-1}$.*
(2) *Der R-Modul der homogenen Polynome vom Grad d in $R[x_1,\ldots,x_n]$ ist frei und hat die Dimension $\binom{d+n-1}{n-1}$.*

Beweis:

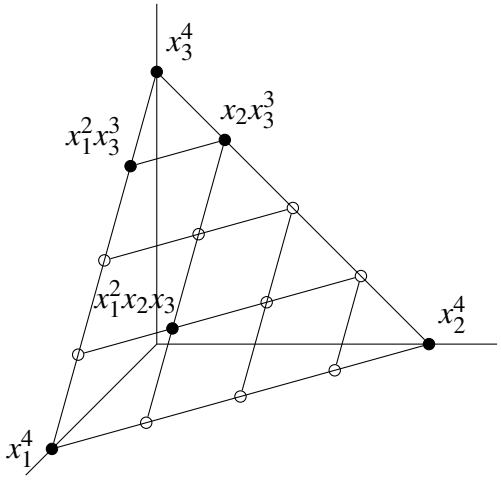
(1) Wir stellen ein Potenzprodukt
$$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = x_1x_1\cdots x_1x_2x_2\cdots x_2\cdots x_nx_n\cdots x_n$$
vom Grad d in der Form $yy\cdots yzyy\cdots yz\cdots zyy\cdots y$ dar.
In diesem Produkt kommt der Buchstabe y genau d-mal vor und der (Trenn-)buchstabe z genau $(n-1)$-mal. Insgesamt sind es also $d+n-1$ Buchstaben. Nach Satz 297 gibt es genau $\binom{d+n-1}{n-1}$ Möglichkeiten, die $n-1$ Buchstaben z auf $d+n-1$ Plätze zu verteilen.
(2) Die Potenzprodukte vom Grad d bilden eine Basis dieses R-Moduls, daher folgt die Aussage aus (1).

Beispiel 299 : Es gibt $\binom{d+1}{1} = d+1$ Potenzprodukte vom Grad d in 2 Variablen und
$$\binom{d+2}{2} = \frac{(d+2)(d+1)}{2}$$
Potenzprodukte vom Grad d in 3 Variablen.

$\underline{n=2}$: 5 Potenzprodukte vom Grad 4



$\underline{n=3}$: 15 Potenzprodukte vom Grad 4



KAPITEL 7

Schaltalgebra

§1. Boole'sche Ringe

Definition 300 : Ein Element a eines Ringes heißt *idempotent*, wenn $a^2 = a$ ist. Ein Ring ist ein *Boole'scher Ring*, wenn alle seine Elemente idempotent sind.

Beispiel 301 : Das Nullelement und das Einselement jedes Ringes ist idempotent. $\mathbb{Z}_2$ ist ein Boole'scher Ring. Ist M eine Menge, dann ist der Ring aller Funktionen von M nach $\mathbb{Z}_2$ ein Boole'scher Ring.

Satz 302 : *Es sei R ein Boole'scher Ring. Dann:*

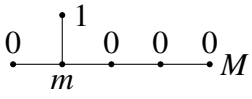
(1) *R hat Charakteristik 2 und ist kommutativ.*
(2) *Die Teilmenge $\{0,1\}$ ist ein zu $\mathbb{Z}_2$ isomorpher Unterring von R und R ist eine $\mathbb{Z}_2$-Algebra.*
(3) *Wenn R endlich ist, dann ist die Anzahl der Elemente von R eine Potenz von 2.*

Beweis:

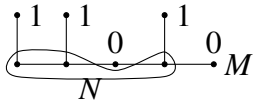
(1) Für $r \in R$ ist $r+r = (r+r)^2 = r^2+r^2+r^2+r^2 = r+r+r+r$, also ist $r+r = 0$ und $r = -r$.
Für $r,s \in R$ ist $r+s = (r+s)^2 = r^2+s^2+rs+sr = r+s+rs+sr$, also ist $rs+sr = 0$ und $rs = -sr = sr$.
(2) Aus (1) folgt $1+1 = 0$. Der Ring $\{0,1\}$ ist zu $\mathbb{Z}_2$ isomorph.
(3) Nach (2) ist R eine $\{0,1\}$-Algebra.

