Zahlentheorie - Eine Mitschrift

Heiko Studt
Florian Pein
Vorlesung: Prof. Niels Schwartz

03. November 2006 - 06. Februar 2007

Dies ist eine Mitschrift der Zahlentheorie-Vorlesung von Prof. Niels Schwartz im Wintersemester 2006/2007 an der Universität Passau. Die Vorlesung ist nahe am Buch **1. Buch-Verweis!** angelehnt, da dieses aber vergriffen war, gab es kein Script. Hiermit wird dies als Mitschrift "nachgeholt".

Inhaltsverzeichnis

1 Einführung

1.1 Themen

- Was sind Zahlen (halbes Semester)

  Natürliche Zahlen (Axiomatisch)

  ...

  Komplexe Zahlen

- Gleichungen / Ungleichungen

  Gleichungen in den Zahlbereichen

1.2 Auch Zahlentheorie, aber kein Thema der Vorlesung

- Primzahltheorie
  Beispiel:
  $3 \leq n \in \mathbb{N}$, $1 \leq r < n$
  r, $r+n$, $r+2n$ arithmetische Progression
  Fragestellung: Wieviele Primzahlen?

- Algebraische Zahlentheorie

- Analytische Zahlentheorie

2 Zahlenbereiche

2.1 Die natürlichen Zahlen - Existenz und Eindeutigkeit

Fragen

1. Sei $3 \leq n \in \mathbb{N}$. Gibt es $x, y, z \in \mathbb{N} : x^n + y^n = z^n$?
2. Sei $n \geq 4$ gerade. Gibt es 2 Primzahlen p, q mit $m = p + q$ (Goldbach'sche Vermutung)

Giuseppe Peano[1] (* 27. August 1858 in Spinetta, Piemont; † 20. April 1932 in Turin) war ein italienischer Mathematiker. Er arbeitete in Turin und befasste sich mit mathematischer Logik, mit der Axiomatik der natürlichen Zahlen (Entwicklung der Peano-Axiome) und mit Differentialgleichungen erster Ordnung.

Definition 1.1: Peano-System

Peano-System ist ein Tripel $(P, \nu, 0)$ bestehend aus:

- Menge P
- Abbildung $\nu : P \mapsto P$ (Nachfolgerabbildung: Nachfolger/ Vorgänger)
- einem ausgezeichnetem Element $0 \in P$

so daß gilt:

- $\forall x \in P : \nu(x) \neq 0$
- $\forall x, y \in P : \nu(x) = \nu(y) \Rightarrow x = y$
- Für jedes $Q \subseteq P$ gilt: $(0 \in Q \wedge x \in Q \Rightarrow \nu(x) \in Q) \Rightarrow (Q = P)$

Existenz beweisen wir nicht.

Eindeutigkeit

Definition 1.2: Isomorphismus

Seien $(P, \nu, 0)$, $(P', \nu', 0')$ Peano Systeme. $f : P \mapsto P$ ist Isomorphismus, wenn gilt:

- $f(0) = 0'$
- $f(\nu(x)) = \nu'(f(x))$
- f ist bijektiv

[1] http://de.wikipedia.org/wiki/Giuseppe_Peano

Satz 1.3: Für $0 \neq y$: Eindeutige Existenz des Nachfolgers

$(P, \nu, 0)$ Peano-System Sei $x \in P$. Daraus folgt $x = 0 \vee \exists! y \in P : x = \nu(y)$.

Beweis:
Eindeutigkeit: ν ist Injektiv
Existenz von y: Sei $M = \{x \in P | x = 0 \vee \exists y \in P : x = \nu(y)\}$
Beweis: $M = P$(Induktion)

- $0 \in M \surd$
- $x \in M \Rightarrow \nu(x) \in M$: $\forall x \in P : \nu(x) \in M \surd$

$\Rightarrow M = P \surd$

Satz 1.4: (rekursive) Abbildungen

$(P, \nu, 0)$, $\emptyset \neq S$: Menge. Sei $c \in S$, $G : P \times S \mapsto S$ Es gibt genau eine Abbildung $F : P \mapsto S$ mit.

(a) $F(0) = c$

(b) $F(\nu(x)) = G(x, F(x))$

Beispiele:

- $F(0) = c$
- $F(\nu(0)) = G(0, c)$
- $F(\nu(\nu(0))) = G(\nu(0), F(\nu(0))) = G(\nu(0), G(0, c))$

Beweis:
Eindeutigkeit: Seien F, F' Abbildungen $P \mapsto S$ mit den Eigenschaften. Setze $M = \{x \in P | F(x) = F'(x)\}$ Zu Zeigen: $M = P$.

- $0 \in M \surd$
- $F(x) = F'(x) \Rightarrow G(x, F(x)) = G(x, F'(x)) = F(\nu(x)) = F'(\nu(x))$

Existenz: Definiere F über den Graphen ($F \subseteq P \times S$)

(a) $(0, c) \in F$

(b) $\forall x \in P : (x, y) \in F \Rightarrow (\nu(x), G(x, y)) \in F$

(c) F Abbildung: $\forall x \in P : \exists s \in S : (x, s) \in F$

(d) $\forall x \in P : \forall s, t \in S : (x, s), (x, t) \in F \Rightarrow s = t$

Da F eine Relation ist, gilt mit den Eigenschaften (a) und (b) auch (c) für F.

Beweis:
Setze $M = \{x \in P | \exists s \in S : (x, s) \in P\}$. (Zu Zeigen: $M = P$)
Sei $\mathfrak{R}$ die Menge aller Relationen. $R \subseteq P \times S$, die (a) und (b) erfüllen. $\mathfrak{R} \neq \emptyset$: $P \times S \in \mathfrak{R}$
Setze $F = \bigcap_{R \in \mathfrak{R}} R$. ($\Rightarrow$ kleinste Relation mit den Eigenschaften!)
Beweis: F erfüllt (a) - (d)

(a) $\surd$

(b) Sei $x \in P \Rightarrow (x, y) \in F \subseteq R, R \in \mathfrak{R}$ beliebig. $\Rightarrow (\nu(x), G(x, y)) \in R$: $\forall R \in \mathfrak{R} \Rightarrow (\nu(x), G(x, y)) \in F \surd$

(c) folgt aus (a) und (b) $\surd$

(d) Setze $M = \{x \in P | \forall s, t \in S : ((x, s) \in F \wedge (x, t) \in F) \Rightarrow s = t\}$

Beweis: $M = P$ (Induktionsbeweis)

- $0 \in M$: Es ist $(0, c) \in F$
  Zu Zeigen: Wenn $(0, s) \in F$, dann ist $s = c$.
  Annahme: $\exists s \neq c$: $(0, s) \in F$
  Def: $R = F \backslash \{(0, s)\} \subsetneq F$
  Behauptung: R hat (a) + (b)
  - (a) $(0, c) \neq (0, s) \Rightarrow (0, c) \in R$
  - (b) Sei $x \in P$, $(x, y) \in R \subseteq F \Rightarrow (0, G(x, y)) \neq (\nu(x), G(x, y)) \in F \Rightarrow (\nu(x), G(x, y)) \in R$ ↯(zur Minimalität von F)
- $x \in M \Rightarrow \nu(x) \in M$
  Behauptung: Sei $(\nu(x), w) \in F \Rightarrow \exists s \in S : (x, s) \in F \wedge w = G(x, s)$
  Annahme: Behauptung falsch.
  $\exists x \in P \exists w \in S \forall s \in S : ((x, s) \in F \vee (w \neq G(x, s)) \wedge (\nu(x), w) \in F)$
  Setze $R = F \backslash \{(\nu(x), x)\} \subsetneq F$.
  Zu Zeigen: R hat (a) + (b)
  (a) $(o, c) \in F$ $(0, c) \neq (\nu(x, w) \Rightarrow (0, c) \in R$
  (b) Sei $(z, t) \in R \Rightarrow (\nu(z), G(z, t)) \in R$
  $(z, t) \in R \Rightarrow (z, t) \in F \Rightarrow (\nu(z), G(z, t)) \in F$
  Dabei ist $(\nu(z), G(z, t)) \neq (\nu(x), w)$
  Annahme: Gleich. $\Rightarrow \nu(z) = \nu(x) \Rightarrow z = x$, $w = G(z, t) \Rightarrow (z, t) = (x, t) \notin F$ ↯zu $(z, t) \in F$
  Da $\nu(x) \in M$ heißt dies: $(\nu(x), s) \in F \wedge (\nu(x), t) \in F \Rightarrow s = t$
  Behauptung liefert $s' \in S$, $t' \in S$ mit $(x, s') \in F$, $(x, t') \in F \wedge s = G(x, s')$, $t = G(x, t')$
  Weil $x \in M \Rightarrow s' = t' \Rightarrow s = t$.

Satz 1.5: Isomorphie aller Peano-Systeme

$(P, \nu, 0)$, $(P, \nu, 0)2$ Peano-Systeme sind isomorph.

Beweis:
In Satz 1.4 setze $S = P'$, $c = 0'$, $G : P \times P' \mapsto P' : (x, x') \mapsto \nu'(x') \Rightarrow \exists! F : P \mapsto P'$ mit $F(0) = 0'$, $F(\nu(x)) = G(x, F(x)) = \nu'(F(x))$
F ist Homomorphismus (siehe Grundstudium), noch zu Zeigen: F bijektiv.

Beweis: Surjektivität
Setze $M' = \{y \in P' | \exists x \in P : y = F(x)\}$. Zu Zeigen $M' = P'$

- $0' \in M'$: $F(0) = 0' \in M'$
- $y \in M' \Rightarrow \nu'(y) \in M'$: Sei $F(x) = y \Rightarrow \nu'(y) = \nu'(F(x)) = F(\nu(x)) \in M'$

Beweis: Injektivität
$M = \{x \in P | \forall z \in P : F(x) = F(z) \Rightarrow x = z\} = \{x \in P | F^{-1}(F(x)) = \{x\}\}$. Zu Zeigen: $M = P$

- $0 \in M$:

  Beweis: $F(0) = 0'$

  Annahme: $x \in P$, $x \neq 0$ mit $F(x) = 0'$. Weil $x \neq 0$: $\exists y \in P : x = \nu(y) \Rightarrow F(x) = F(\nu(y)) = \nu'(F(y))$ d.h. $0' = F(x)$ ist Nachfolger. ↯

- Sei $x \in M \Rightarrow \nu(x) \in M$:

  Beweis:

  Sei $y \in P : F(y) = F(\nu(x))$
  Annahme $y = 0$: $F(y) = 0'$, d.h. $\underbrace{F(\nu(x))}_{=\nu'(F(x))} = 0'$ ↯
  Falls $y \neq 0$: $\Rightarrow \exists z \in P : y = \nu(z)$. $\nu'(F(x)) = F(\nu(x)) = F(y) = F(\nu(z)) = \nu'(F(z))$
  $\Rightarrow F(x) = F(z) \underbrace{\Rightarrow}_{x \in M} x = z \Rightarrow \nu(x) = \nu(z) = y$

2.2 Natürliche Zahlen - Arithmetische Operationen

Einführung

Weil wir wissen $\mathbb{N}$ ist Peano-System, muss es auf jedem Peano-System Rechenoperationen geben. Hierbei ist die Induktion ein zentraler Begriff. Da das Arbeiten mit $\mathbb{N}$ schnell verwirren würde, was wir bereits haben und was wir aus Schul- oder Grundstudiumswissen kennen, wird in diesem Kapitel streng nach Peano-Systemen gearbeitet.

Satz 2.1: (rekursive) Abbildungen innerhalb Peano-Systeme

Peano-System $(P, \nu, 0)$, Abbildung $G : P \times P \mapsto P$, $H : P \mapsto P \Rightarrow \exists! F : P \times P \mapsto P$ mit folgenden Eigenschaften:

(a) F ist Abbildung

(b) $F(x, 0) = H(x)$

(c) $F(x, \nu(y)) = G(x, y, F(x, y))$

Beispiel: Addition: $H(x) = x$, $G(x, y, z) = \nu(z)$

Beweis:
Sei $x \in P$ fest. Sei $c_x = H(x)$. $G_x : P \times P \mapsto P$: $G_x(y, z) = G(x, y, z)$ In Satz 1.4: $S = P$, $c = c_x$, $G = G_x$
$\Rightarrow \exists! F_x : P \mapsto P$ mit $F_x(0) = c_x$, $F_x(\nu(y)) = G_x(y, F_x(y))$ (Rücksubstituieren)
Wenn x variiert: $F : P \times P \mapsto P : (x, y) \mapsto F_x(y)$ $F = \{(x, y, z) \in P \times P \times P | z = F_x(y)\}$

- *F* **Abbildung:**
  Für $(x, y) \in P \times P$: $(x, y, F_x(y)) \in F$ Seien $(x, y, z) \in F$, $(x, y, z') \in F$.
  Behauptung: $z = z'$
  $z = F_x(y) = z' \surd$
- *$F(x, 0) = H(x)$*
  $F(x, 0) = F_x(0) = c_x = H(x) \surd$
- *$F(x, \nu(y)) = G(x, y, F(x, y))$*
  $F(x, \nu(y)) = F_x(x, \nu(y)) = G_x(y, F_x(y)) = G(x, y, F(x, y))$

Eindeutigkeit:
Seien F, F' zwei solche Abbildungen. Zu Zeigen: $\forall x \in P : F_x = F'_x$.

Beweis:
$M = \{y \in P | F_x(y) = F'_x(y)\}$

- $0 \in M$: $F_x(0) = F(x, 0) = H(x) = F'(x, 0) = F'_x(0)$
- $y \in M \Rightarrow \nu(y) \in M$:
  $F_x(\nu(y)) = F(x, \nu(y)) = G(x, y, F(x, y)) = G(x, y, F_x(y)) \underbrace{=}_{y \in M} G(x, y, F'_x(y)) = G(x, y, F'(x, y))$
  $= F'(x, \nu(y)) = F'_x(\nu(y))$

Korollar 2.2:

$G : P \times P$, $H : P \mapsto P$ Abbildungen $\Rightarrow \exists! F : P \times P \mapsto P$ Abbildung mit

(a) $F(x, 0) = H(x)$

(b) $F(x, \nu(y)) = G(x, F(x, y))$

Beweis:
In Satz 2.1 setze: $H_1 = H_2$, $G_1(x, y, z) = G_2(x, z)$. Daraus bekommt man ein eindeutiges $F_1 : P \times P \mapsto P$ mit

(a) $F_1(x, 0) = H_1(x)$

(b) $F_1(x, \nu(y)) = G_1(x, y, F_1(x, y))$

Setze $F_2 = F_1$, dann sind die Bedingungen erfüllt!

Definition 2.3: Addition im Peano-System

Setze in Korollar 2.2 $G(x, y) = \nu(y)$, $H(x) = x$. Dann wird die dadurch bestimmte Abbildung $\alpha : P \times P \mapsto P$ als Addition bezeichnet.

$\boxed{x + y := \alpha(x, y)}$

Rechenregeln:

R1 $x + 0 = \alpha(x, 0) = H(x) = x$

R2 $x + \nu(y) = \alpha(x, \nu(y)) = G(x, \alpha(x, y)) = \nu(\alpha(x, y)) = \nu(x + y)$

$\boxed{1 := \nu(0)}$

Lemma 2.4: $\nu(x) = x + \nu(0)$

$\nu(x) = x + \nu(0)$

Beweis:
$\nu(x) = \nu(x + 0) = x + \nu(0)$ (R2)

Satz 2.5: Assoziativgesetz

$x + (y + z) = (x + y) + z$

Beweis:
$x, y \in P$ fest. Setze $M = \{z \in P | x + (y + z) = (x + y) + z\}$
Zu Zeigen: $M = P$ (Induktion)

- $0 \in M$: $x + \underbrace{(y + 0)}_{=y} = x + y \underbrace{=}_{R1} (x + y) + 0.$
- $z \in M \Rightarrow \nu(z) \in M$: $x + (y + \nu(z)) \underbrace{=}_{R2} x + \nu(y + z) \underbrace{=}_{R2} \nu(x + (y + z)) \underbrace{=}_{z \in M} \nu((x + y) + z) \underbrace{=}_{R2} (x + y) + \nu(z)$

Satz 2.6: Kommutativgesetz der Addition

Sei $(P, \nu, 0)$ ein Peano-System.
Dann gilt: $\forall x, y \in P : x + y = y + x$

Beweis:
Sei $x \in P$ fest
Setze $M = \{y \in P | x + y = y + x\}$
Zu zeigen: $M = P$
Dies geschieht durch Induktion. Es ist zu beachten, dass der Induktionsanfang hier zweiteilig ist:
$0 \in M$**:**

Beweis:
$N = \{z \in P | z + 0 = 0 + z\}$
Zu zeigen: $N = P$
$0 \in N$**:** $0 + 0 = 0 + 0$
$z \in N \rightarrow z + 1 \in N$**:** $(z + 1) + 0 = \nu(z) + 0 = \nu(z) = \nu(z + 0) = \nu(0 + z) = 0 + \nu(z) = 0 + (z + 1)$

$1 \in M$:

Beweis:

Setze $R = \{z \in P | z + 1 = 1 + z\}$
$0 \in R$: $0 + 1 = 1 + 0$ $(Tipp: N = P, vgl. oben)$
$y \in R \rightarrow y + 1 \in R$: $(y + 1) + 1 = (1 + y) + 1 = 1 + (y + 1)$

$y \in M \rightarrow y + 1 \in M$:

Beweis:

$$x + (y + 1) \underbrace{=}_{Asso} (x + y) + 1 \underbrace{=}_{IAnn} (y + x) + 1 \underbrace{=}_{Asso} y + (x + 1) \underbrace{=}_{IAnf} y + (1 + x) \underbrace{=}_{Asso} (y + 1) + x$$

Satz 2.7: Kürzungsregel

$x + z = y + z \Rightarrow x = z$ (ohne Beweis)

Satz 2.8: Einschränkung der Darstellungsmöglichkeit von $y \in P$

Sei $x \in P$, $x \neq 0$.
Dann gilt: $y \neq y + x$ (ohne Beweis)

Satz 2.9: Trichotomie

Sei $(P, \nu, 0)$ ein Peano-System. $\forall x, y \in P$ gilt genau eine der folgenden Aussagen:

(a) $x = y$

(b) $\exists u \in P$, $u \neq 0$: $y = x + u$

(c) $\exists v \in P$, $v \neq 0$: $x = y + v$

Zum einen ist nun zu zeigen, dass nur höchstens eine der drei Aussagen der Trichotomie gelten kann.

Beweis:

(a) und (b) gelten nicht gleichzeitig.
Annahme: (a) und (b) gelten gleichzeitig
Dann muss gelten:
$x \underbrace{=}_{(a)} y \underbrace{=}_{(b)} x + u$ ↯($u \neq 0$ weil (b) gilt + s. vorausgehender Satz)
Der Beweis dass (a) und (c) nicht gleichzeitig gelten können verläuft analog.
Es bleibt zu zeigen, dass (b) und (c) nicht gleichzeitig gelten können.
Annahme: (b) und (c) gelten beide für $x, y \in P$
Dann muss gelten:
$y \underbrace{=}_{(b)} x + u \underbrace{=}_{(c)} (y + v) + u \underbrace{=}_{Asso} y + (v + u)$
Wiederum mit dem vorausgehenden Satz erhält man $v + u = 0$.(*)
(b) und (c) könnten trotzdem noch gleichzeitig gelten. Insbesondere liefert uns jedoch (b):
$u \neq 0$
Daraus folgt u ist Nachfolger eines $w \in P$ wegen Satz 1.1.3.
$u \underbrace{=}_{1.1.3} \nu(w)$
Daher gilt: $v + u = v + \nu(w) = \nu(v + w) \underbrace{\neq}_{1.P.-Ax.} 0$ ↯(zu (*))
Das heisst (b) und (c) können nicht gleichzeitig gelten.

Zum anderen muss noch gezeigt werden, dass immer mindestens eine der drei Aussagen der Trichotomie zutrifft.

