Elementare Zahlentheorie

Zusammenfassung

WS 2013/2014

(Dr. Antonella Perucca)

Julian Palme

(Stand: 18. März 2014)

Dies ist eine Zusammenfassung der Vorlesung 'Elementare Zahlentheorie', gelesen von Frau Dr. Antonella Perucca im Wintersemester 2013/2014 an der Universität Regensburg. Dieses Dokument ist KEIN offizielles Skript und wurde gesetzt in LaTeX von Julian Palme.

Inhaltsverzeichnis

§ 1 Die Sprache der Mathematik 1

I Aussagenlogik 1
1.1 Aussage (Def) . . . 1
1.2 logisch äquivalent (Def) . . . 1

II Konstruktionen mit Aussagen 1
2.1 Negation . . . 1
2.2 Konjunktion . . . 2
2.3 Adjunktion . . . 2

III Implikationen 3
3.1 Implikationen . . . 3
3.2 Äquivalenz . . . 3

IV Prädikate 4
4.1 Prädikat (Def) . . . 4
4.2 Quantoren . . . 4
4.3 Zweiwertige Prädikate . . . 4

V Sätze usw. 4
5.1 Satz (Def) . . . 4
5.2 Typische Bweisstrukturen . . . 4
5.2.1 Direkter Beweis . . . 5
5.2.2 Kontraposition . . . 5
5.2.3 Widerspruchsbeweis . . . 5
5.3 Kompliziertere Sätze . . . 5
5.4 Beispiele und Gegenbeispiele . . . 6
5.4.1 Beispiel (Def) . . . 6
5.4.2 Gegenbeispiel (Def) . . . 6
5.5 Lemma, Korollar, Präposition, Vermutung . . . 6
5.5.1 Lemma (Def) . . . 6
5.5.2 Korollar (Def) . . . 6
5.5.3 Präposition (Def) . . . 6
5.5.4 Vermutung (Def) . . . 6

§ 2 Naive Mengenlehre (Teil I) 7

I Mengen und Teilmengen 7
1.1 Menge (Def) . . . 7
1.2 gleiche Mengen (Def) . . . 7
1.3 Eigenschaften der Gleichheit (Prop) . . . 7
1.4 Teilmenge (Def) . . . 7
1.5 Eigenschaften der Inklusion (Prop) . . . 7
1.6 Spezielle Mengen . . . 8
1.7 Allgemeine Schreibweise . . . 8

II Operationen zwischen Mengen **8**
2.1 Durchschnitt (Def) . . . 8
2.2 disjunkt (Def) . . . 8
2.3 Eigenschaften Durchschnitt (Prop) . . . 9
2.4 Durchschnitt einer Familie von Mengen (Def) . . . 9
2.5 paarweise Disjunkt (Def) . . . 9
2.6 Vereinigung (Def) . . . 9
2.7 Eigenschaften Vereinigung (Prop) . . . 9
2.8 Vereinigung einer Familie von Mengen (Def) . . . 10
2.9 Differenz (Def) . . . 10
2.10 symmetrsiche Differenz (Def) . . . 10
2.11 Ditributivität zwischen Durchschnitt und Vereinigung (Prop) . . . 11
2.12 Eigenschaften Differenz, Durchschnitt, Vereinigung (Prop) . . . 11

III Mächtigkeit für endliche Mengen **11**

§ 3 Binäre Relationen **11**

I Relationen **11**
1.1 binäre Relation (Def) . . . 11
1.2 Eigenschaften für eine Relation auf einer Menge . . . 12
1.3 Halordnung, Striktordnung (Def) . . . 12

II Äquivalenzrelationen **12**
2.1 Äquivalenzrelation (Def) . . . 12
2.2 Äquivalenzklasse, Repräsentant, Quotientenmenge (Def) . . . 13
2.3 Eigenschaften Äquivalenzrelation . . . 13
2.4 Beziehung zu Partitionen (Satz) . . . 13

§ 4 Induktion **13**

I Beweisprinzip der Vollständigen Induktion **13**

§ 5 Gruppen, Ringe und Körper **14**

I Verknüpfungen **14**
1.1 Verknüpfung (Def) . . . 14
1.2 Zusätzliche Eigenschaften Verknüpfung . . . 15
1.3 Verknüpfung (Prop) . . . 15
1.4 Wichtige algebraische Strukturen . . . 15

II Gruppen **15**
2.1 Eigenschaften Gruppen . . . 15
2.2 Ordnung einer Gruppe (Def) . . . 16

§ 6 Die natürlichen Zahlen **16**

I Axiome der natürlichen Zahlen **16**
1.1 Begründung der Axiome . . . 16

1.2 Die Peano Axiome . . . 16
1.3 Surjektivität der Nachfolgerfunktion (Satz) . . . 16
1.4 Eindeutigkeit von $\mathbb{N}$ . . . 16

II Rekursive Folgen 17
2.1 Rekursionssatz nach Dedekind (Satz) . . . 17
2.2 Folge (Def) . . . 17
2.3 rekursive Folge (Def) . . . 17
2.4 k-rekursive Folgen (Def) . . . 17
2.5 k-Rekursionssatz (Satz) . . . 17

III Addition natürlicher Zahlen 18
3.1 Addition (Def) . . . 18
3.2 Iterierte Nachfolgerfunktion . . . 18
3.3 Eigenschaften Addition (Satz) . . . 18
3.4 Addition (Lemma) . . . 18
3.5 Kürzungsregel (Satz) . . . 18

IV Multiplikation natürlicher Zahlen 18
4.1 Multiplikation (Def) . . . 18
4.2 Eigenschaften Multiplikation . . . 19
4.3 Kürzungsregel (Satz) . . . 19
4.4 Kürzungsregel (Kor) . . . 19
4.5 Weitere Eigeschaften Summe und Produkt . . . 19

V Die Anordnung der natürlichen Zahlen 19
5.1 Relation $\geq$ (Satz) . . . 19
5.2 Relation $>$ (Satz) . . . 19
5.3 Monotonie (Satz) . . . 20

VI Potenzen 20
6.1 Potenz (Def) . . . 20
6.2 Rechenregeln der Potenz (Satz) . . . 20
6.3 Kuriosität . . . 20

VII Weitere Operationen 21
7.1 Subtraktion . . . 21
7.2 Subtraktion (Def) . . . 21
7.3 Division mit Rest . . . 21

§ 7 Polynome (Teil I) 22

I Polynome 22
1.1 Polynom (Def) . . . 22
1.2 Grad, Leitkoeffizient (Def) . . . 22

II Addition 23

III Multiplikation 23

IV Ringe der Polynome 24

§ 8 Die ganzen Zahlen **24**

I Definition für $\mathbb{Z}$ **24**
1.1 Definition der ganzen Zahlen (Def) . . . 24

II Die positiven ganzen Zahlen **25**
2.1 Äquivalenzklassen (Prop) . . . 25
2.2 Repräsentant (Satz) . . . 25
2.3 Einbettung $\mathbb{N}$ (Kor) . . . 25

III Verknüpfungen auf $\mathbb{Z}$ **25**
3.1 Addition auf $\mathbb{Z}$ (Def) . . . 25
3.2 $\mathbb{Z}$ mit Addition ist abelsche Gruppe (Satz) . . . 26
3.3 Wichtige Eigenschaften von Gruppen . . . 26
3.4 Subtraktion auf $\mathbb{Z}$ (Def) . . . 26
3.5 Multiplikation auf $\mathbb{Z}$ (Def) . . . 26
3.6 Multiplikation auf$\mathbb{Z}$ (Satz) . . . 26
3.7 Ring $\mathbb{Z}$ (Satz) . . . 26

IV Die Anordnung der ganzen Zahlen **27**
4.1 Relation bzgl. $\mathbb{Z}$und $\mathbb{N}$ (Prop) . . . 27
4.2 Eigenschaften Anordnung (Satz) . . . 27
4.3 Monotonie (Satz) . . . 27

V Die Betragsfunktion **28**
5.1 Betrag (Def) . . . 28
5.2 Betragsregeln (Satz) . . . 28

VI Potenzen **28**
6.1 Rechenregeln der Potenz (Satz) . . . 28

VII Schranken **29**
7.1 Minimum, Maximum, Schranke, beschränkt (Def) . . . 29
7.2 endliche Teilmenge – Genau ein Minimum und ein Maximum (Satz) . . . 29
7.3 untere Schranke/obere Schranke – Minimum/Maximum (Satz) . . . 29

§ 9 Teilbarkeit in $\mathbb{Z}$ **29**

I Division mit Rest in $\mathbb{Z}$ **29**
1.1 Division mit Rest (Satz) . . . 29

II Definition der Teilbarkeit **29**
2.1 teilbar (Def) . . . 29
2.2 äquivalente Aussagen (Prop) . . . 29

III Eigenschaften der Teilbarkeitsrelation **30**
3.1 Eigenschaften der Teilbarkeitsrelation (Satz) . . . 30
3.2 „fast“ antisymmetrische Teilbarkeitsrelation (Satz) . . . 30

IV Weitere Eigenschaften **30**
4.1 Minus, Betrag (Prop) . . . 30
4.2 Produkt, Kürzen (Prop) . . . 30
4.3 Linearkombinationen (Prop) . . . 31

4.4 Beschränkung der Teiler (Prop) . . . 31

V Teilermengen 31
5.1 Teilermenge (Prop) . . . 31
5.2 triviale und echte Teiler . . . 31

VI Linearkombinationen von ganzen Zahlen 32
6.1 Linearkombinationen (Def) . . . 32
6.2 Abgeschlossenheit (Prop) . . . 32
6.3 Kombinationen (Def) . . . 33

§ 10 ggT und kgV 33

I Drei äquivalente Definitionen des ggT 33
1.1 ggT (Def) . . . 33

II Eigenschaften ggT 33

III Teilerfremde Zahlen 34
3.1 Teilerfremde Zahlen (Prop) . . . 34

IV Der ggT mehrerer ganzer Zahlen 34
4.1 ggT meherer ganzer Zahlen (Def) . . . 34

V Eigenschaften ggT mehrerer ganzer Zahlen 35

VI Der ggT als Verknüpfung 35
6.1 Rekursive Definition des ggT . . . 36

VII Das kleinste gemeinsame (streng positive) Vielfache 36
7.1 kgV (Def) . . . 36

VIII Eigenschaften kgV 36

IX Das kgV mehrerer ganzer Zahlen 36
9.1 kgV meherer ganzer Zahlen (Def) . . . 36

X Eigenschaften kgV mehrerer ganzer Zahlen 37

XI Das kgV als Verknüpfung 37
11.1 Rekursive Definition des kgV . . . 37

XII Beziehung zwischen ggT und kgV 37
12.1 Teilbarkeit (Lemma) . . . 38

§ 11 Euklidischer Algorithmus und Lineare Diophantische Gleichungen 38

I Der euklidische Algorithmus 38
1.1 Berechnung des ggT . . . 38
1.2 Euklidischer Algorithmus für den ggT (Satz) . . . 38
1.3 ggT (Lemma) . . . 39
1.4 Berechnung des ggT als Kombination von Zahlen . . . 39
1.5 Euklidischer Algorithmus (Bsp) . . . 39

II Lineare diophantische Gleichungen **39**
2.1 Lineare diophantische Gleichung (Def) . . . 39
2.2 Lösungsmenge . . . 40
2.3 Verknüpfungen auf $\mathbb{Z}^n$ . . . 40
2.4 Äquivalente Gleichungen (Lemma) . . . 40
2.5 Superpositionsprinzip für homogene Gleichungen (Lemma) . . . 40
2.6 Lösbarkeitskriterium für inhomogene Gleichungen (Lemma) . . . 40
2.7 Struktur der Lösungsmenge für inhomogene Gleichungen (Satz) . . . 41

III Lineare diophantische Gleichungen mit einer oder zwei Variablen **41**
3.1 Eine Variable, $ax = c$ . . . 41
3.1.1 Homogen . . . 41
3.1.2 Inhomogen . . . 41
3.2 Spezialfall Homogen, $ax + by = 0$ . . . 41
3.3 Homogen, $ax + by = 0$ (Satz) . . . 41
3.3.1 Spezialfälle . . . 41
3.3.2 Teilerfremde Zahlen . . . 42
3.4 Inhomogen, $ax + by = c$ . . . 42
3.4.1 Lösbarkeitskriterium . . . 42
3.4.2 Lösungsmenge . . . 42
3.4.3 Eine spezielle Lösung . . . 42

IV Die Theorie der linearen diophantischen Gleichungen **43**
4.1 Algebra . . . 43
4.2 Geometrie . . . 43
4.3 Analysis . . . 43
4.4 Lineare Algebra . . . 44
4.5 Algorithmen . . . 44

§ 12 Die g-adische Darstellung natürlicher Zahlen **44**
0.6 System mit Grundzahl in $\mathbb{N}$ (Satz) . . . 45
0.7 Quersumme, alternierende Quersumme (Def) . . . 45
0.8 Quersumme äquivalent modulo (Satz) . . . 45

§ 13 Primzahlen und der Fudamentalsatz der Arithmetik **46**

I Definitionen **46**
1.1 Primzahl (Def) . . . 46
1.2 Unzerlegbarkeitseigenschaft von Primzahlen (Def) . . . 46

II Primeigenschaft **47**
2.1 Primeigenschaft (Lemma) . . . 47
2.2 Primzahl (Def) . . . 47
2.3 Produkt (Satz) . . . 47
2.4 Potenz (Kor) . . . 47
2.5 Zwei Primzahlen (Kor) . . . 47
2.6 Produkt von Primzahlen (Kor) . . . 47

III Weitere Eigenschaften **48**
3.1 Der kleinste Teiler größer Eins (Satz) . . . 48
3.2 Primteiler (Kor) . . . 48

3.3 Euklid (Satz) . . . 48

IV Geneauere Eigenschaften der Primzahlen 48
4.1 Bertrandsches Postulat (Satz) . . . 48
4.2 Primzahlen in arithmetischen Folgen . . . 49
4.3 unendlich viele Primzahlen (Satz) . . . 49
4.4 Dirichletscher Primzahlsatz (Satz) . . . 49
4.5 Primzahlverteilungsfunktion . . . 49
4.6 Großer Primzahlsatz (Satz) . . . 50

V Fundamentalsatz der Arithmetik 50
5.1 Der wichtigeste Fall (Satz) . . . 50
5.2 Die kanonische Primzerlegung (Satz) . . . 50
5.3 Primteiler (Prop) . . . 50
5.4 Primteiler (Kor) . . . 51
5.5 Erweiterete kanonische Primzerlegung - Konvention . . . 51
5.6 eindeutige Darstellung einer Zahl (Satz) . . . 51
5.7 Primzahlen ausßerhalb endlicher Teilmengen (Bem) . . . 51
5.8 kanonische Primzerlegung (Prop) . . . 51
5.9 Verallgemeinerung auf von Null verschiedene ganze Zahlen (Satz) . . . 51
5.10 weitere eindeutige Darstellung einer Zahl (Satz) . . . 52
5.11 kanonische Primzerlegung – Primteiler (Prop) . . . 52
5.12 kanonische Primzerlegungen (Prop) . . . 52

VI Einige Konsequenzen des Fundamentalsatzes 52
6.1 Teilbarkeitskriterium (Satz) . . . 52
6.2 ggT und kgV (Satz) . . . 53
6.3 ggT und kgV (Kor) . . . 53
6.4 teilerfremde Zahlen (Prop) . . . 53
6.5 Anzahl der Teiler (Prop) . . . 53
6.6 Potenzen (Satz) . . . 54

§ 14 Rationale Zahlen 54

I $\mathbb{Q}$ als Körper mit einer totalen Anordnung, der den Ring $\mathbb{Z}$ enthält 54
1.1 $\mathbb{Q}$ (Def) . . . 54
1.2 Verknüpfungen und Anordnung . . . 55
1.3 Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$ . . . 56
1.4 Potenzen und Division . . . 57

II Viele kleine Begriffe 57
2.1 Gekürzte Bruchdarstellung . . . 57
2.2 Hauptnennerdarstellung . . . 57
2.3 Allgemeiner Nenner . . . 58
2.4 Scheinbrüche, Stammbrüche usw. . . . 58
2.5 Prozentrechnung . . . 59

III Kanonische Zerlegung für rationale Zahlen 59
3.1 Teilerfremde Zähler und Nenner . . . 59
3.2 Allgemeinere Darstellung . . . 59

IV Dezimalbruchentwicklung rationaler Zahlen 60

4.1 Periodische reelle Zahlen mit Periode 0 . . . 60
4.2 Rein periodische reelle Zahlen . . . 60
4.3 Periodische reelle Zahlen = Rationale Zahlen . . . 61
4.4 Wichtige Anmerkungen . . . 61

§ 15 Reelle Zahlen, Dezimalbruchentwicklung 62

I Definition 62
1.1 Äquivalenzklassen von Cauchy-Folgen . . . 62
1.2 Dedekindsche Schnitte . . . 62
1.3 Intervallschachtelung . . . 63
1.4 Axiomatische Konstruktion . . . 63
1.5 Struktur von $\mathbb{R}$ . . . 64

II Dezimalbruchentwicklung reeller Zahlen 64
2.1 Kommaschreibweise . . . 64
2.2 Periodenschreibweise . . . 65
2.3 Irrationale Zahlen . . . 65

§ 16 Kongruenzrechnung 65

I Definitionen 65
1.1 Kongruenz modulo m . . . 65
1.2 Restklassen . . . 66
1.3 Restsysteme . . . 66

II Kongruenzrechnung 67
2.1 Rechenregeln . . . 67
2.2 Restklassen bzgl. verschiedenen Moduli . . . 67

III Ringsturktur von $\mathbb{Z}/m\mathbb{Z}$ 68
3.1 Definition . . . 68
3.2 Multiplikatives Inverses, Einheiten . . . 68

IV Kongruenzsysteme: einfache Fälle 69
4.1 Eine lineare Kongruenz . . . 69
4.2 Potenzen derselben Primzahl . . . 69

V Kongruenzsysteme: Paarweise teilerfremde moduli 70
5.1 Chinesischer Restsatz . . . 70
5.2 Verfahren für zwei Kongruenzen . . . 70

VI Allgemeine Kongruenzsysteme 71
6.1 Drei Schritte . . . 71

§ 1
Die Sprache der Mathematik

- Man muss die Sprache der Mathematik ganz wörtlich nehmen.
- Wir dürfen KEINE Mehrdeutigkeit und KEINE Interpretationsfreiheit haben.
- Wenn es KEINE Einschränkung gibt, dann gibt es totale Freiheit.
- Es gibt KEINE Ausnahme von Regeln.
- Wenn etwas NICHT IMMER wahr ist, dann ist es falsch.
- Das Wort *oder* ist KEIN entweder oder.
- *Es gibt ein* bedeutet, es gibt mindestens ein. Ansonsten schreiben wir *es gibt genau ein.*

I Aussagenlogik

1.1 Definition (Aussage)

Eine Aussage ist ein sprachliches Gebilde, von dem es sinnvoll ist zu fragen, ob es wahr oder falsch ist.
Aussagen sind also Sätze, die wahr oder falsch sind.

1.2 Definition (logisch äquivalent)

Zwei Konstruktionen mit Aussagen sind logisch äquivalent, wenn sie dieselben Wahrheitswerte haben.

II Konstruktionen mit Aussagen

2.1 Negation

Die Negation (Verneinung) einer Aussage p ist die Aussage „nicht p“, die mit $\neg p$ bezeichnet wird. Es gilt:

- Wenn p wahr ist, dann ist $\neg p$ falsch.
- Wenn p falsch ist, dann ist $\neg p$ wahr.

Also ergibt sich folgende Wahrheitstabelle:

p	$\neg p$
1	0
0	1

2.2 Konjunktion

Seien p und q Aussagen. Dann ist „p und q“ eine Aussage, die mit $p \wedge q$ bezeichnet wird. Sie ist genau dann wahr, wenn sowohl p als auch q wahr sind.

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Natürlich ist $p \wedge q$ zu $q \wedge p$ äquivalent.

Seien nun p, q, r Aussagen. Da $(p \wedge q) \wedge r$ zu $p \wedge (q \wedge r)$ äquivalent ist, dürfen wir einfach $p \wedge q \wedge r$ schreiben.

Seien nun $p_1, p_2, \ldots, p_n$ Aussagen und $n \in \mathbb{N}$. Dann ist $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ eine Aussage, die genau dann wahr ist, wenn alle $p_1, p_2, \ldots, p_n$ wahr sind.

Selbsttest

Die Konstruktion $p \wedge (\neg p)$ ist immer falsch, d. h. ein *Widerspruch*, egal ob p wahr oder falsch ist.

2.3 Adjunktion

Seien p und q Aussagen. Dann ist „p oder q“ eine Aussage, die mit $p \vee q$ bezeichnet wird. Sie ist genau dann wahr, wenn mindestens eine der Aussagen p, q wahr ist. Also ist das ein „nichtausschließendes oder“.
Für die Adjunktion erhalten wir

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Natürlich ist $p \vee q$ zu $q \vee p$ äquivalent.
Seien nun p, q, r Aussagen. Da $(p \vee q) \vee r$ zu $p \vee (q \vee r)$ äquivalent ist, dürfen wir einfach $p \vee q \vee r$ schreiben.
Seien nun $p_1, p_2, \ldots, p_n$ Aussagen und $n \in \mathbb{N}$. Dann ist $p_1 \vee p_2 \vee \ldots \vee p_n$ eine Aussage, die genau dann wahr ist, wenn mindestens eine der Aussagen $p_1, p_2, \ldots, p_n$ wahr ist.

Bemerkung: Das „entweder oder“ (*Disjunktion* oder *Adjunktion Disjunktion*) wird durch die Formel $(p \vee q) \wedge (\neg(p \wedge q))$ ausgedrückt.

Selbsttest

Die Konstruktion $p \vee (\neg p)$ ist immer wahr, d. h. eine *Tautologie*, egal ob p wahr oder falsch ist.

