

Algebra für Informatiker

Johannes Buchmann

15. März 2005

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Elementare Zahlentheorie | 3 |
| 1.1 | Natürliche Zahlen | 3 |
| 1.2 | Ganze Zahlen | 5 |
| 1.3 | Teilbarkeit | 6 |
| 1.4 | Division mit Rest und Komplexität arithmetischer Operationen | 8 |
| 1.5 | Größter gemeinsamer Teiler | 9 |
| 1.6 | Eindeutige Primfaktorzerlegung | 12 |
| 1.7 | Kongruenzen | 13 |
| 2 | Gruppen | 15 |
| 2.1 | Algebraische Struktur | 15 |
| 2.2 | Halbgruppen | 17 |
| 2.3 | Direkte Produkte | 19 |
| 2.4 | Faktorhalbgruppen | 19 |
| 2.5 | Neutrale Elemente | 20 |
| 2.6 | Invertierbare Elemente | 21 |
| 2.7 | Gruppen | 22 |
| 2.8 | Beispiele von Gruppen | 23 |
| 2.9 | Gruppentafeln | 23 |
| 2.10 | Zyklische Gruppen und Elementordnung | 24 |
| 2.11 | Berechnung der Elementordnung | 26 |

| | |
|--|-----------|
| Version 15. März 2005 | 2 |
| 2.12 Berechnung diskreter Logarithmen | 28 |
| 2.13 Untergruppen | 29 |
| 2.14 Gruppenhomomorphismen | 30 |
| 2.15 Der Satz von Lagrange | 31 |
| 2.16 Anwendung des Satzes von Lagrange | 32 |
| 2.17 Normalteiler und Faktorgruppen | 33 |
| 2.18 Erzeugendensysteme | 34 |
| 2.19 Operation von Gruppen auf Mengen | 34 |
| 2.20 Die symmetrische Gruppe S_n | 35 |
| 2.21 Freie Gruppen | 36 |
| 3 Ringe | 38 |
| 3.1 Ringbegriff | 38 |
| 3.2 Polynomringe | 39 |
| 3.3 Unterringe, Ideale, Restklassenringe | 40 |
| 3.4 Homomorphiesatz | 42 |
| 3.5 Quotientenkörper | 42 |
| 3.6 Nullstellen und Differentiation von Polynomen | 43 |
| 3.7 Euklidische Ringe | 43 |
| 3.8 Teilbarkeit | 44 |
| 3.9 ZPE-Ringe | 44 |
| 3.10 Irreduzibilitätstests | 46 |
| 3.11 Primideale, maximale Ideale | 46 |
| 3.12 Algorithmen für Polynome über endlichen Primkörpern | 47 |
| 3.13 Lemma von Gauß | 47 |

Kapitel 1

Elementare Zahlentheorie

In diesem Kapitel werden wichtige Eigenschaften der ganzen Zahlen besprochen. Die Begriffe und Ergebnisse dieses Kapitels nehmen allgemeinere Begriffe und Ergebnisse, die im Lauf der Vorlesung eingeführt bzw. bewiesen werden, im Spezialfall vorweg. Sie dienen darum später als Beispielmateriale.

1.1 Natürliche Zahlen

Ich setze voraus, daß die Menge der natürlichen Zahlen bekannt ist. Diese Menge wird durch die Axiome von Peano charakterisiert, nämlich

1. 1 ist eine natürliche Zahl.
2. Jede natürliche Zahl a hat einen Nachfolger a^+ in \mathbb{N} .
3. Es gibt keine natürliche Zahl mit dem Nachfolger 1.
4. Stimmen die Nachfolger zweier natürlicher Zahlen a und b überein, so gilt $a = b$.
5. Die einzige Menge von natürlichen Zahlen, die die Zahl 1 enthält und die mit jedem Element a auch dessen Nachfolger enthält, ist \mathbb{N} selbst.

Das letzte Axiom heißt *Prinzip der vollständigen Induktion*. Dieses Prinzip wird benutzt, um Eigenschaften der natürlichen Zahlen zu beweisen und neue Begriffe zu definieren.

Man kann beispielsweise zeigen, daß sich auf genau eine Art jedem Paar x, y natürlicher Zahlen eine natürliche Zahl, $x+y$ genannt, so zuordnen läßt, daß

$$x + 1 = x^+, \quad x \in \mathbb{N},$$

und

$$x + y^+ = (x + y)^+, \quad x, y \in \mathbb{N}$$

gilt. Die Zahl $x + y$ heißt *Summe* von x und y . Statt a^+ schreibe ich ab sofort $a + 1$. Für alle natürlichen Zahlen a, b, c gilt das *Assoziativgesetz*

nat 2

$$(a + b) + c = a + (b + c) \quad (1.1)$$

und das *Kommutativgesetz*

nat 3

$$a + b = b + a. \quad (1.2)$$

Außerdem gilt

nat 4

$$\text{Aus } a + b = a + c \text{ folgt } b = c. \quad (1.3)$$

Statt $a_1 + a_2 + \dots + a_k$ schreibt man kurz $\sum_{i=1}^k a_i$.

Weiter kann man jedem Paar x, y natürlicher Zahlen auf genau eine Weise ihr *Produkt* $x \cdot y$ oder xy so zuordnen, daß

$$x \cdot 1 = x, \quad x \in \mathbb{N}$$

und

$$x(y + 1) = xy + x$$

gilt. Für alle natürlichen Zahlen a, b, c gilt dann das *Assoziativgesetz*

nat 5

$$(ab)c = a(bc), \quad (1.4)$$

das *Kommutativgesetz*

nat 6

$$ab = ba \quad (1.5)$$

und das *Distributivgesetz*

nat 7

$$a(b + c) = ab + ac. \quad (1.6)$$

Ferner gilt

nat 8

$$\text{Aus } ab = ac \text{ folgt } b = c \quad (1.7)$$

Dies nennt man *Kürzungsregel*. Statt $a_1 a_2 \cdots a_k$ schreibt man kurz $\prod_{i=1}^k a_i$. Ist hierbei $a_1 = a_2 = \dots = a_k$ so schreibt man $a_1 a_2 \cdots a_k = a^k$.

Gilt $a = b + u$ für natürliche Zahlen a, b, u , so schreibt man $a > b$ oder $b < a$ und sagt, daß a größer als b ist oder daß b kleiner als a ist. Wiederum beweist man durch vollständige Induktion, daß genau eine der Relationen

nat 9

$$a < b, \quad a = b, \quad a > b \quad (1.8)$$

erfüllt ist. Weiter gilt für alle natürlichen Zahlen a, b, c

nat 10

$$\text{Aus } a < b \text{ und } b < c \text{ folgt } a < c. \quad (1.9)$$

nat 11

$$\text{Aus } a < b \text{ folgt } a + c < b + c. \quad (1.10)$$

nat 12

$$\text{Aus } a < b \text{ folgt } ac < bc. \quad (1.11)$$

Ist $a > b$ so wird die eindeutig bestimmte Lösung der Gleichung $a = b + u$ mit $a - b$ bezeichnet. Für " $a < b$ oder $a = b$ " schreibt man kurz $a \leq b$. Für " $a > b$ oder $a = b$ " schreibt man kurz $a \geq b$.

Weiter gilt der sogenannte Wohlordnungssatz.

nat 1

1.1.1. Satz *Jede nicht leere Menge von natürlichen Zahlen enthält eine kleinste Zahl, d.h. eine solche, die kleiner ist als alle anderen Zahlen der Menge.*

Um mit natürlichen Zahlen rechnen zu können, braucht man eine *Darstellung*. Normalerweise benutzt man die Dezimaldarstellung. Computer verwenden die Binärdarstellung. Etwas allgemeiner führe ich hier die g -adische Darstellung ein wobei g eine feste natürliche Zahl ungleich 1 ist. Man braucht zuerst g viele verschiedene Zeichen. Wenn $g = 2$ ist, also bei der Binärdarstellung, benutzt man die Zeichen 0, 1. Wenn $g = 10$ ist, also bei der Dezimaldarstellung, benutzt man die Zeichen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Wenn $g = 16$ ist, also bei der Hexadezimaldarstellung, benutzt man die Zeichen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Sei Σ die Menge der g verschiedenen Zeichen. Mit Σ^* bezeichne ich die Menge aller endlichen Folgen von Zeichen aus Σ einschließlich der leeren Folge, für die ich ε schreibe. Die Elemente aus Σ^* heißen auch Strings über Σ . Den natürlichen Zahlen $a < g$ seien verschiedene Zeichen der Menge Σ zugeordnet. Die natürliche Zahl 1 wird durch das Zeichen 1 dargestellt. Zusätzlich gibt es noch das Zeichen 0 in Σ dem keine natürliche Zahl entspricht. Die Menge Σ enthält also immer die Zeichen 0, 1. Die von 0 verschiedenen Elemente von Σ werden mit den durch sie dargestellten Zahlen identifiziert. Jedem String

$$s = s_k s_{k-1} \dots s_1 \in \Sigma^*, \quad k \geq 1, s_k \neq 0$$

wird die natürliche Zahl

$$\sum_{i=1}^k s_i g^{k-i}$$

zugeordnet. Dann wird jede natürliche Zahl durch genau einen String über Σ dargestellt.

1.2 Ganze Zahlen

Die Menge der natürlichen Zahlen wird folgendermaßen zur Menge der ganzen Zahlen ergänzt. Man betrachtet die Menge aller Paare (a, b) von natürlichen Zahlen. Man stellt sich vor, daß (a, b) die ganze Zahl $a - b$ repräsentiert. Ganze Zahlen haben dann verschiedene Darstellungen. Um dem Rechnung zu tragen, werden Paare identifiziert, die dieselbe ganze Zahl darstellen. Zwei Paare (a, b) und (x, y) werden äquivalent genannt, wenn $a + y = x + b$ gilt. Dies ist eine Äquivalenzrelation. Die Menge der ganzen Zahlen ist die Menge der Äquivalenzklassen. Sie wird mit \mathbf{Z} bezeichnet.

Man definiert Addition, Multiplikation und Vergleich ganzer Zahlen folgendermaßen. Für natürliche Zahlen a, b, c, d setzt man

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

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc)$$

und man schreibt

$$(a, b) < (c, d) \text{ oder } (c, d) > (a, b), \text{ falls } a + d < b + c.$$

Man verifiziert leicht, daß diese Definitionen von der Wahl der Vertreter unabhängig ist.

Folgendermaßen werden einfachere Bezeichnungen für ganze Zahlen eingeführt. Alle Paare (a, a) gehören zu derselben Äquivalenzklasse. Für diese schreibt man 0. Ist $a > b$ so bezeichnet man die Äquivalenzklasse, die (a, b) enthält mit $a - b$. Ist $a < b$ so schreibt man $-(b - a)$ für die Äquivalenzklasse, die (a, b) enthält. Es ist leicht zu sehen, daß diese Bezeichnungen wohldefiniert sind.

Man verifiziert leicht daß die Rechengesetze (1.1) - (1.11) gelten. Außerdem hat für ganze Zahlen a, b die Gleichung $a = b + x$ stets eine eindeutig bestimmte Lösung x , die ebenfalls eine ganze Zahl ist. Für diese schreibt man auch $a - b$. Schließlich gilt $ab = 0$ genau dann wenn a oder b gleich 0 ist.

Auch die Darstellung ganzer Zahlen wird von der Darstellung natürlicher Zahlen abgeleitet. Die Zahl 0 wird durch das Symbol 0 dargestellt. Es wurde ja vorausgesetzt, daß dieses Symbol zu dem Alphabet Σ gehört. Jede von 0 verschiedene ganze Zahl ist entweder eine natürliche Zahl oder $-a$ für eine natürliche Zahl a . Dies liefert unmittelbar die Darstellung der ganzen Zahlen. Bei der Binärdarstellung kann das Vorzeichen in einem weiteren Bit gespeichert werden. Die Anzahl der Bits, die nötig ist, um eine ganze Zahl z in Binärdarstellung zu speichern ist

$$\text{size}(z) = \begin{cases} 2 & \text{falls } z = 0 \\ \lfloor \log |z| \rfloor + 2 & \text{falls } z \neq 0. \end{cases}$$

Unter einer n -Bit Zahl verstehe ich eine ganze Zahl z mit $\text{size}(z) = n + 1$.

1.3 Teilbarkeit

Nun werden elementare arithmetische Begriffe und Eigenschaften der ganzen Zahlen eingeführt. Eine ganze Zahl a heißt *Teiler* einer ganzen Zahl b , wenn es eine ganze Zahl g gibt, für die $b = ga$ gilt. Dafür schreibt man kurz $a \mid b$ (lies: a teilt b). Das Gegenteil wird mit $a \nmid b$ (lies: a teilt nicht b) bezeichnet. Das Problem, zu entscheiden, ob a ein Teiler von b ist, wird im Zusammenhang mit der Division mit Rest angesprochen.

teil 1

1.3.1. Übung Zeige daß aus $a \mid b$ und $b \neq 0$ folgt daß $|a| \leq |b|$ gilt.

Aus Übung 1.3.1 kann man folgende elementare Tatsachen ableiten.

teil 2

$$\text{Jede ganze Zahl teilt } 0. \tag{1.12}$$

teil 3

$$\text{Der einzige Teiler von } 0 \text{ ist } 0. \tag{1.13}$$

teil 4

$$\text{Die einzigen Teiler von } 1 \text{ sind } \pm 1. \tag{1.14}$$

teil 5

$$\text{Genau dann gilt } a \mid b \text{ und } b \mid a \text{ wenn } a = \pm b \text{ ist} \tag{1.15}$$

teil 6

Jede ganze Zahl a wird von ± 1 und von $\pm a$ geteilt. (1.16)

teil 7

Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$. (1.17)

teil 8

Aus $a \mid b_i$, $1 \leq i \leq k$ folgt $a \mid \sum_{i=1}^k b_i c_i$ für alle c_i , $1 \leq i \leq k$. (1.18)

Die ganze Zahl a wird *echter Teiler* von b genannt, wenn a ein Teiler von b ist und $a \neq \pm 1, \pm b$. Man sieht leicht ein, daß a genau dann ein echter Teiler von b ist, wenn a ein Teiler von b ist und $1 < |a| < b$ gilt. Eine *Primzahl* ist eine von 1 verschiedene natürliche Zahl, die keine echten Teiler hat. Die kleinste Primzahl ist 2. Alle anderen Primzahlen sind ungerade. Eine Primzahl, die eine ganze Zahl b teilt, heißt *Primteiler* von b .

teil 9

1.3.2. Satz *Jede natürliche Zahl $a > 1$ besitzt wenigstens einen Primteiler.*

Beweis: Unter allen Teilern $r > 1$ wähle man den kleinsten aus. Dies geht nach dem Wohlordnungssatz. Der ausgewählte Teiler heiße t . Wenn t keine Primzahl ist, so besitzt t einen Teiler s mit $1 < s < t$. Nach (1.17) ist s auch ein Teiler von a und dies widerspricht der Wahl von t . \square

teil 10

1.3.3. Satz *Es gibt unendlich viele Primzahlen.*

Beweis: Angenommen, die Menge \mathbb{P} aller Primzahlen ist endlich. Setze $a = \prod_{p \in \mathbb{P}} p + 1$. Nach Satz 1.3.2 besitzt a einen Primteiler q . Wenn dieser mit einer Primzahl in \mathbb{P} übereinstimmt, so gilt $q \mid 1 = a - \prod_{p \in \mathbb{P}} p$ nach (1.18). Dies ist aber wegen $q > 1$ unmöglich. \square

Ein zentrales Thema der Zahlentheorie sind die Primzahlen. Es gibt sehr viele interessante algorithmische Probleme im Zusammenhang mit Primzahlen. Mit Hilfe des Siebs des Erathostenes (siehe [9], p.3) kann man z.B. alle Primzahlen unterhalb einer gegebenen Schranke aufzählen. Dies geht in polynomieller Zeit. Viel schwieriger ist es, zu entscheiden, ob eine gegebene natürliche Zahl eine Primzahl ist (siehe [9], Chapter 4, [3] Chapter 9). Es ist bis jetzt kein deterministischer Polynomzeitalgorithmus bekannt, der diese Entscheidung fällt. Es gibt aber effiziente probabilistische Verfahren.

teil 11

1.3.4. Übung Ein *Primzahlzwilling* ist ein Paar (p, q) ungerader Primzahlen mit $q = p + 2$. Es ist nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt. Man schreibe ein Programm, das alle Primzahlzwillinge unterhalb einer gegebenen Schranke ausgibt.