Beweis:
Sei $y \in P$ fest.
Setze $M = \{x \in P |$ Für x,y gilt (a) oder (b) oder (c)$\}$
Zu zeigen: $M = P$

- $0 \in M$:
  Falls $y = 0$: (a) gilt. Falls $y \neq 0$: $y = 0 + y$, d.h. (b) gilt.
- $x \in M \rightarrow x + 1 \in M$:
  - Für x, y gelte (a), d.h. $x = y$.
    Daraus folgt $x + 1 = y + 1$, d.h. (c) gilt
  - Für x, y gelte (c), d.h. $x = y + u$ und $u \neq 0$
    $x + 1 = (y + u) + 1 = y + (u + 1)$, d.h. (c) gilt
  - Für x, y gelte (b), d.h. $y = x + u$ und $u \neq 0$
    $u \neq 0 \Rightarrow \exists w : u = r(w) = w + 1$
    $y = x + (w + 1) = (x + 1) + w$
    Fall 1: $w = 0$: x+1,y erfüllen (a)
    Fall 2: $w \neq 0$: x+1,y erfüllen (b)

Definition 2.10: Multiplikation von natürlichen Zahlen

Setze in Korollar I.2.2:

- $G = \alpha$: $P \times P \rightarrow P$ (Erinnerung: α ist die Addition)
- H: $P \rightarrow P$: $x \mapsto 0$

Dann gibt es eine Abbildung μ: $P \times P \rightarrow P$ mit:

- $\mu(x, 0) = H(x) = 0$
- $\mu(x, \nu(y)) = \alpha(x, \mu(x, y)) = x + \mu(x, y)$

μ heisst Multiplikation auf den natürlichen Zahlen
Schreibweisenvereinbarung: $\boxed{a \cdot b := \mu(a, b)}$
Aus der Definition der Multiplikation folgt(sieht man) sofort:

- $x \cdot 0 = 0$
- $x \cdot (y + 1) = x + x \cdot y$

Satz 2.11: Multiplikation mit Null von links

Sei $(P, \nu, 0)$ ein Peano-System.
Für alle $x \in P$ gilt: $0 \cdot x = 0$

Beweis:
Sei $M = \{x \in P | 0 \cdot x = 0\}$
Zu zeigen: $M = P$

- $0 \in M$: $0 \cdot 0 = 0$ (Definition von μ bzw „$\cdot$“)
- $x \in M \rightarrow x + 1 = \nu(x) \in M$:
  $0 \cdot (x + 1) = \mu(0, \nu(x)) = \alpha(0, \mu(0, x)) = 0 + \mu(0, x) = \mu(0, x) = 0 \cdot x = 0$

Satz 2.12: Beidseitige Neutralität der Eins

Sei $(P, \nu, 0)$ wieder ein Peano-System.
Behauptung: $x \cdot 1 = x = 1 \cdot x$

Beweis:

- $x \cdot 1 = x$:
  $x \cdot 1 = \mu(x, \nu(0)) = \alpha(x, \mu(x, 0)) = x + \mu(x, 0) = x + x \cdot 0 = x + 0 = x$
- $1 \cdot x = x$:
  Sei $M = \{x \in P | 1 \cdot x = x\}$
  - $0 \in M$: $1 \cdot 0 = 0$ (Definition von μ)
  - $x \in M \rightarrow x + 1 \in M$:
    $1 \cdot (x + 1) = \mu(1, \nu(x)) = \alpha(1, \mu(1, x)) = 1 + \mu(1, x) = 1 + 1 \cdot x = 1 + x = x + 1$

Satz 2.13: Rechtsdistributivität

Sei $(P, \nu, 0)$ wieder ein Peano-System.
Dann gilt: $(x + y) \cdot z = x \cdot z + y \cdot z$

Beweis:

Seien x,y fest aber beliebig.
Setze $M = \{z \in P | (x + y) \cdot z = x \cdot z + y \cdot z\}$
Zu zeigen: $M = P$

- $0 \in M$: $(x + y) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + y \cdot 0$
- $x \in M \rightarrow x + 1 \in M$:
  $(x + y) \cdot (z + 1) = \mu((x + y), \nu(z)) = \alpha((x + y), \mu((x + y), z)) = (x + y) + (x + y) \cdot z = (x + y) + x \cdot z + y \cdot z =$
  $(x+x \cdot z)+(y+y \cdot z) = \alpha(x, \mu(x, z))+\alpha(y, \mu(y, z)) = \mu(x, \nu(z))+\mu(y, \nu(z)) = x \cdot \nu(z)+y \cdot \nu(z) = x \cdot (z+1)+y \cdot (z+1)$

Satz 2.14: Kommutativität der Multiplikation

Sei $(P, \nu, 0)$ ein Peano-System. Dann gilt: $\forall x, y \in P : x \cdot y = y \cdot x$

Beweis:

Wähle x beliebig aber fest.
Sei $M = \{y \in P | x \cdot y = y \cdot x\}$
Zu zeigen: $M = P$

- $0 \in M$: $x \cdot 0 \underbrace{=}_{Def.v.\mu} 0 \underbrace{=}_{I.2.11} 0 \cdot x$
- $y \in M \rightarrow y + 1 \in M$
  $x \cdot (y+1) = \mu(x, y+1) = \mu(x, \nu(y)) = \alpha(x, \mu(x, y)) = x+x \cdot y \underbrace{=}_{Ind.ann.} x+y \cdot x = y \cdot x+x = y \cdot x+1 \cdot x \underbrace{=}_{I.2.13} (y+1) \cdot x$

Satz 2.15: Assoziativität der Multiplikation

Sei $(P, \nu, 0)$ ein Peano-System.
Dann gilt: $\forall x, y, z \in P : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (ohne Beweis)

Satz 2.16: Kürzungsregel der Multiplikation

Sei $(P, \nu, 0)$ ein Peano-System.
Dann gilt: $\forall x, y, z \in P$: $z \neq 0 \Rightarrow ((x \cdot z = y \cdot z) \Rightarrow x = y)$ (ohne Beweis)

2.3 Die natürlichen Zahlen - Anordnung

Definition 3.1: Symbolik der Ordnungsrelation

Sei $(P, \nu, 0)$ ein Peano-System und $x, y \in P$.
Dann definieren wir:

- $x < y$, falls $\exists u \in P : u \neq 0$ und $y = x + u$
- $x > y$, falls $\exists u \in P : u \neq 0$ und $x = y + u$
- $x \leq y$, falls $x = y$ oder $x < y$
- $x \geq y$, falls $x = y$ oder $x > y$

Satz 3.2: Trichotomie und Transitivität

Sei $(P, \nu, 0)$ ein Peano-System und seien $x, y, z \in P$.
Es wird behauptet, dass folgende Sachverhalte gelten:

(a) Trichotomie: $(x < y) \vee (x = y) \vee (x > y)$

(b) Transitivität: $((x < y) \wedge (y < z)) \Rightarrow x < z$

Beweis:

(a) Siehe Satz I.2.9

(b) Aus $x < y$ und $y < z$ folgt:
$\left.\begin{array}{l} y = x + u,\ u \neq 0 \\ z = y + v,\ v \neq 0 \end{array}\right\} \Rightarrow z = (x + u) + v = x + (u + v)$
Wenn jetzt $u + v \neq 0$ wäre, so würde gelten: $z > x$
Das lässt sich aber wie folgt sehen:
Da $v \neq 0$ gibt es ein $k \in P$ mit $v = \nu(k)$ (Satz I.1.3)
Daraus folgt: $u + v = u + \nu(k) = \alpha(u, \nu(k)) = \nu(\alpha(u, k)) = \nu(u + k) \underbrace{\neq}_{1.P.-Ax.} 0$

Satz 3.3: Totalität der Ordnung

$\leq$ ist totale Ordnung auf P.

Beweis:

1. Reflexivität
   $x \leq x$ nach Definition
2. Antisymmetrie
   Sei $\underbrace{x \leq y}_{\Rightarrow x=y \vee x<y}$ und $\underbrace{y \leq x}_{\Rightarrow x=y \vee y<x}$.
   Annahme: $x \neq y$
   $\Rightarrow x < y$ und $x > y$ ↯wegen Trichotomie
3. Transitivität
   Seien $x \leq y$ und $y \leq z$.
   Fallunterscheidung:
   - $(x = y \wedge y = z) \Rightarrow x = z \Rightarrow x \leq z$
   - $(x = y \wedge y < z) \Rightarrow x < z \Rightarrow x \leq z$
   - $(x < y \wedge y = z) \Rightarrow x < z \Rightarrow x \leq z$
   - $(x < y \wedge y < z) \Rightarrow x < z$ (Satz I.3.2(b))

Die Totalität folgert man so:
Seien $x, y \in P \underbrace{\Rightarrow}_{Trichotomie} \underbrace{x = y}_{\Rightarrow x \leq y} \vee \underbrace{x < y}_{\Rightarrow x \leq y} \vee \underbrace{x > y}_{\Rightarrow y \leq x}$

Totalgeordnete Mengen sind i.a. nicht Peano-Systeme.
Beispiel: Anordnung der (als „bekannt“ vorausgesetzten) ganzen Zahlen. Die ganzen Zahlen haben kein kleinstes Element. Die natürlichen Zahlen sehr wohl:

Satz 3.4: Kleinstes Element von Peano-Systemen

In $(P, \nu, 0)$ ist 0 kleinstes Element.

Beweis:
Sei $x \in P$, $x \neq 0$.
Wegen $x = 0 + x$, $x \neq 0$ gilt $0 < x$.

Aber auch die Eigenschaft ein kleinstes Element zu besitzen als Zusatz zur Totalität einer Ordnungsrelation ist nicht ausreichend um eine beliebige Menge mit einer darauf definierten Ordnung als geordnetes Peano-System identifizieren zu können.
Beispiel: $[0, \infty) \subset \mathbb{R}$ ist total geordnet und hat ein kleinstes Element. Da aber mit zwei verschiedenen Punkten in diesem Intervall immer das arithmetische Mittel dieser Punkte echt zwischen ihnen liegt, ist es unmöglich die Nachfolgerfunktion auf diesem Intervall zu erklären. Die Aussage die den Widerspruch herstellt ist in Lemma I.3.6(d) formuliert.

Satz 3.5: Wohlordnung der natürlichen Zahlen

Jede Teilmenge $S \subseteq P$ hat ein kleinstes Element.

Lemma 3.6:

(a) $x < \nu(x)$

(b) $x < \nu(y) \Leftrightarrow x \leq y$

(c) $\nu(x) \leq y \Leftrightarrow x < y$

(d) Es gibt kein $z \in P$ mit $x < z < \nu(x)$

Beweis:

(a) $\nu(x) = x + 1$

(b) „$\Leftarrow$“:
($x \leq y$ und nach (a) $y < \nu(y)$) $\Rightarrow x < \nu(y)$
„$\Rightarrow$“:
Annahme: $y < x$, d.h. $x = y + u$, $u \neq 0$
$u \neq 0 \Rightarrow u = \nu(v) = v + 1$
D.h. $x = y + (v + 1) = (y + 1) + v$
$v = 0$: $x = \nu(y)$ $\lightning$ $v \neq 0$: $x > \nu(y)$ $\lightning$

(c) „$\Rightarrow$“:
Nach (a) ist $x < \nu(x)$, daraus folgt diese Richtung nach einer kleinen Fallunterscheidung ($\nu(x) = y$ oder $\nu(x) < y$)
„$\Leftarrow$“:
Annahme: $\nu(x) > y$, d.h. $\nu(x) = y + u$, $u \neq 0$
$u = \nu(z) = z + 1$
Fallunterscheidung:

- $z = 0$: $\nu(x) = y + \nu(0) = y + 1 = \nu(y) \underbrace{\Rightarrow}_{\nu inj.} x = y$ (1)

- $z \neq 0$: $\nu(x) = y + \nu(z)$, $z \neq 0$ $\nu(x) = y + \nu(z) = \nu(y + z)$
  $\underbrace{\Rightarrow}_{\nu inj.}$ $x = y + z$
  Das heisst aber $y < x$ (2)

Somit haben wir die Kontraposition von „$\Leftarrow$“ bewiesen und diese Richtung ist bewiesen.

(d) Sei $x < z \underbrace{\Rightarrow}_{(c)} \nu(x) \leq z$

Das war der Beweis des Lemmas.
Es folgt der Beweis des Satzes I.3.5:

Beweis:
Annahme:
$S \subseteq P$, $S \neq \emptyset$, S hat kein kleinstes Element
Sei $D = \{x \in P | \forall s \in S : x < s\}$

- $D \cap S = \emptyset$ (*)
  Falls $y \in D \cap S : y < y$ ↯(Trichotomie, $y = y$)
  Behauptung: $D = P$

  Beweis:

  - $0 \in D$:
    Falls $0 \notin D : \exists s \in S : s \leq 0 \Rightarrow 0 \in S$ Dann wäre aber 0 sofort kleinstes Element von S, im Widerspruch zur Voraussetzung.
  - $x \in D \rightarrow \nu(x) \in D$
    Annahme: $\nu(x) \notin D \Rightarrow \exists s \in S : s \leq \nu(x)$
    $x \in D \Rightarrow x < s$
    Dann ist $s \underbrace{=}_{l.Lem.(d)} \nu(x)$ Weil aber S kein kleinstes Element hat nach Vorraussetzung, muss es ein $t \in S$ derart geben dass gilt:
    $x < t < s = \nu(x)$ ↯(letztes Lemma, Teil (d))

- D.h. $D = P$ daraus folgt $D \cap S = P \cap S = S$
  $S \neq \emptyset$ nach Voraussetzung ↯(zu (*))

Definition 3.7: Wohlgeordnete Menge

$(M; \leq)$ sei total geordnete Menge.
M ist wohlgeordnet, wenn jeder nicht-leere Teilmenge ein kleinstes Element hat.

Satz 3.8:

Es gibt wohlgeordnete Mengen, die nicht angeordnete Mengen eines Peano Systems sind.

Beweis:
Wir zeigen ein Beispiel für eine wohlgeordnete Menge die kein Peano-System ist.
Die betrachtete Menge ist:
$P \times \{1, 2\}$
Eine Ordnung wird wie folgt darauf definiert:
$(x, i) \leq (y, j)$, falls

- $i = 1$ und $j = 2$ oder
- $i = j$ und $x \leq y$

Damit sind alle Elemente aus $P \times \{1, 2\}$ vergleichbar und diese Menge ist totalgeordnet.
Anders ausgedrückt: $(P \times 1, 2, \leq)$ ist Totalordnung.
Ist $(P \times 1, 2, \leq)$ auch wohlgeordnet?
Sei $\emptyset \neq S \subseteq P \times \{1, 2\}$

Falls es in S ein Element $(x,1)$ gibt:
Setze $M = \{y \in P | (y,1) \in S\}$
$M \neq \emptyset$, da $x \in M$
M hat kleinstes Element z.
$\Rightarrow (z,1)$ kleinstes Element in S.
Falls $S \subseteq P \times \{2\}$:
Setze $M = \{y \in P | (y,2) \in S\}$, es folgt $M \neq \emptyset$
Wenn z das kleinste Element von M ist, so $(z,2)$ kleinstes Element von S.
Kleinstes Element der gesamten Menge S ist $(0,1)$.
Falls $P \times \{1,2\}$ angeordnete Menge eines Peano-Systems ist, muss jedes $(x,i) \neq (0,1)$ Nachfolger sein.
Aber: $(0,2)$ ist kein Nachfolger!
Annahme: $\exists (x,i)$ mit $\nu(x,i) = (0,2)$
$\Rightarrow (x,i) < (0,2)$, d.h. $i = 1$
Nach dem letzten Lemma darf es kein Element geben das echt zwischen diesen beiden Paaren liegt.
Aber: $(x,1) < (\nu(x),1) < (0,2)$

Definition: $a \precnsim b$ ist Kurzschreibweise für $a \prec b \wedge a \neq b$.

Satz 3.9: Korrelation Nachfolger/Anordnung

M $\neq \emptyset$ mit (Ordnungs-)Relation $\prec$.
Gelte:

(a) $\prec$ ist totale Ordnung. (Reflexiv, Transitiv, Antisymmetrisch).

(b) Wohlordnungseigenschaft: Jede Teilmenge von M hat kleinstes Element.
Das kleinste Element von M: μ

(c) Für $a \in M$ gibt es ein $b \in M$ mit:

- $a \precnsim b$
- Ist $a \precnsim c$, so ist $b \prec c$ $\qquad (b = \nu(a))$

(d) Für jedes $a \in M$, $a \neq \mu$ gibt es ein $b \in M$ mit

- $b \precnsim a$
- Ist $c \precnsim a$, so ist $c \prec b$ $\qquad (a = \nu(b))$

Definiere $\sigma : M \mapsto M$: $a \mapsto b$, falls ($a \precnsim b$ und $a \precnsim c$) $\Rightarrow b \prec c$
Dann ist (M, σ, μ) ein Peano-System, die Anordnung $\prec$ ist die zum Peano-System gehörige Anordnung.

Beweis:
σ ist Abbildung, Eindeutigkeit von b in (c). Sei $a \in M$, seien $b, b' \in M$, so daß b, b' beide die Bedingungen in (c) erfüllen. $(a \precnsim b;\ a \precnsim b') \Rightarrow (b \prec b',\ b' \prec b) \underbrace{\Rightarrow}_{\text{Antisymmetrie}} b = b'$
Zu Beweisen ist nun, dass die Axiome eines Peano-Systems gelten.

- $\forall a \in M$: $\mu \neq \sigma(a)$
  Angenommen: $\mu = \sigma(a) \Rightarrow a \precnsim \mu$, $\lightning$(μ kleinstes Element von M)
- σ injektiv.
  Sei $\sigma(a) = c = \sigma(b) \Rightarrow a \precnsim c \wedge b \precnsim c$.
  Totalität: $a \prec b \vee b \prec a$
  Annahme: $a \not\prec b \Rightarrow b \precnsim a \Rightarrow b \precnsim a \precnsim c$ $\lightning$(Definition von σ)
  $b \not\prec a$ analog.
  $\underbrace{\Rightarrow}_{Antisymmetrisch} a = b$

- (Induktionsprinzip) Sei ($S \subseteq M$: $\mu \in S$ und $a \in S \Rightarrow \sigma(a) \in S$) $\Rightarrow S = M$. d.h. $M \backslash S = \emptyset$

  Annahme: $M \backslash S \neq \emptyset$

  $\underbrace{\Rightarrow}_{Wohlordnung}$ Es existiert kleinstes Element $a \in M \backslash S$

  Es ist $a \neq \mu$, da $\mu \in S$ nach Vorraussetzung. Wegen (d): $\exists b \in M : b \precsim a$ und ist $c \precsim a$, so ist $c \prec b$. Dabei ist $b \ni M \backslash S$, d.h. $b \in S \Rightarrow \sigma(b) \in S$.

  Behauptung: $\sigma(b) = a$

  Annahme: $\sigma(b) \neq a$ d.h. $\overbrace{\underbrace{a \precsim \sigma(b)}_{(1)} \vee \underbrace{a = \sigma(b)}_{(2)} \vee \underbrace{\sigma(b) \precsim a}_{(3)}}^{Trichitonie}$

  (1) $b \precsim \sigma(b)$, $b \precsim a \Rightarrow \sigma(b) < a$ ↯

  (2) ↯zur Vorraussetzung.

  (3) Falls $\sigma(b) \precsim a$: $b \precsim \sigma(b) \precsim a$ ↯(Wohlordnung von b)

  Wegen $b \in S$ ist $\sigma(b) = a \in S$ ↯

  $\Rightarrow$ Es ist ein Piano-System.

  Noch zu tun: Ordnung

  $\leq$: Totale Ordnung des Peano-Systems (M, σ, μ)

  Behauptung: "$\leq$" = "$\prec$"

  Induktion Sei $a \in M$. Setze $S = \{b \in M | a \leq b \overbrace{\Rightarrow}^{\text{equiv. zu } \Leftrightarrow \text{SEE}\ [2]} a \prec b\}$. Zu Zeigen: $S = M$

  - $\mu \in S$: Falls $a \neq \mu$: Ausage "$a \leq \mu$" falsch $\Rightarrow$ Implikation richtig.
  - Sei $c \in S$. Behauptung: $\sigma(c) \in S$.

    Falls $\sigma(c) < a$: Vorraussetzung der Induktion falsch, damit Implikation richtig.

    Falls $\sigma(c) = a$: $\Rightarrow a \prec \sigma(c) = a \surd (Reflexivitaet)$

    Falls $\sigma(c) \gtrsim a$: Peano-System $\Rightarrow a \leq c \overbrace{\Rightarrow}^{c \in M} a < c$. Aus dem und $c < \sigma(c)$ folgt wegen Transitivität von $\prec$: $a \prec \sigma(c)$.

[2] Weil totale Ordnung

2.4 Die natürlichen Zahlen - Monotonie der arithmetischen Operationen

Einführung

Dies wird ein sehr kurzer Abschnitt und ist in der Vorlesung nur sehr kurz gefasst. Vieles hier ist recht leicht zu beweisen.
$x < y$ wird für "$x \leq y \wedge x \neq y$" geschrieben.
Ab jetzt nehmen wir $\mathbb{N}$ als das "echte" Peano-System.

Satz 4.1: Erweiterbarkeit

(a) $x < y \Rightarrow x + z < y + z$.

(b) $x < y \wedge z \neq 0 \Rightarrow x * z < y * z$

Beweis:

(a) $y = x + u, u \neq 0 \Rightarrow y + z = (x + u) + z = (x + z) + u \Rightarrow x + z < y + z$

(b) $y = x + u, u \neq 0 \Rightarrow y * z = (x + u) * z = x * z + u * z; \underbrace{u * z \neq 0}_{(!)}$

$u = v + 1,\ z = t + 1,\ z * z = (v * t + v + t) + 1 \neq 0$

Korollar 4.2:

(a) $x < y \wedge z \leq t \Rightarrow x + z < y + t$

(b) $x < y \wedge 0 < z \leq t \Rightarrow x * z < y * t$

Beweis:

(a) $x + z < y + z \leq y + t$

(b) $x * z < y * z \leq y * t$

2.5 Die natürlichen Zahlen - Zählen und Endlichkeit von Mengen

Einführung

Eine wichtige Eigenschaft von $\mathbb{N}$ ist die Zählbarkeit. Der Ursprung der natürlichen Zahlen wird dort vermutet. Nach diesem Kapitel gehen wir weiter zu den ganzen Zahlen und streifen die weiteren Zahlenbereiche, bis wir endlich zu den Gleichungen und Ungleichungen kommen.

Definition 5.1: Endlichkeit

Da wir in der Vorlesung Probleme mit dieser unintuitiven Definition hatten, schreibe ich hier folgend mehrere hinein. Die "offizielle" ist die erste.

- Eine Menge M ist endlich, wenn es keine bijektive Abbildung $F : M \mapsto N$ gibt, N irgendeine Teilmenge von M.
- Eine Menge M ist endlich, wenn es zu keiner echten Teilmenge N eine bijektive Abbildung $F : M \mapsto N$ gibt.
- Eine Menge M ist unendlich, wenn $\exists N \subsetneq M$, $\exists$bijektive Abbildung $f : M \mapsto N$.

Beispiele:

- $\mathbb{R} \mapsto \mathbb{R}^*$ geht.
- $\mathbb{N} \mapsto \mathbb{N}\backslash\{0\}$ geht: $f : n \mapsto n + 1$

Definition 5.2: Menge hat n Elemente

Sei $n \in \mathbb{N}$, M Menge. M hat n Elemente, wenn es eine bijektive Abbildung $\{1, ..., n\} \mapsto M$ gibt.