III Implikationen

3.1 Implikationen

Seien p und q Aussagen. Die Aussage „aus p folgt q“ bzw. „p impliziert q“ oder „p schließt q ein“ wird mir $p \Longrightarrow q$ bezeichnet. Wir nennen p die *Prämisse* (Voraussetzung) und q die *Konklusion* (Folgerung).
Wir sagen, p ist eine *hinreichende Bedingung* für q; q ist eine *notwendige Bedingung* für p.
Die Ausage $p \Longrightarrow q$ bedeutet: wenn p falsch ist (d. h. $\neg p$ ist wahr), dann kann q wahr oder falsch sein. Ist p jedoch wahr, so muss q auch wahr sein.

p	q	$p \Longrightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Die Aussage $p \Longrightarrow q$ ist äquivalent zu $(\neg q) \Longrightarrow (\neg p)$.
Ferner ist $\neg(p \Longrightarrow q)$ äquivalent zu $p \ \wedge \ (\neg q)$ (da $p \Longrightarrow q$ genau dann falsch ist, wenn p wahr ist, aber q falsch).
Die Aussage $q \Longrightarrow p$ heißt *Umkehrung* der Aussage $p \Longrightarrow q$.

Selbsttest

Die Implikation $p \Longrightarrow q$ ist logisch äquivalent zu $(\neg p) \ \vee \ p$.

3.2 Äquivalenz

Seien p und q Aussagen. Dann wird die Aussage „p genau dann, wenn q“ durch die Formel

$$(p \Longrightarrow q) \ \wedge \ (q \Longrightarrow p)$$

ausgedrückt. Sie wird mit $p \Longleftrightarrow q$ bezeichnet. Man kann auch sagen „p ist äquivalent zu q. Ferner gilt:

- p ist eine hinreichende und notwendige Bedingung für q
- q ist eine hinreichende und notwendige Bedingung für p

$p \Longleftrightarrow q$ bedeutet also, dass p und q logisch äquivalent sind.

p	q	$p \Longleftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

IV Prädikate

4.1 Definition (Prädikat)

Eine Formel, die von endlich vielen Variablen abhängt und die Eigenschaft besitzt, für jeden eingesetzten Wert der Variablen eine Aussage zu sein, heißt Prädikat.

Prädikate können einwertig, zweiwertig usw. sein, je nachdem, ob sie von einer, zwei usw. Variablen abhängen.

4.2 Quantoren

Sei $p(x)$ ein einwertiges Prädikat. Dann ist „es gibt/es existiert ein x, sodass $p(x)$“ eine Aussage, die kurz als „$\exists x\colon p(x)$“ geschrieben wird.
Sei $p(x)$ ein einwertiges Prädikat. Dann ist „für alle x ist $p(x)$“ eine Aussage, die kurz als „$\forall x\colon p(x)$“ geschrieben wird.
Wir nennen $\exists$ und $\forall$ *Quantoren*.

Bemerkung: Das resultierende Prädikat hat eine Variable weniger.

In der Mathematik ist $\exists!$ auch ein Quantor, der „es existiert genau ein“ bedeutet. Also haben wir hier auch Eindeutigkeit gegeben.

4.3 Zweiwertige Prädikate

Sei $p(x, y)$ ein zweiwertiges Prädikat. Dann können wir die folgenden Aussagen bilden:

- $\forall x\ \forall y\colon p(x, y)$
- $\forall x\ \exists y\colon p(x, y)$
- $\exists x\ \forall y\colon p(x, y)$
- $\exists x\ \exists y\colon p(x, y)$

Dabei ist „$\forall x\ \forall y\colon p(x, y)$“ äquivalent zu „$\forall y\ \forall x\colon p(x, y)$“. Daher schreiben wir auch „$\forall\, x, y\colon p(x, y)$“.
Ferner ist „$\exists x\ \exists y\colon p(x, y)$“ äquivalent zu „$\exists y\ \exists x\colon p(x, y)$“. Daher schreiben wir auch „$\exists\, x, y\colon p(x, y)$“.
Allerdings gibt es einen großen Unterschied zwischen „$\forall x\ \exists y\colon p(x, y)$“ und „$\exists x\ \forall y\colon p(x, y)$“.

V Sätze usw.

5.1 Definition (Satz)

Ein Satz ist eine Aussage und genauer eine Implikation: die Annahmen (Hypothesen) implizieren die Folgerung (These). Jeder Satz hat mindestens einen Beweis, d. h. eine vollständige Begründung, dass die Aussage wahr ist.

5.2 Typische Bweisstrukturen

Sei H eine Hypothese und T eine These.

5.2.1 Direkter Beweis

Eine Kette logischer Deduktionen: „Sei die Hypothese erfüllt. Dann folgt ... und dann ... und dann folgt die These."

$$H \implies A_1 \implies A_2 \implies A_3 \implies \ldots \implies A_n \implies T$$

5.2.2 Kontraposition

„$H \implies T$" ist äquivalent zu „$(\neg T) \implies (\neg H)$". Beweise somit:

$$\neg T \implies \neg H$$

5.2.3 Widerspruchsbeweis

„$H \implies T$" ist äquivalent zu „$\neg\big(H \wedge (\neg T)\big)$", d. h. es kann NICHT sein, dass H und $\neg T$ gelten. Beweise somit:

$$H \wedge (\neg T)$$

Sei r eine Aussage. Dann heißt

$$r \wedge \neg r$$

Kontradiktion, was eine falsche Aussage für jedes r darstellt.
Um zu zeigen, dass eine Aussage falsch ist, führt man diese zu einer Kontradiktion.

$$H \wedge \neg T \implies \ldots \implies r \wedge \neg r \quad \lightning$$

wobei $\lightning$ einen Widerspruch kennzeichne.

5.3 Kompliziertere Sätze

Manchmal enthalten Sätze doppelte Implikationen, d. h. seien A, B Aussagen und es gelte

$$A \implies B \qquad \text{und} \qquad B \implies A$$

Dies schreiben wir zusammen als

$$A \iff B$$

Manchmal enthalten Sätze mehrere Implikationen. Seien p, q, r Aussagen.

$$p \implies q \qquad \text{und} \qquad q \implies r$$

Dann gilt auch

$$p \implies r$$

Dies benötigen wir zum Beweis von

$$E_1 \implies E_2 \implies \ldots \quad E_n \implies E_1$$

wobei E_i ($i \in \mathbb{N}$) Aussagen seien. Diese Kette von Implikationen beweist dann, dass alle Aussagen E_i ($i \in \mathbb{N}$) äquivalent sind.

5.4 Beispiele und Gegenbeispiele

5.4.1 Definition (Beispiel)

Ein Beispiel für ein Prädikat sind angegebene Werte für die Variablen, sodass das Prädikat mit diesen eingesetzten Werten eine wahre Aussage ist.

5.4.2 Definition (Gegenbeispiel)

Ein Gegenbeispiel für ein Prädikat sind angegebene Werte für die Variablen, sodass das Prädikat mit diesen eingesetzten Werten eine falsche Aussage ist.

$\forall x\colon p(x)$ ist ein einwertiges Prädikat. Findet man ein Beispiel dafür, so weiß man noch NICHT, ob die Eigenschaft wahr oder falsch ist. Findet man jedoch ein Gegenbeispiel, dann ist die Eigenschaft definitiv falsch.

5.5 Lemma, Korollar, Präposition, Vermutung

5.5.1 Definition (Lemma)

Ein *Lemma* ist eine Aussage, die als Hilfssatz im Beweis anderer Sätze verwendet wird.

5.5.2 Definition (Korollar)

Ein *Korollar* ist eine triviale Folgerung, die sich aus einem Satz ohne großen Aufwand ergibt.

5.5.3 Definition (Präposition)

Eine *Präposition* ist ein Satz, der nicht so wichtig ist oder dessen Formulierung nicht so schön ist.

5.5.4 Definition (Vermutung)

Eine *Vermutung* ist eine wichtige Aussage, von der man glaubt, dass sie wahr sei und die man beweisen möchte.

Bsp. elementare Zahlentheorie: Goldbachsche Vermutung
„*Jede gerade Zahl größer als zwei kann als Summe zweier Primzahlen geschrieben werden.*“

§ 2
Naive Mengenlehre (Teil I)

I Mengen und Teilmengen

1.1 Definition (Menge)

Eine Menge ist eine Sammlung von Elementen, die alle verschieden sind.

Ist a ein Element einer Menge M, so schreiben wir $a \in M$. Analog schreiben wir $a \notin M$, falls a NICHT in M enthalten ist.
Besitzt eine Menge kein Element, so heißt diese Menge *leere Menge* und wird mit $\emptyset$ bezeichnet.
Eine Menge von Mengen wird auch als Familie von Mengen bezeichnet.

1.2 Definition (gleiche Mengen)

Zwei Mengen sind gleich, wenn sie dieselben Elemente besitzen.

1.3 Proposition (Eigenschaften der Gleichheit)

Seien A, B, C Mengen. Dann gelten

- $A = A$ (Reflexivität)
- $A = B \implies B = A$ (Symmetrie)
- $(A = B \ \wedge \ B = C) \implies A = C$ (Transitivität)

1.4 Definition (Teilmenge)

Seien A und B Mengen. Dann ist A eine *Teilmenge* von B, wenn jedes Element aus A auch in B enthalten ist. Wir schreiben $A \subseteq B$ oder $B \supseteq A$.

Wir sagen „A ist in B enthalten“ oder „B enthält A“. Wir nennen $\subseteq$ *Inklusion*.

1.5 Proposition (Eigenschaften der Inklusion)

Seien A, B, C Mengen. Dann gelten:

- $A \subseteq A$ (Reflexivität)
- $(A \subseteq B \ \wedge \ B \subseteq A) \implies A = B$ (Antisymmetrie)
- $(A \subseteq B \ \wedge \ B \subseteq C) \implies A \subseteq C$ (Transitivität)
- $\emptyset \subseteq A$

Für eine *echte Teilmenge* gilt

$$A \subseteq B \ \wedge \ A \neq B$$

und wir schreiben $A \subset B$ oder $B \supset A$. Wir nennen $\subset$ *strenge Inklusion*.

1.6 Spezielle Mengen

- $\emptyset$, die leere Menge
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2 \ldots\}$, die ganzen Zahlen
- $\mathbb{N} = \{0, 1, 2, 3, 4 \ldots\}$, die natürlichen Zahlen
- $\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbb{Z} \quad \wedge \quad q \neq 0 \right\}$, die rationalen Zahlen
- $\mathbb{R}$, die reellen Zahlen
- $\mathbb{C}$, die komplexen Zahlen

Es gilt

$$\mathbb{Z}_{>0} \subset \mathbb{Z}_{\geq 0} = \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

1.7 Allgemeine Schreibweise

- **endliche Mengen:** durch Aufzählen ihrer Elemente; Reihenfolge der Elemente egal; ein Element darf auch mehrmals vorkommen
- **Aufzählung oft unpraktisch/unmöglich:** $\left\{ x \in \mathbb{Z} \;\middle|\; x \geq 100 \right\}$
- **klar erkennbarer Fortlauf in einer Menge**: $M = \{3, 6, 9, 12, \ldots, 96, 99\}$
  anders geschrieben: $M = \left\{ x \in \mathbb{Z} \;\middle|\; 3 \,\middle|\, x \;;\; 1 \leq x \leq 100 \right\}$

VORSICHT: $\Big(M = \{1\}\Big) \neq \Big(M' = \{\{1\}\} = M\Big) \neq \Big(M'' = \{1, \{1\}\} = \{1, M\}\Big)$
Die Zahl 1 ist also NICHT dasselbe wie die Menge $\{1\}$.

- Bildung neuer Mengen mittels *Mengenoperatoren* (siehe unten)
- induktive Definition von Mengen: explizite Angabe eines Grundelements und mindestens eine Regel zur Ableitung eines weiteren Elements

II Operationen zwischen Mengen

2.1 Definition (Durchschnitt)

Seien A, B Mengen. Dann definieren wir den *Druchschnitt* von A und B als

$$A \cap B = \left\{ x \;\middle|\; x \in A \quad \wedge \quad x \in B \right\}$$

gesprochen: „A geschnitten B“

2.2 Definition (disjunkt)

Zwei Mengen A, B heißen *disjunkt*, falls $A \cap B = \emptyset$.

2.3 Proposition (Eigenschaften Durchschnitt)

Seien A, B, C Mengen. Dann gelten:

- $A \cap B = B \cap A$ (Kommutativität)
- $A \cap B \subseteq A$ (und $= A \iff A \subseteq B$)
- $A \cap A = A$, $A \cap \emptyset = \emptyset$
- $(A \cap B) \cap C = A \cap (B \cap C) = A \cap B \cap C$ (Assoziativität)

Bemerkung: $A \cap B \subseteq B$ und $\emptyset \cap A = \emptyset$ folgen aus der Kommutativität.

2.4 Definition (Durchschnitt einer Familie von Mengen)

Sei I eine Menge und seien A_i für alle i Mengen. Dann definieren wir den *Druchscnitt dieser Familie von Mengen* als

$$\bigcap_{i \in I} A_i = \left\{ x \;\middle|\; x \in A_i \; \forall i \in I \right\}$$

$\forall\, i_0 \in I\colon \bigcap\limits_{i \in \mathbb{I}} A_I \subseteq A_{i_0}$
Verallgemeinerung der Symmetrieregel: Anordnung der Mengen spielt KEINE Rolle!
Sei $I = \{1, \ldots, n\}$. Dann gilt

$$\bigcap_{i \in I} A_i = \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

2.5 Definition (paarweise Disjunkt)

Sei I eine Menge und seinen A_i für alle $i \in I$ Mengen. Diese Mengen heißen *paarweise disjunkt*, falls für alle $i, j \in I$ mit $i \neq j$ gilt: $A_i \cap A_j = \emptyset$.

Bemerkung: „paarweise Disjunkt“ könnte strenger sein als „Durchschnitt aller Mengen ist leer“.

2.6 Definition (Vereinigung)

Seien A, B Mengen. Dann definieren wir die *Vereinigung* von A und B als

$$A \cup B = \left\{ x \;\middle|\; x \in A \;\; \vee \;\; x \in B \right\}$$

gesprochen: „A vereinigt B“

2.7 Proposition (Eigenschaften Vereinigung)

Seien A, B, C Mengen. Dann gelten:

- $A \cup B = B \cup A$ (Kommutativität)
- $A \cup B \supset A$ (und $= A \iff A \supseteq B$)
- $A \cup A = A$, $A \cup \emptyset = A$

- $(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$ (Assoziativität)

Bemerkung: $A \cup B \supset B$ und $\emptyset \cup A = A$ folgen aus der Kommutativität.

2.8 Definition (Vereinigung einer Familie von Mengen)

Sei I eine Menge und seien A_i für alle $i \in I$ Mengen. Dann definieren wir die *Vereinigung dieser Familie von Mengen* als

$$\bigcup_{i \in I} A_i = \left\{ x_i \;\middle|\; \exists i \in I \colon\; x \in A_i \right\}$$

$\forall\, i_0 \in I \colon\; \bigcup_{i \in I} A_i \subseteq A_{i_0}$
Verallgemeinerung der Symmetrieregel: Anordnung der Mengen spielt KEINE Rolle!
Sei $I = \{1, \ldots, n\}$. Dann gilt

$$\bigcup_{i \in I} A_i = \bigcup_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

2.9 Definition (Differenz)

Seien A, B Mengen. Dann definieren wir die *Differenzmenge* als

$$A \setminus B = \left\{ x \;\middle|\; x \in A \;\wedge\; x \notin B \right\}$$

gesprochen: „A ohne B“
Wird auch als *Komplement* von B in A oder B^C bezeichnet.
$\forall\, A \colon\; A \setminus A = \emptyset \;,\; A \setminus \emptyset = A$
Differenz von Mengen ist NICHT kommutativ: falls $A \neq B \colon\; (A \setminus B) \neq (B \setminus A)$

2.10 Definition (symmetrsiche Differenz)

Seien A, B Mengen. Die *symmetrische Differenz* $A \Delta B$ wird definiert als

$$A \Delta B := (A \setminus B) \cup (B \setminus A)$$

$\forall\, A \colon\; A \Delta A = \emptyset \;,\; A \Delta \emptyset = A$
$\forall\, A, B \colon\; A \Delta B = B \Delta A$ (Kommutativität)

Selbsttest

Seien A, B Mengen. $\forall A, B \colon\; (A \setminus B) \cap (B \setminus A) = \emptyset$ und es gilt

$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

2.11 Proposition (Ditributivität zwischen Durchschnitt und Vereinigung)

Seien A, B, C Mengen. Dann gelten:

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2.12 Proposition (Eigenschaften Differenz, Durchschnitt, Vereinigung)

Seien A, B, C Mengen. Dann gelten:

- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- $A \cap (B \setminus A) = \emptyset$
- $A \cup (B \setminus A) \supseteq B$ (und $= B \iff A \subseteq B$)

III Mächtigkeit für endliche Mengen

- **endlich:** Menge hat nur endlich viele Elemente (incl. $\emptyset$).
- **unendlich:** sonst
- **Mächtigkeit:** Anzahl der Elemente: $|M|$ oder $\#M$

Bemerkungen

- $\#M = 0 \iff M = \emptyset$
- $A \subseteq B \implies \#A \leq \#B$ (Umkehrung i. A. falsch!)
- $A \subset B \implies \#A < \#B$ (Umkehrung i. A. falsch!)

§ 3
Binäre Relationen

Relationen im Sinne der Mathematik sind ausschließlich diejenigen Beziehungen, bei denen stets klar ist, ob sie bestehen oder nicht.

I Relationen

1.1 Definition (binäre Relation)

Seien M, N nichtleere Mengen. Eine *binäre Relation* zwischen den Mengen M und N ist eine Teilmenge $R \subseteq M \times N$.

Relationen, die zwei Elemente vergleichen, heißen binäre Relationen.

1.2 Eigenschaften für eine Relation auf einer Menge

$M = M \implies$ Relation auf M. Sei M eine nichtleere Menge und $R \subseteq M$ eine Relation auf der Menge M. Dann sind folgende Eigenschaften, die *gelten können oder nicht*, wichtig:

- **Reflexivität:** R *reflexiv*, falls $\forall\, x \in M\colon\ (x,x) \in R$
- **Irreflexiv:** R *irreflexiv*, falls $\forall\, x \in M\colon\ (x,x) \notin R$
  Bemerkung: stärkere Eigenschaft als „nicht reflexiv $\big(\exists\, x \in M\colon\ (x,x) \notin R\big)$“
- **Symmetrie:** R *symmetrisch*, falls $\forall\, x,y \in M\colon\ (x,y) \in R \implies (y,x) \in R$
  Bemerkung: sym. Rel. erfüllt automatisch $\forall\, x,y \in M\colon\ (x,y) \in R \iff (y,x) \in R$
- **Asymmetrie:** R *asymmetrisch*, falls $\forall\, x,y \in M\colon\ (x,y) \in R \implies (y,x) \notin R$
  Bemerkung: stärkere Eigenschaft als „nicht symmetrisch“
- **Antisymmetrie:** R *antisymmetrisch*, falls

$$\forall\, x,y \in M\colon\ \big((x,y) \in R \ \wedge\ (y,x) \in R\big) \implies x = y$$

- **Transitivität:** R *transitiv*, falls

$$\forall\, x,y,z \in M\colon\ \big((x,y) \in R \ \wedge\ (y,z) \in R\big) \implies (x,y) \in R$$

- **Totalität:** R *total*, falls $\forall\, x,y \in M\colon\ (x,y) \in R \ \vee\ (y,x) \in R$
  Bemerkung: R total $\implies$ R reflexiv
- **Konnexität:** R *konnex*, falls $\forall\, x,y \in M$ *genau eine* der folgenden Eigenschaften gilt:
  $(x,y) \in R$ ODER $(y,x) \in R$ ODER $x = y$

Sei R Relation auf M und $\emptyset \neq N \subseteq M$. Dann ist $R' = R \cap (N \times N)$ eine Relation auf N. Die Eigenschaften von R gelten auch für die Einschränkung R'. Die Umkehrung ist i. A. nicht immer wahr.

1.3 Definition (Halordnung, Striktordnung)

Sei M eine nichtleere Menge und $R \subseteq M$ eine Relation auf der Menge M.
R heißt *Halbordnung* (oder Ordnung), falls sie reflexiv, antisymmetrisch und transitiv ist (z. B. $\leq$ in $\mathbb{R}$).
R heißt *Striktordnung*, falls sie asymmetrisch und transitiv ist (z. B. $<$ in $\mathbb{R}$).

Bemerkung: asymmetrisch $\implies$ irreflexiv und antisymmetrisch

II Äquivalenzrelationen

2.1 Definition (Äquivalenzrelation)

Sei M eine nichtleere Menge und $R \subseteq M$ eine Relation auf der Menge M. Die Relation ist eine *Äquivalenzrelation*, falls sie reflexiv, symmetrisch und transitiv ist.

Ist eine Äquivalenzrelation gegeben, so heißen zwei Elemente, die die Relation erfüllen, äquivalent.

2.2 Definition (Äquivalenzklasse, Repräsentant, Quotientenmenge)

Sei M eine nichtleere Teilmenge und $R \subseteq M$ eine Äquivalenzrelation auf der Menge M. Sei $x \in M$. Dann nennen wir folgende Teilmenge von M die *Äquivalenzklasse von* x:

$$[x] := \left\{ y \in M \;\middle|\; (x,y) \in R \right\} \overset{\text{Sym.}}{=} \left\{ y \in M \;\middle|\; (y,x) \in R \right\}$$

Jedes Element einer Äquivalenzrelation heißt *Repräsentant* dieser Klasse. Die Menge der Äquivalenzklassen heißt *Quotientenmenge*.

2.3 Eigenschaften Äquivalenzrelation

Für jede Äquivalenzrelation gelten:

- $x \in [x]$
  Jede Äquivalenzklasse ist nicht leer $\implies M = \bigcup\limits_{x \in M} [x]$
- $\forall\, x, y \in M\colon\ (x,y) \in R \iff [x] = [y]$
- $\forall\, x, y \in M\colon\ [x] \cap [y] \neq \emptyset \iff [x] = [y]$

2.4 Satz (Beziehung zu Partitionen)

(1) Die Quotientenmenge einer Äquivalenzrelation auf M ist eine Partition von M, d. h. die Äquivalenzklassen ergeben eine Partition.

(2) Für jede Partition von M gibt es genau eine Äquivalenzrelation auf M, sodass die Partition und die Quotientenmenge übereinstimmen.

§ 4
Induktion

I Beweisprinzip der Vollständigen Induktion

Sei $P(n)$ eine Aussage für alle $n \in \mathbb{N}$. Dann ist $P(n)$ für alle $n \in \mathbb{N}$ wahr.

Beweis (Standard Beweisschema für Induktionsbeweise)

Induktionsanfang

Zeige/Verifiziere/Überprüfe direkt, dass $P(0)$ wahr ist.