1.4 Division mit Rest und Komplexität arithmetischer Operationen

teil 13

1.4.1. Satz Zu jedem Paar a, b ganzer Zahlen mit $b \neq 0$ gibt es genau ein Paar q, r ganzer Zahlen, das die Bedingungen

$$a = qb + r, \quad 0 \leq r < |b|$$

erfüllt.

Beweis: Es genügt, den Fall $b > 0$ zu betrachten. Es ist dann zu zeigen, daß es genau eine ganze Zahl q gibt, für die $qb \leq a < q(b + 1)$ gilt. Dies ist gleichbedeutend mit der Bedingung $q \leq a/b < q + 1$, welcher genau eine ganze Zahl q genügt. \square

Die *arithmetischen Operationen* für ganze Zahlen sind Addition, Subtraktion, Multiplikation und Division mit Rest. Schon aus der Schule sind Verfahren bekannt, wie man ganze Zahlen in Dezimaldarstellung addieren, subtrahieren, dividieren, multiplizieren und mit Rest dividieren kann. Entsprechende Verfahren lassen sich für g -adisch dargestellte Zahlen mit beliebigem g angeben. Eine interessante Frage ist, wie schnell man die arithmetischen Operationen ausführen kann. Um diese Frage sinnvoll stellen zu können, muß man zuerst ein Berechnungsmodell festlegen, z.B. eine Turing-Maschine oder eine Random Access Maschine (RAM). Hier gehen ich davon aus, daß die ganzen Zahlen binär dargestellt sind. Unter der *Rechenzeit*, die ein Verfahren benötigt verstehe ich die Anzahl der arithmetischen Operationen und Vergleiche von Bits, die innerhalb der Rechnung ausgeführt werden. Eine genauer beschriebenes Berechnungsmodell findet sich in [1].

Es ist klar daß man zwei n -Bit Zahlen in Zeit $O(n)$ addieren und subtrahieren kann. Bezeichnet man mit $M(n)$ die minimale Zeit die für die Multiplikation zweier n -Bit Zahlen gebraucht wird und mit $D(n)$ die Zeit die man braucht, um eine Zahl von höchstens $2n$ Bits durch eine n -Bit Zahl zu dividieren, so gilt der folgende, in [1] bewiesene Satz. div 1

1.4.2. Satz Es gibt positive reelle Zahlen c und c' mit $cM(n) \leq D(n) \leq c'M(n)$.

Dies bedeutet, daß Multiplikation und Division mit Rest im wesentlichen gleich schwere Probleme sind. In [1] wird außerdem folgendes bewiesen. div 2

1.4.3. Satz $M(n) = O(n \log n \log \log n)$.

Der Beweis erfolgt, indem diese Laufzeitschranke für den Multiplikationsalgorithmus von Schönhage und Strassen gezeigt wird. Nennt man eine Funktion $f : \mathbb{N} \rightarrow \mathbb{R}_{>0}$ *quasilinear* wenn $f(n) = O(n^{1+\varepsilon})$ für jedes $\varepsilon > 0$ ist, so bedeutet Satz 1.4.3, daß man zwei ganze Zahlen in quasilinearer Laufzeit multiplizieren kann.

Diese Analysen geben zwar ein Gefühl von der Schwierigkeit der Multiplikation und Division von ganzen Zahlen. Sie beantworten aber nicht die Frage, welchen Algorithmus man

in der Praxis verwenden soll. Dies kann man nur durch Bestimmung der O-Konstante und durch Experimente herausfinden. Aber auch dann hängt die Effizienz des verwendeten Verfahrens noch wesentlich von der Implementierung ab. So arbeitet Schönhage schon lange daran zu zeigen, daß sein Multiplikationsverfahren schon für relativ kleine Zahlen effizient ist. Siehe hierzu [10]. Für praktische Informationen und Implementierungshinweise siehe [6].

1.5 Größter gemeinsamer Teiler

ggT 1

1.5.1. Definition Ein gemeinsamer Teiler einer Menge M von ganzen Zahlen ist eine ganze Zahl, die alle Elemente von M teilt. Ein gemeinsamer Teiler d von M heißt größter gemeinsamer Teiler von M , wenn er von allen anderen gemeinsamen Teilern von M geteilt wird und $d \geq 0$ gilt.

ggT 2

1.5.2. Satz Jede Menge M von ganzen Zahlen besitzt genau einen größten gemeinsamen Teiler. Enthält M ein von Null verschiedenes Element, so ist dies die größte natürliche Zahl, die alle Elemente von M teilt.

Beweis: Zuerst wird die Eindeutigkeit gezeigt. Seien d und d' zwei größte gemeinsame Teiler von M , dann ist nach Definition d ein Teiler von d' und d' ein Teiler von d . Also folgt aus (1.15), daß $d = d'$, weil beide nicht negativ sind.

Besteht M nur aus einem einzigen Element, so ist dieses Element der größte gemeinsame Teiler von M . Jetzt wird die Existenz für den Fall nachgewiesen, daß M zwei Elemente a_1 und a_2 enthält. Ohne Beschränkung der Allgemeinheit kann angenommen werden, daß $a_2 > 0$ ist. Führe in folgender Weise Divisionen mit Rest durch:

$$a_1 = q_1 a_2 + a_3, 0 \leq a_3 < a_2$$

$$a_2 = q_2 a_3 + a_4, 0 \leq a_4 < a_3$$

$$a_3 = q_3 a_4 + a_5, 0 \leq a_5 < a_4$$

usw. Die Folge der Reste ist streng monoton fallend. Nach einer endlichen Anzahl von Schritten geht also die letzte Division mit Rest auf, d.h. man hat

$$a_{k-1} = q_{k-1} a_k + a_{k+1}, 0 \leq a_{k+1} < a_k$$

$$a_k = q_k a_{k+1} + 0.$$

Es wird nun behauptet, daß a_{k+1} ein größter gemeinsamer Teiler von a_1 und a_2 ist. Das beweist man so. Einerseits erkennt man beim Durchgang der Rekursionsgleichungen von unten nach oben, daß a_{k+1} alle a_i mit $i \leq k+1$ teilt. Andererseits sieht man beim Durchgang der Rekursionsgleichungen von oben nach unten, daß jeder gemeinsame Teiler von a_1 und a_2 alle a_i teilt für $1 \leq i \leq k+1$, insbesondere also a_{k+1} .

Wenn M nur endlich viele Elemente enthält, so beweist man die Existenz des größten gemeinsamen Teilers induktiv. Der größte gemeinsame Teiler einer unendlichen Menge M ist der kleinste unter den größten gemeinsamen Teilern der endlichen Teilmengen von M .

□

Als Abkürzung für “größter gemeinsamer Teiler” benutzt man “ggT”. Sind a_1, \dots, a_k ganze Zahlen, so bezeichnet $\text{gcd}(a_1, \dots, a_k)$ den ggT von $\{a_1, \dots, a_k\}$.

ggT 3

1.5.3. Satz *Der ggT von ganzen Zahlen a_1, \dots, a_k ist eine ganzzahlige Linearkombination dieser Zahlen, d.h. es gibt ganze Zahlen c_1, \dots, c_k für die $\text{gcd}(a_1, \dots, a_k) = c_1a_1 + \dots + c_k a_k$ gilt.*

Beweis: Ich verwende die Bezeichnungen aus dem Beweis von Satz 1.5.2. Dort ist $\text{gcd}(a_1, a_2) = a_{k+1} = a_{k-1} - q_{k-1}a_k$. Hierin kann man a_k ersetzen mittels $a_k = a_{k-2} - q_{k-2}a_{k-1}$. Setzt man dieses Verfahren fort, so folgt die Behauptung für $k = 2$. Für $k > 2$ zeigt man die Behauptung durch vollständige Induktion. \square

Aus den Beweisen von Satz 1.5.2 und Satz 1.5.3 erhält man Algorithmen zur Berechnung des ggT zweier Zahlen und zur Bestimmung der Koeffizienten in der Darstellung dieses ggT als ganzzahlige Linearkombination. Hier sind die die Algorithmen.

ggT 4

1.5.4. Algorithmus

Euklidischer Algorithmus

INPUT: Ganze Zahlen a, b .

OUTPUT: $d = \text{gcd}(a, b)$

- (1) $d = \max\{|a|, |b|\}$, $r = \min\{|a|, |b|\}$
- (2) **while** ($r \neq 0$) **do**
- (3) $h = r$; $r = d - \lfloor d/r \rfloor r$; $d = h$
- (4) **od**

ggT 5

1.5.5. Algorithmus

Erweiterter Euklidischer Algorithmus

INPUT: Ganze Zahlen a, b OUTPUT: $d = \gcd(a, b)$ und ganze Zahlen e, f mit $d = ae + bf$

```

(1) if ( $|a| \geq |b|$ ) then
(2)    $d = |a|$ ;  $r = |b|$ ,  $e = \text{sign}(a)$ ,  $e' = 0$ ,  $f = 0$ ,
       $f' = \text{sign}(b)$ 
(3) else
(4)    $d = |b|$ ,  $r = |a|$ ,  $f = \text{sign}(b)$ ,  $f' = 0$ ,  $e = 0$ ,
       $e' = \text{sign}(a)$ 
(5) fi
(6) while ( $r \neq 0$ ) do
(7)    $q = \lfloor d/r \rfloor$ 
(8)    $\begin{pmatrix} d & r \\ e & e' \\ f & f' \end{pmatrix} = \begin{pmatrix} d & r \\ e & e' \\ f & f' \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$ 
(9) od

```

Den Beweis folgender Resultate findet man in [2]

ggT 6

1.5.6. Satz Seien a, b zwei ganze Zahlen mit $|a| \geq |b| > 1$.

1. Die Anzahl der Iterationen in Algorithmus 1.5.4 und Algorithmus 1.5.5 ist höchstens $\log |b| \log((1 + \sqrt{5})/2) + 1$.
2. Die Laufzeit von Algorithmus 1.5.4 und Algorithmus 1.5.5 ist $O(\text{size}(a) \text{size}(b))$.
3. Für die Koeffizienten e und f , die in Algorithmus 1.5.5 berechnet werden, gilt $|e| \leq |b|/(2 \gcd(a, b))$ und $|f| \leq |a|/(2 \gcd(a, b))$. Gilt ferner $\gcd(a, b) = e'a + f'b$ für zwei ganze Zahlen e' und f' , so folgt $|e'| \geq e$ und $|f'| \geq f$.

Außerdem wird in [1] folgender Satz bewiesen.

ggT 7

1.5.7. Satz Ist $M(n)$ die Zeit, die man zur Multiplikation zweier n -Bit Zahlen benötigt, so gibt es einen Algorithmus, der den ggT zweier n -Bit Zahlen mit Darstellung in Zeit $O(M(n) \log n)$ berechnet.

Mit diesem Satz und Satz 1.4.3 erhält man folgendes Ergebnis.

ggT 8

1.5.8. Satz Derr ggT zweier n -Bit Zahlen mit darstellung kann in Zeit $O(n \log^2 n \log \log n)$ bestimmt werden.

Wendet man obige Algorithmen iteriert an, so kann man damit auch den ggT mit Darstellung von k Zahlen berechnen. Die Koeffizienten dieser Darstellung sind dann aber alles andere als optimal. Man kann sogar zeigen, daß das Problem, einen bezüglich der Maximumnorm minimalen Koeffizientenvektor zu finden, NP-vollständig ist (siehe [5]).

1.6 Eindeutige Primfaktorzerlegung

primfact 1

1.6.1. Satz 1. Aus $a \mid bc$ und $\gcd(a, b) = 1$ folgt $a \mid c$.

2. Teilt eine Primzahl ein Produkt ganzer Zahlen, so teilt sie wenigstens einen Faktor.

Beweis: Nach Satz 1.5.3 ist $1 = ae + bf$ mit ganzen Zahlen e, f . Daher ist $c = a(ce) + (bc)f$. Hieraus folgt $a \mid c$.

Für zwei Faktoren folgt die zweite Behauptung aus der ersten. Für mehr als zwei Faktoren durch vollständige Induktion. \square

primfact 2

1.6.2. Satz Jede natürliche Zahl $a > 1$ ist ein Produkt von Primzahlen. Die Zerlegung in Primfaktoren ist bis auf die Reihenfolge eindeutig.

Beweis: Die Existenz der Primfaktorzerlegung von a wird durch vollständige Induktion gezeigt. Für $a = 2$ ist die Behauptung wahr. Sei $a > 2$ und sei a keine Primzahl. Nach Satz 1.3.2 besitzt a einen Primfaktor p . Sei $b = a/p$. Dann ist $1 < b < a$ und nach Induktionsannahme ist b ein Produkt von Primzahlen und das beweist die Behauptung.

Seien $p_1 p_2 \cdots p_r = a = q_1 q_2 \cdots q_s$ zwei Primfaktorzerlegungen von a , wobei r minimal sei. Ich führe den Beweis durch vollständige Induktion über r . Ist $r = 1$, so muß $s = 1$ und $q_1 = p_1$ sein, weil Primzahlen keine nicht triviale Zerlegung besitzen. Sei $r > 1$. Dann ist nach Satz 1.6.1 p_r ein Teiler eines der q_i und damit ist $p_r = q_i$ für ein i . Ohne Beschränkung der Allgemeinheit sei $p_r = q_s$, also $p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$. Nach Induktionsannahme sind diese Zerlegungen bis auf die Reihenfolge gleich und das beweist die Behauptung. \square

Nach Satz 1.6.2 kann man für jede von 0 verschiedene ganze Zahl a

$$a = \prod_{p \in \mathbb{P}} p^{e(p,a)}$$

schreiben. Dies definiert also eine Abbildung

$$\mathbb{Z} - \{0\} \times \mathbb{P} \rightarrow \mathbb{Z}_{\geq 0}, \quad (a, p) \mapsto e(p, a).$$

primfact 3

1.6.3. Übung Man zeige, daß für ganze Zahlen $a, b, a_1, \dots, a_k \neq 0$.