Satz 5.3: M endlich $\Leftrightarrow$ M hat n Elemente

M ist endlich $\Leftrightarrow \exists n : n \in \mathbb{N} \wedge M$ hat n Elemente.

Beweis:

Hierfür brauchen wir mehrere Hilfssätze, wir werden zuerst die Richtung Rechts-nach-Links angehen und nachfolgend die um Längen schwerere Richtung Links-nach-Rechts beweisen.[3]

"$\Leftarrow$" Bijektive Abbildung $f : \{1, ..., n\} \mapsto M$ Lemma 5.6: $\{1, ..., n\}$ endlich. Aus Lemma 5.7 folgt: M endlich.

"$\Rightarrow$" Falls für alle $n \in \mathbb{N}$ M nicht n Elemente hat: Das ist die Vorraussetzung von Lemma 5.8, also existiert $f : \mathbb{N} \mapsto M$ injektiv. Mit Lemma 5.9 ist somit M unendlich.

Lemma 5.4: $\emptyset$ ist endlich

$\emptyset$ ist endlich und hat 0 Elemente.

Beweis:

$\{k|1 \leq k \leq 0\} = \emptyset \Rightarrow id : \{1, ..., 0\} \mapsto \emptyset$ ist bijektiv. Also hat $\emptyset$ 0 Elemente.
$\emptyset$ hat keine echte Teilmenge, daher gibt es keine bijektive Abbildung $\emptyset$ und einer echten Teilmenge.
Damit ist $\emptyset$ endlich.

[3] Anmerkung: Den Beweis werde ich bereits hier geben, obwohl er in der Vorlesung (und logisch) nach den folgenden Lemmas stand.

Lemma 5.5: M endlich $\Rightarrow M \cup \{x\}$ endlich

Sei M endlich, dann ist auch $M \cup \{x\}$ endlich.

Beweis:
Falls $x \in M$: $M = M \cup \{x\}$, also endlich.
Falls $x \notin M$, also $M \subsetneq M \cup \{x\}$.
Annahme: $\exists N : N \subsetneq M \cup \{x\}$, $\exists f : M \cup \{x\} \mapsto N$ bijektiv.
Sei $y = f(x)$.

- Falls $y = x$: $f' : M \mapsto N\backslash\{x\} : z \mapsto f(z)$ $\overbrace{\text{ist Abbildung.}}^{\text{Bijektivität}}$
  f' ist bijektiv. $N\backslash\{x\} \subsetneq M$. Sei $t \in M \cup \{x\}\backslash N$
  Wegen $x = y \in N$: $t \neq x$, d.h. $t \in M, t \notin N\backslash\{x\}$ $\lightning$(M endlich)
- Falls $y \neq x$: SEE[4]
  - Falls $x \notin N$: $f' : M \mapsto N\backslash\{y\}$ bijektiv auf echte Teilmenge. $\lightning$
  - Falls $x \in N$: $\sigma : N \mapsto N$: $t \mapsto \begin{cases} t & t \notin \{x, y\} \\ x & t = y \\ y & t = x \end{cases}$ bijektive Abbildung. (Vertausch x und y). Somit ist
    $\sigma \circ f : M \cup \{x\} \mapsto N$ bijektiv. $(\sigma \circ f)(x) = \sigma(y) = x$. Siehe Fall oben: $\lightning$

Lemma 5.6: $\{1, ..., n\}$ endlich

Für $n \in \mathbb{N}$ ist $\{1, ..., n\}$ endlich.

Beweis: Induktion
Sei $S = \{n \in mN | \{1, ..., n\}$ endlich $\}$

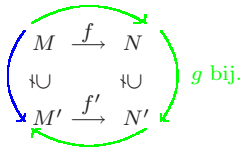
- $0 \in S$: Lemma 5.4
- $n \in S \Rightarrow n + 1 \in S$ $\{1, ..., n\}$ ist endlich ($n \in S$).
  Aus Lemma 5.5 folgt $\{1, ..., n, n + 1\} = \{1, ..., n\} \cup \{n + 1\}$ ist endlich.

Lemma 5.7: Bijektion zwischen endlichen Mengen

Seien M, N Mengen, es gebe eine bijektive Abbildung $f : M \mapsto N$. Falls M endlich ist, dann ist auch N endlich.

Beweis:
Annahme: N ist nicht endlich. Dann gibt es eine echte Teilmenge $N' \subsetneq N$ und eine bijektive Abbildung $g : N \mapsto N'$. Da f bijektiv[5]gibt es ein $M' = f^{-1}[N'] \subsetneq M$

$f'^{-1} \circ g \circ f$ ist bij. $\lightning$



g bij.

Nun können wir bereits die eine Richtung beweisen.

[4]Vielleicht komplizierter als es müsste.
[5]Hier reicht die Injektivität

Lemma 5.8:

Sei M eine nichtleere Menge, die nicht bijektiv auf irgendein Anfangsstück $\{1, ..., n\}$ von $\mathbb{N}$ abgebildet werden kann.
Dann gibt es eine injektive Abbildung von den natürlichen Zahlen in die Menge M.

Beweis:

Wenn es eine injektive Abbildung $f : \mathbb{N}_1 \to M$ von den natürlichen Zahlen ohne Null in diese Menge M gibt, dann gibt es auch eine injektive Abbildung $g : \mathbb{N} \to M$.
Idee: $g := f \circ \nu$ (g injektiv als Komposition injektiver Abbildungen)
Da M nichtleer ist, wähle ein $c \in M$.
Setze $N = M \backslash \{c\}$.
Behauptung: $N \neq \emptyset$
Falls $N = \emptyset : M = \{c\}$
Dann wäre aber die Abbildung $k : \{1\} \to M : 1 \mapsto c$ bijektiv.
Aus diesem Widerspruch zur definitorischen Eigenschaft von M folgt dass $M \backslash \{c\} = N$ nicht leer ist.
Man kann deshalb eine Abbildung g folgendermaßen angeben:
$g : \wp(N) \backslash \{\emptyset\} \to N$ mit $g(x) \in x$
und

$$\overline{g} : \wp(N) \to M : x \mapsto \begin{cases} g(x) & \text{falls } x \neq \emptyset \\ c & \text{falls } x = \emptyset \end{cases}$$

Verwende Satz I.1.4 mit
$S = \wp(M), c = \emptyset$
$G : \mathbb{N} \times \wp(M) \to \wp(M) : (k, X) \to X \cup \{\overline{g}(N \backslash X)\}$
$\Rightarrow \exists! F : \mathbb{N} \to \wp(M)$ mit:

- $F(0) = c = \emptyset$
- $F(n+1) = G(n, F(n)) = F(n) \cup \{\overline{g}(N \backslash F(n))\}$

Erläuterung:
$F(0) = \emptyset$
$F(1) = \{\overline{g}(N)\} \subseteq N$
$F(2) = F(1) \cup \{\overline{g}(N \backslash F(1))\} \subseteq N$
$F(3) = F(2) \cup \{\overline{g}(N \backslash F(2))\} \subseteq N$
Definiere $g : \mathbb{N}_1 \to M : k \to \overline{g}(N \backslash F(k-1))$
f ist Komposition von:
$\mathbb{N}_1 \to \wp(M) : k \to F(k)$
$\wp(M) \to \wp(N) : X \to N \backslash X$
$\overline{g} : \wp(N) \to M$
(D.h. f ist eine Abbildung)
Trivial ist:
$F(0) \subseteq F(1) \subseteq F(2) \subseteq ...$
Behauptung:
$f(\{1, ..., k\}) = F(k)$

Beweis:

Sei $S = \{k \in \mathbb{N} | f(\{1, ..., k\}) = F(k)\}$
Behauptung: $S = N$

- $0 \in S$: $\{1, ..., 0\} = \emptyset$
  $f(\emptyset) = \emptyset = F(0)$
- $k \in S \to k + 1 \in S$
  $F(k+1) = \underbrace{F(k)}_{= f\left(\{1, ..., k\}\right)} \cup \underbrace{\{\overline{g}(N \backslash F(k))\}}_{= f(k+1)} = f(\{1, ..., k, k+1\})$ Annahme:
  $\exists k \in \mathbb{N} : F(k)$ nicht echt in N, d.h. $F(k) = N$ oder $c \in F(k)$.
  Sei K die kleinste natürliche Zahl mit dieser Eigenschaft.
  Dann ist $1 \leq K : F(0) = \emptyset \subset N$
  Behauptung: $F(k) = N$
  Falls $F(K) \neq N : c \in F(k) = f(\{1, ..., K\})$
  $\Rightarrow \exists l \in \{1, ..., K\} : c = f(l)$
  $f(l) = \overline{g}(N \backslash F(l-1)) = \begin{cases} c & \text{, falls } N \backslash F(l-1) = \emptyset \\ N \backslash F(l-1) & \text{, falls } N \backslash F(l-1) \neq \emptyset \end{cases}$
  Wegen $f(l) = c : N \backslash F(l-1) = \emptyset$

Also $F(l-1)$ ist nicht echt in N.
$l-1 < l \leq K$ $\lightning$zur Minimalität von K

Behauptung: Falls $f(k-1) \subset N$ ist, gilt: $f\big|_{\{1,...,k\}}$ injektiv.

Beweis:

Falls nicht injektiv: $\exists r, s : 1 \leq r < s \leq K$ und $f(r) = f(s)$
$f(s) = \overline{g}(\ N \backslash \underbrace{F(s-1)}_{f(r) \in f(\{1,...,s-1\})})$
$s \leq k \Rightarrow s-1 \leq k-1$
$\Rightarrow F(s-1) \subseteq F(k-1) \subset N$
$\Rightarrow N \backslash F(s-1) \neq \emptyset$
$\underbrace{f(s)}_{f(r)} \in N \backslash \underbrace{F(s-1)}_{\in F(r)}$ $\lightning$

Insbesondere:
$F(K-1) \subset N$ (Minimalität von K)
$\Rightarrow f\big|_{\{1,...,k\}}$ injektiv
$\Rightarrow f\big|_{\{1,...,k\}} : \{1,...,k\} \underbrace{\rightarrow}_{\text{bijektiv}} N = F(k)$
$\Rightarrow \overline{f} : \{1,...,K+1\} \rightarrow M : k \mapsto \begin{cases} c & k = K+1 \\ f(k) & k \leq K \end{cases}$
Bijektiv $\lightning$zur Voraussetzung des Lemmas.
Also: $\forall k \in \mathbb{N} : F(k) \subset N$
$\Rightarrow \forall k \in \mathbb{N} : f|\{1,...,k\}$ ist injektiv.
q.e.d.

Lemma 5.9: Unendlichkeit

Wenn es eine injektive Abbildung $f : \mathbb{N} \mapsto M$ gibt, dann ist M unendlich.

Beweis:

Sei $N = M \backslash Bild(f) = M \backslash f[N]$.
$M' = f[\mathbb{N}_1] \cup N \subsetneq M$ (echt: $f(0) \in M \backslash M'$)
$g : M \mapsto M' : x \mapsto \begin{cases} x & x \in \mathbb{N} \\ f(k+1) & x = f(k) \end{cases}$
g ist bijektive Abbildung (ohne Beweis).

2.6 Die ganzen Zahlen

Man definiere sich eine Rechenaufgabe, die nicht (vollständig) lösbar ist. Nun erweitere man den Zahlbereich, so dass diese Rechenaufgabe wiederum lösbar ist. z.B. Reel $\rightsquigarrow$ Komplex usw.

Einführung

Seien $x, y \in \mathbb{N}$. Suche Zahl z mit: $y = x + z$ In $\mathbb{N}$ existiert eine Lösung genau dann, wenn $x \leq y$. Dann gibt es auch genau eine Lösung:

Beweis: Eindeutig
Sei $y = x + z = x + z'$, $z, z' \in \mathbb{N}$. Falls $z \neq z' \Rightarrow \exists u \in \mathbb{N}, u \neq 0 : z' = z + u$ oder $\exists v \in \mathbb{N}, v \neq 0 : z = z' + v$.
$\Rightarrow y = x + z' = (x + z) + u \wedge y = x + z \Rightarrow u = 0$ ↯
$\Rightarrow y = x + z = (x + z') + v \wedge y = x + z' \Rightarrow v = 0$ ↯
Also $z = z'$.

Rechenoperation, die nur teilweise definiert ist:
$\{(x, y) \in \mathbb{N} \times \mathbb{N} | x \leq y\} \mapsto \mathbb{N}$,
$(x, y) \mapsto z$ mit $y = x + z$
Erweitere[6] den Zahlbereich $\mathbb{N}$ so, daß diese Rechenoperation überall definiert ist!
$z \in \mathbb{Z}$; $k, l \in \mathbb{N}$; $z = k - l = (k + 1) - (l + 1)$ ist nicht eindeutig, daher führen wir eine Äquivalenzrelation ein. Die Äquivalenzklassen sind dann die eindeutig bestimmten Elemente. Nachfolgend ist ein Tupel immer $(k, l) \in \mathbb{N} \times \mathbb{N}$.

Satz 6.1: Äquivalenzrelation der ganzen Zahlen

Die Relation $(k, l) \sim (r, s) \Leftrightarrow k + s = r + l$ ist eine Äquivalenzrealtion auf $\mathbb{N} \times \mathbb{N}$.
Man kommt auf diese Definition durch folgende Überlegung:
$z = k - l = r - s \Leftrightarrow z + l + s = k + s = r + l$
Beweis:

- **Reflexivität** $(k, l) \sim (k, l)$: $k + l = k + l$ $\surd$
- **Symmetrie** Sei $(k, l) \sim (r, s) \Rightarrow k + s = r + l \Rightarrow r + l = k + s \Rightarrow (r, s) \sim (k, l)$. $\surd$
- **Transitivität** Seien $(k, l) \underset{\Rightarrow k+s=r+l}{\sim} (r, s)$, $(r, s) \underset{\Rightarrow r+v=u+s}{\sim} (u, v)$.
  $\Rightarrow (r + s) + (r + v) = (r + l) + (u + s)$
  $\Rightarrow (k + v) + (r + s) = (u + l) + (r + s)$
  $\Rightarrow (k + v) = (u + l)$ Kürzungsregel
  $\Rightarrow (k, l) \sim (u, v)$ $\surd$

Definition 6.2: Ganze Zahlen

Die Äquivalenzklassen von $\sim_{6.1}$ sind die "Ganze Zahlen". Die Menge der ganze Zahlen heisst $\mathbb{Z}$.
Die Äquivalenzklasse von $(k, l) \in \mathbb{N} \times \mathbb{N} : k - l$
$\Pi : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{Z}$: $(k, l) \mapsto \Pi(k, l) = k - l$
Anmerkung: In diesem Kapitel nutzen wir die Π-Schreibweise, weil k-l wieder verwirren wuerde, was wir bereits duerfen und was wir noch zu beweisen zu haben.

Satz 6.3: Erweiterung von $\mathbb{N}$

- $\mathbb{N} \mapsto \mathbb{Z}$:$n \mapsto \Pi(n, 0) = n - 0$ ist eine injektive Abbildung.
- Jede ganze Zahl hat einen Repräsentanten $(n, 0)$ oder $(0, n)$ mit $n \in \mathbb{N}$.

[6] Altes bleibt so bestehen wie bisher.

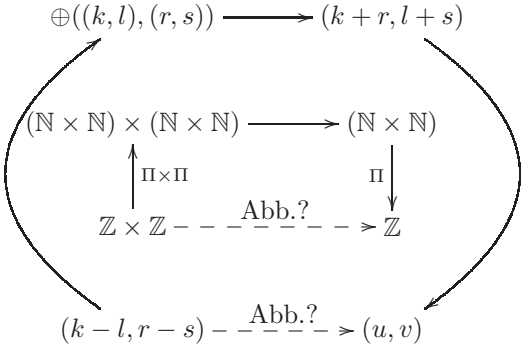
Beweis:

- (Injektiv): Seien $n, m \in \mathbb{N}$ mit $\Pi(n,0) = \Pi(m,0) \Rightarrow (m,0) \sim (n,0)$ d.h. $m = m+0 = n+0 = n$.
- (Repräsentanten): Sei $k - l \in mZ$. $k, l \in \mathbb{N}$. Wegen Trichitonie (Satz 3.2)
  (a) Fall $k < l$: $\exists u \in \mathbb{N} : l = k + u$, d.h. $k + u = 0 + l \Rightarrow (k,l) \sim (0,u)$
  (b) Fall $k = l$: $k + 0 = k = l = 0 + l \Rightarrow (k,l) \sim (0,0)$
  (c) Fall $l < k$: $\exists v \in \mathbb{N} : k = l + v$, d.h. $k + 0 = v + l \Rightarrow (k,l) \sim (v,0)$

Definition: $k - l \in \mathbb{Z}$ ist negativ, wenn $(k,l) \sim (0,n)$ mit $n \in \mathbb{N}, n \neq 0$, d.h. wenn $k < l$.
$\Rightarrow k - l = 0 - n$
Nachfolgend werden wir Rechenoperationen auf $\mathbb{N} \times \mathbb{N}$ und die Anordnung definiere, überprüfen ob diese für $\mathbb{Z}$ passen und auch prüfen, ob sie eingeschränkt auf natürliche Zahlen so funktionieren, wie die dortigen Rechenoperationen (Einbettung!).

Definitionen:

$\oplus$: $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \mapsto (\mathbb{N} \times \mathbb{N})$: $((k,l),(r,s)) \mapsto (k+r, l+s)$
$\otimes$: $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \mapsto (\mathbb{N} \times \mathbb{N})$: $((k,l),(r,s)) \mapsto (k*r + l*s, k*s + l*r)$
Wir wollen ereichen: $(k-l)+(r-s) = (k+r)-(l+s)$, $(k-l)*(r-s) = (k*r+l*s)-(k*s+l*r)$ wegen der Distributivität.



Satz 6.4: Rechtseindeutigkeit

Seien $(k,l) \sim (k',l'), (r,s) \sim (r',s')$
$\Rightarrow (k+r) - (l+s) = (k'+r') - (l'+s')$
$\wedge (kr+ls) - (ks+lr) = (k'r'+l's') - (k's'+l'r')$

Beweis:

- (Addition): $(k,l) \sim (k',l') \Rightarrow k + l' = k' + l$, $(r,s) \sim (r',s') \Rightarrow r + s' = r' + s$

$$\begin{aligned} \Rightarrow (k+l') + (r+s') &= (k'+l) + (r'+s) \\ \Rightarrow (k+r) + (l'+s') &= (k'+r') + (l+s) \\ \Rightarrow ((k+r),(l+s)) &\sim ((k'+r'),(l'+s')) \end{aligned}$$

- (Multiplikation) in zwei Schritten:
  (a) (k,l) wird festgehalten.

$$\begin{aligned} (k*r+l*s, k*s+l*r) &\sim (k*r'+l*s', k*s'+l*r') \\ \Leftrightarrow (k*r+l*s) - (k*s+l*r) &\stackrel{?}{=} (k*r'+l*s') - (k*s'+l*r') \\ \Leftrightarrow (k*r+l*s) + (k*s'+l*r') &= (k*r'+l*s') + (k*s+l*r) \\ \Rightarrow k*(r+s') + l*(s+r') &= k*(r'+s) + l*(s'+r) \\ \Rightarrow r + s' &= s + r' \end{aligned}$$

(b) (r, s) wird festgehalten (analog).

Einige Wiederholungen:
Gegeben: $k, l \in \mathbb{N}$. Suche Zahl $z : l = k + z$.
In $\mathbb{N} \times \mathbb{N}$ haben wir die Äquivalenzrelation $(k, l) \sim (r, s) \Leftrightarrow k + s = l + r$
$\mathbb{Z}$ ist Menge der Äquivalenzklassen, Klasse von $(k, l) : \Pi(k, l) = k - l$
$\mathbb{N}$ ist Eingebettet in $\mathbb{Z}$: $\mathbb{N} \mapsto \mathbb{N} \times \mathbb{N} : k \mapsto (k, 0) \Rightarrow \Pi(k, =) = k - 0$
Definiert sind vertraegliche
"+": $\Pi(k, l) + \Pi(r, s) = \Pi(k + r, l + s)$
"∗": $\Pi(k, l) * \Pi(r, s) = \Pi(k * r + l * s, k * s + l * r)$

Satz 6.5: $(\mathbb{Z}, 0, 1, +, -, *)$ kommutativer Ring

$\mathbb{Z}$ mit $+, *$ ist kommutativer Ring mit 1.