Induktionsschritt

Beweise, dass für alle $n \in \mathbb{N}$ die Implikation gilt:

$$P(n) \implies P(n+1)$$

Dann ist $P(n)$ für alle $n \in \mathbb{N}$ wahr.

□

$P(n)$ heißt *Induktionsvoraussetzung* oder *Induktionsannahme*. $P(n+1)$ heißt *Induktionsbehauptung* oder *Induktionsschluss*.
Bemerkung: Im Induktionsschritt ist n beliebig aber fest!

Sei $P(n)$ eine Aussage für $n \in \mathbb{N}$ mit $n \geq n_0$. Dann ist $P(n)$ für alle $n \geq n_0$ wahr.
Beweis (Induktion mit beliebigem Anfang)

Induktionsanfang

Zeige/Verifiziere/Überprüfe direkt, dass $P(n_0)$ wahr ist.

Induktionsschritt

Beweise, dass für alle $n \geq n_0$ die Implikation gilt:

$$P(n) \implies P(n+1)$$

Dann ist $P(n)$ für alle $n \geq n_0$ wahr.

□

Sei $P(n)$ eine Aussage für alle $n \in \mathbb{N}$ mit $n \geq n_0$. Dann ist $P(n)$ für alle $n \geq n_0$ wahr.
Beweis (Induktion mit erweiterter Induktionsvoraussetzung)

Induktionsanfang

Zeige/Verifiziere/Überprüfe direkt, dass $P(n_0)$ wahr ist.

Induktionsschritt

Beweise, dass für alle $n \geq n_0$ die Implikation gilt:

$$\Big(P(n_0) \text{ und } P(n_0+1) \text{ und } \ldots \text{ und } P(n-1) \text{ und } P(n)\Big) \implies P(n+1)$$

Dann ist $P(n)$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ wahr.

□

§ 5
Gruppen, Ringe und Körper

I Verknüpfungen

1.1 Definition (Verknüpfung)

Sei A eine nicht-leere Menge. Eine (zweistellige) *Verknüpfung* auf A ist eine Abbildung

$$*\colon\ A \times A \longrightarrow A$$

Schreibe $a * b$ für $*((a, b))$, gesprochen „a verknüpft mit b“. Schreibe $(A, *)$ um zu sagen, dass A eine Menge und $*$ eine Verknüpfung auf A ist.
Eine Verknüpfung ist insbesondere eine Funktion, die *eindeutig ausführbar* ist, d. h. $a*b$ existiert in eindeutiger Weise.

1.2 Zusätzliche Eigenschaften Verknüpfung

- **Kommutativität:** $*$ *kommutativ* oder *abelsch*, falls $\forall\ a, b \in A\colon\ a * b = b * a$
- **Assoziativität:** $*$ *assoziativ*, falls $\forall\ a, b, b \in A\colon\ (a * b) * c = a * (b * c)$
- **neutrales Element:** Ein Element aus A heißt *neutrales Element* (für $*$), falls $\forall\ a \in A\colon\ e * a = a * e = a$
- **Inverses Element:** Ein Element $a' \in A$ heißt *inverses Element* von $a \in A$ (für $*$), falls $a' * a = a * a' = e$, wobei e das neutrale Element ist.
  e muss existieren, um von inversen Elementen sprechen zu können.
  Notation: a^{-1} (multiplikativ) und $-a$ (additiv)

1.3 Proposition (Verknüpfung)

(1) $\exists e \implies e$ eindeutig

(2) Sei $*$ assoziativ mit neutralem Element e. $\exists$ Inverses zu $a \in A \implies$ Eindeutigkeit

(3) e kommutiert mit allen Elementen (auch wenn $*$ NICHT kommutativ ist)

(4) Element kommutiert mit seinem Inversen (auch wenn $*$ NICHT kommutativ ist)

1.4 Wichtige algebraische Strukturen

- **Halbgruppe:** $(A, *)$ *Halbgruppe*, falls $*$ assoziativ
- **Monoide:** $(A, *)$ *Monoid*, falls $*$ assoziativ und $\exists e$
- **Gruppe:** $(A, *)$ *Gruppe*, falls $*$ assoziativ, $\exists e$ und $\exists$ Inverses $\forall\ a \in A$
- **ablesche . . . :** $*$ ist abelsch

II Gruppen

2.1 Eigenschaften Gruppen

Sei $(A, *)$ eine Gruppe.

- $\forall\ a \in A\colon\ (a^{-1})^{-1} = a$
- $\forall\ a, b \in A\colon\ (a * b)^{-1} = b^{-1} * a^{-1}$
- Kürzungsregeln: $\forall\ a, b, c \in A\colon\ a * c = b * c \implies a = b \quad ; \quad c * a = c * b \implies a = b$

- $\forall\ a, b \in A$ hat die Gleichung

$$a * x = b$$

genau eine Lösung mit $x \in A$, nämlich $x = a^{-1} * b$. Jede Gleichung der Form $x * a = b$ hat genau eine Lösung $x \in A$, nämlich $x = b * a^{-1}$

2.2 Definition (Ordnung einer Gruppe)

Die Mächtigkeit der Menge A nennt man *Ordnung* der Gruppe A.

§ 6
Die natürlichen Zahlen

I Axiome der natürlichen Zahlen

1.1 Begründung der Axiome

Nachfolgerfunktion, injektiv; 0 ist KEIN Nachfolger!

1.2 Die Peano Axiome

Die natürlichen Zahlen bilden eine Menge $\mathbb{N}$ mit

(1) ausgezeichnetem Element 0

(2) Abbildung (Nachfolgerfunktion) $S\colon \mathbb{N} \longrightarrow \mathbb{N}\ ,\ n \longmapsto S(n)$

Es sollen gelten:

(A) S injektiv, d. h. $n \neq m \implies S(n) \neq S(m)$

(B) $0 \notin S(\mathbb{N})$, d. h.: $\forall\ n \in \mathbb{N}\colon\ S(n) \neq 0$

(C) Induktionsaxiom: Sei $M \subseteq \mathbb{N}$ eine Menge mit den Eigenschaften

(i) $0 \in M$

(ii) $x \in M \implies S(x) \in M$

Dann ist $M = \mathbb{N}$.

1.3 Satz (Surjektivität der Nachfolgerfunktion)

Funktion S ist surjektiv auf $\mathbb{N} \setminus \{0\}$.

1.4 Eindeutigkeit von $\mathbb{N}$

Seien $(N_A, 0_A, S_A)$ und $(N_B, 0_B, S_B)$ zwei Modelle, die obige Eigenschaften erfüllen.
Dann $\exists!\ f\colon\ N_A \longrightarrow N_B$ mit

$$f(0_A) = 0_B\ ,\ f\big(S_A(n)\big) = S_B\big(f(n)\big)$$

Diese Funktion ist eine Bijektion. Somit sind die zwei Modell *kanonisch isomorph.*
$\Longrightarrow$ Eindeutigkeit bis auf Umbenennung der Elemente.

II Rekursive Folgen

2.1 Satz (Rekursionssatz nach Dedekind)

Sei A eine Menge, $T\colon A \longrightarrow A$ eine Abbildung und $\alpha \in A$ ein Element. Dann $\exists!$ Funktion $f\colon \mathbb{N} \longrightarrow A$ mit

- $f(0) = \alpha$
- $f(S(n)) = T(f(n)) \quad \forall\, n \in \mathbb{N}$

2.2 Definition (Folge)

Man nennt eine Abbildung $f\colon \mathbb{N} \longrightarrow A$ *Folge* von Elementen aus A und schreibt auch f_n für $f(n)$, $(f_n)_{n\in\mathbb{N}}$ oder $f_0, f_1, f_2 \ldots$ für f.

2.3 Definition (rekursive Folge)

Eine Funktion wie im Dedekindschen Rekursionssatz nennt man eine *rekursive Folge*. Es wir in diesem Fall eine Abbildung $T\colon\ A \longrightarrow A$ und ein $\alpha \in A$ vorgegeben und erklärt $f_0 = \alpha$; $f_{n+1} = T(f_n)$. Man nennt α das Anfangsglied und $f_{n+1} = T(f_n)$ die Rekursionsgleichung für die Folge f.

2.4 Definition (k-rekursive Folgen)

Allgemeiner kann man rekursive Folgen definieren, indem man angibt, wie ein Folgenglied aus den k vorangegangenen berechnet werden soll (k-fache Rekursion).

2.5 Satz (k-Rekursionssatz)

Sei A eine Menge. Sei $k \geq 1$ und sei $T\colon A^k \longrightarrow A$ eine Funktion. Dann wird durch Vorgabe von $f_0, \ldots, f_{k-1}$ und die *Rekursionsvorschrift*

$$f_{n+k} = T(f_n, \ldots, f_{n+k+-1}) \quad (n \in \mathbb{N})$$

eine eindeutig bestimmte Folge definiert.
Genau $f_0, \ldots, f_{k-1}$ Anfangsgleider nötig um Folge eindeutig zu definieren. Für $k = 1$ ist dies genau der Rekursionssatz von Dedekind.
f_n für $n \geq k$ kann mit Hilfe der vorherigen bestimmt werden.
Über die ersten k Folgenglieder (f_n mit $0 \leq n \leq k-1$) kann man NICHTS aussagen.

III Addition natürlicher Zahlen

3.1 Definition (Addition)

$\exists!$ Funktion

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \ , \ (x, y) \longmapsto x + y$$

mit den Eigenschaften

(a) $x + 0 = x$

(b) $x + S(y) = S(x + y)$

3.2 Iterierte Nachfolgerfunktion

Sei $1 := S(0)$. Dann gilt nach (2):

$$S(x) = x + 1$$

Das heißt, mit der Addition können wir auch die Nachfolgerfunktion sehen als „addiere 1“. Analog kann man das für alle $a \in \mathbb{N}$ mit $a \geq 1$ zeigen.

3.3 Satz (Eigenschaften Addition)

$\forall\ x, y, z \in \mathbb{N}$ gelten

- **Assoziativität:** $(x + y) + z = x + (y + z)$
- **Kommutativgesetz:** $x + y = y + x$
- **neutrales Element:** $0 + x = x + 0 = x$

3.4 Lemma (Addition)

(1) $\forall\ x \in \mathbb{N}\colon\ 0 + x = x$

(2) $\forall\ x, y \in \mathbb{N}\colon\ y + S(x) = S(y) + x$

3.5 Satz (Kürzungsregel)

(1) $\forall\ a, b \in \mathbb{N}\colon\ a + b = 0 \implies a = b = 0$

(2) $\forall\ a, b, c \in \mathbb{N}\colon\ a + c = b + c \implies a = b$

IV Multiplikation natürlicher Zahlen

4.1 Definition (Multiplikation)

$\exists!$ Funktion

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \ , \ (x, y) \longmapsto x \cdot y$$

mit den Eigenschaften

(a) $x \cdot 0 = 0$

(b) $x \cdot S(y) = (x \cdot y) + x$

4.2 Eigenschaften Multiplikation

$\forall\, x, y, z \in \mathbb{N}$ gelten

- **Kommutatuivgesetz:** $x \cdot y = y \cdot x$
- **Assoziativgesetz:** $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- **neutrales Element:** $1 \cdot x = x \cdot 1 = 1$

und bzgl. Addition gelten folgende **Distributivgesetze**:

- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$

Bemerkung: Multiplikation kommutativ $\Longrightarrow$ Distributivgesetze äquivalent

4.3 Satz (Kürzungsregel)

$\forall\, a, b, c \in \mathbb{N}$ mit $c \neq 0$ gilt: $ac = bc \implies a = b$

4.4 Korollar (Kürzungsregel)

$\forall\, a, b \in \mathbb{N}$: $ab = 0 \implies a = 0 \quad \vee \quad b = 0$

Allgemeiner: $\forall\, a_1, \ldots, a_k \in \mathbb{N}$: $\prod_{i=1}^{k} a_i = 0 \implies \exists i \in \{1, \ldots, k\}$: $a_i = 0$

4.5 Weitere Eigeschaften Summe und Produkt

- $+$ und $\cdot$ assoziativ, d. h. wir brauchen keine Klammern für $x + y + z$ bzw. $x \cdot y \cdot z$
- Konvention: Punkt vor Strich

V Die Anordnung der natürlichen Zahlen

- $\geq$: Für $n, m \in \mathbb{N}$ schreiben wir $n \geq m$, falls $n = m + x$ eine Lösung $x \in \mathbb{N}$ hat.
- $>$: Für $n, m \in \mathbb{N}$ schreiben wir $n > m$, falls $n \geq m$ und $n \neq m$.
- $\leq$: Für $n, m \in \mathbb{N}$ schreiben wir $n \leq m$, falls $m \geq n$.
- $<$: Für $n, m \in \mathbb{N}$ schreiben wir $n < m$, falls $m > n$.

5.1 Satz (Relation $\geq$)

Relation $\geq$ ist (analog $\leq$) reflexiv, antisymmetrisch, transitiv und total.

5.2 Satz (Relation $>$)

Relation $>$ ist (analog $<$) irreflexiv, transitiv, asymmetrisch und konnex.

5.3 Satz (Monotonie)

$\forall\ a, b, c \in \mathbb{N}$ gelten:

- $a \geq b \implies a + c \geq b + c$
- $a > b \implies a + c > b + c$
- $a \geq b \implies ac \geq bc$
- $a > b \implies ac > bc$, falls $c > 0$

Analog für $\leq$ und $<$.

VI Potenzen

6.1 Definition (Potenz)

Sei $n \in \mathbb{N}$. Dann ist $0^n = 0$ für $n > 0$. 0^0 ist NICHT definiert.
Grund: $\lim\limits_{x \to 0^+} 0^x = \lim\limits_{x \to 0^+} 0 = 0$, $\lim\limits_{x \to 0^+} x^0 = \lim\limits_{x \to 0^+} 1 = 1$.

Seien nun $a, n \in \mathbb{N}$ mit $a \neq 0$. Dann gilt

$$a^0 = 1 \quad , \quad a^{n+1} = a^n \cdot a$$

wegen des Rekursionssatzes von Dedekind mit $A = \mathbb{N}$, $\alpha = a$ und $T\colon x \longmapsto x \cdot a$. Insbesondere ist $1^n = 1 \quad \forall\ n \in \mathbb{N}$.

6.2 Satz (Rechenregeln der Potenz)

Seien $a, b, n, m \in \mathbb{N}$ mit $a, b \neq 0$. Dann gelten:

- $a^n \cdot a^m = a^{n+m}$
- $(a^n)^m = a^{n \cdot m}$
- $(ab)^n = a^n \cdot b^n$

a^{n^m} bedeutet $a^{(n^m)}$! WICHTIG, da $a^{(n^m)} \neq (a^n)^m$.

Die Potenz ergibt eine Verknüpfung auf $\mathbb{N} \setminus \{0\}$:

$$\mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}\ ,\ (a, n) \longmapsto a^n$$

Diese ist NICHT asoziativ und NICHT kommutativ. Ferner gibt es KEIN neutrales Element.

6.3 Kuriosität

Seien $x, y \in \mathbb{N} \setminus \{0\}$ mit $x \neq y$. Dann gilt:

$$x^y = y^x \implies (x = 2\ ,\ y = 4) \quad \vee \quad (x = 4\ ,\ y = 2)$$

Beweis

$$x^y = y^x \iff y\ln(x) = x\ln(y)$$

Mit $f(x) = \frac{\ln(x)}{x}$ und f injektiv auf $(e, +\infty)$ (da $f' < 0$) folgt also

$$f(x) = f(y)$$

aber nur, falls $x > e$, d. h. $x = 1$ oder $x = 2$.
OBdA sei nun $x < y$.
$x = 1 \implies 1 = 1^y = y^1 = y$, also $y = x = 1$.
$x = 2 \implies 2^y = y^2$, also $y \neq 1, 2$, sondern höchstens $y \geq e$.
$\implies y = 4$ ist einzige Lösung.

□

VII Weitere Operationen

7.1 Subtraktion

$a = x + b$ mit $a, b \in \mathbb{N}$ lösbar in $\mathbb{N}$ ($\exists$ mindestens eine Lösung $x \in \mathbb{N}$)
$\iff a \geq b$ nach Defintion von $\geq$.

$\exists$ höchstens eine Lösung, falls $a = x_1 + b$ und $a = x_2 + b$. Dies folgt aus der Kürzungsregel der Summe, da hier $x_1 = x_2$ gilt.

7.2 Definition (Subtraktion)

KEINE innere Verknüpfung auf $\mathbb{N}$, da z. B. $3 - 5 \notin \mathbb{N}$.

$$-: \left\{(a, b) \in \mathbb{N} \times \mathbb{N} \;\middle|\; a \geq b\right\} \longrightarrow \mathbb{N}\ ,\ (a, b) \longmapsto x$$

wobei x die eindeuitg bestimmte natürliche Zahl $x + b = a$ ist. x existiert und ist eindeutig.
In $\mathbb{Z}$ ist die Subtraktion eine innere Verknüpfung! Einschränkung dieser Funktion ergibt die Subtraktion auf $\mathbb{N}$, d. h. alles was für die Subtraktion bei ganzen Zahlen gilt, gilt auch für natürliche Zahlen.

7.3 Division mit Rest

Division-mit-Rest-Funktion (KEINE Verknüpfung auf $\mathbb{N}$)

$$\mathbb{N} \times (\mathbb{N} \setminus \{0\}) \longrightarrow \mathbb{N} \times \mathbb{N}\ ,\ (a, b) \longmapsto (q, r)$$

mit $a = bq + r\ ,\ 0 \leq r < b$.
Genaueres folgt unten bei den ganzen Zahlen.

$a = x \cdot b$ mit $a, b \in \mathbb{N}$ lösbar $\iff a$ hat Rest Null bei Division durch b

höchstens eine Lösung $x \in \mathbb{N}$: $b \neq 0$, $a = x_1 b$, $a = x_2 b$
$\rightsquigarrow$ Kürzungsregel liefert: $x_1 = x_2$
keine Lösung für $b = 0$ und $a \neq 0$
$\mathbb{N}$ als Lösungsmenge für $b = 0$ und $a = 0$

§ 7
Polynome (Teil I)

I Polynome

1.1 Definition (Polynom)

Sei R ein Ring. Ein *Polynom* (in einer Unbestimmten X) über R ist ein Ausdruck

$$f = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i$$

wobei $n \in \mathbb{N}$ und $a_0, \ldots, a_n$ Elemente aus R sind.
Setze $a_i = 0 \quad \forall\, i \in \mathbb{N}$ mit $i > n$.
a_i $(i \in \mathbb{N})$ nennt man *Koeffizienten* f.

Polynome sind *gleich*, wenn sie diegleichen Koeffizienten besitzen:

$$\sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} b_i X^i \iff a_i = b_i \quad \forall\, i \in \mathbb{N}$$

Konstante Polynome: $a_i = 0 \quad \forall\, i > 0$:

$$\sum_{i=0}^{n} a_i X^i = a_i$$

heißt *konstantes Polynom*. $0 = \sum\limits_{i=0}^{\infty} 0 \cdot X^i$ heißt *Nullpolynom*.

1.2 Definition (Grad, Leitkoeffizient)

Sei $f = \sum\limits_{i=0}^{n} a_i X^i$ mit $n \geq 0$ und $a_n \neq 0$ ein von 0 verschiedenes Polynom. Dann nennt man n den *Grad* von f und a_n den *Leitkoeffizienten* von f.

Nullpolynom besitzt KEINEN Grad und die konstanten Polynome haben immer Grad 0.

Die Menge alles Polynome über R bezeichnen wir mit $R[X]$ und machen $R[X]$ zu einem Ring, indem wir geeignete Addition bzw. Multiplikation von Polynomen einführen.

II Addition

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

Seien $a_0, \ldots, a_n$ bzw. $b_0, \ldots, b_m$ Elemente aus R und seien $a_j = 0$ für $j > n$ und $b_j = 0$ für $j > m$. Nach den Rechengesetzen für R gilt also

$$(a_0 + a_1 y + \ldots + a_n y^n) + (b_0 + b_1 y + \ldots + b_m y^m) = (a_0 + b_0) + (a_1 + b_1) y + \ldots + (a_l + b_l) y^l$$

wobei $l = \max(n, m)$.

- Addition von Polynomen ist assoziativ und kommutativ.
- Neutrales Element für die Addition von Polynomen ist das Nullpolynom.
- Jedes Polynom besitzt ein Inverses bzgl. Addition:

$$\sum_{i=0}^{\infty} a_i X^i \longleftrightarrow \sum_{i=0}^{\infty} -a_i X^i$$

- $\mathrm{Grad}(f + g) \leq \max\big(\mathrm{Grad}(f), \mathrm{Grad}(g)\big)$

III Multiplikation

$$\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{k=0}^{\infty} c_k X^k$$

wobei

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i}$$

- Multiplikation von Polynomen ist assoziativ.
- R Ring mit Eins $\Longrightarrow$ $\exists 1 \in R$ neutrales Element für die Multiplikation von Polynomen

$$\sum_{i=0}^{\infty} a_i X^i \quad \text{mit } a_0 = 1 \ , \ a_i = 0 \text{ für } i > 0$$

- R kommutativer Ring $\Longrightarrow$ Multiplikation von Polynomen kommutativ
- Sei R ohne Nullteiler. Sind $f, g \in R[X]$ von Null verschiedene Polynome, so gilt: $\mathrm{Grad}(f \cdot g) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$
- Auch wenn R Integritätsbereich oder sogar Körper, gibt es nur wenige Polynome, die ein Inverses für die Multiplikation besitzen. Solche Polynome haben die Form

$$\sum_{i=0}^{\infty} a_i X^i \quad \text{mit } a_0 \in R^{\times} \ , \ a_i = 0 \text{ für } i > 0$$

wobei $R^\times$ die Einheiten in R bezeichne, d. h. Elemente von R, die ein multiplikatives Inverses besitzen.
$\Longrightarrow$ nur konstante Polynome (nicht alle!) invertierbar bzgl. Multiplikation

IV Ringe der Polynome

$R[X]$ auf zwei Verknüpfungen definiert und viele Eigenschaften bereits behandelt. Distributivgesetze für Addition und Multiplikation von Polnomen gelten. Also ist $R[X]$ ein Ring.