1. Für alle Primzahlen p gilt $e(p, ab) = e(p, a) + e(p, b)$.

2. a teilt b genau dann, wenn $e(p, a) \leq e(p, b)$ gilt für alle Primzahlen p .
3. Es gilt $a = \pm b$ genau dann, wenn $e(p, a) = e(p, b)$ ist für alle Primzahlen p .
4. $\gcd(a_1, \dots, a_k) = \prod_{p \in \mathbb{P}} p^{\min\{e(p, a_i) : 1 \leq i \leq k\}}$.

Die Primfaktorzerlegung einer natürlichen Zahl tatsächlich zu finden, ist sehr schwer. es ist kein polynomialer Algorithmus bekannt, der dieses Problem löst. Siehe hierzu [9].

Ändert man das Berechnungsmodell und verwendet einen sogenannten Quantencomputer, also einen Computer, der die Gesetze der Quantenmechanik ausnutzt, so kann man tatsächlich in Polynomzeit faktorisieren. Zitat ergänzen. Es ist aber noch nicht klar, ob man einen solchen Computer wirklich bauen kann.

1.7 Kongruenzen

Sei m eine natürliche Zahl.

cong 1

1.7.1. Definition Zwei ganze Zahlen a und b heißen kongruent modulo m , wenn m die Differenz $b - a$ teilt. Man schreibt $a \equiv b \pmod{m}$.

cong 2

1.7.2. Übung Zeige, daß genau dann $a \equiv b \pmod{m}$ gilt, wenn a und b denselben Rest bei der Division durch m lassen.

cong 3

1.7.3. Satz Kongruenz modulo m ist eine Äquivalenzrelation auf \mathbb{Z} .

Die Äquivalenzklasse von a heißt *Restklasse* von $a \pmod{m}$. Ich bezeichne sie mit $a \pmod{m}$. Aus Satz 1.4.1 folgt, daß $a \pmod{m}$ genau einen Vertreter r enthält mit $0 \leq r < m$. Der wird *kleinster nicht negativer Rest* von $a \pmod{m}$ genannt. Es ist auch leicht einzusehen, daß es genau einen Vertreter r in $a \pmod{m}$ gibt mit $-m/2 < r \leq m/2$. Das ist der *absolut kleinste Rest* von $a \pmod{m}$. Die Restklassen \pmod{m} kann man also durch einen dieser Reste eindeutig darstellen. Für jedes a kann man beide Reste in quasilinearer Zeit ausrechnen. Daher kann man in quasilinearer Zeit entscheiden, ob für zwei ganze Zahlen a und b die Restklassen $a \pmod{m}$ und $b \pmod{m}$ übereinstimmen. Dies ist nicht selbstverständlich. es gibt Äquivalenzrelationen, z.B. die Äquivalenz von indefiniten binären quadratischen Formen, für die kein polynomialer Entscheidungsalgorithmus bekannt ist.

cong 2.1

1.7.4. Satz Kongruenz \pmod{m} ist verträglich mit der Addition, Subtraktion und Multiplikation, d.h. aus $a \equiv a' \pmod{m}$ und $b \equiv b' \pmod{m}$ folgt $a + b \equiv a' + b' \pmod{m}$, $a - b \equiv a' - b' \pmod{m}$, $ab \equiv a'b' \pmod{m}$.

Mit Satz 1.7.3 definiert man Addition, Subtraktion und Multiplikation von Restklassen so:

$$a \text{ Mod } m + b \text{ Mod } m = (a+b) \text{ Mod } m, a \text{ Mod } m - b \text{ Mod } m = (a-b) \text{ Mod } m, a \text{ Mod } m \cdot b \text{ Mod } m = (ab) \text{ Mod } m.$$

Es gelten dieselben Rechengesetze wie bei ganzen Zahlen. Stellt man Restklassen durch die kleinsten nichtnegativen Reste dar, so addiert man Restklassen, indem man die Vertreter addiert und dann mod m reduziert. Entsprechend subtrahiert und multipliziert man Restklassen. Dies geht in quasilinearer Zeit. In der Praxis ist das Rechnen mit Restklassen aber erheblich zeitaufwendiger als das Rechnen mit ganzen Zahlen, weil z.B. Division mit Rest langsamer ist als Addition.

Satz 1.7.3 ist sehr nützlich bei der Rechnung mit Kongruenzen. Will man z.B. den Rest einer ganzen Zahl

$$a = \sum_{i=1}^k a_i 10^{k-i}$$

mod 11 bestimmen, so benutzt man

$$10^{k-i} \equiv (-1)^{k-i} \pmod{11}$$

und erhält

$$a \equiv \sum_{i=1}^k a_i (-1)^{k-i} \pmod{11}.$$

Der Ausdruck $\sum_{i=1}^k a_i (-1)^{k-i}$ heißt *alternierende Quersumme* von a . Um Teilbarkeit von a durch 11 festzustellen, braucht man nur zu prüfen, ob die alternierende Quersumme von a durch 11 teilbar ist.

Division mod m ist nicht immer möglich, wie der folgende Satz zeigt.

cong 4

1.7.5. Satz Genau dann gibt es eine ganze Zahl a' mit $aa' \equiv 1 \pmod{m}$ falls $\gcd(a, m) = 1$ ist.

Beweis: Ist $\gcd(a, m) = 1$, so gibt es nach Satz 1.5.3 ganze Zahlen a', c mit $1 = aa' + cm$ also $aa' \equiv 1 \pmod{m}$.

Gilt $aa' \equiv 1 \pmod{m}$ so gibt es eine ganze Zahl c mit $aa' + cm = 1$. Also ist $\gcd(a, m) = 1$. \square

Gilt $\gcd(a, m) = 1$ so heißt $a \text{ Mod } m$ *prime Restklasse* mod m . Gilt $aa' \equiv 1 \pmod{m}$ so schreibe ich auch $a' \equiv a^{-1} \pmod{m}$ und $(a \text{ Mod } m)^{-1} = a' \text{ Mod } m$. Es gilt noch folgende Kürzungsregel.

cong 5

1.7.6. Satz Ist $\gcd(a, m) = 1$ so folgt aus $ab \equiv ac \pmod{m}$, daß auch $b \equiv c \pmod{m}$ gilt.

Beweis: Wähle a' mit $aa' \equiv 1 \pmod{m}$ und erhalte $b \equiv a'ab \equiv aa'c \equiv c \pmod{m}$. \square

Um eine prime Restklasse mod m zu invertieren, muß man den ggT mit Darstellung des Vertreters mit m berechnen. Dies geht auch in quasilinearer Zeit. Division durch prime Restklassen geht also auch in quasilinearer Zeit.

Kapitel 2

Gruppen

2.1 Algebraische Struktur

algstr 1

2.1.1. Definition Es seien X und Y Mengen. Eine Abbildung $f : X \times X \rightarrow X$ heißt innere Verknüpfung auf X . Eine Abbildung $g : X \times Y \rightarrow X$ heißt äußere Verknüpfung auf X mit Operatorenbereich Y . Ein Tupel $(X, f_1, \dots, f_n, Y_1, g_1, \dots, Y_m, g_m)$ bestehend aus einer nicht leeren Menge X , inneren Verknüpfungen f_i auf X , $1 \leq i \leq n$, und äußeren Verknüpfungen g_j auf X mit nicht leerem Operatorenbereich Y_i , $1 \leq i \leq m$ heißt eine algebraische Struktur.

Ist f eine innere Verknüpfung auf einer Menge X , so schreibt man xfy statt $f(x, y)$. Zum Beispiel sind Addition und Multiplikation Verknüpfungen auf der Menge der ganzen Zahlen und auch auf der Menge der Restklassen mod m für jede natürliche Zahl m . Andere Beispiele für innere Verknüpfungen auf Mengen sind die Konkatenation auf der Menge aller Strings über einem endlichen Alphabet und die logischen Verknüpfungen \vee und \wedge auf der Menge $\{0, 1\}$.

algstr 2

2.1.2. Übung Sei m eine natürliche Zahl. Zeige, daß die Multiplikation von Restklassen eine Verknüpfung auf der Menge der primen Restklassen mod m ist. Zeige auch, daß die Addition von Restklassen keine Verknüpfung auf dieser Menge ist.

algstr 3

2.1.3. Beispiel Eine äußere Verknüpfung auf der Menge aller Restklassen nach einem natürlichen Modul m mit Operatorbereich \mathbb{N} ist die *Potenzierung*

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z}/m\mathbb{Z}, \quad (x \text{ Mod } m, n) \mapsto x^n \text{ Mod } m.$$

Für die Menge der primen Restklassen mod m kann man diese Verknüpfung sogar auf den Operatorbereich \mathbb{Z} fortsetzen.

Verknüpfungen auf einer endlichen Menge $X = \{x_1, \dots, x_n\}$ kann man durch eine *Verknüpfungstafel* angeben. Folgende Verknüpfungstafel beschreibt z.B. die Multiplikation auf $\mathbb{Z}/4\mathbb{Z}$.

| | | | | |
|---|---|---|---|---|
| · | 0 | 1 | 2 | 3 |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

algstr 4

2.1.4. Definition Seien $(X, \top_1, \dots, \top_n, Y_1, \perp_1, \dots, Y_m, \perp_m)$ und $(U, \vee_1, \dots, \vee_n, Y_1, \wedge_1, \dots, Y_m, \wedge_m)$ algebraische Strukturen mit gleicher Anzahl innerer und äußerer Verknüpfungen und gleichen Operatorbereichen. Eine Abbildung $f : X \rightarrow U$ heißt Homomorphismus der ersten Struktur in die zweite, wenn sie folgende Bedingungen erfüllt.

1. $f(a \top_i b) = f(a) \perp_i f(b)$ für alle $a, b \in X$ und $1 \leq i \leq n$.
2. $f(y \vee_i a) = y \wedge_i f(a)$ für alle $y \in Y_i$, $a \in X$ und $1 \leq i \leq n$.

Hier sind noch ein paar andere Begriffe. Injektive Homomorphismen heißen *Monomorphismen*, surjektive Homomorphismen heißen *Epimorphismen*, bijektive Homomorphismen heißen *Isomorphismen*. Homomorphismen einer algebraischen Struktur in sich selbst heißen *Endomorphismen*.

algstr 5

2.1.5. Beispiel Sei m eine natürliche Zahl. Dann ist die Abbildung $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$, $a \rightarrow a \text{ Mod } m$ eine Homomorphismus von $(\mathbb{Z}, +, \cdot)$ in $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$.

algstr 6

2.1.6. Definition Eine innere Verknüpfung $\circ : X \times X \rightarrow X$ heißt assoziativ, wenn $a \circ (b \circ c) = (a \circ b) \circ c$ gilt für alle $a, b, c \in X$. Sie heißt kommutativ, wenn $a \circ b = b \circ a$ gilt für alle $a, b \in X$.

Es soll gezeigt werden, daß bei einer assoziativen Verknüpfung das Ergebnis einer Verknüpfung von n Elementen von der Klammerung unabhängig ist.

algstr 7

2.1.7. Definition Sei eine innere Verknüpfung $\circ : X \times X \rightarrow X$ und eine Folge (x_1, \dots, x_n) von Elementen aus X vorgegeben. Die Verknüpfungen dieser Folge (bezüglich \circ) sind induktiv folgendermaßen definiert.

1. Ist $n = 1$ so ist x_1 die einzige Verknüpfung der Folge.
2. Ist $n > 1$, $1 \leq i < n$, ist u eine Verknüpfung von (x_1, \dots, x_i) und v eine Verknüpfung von (x_{i+1}, \dots, x_n) , so ist $u \circ v$ eine Verknüpfung von (x_1, \dots, x_n) .

algstr 8

2.1.8. Satz Ist \circ eine assoziative Verknüpfung auf der Menge X und ist f eine endliche Folge von Elementen von X , so sind alle Verknüpfungen von f gleich.

Beweis: Der Beweis wird durch Induktion über die Länge von f geführt. □

Die einzige Verknüpfung von $f = (x_1, \dots, x_n)$ in Satz 2.1.8 wird mit

$$\bigcirc_{i=1}^n x_i$$

bezeichnet.

algstr 9

2.1.9. Definition Sei M eine Menge. Eine Permutation von M ist eine bijektive Abbildung $M \rightarrow M$. Die Menge aller Permutationen der Menge $\{1, \dots, n\}$ wird mit S_n bezeichnet.

algstr 10

2.1.10. Satz Ist \circ eine assoziative Verknüpfung auf der Menge X und ist $f = (x_1, \dots, x_k)$ eine endliche Folge von Elementen von X , so gilt

$$\bigcirc_{i=1}^n x_i = \bigcirc_{i=1}^n x_{\pi(i)}$$

für alle $\pi \in S_n$.

2.2 Halbgruppen

halb 1

2.2.1. Definition Eine Halbgruppe ist ein Paar (H, \circ) , bestehend aus einer nicht leeren Menge H und einer assoziativen inneren Verknüpfung \circ auf H .

halb 1.1

2.2.2. Beispiel 1. Das Paar $(\mathbb{N}, +)$ ist eine Halbgruppe.

2. Ist Σ ein Alphabet, so ist (Σ^*, \circ) eine Halbgruppe, wobei \circ die Konkatenation von Strings bedeutet.

In einer Halbgruppe (H, \circ) definiert man zu jedem Element $a \in H$ und jeder natürlichen Zahl n die n -te Potenz, indem man $a^1 = a$ und $a^{n+1} = a \circ a^n$ setzt.

halb 2

2.2.3. Satz Für $a \in H$ und $n, m \in \mathbb{N}$ gilt $a^n \circ a^m = a^{n+m}$ sowie $(a^n)^m = a^{nm}$.

Berechnet man a^n durch sukzessive Multiplikation, so braucht man dafür $n - 1$ Multiplikationen in H . Man kann Satz 2.2.3 benutzen, um diese Berechnung wesentlich zu beschleunigen. Hierzu schreibt man den Exponenten n in Binärdarstellung auf, d.h. als

$$n = \sum_{i=0}^k b_i 2^{k-i}.$$

Nach Satz 2.2.3 gilt dann

$$a^n = \prod_{i=1}^k (a^{2^i})^{b_i} = \prod_{b_i=1} (a^{2^i}).$$

Dies legt es nahe, die Potenzen a^{2^i} zu berechnen für $0 \leq i \leq k$ und a^n als Produkt der entsprechenden a^{2^i} zu bestimmen. Hierbei beachte man, daß

$$a^{2^{i+1}} = (a^{2^i})^2$$

ist.