Satz 303 : *Es sei M eine Menge und $\mathcal{F}(M,\mathbb{Z}_2)$ die $\mathbb{Z}_2$-Algebra aller Funktionen von M nach $\mathbb{Z}_2$. Für $m \in M$ sei δ_m die Funktion, die m auf 1 und alle anderen Elemente von M auf 0 abbildet. Für eine Teilmenge N von M sei 1_N die Funktion, die alle Elemente von N auf 1 und alle anderen Elemente auf 0 abbildet („charakteristische Funktion von N").*

$\delta_m = 1_{\{m\}}$:



1_N :



Dann:

(1) *Die Familie* $(\delta_m)_{m\in M}$ *ist eine* $\mathbb{Z}_2$*-Basis von* $\mathcal{F}(M,\mathbb{Z}_2)$.
(2) *Für* $f\in\mathcal{F}(M,\mathbb{Z}_2)$ *ist* $f=\sum_{m\in M} f(m)\delta_m$,
insbesondere ist $1_N=\sum_{m\in N}\delta_m$.
(3) *Ist M eine endliche Menge mit n Elementen, dann hat* $\mathcal{F}(M,\mathbb{Z}_2)$ 2^n *Elemente.*
(4) *Für* $X,Y\subseteq M$ *ist* $1_X\cdot 1_Y=1_{X\cap Y}$, $1_X+1_Y+1_X\cdot 1_Y=1_{X\cup Y}$ *und* $1_M+1_X=1_{M\setminus X}$.

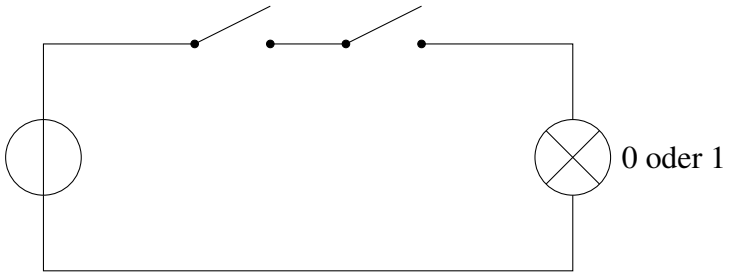
Beweis: Übung.

Beispiel 304 : („Mengenalgebra“) X, Y und Z seien Teilmengen von M.
Zeige, dass $X\cap(Y\cup Z)=(X\cap Y)\cup(X\cap Z)$ ist!
Diese Teilmengen von M sind genau dann gleich, wenn ihre charakteristischen Funktionen gleich sind.
Es ist $1_{X\cap(Y\cup Z)}=1_X\cdot 1_{Y\cup Z}=1_X\cdot(1_Y+1_Z+1_Y\cdot 1_Z)=$
$=1_X\cdot 1_Y+1_X\cdot 1_Z+1_X\cdot 1_Y\cdot 1_Z$ und
$1_{(X\cap Y)\cup(X\cap Z)}=1_{(X\cap Y)}+1_{(X\cap Z)}+1_{(X\cap Y)}\cdot 1_{(X\cap Z)}=$

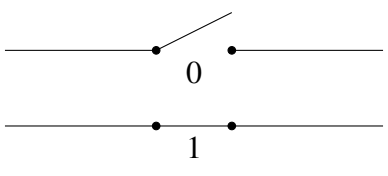
$=1_X\cdot 1_Y+1_X\cdot 1_Z+1_X\cdot 1_Y\cdot 1_X\cdot 1_Z=1_X\cdot 1_Y+1_X\cdot 1_Z+1_X\cdot 1_Y\cdot 1_Z$.