Beweis:

- **+ ist Kommutativ** $\Pi(k, l) + \Pi(r, s) = \Pi(k + r, l + s) = \Pi(r + k, s + l) = \Pi(r, s) + \Pi(k, l)$
- **+ ist Assoziativ** s.o.
- **0-Element** $\Pi(0, 0)$[7] $\Pi(0, 0) + \Pi(k, l) = \Pi(0 + k, 0 + l) = \Pi(k, l)$
- **Inverses Element von** $\Pi(k, l)$ **bzgl.** + $\Pi(k, l) + \Pi(l, k) = \Pi(\underset{(1)}{k + l}, \underset{(2)}{l + k}) = \Pi(\underset{(3)}{0}, \underset{(4)}{0})$
  $\overset{(1)}{(k + l)} + \overset{(4)}{0} = \overset{(2)}{(l + k)} + \overset{(3)}{0}$
- **∗ Kommutativ** $\Pi(k, l) * \Pi(r, s) = \Pi(k * r + l * s, k * s + l * r) = \Pi(r * k + s * l, r * l + s * k) = \Pi(r, s) * \Pi(k, l)$
- **∗ ist Assoziativ**
- **∗ ist Distributiv (über +)**
- **Eins-Element ist** $\Pi(1, 0)$ $\Pi(1, 0) * \Pi(k, l) = \Pi(1 * k + 0 * l, 1 * l + 0 * k) = \Pi(k, l)$

$\mathbb{N}$ ist Einbettung in $\mathbb{Z}$

Beweis:
$m, n \in \mathbb{N}$: $m + n$, $m * n \in \mathbb{N}$
$\Pi(m, 0), \Pi(n, 0) \in \mathbb{Z}$
$m \oplus n \cong \Pi(m, 0) + \Pi(n, 0) = \Pi(m + n, 0) \cong m + n$
$m \otimes n \cong \Pi(m, 0) * \Pi(n, 0) = \Pi(m * n + 0 * 0, m * 0 + n * 0) = \Pi(m * n, 0) \cong m + n$
$\Pi(k, l) \in \mathbb{Z} \Rightarrow \exists m \in \mathbb{N} : \Pi(k, l) = \Pi(m, 0)$ ODER $\exists m \in \mathbb{N} : \Pi(k, l) = \Pi(0, m)$ (Eindeutige Äquivalenzklassen-Darstellung)
$\Pi(\overset{>0}{m}, 0) * \Pi(\overset{<0}{0}, n) = \Pi(0, \overset{<0}{m * n})$
$\Pi(\overset{<0}{0}, m) * \Pi(\overset{<0}{0}, n) = \Pi(\overset{>0}{m * n}, 0)$

In $\mathbb{Z}$ wird die folgende Aufgabe gelöst: Zu $x, y \in \mathbb{Z}$ gibt es $z \in \mathbb{Z}$ mit $y = x + z$.
(Anm Heiko: Verstehe ich jetzt zwar nicht mehr, aber mitgeschrieben:)
$\Rightarrow$ Gilt auch für $\mathbb{N}$.
$\Rightarrow$ Bezüglich +-Gruppe, daher immer lösbar.
$x = \Pi(k, l)$, $y = \Pi(r, s)$ Dann ist $z = (r + l, k + s)$.
$x + z = \Pi(k + (r + l), l + (k + s)) = \Pi(r + (k + l), s + (k + l)) = \Pi(r, s) = y$
Als nächstes kommt die Kürzungsregel die daraus folgt, dass $\mathbb{Z}$ ein Integritätsbereich ist.

Satz 6.6: $\mathbb{Z}$ ist ein Integritätsbereich

$\mathbb{Z}$ ist ein Integritätsbereich, d.h. $a * b = 0 \Rightarrow a = 0 \vee b = 0$

Beweis:
$a = \Pi(m, 0)$ oder $a = \Pi(0, m)$

[7] Wichtig wirklich anzugeben, nicht nur Existenz zu beweisen.

$b = \Pi(n,0)$ oder $b = \Pi(0,n)$
$a * b = 0$

- $\Pi(m,0) * \Pi(n,0) = \Pi(m*n,0) = \Pi(0,0) \Rightarrow m*n = 0 \Rightarrow m = 0$ oder $n = 0$.
- $\Pi(m,0) * \Pi(0,n) = \Pi(0,m*n) = \Pi(0,0) \Rightarrow m*n = 0 \Rightarrow m = 0$ oder $n = 0$.
- (...)
- (...)

Als nächstes besprechen wir die Anordnung der ganzen Zahlen. Achtung: "$\prec$" ist wieder unabhängig von dem fehlenden Strich zu lesen, genau genommen ist es ein "kleinergleich".
Relation $\prec$ auf $\mathbb{N} \times \mathbb{N}$: $(k,l) \prec (r,s) :\Leftrightarrow k + s \leq r + l$ (in $\mathbb{N}$) $\Leftrightarrow (k - l \leq r - s)$

Satz 6.7: Wohlefiniert

$(k,l) \sim (k',l')$ und $(r,s) \sim (r',s')$ Dann $(k,l) \prec (r,s) \Leftrightarrow (k',l') \prec (r',s')$

Beweis:
oBdA genügt eine Richtung zu Zeigen.
$k + s \leq r + l \Rightarrow \underbrace{k + s + l'}_{=k'+l+s} \leq r + l + l' \overset{2.7}{\Rightarrow} k' + s \leq r + l' \Rightarrow (k',l') \prec (r,s) \underset{\text{analog}}{\Rightarrow} (k',l') \prec (r',s')$
$\Rightarrow$ Größenordnungen bestehen auf Äquivalenzklassen.

Definition 6.8: $\leq$ auf $\mathbb{Z}$

Hier gibt es zwei Möglichkeiten, die "offizielle" zuerst, die zweite stammt aus dem Publikum.

- $\Pi(k,l) \leq \Pi(r,s)$ falls $(k,l) \prec (r,s)$ ist eine Relation auf $\mathbb{Z}$.
- $\Pi(k,l) \leq \Pi(r,s)$, falls es ein $n \in \mathbb{N}$ gibt mit $\Pi(r,s) = \Pi(k,l) + \Pi(n,0)$.

Satz 6.9: $\leq$ ist totale Ordnung auf $\mathbb{Z}$

Für $m,n \in \mathbb{N}$ $m \leq n \Leftrightarrow \Pi(m,0) \leq \Pi(n,0) \Leftrightarrow \Pi(0,n) \leq \Pi(0,m)$
Für alle $m,n \in \mathbb{N} : \Pi(0,n) \leq \Pi(m,0)$

Beweis: nicht vollständig

- **Reflexiv**
- **Antisymmetrisch** $\Pi(k,l) \leq \Pi(r,s) \wedge \Pi(r,s) \leq \Pi(k,l)$
  $\left.\begin{array}{l} k+s \leq r+l \\ r+l \leq k+s \end{array}\right\} \Rightarrow k+s = r+l \Rightarrow \Pi(k,l) = \Pi(r,s)$
- **Transivität**
- **Totalität**
- $\Pi(0,n) \leq \Pi(m,0)$ $0 = 0 + 0 \leq m + n \in \mathbb{N}$

Satz 6.10: Monotonie

(ohne Beweis, es gibt noch weitere Varianten)
Sei $\Pi(k,l) \leq \Pi(r,s)$.

(a) $\forall \Pi(u,v) \in \mathbb{Z} : \Pi(k,l) + \Pi(u,v) \leq \Pi(r,s) + \Pi(u,v)$

(b) $\forall \Pi(u,v) \in \mathbb{Z} : \begin{cases} 0 \leq \Pi(u,v) \Rightarrow \Pi(k,l) * \Pi(u,v) \leq \Pi(r,s) * \Pi(u,v) \\ \Pi(u,v) \leq 0 \Rightarrow \Pi(r,s) * \Pi(u,v) \leq \Pi(k,l) * \Pi(u,v) \end{cases}$

Ab sofort sind die Notationen wie die üblichen zu ganzen Zahlen, z.B. $a < b :\Leftrightarrow a \leq b \wedge a \neq b$.

Einschub: Definition "Einheit"
R Ring mit 1
$u \in R$ ist eine Einheit, wenn es ein $v \in R$ gibt mit $u * v = 1 = v * u$. (ex multiplikatives Inverses)
Menge der Einheiten: $R^\times$
Anmerkung: Im Körper ist alles ausser 0 eine Einheit.

Weiterer Einschub: $0 < 1$ $\Pi(0,0) < \Pi(0,1) \Leftrightarrow 0 + 0 < 0 + 1$
Alternativ: Alle Quadrate sind grösser/gleich 0: $1 * 1 = 1$ ist Quadrat.

Satz 6.11: Einheiten in $\mathbb{Z}$

$\mathbb{Z}^\times = \{+1, -1\}$

Beweis:
Existenz: $1 * 1 = 1$, $(-1) * (-1) = 1 * 1 = 1 \Rightarrow 1, -1 \in \mathbb{Z}^\times$
Sei $u * v = 1; u, v \in \mathbb{Z} \Rightarrow u \neq 0, v \neq 0$
Falls $u < 0, v > 0$: $u * v < 0 \Rightarrow 1 < 0$ ↯
Analog $u > 0, v < 0$ ↯
Falls $u > 0, u > 0$: $\Rightarrow u = x + 1, v = y + 1 \quad x, y \in \mathbb{N}$
$\Rightarrow 1 = u * v = x * y + x + y + 1$
$\overset{2.7}{\Rightarrow} 0 = x * y + x + y \Rightarrow x = 0 \wedge y = 0$
$\Rightarrow u = 0 + 1 = 1 = v$
Analog $0 > u, 0 > v$: $1 = u * v = (-u) * (-v) = (-1) * (-1)$
$\Rightarrow u = -1, v = -1$

Nun kommen zwei charakterisierungen der ganzen Zahlen

(a) Aussenbeziehungen zu anderen Ringen (mit 1)

(b) Innere Eigenschaften

Hier fehlt eine Nummer in der Zählung.

Satz 6.13: Eindeutiger Homom. ($f : \mathbb{Z} \mapsto R$)

Sei R ein kommutativer Ring mit 1. Dann gibt es genau einen Homomorphismus von Ringen mit $1\ (1 \mapsto 1)$ $f : \mathbb{Z} \mapsto R$.

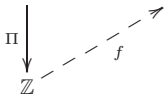
Beweis:
Existenz: Definiere rekursiv (Satz 1.4)
In/Aus 1.4: $S = R$, $0 \in S = R$ $G : (\underset{\mathbb{N} \times R}{\mathbb{N} \times S}) \mapsto \underset{R}{S} : (k, x) \mapsto x + 1$
$\Rightarrow \exists! F : F(0) = 0, F(n+1) = G(n, F(n)) = F(n) + 1$
$F : \mathbb{N} \mapsto R$ ist Homomorphismus bezüglich $+$.

Beweis: $M = \{l \in \mathbb{N} | F(k + l) = F(k) + F(l)\}$

- $0 \in M$ $F(k + 0) = F(k) = F(k) + 0 = F(k) + F(0)$
- $l \in M \Rightarrow l + 1 \in M$
  $F(k + (l + 1)) = F((k + l) + 1) = G(k + l, F(k + l)) = F(k + l) + 1 = F(k) + F(l) + 1 = F(k) + F(l + 1)$

Analog: $F : \mathbb{N} \mapsto R$ ist Homomorphismus bezüglich $*$.

Definiere: $\Phi : \mathbb{N} \times \mathbb{N} \longrightarrow R : (k, l) \longrightarrow F(k) - F(l)$



$z \in \mathbb{Z}, z = k - l$ $f(z) = f(k - l) = F(k) - F(l)$ eindeutig!

Behauptung $(k, l) \sim (k', l') \Rightarrow F(k) - F(l) = F(k') - F(l')$
Beweis $(k, l) \sim (k', l') \Rightarrow k + l' = k' + l \Rightarrow F(k) + F(l') = F(k + l') = F(k' + l) = F(k') + F(l)$

f Homomorphismus

- **(+)** $z = k - l,\ t = r - s$

$$\begin{aligned} f(z+t) &= f(\Pi(k,l) + \Pi(r,s)) \\ &= f(\Pi(k+r, l+s)) \\ &= \Phi(h+r, l+s) = F(k+r) - F(l+s) \\ &= (F(k) - F(l)) + (F(r) - F(s)) \\ &= \Phi(k,l) + \Phi(r,s) \\ &= f(\Pi(k,l)) + f(\Pi(r,s)) \\ &= f(z) + f(t) \end{aligned}$$

- für 0 usw
- **(1)** $f(1) = f(\Pi(1,0)) = \Phi(1,0) = F(1) - F(0) = F(1) = F(0+1) = F(0) + 1 = 1$

Eindeutigkeit von f
Sei $f' : \mathbb{Z} \mapsto R$ ein weiterer Homomorphismus. Behauptung: $f = f'$.
Beweis: $M = \{n \in \mathbb{N} | f(n) = f'(n)\}$

- $0 \in M$ $f(0) = 0 = f'(0)$ Ringhomomorphismus.
- $n \in M \Rightarrow n+1 \in M$ $f(n+1) = f(n) + f(1) = f(n) + 1 = f'(n) + 1 = f'(n) + f'(1) = f'(n+1)$

Damit für $n \in \mathbb{N}$ gleich.

Für ganze Zahlen: Sei $z \in \mathbb{Z}$

- $z \in \mathbb{N}$ $f(z) = f'(z)$
- $z \notin \mathbb{N}$ $-z \in \mathbb{N}$, $-f(z) = f(-z) = f'(-z) = -f'(z)$

$\Rightarrow f(z) = f'(z)$

Satz 6.14: 1. Charakterisierung $\mathbb{Z}$

Sei A ein kommutativer Ring mit 1 mit folgenden Eigenschaft:
(*) Wenn R ein kommutativer Ring mit 1 ist, gibt es genau einen Homomorphismus $g : A \mapsto R$ von Ringen mit 1.
Dann ist $A \underset{\cong}{\text{isomorph}} \mathbb{Z}$.

Beweis:
Wende (*) auf $R = \mathbb{Z}$ an: $g : A \mapsto \mathbb{Z}$.
Wende 6.13 auf $R = A$ an: $f : \mathbb{Z} \mapsto A$.
Dann gilt Isomorphie durch die Eindeutigkeit und $g \circ f : \mathbb{Z} \mapsto \mathbb{Z} = id_{\mathbb{Z}}$,
$f \circ g : A \mapsto A = id_A$.

Das letzte Mal wurde die erste Charakterisierung von $\mathbb{Z}$ besprochen: R kommutativer Ring mit $1 \Rightarrow \exists! f : \mathbb{Z} \mapsto R$ Homomorphismus mit $f(1) = 1$.

Satz 6.15: 2. Charakterisierung $\mathbb{Z}$

R sei total geordneter Integritätsbereich, Positivbereich $R^{\geq} = \{a \in R | 0 \leq a\}$ sei wohlgeordnet.
$\Rightarrow R \cong \mathbb{Z}$

Beweis:
Vorher ein paar Bemerkungen. Die erste haben wir zwar schon mal bewiesen, aber wir wollen sicherzustellen, daß diese im richtigen Kontext bewiesen ist.
Behauptung: $R : 1 > 0$

Beweis:
Annahme: $1 < 0 \Rightarrow -1 > 0 \Rightarrow -1 = -1 * 1 < 0 \Rightarrow -1 < 0$ ↯

Behauptung: 1 ist das kleinste Element von $R^{\geq} \backslash \{0\}$

Beweis:
Annahme: $\exists r \in R : 0 < r < 1$ Wegen der Wohlordnung von R soll r das kleinste Element von $R^{\geq} \backslash \{0\}$ mit dieser Eigenschaft sein. $\Rightarrow 0 < r^2 < r \Rightarrow r^2 < r$ ↯

Wir wissen bereits, dass es genau ein Homomorphismus $\mathbb{Z} \mapsto R$ existiert. ($\mathbb{Z}$ Integritätsbereich $\Rightarrow \mathbb{Z}$ Ring mit 1)
Sei $f : \mathbb{Z} \mapsto R$ der eindeutig bestimmte Homomorphismus mit $f(1) = 1$.
Zu Zeigen: f ist Isomorphismus Behauptung: $f[\mathbb{N}] = R^{\geq}$

Beweis: Induktion
$f[\mathbb{N}] \subseteq R^{\geq}$, $S = \{n \in \mathbb{N} | f(n) \in R^{\geq}\}$

- $0 \in S$: $f(0) = 0 \geq 0$
- $n \in S \Rightarrow n + q \in S$ $f(n+1) \underbrace{=}_{\text{Homom.}} f(n) + 1 \underbrace{>}_{1>0 in R} f(n) \underbrace{\geq}_{} n \in S0$

Beweis:
$R^{\geq} \subseteq f[\mathbb{N}]$
Annahme: $\exists r \in R^{\geq} : r \notin f[\mathbb{N}] \Rightarrow \{r \in R^{\geq} | r \notin f[\mathbb{N}]\} \neq \emptyset$ hat kleinstes Element r mit $r \neq 0$, $r \neq 1 \Rightarrow 1 < r$.
Setze $s = r - 1 > 0$. $s < r$. Wegen Minimalität von r folgt $\exists n \in \mathbb{N} : s = f(n) \Rightarrow f(n+1) = f(n) + 1 = s + 1 = r$ ↯

Behauptung: f injektiv

Beweis:
f injektiv genau dann, wenn nur $0 \overset{f}{\mapsto} 0$, also $|f^{-1}[\{0\}]| = 1$.
f nicht injektiv $\Rightarrow \exists z \in \mathbb{Z}, z \neq 0, f(z) = 0 \Rightarrow f(-z) = 0$
Also $\exists 0 < n \in \mathbb{N} : f(n) = 0$
Sei $n = k + 1$, $k \in \mathbb{N}$. Es folgt $0 = f(n) = f(k+1) = \overbrace{f(k)}^{\geq 0 in R} + 1 > f(k) \geq 0$ ↯$(0 > 0)$

Behauptung: f surjektiv

Beweis:
Sei $r \in R$.
Fall $r \geq 0$: $r \in f[\mathbb{N}]$.
Fall $r < 0$: $-r \in R^{\geq} \Rightarrow \exists n \in \mathbb{N} : -r = f(n) \Rightarrow r = f(-n)$

Die nachfolgende Eigenschaft der ganzen Zahlen ist wichtig für das Rechnen in $\mathbb{Z}$.

Satz 6.16: Division mit Rest in $\mathbb{Z}$

Seien $0 < n \in \mathbb{N}$, $z \in \mathbb{Z}$. Dann gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$, $r \in \mathbb{N}$ mit $z = q * n + r$.

Beweis: Induktion
$M = \{t \in \mathbb{Z} | t > z\}$
Damit wir die Induktion auch anwenden duerfen, muessen wir (positive) natürliche Zahlen (ab 0) haben.Dies erreichen wir durch Translation. Unsere Translation ist τ.
$\tau : z \mapsto \mathbb{Z} : x \mapsto x - (z+1)$, $\tau[M] = \mathbb{N}$
M ist wohlgeordnet!
$N = \{x \in M | \exists a \in \mathbb{Z} : x = a * n\} \neq \emptyset$ hat kleinstes Element. Falls $z \leq 0$: $n \in N$ Falls $z > 0$:
Setze $S = \{t \in \mathbb{N} | \exists a \in \mathbb{N} : a * n > t\}$

- $0 \in S$: $0 < n = 1 * n$
- $t \in S \Rightarrow t + 1 \in S$

  Sei $t < a * n$. Es folgt $t + 1 < a * n + 1 \overset{n \neq 0}{\leq} (a+1) * n$ (archimedische Eigenschaft)

Es folgt mit $M \supseteq N \neq \emptyset$: N hat kleinstes Element x.
$x = a * n \Rightarrow \overbrace{(a-1)}^{q} * n \overbrace{\leq}^{\text{Minim.}} z$ (Weil: $(a-1) * n > z \Rightarrow (a-1) * n \in M, (a-1) * n < x$ ↯)
$z = q * n + r, r = z - q * n$
Behauptung $0 \leq r < n$, $z \geq q * n \Rightarrow z - \overset{=r}{(q * n)} \geq 0$
Annahme $r \geq n$ $z - q * n \geq n \Rightarrow z \geq (q+1) * n = a * n = x \in \mathbb{N}$ Also $x > z$ ↯.

Eindeutigkeit
Sei $z = q * n + r = q' * n + r'$, $0 \leq r, r' < n$
Annahme $r < r'$ $\Rightarrow (q - q') * n = r' * r$, $0 < r' - r \leq r' < n \Rightarrow 0 < \underbrace{(q - q')}_{\neq 0} * n < n$ ↯

Analog: $r > r'$ ↯
$\Rightarrow r = r'$
$\Rightarrow (q - q') * n = 0 = r' - r \Rightarrow q - q' = 0 \Rightarrow q = q'$

Das war das letzte für $\mathbb{Z}$, als nächstes kommen die rationalen Zahlen. Wieder werden wir uns eine Aufgabe stellen, die wir nicht (vollständig) lösen können - ganz ähnlich wie bei der Einführung der ganzen Zahlen. Wir werden wieder den Zahlbereich vergrössern, damit die Aufgabe lösbar sein wird.

2.7 Die rationalen Zahlen

Einführung

Gegeben: $z, t \in \mathbb{Z}$.
Gesucht: Zahl u mit $z = t * u$ - siehe auch den Anfang von $\mathbb{Z}$.
Falls $t = 0$, $z \neq 0$ ist die Aufgabe **nie** lösbar!
Unsere Aufgabe: Vergrößerung des Zahlbereichs,
so daß es zu z, t mit $t \neq 0$ immer ein u gibt, mit $z = t * u$.
Bei der Vergrößerung von $\mathbb{N} \mapsto \mathbb{Z}$ konnten wir die Aufgabenstellung bereits partiell definieren, diesmal ist es nicht so einfach. Daher versuchen wir es gar nicht erst.
Sei $z = t * u = t * u'$. Behauptung: $u = u'$: $t * u = tu'$, $t \neq 0$, $t(u - u') = 0 \Rightarrow u - u' = 0 \Rightarrow u = u'$.
Seien z, t Zahlen. Suche Zahl "Quotienten" $u : z = t * u$, $t \neq 0$, die bestimmt ist durch z, t.
Dies ist nicht eindeutig: $\frac{2}{3} = 2 : 3 = 4 : 6 = ...$

Satz 7.1: Äquivalenzrelation von $\mathbb{Q}$

Auf der Menge $\mathbb{Z} \times \mathbb{N}_1$ ist folgende Äquivalenzrelation definiert: $(z, k) \sim (t, l)$, falls $z * l = t * k$.