Dies führt zu folgendem Algorithmus.

halb 3

2.2.4. Algorithmus

| |
|---|
| <p style="text-align: center;">Schnelle Exponentiation</p> <p>INPUT: $a \in H, n \in \mathbb{N}$ OUTPUT: $b = a^n$</p> <hr/> <pre> (1) $b = 1; c = a$ (2) while ($n > 0$) do (3) if ($n \equiv 1 \pmod{2}$) then (4) $b = bc; n = n - 1;$ (5) fi (6) $d = d/2, c = c^2$ (7) od </pre> |
|---|

halb 4

2.2.5. Satz *Algorithmus 2.2.4 benötigt höchstens $2\lceil \log n \rceil$ Multiplikationen in H .*

halb 5

2.2.6. Übung Eine Variante der schnellen Exponentiation in Halbgruppen beruht auf folgender Formel

$$g^n = \begin{cases} (g^{n/2})^2 & \text{für } n \equiv 0 \pmod{2} \\ g \cdot (g^{(n-1)/2})^2 & \text{für } n \not\equiv 0 \pmod{2} \end{cases}.$$

Man gebe den entsprechenden Algorithmus an und analysiere ihn.

Exponentiation (H, \circ) kann zu kryptographischen Zwecken verwendet werden. Wollen sich zwei Kommunikationspartner A und B einen geheimen Schlüssel über eine unsichere Leitung einigen, so einigen sie sich öffentlich auf ein Element $h \in H$. Dann wählt A einen geheimen Exponenten a , bestimmt $\alpha = h^a$ und schickt α an B. B wählt einen geheimen

Exponenten b , bestimmt $\beta = h^b$ und schickt β an A. Danach bestimmt A das Element $\beta^a = (h^b)^a = h^{ab}$ und B bestimmt das Element $\alpha^b = (h^a)^b = h^{ab}$. Beide haben also das selbe Element h^{ab} , das sie als Schlüssel verwenden. Man beachte, daß hier mehrfach die Potenzgesetze aus Satz 2.2.3 verwendet wurden. Ein Lauscher kennt H, h, α, β . Hieraus h^{ab} zu berechnen bezeichnet man als das *Diffie-Hellman-Problem* in H nach den Erfindern dieses Verfahrens Diffie und Hellman (siehe [4]). Der Lauscher könnte h^{ab} ermitteln, wenn er die Exponenten a und b bestimmen könnte. Der Exponent a heißt *diskreter Logarithmus* von α zur Basis h . Es ist klar, daß das Diffie-Hellman-Problem höchstens so schwer ist, wie das Problem, in H diskrete Logarithmen zu berechnen. Die Umkehrung ist nicht bekannt und gehört zu den wichtigen offenen Problemen der Kryptoanalyse. In der Praxis wird vor allem die multiplikative Halbgruppe der primen Restklassen nach einem großen Primzahlmodul p verwendet. Hat p mehr als 200 Dezimalstellen, so gelten obige Probleme zur Zeit als unlösbar.

2.3 Direkte Produkte

Es sei I eine nicht leere Menge, die hier als Indexmenge gebraucht wird. Es sei $\{H_\alpha, \top_\alpha\}$ eine Familie von Halbgruppen. Auf dem mengentheoretischen direkten Produkt

$$\prod_{\alpha \in I} H_\alpha = \{f \mid f : I \rightarrow \cup_{\alpha \in I} H_\alpha \text{ mit } f(\alpha) \in H_\alpha\}$$

definiert man komponentenweise eine innere Verknüpfung

$$\top : \prod_{\alpha \in I} H_\alpha \times \prod_{\alpha \in I} H_\alpha \rightarrow \prod_{\alpha \in I} H_\alpha$$

durch

$$(f \top g)(\alpha) = f(\alpha) \top_\alpha g(\alpha).$$

Diese Verknüpfung ist assoziativ. Also ist $(\prod_{\alpha \in I} H_\alpha, \top)$ eine Halbgruppe. Sie heißt *direktes Produkt* der Halbgruppen $\{H_\alpha, \top_\alpha\}$.

Analog werden direkte Produkte beliebiger algebraischer Strukturen definiert.

2.4 Faktorhalbgruppen

Wieder sei (H, \circ) eine Halbgruppe.

In diesem Abschnitt sei (H, \circ) eine Halbgruppe und R eine Äquivalenzrelation auf H . fakthg 1

2.4.1. Definition Die Äquivalenzrelation R heißt mit der Verknüpfung \circ linksverträglich bzw. rechtsverträglich, wenn für alle $(x, y) \in R$ und alle $a \in H$ auch $(a \circ x, a \circ y)$ bzw. $(x \circ a, y \circ a)$ in R liegt. Die Relation R heißt verträglich mit \circ , wenn sie linksverträglich und rechtsverträglich mit \circ ist.

fakthg 2

2.4.2. Beispiel Sei $\Sigma = \{0, 1\}$ und \circ die Konkatenation auf Σ^* . Wir betrachten die Halbgruppe (Σ^*, \circ) . Wir nennen zwei Strings in Σ^* äquivalent, wenn sie gleich lang sind. Dies ist eine Äquivalenzrelation, die mit \circ verträglich ist.

fakthg 3

2.4.3. Übung Betrachte die Halbgruppe der $(\mathbb{Z}^{n \times n}, \cdot)$. Wir nennen zwei Matrizen $A, B \in \mathbb{Z}^{n \times n}$ äquivalent, wenn es eine Matrix $U \in \mathbb{Z}^{n \times n}$ gibt mit $\det U = 1$ und $A = UB$. Zeige, daß dies eine Äquivalenzrelation ist. Untersuche, ob die Äquivalenzrelation mit \cdot verträglich ist.

fakthg 4

2.4.4. Satz Genau dann ist \circ mit R verträglich, wenn mit $(x, y), (u, v) \in R$ auch $(x \circ u, y \circ v)$ zu R gehört.

Beweis: Sind die angegebenen Bedingungen erfüllt, so ist R mit \circ verträglich, weil man $(x, y) = (a, a)$ und $(u, v) = (a, a)$ setzen kann.

Sei R mit \circ verträglich und $(x, y), (u, v) \in R$. Dann gilt $(x \circ u, y \circ u) \in R$ und $(y \circ u, y \circ v) \in R$. Daher folgt aus der Transitivität von R , daß auch $(x \circ u, y \circ v)$ zu R gehört. \square

Die Äquivalenzklasse von $a \in H$ wird mit $[a]_R$ oder kurz $[a]$ bezeichnet. Die Menge aller Äquivalenzklassen wird H/R geschrieben.

fakthg 5

2.4.5. Satz Sei R verträglich mit \circ . Definiert man $[a] \circ [b] = [a \circ b]$ für $a, b \in H$, so ist $(H/R, \circ)$ eine Halbgruppe.

Beweis: \square

Die in Satz 2.4.5 konstruierte Halbgruppe heißt *Faktorhalbgruppe* oder *Restklassenhalbgruppe* von R nach H .

2.5 Neutrale Elemente

Wieder sei (H, \circ) eine Halbgruppe.

neutr 1

2.5.1. Definition Ein Element $e \in H$ heißt rechtsneutrales bzw. linksneutrales Element der Halbgruppe, wenn $a \circ e = a$ bzw. $e \circ a = a$ gilt für alle $a \in H$. Ist e zugleich rechtsneutrales und linksneutrales Element der Halbgruppe, so heißt e neutrales Element der Halbgruppe.

neutr 2

2.5.2. Beispiel Betrachte die Menge H aller 2×2 -Matrizen mit ganzzahligen Einträgen, in denen beide Einträge in der zweiten Spalte 0 sind. Zusammen mit der Matrixmultiplikation ist das eine Halbgruppe. Diese Halbgruppe besitzt kein linksneutrales Element und das rechtsneutrale Element

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

neutr 3

2.5.3. Satz *Ist e ein linksneutrales und f ein rechtsneutrales Element der Halbgruppe, so ist $e = f$. Insbesondere besitzen Halbgruppen höchstens ein neutrales Element.*

Beweis: Es gilt $e = ef = f$. □

2.6 Invertierbare Elemente

Wieder (H, \circ) eine Halbgruppe mit neutralem Element e . inv 1

2.6.1. Definition *Ein Element $a \in H$ heißt linksinvertierbar bzw. rechtsinvertierbar in der Halbgruppe, wenn es $b \in H$ gibt mit $b \circ a = e$ bzw. $a \circ b = e$. Ein links- und rechtsinvertierbares Element heißt invertierbar.* inv 2

2.6.2. Satz *Ist $a \in H$ invertierbar mit Linksinversem b und Rechtsinversem b' , dann gilt $b = b'$.*

Beweis: $b = b \circ e = b \circ (a \circ b') = (b \circ a) \circ b' = b'$. □

Die Menge der invertierbaren Elemente in H wird mit H^* bezeichnet. Ihre Elemente heißen *Einheiten* von H . Man beachte, daß die Definition von H^* von der Verknüpfung \circ abhängt. inv 3

2.6.3. Beispiel Betrachte die Halbgruppe (\mathbb{Z}, \cdot) . Dann ist $\mathbb{Z}^* = \{\pm 1\}$. Betrachte die Halbgruppe $(\{x + y\sqrt{5} : x, y \in \mathbb{Z}\}, \cdot)$. In dieser Halbgruppe ist z.B. $\alpha = (1 + \sqrt{5})/2$ invertierbar mit dem Inversen $\alpha' = (-1 + \sqrt{5})/2$. Außerdem sind alle Potenzen von $\pm\alpha$ und $\pm\alpha'$ invertierbar. Andere invertierbare Elemente gibt es in dieser Halbgruppe nicht.

2.7 Gruppen

gruppe 1

2.7.1. Definition Eine Halbgruppe (H, \cdot) heißt Gruppe wenn sie ein linksneutrales Element e besitzt und wenn es für alle $a \in H$ ein $b \in H$ gibt mit $b \cdot a = e$.

gruppe 2

2.7.2. Satz Gilt $a^2 = a$ für ein Element a einer Gruppe (G, \cdot) mit linksneutralem Element e , dann ist $a = e$.

Beweis: Sei $b \in G$ mit $ba = e$. Dann gilt $a = ea = (ba)a = b(a^2) = ba = e$. □

gruppe 3

2.7.3. Satz Eine Halbgruppe (G, \cdot) ist genau dann eine Gruppe, wenn sie ein genau ein neutrales Element enthält und alle Elemente von G invertierbar sind.

Beweis: Wir müssen nur zeigen, daß Gruppen die obigen Eigenschaften haben. Sei (G, \cdot) eine Gruppe mit Linksneutralem Element e . Sei $a, b \in G$ mit $ba = e$. Dann gilt $(ab)(ab) = a(ba)b = aeb = ab$. Also ist $ab = e$ nach Satz 2.7.2. Weiter gilt $a = ea = (ab)a = a(ba) = ae$. Also ist e auch rechtsneutrales Element. Aus Satz 2.5.3 folgt, daß e das eindeutig bestimmte neutrale Element von G ist. □

Das Inverse eines Elementes a einer Gruppe G bezeichnet man mit a^{-1} .

gruppe 4

2.7.4. Satz Ist (H, \circ) eine Halbgruppe mit neutralem Element e , so ist (H^*, \circ) eine Gruppe.

Sei in Zukunft (G, \cdot) eine Gruppe mit neutralem Element e .

gruppe 5

2.7.5. Satz Für $a, a_1, \dots, a_n \in G$ gelten folgende Rechengesetze.

1. $(a^{-1})^{-1} = a$.
2. $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.
3. $(a^{-1})^m = (a^m)^{-1}$.

Setzt man $a^0 = e$ und $a^n = (a^{-1})^n$ so folgen aus Satz 2.7.5 die üblichen Potenzgesetze.

gruppe 6

2.7.6. Satz Eine Halbgruppe (H, \cdot) ist genau dann eine Gruppe, wenn es zu je zwei Elementen a, b Elemente x, y gibt mit $ax = b$ und $ya = b$.

Die folgenden Rechengesetze werden als *Kürzungsregeln* bezeichnet.

gruppe 7

2.7.7. Satz Für alle $a, b, c \in G$ folgt aus $ac = bc$ daß auch $a = b$ gilt und aus $ca = cb$, daß auch $a = b$ gilt.

Ist G endlich, so heißt die Elementanzahl von G auch *Ordnung* von G . Ist \cdot kommutativ, so heißt die Gruppe G *kommutativ* oder *abelsch*.

2.8 Beispiele von Gruppen

Bekannt sind schon folgende abelsche Gruppen: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ für $m \in \mathbb{N}$. Letzere Gruppe heißt *prime Restklassengruppe mod m* .

Die Menge der Permutationen $S(X)$ einer nicht leeren Menge X ist zusammen mit der Hintereinanderausführung eine Gruppe. Sie heißt *symmetrische Gruppe* von X . Die symmetrische Gruppe von $\{1, \dots, n\}$ bezeichnet man auch als S_n und nennt sie *symmetrische Gruppe der Stufe n* .

beispgr 1

2.8.1. Satz Es gilt $|S_n| = n!$.

Unter einer *Bewegung* des \mathbb{R}^n versteht man eine Permutation des \mathbb{R}^n , die die Abstände zwischen zwei Punkten unverändert läßt. Die *Symmetrieneiner* Teilmenge F des \mathbb{R}^n sind die Bewegungen f des \mathbb{R}^n , die F in sich selbst abbilden, d.h. für die $f(F) = F$ gilt. Die Symmetrien von F bilden zusammen mit der Hintereinanderausführung eine Gruppe, die *Symmetriegruppe* von F .

Betrachte als Beispiel ein Quadrat.

....

2.9 Gruppentafeln

Wir sind daran interessiert, alle Gruppen einer festen endlichen Ordnung zu finden. Dies ist so noch keine vernünftige Aufgabe, weil die Elemente beliebige Namen haben können. Z.B. ist $(\{e\}, \cdot)$ eine Gruppe, wenn man einfach $e \cdot e = e$ setzt. Dies ist eine Gruppe der Ordnung 1. Benennt man e um, so erhält man eine andere Gruppe der Ordnung 1. Diese ist aber isomorph zur ersten. Isomorphie von Gruppen ist eine Äquivalenzrelation ist. Die Äquivalenzklassen heißen *Isomorphieklassen* von Gruppen. Zwei endliche Gruppen sind genau dann isomorph, wenn sie, nach Umbenennung der Elemente dieselbe Verknüpfungstafel haben. Die Verknüpfungstafel einer Gruppe heißt *Gruppentafel*. Es kann also nur endlich viele Isomorphieklassen von Gruppen einer festen endlichen Ordnung geben. Die Aufgabe lautet nun, für jede dieser Klassen einen Vertreter zu finden. Dies kann man machen, indem man alle möglichen Gruppentafeln angibt.

Aus der Kürzungsregel folgt, daß die Zeilen und Spalten einer Gruppentafel Permutationen der Gruppenelemente sind. In der Zeile und Spalte des neutralen Elementes stehen die Gruppenelemente in der Originalreihenfolge. Sind diese beiden Regeln erfüllt, so ist die Existenz von neutralem Element und der inversen Elemente gesichert und man muß noch die Assoziativität nachprüfen. Diese spiegelt sich in der Gruppentafel nicht unmittelbar wieder. Dagegen ist die Gruppe genau dann kommutativ, wenn ihre Gruppentafel symmetrisch ist bezüglich der Diagonalen von links oben nach rechts unten.