§2. Schaltalgebra

Eine *Schaltung* besteht aus mehreren Schaltern, Leitungen, einer Stromquelle und einem Verbraucher (zum Beispiel einer Lampe), an dem man sieht, ob Strom fließt oder nicht. Diese zwei möglichen Zustände des Verbrauchers beschreiben wir durch $0\in\mathbb{Z}_2$ (Strom fließt nicht) und $1\in\mathbb{Z}_2$ (Strom fließt).

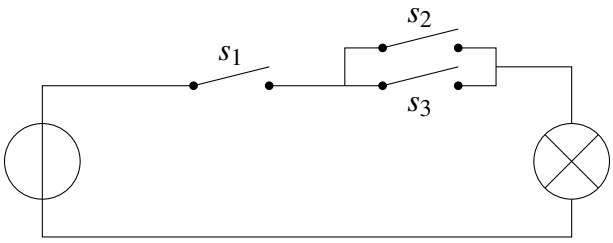


Die Schalter haben auch zwei Zustände, diese bezeichnen wir auch mit $0\in\mathbb{Z}_2$ und $1\in\mathbb{Z}_2$.



Der *Zustand von n Schaltern* wird durch ein n-Tupel in $\mathbb{Z}_2^n$ beschrieben. Statt Schaltungen können auch elektronische Bauteile mit n Eingängen und einem Ausgang betrachtet werden.
Die *Schaltfunktion* einer Schaltung mit n Schaltern ordnet jedem Zustand der n Schalter der Schaltung den Zustand des Verbrauchers zu, ist also eine Funktion von $\mathbb{Z}_2^n$ nach $\mathbb{Z}_2$.

Beispiel 305 : Die Schaltfunktion der Schaltung



ist $f : \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2$, wobei $f(z_1,z_2,z_3)$ der Zustand des Verbrauchers ist, wenn (z_1,z_2,z_3) die Zustände der drei Schalter sind. Zum Beispiel ist $f(1,1,0) = 1$ (es fließt Strom durch den Verbraucher, wenn s_1 und s_2 geschlossen sind und s_3 offen ist).

Satz 306 : *Es seien n eine positive ganze Zahl,* $V := \mathbb{Z}_2^n$ *und* $p_i : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2\,, (x_1,\ldots,x_n) \longmapsto x_i\,,$ *die i-te Projektion,* $1 \leq i \leq n$.

(1) *Für* $x \in \mathbb{Z}_2^n$ *ist* $\delta_x = \left(\prod_{i,x_i=1} p_i\right) \cdot \prod_{i,x_i=0}(1_V + p_i)$.
(2) *Für* $f \in \mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ *ist* $f = \sum_{x\in V} f(x) \left(\prod_{i,x_i=1} p_i\right) \cdot \prod_{i,x_i=0}(1_V + p_i)$.

Beweis:

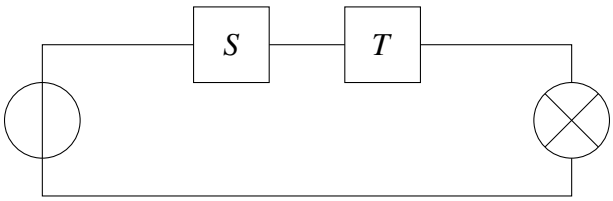
(1) Übung.
(2) Folgt aus (1) und Satz 303, (2).

Beispiel 307 : Für $n = 4$ und $x = (1,0,0,1)$ ist $\delta_x = p_1(1_V + p_2)(1_V + p_3)p_4$.