Beweis:
(unvollständig) **Transitivität** Seien $(z, k) \sim (t, l)$, $(t, l) \sim (u, m)$ Dann gilt $z * l = t * k$, $t * m = u * l$
$\Rightarrow z * l * t * m = t * k * u * l \Rightarrow (z * m)(t * l) = (u * k) * (t * l)$ Durch Kürzen (Fall $t * l \neq 0$) erhält man $(z * m) = (u * k)$.
Fall $t * l = 0$: Es folgt aus $l \neq 0$: $t = 0$. Aus $t * m = u * l \Rightarrow u = 0 \wedge z = 0 \Rightarrow z * m = 0, u * k = 0$, daher wiederum Transitiv.

Definition 7.2: $\mathbb{Q}$

Menge der Äquivalenzklassen der vorhergehenden Äquivalenzrelation bilden $\mathbb{Q}$ - die rationalen Zahlen. Eine rationale Zahl ist eine Äquivalenzklasse.
$\Pi : \mathbb{Z} \times \mathbb{N}_1 \mapsto \mathbb{Q} : (z, k) \mapsto \frac{z}{k}$ Äquivalenzklasse von (z, k).
z: Zähler
k: Nenner
Die übliche Notation ist zwar eingeführt und wird verwendet, aber dennoch müssen wir sehr vorsichtig damit umgehen.

Satz 7.3: Ausgezeichnete Element (gekürzt)

Sei $q \in \mathbb{Q}$. Dann gibt es unter allen Elementen der Äquivalenzklasse genau eines mit kleinstem Nenner. Wenn (z, k) dieses Element ist, heisst es $q = \frac{z}{k}$ ist in gekürzter Darstellung.

Beweis:
Sei $N_q = \{k \in \mathbb{N}_1 | \exists z \in \mathbb{Z} : q = \frac{z}{k}\}$. $N_q \neq \emptyset$. Wegen Wohlordnung hat N_q ein kleinstes Element k.
Eindeutigkeit
Sei k das Minimum in N_q. Sei $q = \frac{z}{k} = \frac{z'}{k}$, d.h. $z * k = z' * k \Leftrightarrow z = z'$ (k positiv, $\mathbb{Z}$ Integritätsbereich, daher kürzbar)

Lemma 7.4: $\mathbb{Z}$ ist eingebettet in $\mathbb{Q}$

Durch $z \mapsto \frac{z}{1} = \Pi(z, 1)$ wird $\mathbb{Z}$ injektiv in $\mathbb{Q}$ abgebildet. Bild ist die Menge rationaler zahlen, die in gekürzter Darstellung den Nenner 1 haben. (Beweis mündlich)
Identifiziere $\mathbb{Z} \ni z = \frac{z}{1} \in \mathbb{Q}$.
Dies ist eine Vergrößerung des Zahlbereichs.
(Anmerkung Heiko: In der Mitschrift nutze ich nachfolgend wenn möglich kein "*" mehr, sondern schreibe Buchstaben nebeneinander - dies ist als Multiplikation zu werten...)

Satz 7.5: "gleiche" Brüche

Sei $q = \frac{z}{k}$ gekürzt. Dann gilt $\frac{t}{l} = q \Leftrightarrow \exists n \in \mathbb{N}_1 : t = zm \wedge l = km$

Beweis:

- "$\Leftarrow$" $\surd$
- "$\Rightarrow$" Dividiere l mit Rest durch k: $l = qk + r$

  Nun ist zu Zeigen: $r = 0$, dies ist ein häufiger Trick um zeigen zu können, l ist Vielfaches von k.

  $\frac{t}{l} = \frac{z}{k}$, d.h. $tk = zl = zqk + zr \Rightarrow (t - zq)k = zr \quad 0 \leq r < k$

  Annahme $r \neq 0$: $\Rightarrow \frac{z}{k} = \frac{t-zq}{r}$, aber $r < k$, aber $\frac{z}{k}$ in gekürzter Darstellung. $\lightning$

  Also $r = 0$. Es folgt $l = qk$. Daraus folgt $tk = zqk + zr = zqk \Rightarrow t = zq$ (kürzen)

  Aus $l = qk + r$ folgt $q \in \mathbb{N}_1$

Nachfolgend werden die Rechenstrukturen und die Anordnung der rationalen Zahlen durchgenommen und auf Verträglichkeit mit der Einbettung der ganzen Zahlen überprüft.
Zur Erinnerung aus den ganzen Zahlen: Wir haben auf $\mathbb{N} \times \mathbb{N}$ die Operationen $\oplus$, $\otimes$ definiert und daraus dann verträgliche Operationen auf die Äquivalenzklassen herausgelesen. Analog auch hier. Auch haben wir, wie nachfolgend wieder passiert, die "intuitiv" in $\mathbb{Z}$ bekannten Berechnungen genutzt um die Operationen zu definieren.
(Auf Nachfrage:) Wir brauchen für dies hier noch kein Auswahlaxiom, da alle Mengen abzählbar sind.

$\oplus : (\mathbb{Z} \times \mathbb{N}_1) \times (\mathbb{Z} \times \mathbb{N}_1) \mapsto (\mathbb{Z} \times \mathbb{N}_1)$: $((z,k),(t,l)) \mapsto (zl + tk, kl)$

$\otimes : (\mathbb{Z} \times \mathbb{N}_1) \times (\mathbb{Z} \times \mathbb{N}_1) \mapsto (\mathbb{Z} \times \mathbb{N}_1)$: $((z,k),(t,l)) \mapsto (zt, kl)$

$$\begin{array}{ccc} (\mathbb{Z} \times \mathbb{N}_1) \times (\mathbb{Z} \times \mathbb{N}_1) & \longrightarrow & (\mathbb{Z} \times \mathbb{N}_1) \\ \text{Von Ausw. unabhängig} \Big(\downarrow \Pi \times \Pi & & \Pi \downarrow \\ \mathbb{Q} \times \mathbb{Q} & \overset{\text{Abb.?}}{- - \succ} & \mathbb{Q} \end{array}$$

Satz 7.6: $\otimes$, $\oplus$ Abbildung in $\mathbb{Q}$

Seien $(z,k) \sim (z',k')$, $(t,l) \sim (t',l')$ in $\mathbb{Z} \times \mathbb{N}_1$. Dann gilt $\Pi((z,k) \overset{\oplus}{\otimes} (t,l)) = \Pi((z',k') \overset{\oplus}{\otimes} (t',l'))$

Beweis:

$zk' = z'k$, $tl' = t'l$, wir dürfen erweitern!

$\Pi((z,k) \oplus (t,l)) = \Pi(zl + tk, kl) = \Pi(\underbrace{zk'}_{z'k} ll' + \underbrace{tl'}_{t'l} kk', klk'l') = \Pi(z' \not{k} \not{l}l' + t' \not{l} \not{k}k', \not{k} \not{l}k'l')$

$= \Pi(z'l' + t'k', k'l') = \Pi((z',k') \oplus (t',l'))$

$\oplus$ analog, wenngleich einfacher.

Im nächsten Satz verifizieren wir die Eigenschaften von $+$, $*$ nutzen aber schon die "übliche" Notation. Wir werden ihn nur exemplarisch beweisen, die restlichen Teile sind Analog zu bereits bewiesenen Sätzen und Teilen.

Satz 7.7: $\mathbb{Q}$ mit $+$, $*$ ist (kommutativer!) Körper

$\mathbb{Q}$ mit $+$, $*$ ist (kommutativer!) Körper. Die Rechenoperationen $+$ und $*$ lassen sich auf $\mathbb{Z}$ einschränken und ergeben dort die bereits vorhandenen (bekannten) Rechenoperationen.

Beweis:

Eine Auflistung der formalen Todos, die neutralen Elemente explizit benannt. Für die Inversen Element explizite Rechenvorschriften gegeben.

$+$ kommutativ

$+$ assoziativ

$+$ hat neutrales Element: 0

Es gibt ein inverses Element bezüglich $+$

$*$ kommutativ

$*$ assoziativ

$*$ ist distributiv über $+$

$*$ hat neutrales Element: 1

Es gibt ein inverses Element bezüglich $*$

Nachfolgend Beweise von einzelnen Sachen:

- **0-Element** $\mathbb{Q} \ni \frac{0}{1} = 0 \in \mathbb{Z}$ $\frac{0}{1} + \frac{z}{k} = \frac{0k+z1}{1k} = \frac{z}{k}$
- **Inverses Element bezüglich** $+$ Inverses von $\frac{z}{k}$ ist $\frac{-z}{k}$
- **1-Element** $\frac{1}{1} = 1$
- **Inverses Element von** $\frac{z}{k} \neq \frac{0}{1}$ **bezüglich** $*$ ($\frac{z}{k} \neq \frac{0}{1} \Leftrightarrow z \neq 0$)
  Falls $z > 0$: $\frac{k}{z}$.
  Falls $z < 0$: $\frac{-k}{-z}$.
- **Einschränkung auf ganze Zahlen** $\mathbb{Z} \mapsto \mathbb{Q}$ ist Homomorphismus.
  $\frac{z}{1} + \frac{z}{1} = \frac{z1+t1}{1*1} = \frac{z+t}{1}$
  Multiplikation analog.

Anordnung Ganz genauso wie bei den ganzen Zahlen eingeführt und wesentliche Eigenschaften gezeigt. Wieder ist trotz Notation "kleinergleich" gemeint.
Definiere Relation auf $\mathbb{Z} \times \mathbb{N}_1$: $(z,k) \prec (t,l)$, falls $zl \leq tk$ in $\mathbb{Z}$. $\frac{z}{k} \leq \frac{t}{l} \Leftrightarrow zl \leq tk$

Satz 7.8: Anordnung ist verträglich mit Äquivalenzklassen

Seien $(z,k) \sim (z',k')$, $(t,l) \sim (t',l')$ in $\mathbb{Z} \times \mathbb{N}_1$. Dann $(z,k) \prec (t,l) \Leftrightarrow (z',k') \prec (t',l')$ (ohne Beweis)
Relation auf $\mathbb{Q}$: $\frac{z}{k} \leq \frac{t}{l}$, falls $(z,k) \prec (t,l)$.
Die Unabhängigkeit vom Repräsentanten ist wichtig!

Satz 7.9: $\leq$ ist totale Ordnung auf $\mathbb{Q}$

$\leq$ ist totale Ordnung auf $\mathbb{Q}$. Einschränkung auf $\mathbb{Z}$ ist verträglich mit der bereits vorhandenen totalen Ordnung auf $\mathbb{Z}$.
Monotonie. Sei $q \leq p$:

- $q + u \leq p + u \quad (\forall u \in \mathbb{Q})$
- $q * u \leq p * u \quad (\forall u \in \mathbb{Q}, 0 < u)$
- $q + u \geq p + u \quad (\forall u \in \mathbb{Q}, 0 < -u)$

Beweis: exemplarisch

- $\leq$ **transitiv** (nachdem Reflexivität und Antisymmetrie bewiesen sei)
  Gelten $\frac{z}{k} \leq \frac{t}{l}$, $\frac{t}{l} \leq \frac{x}{m}$. Damit gilt: $zl \leq tk \wedge tm \leq xl$
  $\Leftrightarrow zlm \leq tkm \wedge tmk \leq xlk$, da $k, m > 0$.
  $\Leftrightarrow zlm \leq xlk \Rightarrow zm \leq xk$, d.h. $\frac{z}{k} \leq \frac{x}{m}$
- **Einschränkung auf** $\mathbb{Z}$ $z \leq t$ (in $\mathbb{Z}$) $\Rightarrow z * 1 \leq t * 1$ (in $\mathbb{Z}$) $\Rightarrow \frac{z}{1} \leq \frac{t}{1}$ (in $\mathbb{Q}$) $\surd$
- **Monotonie (3)** $q = \frac{z}{k}$, $p = \frac{t}{l}$, $u = \frac{x}{m}$
  $0 < -u$ heißt: $0 \neq u$, d.h. $x \neq 0$
  $0 \leq -u$ heißt: $\frac{0}{1} \leq \frac{-x}{m}$
  d.h. $0 = 0m \leq (-x) * 1 = -x$, d.h. $x \leq 0$ in $\mathbb{Z}$
  $q \leq p$: $z * l \leq t * k$
  $qu = \frac{zx}{km}$, $pu = \frac{tx}{lm}$
  $zxl \not{m} \geq txk \not{m}$ kürzen, $m > 0, x < 0$
  $(zl)x \geq (tk)x$

In jeder Hinsicht ist nun $\mathbb{Q}$ eine Erweiterung von $\mathbb{Z}$, doch ist die Aufgabe auch wirklich gelöst?
$z, t \in \mathbb{Q}$, $t \neq 0$
Gilt wirklich $\exists u \in \mathbb{Q} : z = tu$? Seien $z = \frac{a}{k}, t = \frac{b}{l}$ Setze $u = z * t^{-1}$. $u = \frac{al}{kb}$ (Falls $b > 0$, ansonsten analog ...)
Nachfolgend kommt noch diverses Brauchbares, Wissenwerten und Interessantes über rationalen Zahlen. Zuerst eine Charakterisierung von $\mathbb{Q}$ über externe Objekte, analog zur ersten Charakterisierung von $\mathbb{Z}$. Es gibt zwar eine Charakterisierung ähnlich der zweiten von $\mathbb{Z}$ durch interne Eigenschaften, doch diese ist schwerer.

Definition 7.10: Charakteristik von Ringen mit 1

(Siehe auch Algebra-Vorlesungen) Sei R ein kommutativer Ring mit 1 (Also $1 \neq 0$!)
Die Charakteristik von R ist 0, wenn $n * 1 \neq 0$ für alle $1 \leq n \in \mathbb{N}$ ist.
Die Charakteristik von R ist p $1 \leq p \in \mathbb{N}$, wenn $\{n \in \mathbb{N} | 1 \leq n, n * 1 = 0\} \neq \emptyset$ ist und p darin das kleinste Element ist.
Notation: $\text{Char}(R) = \begin{cases} 0 & \dots \\ p & \dots \end{cases}$
Bemerkung: Wegen $1 \neq 0$ in R gilt: $1 * 1 \neq 0$, d.h. $\text{Char}(R) \neq 1$.
Die Charakteristik ist die wichtigste numerische Größe um Körper unterscheiden zu können!
Auch wenn wir bislang nicht über Primzahlen geredet haben, werden wir diesen Begriff im nachfolgenden Satz nutzen. [Anm: Dieser soll wie bereits in anderen Mathevorlesungen (Lineare Algebra I) verstanden werden.]
Definieren kann man ihn bereits mit den Mitteln der natürlichen Zahlen.
Ausserdem sei anzumerken: Ein Körper ist immer auch ein Integritätsbereich.

Satz 7.11: K Körper: $\text{Char}(K)$ ist 0 oder Prim

Wenn R Körper ist gilt: $\text{Char}(R) = 0$ oder $\text{Char}(R) = p$ mit p ist Primzahl.

Beweis:
Sei R Körper und $\text{Char}(R) = p \neq 0$.
Annahme: p ist nicht Primzahl.
Damit gibt es $k, l < p$ mit $p = kl$. Dann ist $kl \neq 0$, $l * 1 \neq 0$. Daraus folgt aber
$0 \neq (k * 1)(l * 1) = (k * l) * 1 = p * 1 = 0$ ↯im Integritätsbereich

Satz 7.12: Charakterisierung der Charakteristik

Seien R Ring, $F : \mathbb{Z} \mapsto R$ Homomorphismus. Dann gilt

(a) $\text{Char}(R) = 0 \Leftrightarrow f$injektiv

(b) $\text{Char}(R) = p \Leftrightarrow |Bild(f)| = p$

Beweis: (a)

"⇐" Sei $1 \leq n \in \mathbb{N}$. $n * 1$ in $R \stackrel{?}{=} 0$
$n * 1 = f * f(1) = f(n * 1) = f(n) \neq 0$ wegen f injektiv.

"⇒" **Annahme** f nicht injektiv, etwa $f(z) = f(t)$ mit $z, t \in \mathbb{Z}$ $z \neq t$. oBdA $0 \leq z < t$, d.h. $t - z \in \mathbb{N}$.
$0 = f(t) - f(z) = f(t - z) = (t - z) * 1$ in R ↯$\text{Char}(R) = 0$

Beweis: (b)

"⇒" $f|_{\{0,\dots,p-1\}}$ ist injektiv (wegen p minimal). $\Rightarrow |Bild(f)| \geq p$. Sei $z \in \mathbb{Z}$. Division mit Rest durch p:
$z = qp + r$. $f(z) = q * \underbrace{f(p)}_{=p*1=0} + f(r) = f(r) \in f[\{0,\dots,p-1\}]$, $r \in \{0,\dots,p-1\}$

"⇐" $|Bild(f)| = p$. $f(0),\dots,f(p)$ sind $p+1$ Elemente in $Bild(f)$. $\Rightarrow \exists 0 \leq i < j \leq p$: $f(i) = f(j)$
$\Rightarrow 0 = f(j) - f(i) = f(j - i) = (j - i) * 1$ $(j - i) \in \{1,\dots,p\} \Rightarrow q = \text{Char}(R) \leq j - i$. Dann gilt $|Bild(f)| = q$, also $p = q$.

Lemma 7.13: $\mathrm{Char}(\mathbb{Q}) = 0$

$\mathrm{Char}(\mathbb{Q}) = 0$

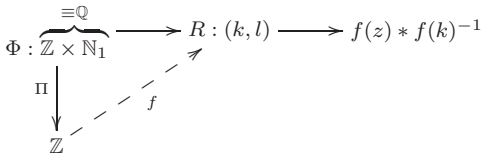
Beweis:
$\mathbb{Z} \mapsto \mathbb{Q}$ injektiv.

Satz 7.14: Charakterisierung von $\mathbb{Q}$

Sei K ein Körper der Charakterisierung 0. Dann gibt es einen eindeutig bestimmten Homomorphismus $F : \mathbb{Q} \mapsto K$. Wenn L ein Körper ist mit: Für jeden Körper K mit $\mathrm{Char}(K) = 0$ gibt es (genau) einen Homomorphismus $L \mapsto K$, dann ist L isomorph zu $\mathbb{Q}$.

Beweis:
Existenz von F:
$\exists! f : \mathbb{Z} \mapsto K$ Homomorphismus mit $1 \mapsto 1$. f ist injektiv, weil $\mathrm{Char}(K) = 0$.

Definiere: (Wegen injektiv $\neq 0$, K Körper, daher existiert das Inverse.)

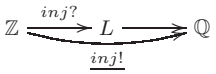


F existiert, falls gilt: Für $\frac{z}{k} = \frac{t}{l}$ in $\mathbb{Q}$ ist $f(z) * f(k)^{-1} = f(t) * f(l)^{-1}$.

Beweis:

$$\begin{aligned} f(z)f(k)^{-1} &= f(t)f(l)^{-1} \\ \Leftrightarrow f(z)f(l) &= f(t)f(k) \\ \Rightarrow f(zl) &= f(tk) \\ \text{Gilt, weil} \quad & zl = tk. \end{aligned}$$

$F(\frac{z}{k}) = f(z)f(k)^{-1}$ unabhängig von Wahl des Repräsentanten.
Homomorphie nicht bewiesen.
F eindeutig
Sei $F'\mathbb{Q} \mapsto K$ Homomorphismus. $\Rightarrow$ $\left.\begin{matrix} F|_{\mathbb{Z}} : \mathbb{Z} \mapsto K \\ F'|_{\mathbb{Z}} : \mathbb{Z} \mapsto K \end{matrix}\right\}$ Nur ein Homomorphismus $\mathbb{Z} \mapsto K \Rightarrow F|_{\mathbb{Z}} = F'|_{\mathbb{Z}}$
Sei $q = \frac{z}{k} \in \mathbb{Q}$ $F(q) = F(z) * F(k)^{-1} = f(z)f(k)^{-1} = F'(z)F'(k)^{-1} = F'(q)$
L isomorph $\mathbb{Q}$ Sei L wie in der Behauptung. $g : L \mapsto \mathbb{Q}$, $h : \mathbb{Q} \mapsto L$. $\mathrm{Char}(L) = 0$



Weil es genau einen Homomorphismus von $L \mapsto L$ bzw $\mathbb{Q} \mapsto \mathbb{Q}$ gibt:
$h \circ g : L \mapsto L$, $id_L : L \mapsto L \Rightarrow id_L = h \circ g$
$g \circ h : \mathbb{Q} \mapsto \mathbb{Q}$, $id_{\mathbb{Q}} : \mathbb{Q} \mapsto \mathbb{Q} \Rightarrow id_{\mathbb{Q}} = g \circ h$
$\Rightarrow$ es ist Isomorphismus.

Zum Schluss noch zwei Eigenschaften der Anordnung. Erst das archimedisches Prinzip, dann "dicht geordnet".

Definition 7.15: archimedisch

R sei ein total geordneter Ring (es geht auch Gruppe, nur die Addition wird genutzt).
R ist archimedisch, wenn gilt:
Für $0 < a, b \in R$ gibt es natürliche Zahlen $r, s \in \mathbb{N}$ mit $a \leq r * b$, $b \leq s * a$.

Satz 7.16: $\mathbb{Q}$ ist archimedisch geordnet

$\mathbb{Q}$ ist archimedisch geordnet

Beweis:
Seien $\frac{z}{k}, \frac{t}{l} > 0$. oBdA $\frac{z}{k} \leq \frac{t}{l} \Rightarrow \frac{z}{k} \leq 1 * \frac{t}{l}$. Wegen $zl \leq tk$. Division mit Rest: $tk = q(zl) + r$, $0 \leq r < zl$.
$\Rightarrow tk < q(zl) + (zl) = (q+1)(zl) \Rightarrow \frac{t}{l} < (q+1)\frac{z}{k}$.

Es gibt auch Körper $\ncong \mathbb{Q}$, die archimedisch sind. z.B. die reelen Zahlen.