Betrachte konstante Polynome (als Gegenbeispiel):

- $R[X]$ kommutativ $\iff$ R kommutativ
- $R[X]$ Ring mit Eins $\iff$ R Ring mit Eins
- $R[X]$ nullteilerfrei $\iff$ R nullteilerfrei
- $R[X]$ Integritätsbereich $\iff$ R Integritätsbereich
- Einheiten von $R[X]$ sind die Einheiten von R
- kostante Polynome sind ein Unterring und mit der Identifizierung

$$R \longleftrightarrow \text{konstante Polynome}$$

ist $R \subseteq R[X]$ ein Unterring.

§ 8
Die ganzen Zahlen

I Definition für $\mathbb{Z}$

1.1 Definition (Definition der ganzen Zahlen)

Die Menge $\mathbb{Z}$ ist die Quotientenmenge der folgenden Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.
$\forall$ (a, b) und $(c, d$ in $\mathbb{N} \times \mathbb{N}$ gilt

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Also ist $\mathbb{Z}$ die Menge der Äquivalenzklassen dieser Äquivalenzrelation. Eine ganze Zahl ist eine Äquivalenzklasse. Die Äquivalenzklasse von (a, b) ist die Menge

$$[(a, b)] := \left\{ (c, d) \;\middle|\; (a, b) \sim (c, d) \right\} = \left\{ (c, d) \;\middle|\; a + d = c + b \right\}$$

II Die positiven ganzen Zahlen

2.1 Proposition (Äquivalenzklassen)

(a) $\forall\ a, b, k \in \mathbb{N}$ ist $[(a, b)] = [(a + k, b + k)]$.

(b) Falls $a \geq b$: $\exists!\ n \in \mathbb{N}$ mit $[(a, b)] = [(n, 0)]$

(c) Falls $a \leq b$: $\exists!\ n \in \mathbb{N}$ mit $[(a, b)] = [(0, n)]$

(d) $a = b \iff [(a, b)] = [(0, 0)]$

(e) $\forall\ n, m \in \mathbb{N}$: $(n, 0) \sim (0, m) \implies n = m = 0$

Eine Konsequnz dieser Proposition ist folgender Satz:

2.2 Satz (Repräsentant)

Als *Repräsentant* für eine ganze Zahl können wir auf eindeutige Weise entweder $(0, 0)$ oder $(n, 0)$ oder $(0, n)$ mit $n \geq 1$ nehmen.

2.3 Korollar (Einbettung $\mathbb{N}$)

Die Abbildung

$$\mathbb{N} \longrightarrow \mathbb{Z}\ ,\ n \longmapsto [(n, 0)]$$

ist injektiv.

Notationen: $n := [(n, 0)]\ ,\ -n := [(0, n)] \quad \forall\ n \in \mathbb{N}$
$n = -n \iff n = 0$.

Die Zahlen $\mathbb{N} \subseteq \mathbb{Z}$ heißen *positive Zahlen* und die Zahlen $-\mathbb{N} \subseteq \mathbb{Z}$ heißen *negative Zahlen.*

Falls $z = [(a, b)]$ eine ganze Zahl ist, definieren wir (minus z) als $-z := [(b, a)]$. Dann ist $-(-z) = z \quad \forall\ z \in \mathbb{Z}$.
$z \in \mathbb{N}$ und $-z \in \mathbb{N} \iff z = 0$

Selbsttest

Zeige: Für $z \in -\mathbb{N}_{>0}$ ist $-z \in \mathbb{N}_{>0}$.

III Verknüpfungen auf $\mathbb{Z}$

3.1 Definition (Addition auf $\mathbb{Z}$)

$$[(a, b)] + [(c, d)] := [(a + c, b + d)]$$

Die *Addition auf* $\mathbb{Z}$ ist eine Verknüpfung

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

3.2 Satz ($\mathbb{Z}$ mit Addition ist abelsche Gruppe)

Die Menge $\mathbb{Z}$ mit der Addition $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit neutralem Element $0 := [(0,0)]$ und Inversem $-z = [(b,a)]$ zum Element $z = [(a,b)]$.

$\forall\ a \in \mathbb{Z}\ \exists!\ z \in \mathbb{Z}\colon\ z + a = a + z = 0 \implies z = -a$

3.3 Wichtige Eigenschaften von Gruppen

- Kürzungsregel: $\forall\ a,b,c \in \mathbb{Z}\colon\ a + c = b + c \iff a = b$
- (additive) Gleichung: $\exists!$ Lösung $x \in \mathbb{Z}$ für $a + x = b$ mit $a, b, \in \mathbb{Z}$
- Inverses des Inversen: $\forall\ a \in \mathbb{Z}\colon\ -(-a) = a$

3.4 Definition (Subtraktion auf $\mathbb{Z}$)

Die *Subtraktion auf* $\mathbb{Z}$ ist eine Verknüpfung

$$-\colon \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$\forall\ a, g \in \mathbb{Z}\colon\ a - b := a + (-b)$
Die Subtraktion ist NICHT kommutativ, hat KEIN neutrales Element und ist nicht Assoziativ! Multiplikation ist bzgl. Subtraktion distributiv.

3.5 Definition (Multiplikation auf $\mathbb{Z}$)

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ [(a,b)] \cdot [(c,d)] := [(ac + bd, ad + bc)]$$

$\implies z \cdot 0 = 0 \quad \forall\ z \in \mathbb{Z}$

3.6 Satz (Multiplikation auf$\mathbb{Z}$)

Die Multiplikation auf $\mathbb{Z}$ ist assoziativ, kommutativ und besitzt das neutrale Element $1 := [(1,0)]$.

$(\mathbb{Z}, \cdot)$ ist ein abelsches Monoid.
Notation: $a \cdot b = ab$

3.7 Satz (Ring $\mathbb{Z}$)

$(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich, d. h. ein kommutativer Ring mit Eins und nullteilerfrei.

$$\forall\ a,b \in \mathbb{Z}\colon\ (-a)b = a(-b) = -(ab) \quad , \quad (-a)(-b) = ab$$

Insbesondere gelten:

$$1 = (-1)(-1) = 1 \cdot (-(-1)) = -(-1) \quad , \quad -a = (-1)a = 1(_a) \quad \forall\ a \in \mathbb{Z}$$

$\mathbb{Z}$ Integritätsbereich $\Longrightarrow$ Kürzungsregel für Multiplikation

$$c \neq 0\colon\ ac = bc \implies a = b$$

IV Die Anordnung der ganzen Zahlen

- $\geq$: Für $a, b \in \mathbb{Z}$ schreiben wir $a \geq b$, falls $a = b + x$ eine Lösung $x \in \mathbb{N}$ hat.
- $>$: Für $a, b \in \mathbb{Z}$ schreiben wir $a > b$, falls $a \geq b$ und $a \neq b$.
- $\leq$: Für $a, b \in \mathbb{N}$ schreiben wir $a \leq b$, falls $a \geq b$.
- $<$: Für $a, b \in \mathbb{N}$ schreiben wir $a < b$, falls $a > b$.

4.1 Proposition (Relation bzgl. $\mathbb{Z}$und $\mathbb{N}$)

$$\forall\ a, b \in \mathbb{Z}\colon\ a \geq b \iff a - b \in \mathbb{N}$$

4.2 Satz (Eigenschaften Anordnung)

Die Relation $\geq$ (analog für $\leq$) ist

- reflexiv
- antisymmetrisch
- transitiv
- total

Die Raltaion $>$ (analog für $<$) ist

- irreflexiv
- transitiv
- konnex

4.3 Satz (Monotonie)

$\forall\ a, b, c \in \mathbb{Z}$ gelten:

- $a \geq b \implies a + c \geq b + c$ $\qquad$ $a \leq b \implies a + c \leq b + c$
- $a > b \implies a + c > b + c$ $\qquad$ $a < b \implies a + c < b + c$
- $c \geq 0\colon\ a \geq b \implies ac \geq bc$ $\qquad$ $a \leq b \implies ac \leq bc$
- $c > 0\colon\ a > b \implies ac > bc$ $\qquad$ $a < b \implies ac < bc$
- $c \leq 0\colon a \geq b \implies ac \leq bc$ $\qquad$ $a \leq b \implies ac \geq bc$
- $c < 0\colon\ a > b \implies ac < bc$ $\qquad$ $a < b \implies ac > bc$

V Die Betragsfunktion

5.1 Definition (Betrag)

$$|.|: \mathbb{Z} \longrightarrow \mathbb{N}\ ,\ |a| = \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0 \end{cases}$$

Analoge Definition: $\{|a|\} = \{a, -a\} \cap \mathbb{N}$
Betrag ist auf $\mathbb{N}$ surjektiv.
Betrag ist NICHT injektiv.

5.2 Satz (Betragsregeln)

Seien $a, b \in \mathbb{Z}$.

- $|a| \geq 0$
- $|a| = 0 \iff a = 0$
- $|a| = |-a|$
- $|ab| = |a||b|$
- $||a| - |b|| \leq |a + b| \leq |a| + |b|$

Seien $a_1, \ldots, a_n \in \mathbb{Z}$. Dann gilt

$$\left| \sum_{i=1}^{n} a_i \right| \leq \sum_{i=1}^{n} |a_i|$$

VI Potenzen

Erweiterung der Definition von Potenzen mit Basis $\mathbb{N}$ auf Basis $\mathbb{Z}$.

6.1 Satz (Rechenregeln der Potenz)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$ und seien $n, m \in \mathbb{N}$. Dann gelten:

- $a^n \cdot a^m = a^{n+m}$
- $(a^n)^m = a^{n \cdot m}$
- $(ab)^n = a^n \cdot b^n$

$$\forall\ n \in \mathbb{N}\colon\ (-1)^n = \begin{cases} 1 & \text{falls } n \text{ gerade} \\ -1 & \text{falls } n \text{ ungerade} \end{cases}$$

Konsequenz:

$$\forall\ a \in \mathbb{Z} \setminus \{0\} \quad \forall \mathbb{N}\colon\ (-a)^n = \begin{cases} a^n & \text{falls } n \text{ gerade} \\ -a^n & \text{falls } n \text{ ungerade} \end{cases}$$

VII Schranken

7.1 Definition (Minimum, Maximum, Schranke, beschränkt)

Sei $M \subseteq \mathbb{Z}$ eine nicht-leere Teilmenge. Ein *Minimum* (*Maximum*) für M ist ein $a \in M$: $a \leq m$ $(a \geq m) \quad \forall\, m \in M$.

Eine *untere Schranke* (*obere Schranke*) von M ist ein $b \in \mathbb{Z}$: $b \leq m$ $(b \geq m) \quad \forall\, m \in M$.

M heißt *nach unten beschränkt* (*nach oben beschränkt*), falls es eine untere Schranke (obere Schranke) gibt.

Ein Minimum (Maximum) ist insbesondere eine untere (obere) Schranke.
Das Minimum/Maximum ist eindeutig bestimmt.

7.2 Satz (endliche Teilmenge – Genau ein Minimum und ein Maximum)

nicht-leere Teilmenge $M \subseteq \mathbb{Z}$ endlich $\Longrightarrow$ $\exists!$ Maximum und $\exists!$ Minumum von M

7.3 Satz (untere Schranke/obere Schranke – Minimum/Maximum)

nicht-leere Teilmenge $M \subseteq \mathbb{Z}$ nach unten/oben beschränkt $\Longrightarrow$ M hat ein Minimum/Maximum

§ 9
Teilbarkeit in $\mathbb{Z}$

I Division mit Rest in $\mathbb{Z}$

1.1 Satz (Division mit Rest)

Seien a, b im $\mathbb{Z}$ mit $b \neq 0$. Dann gibt es zu a, b genau ein geordnetes Paar (q, r) von ganzen Zahlen mit

$$a = qb + r \quad \text{mit } 0 \leq r < |b|$$

wobei q der unvollständige Quotient von a druch b und r den Divisionsrest bezeichnen.
Quotient und Rest sind eindeutig.

II Definition der Teilbarkeit

2.1 Definition (teilbar)

Seien $a, b \in \mathbb{Z}$. a ist durch b *teilbar*, wenn es ein $t \in \mathbb{Z}$ mit $a = tb$ gibt.

2.2 Proposition (äquivalente Aussagen)

Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Dann sind folgende Aussagen äquivalent:

(i) $\exists t \in \mathbb{Z}$: $a = tb$

(ii) Rest der Division $a : b$ ist Null

(iii) $\frac{a}{b} \in \mathbb{Z}$

a ist durch b teilbar $\iff b \mid a \iff a$ ist ein *Vielfaches* von b
Wenn b die Zahl a NICHT teilt, schreiben wir: $b \nmid a$

III Eigenschaften der Teilbarkeitsrelation

Teilbarkeit ergibt eine Relation auf $\mathbb{Z}$: Paare $(a, b) \in \mathbb{Z} \times \mathbb{Z}$: $a \mid b$

3.1 Satz (Eigenschaften der Teilbarkeitsrelation)

Die Teilbarkeitsrelation ist

- reflexiv
- transitiv
- NICHT symmetrisch
- NICHT antisymmetrisch

3.2 Satz („fast“ antisymmetrische Teilbarkeitsrelation)

Seien $a, b, \in \mathbb{Z}$.

$$a \mid b \quad \wedge \quad b \mid a \implies |a| = |b| \quad (a = \pm b)$$

Die Einschränkung der Teilbarkeitsrelation auf $\mathbb{N}_{>0}$ ist somit antisymmetrisch.

IV Weitere Eigenschaften

4.1 Proposition (Minus, Betrag)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann gilt:

$$a \mid b \iff a \mid -b \iff -a \mid b \iff -a \mid -b \iff |a| \mid |b|$$

4.2 Proposition (Produkt, Kürzen)

Seien $a, b, c, d \in \mathbb{Z} \setminus \{0\}$.

$$a \mid b \quad \wedge \quad c \mid d \implies ac \mid bd$$

Insbesondere gilt

$$a \mid b \overset{c \neq 0}{\iff} ac \mid bc$$

4.3 Proposition (Linearkombinationen)

Seien $a, b, c \in \mathbb{Z} \setminus \{0\}$.

$$a \mid b \ \wedge \ a \mid c \implies a \mid (bx + cy) \quad \forall\, x, y \in \mathbb{Z}$$

Insbesondere gilt

$$a \mid (b + c) \qquad , \qquad a \mid (b - c)$$

4.4 Proposition (Beschränkung der Teiler)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$.

$$a \mid b \implies |a| \leq |b|$$

V Teilermengen

Für $a \in \mathbb{Z}$ schreiben wir $\mathcal{T}(a)$ für die *Teilermenge*, d. h. die Menge der Teiler von a.
$\mathcal{T}^+(a)$ sei die Menge der positiven Teiler; $\mathcal{T}^-(a)$ die Menge der negativen Teiler.

5.1 Proposition (Teilermenge)

$\forall\, a \in \mathbb{Z} \setminus \{0\}$ gelten:

(1) $0 \notin \mathcal{T}(a)$
Insbesondere ist $\mathcal{T}^+(a)$ ($\mathcal{T}^-(a)$) auch die Menge der streng positiven (negativen) Teiler.
$\mathcal{T}^+(a)$ und $\mathcal{T}^-(a)$ ergeben eine Partition von $\mathcal{T}(a)$.

(2) $\mathcal{T}(a) = -\mathcal{T}(a)$
Dann ist $\mathcal{T}^-(a) = -\mathcal{T}^+(a)$ und $\mathcal{T}^+(a) = -\mathcal{T}^-(a)$

(3) $\mathcal{T}(a) \supseteq \{1, -1, a, -a\}$
Insbesondere ist $\mathcal{T}^+(a) \supseteq \{1, |a|\}$ und $\mathcal{T}^-(a) \supseteq \{-1, -|a|\}$

(4) $\mathcal{T}^+(a) \subseteq \{1, 2, \ldots, |a|\}$ und $\mathcal{T}^-(a) \subseteq \{-1, -2, \ldots, -|a|\}$
Dann ist $\mathcal{T}(a)$ eine endliche Menge mit höchstens $2|a|$ Elementen.

(5) $\mathcal{T}(a) = \mathcal{T}(-a) = \mathcal{T}(|a|)$

5.2 triviale und echte Teiler

triviale Teiler von a: $\pm 1, \pm a$
echte Teiler von a: alle diejenigen ganzen Zahlen, die KEINE trivialen Teiler sind

Selbsttest

Beweise: $a \neq 0$ und b echter Teiler von $a \implies \left(|b| \leq \frac{1}{2}|a| \iff 2|b| \leq |a|\right)$
Insbesondere gelte $|b| < |a|$.
Hinweis: $a = tb$, $b \neq 0, \pm a \implies |t| > 1$, also $|a| = |t||b| \geq 2|b|$.

VI Linearkombinationen von ganzen Zahlen

Sei $a \in \mathbb{Z}$. Die Menge

$$a\mathbb{Z}. = \left\{ ax \;\middle|\; x \in \mathbb{Z} \right\} \subseteq \mathbb{Z}$$

ist die Menge der *Vielfachen* von a.

Selbsttest

Beweise: $\forall\, a \in \mathbb{Z}$ gelten: $a\mathbb{Z} = (-a)\mathbb{Z}$ und $\{a, -a\} \subseteq a\mathbb{Z}$

Selbsttest

Beweise: $\forall\, a, b \in \mathbb{Z}$: $a\mathbb{Z} \subseteq b\mathbb{Z} \iff b \,\big|\, a$
Hinweis: beweise zuerst: $a\mathbb{Z} \subseteq b\mathbb{Z} \iff a \in b\mathbb{Z}$

6.1 Definition (Linearkombinationen)

Seien $a, b \in \mathbb{Z}$. Die Menge

$$a\mathbb{Z} + b\mathbb{Z} := \left\{ ax + by \;\middle|\; x, y \in \mathbb{Z} \right\} \subseteq \mathbb{Z}$$

ist die Menge aller *Linearkombinationen* von a und b mit ganzen Zahlen als Koeffizienten.

▽ Linearkombination positiv $\not\Longrightarrow$ Koeffizienten positiv
•
Koeffizienten sind NICHT eindeutig!

6.2 Proposition (Abgeschlossenheit)

Seien $a, b \in \mathbb{Z}$. Die Menge $a\mathbb{Z} + b\mathbb{Z}$ ist bzgl. Vielfachen, Summen und Produkten abgeschlossen.

Selbsttest

Kombinationen von Kombinationen von a und b sind wieder Kombinationen von a und b.
Hinweis: Diese Aussage folgt aus obiger Proposition bzgl. Abgeschlossenheit. ODER direkt, falls $m = ax + by$ und $n = ax' + by'$, dann ist $cm + dn = \ldots$

Selbsttest

Beweise:

- Es gelten: $(a\mathbb{Z} + b\mathbb{Z}) = (b\mathbb{Z} + a\mathbb{Z})$ und $(a\mathbb{Z} + b\mathbb{Z}) = -(a\mathbb{Z} + b\mathbb{Z}) = \mathbb{Z}(|a|) + \mathbb{Z}(|b|)$
- $(a\mathbb{Z} + b\mathbb{Z}) \subseteq b\mathbb{Z} \iff b \,\big|\, a$

6.3 Definition (Kombinationen)

Seien $a_, \ldots, a_n \in \mathbb{Z}$ mit $n \geq 1$. Wir definieren die *Kombinationen* von $a_1, \ldots, a_n$ als die Elemente der Menge

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_n\mathbb{Z} = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; x_i \in \mathbb{Z} \right\} \subseteq \mathbb{Z}$$

Auch diese Menge ist bzgl. Vielfachen, Summen und Produkten abgeschlossen.
Die Kombinationen von Kombinationen der Zahlen $a_1, \ldots, a_n$ sind wieder Kombinationen der Zahlen $a_1, \ldots, a_n$.

§ 10
ggT und kgV

I Drei äquivalente Definitionen des ggT

1.1 Definition (**ggT**)

Seien $a, b \in \mathbb{Z}$. Für $a = b = 0$ ist $\mathrm{ggT}(a, b) := 0$. Für a, b nicht beide Null definieren wir den ggT wie folgt: Es sind äquivalent:

(1) Maximum der Menge der gemeinsamen Teiler

$$\max\left(\mathcal{T}(a) \cap \mathcal{T}(b)\right)$$

(2) einziger, streng positiver, gemeinsamer Teiler d, der durch jeden gemeinsamen Teiler teilbar ist; es gelten folgende Eigenschaften für d:

(i) $d \,\middle|\, a$ und $d \,\middle|\, b$

(ii) $\forall\, t \in \mathbb{Z}\colon\ t \,\middle|\, a \ \wedge\ t \,\middle|\, b \implies t \,\middle|\, d$

(iii) $d > 0$

(3) kleinste streng positive Linearkombination

$$\min\left((a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{Z}_{>0}\right)$$

Notation: Schreibe (a, b) oder $\mathrm{ggT}(a, b)$ für den ggT von a und b.

II Eigenschaften ggT

- **Reihenfolge:** $\forall\, a, b \in \mathbb{Z}\colon\ (a, b) = (b, a)$
- **gemeinsame Teiler sind genau die Teiler des ggT**
  $\forall\, a, b \in \mathbb{Z}\colon\ \mathcal{T}(a) \cap \mathcal{T}(b) = \mathcal{T}\big((a, b)\big)$

- **Linearkombinationen sind genau die Vielfachen des ggT**
  $\forall\ a, b \in \mathbb{Z}\colon\ a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$
- **Vorzeichen:** $\forall\ a, b \in \mathbb{Z}\colon\ (a, b) = (|a|, |b|)$
  folglich gilt: $(a, b) = (-a, b) = (-a, -b) = (a, -b)$
- **Ungleichung:** $\forall\ a, b \in \mathbb{Z}\colon\ 0 \leq (a, b) \leq \min\{|a|, |b|\}$
  $\forall\ a, b \in \mathbb{Z}$, nicht beide Null, gilt: $1 \leq (a.b) \leq \min\{|a|, |b|\}$
- **Teilbarkeit und ggT:** $\forall\ a, b \in \mathbb{Z}\colon\ a \mid b \iff (a, b) = |a|$
  folglich gilt: $(a, 1) = 1$ und $(a, a) = |a|$ und $(a, 0) = |a|$
- **gemeinsame Faktoren:** $\forall\ a, b, c \in \mathbb{Z}\colon\ (ac, bc) = |c| \cdot (a, b)$
- **ggT und Rest:** $\forall\ a, b \in \mathbb{Z}\colon\ (a, b + ax) = (a, b) \quad \forall\ x \in \mathbb{Z}$
  insbesondere: $(a, b) = (a, b - a)$ und $(a, b) = (a, r)$, wobei r der Rest von $b : a$ ist.