Auf diese Weise werden jetzt die endlichen Gruppen der Ordnung ≤ 4 klassifiziert.

Es ist klar, daß es genau eine Gruppe der Ordnung 1 gibt.

Die einzig mögliche Gruppentafel für eine Gruppe der Ordnung 2 ist

$$\begin{array}{cc} e & a \\ a & e \end{array}$$

Diese Gruppe ist isomorph zu $\mathbb{Z}/2\mathbb{Z}$. Sie ist abelsch.

Die einzig mögliche Gruppentafel für eine Gruppe der Ordnung 3 ist

$$\begin{array}{ccc} e & a & b \\ a & b & e \\ b & e & a \end{array}$$

Diese Gruppe ist isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Sie ist abelsch.

gruta 1

2.9.1. Übung Man entwickle einen Algorithmus, der nach obigem Vorbild alle endlichen Gruppen einer festen Ordnung n klassifiziert und schätze seine Komplexität ab.

2.10 Zyklische Gruppen und Elementordnung

Sei (G, \cdot) eine Gruppe mit neutralem Element e .

zyk 1

2.10.1. Satz Für alle $a \in G$ ist $(\{a^n : n \in \mathbb{Z}\}, \cdot)$ eine Gruppe.

zyk 2

2.10.2. Definition 1. Für $a \in G$ heißt $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ die von a erzeugte Untergruppe. Die Ordnung von a ist die Ordnung von $\langle a \rangle$. Sie wird mit $\text{ord}_G a$ bezeichnet.

2. G heißt zyklisch falls $G = \langle a \rangle$ ist für ein $a \in G$.

zyk 3

2.10.3. Beispiel ...

Bemerkung: Definition des vollen Restsystems nachtragen.

zyk 4

2.10.4. Satz Sei $a \in G$.

1. Gibt es eine natürliche Zahl k mit $a^k = e$, so ist $\text{ord}_G a = \min\{k : a^k = e\}$ und für $n, m \in \mathbb{Z}$ gilt $a^n = a^m$ genau dann, wenn $n \equiv m \pmod{\text{ord}_G a}$.
2. Ist $\text{ord}_G a$ endlich und R ein volles Restsystem $\pmod{\text{ord}_G a}$ so gilt $\langle a \rangle = \{a^r : r \in R\}$.
3. Gilt $a^k \neq e$ für alle natürlichen Zahlen k , dann ist a von unendlicher Ordnung und für $n, m \in \mathbb{Z}$ gilt $a^n = a^m$ genau dann, wenn $n = m$ ist.

Beweis: Sei $m = \min\{k : a^k = e\}$ und $n, m \in \mathbb{N}$. Schreibe $n - m = qm + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < m$. Dann gilt $a^n = a^m$ genau dann, wenn $e = a^{n-m} = a^{qm+r} = a^r$. Wegen der Minimalität von m ist dies gleichbedeutend mit $r = 0$. Die Anzahl der verschiedenen Potenzen von a ist also gleich der Anzahl der Restklassen \pmod{m} . Hieraus folgen alle drei Behauptungen. \square

Alle endlichen zyklischen Gruppen sind zu $\mathbb{Z}/n\mathbb{Z}$ isomorph. Dieser Satz ist nachzutragen und dann muß das Nachfolgende entsprechend geändert werden.

zyk 4.1

2.10.5. Korollar Für $a \in G$, $n \in \mathbb{Z}$ gilt genau dann $a^n = e$ wenn n ein Vielfaches der Ordnung von a ist.

zyk 5

- 2.10.6. Satz**
1. Für $a \in G$ und $m \in \mathbb{Z}$ gilt $\text{ord}_G a^m = \text{ord}_G a / \gcd(\text{ord}_G a, m)$.
 2. Für $a, b \in G$ folgt aus $ab = ba$ und $\gcd(\text{ord}_G a, \text{ord}_G b) = 1$ daß $\text{ord}_G(ab) = (\text{ord}_G a)(\text{ord}_G b)$ ist.

Beweis: Sei $\alpha = \text{ord}_G a$. Dann gilt $(a^m)^n = e$ genau dann, wenn $\alpha | nm$. Dies ist gleichbedeutend damit, daß $\alpha / \gcd(\alpha, m)$ ein Teiler von n ist. Die kleinste Zahl n , die das erfüllt ist $\alpha / \gcd(\alpha, m)$. Diese ist nach Satz 2.10.4 die Ordnung von a^m .

Die zweite Behauptung wird als Übung bewiesen. \square

zyk 6

- 2.10.7. Satz**
1. Eine unendliche zyklische Gruppe hat genau zwei Erzeuger. Ist a ein Erzeuger, so ist a^{-1} der andere.
 2. Eine endliche zyklische Gruppe hat genau $\varphi(|G|)$ Erzeuger. Ist a ein Erzeuger, so ist $\{a^m : \gcd(|G|, m) = 1\}$ die Menge aller Erzeuger.

Beweis: Sei a ein Erzeuger der zyklischen Gruppe G .

Sei G unendlich. Sei $m \in \mathbb{Z}$ und a^m ein anderer Erzeuger von G . Dann muß es für alle $n \in \mathbb{Z}$ ein $x \in \mathbb{Z}$ geben mit $a^n = a^{xm}$. Aus Satz 2.10.4 folgt, daß $n = xm$ lösbar sein muß für alle $n \in \mathbb{N}$. Damit ist $m = \pm 1$.

Sei G endlich. Ein Element a^m ist genau dann ein Erzeuger von G , wenn $\text{ord}_G a^m = \text{ord}_G a$. Dies ist nach Satz 2.10.6 gleichbedeutend damit, daß $\text{gcd}(|G|, m) = 1$ ist. Aus Satz 2.10.4 folgt, daß die Anzahl der Erzeuger gerade $\varphi(|G|)$ ist. \square

Ist m eine natürliche Zahl und ist $b \in G$ so nennt man eine Lösung x der Gleichung $x^m = b$ eine m -te Wurzel von b . zyk 7

2.10.8. Satz Sei m eine natürliche Zahl. Ein Element b einer endlichen zyklischen Gruppe hat genau dann eine m -te Wurzel, wenn $b^{|G|/\text{gcd}(m, |G|)} = 1$ ist. Die Anzahl der m -ten Wurzeln ist dann $\text{gcd}(m, |G|)$.

Beweis: Sei a ein Erzeuger von G , $a^\beta = b$. Der Ansatz $x = a^\xi$ führt zu der Gleichung $a^{m\xi} = a^\beta$, also nach Satz 2.10.4 zu der Kongruenz $m\xi \equiv \beta \pmod{|G|}$. Diese Kongruenz ist genau dann lösbar, wenn $\text{gcd}(m, |G|) | \beta$, d.h. $\text{gcd}(m, |G|) | \text{gcd}(|G|, \beta)$, d.h. $\text{ord}_G b = |G|/\text{gcd}(|G|, \beta) | |G|/\text{gcd}(|G|, m)$, d.h. $b^{|G|/\text{gcd}(|G|, m)} = e$. Die Anzahl der mod $|G|$ verschiedenen Lösungen der Kongruenz ist die Anzahl der m -ten Wurzeln. \square

zyk 8

2.10.9. Satz Eine endliche Gruppe G ist genau dann zyklisch, wenn sie abelsch ist und e höchstens n verschiedene n -te Wurzeln hat für alle natürlichen Zahlen $n < |G|$.

Beweis: Endliche zyklische Gruppen haben nach Satz 2.10.8 obige Eigenschaften.

Habe umgekehrt die endliche Gruppe G obige Eigenschaften. Wir zeigen die Existenz eines Elementes der Ordnung $|G|$. Sei a ein Element maximaler Ordnung n in G . Sei $b \in G$ ein Element der Ordnung m . Dann ist m ein Teiler von n . Andernfalls gibt es einen Primteiler p von m , der nicht in n aufgeht. Die Ordnung von $c = b^{m/p^{e(p,m)}}$ ist $e(p, m)$ nach Satz 2.10.6. Die Ordnung von ac ist $np^{e(p,m)}$ ebenfalls nach Satz 2.10.6. Dies aber widerspricht der Maximalität von n . Damit gilt $b^n = 1$ für alle $b \in G$. Nach Voraussetzung kann es aber höchstens n viele solche Elemente in G geben. Damit ist $n = |G|$. \square

2.11 Berechnung der Elementordnung

Sei (G, \cdot) eine Gruppe. Als *elementare Operationen* in G bezeichnen wir

1. die Entscheidung, ob zwei Elemente in G gleich sind,
2. die Berechnung des Produkts zweier Gruppenelemente,

3. Die Berechnung des Inversen eines Gruppenelementes.

Ist G endlich, so besteht eine einfache Aufgabe darin, die Ordnung eines Elementes g zu berechnen. Dies kann man machen, indem man durch sukzessive die Potenzen g, g^2, \dots berechnet, bis der erste Exponent x gefunden ist mit $g^x = 1$. Hierzu sind $\text{ord}_G g$ viele Multiplikationen und Vergleiche in G nötig. Außerdem müssen konstant viele Gruppenelemente gespeichert werden. Man kann dieses Verfahren aber auf Kosten des Speicherplatzes beschleunigen. Hierzu benutzt man folgende Methode, um die natürlichen Zahlen aufzuzählen, die auf folgender Aussage beruht.

compord 1

2.11.1. Satz Sei v eine gerade natürliche Zahl.

1. Die Menge der natürlichen Zahlen ist die Menge aller Zahlen $x = 2^k v q + r$ mit $k \in \mathbb{N}$, $1 \leq r \leq 2^k v$, $\lfloor 4^{k-1} \rfloor v^2 \leq 2^k v q < 4^k v^2$.
2. Die obige Darstellung der natürlichen Zahlen ist eindeutig, d.h. zwei so dargestellte Zahlen sind genau dann gleich, wenn k, q, r übereinstimmen.

Beweis: Wir zeigen zuerst, daß jede natürliche Zahl in der obigen Weise dargestellt werden kann. Wähle hierzu k so, daß $\lfloor 4^{k-1} \rfloor v^2 \leq x < 4^k v^2$. Schreibe dann $x = 2^k v q + r$ mit $0 \leq r < 2^k v$. Dann ist $\lfloor 4^{k-1} \rfloor v^2 - 2^k v < 2^k v q \leq 4^k v^2 - 1$. Daraus folgt, daß $2^k v q < 4^k v^2$ ist. Außerdem erhält man $-v < v q$, also $0 \leq v q$ für $k = 0$. Für $k \geq 1$ gilt $4^{k-1} v^2 - 2^k v < 2^k v q$, also $2^{k-1}(v/2) - 1 < q$. Weil v gerade ist, folgt daraus $2^{k-1}(v/2) \leq q$, also $4^{k-1} v^2 \leq 2^k v q$.

Nun zeigen wir die Eindeutigkeit der Darstellung. Sei x in der beschriebenen Weise dargestellt. Dann gilt $\lfloor 4^{k-1} \rfloor v^2 \leq 2^k v q < 4^k v^2$. Daraus folgt, daß $q < 2^k v$, also $q \leq 2^k v - 1$, also $x = 2^k v q + r < 2^k v(2^k v - 1) + 2^k v = 4^k v^2$. Für $k = 0$ folgt außerdem $x \geq 1$ und für $k > 0$ hat man $x \geq 4^{k-1} v^2$. \square

Die Ordnung x wird in der Darstellung $x = y + r$ bestimmt, wobei $y = 2^k v q$ und q, r in den in Satz 2.11.1 angegebenen Schranken liegt. Der Parameter k durchläuft die Werte $0, 1, 2, \dots$ bis die Zuerst wird die Menge

$$R = \{(g^{-r}, r) : 1 \leq r \leq 2^k v\}$$

vorberechnet. Diese Menge hängt natürlich von k ab und muß für jedes neue k vergrößert werden. Dann wird für alle zulässigen y getestet, ob $g^{y+r} = 1$ ist für ein zulässiges r . Dies geschieht, indem geprüft wird, ob (g^y, r) in R vorkommt für ein r . Sobald ein passendes Paar gefunden ist, ist die Elementordnung $x = y+r$ gefunden. Der Vorteil dieses Vorgehens ist, daß man nur $O(\sqrt{x})$ viele Multiplikationen in G braucht, um die Ordnung zu finden. Außerdem kann man in vielen Gruppen die Elemente sortieren. Dies erlaubt es, den Test, ob (g^y) zu R gehört mittels binärer Suche durchzuführen. Die Ordnung x von g kann dann mittels $O(\sqrt{x})$ elementaren Operationen in G gefunden werden. Dafür muß man aber auch \sqrt{x} viele Gruppenelemente speichern. Die Zeitersparnis geht also auf Kosten des verbrauchten Speicherplatzes.

Hier ist die formale Version des Verfahrens.

compord 2

2.11.2. Algorithmus

| |
|---|
| <p style="text-align: center;">Berechnung der Elementordnung</p> <p>INPUT: $g \in G, v \in 2\mathbb{N}$ OUTPUT: $x = \text{ord}_G g$</p> |
| <pre> (1) $x = 0; u = v; s = 1; h = g^{-1}; a = 1; R = \emptyset;$ (2) $y = 0; b = 1; c = a^v;$ (3) while ($x = 0$) do (4) for ($r = s, s + 1 \dots, u$) do (5) $a = ah; R = R \cup \{(a, r)\}$ (6) od (7) while ($x = 0$ and $y < u^2$) do (8) if ($(b, r) \in R$ for some r) then (9) $x = y + r$ (10) else (11) $y = y + u; b = bc$ (12) fi (13) od (14) $s = u; u = 2u; c = c^2$ (15) od </pre> |

compord 3

2.11.3. Satz *Algorithmus 2.11.2 benötigt $O(\sqrt{\text{ord}_G g})$ Multiplikationen und Speicherplatz für $O(\sqrt{\text{ord}_G g})$ Gruppenelemente.*

Der beschriebene Algorithmus beruht auf einer Idee von D. Shanks [11]. Ich weise daraufhin, daß man die Berechnung der Elementordnung noch wesentlich beschleunigen kann, wenn man die Gruppenordnung kennt. Dies wird später noch diskutiert. Im übrigen ist der vorgestellte Algorithmus der schnellste, der für beliebige Gruppen bekannt ist.

2.12 Berechnung diskreter Logarithmen

Die Ideen des vorigen Abschnitts können auch angewendet werden, um diskrete Logarithmen in beliebigen Gruppen zu berechnen. Sei (G, \cdot) eine endliche Gruppe und seien g, d Gruppenelemente. Es soll entschieden werden, ob d zu der von g erzeugten Untergruppe gehört und wenn ja, soll $z = \log_g d$ bestimmt werden. Hierzu beachte man zuerst, daß im Fall der Existenz des diskreten Logarithmus $z < \text{ord}_G g$ gilt. Wie in Algorithmus 2.11.2 wird die Ordnung von g in G bestimmt, d.h. es wird versucht, Zahlen y und r zu finden mit $g^{y+r} = d$. Für jedes y wird aber vorher getestet, ob nicht vielleicht $g^{y+r} = 1$, d.h.