Definition 7.17: Dicht geordnet

Sei $(M, \leq)$ eine total geordnete Menge.
M heisst dicht geordnet, falls: $\forall a, b \in M : a < b \Rightarrow \exists c \in M : a < c < b$.
Dicht geordnet $\equiv$ es gibt keine aufeinander folgende Zahlen.
Jeder angeordnete Körper ist dicht geordnet, $\mathbb{Z}$ ist nicht dicht geordnet.

Satz 7.18: $\mathbb{Q}$ ist dicht geordnet

Beweis:
Seien $x, y \in \mathbb{Q}$, $x < y$. Sei $x = \frac{z}{k}$, $y = \frac{t}{l}$. Dann ist $zl < tk$. (Könnten direkt aufeinanderfolgend sein, wenn wir es verdoppeln ist dieser Fall ausgeschlossen.)
$\Rightarrow 2zl < 2zl + 1 < ztk \Rightarrow x = \frac{z}{k} = \frac{2zl}{2kl} < \frac{2zl+1}{2kl} < \frac{2tk}{2kl} = \frac{t}{l} = y$

Der nächste Abschnitt geht über die reelen Zahlen. $\mathbb{Q}$ haben wir in diesem Kapitel nicht vollständig erschöpfend behandelt, aber die Herangehensweise sollte klar und nun bekannt geworden sein. Auch die anderen Eigenschaften können axiomatisch gezeigt werden.

2.8 Die reellen Zahlen

Einführung

[Anmerkung Heiko:] Die Zeichnungen in diesem Kapitel dienen zur Veranschaulichung und Heranführen, die Beweise sind (bislang) nicht vollständig daran geführt worden.
Wieder wollen wir den Zahlbereich erweitern, auch hier könnten wir die Rechenoperationen nutzen, um dies zu erreichen. (z.B. mit der Quadratwurzel für alle rationalen Zahlen). Dies gehört aber eher in die Algebra-Vorlesung. Für reele Zahlen stellen wir uns eine andere Aufgabe: Das Supremum.
Sei M eine nichtleere Teilmenge von $\mathbb{Q}$. **Gesucht:** Vergrößerter Zahlbereich in dem jede nicht-leere Teilmenge ein Supremum hat.
Wir brauchen jetzt noch eine sinnvolle Einschränkung, denn:
Sei M der Zahlbereich. Sei a das Supremum. $a < a+1$, $a+1 \in M \Rightarrow a+1 \leq a$ unmöglich.
Damit ist die Forderung unerfüllbar.
Also modifizieren wir unsere Forderung: Jede nach oben beschränkte nicht-leere Teilmenge hat ein Supremum.
Einschub: Supremum $(M, \leq)$ total geordnet, $a \subset M$ Teilmenge. $x \in M$ ist Supremum, von A, falls: $\forall a \in A : a \leq x \; wedge \forall y \in M : (\overbrace{\forall a \in A : a \leq y}^{y \text{ auch obere Schranke}}) \Rightarrow x \leq y$
Frage: Ist $\mathbb{Q}$ bereits mit der Eigenschaft?
Beispiel: In $\mathbb{Q}$ gibt es nach oben beschränkte nicht-leere Teilmengen, die kein Supremum haben.
Setze
$M = \{x \in \mathbb{Q} | 0 < x \wedge x^2 < 2\}$

- $M \neq \emptyset$: $1 \in M$
- M n.o. beschränkt: $\forall x \in M : x < 2$ (Wenn $x \geq 2 : x^2 \geq 4 > 2 \Rightarrow x \notin M$).

Behauptung M hat kein Supremum (in $\mathbb{Q}$)
Annahme M hat Supremum $q \in \mathbb{Q}$. Es ist $1 \leq q$. Schreibe $q = \frac{k}{l}$ gekürzt. Dann ist $l \leq k$.
Annahme $q^2 > 2$: Weil $\mathbb{Q}$ archimedisch ist: $\exists N \in \mathbb{N} : N * (q^2 - 2) > 2q$. $\frac{1}{N} > 0$. Sei $0 < r < \frac{1}{N}$, $r \in \mathbb{Q}$.
$\Rightarrow q^2 - 2 > 2\frac{1}{N} * q > 2rq$
$\Rightarrow q^2 - 2rq + r^2 > 2$
$\Rightarrow (q-r)^2 > 2$
$\Rightarrow q - r \notin M$ für alle $0 < r < \frac{1}{N} \Rightarrow q$ ist nicht Supremum von M. $\lightning$
Annahme $q^2 < 2$: Weil $\mathbb{Q}$ archimedisch ist: $\exists N \in \mathbb{N} : N * (2 - q^2) > 2q + 1$.
$\Rightarrow 2 > q^2 + 2\frac{1}{N} * q + \frac{1}{N} > q^2 + 2\frac{1}{N} * q + \frac{1}{N^2} = (q + \frac{1}{N})^2 \Rightarrow q + \frac{1}{N} \in M \Rightarrow q$ ist nicht Supremum von M. $\lightning$
Also $q^2 = 2$, d.h. $k^2 = 2 * l^2$
Nun kann man mittels Primzahlen und Teilbarkeit argumentieren, wenn wir darüber etwas gemacht hätten ($2|k^2$, ...). Wir nehmen das gleiche Argument, müssen aber bisserl drumherum labern.
Division mit Rest: $k = 2a + b$, $0 \leq b < 2$
Annahme: $b = 1$ $k^2 = 4a^2 + 4a + 1 = 2l^2 \Rightarrow 1 = 2(l^2 - 2a^2 - 2a) \Rightarrow 2 \in \mathbb{Z}^x = \{+1, -1\}$ (2 ist Einheit) $\lightning$.
Also $b = 0$ $4a^2 = k^2 = 2l^2 \Rightarrow 2a^2 = l^2$ Analog wie oben: $l = 2 * c$, $c \in \mathbb{N}$.
Also $q = \frac{k}{l} = \frac{2a}{2c} = \frac{a}{c}$, $c < l$, weil $c + c = l$. $\lightning(q$ gekürzt)
$\Rightarrow q \notin \mathbb{Q}$
Nachfolgend die Konstruktion der reellen Zahlen...

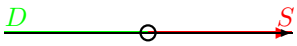
> **Julius Wilhelm Richard Dedekind**[8] (* 6. Oktober 1831 in Braunschweig; Tod: 12. Februar 1916 ebd.) war ein deutscher Mathematiker. [Anmerkung: Zahlentheoretiker]

[8] http://de.wikipedia.org/wiki/Richard_Dedekind

Definition 8.1: Dedekind'scher Schnitt

Ein Dedekind'scher Schnitt in $\mathbb{Q}$ ist ein Paar (D, S) mit folgenden Eigenschaften:

- $D \subseteq \mathbb{Q}$, $S \subseteq \mathbb{Q}$.
- $D \neq \emptyset$, $S \neq \emptyset$, $D \cap S = \emptyset$, $|\mathbb{Q} \backslash (D \cup S)| \leq 1$ (letzteres kann auch anders gemacht werden)
- $\forall x \in \mathbb{Q} \forall d \in D : x < d \Rightarrow x \in D$
- $\forall x \in \mathbb{Q} \forall s \in S : s < x \Rightarrow x \in S$
- D hat kein größtes Element, S hat kein kleinstes Element.
- D Untermenge, S Obermenge.



Menge der Schnitte wird Menge der reellen Zahlen. Es gibt viele andere Möglichkeiten die Reelle Zahlen axiomatisch einzuführen, z.B. mittels den Cauchy-Folgen (Ohne Limes), Konvergenz oder Dezimalfolgen, was dann aber deutlich aufwändiger ist. In München hat ein (späterer) Kollege diesen Ansatz verfolgt und ein ganzes Semester gebraucht um die reellen Zahlen einzuführen...
Die "reellen" Zahlen nehmen wir nur als Hintergrundwissen, zum Teil sind die Eigenschaften redundant - im Satz 8.3 werden sie genauer charakterisiert.

Beispiel 8.2: Dedekind'sche Schnitte

(a) Sei $q \in \mathbb{Q}$. $D_q = \{x \in \mathbb{Q} | x < q\}$. $S_q = \{x \in \mathbb{Q} | q < x\}$. Es gelten die Eigenschaften. ($\surd$)

(b) $D = \{x \in \mathbb{Q} | x \leq 0 \vee x > 0 \wedge x^2 < 2\}$ $S = \{x \in \mathbb{Q} | x > 0 \wedge x^2 > 2\}$

(Das ist M vereinigt mit den negativen Zahlen (s.o.), die Eigenschaften sind erfüllt.
$|\mathbb{Q} \backslash (D \cup S)| = 0$

Satz 8.3: Abhängigkeit Untermenge $\leftrightarrow$ Obermenge

Sei $\mathcal{U}$ die Menge der Teilmengen $Y \subseteq \mathbb{Q}$ mit:

- $Y \neq \emptyset$
- $\forall x \in \mathbb{Q} \forall y \in Y : (x < y \rightarrow x \in Y)$
- $\mathbb{Q} \backslash Y \neq \emptyset$
- Y hat kein größtes Element.

Sei $\mathcal{O}$ die Menge der Teilmengen $Z \subseteq \mathbb{Q}$ mit:

- $Z \neq \emptyset$
- $\forall x \in \mathbb{Q} \forall z \in Z : (z < x \rightarrow x \in Z)$
- $\mathbb{Q} \backslash Z \neq \emptyset$
- Y hat kein kleinstes Element.

Dann sind die Abbildungen
[$\mathbb{Q}^c$: Menge der dedekind'schen Schnitte.]
$\mathbb{Q}^c \to \mathcal{U} : (D, S) \mapsto D$
$\mathbb{Q}^c \to \mathcal{O} : (D, S) \mapsto S$
bijektiv.

Beweis:
Der Beweis wird nur für $\mathcal{U}$ durchgeführt.
Die Abbildung ist injektiv:
$(D, S), (D', S') \in \mathbb{Q}^c, D = D'$
Setze $\overline{S} = \mathbb{Q} \backslash D$
Falls $\overline{S}$ kein kleinstes Element hat:
$\left(D, \overline{S}\right) \in \mathbb{Q}^c$
$S = \overline{S} = S'$
$S, S' \subseteq \overline{S}$
$|\mathbb{Q} \backslash (D \cup S)| \leq 1$
$|\mathbb{Q} \backslash (D \cup S')| \leq 1$
$D \cup S, D \cup S' \subseteq D \cup \overline{S}$
Falls $S \neq \overline{S} : \overline{S} = S \dot\cup \{q\}$
Dann ist q kleinstes Element von $\overline{S}$
Sonst: $\exists x \in \overline{S} : x < q$
Dann $x \in S$ also $q \in S$ ↯
Also $S = \overline{S}$ (Ebenso: $S' = S$
Falls $\overline{S}$ kleinstes Elmement hat, etwa q:
$\overline{S} = S \dot\cup \{q\}$
Ebenso: $\overline{S} = S' \dot\cup \{q\}$
$\Rightarrow S = S'$
Damit ist die Injektivität gezeigt.
Es bleibt die Surjektivität zu zeigen:
Sei $Y \in \mathcal{U}$
Setze $D = Y$ und
$$S = \begin{cases} \mathbb{Q} \backslash Y & \text{, falls } \mathbb{Q} \backslash Y \text{ kein kleinstes Element hat} \\ (\mathbb{Q} \backslash Y) \backslash \{q\} & \text{, falls } \mathbb{Q} \backslash Y q \text{ als kleinstes Element hat} \end{cases}$$

Satz 8.4: Dedekind'scher Schnitt ist beliebig nahe

Es sei $(D, S) \in \mathbb{Q}^c$.
Dann gilt:
$\forall s \in S \forall d \in D : s - d > 0$
und
Für alle $N \in \mathbb{N}_1$ gibt es $s_N \in S$ und $d_N \in D : s_N - d_N < \frac{1}{N}$

Beweis:
Annahme: $\exists 1 \leq N : \forall s \in S : \forall d \in D : s - d \geq \frac{1}{N}$
Sei $d \in D$ fest gewählt.
Setze $M = \{l \in \mathbb{N} | d + \frac{l}{3N} \in S\}$.
$M \neq \emptyset \Rightarrow$ es existiert ein kleinstes Element $k + 1 \in M$.
$k \notin M$, d.h. $d + \frac{k-1}{3N} \in D$, $d + \frac{k+1}{3N} \in S$
$M \neq \emptyset$
$S \neq \emptyset$, also $\exists s \in S$
Zu $d, s \in \mathbb{Q} \exists a \in \mathbb{N}_1 : sa, da \in \mathbb{Z}$
$\Rightarrow 3N(sa - da) \in \mathbb{N}_1$.
Wähle $k \in \mathbb{N}_1 : 3N(s - d)a < ka$ (Archimedizität)
$\Rightarrow s < d + \frac{k}{3N}$

Satz 8.5: $\leq$ auf Dedekind'sche Schnitte

$(D, S), (D', S') \in \mathbb{Q}^c$.

Defniniere die Relation: $(D,S) \leq (D',S')$, falls $D \subseteq D'$
$\Rightarrow \leq$ ist totale Ordnung auf $\mathbb{Q}^c$.

Beweis:
Reflexivität und Transitivität sind trivial zu sehen.(elementare Mengenlehre)
Wir gehen auf die Antisymmetrie ein:
$(D,S) \leq (D',S')$ und $(D',S') \leq (D,S)$
$\Rightarrow D = D' \underbrace{\Rightarrow}_{S.I.8.3} (D,S) = (D',S')$
Letztlich bleibt noch die Totalität zu zeigen:
Seien $D, D' \in \mathcal{U}$(Menge der Unterklassen)
Sei D keine Teilmenge von $D' \Rightarrow \exists d \in D : d \notin D'$
Sei $d' \in D'$ beliebig $\Rightarrow d' < d$ (aus $d' \geq d \Rightarrow d \in D'$ ↯)
$\Rightarrow d' \in D \Rightarrow D' \subset D$

Satz 8.6: $q \mapsto (D_q, S_q)$

Die Abbildung $\mathbb{Q} \to \mathbb{Q}^c : q \mapsto (D_q, S_q)$ ist injektiv und ordnungserhaltend.
Desweiteren ist ihr Bild $B = \{(D,S) \in \mathbb{Q}^c || \mathbb{Q} \backslash (D \cup S)| = 1\}$

Beweis:
Seien $q, r \in \mathbb{Q}, q < r$.
$\Rightarrow D_q \subset D_r$ weil $q \in D_r, q \notin D_q$.
Damit ist schon die Injektivität und die Ordnungserhaltung gezeigt.
Falls $|\mathbb{Q}\backslash(D \cup S)| = 1 : \{q\} = \mathbb{Q}\backslash(D \cup S)$
Dann ist $D_q = D$!
Erläuterung der letzten Zeile:
$\forall d \in D : d < q \Rightarrow D \subseteq D_q$
Sei andererseits $x \in D_q \Rightarrow x < q$(natürlich: $x \neq q$)
$\Rightarrow x \in D \vee x \in S$ Falls $x \in S \Rightarrow q \in S$ ↯$\Rightarrow x \in D$.
$\Rightarrow D_q \subseteq D$
q.e.d.

Satz 8.7: $\mathbb{Q}$ ist dicht in $\mathbb{Q}^c$

$\mathbb{Q}$ ist dicht in $\mathbb{Q}^c$.

Beweis:
Seien $(D,S), (D',S') \in \mathbb{Q}^c, (D,S) < (D',S')$
$\Rightarrow \exists q \in \mathbb{Q} : q \in D' \wedge q \notin D$
Sei $r \in \mathbb{Q} : q < r \in D'$
$\Rightarrow (D,S) < (D_r, S_r) < (D',S')$
q.e.d.

Wichtige Eigenschaft der Dedekind'sche Schnitte: Elemente kommen sich beliebig nahe.

Satz 8.8: Existenz von Supremum/Infimum

In $\mathbb{Q}^c$ hat jede nach oben beschränkte nicht-leere Menge ein Supremum und jede nach unten beschränkte nicht-leere Menge ein Infimum.

Beweis: Supremum
Sei $M \subseteq \mathbb{Q}^c$, $M \neq \emptyset$, $\exists (D_0, S_0) \in \mathbb{Q}^c. \forall (D,S) \in M : (D,S) \leq (D_0, S_0)$.
Setze $\overline{D} := \bigcup_{(D,S) \in M} D$.

Behauptung $\overline{D} \in \mathcal{U}$

Beweis:

- $\overline{D} \neq \emptyset$ $M \neq \emptyset$. Sei $(D,S) \in M$. $\Rightarrow D \neq \emptyset \wedge D \subseteq \overline{D}$

- $\mathbb{Q}\backslash\overline{D} \neq \emptyset$ Sei $s \in S_0$. $\Rightarrow s \notin D$ für alle $(D,S) \in M$. $\Rightarrow s \notin \overline{D}$.
- **Sei** $d \in \overline{D}$, $x < d \Rightarrow x \in \overline{D}$ $d \in \overline{D} \Rightarrow \exists (D,S) \in M : d \in D$, $x < d \Rightarrow x \in D \subseteq \overline{D}$
- $\overline{D}$ **hat kein größtes Element.** Annahme $d \in \overline{D}$ ist größtes Element. Dann gibt es $(D,S) \in M$ mit $d \in D$. D hat kein größtes Element, also $\exists r \in D : d < r \Rightarrow d < r \in \overline{D}$ ↯

Sei $(\overline{D},\overline{S})$ der Dedekind'sche Schnitt mit Unterklasse $\overline{D}$.
Behauptung $\forall (D,S) \in M : (D,S) \leq (\overline{D},\overline{S})$ ✓

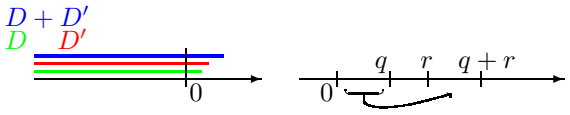
Behauptung $(\overline{D},\overline{S})$ **ist kleinste obere Schranke**

Beweis:
Sei (D',S') irgend eine obere Schranke.
$\Rightarrow \forall (D,S) \in M : D \subseteq D'$
$\Rightarrow \overline{D} = \bigcup_{(D,S)\in M} D \subseteq D'$
$\Rightarrow (\overline{D},\overline{S}) \subseteq (D',S')$ ✓

Die ursprüngliche Forderung ist damit erfüllt, jetzt gehen wir an die Rechenoperationen heran. Als erstes die Addition, die Multiplikation ist schwerer/komplexer.
$D + D' := \{d + d' | d \in D, d' \in D'\}$

Satz 8.9: Addition in $\mathbb{R}$

Seien (D,S), $(D',S') \in \mathbb{Q}^c$. Dann ist $(D+D', S+S')$ ein Dedekind'scher Schnitt. Damit ist $((D,S),(D',S')) \mapsto (D+D',S+S') =: (D,S)+(D',S')$ Verknüpfung.
Dann ist $\mathbb{Q}^c$ mit dieser Verknüpfung eine abelsche Gruppe. Es gilt das Monotoniegesetz $(D,S) \leq (D',S') \Rightarrow (D,S)+(D_1,S_1) \leq (D',S')+(D_1,S_1)$.
Die Verknüpfung läßt sich auf $\mathbb{Q}$ einschränken und gibt dort die bekannte Addition.



Beweis:
$(D+D', S+S')$ Dedekindscher Schnitt

- $D + D' \neq \emptyset$ $d \in D$, $d' \in D \Rightarrow d + d' \in D + D'$
  $S + S' \neq \emptyset$ analog
- $(D+D') \cap (S+S') = \emptyset$ Annahme falsch: Sei $x \in (D+D') \cap (S+S')$. $x = d + d' = s + s'$
  $\Rightarrow \underbrace{s-d}_{>0} = d' - s' = \underbrace{-(s'-d')}_{<0}$ ↯ $\underbrace{\qquad}_{>0}$
- $x < d + d', d \in D, d' \in D' \Rightarrow x \in D + D'$ $x - d' < d \in D \Rightarrow x - d' \in D$
  $x = (x - d') + d' \in D + D'$
  $x > s + s', s \in S, s' \in S' \Rightarrow x \in S + S'$ analog
- $D + D'$ **hat kein größtes Element** Sei $d + d' \in D + D'$. Sei $d < r \in D$. Es folgt $d + d' < r + d' \in D + D'$.
  $S + S'$ **hat kein kleinstes Element** analog
- $|\mathbb{Q}\backslash((D+D') \cup (S+S'))| \leq 1$ **Annahme:** $x, y \notin (D+D') \cup (S+S'), x < y$. Sei $1 \leq N \in \mathbb{N}$ mit $x + \frac{1}{N} < y$.
  Nach 8.4: Zu $\frac{1}{N}$ gibt es $d \in D, d' \in D', s \in S, s' \in S'$ $s - d, s' - d' < \frac{1}{2N}$.
  $d + d' \in D + D', s + s' \in S + S'$. $(s + s') - (d + d') = (s - d) + (s' - d') < \frac{1}{N}$. Dann ist $s + s' < y$ oder $x < d + d'$. Damit $x - d' < d \in D \Rightarrow x - d' \in D$, $x = (x - d') + d' \in D + D'$ ↯
  (Analog: $s + s' < y$ ↯)

Rechenregeln für Addition

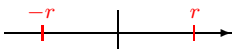
- **+ ist assoziativ, kommutativ(analog**
  $\left.\begin{array}{l}((D,S)+(D',S'))+(D'',S'') \\ (D,S)+((D',S')+(D'',S''))\end{array}\right\}$ sind Dedekindsche Schnitte
  Unterklassen:
  $\left.\begin{array}{l}(D+D')+D'' \\ D+(D'+D'')\end{array}\right\}$ gleich, weil + in $\mathbb{Q}$ assoziativ

- **Neutrales Element** (D_0, S_0)
  Nachrechnen: $(D, S) + (D_0, S_0) = D, S)$
  Unterklassen: $D + D_0 = D$?