Seien $a, b \in \mathbb{Z}$. Dann kann man den $\mathrm{ggT}(a, b)$ auch folgendermaßen definieren: es sind äquivalent:

- einzige positive ganze Zahl d, sodass $\mathcal{T}(a) \cap \mathcal{T}(b) = \mathcal{T}(d)$
- einzige positive ganze Zahl d, sodass $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

III Teilerfremde Zahlen

Seien $a, b \in \mathbb{Z}$ und $(a, b) = 1$. Dann heißen a und b *teilerfremd*.
Ganze Zahlen $a_1, \ldots, a_n$ heißen *paarweise teilerfremd*, falls $\forall\ i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt: $\mathrm{ggT}(a_i, a_j) = 1$

3.1 Proposition (Teilerfremde Zahlen)

Seien $a, b \in \mathbb{Z}$. Dann sind äquivalent:

(i) $(a, b) = 1$

(ii) gemeinsame Teiler von a und b sind -1 und 1

(iii) jede ganze Zahl ist eine Kombination von a und b, d. h. $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

(iv) 1 ist eine Kombination von a und b, d. h. $\exists x, y \in \mathbb{Z}\colon\ 1 = ax + by$

IV Der ggT mehrerer ganzer Zahlen

4.1 Definition (ggT meherer ganzer Zahlen)

Sei $n \geq 2$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Für $a_1 = \ldots = a_n = 0$ ist $\mathrm{ggT}(0, 0, \ldots, 0) := 0$. Für $a_1, \ldots, a_n$ nicht alle Null definieren wir den ggT wie folgt: Es sind äquivalent:

(a) Maximum der Menge $\bigcap_{i=1}^{n} \mathcal{T}(a_i)$

(b) einzige Zahl $d \in \mathbb{Z}$ mit folgenden Eigenschaften:

(i) $d \mid a_i \quad \forall\, i$

(ii) $t \mid a_i \quad \forall\, i \implies t \mid d$

(iii) $d > 0$

(c) kleinste streng positive Kombination der a_i

V Eigenschaften ggT mehrerer ganzer Zahlen

Seien $a_1, \ldots, a_n \in \mathbb{Z}$ mit $n \geq 2$. Dann gelten:

- **Reihenfolge:** Sei f eine bijektive Funktion von $\{1, \ldots, n\}$ nach $\{1, \ldots, n\}$. Dann gilt:

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_{f(1)}, \ldots, a_{f(n)})$$

- **gemeinsame Teiler sind genau die Teiler des ggT**

$$\bigcap_{i=1}^{n} \mathcal{T}(a_i) = \mathcal{T}\big(\mathrm{ggT}(a_1, \ldots, a_n)\big)$$

- **Linearkombinationen sind genau die Vielfachen des ggT**

$$a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = \big(\mathrm{ggT}(a_1, \ldots, a_n)\big)\mathbb{Z}$$

- **Vorzeichen:** $\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(|a_1|, \ldots, |a_n|)$

- **Ungleichung:** $0 \leq \mathrm{ggT}(a_1, \ldots, a_n) \leq \min\limits_{i \in I}\{|a_i|\}$
  Sind nicht alle $a_1, \ldots, a_n$ Null, so gilt: $1 \leq \mathrm{ggT}(a_1, \ldots, a_n) \leq \min\limits_{i \in I}\{|a_i|\}$

- **gemeinsame Faktoren:** $\forall\, c \in \mathbb{Z}$: $\mathrm{ggT}(ca_1, \ldots, ca_n) = |c| \cdot \mathrm{ggT}(a_1, \ldots, a_n)$

Sei $n \geq 2$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Dann kann man den $\mathrm{ggT}(a, b)$ mehrere ganzer Zahlen auch folgendermaßen definieren: es sind äquivalent:

- einzige positive ganze Zahl d, sodass $\bigcap\limits_{i=1}^{n} \mathcal{T}(a_i) = \mathcal{T}(d)$
- einzige positive ganze Zahl d, sodass $a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = d\mathbb{Z}$

VI Der ggT als Verknüpfung

$$\mathrm{ggT}\colon\ \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ a * b = \mathrm{ggT}(a, b) \quad \forall\, a, b \in \mathbb{Z}$$

ist kommutativ und assoziativ.

6.1 Rekursive Definition des ggT

Sei $n \geq 2$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Dann ist

$$\mathrm{ggT}(a_1, \ldots, a_n) := a_1 * \ldots * a_n$$

∇ $a_1, \ldots, a_n$ paarweise teilerfremd $\implies$ $\mathrm{ggT}(a_1, \ldots, a_n) = 1$

VII Das kleinste gemeinsame (streng positive) Vielfache

7.1 Definition (kgV)

Seien $a, b \in \mathbb{Z}$. Sind a oder b gleich Null, so ist $\mathrm{kgV}(a, b) := 0$. Falls a und b von Null verschhieden sind, definiert man das kgV von a und b wie folgt: Es sind äquivalent:

(1) Minimum der Menge $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{Z}_{>0}$

(2) eindeutig bestimmtes $m \in \mathbb{Z}$ mit folgenden Eigenschaften:

(i) $a \mid m$ und $b \mid m$

(ii) $a \mid b$ und $b \mid t \implies m \mid t$

(iii) $m > 0$

Notation: Schreibe $\mathrm{kgV}(a, b)$ für das kgV von a und b.

VIII Eigenschaften kgV

- **Reihenfolge:** $\forall\, a, b \in \mathbb{Z}$: $\mathrm{kgV}(a, b) = \mathrm{kgV}(b, a)$
- **gemeinsame Vielfache sind die Vielfachen des kgV**
  $\forall\, a, b \in \mathbb{Z}$: $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{kgV}(a, b)\mathbb{Z}$
- **Vorzeichen:** $\forall\, a, b \in \mathbb{Z}$: $\mathrm{kgV}(a, b) = \mathrm{kgV}(|a|, |b|)$
  folglich gilt: $\mathrm{kgV}(a, b) = \mathrm{kgV}(-a, b) = \mathrm{kgV}(-a, -b) = \mathrm{kgV}(a, -b)$
- **Teilbarkeit und kgV:** $\forall\, a, b \in \mathbb{Z}$: $b \mid a \iff \mathrm{kgV}(a, b) = |a|$
  insbesondere: $\mathrm{kgV}(a, 1) = |a|$ und $\mathrm{kgV}(a, a) = |a|$
- **gemeinsame Faktoren:** $\forall\, a, b, c \in \mathbb{Z}$: $\mathrm{kgV}(ac, bc) = |c| \cdot \mathrm{kgV}(a, b)$

Seien $a, b \in \mathbb{Z}$. Dann kann man $\mathrm{kgV}(a, b)$ auch definieren als

- einzige positive ganze Zahl m mit $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

IX Das kgV mehrerer ganzer Zahlen

9.1 Definition (kgV meherer ganzer Zahlen)

Sei $n \geq 2$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Für ein oder mehrere der a_i gleich Null ist $\mathrm{kgV}(a_1, \ldots, a_n) := 0$. Für $a_1, \ldots, a_n$ alle von Null verschieden definieren wir das kgV wie folgt: Es sind äquivalent:

(a) Minimum der Menge $\bigcap_{i=1}^{n} a_i\mathbb{Z} \cap \mathbb{N}_{>0}$

(b) einzige Zahl $m \in \mathbb{Z}$ mit folgenden Eigenschaften:

(i) $a_i \mid m \quad \forall\, i$

(ii) $a_i \mid t \quad \forall\, i \implies m \mid t$

(iii) $m > 0$

X Eigenschaften kgV mehrerer ganzer Zahlen

Seien $a_1, \ldots, a_n \in \mathbb{Z}$ mit $n \geq 2$. Dann gelten:

- **Reihenfolge:** Sei f eine bijektive Funktion von $\{1, \ldots, n\}$ nach $\{1, \ldots, n\}$. Dann gilt:

$$\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(a_{f(1)}, \ldots, a_{f(n)})$$

- **gemeinsame Vielfache sind die Vielfachen des kgV**

$$\bigcap_{i=1}^{n} a_i\mathbb{Z} = \mathrm{kgV}(a_1, \ldots, a_n)\mathbb{Z}$$

- **Vorzeichen:** $\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(|a_1|, \ldots, |a_n|)$
- **Ungleichung:** $\max\limits_{i \in I}\{|a_i|\} \leq \mathrm{ggT}(a_1, \ldots, a_n) \leq \prod\limits_{i \in I} |a_i| = |a_1 \cdot \ldots \cdot a_n|$
- **gemeinsame Faktoren:** $\forall\, c \in \mathbb{Z}\colon \quad \mathrm{kgV}(ca_1, \ldots, ca_n) = |c| \cdot \mathrm{kgV}(a_1, \ldots, a_n)$

Sei $n \geq 2$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Dann kann man das $\mathrm{kgV}(a, b)$ mehrere ganzer Zahlen auch definieren als:

- einzige positive ganze Zahl m mit $\bigcap_{i=1}^{n} a_i\mathbb{Z} = m\mathbb{Z}$

XI Das kgV als Verknüpfung

$$\mathrm{kgV}\colon \ \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}\ , \ a * b = \mathrm{kgV}(a, b) \quad \forall\, a, b \in \mathbb{Z}$$

ist kommutativ und assoziativ.

11.1 Rekursive Definition des kgV

Sei $n \geq 2$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Dann ist

$$\mathrm{kgV}(a_1, \ldots, a_n) := a_1 * \ldots * a_n$$

XII Beziehung zwischen ggT und kgV

Seien $a, b \in \mathbb{Z}$. Dann gilt:

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = |ab|$$

12.1 Lemma (Teilbarkeit)

Für $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ mit $ab = cd$ gilt:

$$a \mid c \implies d \mid b$$

§ 11
Euklidischer Algorithmus und Lineare Diophantische Gleichungen

I Der euklidische Algorithmus

Unter einem *Algorithmus* versteht man einen Rechenvorgang, der nach einem bestimmten Schema in endlich vielen elementaren Schritten abläuft. Jeder Algorithmus kann prinzipiell von Rechenmaschinen durchgeführt werden. Der *euklidische Algorithmus* berechnet sehr schnell den ggT von zwei ganzen Zahlen und berechnet diesen als Kombination der zwei Zahlen.

1.1 Berechnung des ggT

Man kann die Berechnung auf den Fall $a \geq b > 0$ zurückführen:

- a oder b gleich Null: $a = 0 \implies \text{ggT}(ab) = |b|$ und $b = 0 \implies \text{ggT}(a, b) = |a|$
- Negative Zahlen: $(a, b) = (|a|, |b|)$
- Anordnung: $a < b \implies (a, b) = (b, a)$

1.2 Satz (Euklidischer Algorithmus für den **ggT**)

Seien $a \geq b > 0$. Definiere $a_n \in \mathbb{Z}$ mit $n \geq 0$ wie folgt: setze $a_0 = a$ und $a_1 = b$. Für $n \geq 2$ und $a_{n-1} \neq 0$ definiere a_n als Rest der Division $a_{n-2} : a_{n-1}$. Dann gibt es ein kleinstes $n \geq 3$ mit $a_n = 0$ und wir haben $(a, b) = a_{n-1}$.

Zusammenfassung: Seien $a \geq b > 0$.

$a_0 := a$

$a_1 := b$

$a_2 :=$ Rest von $a_0 : a_1$

...

$a_n :=$ Rest von $a_{n-2} : a_{n-1}$

Sobald $a_n = 0 \implies (a, b) = a_{n-1}$

1.3 Lemma (ggT)

Seien $\alpha, \beta\gamma, h \in \mathbb{Z}$ mit $\alpha = h\beta + \gamma$. Dann gilt: $(\alpha, \beta) = (\beta, \gamma)$

1.4 Berechnung des ggT als Kombination von Zahlen

Bemerkung: Diese Berechnung folgt aus obiger Berechnung des ggT!

Seien $a \geq b > 0$. Definiere $a_n \in \mathbb{Z}$ mit $n \geq 0$ wie folgt: setze $a_0 = a$ und $a_1 = b$. Für $n \geq 2$ und $a_{n-1} \neq 0$ definiere a_n als Rest der Division $a_{n-2} : a_{n-1}$. Dann gibt es ein kleinstes $n \geq 3$ mit $a_n = 0$ und wir haben $\mathrm{ggT}(a, b) = a_{n-1}$.

Zusammenfassung: Seien $a \geq b > 0$ und sei $x_i \in \mathbb{Z}$ mit $i \in \mathbb{N}$.

$a_0 := a$

$a_1 := b$

$a_0 = x_1 \cdot a_1 + a_2$

$a_1 = x_2 \cdot a_2 + a_3$

$\ldots a_{n-2} = x_{n-1} a_{n-1} + a_n$

Sobald $a_n = 0 \implies \mathrm{ggT}(a, b) = a_{n-1}$

1.5 Beispiel (Euklidischer Algorithmus)

$a := 12 (= a_0)$; $b := 50 (= a_1)$
$\mathrm{ggT}(a, b) = xa + yb$

$$
\begin{array}{lccccccc}
(0) & \underset{(a_0)}{12} & = & \underline{0} & \cdot & \underset{(a_1)}{50} & + & \underset{(a_2)}{\underline{12}} \\
(1) & \underset{(a_1)}{50} & = & \underline{4} & \cdot & \underset{(a_2)}{12} & + & \underset{(a_3)}{\underline{2}} \\
(2) & \underset{(a_2)}{12} & = & \underline{6} & \cdot & \underset{(a_3)}{2} & + & \underset{(a_4)}{\underline{0}}
\end{array}
$$

$$
\implies \mathrm{ggT}(a, b) = \underbrace{2}_{(a_{n-1}=a_3)} \overset{(1)}{=} 50 - 4 \cdot 12 = \underbrace{(-4)}_{x} \cdot \underbrace{12}_{a} + \underbrace{1}_{y} \cdot \underbrace{50}_{b}
$$

II Lineare diophantische Gleichungen

2.1 Definition (Lineare diophantische Gleichung)

Eine *lineare diophantische Gleichung* ist eine Gleichung der Form

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + \ldots + a_n x_n = \sum_{i=1}^{n} a_i x_i = c$$

mit $n \geq 1$. Variablen $x_1, \ldots, x_n$ und Koeffizienten $a_1, \ldots, a_n$ sind ganze Zahlen.
Der Spezialfall $c = 0$ heißt *homogene lineare diophantische Gleichung.*

2.2 Lösungsmenge

- für uns nur ganzzahlige Lösungen interessant
- Lösungsmenge ist somit Teilmenge von $\mathbb{Z}^n$, wobei n die Anzahl der Variablen bezeichne
- Lösung ist ein n-Tupel von ganzen Zahlen

2.3 Verknüpfungen auf $\mathbb{Z}^n$

Seien $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ beliebig. Dann hat die Menge $\mathbb{Z}^n$ eine Verknüpfung *Summe* und eine Verknüpfung *Produkt*: komponentenweise addition bzw. multiplikation von n-Tupeln:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$$

Sei weiter $m \in \mathbb{Z}$. Dann gilt:

$$m \cdot (a_1, \ldots, a_n) = (ma_1, \ldots, ma_n)$$

Analog kann man auch die Subtraktion definieren:

$$(a_1, \ldots, a_n) - (b_1, \ldots, b_n) = (a_1 - b_1, \ldots, a_n - b_n)$$

2.4 Lemma (Äquivalente Gleichungen)

$\forall\ h \neq 0$ gilt:

$$\sum_{i=1}^{n} a_i x_i = c \iff \sum_{i=1}^{n} (a_i \cdot h) x_i = c \cdot h$$

2.5 Lemma (Superpositionsprinzip für homogene Gleichungen)

Summe, Differenz und Vielfache von Lösungen einer homogenen linearen diophantischen Gleichung sind wieder Lösungen der Gleichung.

2.6 Lemma (Lösbarkeitskriterium für inhomogene Gleichungen)

Bemerkung: Homogene Gleichungen sind immer lösbar, da $(x_1, \ldots, x_n) = (0, \ldots, 0)$ eine Lösung ist. Inhomogene Gleichungen sind NICHT immer lösbar.

$$\sum_{i=1}^{n} a_i x_i = c \text{ lösbar} \iff c \in a_i\mathbb{Z} + \ldots + a_n\mathbb{Z} \iff c = k \cdot \mathrm{ggT}\,(a_1, \ldots, a_n) \quad (k \neq 0)$$

2.7 Satz (Struktur der Lösungsmenge für inhomogene Gleichungen)

Sei $\sum_{i=1}^{n} a_i x_i = c$ eine lösbare lineare diophantische Gleichung.
Die Differenz von zwei Lösungen ist eine Lösung der assoziierten homogenen Gleichung.
Die Summe eine speziellen Lösung der inhomogenen Gleichung und einer beliebigen Lösung der assoziierten homogenen Gleichung ist eine Lösung der inhomogenen Gleichung.
Daher hat die Lösungsmenge folgende Form

$$\mathcal{L} = \Big\{(x_{\text{sp},1} + x_{\text{hom},1}, \ldots, x_{\text{sp},n} + x_{\text{hom},n})\Big\}$$

wobei $(x_{\text{sp},1}, \ldots, x_{\text{sp},n})$ eine fixierte spezielle Lösung der inhomogenen Gleichung ist und $(x_{\text{hom},1}, \ldots, x_{\text{hom},n})$ eine beliebige Lösung der homogenen Gleichung.

III Lineare diophantische Gleichungen mit einer oder zwei Variablen

3.1 Eine Variable, $ax = c$

3.1.1 Homogen

$ax = 0$ mit $a \neq 0$ hat nur die Lösung $x = 0$.
$0x = 0$ hat als Lösungsmenge $\mathbb{Z}$, da jedes $x \in \mathbb{Z}$ eine Lösung ist.

3.1.2 Inhomogen

$ax = c$ mit $x \in \mathbb{Z}$ lösbar $\iff a \mid c$ (laut Definition der Teilbarkeit)
Falls $a \neq 0$ und Gleichung lösbar $\implies \exists!$ Lösung: $c : a$, also $\frac{c}{a} \in \mathbb{Z}$
$0x = c$ ist NICHT lösbar, falls $c \neq 0$. Ist $c = 0$, so hat $0x = 0$ die Lösungsmenge $\mathbb{Z}$.

3.2 Spezialfall Homogen, $ax + by = 0$

$a = b = 0 \implies$ Lösungsmenge $\mathcal{L} = \mathbb{Z}^2$

3.3 Satz (Homogen, $ax + by = 0$)

Seien $a, b \in \mathbb{Z}$ nicht beide Null. Dann hat die Gleichung $ax + by = 0$ die Lösungsmenge

$$\mathcal{L} = \left\{(x, y) \in \mathbb{Z}^2 \;\middle|\; (x, y) = \left(\frac{b}{(a,b)} \cdot t\ ,\ -\frac{a}{(a,b)} \cdot t\right)\ ,\ t \in \mathbb{Z}\right\}$$

3.3.1 Spezialfälle

$a = 0$ und $b \neq 0 \implies$ Lösungen sind Paare $(x, 0)$ mit $x \in \mathbb{Z}$ beliebig, also $\mathcal{L} = \mathbb{Z} \times \{0\}$

$b = 0$ und $a \neq 0 \implies$ Lösungen sind Paare $(0, y)$ mit $y \in \mathbb{Z}$ beliebig, also $\mathcal{L} = \{0\} \times \mathbb{Z}$

3.3.2 Teilerfremde Zahlen

Falls a und b teilerfremd sind, dann ist $(a, b) = 1$, also

$$\mathcal{L} = \left\{ (bt, -at) \;\middle|\; t \in \mathbb{Z} \right\}$$

3.4 Inhomogen, $ax + by = c$

3.4.1 Lösbarkeitskriterium

Eine Lösung zu haben bedeutet, dass c eine Kombination von a und b ist.
Es gibt genau eine Lösung, wenn c ein Vielfaches von (a, b) ist.

3.4.2 Lösungsmenge

Sei $ax + by = c$ lösbar, d. h. $(a, b) \mid c$. Dann ist die Lösungsmenge von der Form

$$\mathcal{L} = \left\{ (x_{\text{sp}} + x_{\text{hom}}, y_{\text{sp}} + y_{\text{hom}} \right\}$$

wobei $(x_{\text{sp}}, y_{\text{sp}})$ eine fixierte spezielle Lösung der inhomogenen Gleichung ist und $(x_{\text{hom}}, y_{\text{hom}})$ eine beliebige Lösung der homogenen Gleichung.
Lösund der homogenen Gleichung ist bereits bekannt $\Longrightarrow$ es reicht, eine spezielle Lösung $(x_{\text{sp}}, y_{\text{sp}})$ zu bestimmen.
Falls $a = b = 0$, dann ist $\mathcal{L} = \mathbb{Z}^2$ für $c = 0$ und $\mathcal{L} = \emptyset$ für $c \neq 0$.
Falls a, b nicht beide Null, dann ist die Lösungsmenge

$$\mathcal{L} = \left\{ \left(x_{\text{sp}} + \frac{b}{(a,b)} \cdot t \;,\; y_{\text{sp}} - \frac{a}{(a,b)} \cdot t \right) \;\middle|\; t \in \mathbb{Z} \right\}$$

3.4.3 Eine spezielle Lösung

Sei $ax + by = c$ lösbar. Lösungen dürfen geraten werden, aber das Ergebnis muss verifiziert werden. Raten ist besonders bei (im Betrag) kleinen Koeffizienten günstig. Schreibe dann

$$c = (a, b) \cdot n \qquad (n \in \mathbb{Z})$$

da die Gleichung lösbar ist.
Bestimme mit Hilfe des euklidischen Algorithmus zwei Zahlen $s_a, s_b \in \mathbb{Z}$, sodass

$$(a, b) = a \cdot s_a + b \cdot s_b$$

Dann ist eine spezielle Lösung der Gleichung das Paar $(s_a n, s_b n) \in \mathbb{Z}^2$.