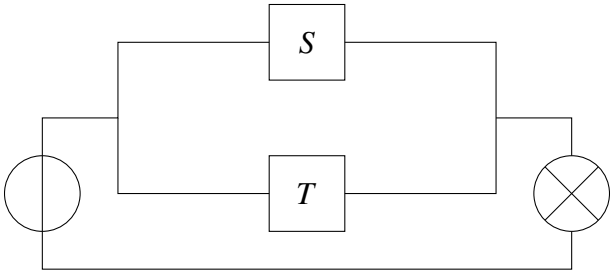
Definition 308 : Für $f,g \in \mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ sei

$$\neg f := 1_V + f,\ \ f \wedge g := f \cdot g \ \text{ und } \ f \vee g := f + g + f \cdot g.$$

Sind S und T Schaltungen mit Schaltfunktion f und g, dann ist $f \wedge g$ die Schaltfunktion der „Serienschaltung“ von S und T



und $f \vee g$ die Schaltfunktion der „Parallelschaltung“ von S und T.



Satz 309 :

(1) *Für* $f,g,h \in \mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ *ist*
$(f \vee g) \vee h = f \vee (g \vee h)$ *(„*$\vee$ *ist assoziativ“).*

(2) *Für* $f,g \in \mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ *ist*
$\neg(f \wedge g) = (\neg f) \vee (\neg g)$ *und* $\neg(f \vee g) = (\neg f) \wedge (\neg g)$.

Beweis:

(1) Nachprüfen.

(2) $\neg(f \wedge g) = 1_V + f \cdot g$

$$\begin{aligned}(\neg f) \vee (\neg g) &= (1_V + f) + (1_V + g) + (1_V + f)(1_V + g) = \\ &= f + g + f + g + 1_V + f \cdot g = \\ &= 1_V + f \cdot g\end{aligned}$$

Analog: $\neg(f \vee g) = (\neg f) \wedge (\neg g)$.

Ist eine Schaltung gegeben, dann kann die entsprechende Schaltfunktion leicht beschrieben werden. Zum Beispiel: Sind n Schalter in Serie geschalten, dann ist

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$$

die zugehörige Schaltfunktion. Sind n Schalter parallel geschalten, dann ist

$$p_1 \vee p_2 \vee \ldots \vee p_n : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$$

die zugehörige Schaltfunktion.

Oft ist die Schaltfunktion vorgegeben und eine entsprechende Schaltung gesucht. Zum Beispiel: Eine Lampe im Erdgeschoß eines Stiegenhauses soll von drei Schaltern (im Keller, im Erdgeschoß und im ersten Stock) ein- und ausgeschalten werden. Bei jeder Änderung des Zustandes eines Schalters

soll sich der Zustand der Lampe ändern (man möchte ja z. B. die Lampe im Stiegenhaus im Keller einschalten und im ersten Stock wieder ausschalten können). Die Funktion $f = p_1 + p_2 + p_3$ könnte dafür gewählt werden. Um die entsprechende Schaltung zu finden, benutzen wir den folgenden Satz.

Definition 310 : Für eine endliche Familie $(f_i)_{i\in I}$ in $\mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ sei

$$\bigwedge_{i\in I} f_i := f_{\sigma(1)} \wedge f_{\sigma(2)} \wedge \ldots \wedge f_{\sigma(k)} \left(= \prod_{i\in I} f_i \right)$$

und

$$\bigvee_{i\in I} f_i := f_{\sigma(1)} \vee f_{\sigma(2)} \vee \ldots \vee f_{\sigma(k)}$$

(für eine bijektive Funktion $\sigma : \{1, 2, \ldots, k\} \longrightarrow I$).

Satz 311 : *Es seien n eine positive ganze Zahl,* $V := \mathbb{Z}_2^n$ *und* $p_i : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2, (x_1, \ldots, x_n) \longmapsto x_i$, *die i-te Projektion,* $1 \leq i \leq n$.

(1) *Für* $f \in \mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ *ist*

$$f = \bigvee_{x\in V, f(x)=1} \left(\left(\bigwedge_{i, x_i=1} p_i \right) \wedge \left(\bigwedge_{i, x_i=0} (\neg p_i) \right) \right)$$

(„disjunktive Normalform von f“).