  "$\subseteq$" Sei $d \in D$, $c \in D_0$. d.h. $c < 0$
  $\Rightarrow d + c < d$ (+ monoton in $\mathbb{Q}$)
  $\Rightarrow d + c \in D$

  "$\supseteq$" Sei $d \in D$. D hat kein größtes Element.
  $\Rightarrow \exists d' \in D : d < d'$
  $\Rightarrow d - d' < 0$, d.h. $d - d' \in D_0$
  Schreibe $d = d' + (d - d') \in D + D_0$

- **Inverses Element zu** $(D, S) \in \mathbb{Q}^c$



  Setze $D' = -S$, $S' = -D$. Damit $(D', S') \in \mathbb{Q}^c$.
  $(D, S) + (D', S') = (D_0, S_0)$? d.h. $D + D' = D_0$

  "$\subseteq$" Sei $d \in D$, $d' \in D' = -S$, d.h. $-d' \in S \Rightarrow d < -d' \Rightarrow d + d' < 0$, d.h. $d + d' \in D_0$.

  "$\supseteq$" Sei $q \in D_0$, d.h. $q < 0$.
  Zu Zeigen: $q = d - s$, $d \in D$, $s \in S$, d.h. $s = d \underbrace{-q}_{>0}$
  Zu $-q$ gibt es $d \in D$, $s \in S$ mit $s - d < -q \Rightarrow s < d - q \Rightarrow d - q \in S$. Damit $q = d - \underbrace{(d - q)}_{s}$.

- **Monotonie** Sei $(D, S) < (D', S')$.
  Zu Zeigen: $(D, S) + (D'', S'') < (D', S') + (D'', S'')$
  d.h. $D + D'' \subsetneq D' + D''$. $(\surd)$

- **Einschränkung von + auf** $\mathbb{Q}$ Seien $q, r \in \mathbb{Q}$. Seien zugehörig $(D_q, S_q), (D_r, S_r) \in \mathbb{Q}^c$.
  Behauptung: $D_q + D_r = D_{q+r}$

  "$\subseteq$" $(\surd)$

  "$\supseteq$" Sei $x \in D_{q+r}$. Sei $x' \in D_{q+r}$, $x < x'$. Es folgt $x' - r < q$, d.h. $x' - r \in D_q$.
  $x = \underbrace{(x' - r)}_{\in D_q} + \underbrace{(r + x - x')}_{\in D_r}$

Achtung: Nachfolgend entspricht (D_0, S_0) der 0 im Anschaulichen.

Korollar 8.10: $\mathbb{Q}^c$ ist eine archimedisch angeordnete Gruppe

$\mathbb{Q}^c$ ist eine archimedisch angeordnete Gruppe.

Beweis:

Seien $(D, S), (D', S') > (D_0, S_0)$ Suche $M, N \in \mathbb{N}$ mit: $(D', S') < M \overset{M-FacheAddition}{*} (D, S)$,
$(D, S) < N * (D', S')$.
oBdA $(D, S) \leq (D', S') \Rightarrow (D, S) < 2 * (D', S')$.
In D: $0 < d$. Wähle $0 < s' \in S'$. Es gibt $N \in \mathbb{N}_1 : s' < N * d$.
$\Rightarrow N * d$ ist in der Unterklasse von $N * (D, S)$
$\Rightarrow s'$ liegt auch darin $\Rightarrow D' \subsetneq$ Unterklasse $N * (D, S)$

Multiplikation wird drastisch komplizierter, egal wie wir es anstellen wollen. Der Grund ist, dass es zwei Monotoniegesetze (positiv und negativ) gibt, damit gibt es immer Fallunterscheidungen. Diese versuchen wir aber möglichst zu vermeiden. Die Idee hinter den nachfolgenden Lemma und Sätzen ist erstmal nur mit positiven Zahlen zu arbeiten und einen monotonen Homomorphismus zu finden. Erst danach wird dieser auf negative Zahlen ausgedehnt (wo er Antimonoton ist).
Nachfolgende sind die beiden nachfolgenden Notationen verwendet:
$(\mathbb{Q}^c)^> = \{(D, S) \in \mathbb{Q}^c | (D, S) > (D_0, S_0)\}$
$(\mathbb{Q}^c)^\geq = \{(D, S) \in \mathbb{Q}^c | (D, S) \geq (D_0, S_0)\}$
Wir werden im nächsten Satz erstmal (D, S) festhalten und (A, B) variieren. Dies verhält sich aber völlig symmetrisch, so daß wir nachfolgend die Kommutativität leicht beweisen können.

Lemma 8.11: Multiplikation im positiven

Seien $(D,S),(A,B) \in (\mathbb{Q}^c)^{\geq}$. Dann ist $S*B \in \mathcal{O}$ (Menge der Oberklassen) Sei $\sigma_{(D,S)}(A,B)$ der zugehörige Dedekindsche Schnitt. Es ist $\sigma_{(D,S)}(A,B) \in (\mathbb{Q}^c)^{\geq}$.
$\sigma_{(D,S)}(A,B) = (D_0,S_0) \Leftrightarrow (D,S) = (D_0,S_0) \vee (A,B) = (D_0,S_0)$

Beweis: $s*B \in \mathcal{O}$

- $S*B \neq \emptyset$ Wähle $s \in S, b \in B \Rightarrow s*b \in S*B$
- $\mathbb{Q}\backslash S*B \neq \emptyset$ $S,B \subseteq \mathbb{Q}^{>} \Rightarrow S*B \subseteq \mathbb{Q}^{>}$, $0 \notin S*B$
- $x \in SB$, $x<y \Rightarrow y \in SB$ Schreibe $x = sb$. $1 < \frac{y}{x} \Rightarrow s < \frac{y}{x}*s$, d.h. $\frac{y}{x}s \in S$ und $\frac{y}{x}(s*b) = (\frac{y}{x}*s)*b \in SB$
- $S*B$ **hat kein kleinstes Element** Seien $s \in S$, $b \in B \Rightarrow \exists s' \in S, b' \in B : s' < s, b' < b$
  $\Rightarrow s'*b' \in SB \wedge s'*b' < s*b$

$\sigma_{(D,S)}(A,B) \in (\mathbb{Q}^c)^{\geq}$, weil $S*B \subset S_0$

Beweis: $a*b = 0 \Leftrightarrow a = 0 \vee b = 0$

"$\Leftarrow$" Sei $(D,S) = (D_0,S_0) \Rightarrow S*B = S_0$.
Sei $(A,B) = (D_0,S_0) \Rightarrow S*B = S_0$.

"$\Rightarrow$" Seien $(A,B),(D,S) \in (\mathbb{Q}^c)^{>}$. Seien $q,r \in \mathbb{Q}^{>}$ mit $q \in S, r \notin B \Rightarrow q*r \notin SB$

Zu $(D,S) \in (\mathbb{Q}^c)^{\geq}$:
Wissen: $\sigma_{(D,S)} : (\mathbb{Q}^c)^{\geq} \mapsto (\mathbb{Q}^c)^{\geq} : (A,B) \mapsto \sigma_{(D,S)}(A,B)$
Symmetrie zwischen $(A,B),(D,S)$
Man sollte grundsätzlich so früh wie möglich die Kommutativität beweisen.

Lemma 8.12: Multiplikation kommutativ und distributiv über Addition

$(D,S),(D',S'),(A,B),(A',B') \in (\mathbb{Q}^c)^{\geq}$
Dann gilt:

(a) $\sigma_{(D,S)}(A,B) = \sigma_{(A,B)}(D,S)$ (Kommutativ)

(b) $\sigma_{(D,S)}((A,B)+(A',B')) = \sigma_{(D,S)}(A,B) + \sigma_{(D,S)}(A',B')$ (Rechts-Distributiv)

(c) $\sigma_{((D,S)+(D',S'))}(A,B) = \sigma_{(D,S)}(A,B) + \sigma_{(D',S')}(A,B)$ (Links-Distributiv)

Beweis:

(a) klar (Symmetrisch)

(b) $(A,B)+(A',B') = (A+A',B+B')$. $\sigma_{(D,S)}((A,B)+(A',B'))$ hat Oberklasse: $S*(B+B')$
$\sigma_{(D,S)}(A,B) : S*B$ "+" $\sigma_{(D,S)}(A,B) : S*B'$ "=" $SB+SB'$
$S*(B+B') = SB+SB'$ (Distributivität in $\mathbb{Q}$)

(c) Mit (a) und (b) klar.

Wissen
* Homomorphismus bezüglich Addition,
* Symmetrie zwischen (D,S) und (A,B).
Zu tun: Ausdehnen auf Gruppe der Dedekindsche Schnitte, da gibt es wieder verschiedene Möglichkeiten das zu machen. Wir versuchen uns möglichst viele Fallunterscheidungen zu sparen, da diese sich (exponentiell) vermehren.

Lemma 8.13: Wohldefiniertheit von σ (Homom.)

$(D,S) \in (\mathbb{Q}^c)^{\geq}$; $(A,B),(A_1,B_1),(A_2,B_2),(A_3,B_3) \in (\mathbb{Q}^c)^{\geq}$. Sei
$(A,B)-(A_1,B_1) = (A_2,B_2)-(A_3,B_3)$ Dann gilt:
$\sigma_{(D,S)}(A,B) - \sigma_{(D,S)}(A_1,B_1) = \sigma_{(D,S)}(A_2,B_2) - \sigma_{(D,S)}(A_3,B_3)$

Beweis:
$\sigma_{(D,S)}(A,B)+\sigma_{(D,S)}(A_3,B_3)=\sigma_{(D,S)}((A,B)+(A_3,B_3))=\sigma_{(D,S)}((A_2,B_2)+(A_1,B_1))=$
$\sigma_{(D,S)}(A_2,B_2)+\sigma_{(D,S)}(A_1,B_1)$.

Wissen
$\sigma_{(D,S)}:\mathbb{Q}^c\mapsto\mathbb{Q}^c\ (Z,T)\mapsto\sigma_{(D,S)}(Z,T)=\sigma_{(D,S)}(A,B)-\sigma_{(D,S)}(A_1,B_1)=(A,B)-(A_1,B_1)$ mit $(A,B),(A_1,B_1)\in(\mathbb{Q}^c)^{\geq}$ ist wohldefiniert (8.13)
Auch nachfolgend gilt die Grundvoraussetzung: $(D,S),(A,B)\geq 0$
[Heiko: Nachfolgendes Lemma ergab in der VL Probleme - diese Mitschrift sollte hier eigentlich alles wichtige zusammengefasst haben.]

Lemma 8.14: $\sigma_{(D,S)}(D_0,S_0)$ konstant, $\sigma_{(D,S)}$ ordnungserhaltender Isomorphismus

(a) $\sigma_{(D_0,S_0)}:\mathbb{Q}^c\mapsto\mathbb{Q}^c$ ist konstant auf (D_0,S_0). ($\surd$)

(b) Sei $(D,S)\neq(D_0,S_0)$: $\sigma_{(D,S)}:\mathbb{Q}^c\mapsto\mathbb{Q}^c$ ist ein ordnungserhaltender Isomorphismus.

Beweis:

- **Homomorphismus**
  $(Z,T),(Z',T')\ \sigma_{(D,S)}((Z,T)+(Z',T'))=\sigma_{(D,S)}(Z,T)+\sigma_{(D,S)}(Z',T')$
  $\left.\begin{array}{l}(Z,T)=(A,B)-(A_1,B_1)\\(Z',T')=(A',B')-(A'_1,B'_1)\end{array}\right\}$ alle >0
- **injektiv**
  Zu Zeigen: $\sigma_{(D,S)}(X,T)=(D_0,S_0)\Rightarrow(X,T)=(D_0,S_0)$
  Sei $\sigma_{(D,S)}(X,T)=(D_0,S_0)$. Es folgt $\sigma_{(D,S)}(-(X,T))=(D_0,S_0)$. Deshalb oBdA $(X,T)\geq(D_0,S_0)$.
  $\sigma_{(D,S)}(X,T)=(D_0,S_0)\Leftrightarrow(X,T)=(D_0,S_0)$ oder $(D,S)=(D_0,S_0)$ [$\lightning$Voraus.]
- **monoton** $(X,T)\leq(Y,Z)\Rightarrow\sigma_{(D,S)}(X,T)\leq\sigma_{(D,S)}(Y,Z)$
  Sei $(A,B)=(Y,Z)-(X,T)\geq(D_0,S_0)$. Dann ist $\sigma_{(D,S)}(A,B)\geq(D_0,S_0)$.
  $\Rightarrow\sigma_{(D,S)}(Y,Z)=\sigma_{(D,S)}(X,T)+\sigma_{(D,S)}(A,B)\geq\sigma_{(D,S)}(X,T)$
- **surjektiv** Sei $(X,T)\in\mathbb{Q}^c$ Gesucht (A,B) mit $\sigma_{(D,S)}(A,B)=(X,T)$
  Äquivalent: $\exists(A,B)$ mit $\sigma_{(D,S)}(A,B)=(X,T)$ und $\exists(A',B')$ mit $\sigma_{(D,S)}(A',B')=-(X,T)$.
  (nämlich: $(A',B')=-(A,B)$)
  Damit oBdA $(X,T)>(D_0,S_0)$. (Beachte: $\sigma_{(D,S)}(D_0,S_0)=(D_0,S_0)$)
  Definiere $B=\{r\in\mathbb{Q}|\exists t\in T:\forall s\in S:r*s>t\}$

Bemerkungen
$B\subseteq\mathbb{Q}^{>}$.
Für $r\in\mathbb{Q}^{>}$ ist $r*S$ eine Oberklasse.
Behauptung B ist Oberklasse.

- $B\neq\emptyset$ Sei $t\in T$. Wähle $x\in D$. Setze $r=\frac{t}{x}$. Sei $s\in S$. Es folgt $rs=t\underbrace{\frac{s}{x}}_{>1}>t$
- $\mathbb{Q}\backslash B\neq\emptyset\ 0\in\mathbb{Q}\backslash B$
- **Sei** $b\in B$, $q>b\Rightarrow q\in B$ Wähle $s\in S$ beliebig. Dann gilt $sq>sb>t$, wobei $t<S*b$ ist.
- B **hat kein kleinstes Element** Sei $b\in B$. Es gibt $t\in T:t<S*b$. Sei $0<t'<t$, $t'\in T$. Dann ist $0<\frac{t'}{t}<1$. Es folgt $\frac{t'}{t}b<b$. $\frac{t'}{t}b\in B$. Sei $s\in S$. $\Rightarrow\frac{t'}{t}*\underbrace{b*s}_{>t}>\frac{t'}{t}t=t'$.

(A,B): Dedekindscher Schnitt mit Oberklasse B.
Behauptung $\sigma_{(D,S)}(A,B)=(X,T)$, d.h. $S*B=T$

"$\subseteq$" trivial.

"$\supseteq$" Sei $t \in T$. Sei $0 < t' < t$, $t' \in T$. Wähle $d \in D$, $s \in S$ mit: $1 < \frac{s}{d} < \frac{t}{t'}$.
Betrachte $\frac{t'}{d}$.
Zu Zeigen: $\frac{t'}{d} \in B$. Sei $x \in S$. $x\frac{t'}{d} = \underbrace{\frac{x}{d}}_{>1} t' > t'$.
$\frac{t'}{d} * S$ ist Oberklasse. $\frac{t'}{d} * s = \frac{s}{d} * t' < \frac{t}{t'}t' = t \Rightarrow t \in \frac{t'}{d} * S \subseteq B * S$

Der nächste logische Schritt ist das Ausdehnen des Zahlbereichs auf negative (D, S), dies ist recht unproblematisch.

Lemma 8.15:

Sei $(D, S) - (D_1, S_1) = (D', S') - (D'_1, S'_1)$. Es folgt
$\forall (X, Y) \in \mathbb{Q}^c : \sigma_{(D,S)}(X, Y) - \sigma_{(D_1,S_1)}(X, Y) = \sigma_{(D',S')}(X, Y) - \sigma_{(D'_1,S'_1)}(X, Y)$
(Anm: (D, S) in Variation ≥ 0, Vergleiche mit Beweis von Lemma 8.13)

Damit: Sei $(Z, T) \in \mathbb{Q}^c$. Schreibe $(Z, T) = (D, S) - (D_1, S_1)$
Definiere $\sigma_{(Z,T)}(X, Y) = \sigma_{(D,S)}(X, Y) - \sigma_{(D_1,S_1)}(X, Y)$. (ist wohldefiniert!)
$\sigma_{(Z,T)}$ ist die Differenz der Homomorphismen $\sigma_{(D,S)}$, $\sigma_{(D_1,S_1)}$ in der Gruppe der Homomorphismen $\mathbb{Q}^c \mapsto \mathbb{Q}^c$.

Normalerweise: G, H abelsche Gruppen. $f, g : G \mapsto H$. $(f + g)(x) = f(x) + g(x)$

Satz 8.16: $(\mathbb{Q}^c, (D_0, S_0), (D_1, S_1), +, -, \sigma, ()^{-1})$ bildet einen Körper

Mit $\mathbb{Q}^c \times \mathbb{Q}^c \mapsto \mathbb{Q}^c$: $((D, S), (A, B)) \mapsto \sigma_{(D,S)}(A, B)$ als Multiplikation ist $\mathbb{Q}^c$ ein total geordneter Körper. Die Multiplikation von $\mathbb{Q}^c$ kann auf $\mathbb{Q}$ eingeschränkt werden, dabei ergibt sich die dort bereits vorhandene Multiplikation.

Wir wissen bereits viel vom Behaupteten, nachfolgend kommen die restlichen Schritte. Hierbei ist die Reihenfolge durchaus wichtig. Standardverfahren für die Behandlung von negativen Zahlen ist die Darstellung als Differenz. Dadurch bekommt man "oBdA"s, was eine Vereinfachung zur Folge hat.
Der Beweis der Assoziativität ist an der Stelle mühsam, manchmal ist er aber auch einfacher als der Beweis der Kommutativität.
ACHTUNG: Nachfolgend sind die (D_x, S_x) (Beachte den Index x) nicht immer als Dedekind'scher Schnitt der rationalen Zahl x zu werten. Bitte also mit Vorsicht lesen.

Beweis:

- $*$ **kommutativ**
  $(D, S) = (X, Y) - (X_1, Y_1)$,$(A, B) = (U, V) - (U_1, V_1)$ (alle $\geq (D_0, S_0)$)

$$\begin{aligned}
\sigma_{(D,S)}(A, B) &= \sigma_{(X,Y)}(A, B) - \sigma_{(X_1,Y_1)}(A, B) \\
&= \sigma_{(X,Y)}(U, V) - \sigma_{(X,Y)}(U_1, V_1) - \sigma_{(X_1,Y_1)}(U, V) + \sigma_{(X_1,Y_1)}(U_1, V_1) \\
&= \sigma_{(U,V)}(X, Y) - \sigma_{(U_1,V_1)}(X, Y) - \sigma_{(U,V)}(X_1, Y_1) + \sigma_{(U_1,V_1)}(X_1, Y_1) \\
&= \sigma_{(A,B)}(X, Y) - \sigma_{(A,B)}(X_1, Y_1) \\
&= \sigma_{(A,B)}(D, S)
\end{aligned}$$

- $*$ **distributiv über** $+$
  Mult. von Links: $\sigma_{(D,S)}((A, B) + (A_1, B_1)) \underbrace{=}_{(s.u.)} \sigma_{(D,S)}(A, B) + \sigma_{(D,S)}(A_1, B_1)$
  $\sigma_{(D,S)}$ ist Homomorphismus bezüglich $+$
- $*$ **assoziativ** $\sigma_{(A,B)}(\sigma_{(D,S)}(E, F)) \stackrel{?}{=} \sigma_{\sigma_{(A,B)}(D,S)}(E, F)$
  $(E, F) = (E_1, F_1) - (E_2, F_2)$
  $\sigma_{(A,B)}(\sigma_{(D,S)}(E_1, F_1) - \sigma_{(D,S)}(E_2, F_2)) = \sigma_{(A,B)}(\sigma_{(D,S)}(E_1, F_1)) - \sigma_{(A,B)}(\sigma_{(D,S)}(E_2, F_2))$
  $\sigma_{\sigma_{(A,B)}(D,S)}(E_1, F_1) - \sigma_{\sigma_{(A,B)}(D,S)}(E_2, F_2) = ...$
  Es genügt daher: $(E, F) \geq (D_0, S_0)$
  $(D, S) = (D_1, S_1) - (D_2, S_2)$

$\sigma_{(A,B)}(\sigma_{(D_1,S_1)}(E,F)) - \sigma_{(A,B)}(\sigma_{(D_2,S_2)}(E,F)) = \sigma_{\sigma_{(A,B)}(D_1,S_1)}(E,F) - \sigma_{\sigma_{(A,B)}(D_2,S_2)}(E,F)$
Es genügt daher: $(D,S) \geq (D_0,S_0)$

Analog: $(A,B) \geq (D_0,S_0)$

(oBdA also alle $\geq (D_0,S_0)$)
Oberklassen von $\sigma_{(A,B)}(\sigma_{(D,S)}(E,F))$: $B*(S*F)$
Oberklassen von $\sigma_{(A,B)\sigma_{(D,S)}}(E,F)$: $(B*S)*F$

Da Oberklassen Mengen in $\mathbb{Q}$ sind, gilt $B*(S*F) = (B*S)*F$. Damit gilt dies auch für σ.