IV Die Theorie der linearen diophantischen Gleichungen

Alle Gebiete der Mathematik hängen zusammen. Betrachte dazu einzelne Teilgebiete:

4.1 Algebra

Folgende Methoden wurden in diesem Kapitel verwendet:

- Umformungen
- Summe von Lösungen
- Argumentation mit Teilbarkeitsrelation

4.2 Geometrie

- $ax + by = c$ beschreibt eine Gerade g im $\mathbb{R}^2$, falls a und b nicht beide Null sind.
- Lösungen der Gleichung sind Punkte $(x, y) \in g$ mit Koordinaten $x, y \in \mathbb{Z}$
- Lösungsmenge ist $g \cap \mathbb{Z}^2$ mit $\mathbb{Z}^2$ als ganzzahliges Gitter.
- $ax + by = 0$ sind Geraden durch den Ursprung, vertikale Geraden oder Geraden mit rationaler Steigung $-\frac{a}{b} \in \mathbb{Q}$.
- Systeme von Gleichungen:

  (1) $ax + by = c$ ist die Gerade g

  (2) $a'x + b'y = c'$ ist die Gerade g'

  Lösungsmenge ist $\mathcal{L} = (g \cap \mathbb{Z}^2) \cap (g' \cap \mathbb{Z}^2) = g \cap g' \cap \mathbb{Z}^2$
  genau eine (oder keine) Lösung $\iff$ g und g' schneiden sich in einem Punkt
  keine Lösung: $g \parallel g'$
  unendlich viele (oder keine) Lösungen: $g = g'$

4.3 Analysis

- $ax + by = c$ mit $b \neq 0$ ist der Graph der Funktion

$$\mathbb{R} \longrightarrow \mathbb{R} \ , \ x \longmapsto y(x) \ , \ y = -\frac{a}{b} \cdot x + \frac{c}{b}$$

- Betrachte Funktion mit der Definitionsmenge $\mathbb{R}_{>0}$ und finde nützliche Lösungen mit $x > 0$ und $y > 0$.
- Benutze, dass die Gleichung eine monotone Funktion beschreibt und erhalte Lösungen im ersten Quandranten.
- Wächst die Funktion oder ist diese konstant und existiert eine Lösung im ersten Quadranten, dann gibt es dort unendlich viele Lösungen.

- Fällt die Funktion, dann können wir höchstens endlich viele Lösungen im ersten Quadranten finden.
- Analog betrachtet man die anderen Quadranten.

4.4 Lineare Algebra

- lineare diophantische Gleichung (mit n Variablen) ist eine lineare Gleichung mit reellen Koeffizienten
- finde reelle Lösungen der Gleichung: Beschreibung durch $n-1$ reelle Parameter, falls die Gleichung lösbar ist
- somit erhält man eine Hyperebene im $\mathbb{R}^n$, auf der wir Punkte mit ganzzahligen Koordinaten bestimmen wollen
- System von linearen homogenen diophantischen Gleichungen ist ein lineares homogenes System der linearen Algebra
- Lösung durch einige freie ganzzahlige Paramter beschrieben: „Anzahl der Variablen“ minus „Anzahl der unabhängigen Gleichungen“
- Methode der linearen Algebra liefert alle Lösungen in $\mathbb{Q}$ mit Parametern in $\mathbb{Q}$
- Lösung eines Kongruenzsystems nötig; Beschränkung auf ganzzahlige Parameter reicht NICHT aus!

4.5 Algorithmen

- Computer kann prinzipiell Systeme von linearen diophantischen Gleichungen mit n Variablen lösen

§ 12
Die g-adische Darstellung natürlicher Zahlen

Wir sind gewöhnt, natürliche Zahlen im *Dezimalsystem* darzustellen und mit diesen Darstellungen zu rechnen. Dazu führt man zehn Zeichen (*Ziffern*) ein, üblicherweise

$$0\ ,\ 1 := 0'\ ,\ 2 := 1'\ ,\ 3 := 2'\ ,\ 4 := 3'\ ,\ 5 := 4'\ ,\ 6 := 5'\ ,\ 7 := 6'\ ,\ 8 := 7'\ ,\ 9 := 8'$$

Sind $a_0, a_1, \ldots, a_n \in \{0, 1, 2, \ldots, 9\}$ solche Ziffern, $n \geq 1$ und $a_n \neq 0$, so bedeutet die Ziffernfolge

$$a_n a_{n-1} \cdot \ldots \cdot a_1 a_0 \qquad (*)$$

die Zahl

$$a_n \cdot 9'^n + a_{n-1} 9'^{n-1} + \ldots + a_1 9' + a_0$$

Jede Zahl $z \in \mathbb{N}$ hat genau eine Darstellung $(*)$ mit Ziffern aus $\{0, 1, 2, \ldots, 9\}$. Man spricht von der *Dezimaldarstellung* der Zahl z. Hier ist die Grundzahl zehn.

0.6 Satz (System mit Grundzahl in $\mathbb{N}$)

Sei $g \in \mathbb{N}$ mit $g \geq 2$. Dann lässt sich jedes $a \in \mathbb{N}$ eindeutig schreiben in der Form

$$a = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_2 g^2 + a_1 g + a_0$$

wobei $a_0, \ldots, a_n \in \mathbb{N}$ mit $n \geq 0$, $0 \leq n_i < g$ und $a_n \neq 0$ falls $a \neq 0$.

Hat man für die ganzen Zahlen z mit $0 \leq z < g$ Zeichen (Ziffern, Chiffren) vereinbart, so schreibt man für a auch die Aneinanderreihung der betreffenden Zeichen für $a_0, \ldots, a_n$:

$$a_n a_{n-1} \ldots a_1 a_0$$

bedeutet die Zahl

$$a_n g^n + a_{n-1} g^{n-1} + \ldots + a_2 g^2 + a_1 g + a_0 = a$$

Beide Schreibweisen nennt man die *g-adische Darstellung* von a.

Zur Unterscheidung der verschiedenen Systeme kann man einen Index g für die g-adische Ziffernfolge angeben, z. B.

$$(1537)_{10} = (2087)_9$$

0.7 Definition (Quersumme, alternierende Quersumme)

(a) Die *Quersumme* von a (bzgl. g) ist die Zahl

$$\mathcal{Q}(a) := a_0 + a_1 + \ldots + a_n$$

(b) Die *alternierende Quersumme* von a (bzgl. g) ist die Zahl

$$\mathcal{Q}'(a) := a_0 - a_1 + \ldots + (-1)^n a_n$$

0.8 Satz (Quersumme äquivalent modulo)

$$a \equiv \mathcal{Q}(a) \mod (g-1) \quad \text{und} \quad a \equiv \mathcal{Q}'(a) \mod (g+1)$$

§ 13
Primzahlen und der Fudamentalsatz der Arithmetik

I Definitionen

1.1 Definition (Primzahl)

Eine natürliche Zahl p heißt *Primzahl*, falls die folgenden Eigenschaften gelten:

(1) $p > 1$

(2) p hat keine echten Teiler.

Menge der Primzahlen schreiben wir als

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19 \ldots\}$$

Sei $p \in \mathcal{P}$. Da p KEINE echten Teiler hat, sind die Teiler von p genau die trivialen Teiler, also

$$\mathcal{T}(p) = \{1, -1, p, -p\}$$

Wegen $p > 1$ folgt $p \neq \pm 1$ und es gilt: $\#\mathcal{T}(p) = 4$. Wegen $p \geq 0$ folgt

$$\mathbb{T}^+(p) = \{1, p\}$$

und $\#\mathcal{T}^+(p) = 2$.

$$p \in \mathbb{Z} \text{ mit } p > 1 \text{ Primzahl } \iff \#\mathcal{T}(p) = 4 \iff \#\mathcal{T}^+(p) = 2$$

Ferner gilt:

$$p \in \mathbb{Z} \text{ mit } p > 1 \text{ Primzahl } \iff p \text{ hat KEINE echten positiven Teiler}$$

1.2 Definition (Unzerlegbarkeitseigenschaft von Primzahlen)

Eine natürliche Zahl p heißt *Primzahl*, falls folgende Eigenschaften gelten:

(1) $p > 1$

(2) $p = ab$ mit $a, b \in \mathbb{N} \implies a = 1$ oder $b = 1$

II Primeigenschaft

2.1 Lemma (Primeigenschaft)

Sei $p \in \mathcal{P}$ und sei $a \in \mathbb{Z}$. Dann ist

$$(a,p) = \begin{cases} 1 & \text{falls } p \nmid a \\ p & \text{falls } p \mid a \end{cases}$$

2.2 Definition (Primzahl)

Eine natürliche Zahl heißt *Primzahl*, falls die folgenden Eigenschaften gelten:

(1) $p > 1$

(2) $p \mid ab$ mit $a, b \in \mathbb{Z} \implies p \mid a \quad \vee \quad p \mid b$

2.3 Satz (Produkt)

Sei $p \in \mathcal{P}$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$ mit $n \geq 1$. Dann gilt:

$$p \mid a_1 \cdot \ldots \cdot a_n \implies \exists\, i_0 \in \{1, \ldots, n\}\colon\ p \mid a_{i_0}$$

2.4 Korollar (Potenz)

Sei $p \in \mathcal{P}$ und seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}_{\geq 1}$. Dann gilt:

$$p \mid a^n \implies p \mid a$$

2.5 Korollar (Zwei Primzahlen)

Seien $p, q \in \mathcal{P}$ und $n \in \mathbb{N}_{\geq 1}$. Dann gilt:

$$p \mid q^n \iff p = q$$

2.6 Korollar (Produkt von Primzahlen)

Seien $p, q_1, \ldots, q_n \in \mathcal{P}$ und $n \in \mathbb{N}_{\geq 1}$. Dann gilt:

$$p \mid \prod_{i=1}^{n} q_i \implies \exists\, i_0 \in \{1, \ldots, n\}\colon\ p = q_{i_0}$$

Selbsttest

Sei $p \in \mathcal{P}$. Dann ist p die einzige Primzahl, die durch p teilbar ist.

Selbsttest

Sei $a \in \mathbb{Z}$. Dann ist $a\mathbb{Z} \cap \mathcal{P}$ nicht-leer, nur wenn $a = \pm 1$ ($a\mathbb{Z} \cap \mathcal{P} = \mathcal{P}$) oder wenn $|a| \in \mathcal{P}$ ($a\mathbb{Z} \cap \mathcal{P} = \{|a|\}$).

III Weitere Eigenschaften

3.1 Satz (Der kleinste Teiler größer Eins)

Sei $n \in \mathbb{Z} \setminus \{0, 1, -1\}$. Dann ist

$$\min\left\{\mathcal{T}(n) \cap \mathbb{N}_{>1}\right\} \in \mathcal{P}$$

d. h. der kleinste Teiler größer Eins ist eine Primzahl.
Dies ist entweder $|n|$, falls $|n|$ selbst prim ist oder der kleinste echt positive Teiler t mit $1 < t \leq \sqrt{|n|}$.

3.2 Korollar (Primteiler)

Sei $n \in \mathbb{Z} \setminus \{0, 1, -1\}$. Dann besitzt n einen *Primteiler*, d. h. einen Teiler, der eine Primzahl ist.

3.3 Satz (Euklid)

Es gibt unendlich viele Primzahlen: $\#\mathcal{P} = \infty$

Selbsttest

Sei $n \geq 2$. Dann ist $n! + 1$ durch KEINE Zahl von 2 bis n teilbar. Insbesondere ist der kleinste Primteiler von $n! + 1$ größer als n.

Um alle Primzahlen bis N schnell zu bestimmen gibt es einen Algorithmus: *Sieb des Eratosthenes.*

Erklärung findet man auf Wikipedia und wird noch ergänzt.

Die größte bekannte Primzahl hat heute 20 Millionen Dezimalstellen. Das heißt jedoch NICHT, dass alle Primzahlen bis hin zu dieser Zahl bekannt sind, da jene oft eine spezielle Form haben.

IV Geneauere Eigenschaften der Primzahlen

4.1 Satz (Bertrandsches Postulat)

$\forall\ n \geq 2$ gibt es (mindestens) eine Primzahl mit $n < p < 2n$.

Selbsttest

$\forall\ n \geq 3$ gibt es (mindestens) eine Primzahl mit $n < p < n! - 1$.
Hinweis: Betrachte den kleinsten Primteiler von $n! - 1$.

Selbsttest

Sei $n \geq 1$. Die n Zahlen zwischen $(n+1)! + 2$ und $(n+1)! + n + 1$ sind KEINE Primzahlen.

4.2 Primzahlen in arithmetischen Folgen

Selbsttest

Es gibt unendlich viele Primzahlen der Form $3n+2$.
Hinweis: Seien diese Primzahlen $p_1, \ldots, p_n$ endlich. Die Zahl $a = 3\left(\prod_{i=1}^{n} p_i\right) - 1$ hat die Form $3n+2$ und ihre Primteiler sind alle von $3, p_1, \ldots, p_n$ verschieden. Dann sind alle Primteiler der Form $3n+1$. Es folgt, dass a der Form $3n+1$ sein muss; Grunddafür ist: $(3n+1)(3m+1) = 3(nm+n+m)+1$. Also erhält man einen Widerspruch.

4.3 Satz (unendlich viele Primzahlen)

Sei $p \in \mathcal{P}$ und $0 < r < p$. Dann gibt es unendlich viele Primzahlen der Form

$$pn + r$$

Der Grenzwert

$$\lim_{x \to +\infty} \frac{\#\left(\mathcal{P}_{\leq x} \cap \left\{ pn + r \;\middle|\; n \in \mathbb{N} \right\}\right)}{\#(\mathcal{P}_{\leq x})}$$

existiert und hat den Wert $\frac{1}{p-1}$.

Allgemeiner gilt:

4.4 Satz (Dirichletscher Primzahlsatz)

Sei $d > 1$ und $0 \leq r < d$ mit $(r, d) = 1$. Dann gibt es unendlich viele Primzahlen der Form

$$dn + r$$

Der Grenzwert

$$\lim_{x \to +\infty} \frac{\#\left(\mathcal{P}_{\leq x} \cap \left\{ dn + r \;\middle|\; n \in \mathbb{N} \right\}\right)}{\#(\mathcal{P}_{\leq x})}$$

existiert und hat den Wert $\frac{1}{\varphi(d)}$ wobei

$$\varphi(d) := \#\Big\{ x \in \mathbb{N} \;,\; 0 < x < d \;,\; (x, d) = 1 \Big\}$$

Falls $(r, d) \neq 1$, dann gibt es höstens eine Primzahl mit Rest r in der Division mit d.

4.5 Primzahlverteilungsfunktion

Anzahl der Primzahlen, die kleiner oder gleich x sind, heißt *Primzahlverteilungsfunktion*:

$$\pi(x) := \sum_{\substack{p \in \mathcal{P} \\ p \leq x}} 1$$

4.6 Satz (Großer Primzahlsatz)

$$\lim_{x\to+\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

Bessere Abschätzung:

$$\mathrm{li}(x) := \int_2^x \frac{1}{\ln(t)}\,\mathrm{d}t$$

da $\pi(x) \sim \mathrm{li}(x) - \mathrm{li}(2)$
Bemerkung: Die Funktion li steht für „logarithmisches Integral“.

Es gibt viele ungelöste Probleme, die für die heutigen Mathematikkenntnisse zu schwierig sind. Die *Goldbachsche Vermutung* besagt, dass sich jede gerade Zahl größer als zwei als Summe zweier Primzahlen schreiben lässt. Diese Vermutung ist jedoch noch nicht bewiesen.

V Fundamentalsatz der Arithmetik

5.1 Satz (Der wichtigeste Fall)

Jede ganze Zahl $a > 1$ besitzt eine Darstellung

$$a = p_1 \cdot \ldots \cdot p_n = \prod_{i=1}^{n} p_i$$

wobei $p_1, \ldots, p_n \in \mathcal{P}$. Diese Darstellung ist bis auf Anordnung eindeutig.

5.2 Satz (Die kanonische Primzerlegung)

Jede ganze Zahl $a > 1$ besitzt genau eine Darstellung

$$a = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} = \prod_{i=1}^{r} p_i^{e_i}$$

wobei $r \in \mathbb{N}_{\geq 1}$ und $p_1, \ldots, p_r \in \mathcal{P}$ mit $p_1 < \ldots < p_r$ und $e_1, \ldots, e_r \in \mathbb{N}_{>0}$.
$r, p_1, \ldots, p_r, e_1, \ldots, e_r$ sind durch a eindeutig bestimmt.

5.3 Proposition (Primteiler)

Die Primzahlen der kanonischen Primzerlegung von a sind genau die Primteiler von a.
Bemerkung: Die Menge der Primteiler ist $\mathcal{T}(a) \cap \mathcal{P}$.

Sei p ein Primteiler von a. Dann ist die Potenz von p in der kanonischen Primzerlegung von a die größte Potenz von p, die a teilt.

Selbsttest

Sei $z \mid (x, y)$ $\Big(\iff z \mid x$ und $z \mid y\Big)$. Dann sind $x \mid y$ und $\frac{x}{z} \mid \frac{y}{z}$ gleichbedeutend.

5.4 Korollar (Primteiler)

Die Primteiler von a sind die Primzahlen, die in einer bliebigen Primzerlegung auftauchen.

5.5 Erweiterete kanonische Primzerlegung - Konvention

$$a = \prod_{p\in\mathcal{P}} p^{a_p} = \prod_{p|a} p^{a_p} \cdot \prod_{p\nmid a} p^0 = \prod_{p|a} p^{a_p} \cdot \prod_{p\nmid a} 1 = \prod_{p|a} p^{a_p}$$

5.6 Satz (eindeutige Darstellung einer Zahl)

Jede ganze Zahl $a > 1$ besitzt genau eine Darstellung

$$a = \prod_{p\in\mathcal{P}} p^{a_p}$$

mit $a_p \in \mathbb{N}$.

5.7 Bemerkung (Primzahlen außerhalb endlicher Teilmengen)

$\forall\ p \in \mathcal{P}$ außerhalb einer endlichen Teilmenge gilt $a_p = 0$.

$$a_p > 0 \iff p \,\Big|\, a$$

5.8 Proposition (kanonische Primzerlegung)

Seien $a, b > 1$ und seien

$$a = \prod_{p\in\mathcal{P}} p^{a_p} \quad , \quad b = \prod_{p\in\mathcal{P}} p^{b_p}$$

die kanonischen Primzerlegungen von a und b. Dann gelten:

(i) $a = b \iff a_p = b_p \quad \forall\ p \in \mathcal{P}$

(ii) Die kanonische Primzerlegung von ab ist

$$ab = \prod_{p\in\mathcal{P}} p^{a_p+b_p}$$

Falls $b \,\Big|\, a$, so ist die kanonische Primzerlegung von $\frac{a}{b}$ gleich

$$\frac{a}{b} = a = \prod_{p\in\mathcal{P}} p^{a_p-b_p}$$

5.9 Satz (Verallgemeinerung auf von Null verschiedene ganze Zahlen)

Jede ganze Zahl $a \neq 0$ besitzt genau eine Darstellung

$$a = \varepsilon_a \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} = \varepsilon_a \cdot \prod_{i=1}^{r} p_i^{e_i}$$

wobei $\varepsilon_a = \frac{a}{|a|}$ und $p_1, \ldots, p_r \in \mathcal{P}$ mit $p_1 < \ldots < p_r$ und $e_1, \ldots, e_r \in \mathbb{N}_{>0}$.

5.10 Satz (weitere eindeutige Darstellung einer Zahl)

Jede ganze Zahl $a \neq 0$ besitzt genau eine Darstellung

$$a = \varepsilon_a \cdot \prod_{p \in \mathcal{P}} p^{a_p}$$

wobei $\varepsilon_a = \frac{a}{|a|} \in \{\pm 1\}$ und $a_p \in \mathbb{N}$ eindeutig durch a bestimmt.

5.11 Proposition (kanonische Primzerlegung – Primteiler)

Die Primzahlen der kanonischen Primzerlegung von a sind genau die Primteiler von a.
Sei p Primteiler von a. Die Potenz von p in der kanonischen Primzerlegung von a ist die größte Potenz von p, die a teilt.

5.12 Proposition (kanonische Primzerlegungen)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$ und seien

$$a = \varepsilon_a \cdot \prod_{p \in \mathcal{P}} p^{a_p} \quad , \quad b = \varepsilon_b \cdot \prod_{p \in \mathcal{P}} p^{b_p}$$

die kanonischen Primzerlegungen von a und b. Dann gelten:

(i) $a = b \iff \varepsilon_a = \varepsilon_b$ und $a_p = b_p \quad \forall\, p \in \mathcal{P}$

(ii) Wir haben

$$ab = \varepsilon_a \varepsilon_b \cdot \prod_{p \in \mathcal{P}} p^{a_b + b_p}$$

und folglich, falls $b \mid a$

$$\frac{a}{b} = \varepsilon_a \varepsilon_b \cdot \prod_{p \in \mathcal{P}} p^{a_b - b_p}$$

VI Einige Konsequenzen des Fundamentalsatzes

6.1 Satz (Teilbarkeitskriterium)

Sei $a \in \mathbb{Z} \setminus \{0\}$ und sei

$$a = \varepsilon_a \cdot \prod_{p \in \mathcal{P}} p^{a_p}$$

die kanonische Primzerlegung. Dann sind die Teiler von a genau die ganzen Zahlen $t \neq 0$ mit kanonischer Primzerlegung

$$t = \varepsilon_t \cdot \prod_{p \in \mathcal{P}} p^{t_p}$$

sodass $t_p \leq a_p \quad \forall\, p \in \mathcal{P}$.

6.2 Satz (ggT und kgV)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$ mit kanonischen Primzerlegungen

$$a = \varepsilon_a \cdot \prod_{p \in \mathcal{P}} p^{a_p} \quad , \quad b = \varepsilon_b \cdot \prod_{p \in \mathcal{P}} p^{b_p}$$

Dann ist

$$\mathrm{ggT}(a,b) = \prod_{p \in \mathcal{P}} p^{\min(a_p, b_p)} \quad , \quad \mathrm{kgV}(a,b) = \prod_{p \in \mathcal{P}} p^{\max(a_p, b_p)}$$

6.3 Korollar (ggT und kgV)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann gilt:

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = |ab|$$

Selbsttest

Gib die Formel für $\mathrm{ggT}\,(a_1, \ldots, a_n)$ an, mit Hilfe der Exponenten $a_{i,p}$. Ebenso für das kgV.

6.4 Proposition (teilerfremde Zahlen)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann gilt:

$$a \text{ und } b \text{ teilerfremd} \iff a \text{ und } b \text{ besitzen KEINE gemeinsamen Primteiler}$$

Das heißt auch: $a_p > 0 \implies b_p = 0$.