(2) *Für* $f \in \mathcal{F}(\mathbb{Z}_2^n, \mathbb{Z}_2)$

$$f = \bigwedge_{x\in V, f(x)=0} \left(\left(\bigvee_{i, x_i=1} (\neg p_i) \right) \vee \left(\bigvee_{i, x_i=0} p_i \right) \right)$$

(„konjunktive Normalform von f“).

Beweis:

(1) Folgt direkt aus Satz 306 (2).

(2) Nach (1) und Satz 309 ist

$$\neg f = \bigvee_{x\in V, (\neg f)(x)=1} \left(\left(\bigwedge_{i, x_i=1} p_i \right) \wedge \left(\bigwedge_{i, x_i=0} (\neg p_i) \right) \right) \text{ und}$$

$$f = \neg(\neg f) = \neg\Big(\bigvee_{x\in V, f(x)=0} \left(\left(\bigwedge_{i, x_i=1} p_i \right) \wedge \left(\bigwedge_{i, x_i=0} (\neg p_i) \right) \right) \Big) =$$

$$= \bigwedge_{x\in V, f(x)=0} \left((\neg(\bigwedge_{i, x_i=1} p_i)) \vee (\neg(\bigwedge_{i, x_i=0} (\neg p_i))) \right) =$$

$$= \bigwedge_{x\in V, f(x)=0} \left(\left(\bigvee_{i,x_i=1} (\neg p_i) \right) \vee \left(\bigvee_{i,x_i=0} p_i \right) \right) .$$

Beispiel 312 : Die Funktion $f : \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2$ ist durch die Tabelle

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

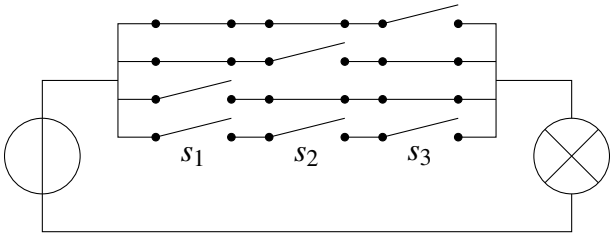
definiert. Es ist $f = p_1 + p_2 + p_3$. Die disjunktive Normalform ist

$$f = ((\neg p_1) \wedge (\neg p_2) \wedge p_3)) \vee ((\neg p_1) \wedge p_2 \wedge (\neg p_3)) \vee$$
$$\vee (p_1 \wedge (\neg p_2) \wedge (\neg p_3)) \vee (p_1 \wedge p_2 \wedge p_3) ,$$

die konjunktive Normalform ist

$$f = (p_1 \vee p_2 \vee p_3) \wedge (p_1 \vee (\neg p_2) \vee (\neg p_3)) \wedge ((\neg p_1) \vee p_2 \vee (\neg p_3)) \wedge$$
$$\wedge ((\neg p_1) \vee (\neg p_2) \vee p_3).$$

Verwendet man die disjunktive Normalform der Schaltfunktion, so kann die Schaltung als Parallelschaltung von 4 Serienschaltungen mit je 3 Schaltern gebaut werden. Von diesen insgesamt 12 Schaltern sind jeweils 4 (die 4 Schalter links, die 4 Schalter in der Mitte und die 4 Schalter rechts) zu einem Schalter zusammengefasst (s_1, s_2 und s_3).



Verwendet man die konjunktive Normalform der Schaltfunktion, so kann die Schaltung als Serienschaltung von 4 Parallelschaltungen mit je 3 Schaltern gebaut werden. Von diesen insgesamt 12 Schaltern sind jeweils 4 (die 4 Schalter oben, die 4 Schalter in der Mitte und die 4 Schalter unten) zu einem Schalter zusammengefasst (s_1, s_2 und s_3).