$d^{-1}g^y = g^r$, d.h. $(d^{-1}g^y, r) \in R$ ist für ein r . Dann ist nämlich der diskrete Logarithmus von d zur Basis g gefunden. Sobald aber die Ordnung von g bestimmt ist, kann es keinen diskreten Logarithmus von d zur Basis g mehr geben, weil der ja kleiner als die Ordnung sein müßte. Damit ergibt sich folgender Algorithmus.

compdl 1

2.12.1. Algorithmus

| |
|--|
| <p>DL-Berechnung</p> <p>INPUT: $g, d \in G, v \in 2\mathbb{N}$ OUTPUT: $x = \text{ord}_G g$ oder $z = \log_g d$</p> |
| <pre> (1) $x = 0$ $z = 0$; ; $u = v$; $s = 1$; $h = g^{-1}$; $a = 1$; $R = \emptyset$; (2) $y = 0$; $b = 1$; $c = a^v$; $e = d^{-1}$ (3) while ($x = 0$ and $y = 0$) do (4) for ($r = s, s + 1 \dots, u$) do (5) $a = ah$; $R = R \cup \{(a, r)\}$ (6) od (7) while ($x = 0$ and $z = 0$ and $y < u^2$) do (8) if $((eb, r) \in R$ for some r) then (9) $z = y + r$ (10) else (11) if $((b, r) \in R$ for some r) then (12) $z = y + r$ (13) fi (14) else (15) $y = y + u$; $b = bc$ (16) fi (17) od (18) $s = u$; $u = 2u$; $c = c^2$ (19) od </pre> |

compdl 2

2.12.2. Satz *Gilt $d \in \langle g \rangle$ so benötigt Algorithmus 2.12.1 $O(\sqrt{\log_d g})$ Multiplikationen und Speicherplatz für $O(\sqrt{\text{ord}_G g})$ Gruppenelemente. Andernfalls benötigt Algorithmus 2.12.1 $O(\sqrt{\text{ord}_G g})$ Multiplikationen und Speicherplatz für $O(\sqrt{\text{ord}_G g})$ Gruppenelemente.*

2.13 Untergruppen

Sei (G, \cdot) eine Gruppe.

unter 1

2.13.1. Definition Eine Teilmenge U von G heißt Untergruppe von G , wenn U bezüglich der in G definierten Verknüpfung eine Gruppe ist.

unter 2

2.13.2. Definition Seien K, L nicht leere Teilmengen von G .

1. Das Komplexprodukt von K und L ist $KL = \{kl : k \in K, l \in L\}$.
2. Das Komplexinverse von K ist $K^{-1} = \{k^{-1} : k \in K\}$.
3. Für $a \in G$ setzt man außerdem $aK = \{a\}K$ und $Ka = K\{a\}$.

unter 3

2.13.3. Satz Sei U eine nicht leere Teilmenge von G .

1. Genau dann ist U eine Untergruppe von G , wenn $UU^{-1} \subset U$ ist.
2. Ist U endlich, so ist U genau dann eine Untergruppe von G , wenn $UU \subset U$ ist.

Beweis: [7] Satz 2.4.7.

□

unter 4

2.13.4. Satz Der Durchschnitt beliebig vieler Untergruppen von G ist wieder eine Untergruppe von G .

2.14 Gruppenhomomorphismen

Es seien G, H Gruppen. Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus, e das neutrale Element von G und e' das neutrale Element von H .

ghom 1

2.14.1. Satz 1. $\varphi(e)$ ist das neutrale Element von H .

2. $\varphi(a^n) = \varphi(a)^n$ für alle $a \in G$ $n \in \mathbb{Z}$.

Man setzt

$$\begin{aligned} \text{Bild}\varphi &= \{\varphi(x) : x \in G\} \\ \text{Kern}\varphi &= \{x \in G : \varphi(x) = e'\} \end{aligned}$$

ghom 1.1

2.14.2. Satz 1. Das Bild von φ ist eine Untergruppe von H .

2. Der Kern von φ ist eine Untergruppe von G .

ghom 2

2.14.3. Satz *Der Homomorphismus φ ist genau dann injektiv, wenn Kern $\varphi = \{e\}$ ist.*

Die Automorphismen von G bilden eine Gruppe, die sogenannte *Automorphismengruppe* von G . Ist $x \in G$ so ist

$$\varphi_x : G \rightarrow G, a \mapsto x^{-1}ax$$

ein Automorphismus von G . Solche Automorphismen heißen *innere Automorphismen* von G . Zwei Elemente $a, b \in G$ heißen *konjugiert*, wenn $b = x^{-1}ax$ ist für ein $x \in G$. Zwei Untergruppen U, V von G heißen *konjugiert*, wenn $V = x^{-1}Ux$ ist für ein $x \in G$. ghom 3

2.14.4. Satz *Jede Gruppe G ist isomorph zu einer Untergruppe der Permutationsgruppe $S(G)$.*

Beweis: Für $g \in G$ definiere $L(g) \in S(G)$ durch $x \mapsto gx$. Man zeigt, daß $L(G) = \{L(g) : g \in G\}$ eine Untergruppe von $S(G)$ ist und daß die Abbildung $L : G \rightarrow L(G), g \mapsto L(g)$ ein Gruppenisomorphismus ist. □

Es folgt, daß jede endliche Gruppe isomorph ist zu einer Untergruppe der S_n ist.

2.15 Der Satz von Lagrange

Sei G eine Gruppe und U eine Untergruppe von G . lagr 1

2.15.1. Definition *Die Relation R_U wird definiert durch $R_U = \{(x, y) \in G \times G : xy^{-1} \in U\}$.* lagr 2

2.15.2. Satz *Die Relation R_U ist eine mit der Verknüpfung in G rechtsverträgliche Äquivalenzrelation.*

Die Äquivalenzklasse von $x \in G$ ist Ux . Sie heißt *Rechtsnebenklasse* von U in G . Entsprechend definiert man L_U und die *Linksnebenklassen* von U . lagr 3

2.15.3. Satz *1. Die Gruppe G ist disjunkte Vereinigung der Rechtsnebenklassen bzw. Linksnebenklassen von U in G .*

2. Alle Rechtsnebenklassen bzw. Linksnebenklassen haben die gleiche Mächtigkeit wie U . lagr 4

2.15.4. Definition *Die Anzahl der Rechtsnebenklassen von U in G heißt Index von U in G und wird mit $(G : U)$ bezeichnet.*

lagr 5

2.15.5. Satz (Lagrange) Die Anzahl der Rechtsnebenklassen von U in G ist gleich der Anzahl der Linksnebenklassen von U in G und es gilt $|G| = (G : U)|U|$.

lagr 6

2.15.6. Satz Ist G endlich, so folgt $a^{|G|} = 1$ für alle $a \in G$.

lagr 7

2.15.7. Übung Satz von Fermat, Fermattest, Pseudoprimzahl.

lagr 8

2.15.8. Satz Jede Gruppe von Primzahlordnung ist zyklisch.

lagr 9

2.15.9. Satz Ist G zyklisch und ist a ein Erzeuger von G , so ist $\langle a^d \rangle$ für alle Teiler d von $|G|$ die eindeutig bestimmte Untergruppe von G mit Index d . Ist G unendlich, so ist $\langle e \rangle$ die eindeutig bestimmte Untergruppe von G mit Index ∞ .

2.16 Anwendung des Satzes von Lagrange

Sei G eine endliche Gruppe. Ist die Gruppenordnung bekannt, so kann man die Ordnung eines Elementes g von G bestimmen, indem man nach dem kleinsten Teiler x von $|G|$ sucht, für den $g^x = 1$ gilt.

anwlag 0

2.16.1. Übung Entwickle einen Algorithmus, der die Ordnung eines Elementes der S_n berechnet.

Sei nun G abelsch. Dann kann man dieses Verfahren noch beschleunigen. Hierzu benutzt man das folgende Ergebnis.

anwlag 2

2.16.2. Satz Sei $|G| = m_1 m_2 \cdots m_k$ eine Faktorisierung der Ordnung von G in ein Produkt paarweise teilerfremder natürlicher Zahlen m_i , $1 \leq i \leq k$. Dann ist die Ordnung eines Elementes $g \in G$ das Produkt der Ordnungen der Elemente $g^{|G|/m_i}$, $1 \leq i \leq k$.

Beweis: Sei $M_i = |G|/m_i$ und x_i die Ordnung von $g_i = g^{M_i}$, $1 \leq i \leq k$. Dann ist $g_i^{x_i} = 1$ und nach dem Satz von Lagrange ist $g_i^{m_i} = 1$ für $1 \leq i \leq k$. Daher ist x_i ein Teiler von m_i und von x für $1 \leq i \leq k$. Weil die m_i paarweise teilerfremd sind, ist das Produkt der x_i ein Teiler von x . Andererseits gibt es ganze Zahlen a_i , $1 \leq i \leq k$ mit $a_1 M_1 + \dots + a_k M_k = 1$. Daher ist $g^{x_1 \cdots x_k} = g^{(a_1 M_1 + \dots + a_k M_k)(x_1 \cdots x_k)} = 1$. Daraus folgt die Behauptung. \square

Eine weitere Anwendung des Satzes von Lagrange besteht in der schnelleren Berechnung von diskreten Logarithmen. Sei hierzu G zyklisch mit Erzeuger a . Sei außerdem $b \in G$. Es soll ein Exponent x gefunden werden mit $a^x = b$.

Teilerfremde Zerlegung von $|G|$.

DL für Primzahlpotenzen.

Übung: Löse auf diese Weise das Entscheidungsproblem.

2.17 Normalteiler und Faktorgruppen

Sei G eine Gruppe mit Untergruppe U .

normteil 1

2.17.1. Definition Die Untergruppe U heißt Normalteiler, wenn $aU = Ua$ gilt für alle $a \in G$.

normteil 2

2.17.2. Satz Genau dann ist U ein Normalteiler, wenn $aUa^{-1} \subset U$ für alle $a \in G$.

Ist U ein Normalteiler, so für alle $a \in G$ die Rechtsnebenklasse Ua gleich der Linksnebenklasse aU . Diese nennt man daher *Nebenklasse*.

normteil 3

2.17.3. Satz Ist U ein Normalteiler von G , so bilden die Nebenklassen von U in G eine Gruppe bezüglich der Komplexmultiplikation.

normteil 4

2.17.4. Definition Ist U ein Normalteiler von G , so heißt die Gruppe der Nebenklassen von U in G Faktorgruppe von U nach G .

normteil 5

2.17.5. Satz Ist H eine weitere Gruppe und $\varphi : G \rightarrow H$ ein Homomorphismus, so ist $G' = \text{Kern } \varphi$ ein Normalteiler von G und die Abbildung $G/G' \rightarrow H, aG' \mapsto \varphi(a)$ ist ein Isomorphismus.

2.18 Erzeugendensysteme

Sei G eine Gruppe und $S \subset G$.

erzeug 1

2.18.1. Definition 1. Die von S erzeugte Gruppe ist der Durchschnitt aller Untergruppen von G , die S enthalten. Sie wird mit $\langle S \rangle$ bezeichnet.

2. Ist $\langle S \rangle = G$ so heißt S Erzeugendensystem von G .

3. Hat G ein endliches Erzeugendensystem, so heißt G endlich erzeugt.

erzeug 2

2.18.2. Satz Es ist $\langle \emptyset \rangle = \{e\}$. Ist $S \neq \emptyset$, so besteht $\langle S \rangle$ aus allen endlichen potenzprodukten von Elementen aus S .

2.19 Operation von Gruppen auf Mengen

Sei X eine Menge und G eine Gruppe.

oper 1

2.19.1. Definition Wir sagen, daß G auf X operiert, wenn es eine Abbildung $\cdot : G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$ gibt, mit

$$1. (gh) \cdot x = g \cdot (h \cdot x),$$

$$2. ex = x$$

für alle $x \in X$ und $g, h \in G$.

oper 2

2.19.2. Satz In der Situation von Definition 2.19.1 ist $R = \{(x, y) \in X \times X : \text{Es gibt } g \in G \text{ mit } y = gx\}$ eine Äquivalenzrelation.

Die Äquivalenzklassen von R aus Satz 2.19.2 heißen G -Orbits oder G -Bahnen von X . Die Menge X ist disjunkte Vereinigung ihrer G -Orbits.

2.20 Die symmetrische Gruppe S_n

Sei n eine natürliche Zahl.

symm 1

2.20.1. Definition Für r paarweise verschiedene Zahlen a_1, \dots, a_r aus $\{1, \dots, n\}$ bezeichnet (a_1, \dots, a_r) die Permutation der S_n , die a_i auf a_{i+1} abbildet für $i < r$ und a_r auf a_1 . Diese Permutation heißt r -Zykel. 2-Zykeln heißen Transpositionen.

Transpositionen haben die Ordnung 2. Zykel der Länge 1 heißen *trivial*. Die anderen heißen nicht trivial.

symm 2

2.20.2. Satz Die S_{n+1} ist disjunkte Vereinigung der Nebenklassen $(i, n+1)S_n$, $1 \leq i \leq n+1$.

Beweis: Sei $f \in S_{n+1}$. Dann ist $(f(n+1), n+1) \circ f \in S_n$ und $f = (f(n+1), n+1)^2 \circ f$. Also ist S_{n+1} Vereinigung der Nebenklassen $(i, n+1)S_n$, $1 \leq i \leq n+1$. Diese Vereinigung ist disjunkt, weil die Transposition das Bild von $n+1$ bestimmt. \square

symm 3

2.20.3. Korollar Es gilt $|S_{n+1}| = (n+1)S_n$, $|S_n| = n!$.

symm 4

2.20.4. Korollar Jede Permutation ist Produkt von Transpositionen.

symm 5

2.20.5. Übung Der Beweis von Satz 2.20.2 enthält einen Algorithmus zur Zerlegung einer Permutation in ein Produkt von Transpositionen. Man formuliere und analysiere diesen Algorithmus.

symm 6

2.20.6. Definition Zwei Zykel (x_1, \dots, x_r) und (y_1, \dots, y_s) heißen elementfremd, wenn der Durchschnitt der Mengen $\{x_1, \dots, x_r\}$ und $\{y_1, \dots, y_s\}$ leer ist.

symm 7

2.20.7. Satz Jede Permutation $f \neq (1)$ kann als Produkt elementfremder nicht trivialer Zyklen geschrieben werden. Diese Darstellung ist bis auf die Reihenfolge eindeutig.

Beweis: Sei $f \in S_n$. Die Abbildung $(f^j, i) \mapsto f^j(i)$ definiert eine Operation von $\langle f \rangle$ auf $\{1, \dots, n\}$. Also zerfällt $\{1, \dots, n\}$ in paarweise disjunkte $\langle f \rangle$ -Orbits. Ist $f \neq (1)$ so hat wenigstens ein Orbit mehr als ein Element. Für einen solchen nicht trivialen Orbit Y definiere die Permutation f_Y durch $f_Y(i) = f(i)$ falls $i \in Y$ und $f_Y(i) = i$ andernfalls. Dann sind die f_Y elementfremde nicht triviale Zyklen und f ist das Produkt der f_Y .