Aufgabe

Seien $a, b \geq 1$ mit $(a,b) = 1$. Für $t \in \mathcal{T}^+(ab)$ gilt

$$t = s_a \cdot s_b$$

mit $s_a \in \mathcal{T}^+(a)$ und $s_b \in \mathcal{T}^+(b)$ beliebig und eindeutig bestimmt.
Hinweis: $t = \prod\limits_{p|ab} p^{t_p} = \prod\limits_{p|a} p^{t_p} \cdot \prod\limits_{p|b} p^{t_p}$, da Primteiler von a und b disjunkt. Außerdem ist

$$\mathcal{T}^+(a) \times \mathcal{T}^+(b) \longrightarrow \mathcal{T}^+(ab) \ , \ t_a, t_b \longmapsto t_a \cdot t_b$$

wohldefiniert und eine Bijektion. Für a, b NICHT teilerfremd ist die Funktion NICHT mehr injektiv; surjektiv ist sie immer.

6.5 Proposition (Anzahl der Teiler)

Wir haben

$$\#\mathcal{T}^+(a) = \prod_{p|a} (a_p + 1) \quad , \quad \#\mathcal{T}(a) = 2 \cdot \prod_{p|a} (a_p + 1)$$

6.6 Satz (Potenzen)

$a \in \mathbb{Z}$ mit $a \geq 1$ ist n-te Potenz ($n \geq 1$) einer ganzen Zahl $\iff n \mid a_p \quad \forall\, p \in \mathcal{P}$

§ 14
Rationale Zahlen

I $\mathbb{Q}$ als Körper mit einer totalen Anordnung, der den Ring $\mathbb{Z}$ enthält

1.1 Definition ($\mathbb{Q}$)

$$a = b + x \text{ lösbar mit } x \in \mathbb{N} \iff a \geq b$$

Für $b > a$ gilt: $x = a - b \in \mathbb{Z}$

$$a = bx \text{ lösbar mit } x \in \mathbb{Z} \iff b \mid a$$

Für $b \nmid a$ und $b \neq 0$ existiert auch ein $x = \frac{a}{b} \in \mathbb{Q}$.
Eine rationale Zahl ist eine Äquivalenzklasse von Brüchen!!!

Bruch

geordnetes Paar $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \left\{ (a, b) \;\middle|\; a, b \in \mathbb{Z} \quad \wedge \quad b \neq 0 \right\}$$

Man schreibt (a, b) als $\frac{a}{b}$, wobei a als Zähler und b als Nenner bezeichnet wird.

NNN – Nenne Nie Null

In der Mathematik darf NIE durch 0 geteilt werden!

Äquivalenzrelation

Die Relation

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$$

ist eine Äquivalenzrelation auf der Menge der Brüche. Insbesondere gilt:

$$\frac{a}{b} \sim \frac{at}{bt} \quad \forall\, t \in \mathbb{Z} \setminus \{0\}$$

Rationale Zahl

Jede Äquivalenzklasse heißt rationale Zahl. Es gilt:

$$\left[\frac{a}{b}\right] = \left\{ \frac{c}{d} \;\middle|\; c, d \in \mathbb{Z}\ ,\ d \neq 0\ ,\ ad = bc \right\}$$

Definition von $\mathbb{Q}$

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist die Quotientenmenge von $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ bzgl. der Äquivalenzrelation $\sim$.

Notation

Eine rationale Zahl r ist eine Äquivalenzklasse $\left[\frac{a}{b}\right]$, aber wir schreiben $r = \frac{a}{b}$ (Repräsentant).

Bemerkung: $ad = bc \iff ad - bc = 0$ und dies ist die Determinante der Matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

Zwei Brüche sind also genau dann äquivalent, wenn die Vektoren $\begin{pmatrix} a \\ b \end{pmatrix}$ und $\begin{pmatrix} c \\ d \end{pmatrix}$ in $\mathbb{R}^2$ linear abhängig sind.

1.2 Verknüpfungen und Anordnung

Summe, Produkt, Anordnung

Wir definieren für alle rationalen Zahlen $\frac{a}{b}, \frac{c}{d}$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
$$\frac{a}{b} \geq \frac{c}{d} \quad \text{falls } ad - bc \geq 0$$

Diese zwei Verknüpfungen und die Anoordnung sind wohldefiniert.

Proposition

Aus $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$ folgen

- $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$
- $\frac{ac}{bd} = \frac{a'c'}{b'd'}$
- $ad - bc \geq 0 \iff a'd' - b'c' \geq 0$

Aus den Eigenschaften von $\mathbb{Z}$ folgt:

Eigenschaften Summe und Produkt

Die Summe ist kommutatuiv, assoziativ, mit neutralem Element 0 und Inversem.

$$-\left(\frac{a}{b}\right) := \frac{-a}{b} = \frac{a}{-b}$$

Das Produkt ist kommutativ, assoziativ, mit neutralem Element 1 und jedes $\frac{a}{b} \neq 0$ hat multiplikatives Inverses $\frac{b}{a}$. Es gelten die Distibutivgesetze.

Satz

$(\mathbb{Q}, +, \cdot)$ ist ein Körper.
$(\mathbb{Q}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind abelsche Gruppen.
Insbesondere gelten die Kürzungsregel und die Lösungen von einfachen Gleichungen für alle $x, y, z \in \mathbb{Q}$:

$$x + z = y + z \implies x = y$$
$$xz = yz \implies x = y \quad \text{falls } z \neq 0$$
$$z = x + y \implies x = z - y$$
$$z = xy \implies x = z \cdot y^{-1} \quad \text{falls } y \neq 0$$

Eigenschaften Anordnung

Anordnung $\geq$ auf $\mathbb{Q}$ ist transitiv, antisymmetrisch, reflexiv und total.
Anordnung $>$ auf $\mathbb{Q}$ ist transitiv, trichotomisch, irreflexiv und konnex.

$\frac{a}{b} \in \mathbb{Q}$ heißt (streng) positiv, wenn sie ≥ 0 (> 0), d. h. $ab \geq 0$ $(ab > 0)$.

Monotonieregeln gelten auch für $\mathbb{Q}$. Insbesondere ist $\mathbb{Q}^+$ bzgl. Summe und Produkt abgeschlossen.

Aufgabe

Elemente von $\mathbb{Q}$ liegen dicht. Das heißt, für $r, s \in \mathbb{Q}$ mit $r < s$ liegt immer noch ein $t \in \mathbb{Q}$ dazwischen, also $r < t < s$.

1.3 Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$

Die Funktion

$$\mathbb{Z} \longrightarrow \mathbb{Q}\ ,\ a \longmapsto \left[\frac{a}{1}\right]$$

ist wohldefiniert und injektiv, aber NICHT surjektiv. Mit dieser Identifizierung schreiben wir $\mathbb{Z} \subset \mathbb{Q}$. Da $\mathbb{N} \subseteq \mathbb{Z}$, haben wir auch eine Einbettung $\mathbb{N} \longrightarrow \mathbb{Q}$.
Notation: schreibe a statt $\frac{a}{1}$.

Aufgabe

Obige Funktion ist wohldefiniert und injektiv. Die rationale Zahl $\left[\frac{3}{6}\right] = \frac{1}{2}$ ist NICHT in der Bildmenge, weil aus $\frac{a}{1} = \frac{t}{2t}$ mit $t \in \mathbb{Z}$ folgt, dass $2 \mid 1$. Das kann NICHT sein.

Ganze Zahlen

Sei $r \in \mathbb{Q}$ der Form $r = \frac{a}{b}$, wobei $a, b \in \mathbb{Z} \setminus \{0\}$. Dann sind folgende Aussagen äquivalent:

(1) $r \in \mathbb{Z}$

(2) $\frac{a}{b} \sim \frac{s}{1}$ mit $s \in \mathbb{Z}$

(3) $b \mid a$

(4) falls a und b teilerfremd, gilt: $b = \pm 1$

$\mathbb{Q}$ ist abzählbar, d. h. es gibt bijektive Abbildungen $\mathbb{N} \longrightarrow \mathbb{Q}$ und $\mathbb{Z} \longrightarrow \mathbb{Q}$. Die kanonischen Einbettungen von $\mathbb{N}$ und $\mathbb{Z}$ sind NICHT surjektiv!

1.4 Potenzen und Division

Sei $x = \frac{a}{b} \in \mathbb{Q}$. Wir definieren x^n für $n \geq 0$ als $x^n = \frac{a^n}{b^n}$ und für $n > 0$ definieren wir x^{-n} als

$$x^{-n} = \frac{b^n}{a^n} = \left(\frac{b}{a}\right)^n = \left(\frac{a^n}{b^n}\right)^{-1}$$

Aufgabe

Diese Definition ist nur von der rationalen Zahl abhängig – NICHT von dem Bruchrepräsentant.

Division

$\frac{\frac{a}{b}}{\frac{c}{d}}$ mit $\frac{c}{d} \neq 0$ ist $\frac{ad}{bc}$, also $\frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1}$.
Produkt und multiplikatives Inverses NICHT von der Wahl der Repräsentanten abhängig $\Longrightarrow$ rationale Zahl ist durch eine von Null verschiedene rationale Zahl teilbar

II Viele kleine Begriffe

2.1 Gekürzte Bruchdarstellung

Sei $r \in \mathbb{Q}$, also $r = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$. Wir berechnen (a, b) und dieser ggT ist $\neq 0$, da a, b NICHT beide Null. Die ganzen Zahlen $a' = \frac{a}{(a,b)}$ und $b' = \frac{b}{(a,b)}$ sind teilerfremd und es gilt $b' \neq 0$ und $r = \frac{a'}{b'}$. Somit haben wir einen Algorithmus um r als Bruch mit teilerfremdem Zähler und Nenner zu schreiben.

2.2 Hauptnennerdarstellung

Seien $r = \frac{b}{a}$ und $r' = \frac{c}{d}$ rationale Zahlen. Die rationale Zahl $r + r'$ kann als Bruch mit Nenner $\mathrm{kgV}(b, d)$ geschrieben werden. Wir schreiben $r = \frac{a'}{\mathrm{kgV}(a,b)}$ und $r' = \frac{c'}{\mathrm{kgV}(b,d)}$ und wir addieren $r + r' = \frac{a'+c'}{\mathrm{kgV}(b,d)}$. Das ist in der Praxis oft besser als $r + r' = \frac{ad+cb}{bd}$ zu berechnen.
Für mehrere Brüche benutzen wir das kgV der Nenner (Hauptnenner).

Auch wenn man das kgV NICHT berechnen kann, ist jedes gemeinsame Vielfache gut: wenn man ein gemeinsames Vielfaches, das im Betrag kleiner als das Produkt ist, findet, lohnt es sich

schon.
Brüche, die in ihrem Nenner übereinstimmen, heißen *gleichnamig.*

2.3 Allgemeiner Nenner

- Sei b eine Zahl, die höchstens 2 und 5 als Primteiler hat. Sei also $b = 2^\alpha 5^\beta$ mit $\alpha, \beta \in \mathbb{N}$. Wählen wir ein $N \in \mathbb{N}$ mit $N \geq \alpha$ und $N \geq \beta$, d. h. $N \geq \max(\alpha, \beta)$. Dann gilt:

$$b \mid 10^N$$

- Sei b eine zu 10 teilerfremde Zahl. Wir werden mit Hilfe der Kongruenzrechnung beweisen, dass

$$b \mid (10^N - 1) = \underbrace{9999\ldots9}_{N}$$

für ein N (NICHT eindeutig). Ein N, das gut für b ist, jedoch i. A. NICHT minimal, ist $N = \varphi(b)$ (Eulersche φ-Funktion). Also falls $p \in \mathcal{P}$ ist mit $p \neq 2, 5$, dann gilt sicher

$$p \mid 10^{p-1} - 1$$

Zusatz: I. A. ist $N > 0$ ein beliebiges positives Vielfaches der multiplikativen Ordnung von 10 modulo b (siehe Kongruenzrechnung).

- Sei $b > 0$ und $b \in \mathbb{N}$. Es gilt $b = b_1 b_2$, sodass $(b_2, 10) = 1$ und b_1 höstens 2 und 5 als Primteiler hat. Nimm eine Primfaktorzerlegung von b und definiere b_1 als Produkt der Primaktoren 2 und 5 und b_2 als das Produkt der restlichen Faktoren. Daher gilt:

$$b \mid 1000\ldots0 \qquad b_2 = 1$$
$$b \mid 999\ldots9 \qquad b_1 = 1$$
$$b \mid 999\ldots9000\ldots0 \qquad b_1, b_2 > 1$$

Also teilt jede natürliche Zahl $b > 0$ eine Zahl der Form

$$(10^N - 1) \cdot 10^M$$

wobei $N, M \geq 0$. Also können wir als Nenner für eine rationale Zahl immer eine Zahl dieser FOrm benutzen. Wir finden obige Zahlen wieder, wenn wir eine periodische reelle Zahl als Bruch schreiben.

2.4 Scheinbrüche, Stammbrüche usw.

Wir arbeiten jetzt nur mit positiven rationalen Zahlen und auch Brüchen, sodass sowohl Zähler als auch Nenner positiv sind.

Ein Bruch heißt *Stammbruch*, falls der Nenner 1 ist. Ein Bruch, sodass Zähler den Nenner teilt, wir ein Stammbruch, wenn man durch den Zähler kürzt. Stammbrüche sind genau die Kehrwerte

der von Null verschiedenen natürlichen Zahlen. Ein Bruch, welcher KEIN Stammbruch ist, heißt *abgeleiteter Bruch* oder *Zweigbruch*.

Ein Bruch ist *echt* oder *eigentlich*, falls der Zähler kleiner als der Nenner ist. Die anderen Brüche heißen *unecht* oder *uneigentlich*.

Ein *Scheinbruch* ist ein Bruch, indem der Nenner den Zähler teilt; also ein Bruch, indem wir den Nenner 1 wählen können.

Ein Bruch heißt **Dezimalbruch**, falls der Nenner eine Potenz von 10 ist.

Die ‚normalen Brüche' heißen *gewöhnlich*. Die ‚nicht normalen Brüche' heißen *gemischt*.

2.5 Prozentrechnung

Die Prozentrechnung ist nichts weiter als Bruchrechnung, wobei das Symbol % für $\frac{1}{100}$ steht. Man benutzt auch Promille für $\frac{1}{1000}$ mit dem Symbol ‰.

III Kanonische Zerlegung für rationale Zahlen

3.1 Teilerfremde Zähler und Nenner

Sei $x \in \mathbb{Q} \setminus \{0\}$ und sei $x = \frac{a}{b}$ mit $a, b \neq 0$ und $(a, b) = 1$. Dann sind die Mengen der Primteiler von a und b disjunkt. Wir schreiben

$$x = \frac{\varepsilon_a}{\varepsilon_b} \cdot \frac{\prod\limits_{p|a} p^{a_p}}{\prod\limits_{p|b} p^{b_p}}$$

Dann haben wir

$$x = \varepsilon_x \cdot \prod_{p|ab} p^{x_p}$$

wobei

$$x_p = a_p - b_p = \begin{cases} 0 & p \nmid ab \\ a_p & p \mid a \\ -b_p & p \mid b \end{cases}$$

und $\varepsilon_x = \varepsilon_{ab} = \frac{\varepsilon_a}{\varepsilon_b} \in \{\pm 1\}$. Das Vorzeichen von x und die Exponenten $x_p \in \mathbb{Z}$ sind eindeutig bestimmt.

3.2 Allgemeinere Darstellung

Kanonische Darstellung einer von Null verschiedenen rationalen Zahl ist

$$x = \varepsilon_x \cdot \prod_{p \in \mathcal{P}} p^{x_p} \quad (x_p \in \mathbb{Z})$$

x_p fast alle Null. Schreibe x als Bruch und p teilt weder Zähler noch Nenner, so ist $x_p = 0$. Falls Zähler und Nenner teilerfremd, dann gilt:

$$x_p = 0 \iff p \text{ teilt weder Zähler noch Nenner}$$

Sei $x = \frac{a}{b}$. Dann gilt – auch wenn a und b NICHT teilerfremd:

$$x = \varepsilon_{ab} \cdot \prod_{p \in \mathcal{P}} p^{a_p - b_p}$$

IV Dezimalbruchentwicklung rationaler Zahlen

Der Einfachheit halber betrachten wir nur positive Zahlen.

Eine positive Zahl ist entweder eine ganze Zahl oder ihre Abrundungsfunktion plus ist ein echter (streng positiver) Bruch. Beschränke nun auf echte Brüche. Abrundungsfunktion ergibt die Ziffern vor dem Komma und der echte Bruch die Ziffern nach dem Komma.

4.1 Periodische reelle Zahlen mit Periode 0

Sei $r = \frac{a}{10^N}$. Wir schreiben $a = (a_n, \ldots, a_0)_{10}$ und dann setzen wir das Komma zwischen die Ziffern a_{N+1} und a_N. Falls $N \geq n$, schreiben wir zusätzlich Nullziffern am Anfang. Schließlich entfernen wir die Nullziffern am Ende, falls N NICHT minimal gewählt wurde.

Umgekehrt wird eine reelle Zahl mit Periode Null durch Multiplikation mit einer Potenz von 10 zu einer ganzen Zahl a. Zum Beispiel mit 10^M, falls es M Ziffern nach dem Komma vor der Periode 0 gibt. Also ist eine reelle Zahl mit Periode 0 eine rationale Zahl der Form $\frac{a}{10^M}$, wobei $M \geq 1$.

Die reellen Zahlen, die periodisch sind mit Periode 0, sind die rationalen Zahlen, deren Nenner eine Potenz von 10 teilt und insbesondere alle ganzen Zahlen. Diese Zahlen der Periode 0 haben eine endliche Dezimaldarstellung.

4.2 Rein periodische reelle Zahlen

Rein periodische reelle Zahlen haben die Form

$$0, \underbrace{\overline{a_{N-1} \ldots a_0}}_{N \text{ Ziffern}} = \sum_{i=1}^{+\infty} a \cdot (10^{-N})^i = \frac{a}{10^N - 1} = \frac{a}{\underbrace{999 \ldots 9}_{N \text{ Ziffern}}}$$

nach der Formel für die geometrische Reihe

$$\sum_{i=1}^{+\infty} (10^{-N})^i = \frac{1}{1 - 10^{-N}}$$

und wobei

$$a = (a_{N-1}, \ldots, a_0)_{10}$$

Bemerkung: Dies ist NICHT unbedingt die kanonische Darstellung von a in Basis 10, da eine oder mehrere Ziffern am Anfang 0 sein können.

Also lässt sich der Algorithmus

- Zähler = Ziffern der Periode
- Nenner = so oft 9, wie die Periodenlänge ist

einfach mit einer geometrischen Reihe erklären. Wir erhalten:
Jede rein periodische reelle Zahl ist eine rationale Zahl (zwischen 0 und 1), deren Nenner in der reduzierten Bruchdarstellung eine Zahl der From $10^N - 1$ teilt.
Man kann auch sagen, dass der Nenner zu 10 teilerfremd ist.

Algortihmus, um Zähler und Nenner zu bestimmen: berechne geometrische Reihe und kürze ggf.

Algorithmus, um Periode zu berechnen: finde N so, dass Nenner 10^{N-1} teilt und schreibe rationale Zahl mit solchem Nenner; Zähler ergibt die Ziffern für die Periode; nehme ggf. minimale Periode.

4.3 Periodische reelle Zahlen = Rationale Zahlen

Jede periodische reelle Zahl ist die Summe von

(a) einer rein periodischen reellen Zahl mal einer Potenz von 10.

(b) einer rellen Zahl mit Periode 0.

4.4 Wichtige Anmerkungen

- Jeder rellen Zahl lässt sich eine Dezimalbruchentwicklung zuordnen. D. h. schreibe eine Reihe, deren Summanden Zahlen von 0 bis 9 mal eine Potenz von 10 sind und dessen Grenzwert die reelle Zahl ist. Es gibt nur endlich viele Terme mit positiven Exponenten und entweder endlich oder unendlich viele Terme mit negativen Exponenten.
- Die rellen Zahlen, die KEINE rationalen Zahlen sind/NICHT periodisch sind, heißen *irrationale Zahlen*. Man kann i. d. R. NICHT alle Ziffern einer irrationalen Zahl angeben.
- Man benutzt das Dezimalsystem, um reelle Zahlen in Ziffern zu schreiben. DIe Zahl 10 hat KEINE mathematische Bedeutung; besser wäre z. B. in Basis 2 zu arbeiten.
  In einem anderen Stellenwertsystem (g-adische Darstellung) benutzt man Potenzen von g mit positiven Exponenten, um ganze Zahlen darzustellen und auch negative Exponenten für reelle Zahlen. Der Unterschied ist, dass wir zwischen ganzen Zahlen, die eine Potenz von g teilen und ganzen Zahlen, die zu g teilerfremd sind, unterscheiden.

§ 15
Reelle Zahlen, Dezimalbruchentwicklung

I Definition

1.1 Äquivalenzklassen von Cauchy-Folgen

Menge der reellen Zahlen entpricht Menge aller Punkte der Zahlengeraden. Auf der Zahlengeraden gibt es auch die rationalen Zahlen, die dicht liegen. Man kann alle punkte der Zahlgeraden als Grenzwerte von Folgen rationaler Zahlen betrachten.
Konstruktion der rellen Zahlen: man betrachte die Cauchy-Folgen von rationalen Zahlen, d. h. die Folgen $\{a_n\}_{n\geq 0}$, sodass

$$\forall\, \varepsilon > 0 \quad \exists\, N \in \mathbb{N} \quad \forall\, m, n \geq N\colon\ |a_m - a_n| < \varepsilon$$

Betrachte eine Äquivalenzrelation auf der Menge der Cauchy-Folgen. Wir sagen, dass zwei Folgen $\{a_n\}_{n\geq 0}$ und $\{b_n\}_{n\geq 0}$ äquivalent sind, falls die Differenzfolge $\{a_n - b_n\}_{n\geq 0}$ konvergiert und den Grenzwert 0 hat:

$$\forall\, \varepsilon > 0 \quad \exists\, N \in \mathbb{N} \quad \forall\, n \geq N\colon\ |a_n - b_n| < \varepsilon$$

Die Äquivalenzklassen sind genau die reellen Zahlen.

Die rationalen Zahlen können wir als die Äquivalenzklassen von konstanten Folgen sehen. Dies ergibt eine injektive Funktion

$$\mathbb{Q} \longrightarrow \mathbb{R}$$

da verschiedene konstante Folgen verschieden Grenzwerte haben. Die reellen Zahlen, die KEIN rationalen Zahlen sind, heißen *irrational*.