Sei eine weitere Zerlegung von f gegeben und sei g ein Zyklus, der in dieser Zerlegung vorkommt. Dann gibt es genau einen nicht trivialen $\langle f \rangle$ -Orbit Y , auf dem g nicht die Identität ist. Hierfür gilt $g = f_Y$. \square

Algorithmus.

symm 8

2.20.8. Satz Die Anzahl der Permutationen, in die eine Permutation faktorisiert werden kann, ist stets gerade oder stets ungerade.

Beweis: Für $f \in \mathfrak{S}_n$ setze

$$\varepsilon(f) = \prod_{1 \leq i < j \leq n} \frac{f(i) - f(j)}{i - j}.$$

Durch Induktion sieht man, daß $\varepsilon(f) \in \{pm1\}$. Außerdem verifiziert man, daß $\varepsilon : S_n \rightarrow \{\pm 1\}$ ein Homomorphismus von Gruppen ist und daß $\varepsilon(f) = -1$ ist für jede Transposition f . Hieraus folgt die Behauptung. \square

Permutationen, die in eine gerade Anzahl von Transpositionen faktorisiert werden können, heißen *gerade*. Permutationen, die in eine ungerade Anzahl von Transpositionen faktorisiert werden können, heißen *ungerade*. Die Menge der geraden Permutationen in S_n ist ein Normalteiler der S_n vom Index 2, heißt *alternierende Gruppe vom Grad n* und wird mit A_n bezeichnet.

2.21 Freie Gruppen

Sei X ein Alphabet, also eine nicht leere aber nicht notwendig endliche Menge. Für jedes Symbol $x \in X$ benutze auch das Symbol x^{-1} und setze $X^{-1} = \{x^{-1} : x \in X\}$. Mit $W(X)$ bezeichne die Menge aller Wörter über $X \cup X^{-1}$. Für $x \in X$ setze ferner $(x^{-1})^{-1} = x$. Damit hat jedes Zeichen aus $X \cup X^{-1}$ ein Inverses.

frei 1

2.21.1. Definition Ein Wort w in $W(X)$ heißt *reduziert*, wenn in w kein Zeichen neben seinem Inversen steht. Die Menge der reduzierten Wörter in $W(X)$ wird mit $W_0(X)$ bezeichnet.

Ein Verfahren, daß ein gegebenes Wort $w \in W(X)$ reduziert, funktioniert wie folgt. Man geht w von links nach rechts durch. Wenn man auf das erste Paar xx^{-1} oder $x^{-1}x$ stößt, läßt man dieses Paar weg. Diese Prozedur wird solange wiederholt, bis das Wort reduziert ist. Das Ergebnis bezeichnet man mit $\rho(w)$.

Durch Induktion beweist man folgendes.

frei 2

2.21.2. Lemma 1. $\rho(uxx^{-1}v) = \rho(uv)$ für $u, v \in W(X)$, $x \in X \cup X^{-1}$.

2. $\rho(uv) = \rho(\rho(u)v) = \rho(u\rho(v))$ für $u, v \in W(X)$.

frei 3

2.21.3. Satz Die Relation $R = \{(u, v) : \rho(u) = \rho(v)\}$ ist eine Äquivalenzrelation, die mit der Konkatenation verträglich ist.

Beweis: Offensichtlich ist R eine Äquivalenzrelation. Die Verträglichkeit folgt aus der zweiten Behauptung von Lemma 2.21.2. \square

Bezeichnet man die Äquivalenzklassen mit $[w]$, so ist nun eine Multiplikation $[u][v] = [uv]$ definiert. Zusammen mit dieser Multiplikation ist die Menge $F(X)$ der Äquivalenzklassen eine Gruppe.

frei 3.1

2.21.4. Definition Die Gruppe $F(X)$ heißt die von X frei erzeugte Gruppe.

frei 4

2.21.5. Satz In jeder Äquivalenzklasse aus $F(X)$ gibt es genau ein reduziertes Wort.

Beweis: Es ist stets w äquivalent zu $\rho(w)$. Dies zeigt die Existenz. Für zwei äquivalente reduzierte Wörter u und v gilt $u = \rho(u) = \rho(v) = v$. Dies beweist die Existenz. \square

Sei R eine Teilmenge von $F(X)$. Mit $N(R)$ bezeichne den Durchschnitt aller Normalteiler von $F(X)$ die R enthalten. Eine Gruppe, die isomorph zu $S(X)/N(R)$ ist, heißt durch die erzeugende Menge X und die Relationen R präsentiert.

frei 5

2.21.6. Definition Eine Gruppe H heißt endlich präsentierbar, wenn H durch ein endliches Erzeugendensystem und durch endlich viele Relationen präsentiert werden kann.

Zum Beispiel ist die Gruppe der Bewegungen des regelmäßigen n -Ecks, die sogenannte Diedergruppe D_n endlich präsentierbar als

$$D_n = G(d, s : d^n = e, s^2 = e, (ds)^2 = e).$$

Kapitel 3

Ringe

3.1 Ringbegriff

ringb 1

3.1.1. Definition Ein Ring ist eine algebraische Struktur $(R, +, \cdot)$, wobei

1. $(R, +)$ eine abelsche Gruppe und (R, \cdot) eine Halbgruppe ist und
2. $a(b + c) = ab + ac$ sowie $(b + c)a = ba + ca$ gilt für alle $a, b, c \in R$.

Der Ring R heißt kommutativ, wenn die Halbgruppe (R, \cdot) kommutativ ist.

Sei R ein Ring, $a, b, c, e \in R$. Das neutrale Element bezüglich $+$ sei 0 .

$a \in R$ heißt Nullteiler von R , wenn es ein $b \neq 0$ gibt mit $ab = 0$ oder $ba = 0$.

R heißt nullteilerfrei, wenn R keine Nullteiler außer 0 enthält.

R heißt Integritätsbereich, wenn $R \neq \{0\}$ kommutativ und nullteilerfrei ist.

Genau dann ist R nullteilerfrei, wenn in R die Kürzungsregel gilt.

a heißt Teiler von b , wenn es $c \in R$ gibt mit $b = ca$ oder $b = ac$.

e heißt Einselement von R , wenn $e \neq 0$ und $ae = ea = a$ für alle $a \in R$ ist.

In einem kommutativen Ring mit Einselement e setzt man $a^0 = e$ und es gelten dann der Binomialsatz

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

und

$$a^n - b^n = (a - b) \sum_{i=1}^{n-1} a^i b^{n-i-1}.$$

Sei e ein Einselement von R . a heißt *Einheit* von R , wenn es $b \in R$ gibt mit $ab = ba = e$. Man schreibt $b = a^{-1}$ und nennt b das *Inverse* von a . Einheiten sind nie Nullteiler. Die Menge R^* der Einheiten von R ist eine Gruppe, die *Einheitengruppe* von R .

Ein *Schiefkörper* ist ein Ring mit Eins, in dem jedes von Null verschiedene Element ein Inverses hat. Ein *Körper* ist ein kommutativer Schiefkörper.

Eine Teilmenge T von R , die bezüglich $+$, \cdot ein Ring ist, heißt *Teilring* oder *Unterring* von R . R heißt dann *Oberring* von T .

3.2 Polynomringe

Sei R ein kommutativer Ring mit Einselement 1 und S ein kommutativer Oberring von R mit Einselement 1. Sei $z \in S$.

Ein Element p von S heißt *Polynom* in z über R falls p eine Darstellung poly 1

$$p = p_0 z^n + p_1 z^{n-1} + \dots + p_n \quad (3.1)$$

hat mit $p_i \in R$, $0 \leq i \leq n$. Diese Darstellung ist i.a. nicht eindeutig. Die Menge aller Polynome in z über R wird mit $R[z]$ bezeichnet.

x heißt *Unbestimmte* über R oder *transzendent* über R , falls x zu einem kommutativen Oberring von R gehört und aus $p_0 x^n + p_1 x^{n-1} + \dots + p_n = 0$ mit $n \geq 0$ und $p_i \in R$, $0 \leq i \leq n$ folgt, daß $p_i = 0$, $0 \leq i \leq n$. Ist z transzendent über R , so ist die Darstellung (3.1) eines Polynoms $p \neq 0$ eindeutig, wenn man noch fordert, daß $p_0 \neq 0$ ist. Dabei heißt dann n der *Grad* von p , kurz $n = \deg p$, p_i die *Koeffizienten* von p , $0 \leq i \leq n$, p_0 der *höchste Koeffizient* von p , kurz $p_0 = H(p)$, und p_n ist das *konstante Glied* von p . Es wird auch noch vereinbart, daß $\deg 0 = -\infty$ ist. poly 1

3.2.1. Satz *Es gibt mindestens eine Unbestimmte über R .*

Insbesondere können wir also induktiv Polynome in mehreren Unbestimmten konstruieren. Sei $R[x_1, \dots, x_{n-1}]$ ein Erweiterungsring von R mit $n - 1$ Unbestimmten. Dann ist $R[x_1, \dots, x_n] := (R[x_1, \dots, x_{n-1}])[x_n]$ ein Ring in n Unbestimmten.

Polynome aus dem Ring $R[x_1, \dots, x_n]$ heißen *univariat*, falls $n = 1$, sonst *multivariat*. Ein Polynom $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ sieht dann so aus:

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n=0}^m a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

In dieser Darstellung heißen die $a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$ *Monome*, die a_{i_1, \dots, i_n} heißen *Koeffizienten*, die $x_1^{i_1} \cdots x_n^{i_n}$ heißen *Terme*, $\max\{\sum_{j=1}^n i_j \mid a_{i_1, \dots, i_n} \neq 0\}$ heißt *totaler Grad* von f , kurz $\deg f$.

Betrachtet man f als Polynom über $(R[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n])[x_i]$, $1 \leq i \leq n$, also als Polynom in einer Unbestimmten mit Koeffizienten aus $R[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$, so kann man dieses Polynom auch als $f_{i0} \cdot x_i^n + \dots + f_{in} \cdot x_i^0$ schreiben; dann heißt n *Grad von f in x_i* , kurz $n = \deg_{x_i} f$.

3.2.2. Beispiel Sei $f = 3x_1^4 x_2^2 x_3 + 5x_1^2 x_2^5 x_3^2 + 5x_2^5 x_3^7$. Dann ist $\deg f = 12$, $\deg_{x_1} f = 4$, $\deg_{x_2} f = 5$, $\deg_{x_3} f = 7$.

Sei nun S ein Ring mit $R \subseteq S$, $c_1, \dots, c_n \in S$. Dann ist die folgende Abbildung ein Homomorphismus zwischen Ringen:

$$\begin{aligned} \varphi_{c_1, \dots, c_n} : R[x_1, \dots, x_n] &\longrightarrow S \\ f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n=0}^m a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} &\longmapsto \sum_{i_1, \dots, i_n=0}^m a_{i_1, \dots, i_n} c_1^{i_1} \cdots c_n^{i_n}. \end{aligned}$$

$\varphi_{c_1, \dots, c_n}$ heißt *Spezialisierung von f* . Für $\varphi_{c_1, \dots, c_n}(f)$ schreibt man auch $f(c_1, \dots, c_n)$. Falls $\varphi_{c_1, \dots, c_n}(f) = 0$, so heißt $\varphi_{c_1, \dots, c_n}$ Nullstelle von f , man nennt auch (c_1, \dots, c_n) Nullstelle von f .

3.3 Unterringe, Ideale, Restklassenringe

Sei R ein kommutativer Ring mit Einselement 1.

Ein *Teiltring* oder *Unterring* von R ist eine Teilmenge von R , die bezüglich der in R definierten Verknüpfungen ein Ring ist. Entsprechend sind Teilkörper definiert.

Sei U ein Unterring von R . Für $a, b \in R$ heißt a kongruent zu b modulo U (Bezeichnung: $a \equiv b \pmod{U}$), wenn $b - a \in U$ ist. Kongruenz modulo U ist eine Äquivalenzrelation. Die Äquivalenzklassen heißen *Kongruenzklassen* modulo U . Diese ist genau dann mit den Operationen in R verträglich, wenn U ein Ideal in folgendem Sinne ist.

ideal 1

3.3.1. Definition 1. Eine Teilmenge I von R heißt *Ideal von R* , wenn I ein Unterring von R ist, der $aI \subset I$ für alle $a \in R$ erfüllt.

2. Ist I ein Ideal von R , so heißt die Menge der Kongruenzklassen zusammen mit der vertreterweise definierten Multiplikation und Addition *Restklassenring von R modulo I* .

3.3.2. Beispiel Die Ideale von \mathbb{Z} sind genau die Teilmengen der Form $a\mathbb{Z}$ für ein $a \in \mathbb{Z}_{\geq 0}$: Klar ist, daß diese Mengen Ideale sind. Sei nun $\{0\} \neq I \subseteq \mathbb{Z}$ ein Ideal, a die kleinste positive Zahl in I , $b \in I$. Dann existieren q, r mit $b = aq + r$, $0 \leq r < a$. Da ein Ideal ein Unterring ist, ist also $r \in I$, also $r = 0$.

Also sind die Restklassenringe von \mathbb{Z} von der Form $\mathbb{Z}/m\mathbb{Z}$ mit vertreterweise definierten Operationen.

ideal 2

3.3.3. Satz *Der Durchschnitt beliebig vieler Ideale von R ist wieder ein Ideal von R .*

ideal 3

3.3.4. Definition 1. *Ist S eine Teilmenge von R , dann heißt der Durchschnitt I aller Ideale, die S enthalten, das von S erzeugte Ideal, kurz $\langle S \rangle_R$ bzw. $\langle S \rangle$. Die Menge S heißt R -Erzeugendensystem von I .*

2. *Wird ein Ideal von R von einer endlichen Teilmenge von R erzeugt, so heißt es endlich erzeugt.*

3. *Wird ein Ideal I von R von einer einelementigen Menge $\{r\}$ erzeugt, so wird I Hauptideal genannt und r heißt Erzeuger von I . Man schreibt dann $I = \langle r \rangle$.*

ideal 4

3.3.5. Satz *Sei S eine Teilmenge des kommutativen Rings R . Dann ist*

$$\left\{ \sum_{i=1}^n r_i s_i : n \in \mathbb{N}, r_i \in R, s_i \in S, 1 \leq i \leq n \right\}$$

das von S erzeugte Ideal. Für $a \in R$ ist aR das von a erzeugte Hauptideal.

Beweis: Offensichtlich ist $\{\sum_{i=1}^n r_i s_i : n \in \mathbb{N}, r_i \in R, s_i \in S, 1 \leq i \leq n\}$ in dem von S erzeugten Ideal enthalten und diese Menge enthält S , da insbesondere $1 \cdot s = s$ für alle $s \in S$ in dieser Menge enthalten ist. Außerdem ist diese Menge ein Ideal. Dies beweist die Behauptung. \square

3.3.6. Beispiel Betrachte die folgenden Gleichungen mit Koeffizienten aus \mathbb{Z} .

$$\begin{aligned} f(x_1, x_2, x_3) &:= x_1^2 x_2^3 + x_1 x_2 + x_2 x_3 = 0 \\ g(x_1, x_2, x_3) &:= x_1 x_2^4 + 3x_1 x_2 x_3^2 + x_1 x_2^2 = 0 \end{aligned}$$

Die Lösung dieses Gleichungssystems sind die Nullstellen des Polynoms f die zugleich Nullstellen von g sind.

Dieses Problem ist in einem geeigneten Ring leicht zu lösen: Es gilt nämlich: Jede Nullstelle von f und g ist Nullstelle von allen Polynomen aus $\langle \{f, g\} \rangle$. Damit ist in $R[x_1, x_2, x_3]/\langle \{f, g\} \rangle$ 0 die einzige Nullstelle von f und g . Will man alle Lösungen in \mathbb{R} haben, nutzt dies jedoch noch nicht besonders viel.

Wichtige algorithmische Probleme im Zusammenhang mit Idealen sind die folgenden Fragen:

- Ist ein Ideal ein Hauptideal? bzw. Wie viele Elemente braucht man um das Ideal zu erzeugen?

- Gehört ein Element zu einem Ideal?
- Erzeugen zwei Mengen das gleiche Ideal?

Das erste Problem ist wichtig, da die Schwierigkeit vieler Berechnungen mit Idealen von der Größe des Erzeugendensystems abhängt, für Hauptideale sind die meisten Rechnungen besonders einfach. Wenn wir z.B. im obigen Problem erkennen, daß f und g ein Hauptideal erzeugen und den Erzeuger finden, dann brauchen wir nur noch eine Gleichung zu lösen.

Die zweite Fragestellung kann in unserem Beispiel von Bedeutung sein, wenn wir schon die Nullstellen einiger Polynome kennen. Dann können wir "leicht" überprüfen, ob auch f und g eine dieser Nullstellen als Nullstelle haben.

Die dritte Frage läßt sich leicht beantworten, wenn man die zweite Frage beantworten kann: Man teste, ob alle Elemente der ersten Menge zum von der zweiten Menge erzeugten Ideal gehören und umgekehrt.

ideal 5

3.3.7. Definition Seien I und J Ideale von R .

1. Die Summe von $I + J$ ist die Komplexsumme von I und J .
2. Das Produkt von I und J ist $IJ = \{\sum_{i=1}^n a_i b_i : n \in \mathbb{N}, a_i \in I, b_i \in J, 1 \leq i, j \leq n\}$.

ideal 6

3.3.8. Satz Summe und Produkt zweier Ideale sind wieder Ideale.

Ideale quadratischer Ordnungen.

3.4 Homomorphiesatz

Sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus. Der *Kern* von φ ist die Menge aller Elemente aus R , die auf 0 abgebildet werden.

homo 1

3.4.1. Satz Der Kern von φ ist ein Ideal von R und die Abbildung, die die Restklasse eines Elementes a mod Kern φ auf $\varphi(a)$ abbildet ist ein Isomorphismus von $R/\text{Kern}\varphi$ nach $\varphi(R)$.

3.5 Quotientenkörper

Quotientenkörper

Primkörper

3.6 Nullstellen und Differentiation von Polynomen

Division mit Rest durch Polynome deren höchster Koeffizient eine Einheit ist.

Nullstelle

a Nullstelle genau dann wenn $x - a$ Teiler.

Verallgemeinerung auf mehrere verschiedene Nullstellen, wenn der Ring nullteilerfrei ist.

Polynome vom Grad n über Integritätsbereichen haben höchstens n verschiedene Nullstellen.

k -fache Nullstelle

Ableitung, Produktregel

mehrfache Nullstellen sind gemeinsame Nullstellen von f und f' .

Lagrange Interpolationsformel.

Newton Interpolation:

Sei $(a_i)_{i \geq 0}$ eine Folge von Ringelementen. Wir konstruieren induktiv Polynome

$$p_k(x) = c_0 + c_1(x - a_0) + c_2(x - a_0)(x - a_1) + \dots + c_k(x - a_0) \cdots (x - a_k)$$

mit

$$p_k(a_i) = b_i, \quad 0 \leq i \leq k.$$

Hierzu geht man folgendermaßen vor.

3.7 Euklidische Ringe

R Integritätsbereich.

R *euklidisch* wenn es eine Funktion $h : R - \{0\} \rightarrow \mathbb{N} \cup \{0\}$ gibt mit folgender Eigenschaft. Für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit

$$a = qb + r, \quad r = 0 \text{ oder } h(r) < h(b).$$

Beispiele

\mathbb{Z} , $K[x]$, $\mathbb{Z}[i]$.

Beweis der letzteren Behauptung. Setze $h(x + iy) = x^2 + y^2$. Die Behauptung wird geometrisch bewiesen. Seien $a, b \in \mathbb{Z}[i]$. Diese Zahlen werden als Vektoren in der Gausschen Ebene aufgefaßt. Mit a^* bezeichne die Projektion von a auf das orthogonale Komplement

von b . Dann gilt $a = a^* + \mu b$ mit $\mu \in \mathbb{R}$. Ist $|\mu| > 1$ so kann man $q = \lfloor \mu \rfloor$ setzen. Andernfalls muß b um 90 Grad gedreht werden.

Problem: Finde euklidische Ringe und beweise Nichteuklidizität.

Jeder euklidische Ring ist Hauptidealring.

3.8 Teilbarkeit

R kommutativer Ring mit 1.

assozierte Elemente, Assoziiertheit ist Äquivalenzrelation.

Teilbarkeitsregeln.

a teilt b genau dann wenn bR in aR enthalten ist.

ggT, Eindeutigkeit bis auf Assoziiertheit

Existenz und Darstellbarkeit des ggT in Hauptidealringen

3.9 ZPE-Ringe

R Integritätsbereich mit 1.

Triviale Teiler von $a \in R$ sind die Einheiten und die zu a assoziierten Elemente.

$a \in R$ heißt *irreduzibel*, wenn a von Null verschiedene Nichteinheit ist, die nur triviale Teiler hat.

Beispiel: Irreduzible Polynome über F_2 vom Grad ≤ 3 . Irreduzible Elemente in $\mathbb{Z}[i]$

$p \in R$ heißt *Primelement*, wenn p mit jedem Produkt ab , $a, b \in R$, einen der Faktoren a oder b teilt.

Beispiel: in $\mathbb{Z}[\sqrt{-3}]$ ist $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

Assoziierte von Primelementen und irreduziblen Elementen sind Primelemente bzw. irreduzible Elemente.

Satz. Jedes Primelement ist irreduzibel. Beweis: $p = ab$. p teilt a . $a = up$. $p = upb$. $ub = 1$. b Einheit.

Satz: Ist R Hauptidealring, so ist jedes irreduzible Element ein Primelement.

Beweis: Sei p irreduzibel und teile p das Produkt ab . Angenommen, p teilt nicht a . Dann kann man $1 = xa + yp$ schreiben, also $b = xab + ypb$ woraus folgt, daß p ein Teiler von b ist.

R heißt ZPE-Ring, wenn jede von Null verschiedene Nichteinheit von R ein Produkt irreduzibler Elemente ist und die in diesem Produkt vorkommenden irreduziblen Elemente bis auf Assoziiertheit eindeutig bestimmt sind.

Bewertungsfunktion.

Satz: Folgende Aussagen sind äquivalent.

1. R ist ZPE-Ring.
2. Jede von Null verschiedene Nichteinheit ist Produkt irreduzibler Elemente und jedes irreduzible Element ist Primelement.
3. Jede von Null verschiedene Nichteinheit ist Produkt von Primelementen.

Beweis:

Sei R ein ZPE-Ring. Dann ist nach definition jede von Null verschiedene Nichteinheit ein Produkt irreduzibler Elemente. Sei p irreduzibel, p ein Teiler von ab . Dann kommt p in der Zerlegung von ab vor und wegen der Eindeutigkeit erhält man diese Zerlegung aus der Zerlegung von a und b .

Die zweite Beh. Impliziert die dritte.

Gelte die dritte Behauptung. Dann ist nur die Eindeutigkeit der Zerlegung zu beweisen und das macht man wie in \mathbf{Z} mit Induktion.

Satz: Ist R ein Hauptidealring, so ist R ein ZPE-Ring.

Beweis: Angenommen, R ist nicht ZPE-Ring. Ich zeige, daß es eine Folge a_1, a_2, \dots von Null verschiedener Nichteinheiten gibt, die alle nicht als Produkt von Primelementen geschrieben werden können und in der a_i den Nachfolger a_{i+1} echt teilt. Dies geht so. Für a_1 wähle eine von Null verschiedene Nichteinheit, die nicht Produkt von Primelementen ist. Angenommen, a_i ist konstruiert. Dann ist a_i nicht irreduzibel und besitzt einen nicht trivialen Teiler a_{i+1} , der nicht als Produkt von Primelementen geschrieben werden kann.

Sei I das Ideal, das von den a_i erzeugt wird. Sei a ein Erzeuger von I . Dann kann $a = r_1 a_1 + \dots + r_k a_k$ geschrieben werden. a teilt a_{k+1} und wird von a_k geteilt. Also a_k teilt a_{k+1} und umgekehrt. Widerspruch.

3.10 Irreduzibilitätstests

Sei R ein ZPE-Ring. $f(x) = a_0 + a_1x + \dots + a_nx^n$

Satz von Eisenstein: Wenn es ein Primelement p in R gibt, so daß alle Koeffizienten außer dem letzten durch p teilbar sind und der erste nicht durch p^2 , dann ist f irreduzibel. Beweis: Sei $f = gh$. O.B.d.A. ist das absolute Glied von g nicht durch p teilbar aber das absolute Glied von h wohl. Außerdem ist g nicht durch p teilbar. Also gibt es einen ersten Koeffizienten, der nicht durch p teilbar ist. Schreibt man die Formel für a_i auf, so folgt aus der Teilbarkeit von a_i durch p daß b_i wohl durch p teilbar ist.

Anwendung: $x^m - p$, p Primzahl in $\mathbb{Z}[x]$. Kreisteilungspolynome $x^{p-1} + x^{p-2} + \dots + 1$. Wende die Transformation $x \mapsto x + 1$ an.

3.11 Primideale, maximale Ideale

Sei R ein kommutativer Ring mit 1.

Ein Ideal P von R heißt *Primideal*, wenn für $a, b \in R$ mit $ab \in P$ eines der Elemente a oder b zu P gehört.

Satz: Genau dann ist P ein Primideal, wenn R/P ein Integritätsbereich ist.

Beispiele: (x) , Beweis: $f, g \in \mathbb{Z}[x]$, fg durch x teilbar, dann ist das absolute Glied des Produkts 0 und daher ist auch das absolute Glied eines Faktors 0.

Satz: Ist R Integritätsbereich mit 1. Ein Hauptideal von R ist genau dann ein Primideal, wenn es von einem Primelement erzeugt wird. Beweis. Angenommen, (p) ist ein Primideal. Sei $ab \in (p)$. Dann teilt p das Produkt ab . Also teilt p einen Faktor, etwa a . Also ist a in (p) enthalten. Umgekehrt: ...

Satz: In einem Hauptidealring sind die von $\{0\}$ verschiedenen Primideale genau die von den Primelementen erzeugten Ideale. Beweis: p Primelement. $ab \in pR$. Dann p teilt ab . Dann z.B. p teilt a . Dann $a \in pR$.

Ein Ideal M von R heißt *maximal*, wenn es ungleich R ist und in keinem anderen Ideal ungleich R echt enthalten ist.

primid 1

3.11.1. Satz Genau dann ist ein Ideal M maximal, wenn R/M ein Körper ist.

Satz: Maximale Ideale sind stets Primideale. Beweis: M maximal, $ab \in M$, $a \notin M$. Dann $R = (a, m)$. Also $1 = xa + m$. Also $b = xab + mb \in M$.

Satz: In einem Hauptidealring sind die von $\{0\}$ verschiedenen Primideale maximal. Beweis: pR echt enthalten in bR . Dann b echter Teiler von p , also $b = 1$.

3.12 Algorithmen für Polynome über endlichen Primkörpern

Sei p eine Primzahl und $f \in F_p[x]$. Ziel ist es, f in seine irreduziblen Faktoren zu zerlegen.

Satz: Ist K ein Körper und $g \in K[x]$. Wenn g vom Quadrat eines Polynoms aus $K[x]$ geteilt, dann gehört $\gcd(g, g')$ nicht zu K .

Beweis: Sei $g = p^2h$. Dann ist $g' = p(2p'h + ph')$.

Falls $d(x) = \gcd(f, f')$ ein echter Teiler von f ist, hat man die Zerlegung $f = (f/d)d$ gefunden. Man kann Faktorverfeinerung benutzen und f in ein Produkt teilerfremder Polynome zerlegen.

Satz: Ist $g \in F_p[x]$, so ist $g(x)^p = g(x^p)$.

Beweis: Die Binomialkoeffizienten $\binom{p}{i}$ sind für $1 \leq i \leq p-1$ durch p teilbar. Man beweist damit, daß $(u+v)^p = u^p + v^p$ ist. Dann wendet man Induktion an.

Satz: Ist $d(x) = 0$ so ist $f(x) = v(x^p)$ für ein v .

Beweis: Nur die Koeffizienten x^i , wo i ein Vielfaches von p ist, können ungleich Null sein.

Ist also $d(x) = 0$, so schreibe $f(x) = v(x)^p$.

Durch wiederholte Anwendung der obigen Verfahren kann man dafür sorgen, daß f ein Potenzprodukt quadratfreier Polynome wird.

Man kann jetzt also annehmen, daß f quadratfrei ist.

3.13 Lemma von Gauß

R sei ZPE-Ring

Inhalt eines Polynoms

primitive Polynome

Satz: $\text{Inhalt}(fg)$ assoziiert zu $\text{Inhalt}(f)\text{Inhalt}(g)$. Beweis:

Literaturverzeichnis

- [1] Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1974.
- [2] J. Buchmann, H.C. Williams, *Algorithms for quadratic forms and quadratic fields*, Manuskript 1995.
- [3] Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, Heidelberg, New York 1993.
- [4] W. Diffie, M. Hellman
- [5] George Havas,
- [6] Donald E. Knuth, *The art of computer programming*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1981.
- [7] Otto Körner, *Algebra*, Akademische Verlagsgesellschaft, Frankfurt am Main 1974.
- [8] K. Meyberg, *Algebra Teil 1*, Carl Hanser verlag, München, Wien 1980.
- [9] Hans Riesel, *Prime numbers and Computer Methods for Factorization*, Birkhäuser, Boston, Basel, Stuttgart 1985.
- [10] A. Schönhage,
- [11] babystep-giantstep
- [12] B.L. van der Waerden, *Algebra I*, Springer-Verlag, Berlin, Heidelberg, New York 1971.