1.2 Dedekindsche Schnitte

Dedekindsche Schnitte werden durch ein geordnetes Paar von Teilmengen rationaler Zahlen A (Untermenge) und B (Obermenge) über folgende Axiome definiert:

- A und B ergeben Partition von $\mathbb{Q}$
- Jedes Element von A ist kleiner als jedes Element von B.
- B hat KEIN Minimum.

Die reelle Zahl, die dem Paar aus A und B zugeordnet wird, ist das Maximum von A (falls dies existiert) oder die ienzige reelle Zahl zwischen A und B, also diejenige, die größer als alle Elemente von A und kleiner als alle Elemente von B ist. Im ersten Fall haben wir eine rationale Zahl, Im zweiten Fall eine irrationale Zahl.

1.3 Intervallschachtelung

Eine andere Weise eine reelle Zahl anzunähern ist, sie durch immer kleinere von rationalen Zahlen bregrenzte Intervalle einzuschachteln.
Man beginnt mit einem beschränkten Intervall und wählt daraus ein abgeschlossenes Intervall, das komplett im vorherigen liegt. Darin wählt man wieder ein abgeschlossenes Intervall usw.
Werden die Längen der Intervalle beliebig klein, konvergiert die Länge gegen 0. Somit gibt es genau eine reelle Zahl, die in allen Intervallen enthalten ist.
Mathematisch exakt besteht eine Intervallschachtelung aus zwei Folgen von rationalen Zahlen:

- $\{a_n\}_{n\geq 0}$ und $\{b_n\}_{n\geq 0}$ sind folgen rationaler Zahlen
- $\{a_n\}_{n\geq 0}$ ist monoton wachsend und $\{b_n\}_{n\geq 0}$ ist monoton fallend
- $a_n \leq b_n \quad \forall\, n \in \mathbb{N}$
- Differenzfolge $\{b_n - a_n\}_{n\geq 0}$ ist eine Nullfolge, d. h. $\lim\limits_{n\to\infty}(b_n - a_n) = 0$

Es gibt mehrere Intervallschachtelungen für eine Zahl.

Zwei Intervallschachtelungen $\{a_n\}_{n\geq 0}$, $\{b_n\}_{n\geq 0}$ und $\{c_n\}_{n\geq 0}$, $\{d_n\}_{n\geq 0}$ sind äquivalent, falls $\{a_n\}_{n\geq 0}$, $\{d_n\}_{n\geq 0}$ und $\{c_n\}_{n\geq 0}$, $\{b_n\}_{n\geq 0}$ wieder Intervallschachtelungen sind.
Man identifiziert äquivalente Intervallschachtelungen. Also findet man reelle Zahlen als Äquivalenzklassen von Intervallschachtelungen.
Die rationalen Zahlen sind Äquivalenzklassen von konstanten Intervallschachtelungen. Also falls $q \in \mathbb{Q}$, so ergibt $a_n = b_n = q$ eine Intervallschachtelung mit entsprechender Zahl q.

1.4 Axiomatische Konstruktion

Man kann die reellen Zahlen durch folgende Axiome definieren:

- Die reellen Zahlen sind ein Körper.
- Die reellen Zahlen besitzen eine Anordnung $<$, die total, transitiv und konnex ist.
- Die Monotonie bzgl. Addition und Multiplikation sollte gelten:

  $$a < b \implies a + c < b + c$$
  $$a < b \implies ac < bc \quad (c > 0)$$

  wobei 0 das neutrale Element der Addition ist.
- Jede nichtleere, nach oben beschränkte Teilmenge von $\mathbb{R}$ besitzt ein Supremum.

Andere wichtige Axiome, die man laternativ in der Definition der reellen Zahlen verwenden kann:

- Achimedisches Axiom: Sind $a, b > 0$ reelle Zahlen, dann gibt es ein $n \in \mathbb{N}$, sodass $na > b$.
- Vollständigkeitsaxiom: Jede Cauchy-Folge von reellen Zahlen konvergiert.

- Intervallschachtelungsaxiom: Der Durchschnitt jeder monoton fallenden Folge abgeschlossener beschränkter Intervalle ist nichtleer.

1.5 Struktur von $\mathbb{R}$

$\mathbb{R}$ ist ein Körper für Addition und Multiplikation. Mit jeder Definition werden diese Verknüpfungen für Repräsentanten definiert und danach für Äquivalenzklassen.
Es gibt auch eine Anordnung $<$, die total, transitiv und konnex ist. Dann entscheidet man zwischen positiven und negativen reelen Zahlen (Vorzeichen). Alle Eigenschaften des Körpers sind erfüllt. 0,1 sind die neutralen Elemente bzgl. Addition und Multiplikation. Additives Inverses von a ist $-a$. Jede zahl $\neq 0$ hat ein multiplikatives Inverses. Usw.

II Dezimalbruchentwicklung reeller Zahlen

Jede reelle Zahl lässt sich einer Dezimalbruchentwicklung zuordnen. Diese ist eine Reihe, deren Summanden Zahlen von 0 bis 9 multipliziert mit einer Zehnerpotenz sind und dessen Grenzwert die reelle Zahl ist:

$$r = \sum_{n=-\infty}^{+\infty} r_n \cdot 10^n \qquad r_n \in \{0, 1, \ldots, 9\}$$

Außerdem gibt es $r_n = 0$ für alle n positiv und groß genug. Grund ist, dass die Reihe konvergieren muss.

2.1 Kommaschreibweise

Schreiben wir eine reelle Zahl r als Reihe:

$$r = \sum_{n=-\infty}^{+\infty} r_n \cdot 10^n \qquad r_n \in \{0, 1, \ldots, 9\}$$

Sei $r_n = 0 \quad \forall\, n > m \geq 0$. Dann schreibt man die Ziffern wie folgt:

$$r = r_m r_{m-1} \ldots r_1 r_0, r_{-1} r_{-2} r_{-3} \ldots$$

Die Wertigkeit einer Ziffer ist die Zehnerpotenz 10^i. Der Index i beschreibt den Stellenwert der jeweiligen Ziffer. Ein Komma trennt die Zehnerpotenzen mit positiven Exponenten von denen mit streng negativen Exponenten.
Man löscht/vergisst alle „Nullstellen am Anfang“; jedoch benutzt man immer mindestens eine Ziffer vor dem Komma. Also nimmt man $m \geq 0$ minimal, sodass $r_n = 0 \quad \forall\, n > m$ und schreibt

$$r = r_m r_{m-1} \ldots r_1 r_0, r_{-1} r_{-2} r_{-3} \ldots$$

Es gibt also immer nur endlich viele Stellen vor dem Komma und entweder endlich oder unendlich viele Stellen nach dem Komma.

2.2 Periodenschreibweise

Schreiben wir eine reelle Zahl r als Reihe:

$$r = \sum_{n=-\infty}^{+\infty} r_n \cdot 10^n \qquad r_n \in \{0, 1, \ldots, 9\}$$

oder mit Ziffern

$$r = r_m r_{m-1} \ldots r_1 r_0, r_{-1} r_{-2} r_{-3} \ldots$$

Es kann sein, dass ein $t > 0$ existiert, sodass für alle n klein genug gilt: $r_{n-t} = r_n$. In diesem Fall sagen wir, dass die reelle Zahl periodisch ist mit Periodenlänge t und die Periode besteht aus einer endlichen geordneten Liste von t Ziffern, de sich immer wiederholen. Falls die Länge $t > 0$ minimal ist, sprechen wir von einer minimalen Periode. Für periodische Dezimalbruchentwicklungen ist eine Schreibweise üblich, bei der sich der periodisch wiederholende Teil der Nachkommastellen durch einen Überstrich markiert wird.
In der kanonischen Darstellung sollte die Periode minimal sein und sollte auch so früh wie möglich anfangen, aber immer nach dem Komma.
Man schreibt die Periode 0 NICHT.

Proposition

Alle möglichen Periodenlängen sind genau die Vielfachen der minimalen Periodenlänge.

2.3 Irrationale Zahlen

Die reellen Zahlen, die KEINE rationalen Zahlen sind/NICHT periodisch sind, heißen *irrationale Zahlen*. Man kann i. d. R. NICHT alle Ziffern einer irrationalen Zahl angeben.

§ 16
Kongruenzrechnung

I Definitionen

1.1 Kongruenz modulo m

Sei $m \in \mathbb{N}$ mit $m \geq 2$.
Zwei ganze Zahlen a, b heißen *kongreunt modulo* m, wenn

$$m \mid (a - b)$$

oder äquivalent, wenn a und b bei der Division durch m den gleichen Rest lassen.
Schreibweise für „a ist kongreunt zu b modulo m“:

$$a \equiv b \mod m$$

Notation: Die Schreibweise $a \not\equiv b \mod m$ bedeutet, dass a und b NICHT kongreunt modulo m sind.

Die Kongreunzrelation modulo m ist eine Äquivalenzrelation auf $\mathbb{Z}$.

- Folglich ergeben die Äquivalenzklassen eine Partition von $\mathbb{Z}$.
- zwei ganze Zahlen gehören zur selben Klasse $\Longleftrightarrow$ zwei Zahlen sind kongruent modulo m
- Verschiedene Äquivalenzklassen sind disjunkt.
- Jede ganze Zahl gehört genau zu einer Klasse.
- Äquivalenzklassen für diese Äquivalöenzrelation heißen auch Restklassen oder Kongruenzklassen.

1.2 Restklassen

Mögliche Divisionsreste modulo m sind die m Zahlen

$$0, 1, \ldots, m-1$$

also gibt es genau m Restklassen modulo m. Die Restklasse einer ganzen Zahl a besteht aus denjenigen Zahlen, die zu a kongruent sind.
Notation: $[a]_m$.
Wir haben daher

$$[a]_m = \left\{ a + mt \;\middle|\; t \in \mathbb{Z} \right\}$$

Rest 0 haben $\quad 0\ ,\ \pm m\ ,\ \pm 2m\ ,\ \pm 3m\ \ldots$
Rest 1 haben $\quad 1\ ,\ 1 \pm m\ ,\ 1 \pm 2m\ ,\ 1 \pm 3m\ \ldots$
$\vdots$
Rest r haben $\quad r\ ,\ r \pm m\ ,\ r \pm 2m\ ,\ r \pm 3m\ \ldots$
$\vdots$
Rest $m-1$ haben $\quad m-1\ ,\ m-1 \pm m\ ,\ m-1 \pm 2m\ ,\ m-1 \pm 3m\ \ldots$

Für jedes $m \geq 2$ ist wahr, dass $[0]_m = m\mathbb{Z}$, d. h. die ganzen Zahlen, die zu m kongruent sind, sind genau die Vielfachen von m.

1.3 Restsysteme

Eine Menge von Zahlen $a_1, \ldots, a_m$ heißt *vollständiges Repräsentantensystem* (Restsystem) modulo m, wenn $[a_1]_m, [a_2]_m, \ldots, [a_m]_m$ gerade die m verschiedenen Restklassen modulo m sind, d. h. wenn

$$a_i \not\equiv a_j \mod m \qquad \text{falls } i \neq j$$

Ist $a_1, \ldots, a_m$ ein vollständiges Restsystem modulo m, so gilt dies auch für $a_1 + c, \ldots, a_m + c$ mit $c \in \mathbb{Z}$.

Insbesondere gilt: Je m aufeinanderfolgende Zahlen bilden ein vollständiges Restsystem modulo m.

II Kongruenzrechnung

2.1 Rechenregeln

Im Folgenden sei $m \geq 2$ fest vorgegeben.

Satz

(a) $a \equiv b \implies a \pm c \equiv b + c$

(b) $a \equiv b \implies ac \equiv bc$

(c) $a \equiv b \implies a^n \equiv b^n \quad \forall\, n \in \mathbb{N}$

(d) Ist $f(x) = c_0 + c_1 x + \ldots + c_n x^n$ Polynomfunktion in der Variablen x, so folgt aus $a \equiv b$ schon $f(a) \equiv f(b)$.

Satz

(a) $ac \equiv bc \mod m$ und $(c, m) = 1 \implies a \equiv b \mod m$

(b) $a \equiv b \mod m \iff ac \equiv bc \mod cm$

(c) $a \equiv b \mod m$, $n \mid m$ und $n > 0 \implies a \equiv b \mod n$

(d) $a \equiv b \mod m \implies (a, m) = (b, m)$

2.2 Restklassen bzgl. verschiedenen Moduli

Kongruenz modulo m impliziert dieselbe Kongruenz modulo jedes Teilers von m.
Umgekehrt gilt die Implikation NICHT.
Falls m größer ist, dann ist die Kongruenz stärker und die Äquivalenzklassen sind kleiner. Sei $m' \mid m$. Dann ist jede Kongruenzklasse modulo m in einer Äquivalenzklasse modulo m' enthalten. Jede Restklasse modulo m' ist die Vereinigung von Restklassen modulo m. Die Partition von $\mathbb{Z}$ bzgl. Restklassen modulo m ist eine feinere Partition.

Proposition

Seien $m, d > 0$ mit $d \mid m$ und sei $m' = \frac{m}{d}$. Jede Restklasse modulo m' ist die Vereinigung von d Restklassen modulo m. Genauer gilt für alle $a \in \mathbb{Z}$:

$$[a]_{m'} = [a]_m \cup [a + m']_m \cup [a + 2m']_m \cup \ldots \cup [a + (d-1)m']_m$$

III Ringsturktur von $\mathbb{Z}/m\mathbb{Z}$

3.1 Definition

Die Menge der Restklassen modulo m schreibt man als $\mathbb{Z}/m\mathbb{Z}$. Das ist eine Menge mit m Elementen. Man kann eine Addition und Multiplikation von Restklassen definieren. Somit wird

$$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$$

zum kommutativen Ring mit 1, der genau dann ein Körper ist, wenn m eine Primzahl ist.

Definition

Seien $a, b \in \mathbb{Z}$. Setze

$$[a]_m + [b]_m = [a+b]_m$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

Diese Addition und Multiplikation werden durch Repräsentanten definiert. Das Ergebis ist eine Restklasse, die unabhängig von der Wahl der Repräsentanten ist. Deswegen seind diese Verknüpfungen wohldefiniert für Klassen.

3.2 Multiplikatives Inverses, Einheiten

- Das Inverse von $[1]_m$ für die Miltiplikation ist $[1]_m$.
- Das Inverse von $[a]_m$ für die Multiplikation existiert $\iff$ $(a, m) = 1$.
- Die Restklassen $[a]_m$ mit $(a, m) \neq 1$ und $[a]_m \neq [0]_m$ sind Nullteiler.
- Die Anzahl der Elemente mit einem multiplikativen Inversen ist genau $\varphi(m)$ (Eulersche φ-Funktion).
- Falls a invertierbar ist, d. h. $(a, m) = 1$, bestimmt man ein Inverses durch Raten oder indem wir eine lineare diophantische Gleichung lösen.

  $$[a]_m \cdot [x]_m = [1]_m \quad , \quad ax \equiv 1 \mod m$$

  Also finden wir eine Lösung für $ax = 1 + my$ in der Variablen (x, y) und behalten nur das x.
- Für $m = p \in \mathcal{P}$ sind $[1], \ldots, [p-1]$ Einheiten und es gint KEINE Nullteiler. Falls $m \notin \mathcal{P}$, entspricht jeder echte Teiler von m einer Restklasse, die ein Nullteiler ist.

Ein *reduziertes Restsystem modulo m* ist ein System von $\varphi(m)$ paarweise inkongruenter Zahlen mod m, welche zu m teilerfremd sind. D. h. diese zahlen ergeben die Restklassen, die Einheiten sind. Man erhält es aus einem vollstädnigen Restsystem modulo m, indem man alle Zahlen weglässt, die mit m einen Teiler $t > 1$ gemeinsam haben.

Der kleine Satz von Fermat

Sei $m \geq 2$. Dann gilt

$$(a, m) = 1 \iff a^{\varphi(m)} \equiv 1 \mod m$$

Korollar

Für $p \nmid a$ ist $a^{p-1} \equiv 1 \mod p$. Also gilt:

$$a^p \equiv a \mod p \quad \forall\, a \in \mathbb{Z}$$

IV Kongruenzsysteme: einfache Fälle

4.1 Eine lineare Kongruenz

Seien $m \geq 2$ und $a, b \in \mathbb{Z}$. Die Kongruenz

$$ax \equiv b \mod m$$

mit der Variablen x hat alle ganzen Zahlen x, sodass ax und b kongruent modulo m sind, als Lösungen. D. h. $m \mid (ax - b)$ oder äquivalent, $ax - b = my$ mit $x, y \in \mathbb{Z}$.
Falls es Lösungen gibt, sagen wir, dass die Kongruenz lösbar ist.
Bemerkung: Diese Kongruenz ist nur eine andere Schreibweise für die lineare diophantische Gleichung $ax + my = b$, wobei uns nur die möglichen Werte von x interessieren.
Genauer haben wir:

- Kongruenz $ax = b \mod m$ lösbar $\iff (a, m) \mid b$
- Falls lösbar, ist die Lösung eine Restklasse modulo

$$\frac{m}{(a, m)}$$

  und insbesondere eine Vereinigung von Restklassen modulo m.

Aufgabe

Falls man a oder b durch kongruente Zahlen ersetzt, bleibt die Lösungsmenge gleich.

4.2 Potenzen derselben Primzahl

Seien $p \in \mathcal{P}$, $r \geq 2$, $c_1, \ldots, c_r \in \mathbb{Z}$, $(e_1, \ldots, e_r) > 0$. Wir betrachten das System

$$\begin{cases} x \equiv x_1 \mod p^{e_1} \\ \quad \cdots \\ x \equiv c_r \mod p^{e^r} \end{cases}$$

Es gilt:

- Durch Umprdnen können wir annehmen, dass $e_1 \geq e_2 \geq \ldots \geq e_r$. Die Lösungsmenge ist entweder leer oder die Restklasse von c_1 modulo p^{e_1}. D. h. das System ist entweder NICHT lösbar oder äquivalent zu
$$x \equiv c_1 \mod p^{e_1}$$
- System lösbar $\iff c_1 \equiv c_h \mod p^{e_h} \quad \forall\, h \geq 2$

V Kongruenzsysteme: Paarweise teilerfremde moduli

5.1 Chinesischer Restsatz

Sei $r \geq 2$ und $m_1, \ldots, m_r \geq 2$ paarweise teilerfremd. Seien $a_1, \ldots, a_r \in \mathbb{Z}$. Dann hat das Kongruenzsystem
$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad\vdots \\ x \equiv a_r \mod m_r \end{cases}$$
als Lösungsmenge genau eine Restklasse modulo $m = m_1 \cdot \ldots \cdot m_r$.

Insbesondere gibt es ein $a \in \mathbb{Z}$, sodass obiges System zur Kongruenz
$$x \equiv a \mod (m_1 \cdot \ldots \cdot m_r)$$
äquivalent ist.

5.2 Verfahren für zwei Kongruenzen

Seien m_1, m_2 teilerfremd und $a_1, a_2 \in \mathbb{Z}$. Wir lösen das System
$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases}$$
Die Lösung ist (nach chinesischem Restsatz) eine Restklasse $[a]_m$ modulo m. Also ist das System äquivalent zu
$$x \equiv a \mod (m_1 \cdot m_2)$$
Wie findet man a?
Es gilt
$$a = a_1 x_1 + a_2 x_2$$
wobei x_1 und x_2 lösen bzw.
$$\begin{cases} x \equiv 1 \mod m_1 \\ x \equiv 0 \mod m_2 \end{cases} \forall\, j \neq i \qquad , \qquad \begin{cases} x \equiv 0 \mod m_1 \\ x \equiv 1 \mod m_2 \end{cases} \forall\, j \neq i$$

Nach Kongruenzrechnung gilt:

$$a = a_1x_1 + a_2x_2 \equiv a_1 \cdot 1 + a_2 \cdot 0 \equiv a_1 \mod m_1$$
$$a = a_1x_1 + a_2x_2 \equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_1 \mod m_1$$

Also ist a eine Lösung.
Wir können x_1 und x_2 durch eine lineare diophantische Gleichung berechnen. Zeige exemplarisch für x_1:
Wir suchen $x_1 \in \mathbb{Z}$ und $t_1, t_2 \in \mathbb{Z}$ so, dass $x_1 = 1 + m_1t_1 = m_2t_2$. Mit dem euklidischen Algorithmus finden wir eine Lösung $(t_{1,sp}, t_{2,sp})$ der linearen diophantischen Gleichung

$$1 + m_1t_1 = m_2t_2$$

Daher dürfen wir $x_1 = m_1t_{1,sp}$ nehmen.

VI Allgemeine Kongruenzsysteme

6.1 Drei Schritte

Seien $r \geq 2$, $m_1, \ldots, m_r \geq 2$ und $a_1, \ldots, a_r \in \mathbb{Z}$. Dann ist das Kongruenzsystem

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad\vdots \\ x \equiv a_r \mod m_r \end{cases}$$

entweder NICHT lösbar oder die Lösung ist genau eine Restklasse modulo des kgV $(m_1, \ldots, m_r)$.

- Sei $m \geq 2$ und $m = \prod_{p|m, p\in\mathcal{P}} p^{m_p}$ (kanonische Primfaktorzerlegung für m). Nach chinesischem Restsatz dürfen wir eine Kongruenz

  $$x \equiv a \mod m$$

  durch fpögende äquivalenten Kongruenzen ersetzen

  $$x \equiv a \mod p^{m_p}$$

  also eine Kongruenz pro Primteiler von m mit dem passenden Exponenten.

- Fasse Kongruenzen bzgl. Potenzen derselben Primzahl zusammen. Falls diese für eine Primzahl NICHT kompatibel sind, hat ursprüngliches System Lösungsmenge $\emptyset$. Falls kompatibel, behalten wir eine Kongruenz pro Primzahl, d. h. wir streichen überflüssige Kongruenzen weg.

- Nun sind wir im Fall teilerfremder Moduli. Fasse zwei Kongruenzen zusammen und er-

setze diese durch eine Kongreunz modulo des Produktes der Moduli. Jedesmal haben wir eine Kongruenz weniger, bis wir genau eine Kongruenz übrigbehalten, die einer Restklasse entspricht. Finde also Lösungsmenge, die eine Restklasse modulo des Produktes der Primzahlpotenzen ist, d. h. modulo des kgV der ursprünglichen Moduli.