- **1-Element** $(D_1,S_1) = 1$
$(A,B) = (X,Y) - (X_1,Y_1)$.
$\sigma_{(D_1,S_1)}(A,B) = \sigma_{(D_1,S_1)}(X,Y) - \sigma_{(D_1,S_1)}(X_1,Y_1) \stackrel{?}{=} (X,Y) - (X_1,Y_1) = (A,B)$

oBdA $(A,B) \geq (D_0,S_0)$. Mit Oberklassen: $S_1 * B \stackrel{?}{=} B$

"$\subseteq$" $\underbrace{s \in S_1}_{>1}, b \in B \Rightarrow s*b > b \in B \Rightarrow s*b \in B$

"$\supseteq$" Sei $b \in B$. Es gibt $b' \in B$, $0 < b' < b$. $1 < \frac{b}{b'}$, d.h. $\frac{b}{b'1} \in S_1 \Rightarrow b = \frac{b}{b'} * b' \in S_1 * B$

- **Multiplikativ-Inverses zu** $(A,B) \neq (D_0,S_0)$
Falls $(X,Y)*(-(A,B)) = (D_1,S_1)$: $(-(X,Y))*(A,B) = (D_1,S_1)$. Daher oBdA $(A,B) > (D_0,S_0)$
$\sigma_{(A,B)}$ ist Automorphismus von $\mathbb{Q}^c$ (Lemma 8.14). Insbesondere ist es surjektiv, also
$\exists (X,Y) : \sigma_{(A,B)}(X,Y) = (D_1,S_1)$. Also ist (X,Y) multiplikativ invers zu (A,B).

- **Monotonie** $(A,B) > (D_0,S_0)$
$(X,Y) \leq (Z,T) \Rightarrow \sigma_{(A,B)}(X,Y) \leq \sigma_{(A,B)}(Z,T)$, weil $\sigma_{(A,B)}$ monoton, $(A,B) > (D_0,S_0)$. (Lemma 8.14)

- **Einschränkung der Multiplikation auf** $\mathbb{Q}$
Es gibt zwei verschiedene Möglichkeiten dies zu Zeigen. Erstens zwei nehmen und vergleichen und zweitens wie hier es raffinierter aufzuziehen...

$\mathbb{Q}^c$ hat Charakteristik 0

Beweis:

Sei $(D,S) \neq (D_0,S_0)$, $1 \leq n \in \mathbb{N}$.
$\underbrace{n*(D,S)}_{\text{n-fach addieren}} = (n*D, n*S) \neq (D_0,S_0)$ $(D,S) > (D_0,S_0) \Rightarrow d > 0 \in D \Rightarrow 0 \in D \Rightarrow D_0 \neq D$.

Sei $f : \mathbb{Q} \mapsto \mathbb{Q}^c$ der eindeutig bestimmte Homomorphismus (Lemma 7.14).
Sei $q \in \mathbb{Q}$. Dann ist $f(q) = (D_q,S_q)$!
$f(0) = (D_0,S_0)$, $f(1) = (D_1,S_1)$ wegen Homomorphismus.
Sei $n \in \mathbb{N}$. $f(n*1) = n*(D_1,S_1) = (n*D_1, n*S_1) = (D_n,S_n)$.
$f(-n*1) = -f(n*1) = -(D_n,S_n) = (D_{-n},S_{-n})$.
Sei $q \in \mathbb{Q}$, $q \neq 0$. $q = \frac{k}{l}$, $l > 0$.
$l*f(q) = f(l*q) = f(k) = (D_k,S_k)$
$l*(D_q,S_q) = (D_{l*q},S_{l*q}) = (D_k,S_k)$
$\Rightarrow f(q) = (D_q,S_q)$

Damit: $f[\mathbb{Q}] = \{(D_q,S_q) | q \in \mathbb{Q}\}$ ist Unterkörper von $\mathbb{Q}^c$.

Ab nun verwenden wir die Bezeichnungen/Notationen wie üblich, es wird aber zum Teil vorkommen, dass wir über Dedekind'sche Schnitte reden.
$\mathbb{R} := \mathbb{Q}^c$
reelle Zahlen := Dedekind'sche Schnitte.

Zum Schluss werden wir wie bei den anderen Zahlbereichen auch noch eine Charakteristik für die reellen Zahlen zeigen: $\mathbb{R}$ ist der größte archimedische Körper/Gruppe.

Hans Hahn[9] (* 27. September 1879 in Wien, Tod: 24. Juli 1934 in Wien) war ein österreichischer Mathematiker und Philosoph, der vor allem für den Satz von Hahn-Banach bekannt ist.

[9] http://de.wikipedia.org/wiki/Hans_Hahn

Satz 8.17: Hahn'scher Einbettungssatz

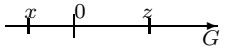
(a) (additive Version) G abelsche Gruppe, archimedisch total geordnet. Dann gibt es $f : G \mapsto (\mathbb{R}, +)$ injektiven, monotonen Homomorphismus. $\Rightarrow G$ Untergruppe von $\mathbb{R}$

Ist $g : G \mapsto (\mathbb{R}, +)$ ein weiterer solcher Homomorphismus, so gibt es genau eine reelle Zahl $r > 0$ mit $g(x) = r * f(x)$, $x \in G$.

(b) (multiplikative Version) R archimedisch total geordneter Ring mit 1.
$\exists! f : \mathbb{R} \mapsto \mathbb{R}$ Homomorphismus von Ringen mit 1.

Der Beweis ist relativ ausführlich, Teil b wird auf Teil a zurückgeführt.

Beweis: (a)
Falls $G = \{0\}$: Es gibt genau ein Homomorphismus. $G \mapsto (\mathbb{R}, +)$. Sei jetzt $G \neq \{0\}$.
Wähle $z \in G$, $z > 0$. (Anm: Damit gilt $-z \in G$)
Sei $x \in G$ beliebig. Für $q \in \mathbb{Q}$, $q = \frac{k}{l}$:



$q \in D_X$, falls $k * z < l * x$
$q \in S_X$, falls $k * z > l * x$
$\Rightarrow \frac{k}{l} > x$, aber es wird keine Multiplikation verwendet! Im Nachfolgenden müssen wir beweisen, dass dies nicht abhängig von der Darstellung als rationale Zahl ist.
Erinnerung: $\frac{k}{l} = \frac{k}{l} \Leftrightarrow kl' = k'l$

Behauptung: $(\frac{k}{l} = \frac{k'}{l'}) \Rightarrow (k'z < l'x \Leftrightarrow kz < lx)$
Es genügt die Replikation zu zeigen:
$kz < lx \Rightarrow l'kz < l'lx \Leftrightarrow k'lz < l'lx \Rightarrow k'z < l'x$
Sei $y \in G$.
1. Fall: $y > 0 \Rightarrow \exists N \in \mathbb{N}_1 : y < Nz$ (Archimedizität)
2. Fall: $y \leq 0 \Rightarrow y < 1 * z$
Also $\exists N \in \mathbb{N}_1 : y < Nz$

Behauptung: $\exists M \in \mathbb{Z} : Mz < y$
Gezeigt: $\exists M \in \mathbb{N}_1 : -y < Mz$
$\Rightarrow (-M) * z < y$

Behauptung: (D_x, S_x) **Dedekind'scher Schnitt**

- $D_x \neq \emptyset$ Sei $M \in \mathbb{Z}$: $Mz < x \Rightarrow M \in D_x$
- $S_x \neq \emptyset$ Sei $N \in \mathbb{N}_1$: $x < Nz \Rightarrow N \in S_x$
- $D_x \cap S_x = \emptyset$ Annahme $\frac{k}{l} \in D_x \cap S_x$. Es folgt $k * z < l * x \wedge k * z > l * x$ ↯
- $|\mathbb{Q} \backslash (D_x \cup S_x)| \leq 1$ Seien $\frac{k}{l}, \frac{k'}{l'} \notin D_x$, $\frac{k}{l} < \frac{k'}{l'}$. Behauptung: $\frac{k'}{l'} \in S_x$.
  $k * z \geq l * x \Rightarrow k * l' * z \geq l' * l * x$, $k * l' < k' * l$.
  $\Rightarrow k' * l * z > k * l' * z \geq l' * l * x$
  $\Rightarrow l' * x < k' * z \Rightarrow \frac{k'}{l'} \in S_x$
- $\frac{k'}{l'} < \frac{k}{l} \in D_x \Rightarrow \frac{k'}{l'} \in D_x$, **analog für** S_x
  Ab hier würde es genügen, nur über S_x zu reden. Von Anfang an geht dies nicht, da wir bereits vorher beides definieren - man also zeigen muss, dass das jeweils andere genau so ausschaut.
- D_x **hat kein größtes Element** Sei $\frac{k}{l} \in D_x$, d.h. $k * z < l * x$
  $l * x - k * z > 0$ Wegen Archimedizität: $\exists N \in \mathbb{N}_1 : N(l * x - k * z) > z$
  d.h. $Nlx - (Nk + 1)z > 0 \Rightarrow \frac{Nk+1}{Nl} \in D_x$, $\frac{k}{l} < \frac{Nk+1}{Nl}$

Definiere $f : G \mapsto \mathbb{R} : x \mapsto (D_x, S_x)$
$z \mapsto (D_1, S_1)$ (z wird nach 1 abgebildet).
Wahl von z beeinflußt welchen Homomorphismus man bekommt.

- f **monoton**
  $x < y$ in G. Zu Zeigen: $D_x \underbrace{\subset}_{\text{wg. Inj}} D_y$

  Beweis:
  Sei $\frac{k}{l} \in D_x$, d.h. $kz < lx < ly = \frac{k}{l} \in D_y$

- **f Homomorphismus**
  $x, y \in G \Rightarrow f(x+y) = f(x) + f(y)$
  Zu Zeigen: $D_{x+y} = D_x + D_y$

  "$\supseteq$" $\frac{k}{l} \in D_x$, $\frac{k'}{l'} \in D_y$. $\left.\begin{array}{l} k*z < l*x \\ k'*z < l'*y \end{array}\right\} (kl' + k'l)z < ll'(x+y)$ (klar)

  "$\subseteq$" Sei $\frac{k}{l} \in D_{x+y}$, d.h. $kz < l(x+y)$
  Wähle $\frac{k'}{l'} \in D_{x+y}$, $\frac{k}{l} < \frac{k'}{l'}$. Sei $\frac{r}{s} \in D_x$ mit $\frac{r}{s} + (\frac{k'}{l'} - \frac{k}{l}) \in S_x$ (D,S beliebig nahe)
  Dann gilt $\frac{k}{l} - \frac{r}{s} \in D_y$.
  $k'z < l'(x+y) \Rightarrow k'slz < l'slx + l'sly$
  $\frac{ll'r + k'sl - kl's}{sll'} \in S_x$
  d.h. $(ll'r + k'sl - kl's)z > sl'lx$
  $k'slz - (ll'r + k'sl - kl's)z < l'sly$ (hat kein x mehr $\Rightarrow$ Element von D_y)
  $(k* \not{l}' * s - l* \not{l}' * r) * z < \not{l}' * s * l * g$
  $\Rightarrow \frac{k}{l} - \frac{r}{s} = \frac{ks - lr}{sl} \in D_y$

- **f injektiv**
  Sei $f(x) = (D_0, S_0) \Rightarrow f(-x) = (D_0, S_0) \Rightarrow$ oBdA$x \geq 0$.
  Zu Zeigen: $x = 0$
  Annahme $x > 0$: Wegen der Archimedizität gilt: $\exists N \in \mathbb{N}_1 : z < Nx$. Damit folgt $0 < \frac{1}{N} \in D_x \Rightarrow D_x \neq D_0$,
  d.h. $\lightning f(x) = (D_0, S_0)$

- **f eindeutig**
  Sei $g : G \mapsto \mathbb{R}$ ein weiterer Homomorphismus. Wegen Injektivitität und Monotonie folgt $r = g(z) > 0$ in $\mathbb{R}$.
  Sei $x \in G$, sei $\frac{k}{l} \in D_x$, $\frac{p}{q} \in S_x$. Es folgt $\frac{k}{l} < f(x) < \frac{p}{q} \Rightarrow r\frac{k}{l} < rf(x) < r\frac{p}{q}$.
  $\frac{k}{l} \in D_x \Rightarrow kz < lx \Rightarrow kg(z) < lg(x)$
  $\frac{p}{q} \in S_x \Rightarrow pz > qx \Rightarrow pg(z) > pg(x)$
  $\Rightarrow \frac{k}{l}r < g(x) < \frac{p}{q}r$.
  Weil $\frac{k}{l}$, $\frac{p}{q}$ beliebig nahe kommen und beide Ungleich gleich sind und gelten folgt:
  $g(x) = inf\{r\frac{p}{q} | \frac{p}{q} \in S_x\} = rf(x)$

Beweis: (b)

1 muss auf 1 abgebildet werden, eine beliebige positive Zahl kann als "Einheit" verwendet werden. Es gibt "viele" Möglichkeiten die Abbildung zu definieren...

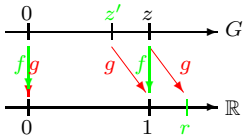


Abbildung $f : R \mapsto \mathbb{R}$ entsprechend (a) mit $f(1) = 1$. Dies ist ein injektiver, monotoner
Additions-Homomorphismus mit $f(1) = 1$ (und damit Eindeutig, da $g(1) = r * f(1) = 1$).
Noch zu Zeigen: Seien $x, y \in R$. Dann gilt $f(x*y) = f(x)*f(y)$ (f ist ein Multiplikations-Homomorphismus.)
$x = x_1 - x_2$, $y = y_1 - y_2$ mit $x_1, x_2, y_1, y_2 > 0$ (Dies geht gut, weil totalgeordnet.)
Falls die Homomorphieeigenschaft für Produkte von positiven Elementen gilt, folgert sich daraus:

$$\begin{aligned} f(x*y) &= f(x_1*y_1) + f(x_2*y_2) - f(x_1*y_2) - f(x_2*y_1) \\ &= f(x_1)*f(y_1) + f(x_2)*f(y_2) - f(x_1)*f(y_2) - f(x_2)*f(y_1) \\ &= (f(x_1) - f(x_2))*(f(y_1) - f(y_2)) \\ &= f(x)*f(y) \end{aligned}$$

Der Rest muss über die Dedekind'schen Schnitte laufen.
Ab jetzt gilt $x, y > 0$. Zu Zeigen ist: $(D_x, S_x) * (D_y, S_y) = (D_{x*y}, S_{x*y})$.
Seien $\frac{k}{l} \in S_x$, $\frac{p}{q} \in S_y$. Es folgt $k*1 > l*x$, $p*1 > q*y \Rightarrow k*p*1 > l*q*x*y \Rightarrow \frac{k*p}{l*q} \in S_{x*y}$.
Seien $0 < \frac{k}{l} \in D_x$, $0 < \frac{p}{q} \in D_y$. Es folgt $k*1 < l*x$, $p*1 < q*y \Rightarrow k*p*1 < l*q*x*y \Rightarrow \frac{k*p}{l*q} \in D_{x*y}$.
Damit sind die zwei Schnitte gleich.

Mit den reellen Zahlen kann noch viel gemacht werden, hier aber wollen wir sie nicht weiterführen. Praktisch sind wir mit diesem Kapitel dort angekommen, wo man in der Analysis beginnt. Die hier erwähnten Eigenschaften und Definitionen setzt man dort zum Teil stillschweigend oder überfliegend voraus.
Damit ist das Kapitel der reellen Zahlen abgeschlossen.

2.9 Restklassenringe der ganzen Zahlen

Einführung

Die Restklassenringe der ganzen Zahlen spielen in der Anwendung eine bedeutende Rolle, da Rechnungen in Ihnen normalerweise explizit berechenbar sind. Wir führen hier nur einige einfache Rechenoperationen ein. Sehr wahrscheinlich ist dies das letzte Kapitel in diesem Teil. In Algebra werden die Restklassenringe viel allgemeiner eingeführt, sie basieren auf irgendwelchen Ringen und sind dort Ideale (...).
Hier bleiben wir aber ganz eng bei den ganzen Zahlen, wir führen Äquivalenzklassen ein und definieren dort dann die Rechenoperationen.
Gegeben seien immer $\mathbb{Z}$ und $2 \leq N \in \mathbb{N}$.

Satz 9.1: Äquivalenzrelation/Repräsentantensystem

Relation auf $\mathbb{Z}$: $z \sim t$, falls $N \mid z - t$ (weil $N * c = z * t$)

- Dies ist eine Äquivalenzrelation
- $\{0, ..., N-1\}$ sind ein Repräsentantensystem ($\Rightarrow$ endlich, mit N Elementen)
- z liegt in der Äquivalenzklasse von $r \in \{0, ..., N-1\}$ genau dann, wenn r der $\underbrace{\text{Divisionsrest}}_{\Rightarrow \text{“Restklasse”}}$ von z bei Division durch N ist.

Beweis:

- **Reflexiv**
  $N \mid z - z = 0 \surd$
- **Symmetrisch**
  $N \mid z - t \Leftrightarrow N \mid t - z \surd$
- **Transitiv**
  $x \sim y$, $y \sim z$
  $x - y = k * N$, $y - z = l * N \Rightarrow x - z = (x - y) + (y - z) = (k + l) * N \surd$
- **Repräsentanten**

  (a) Seien $i, j \in \{0, ..., N-1\}$ mit $i \sim j$. oBdA $i < j$.
  Behauptung: $i = j$
  $0 \leq j - i = k * N$
  Annahme $k > 0 : N > j \geq j - i > N$ ↯
  Es folgt: $i = j$

  (b) Sei $z \in \mathbb{Z}$. Behauptung: $\exists r \in \{0, ..., N-1\} : z \sim r$
  Dividiere z mit Rest durch N: $z = q * N + r$, $r \in \{0, ..., N - q\}$ $\surd$

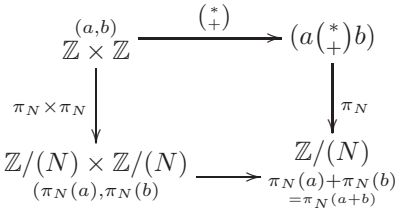
Unsere Aufgabe nun ist es die Rechenoperationen + und * zu definieren, so daß ein Ring entsteht. Dabei haben wir die Vorgabe, daß der Zusammenhang zu $\rightarrow \mathbb{N}/\mathbb{Z}$ bestehen bleibt.

Notation

Menge der (Rest-)Äquivalenzklassen: $\mathbb{Z}/(N)$ “$\mathbb{Z}$ modulo N”.
$\pi_N : \mathbb{Z} \mapsto \mathbb{Z}/(N)$ ist die kanonische Abbildung $\pi_N : z \mapsto \overline{z} = \underbrace{z + (N)}_{\text{für versch. Modulo}}$ Äquivalenzklassen von z
(N): alle Vielfachen von N. $:= \{k * N | k \in \mathbb{Z}\}$
Ideal in $\mathbb{Z}$: $z + (N) = \{z + k * N | k \in \mathbb{Z}\} = [z]_\sim$ ist Äquivalenzklasse von z.
$[z \sim t = z - t = kN \Rightarrow t = z + (-k) * N]$

$\alpha, \beta, \ldots$ (griechische Buchstaben) werden für Elemente benutzt.

Ziel: $+, *$ auf $\mathbb{Z}/(N)$ so zu definieren, so daß $\mathbb{Z}/N$ Ring (mit 1) und π_N Homomorphismus ist.
$\pi_N(a+b) = \pi_N(a) + \pi_N(b)$.
Zur Verdeutlichung das Diagramm:



Lemma 9.2: Wohldefiniertheit (!)

Seien $\alpha, \beta \in \mathbb{Z}/(N)$
$a, a' \in \alpha$; $b, b' \in \beta$
$\Rightarrow a+b \sim a'+b' \wedge a*b \sim a'*b'$

Beweis:
$a - a' = k*N$, $b - b' = l*N$
$\Rightarrow (a+b) - (a'+b') = (k+l)N$
$ab - a'b' = ab - a'b + a'b - a'b' = (a-a')b + a'(b-b') = bkN + a'lN = (bk + a'l) * N$

Definiere Verknüpfung auf $\mathbb{Z}/(N)$
$+ : \overline{a} + \overline{b} = \overline{a+b}$
$* : \overline{a} * \overline{b} = \overline{a*b}$

Satz 9.3: $\mathbb{Z}/(N)$ ist kommutativer Ring mit 1 mit $\mathrm{Char}(\mathbb{Z}/(N)) = N$

- $\mathbb{Z}/(N)$ ist kommutativer Ring mit 1.
- $\pi_N : \mathbb{Z} \mapsto \mathbb{Z}/(N)$ ist Homomorphismus.
- $\mathrm{Char}(\mathbb{Z}/(N)) = N$
- $\mathbb{Z}/(N)$ ist Körper $\Leftrightarrow$ N Primzahl.

Beweis:
(z.T. exemplarisch)

- **π_N Homomorphismus**
  $\pi_N(a\binom{+}{*}b) = \overline{a\binom{+}{*}b} = \overline{a}\binom{+}{*}\overline{b} = \pi_N(a)\binom{+}{*}\pi_N(b)$
  $\pi_N(1) = 1$
- **$+$ assoziativ, $+$ kommutativ, 0-Element: $\overline{0}$, inverses zu $\overline{a}$: $-\overline{a}$**
  surjektiver Homomorphismus $\Rightarrow$ Ringeigenschaften werden übertragen.
- *** assoziativ, * kommutativ**
- *** distributiv über $+$** (stellvertretend bewiesen)
  $\overline{a}(\overline{b}+\overline{c}) = \overline{a} * \overline{b+c}) = \overline{a(b+c)} = \overline{a*b + a*c} = \overline{a*b} + \overline{a*c} = \overline{a}*\overline{b} + \overline{a}*\overline{c}$
- **1-Element**
  $\overline{1} * \overline{b} = \overline{1*b} = \overline{b}$
- $\mathrm{Char}(\mathbb{Z}/(N) = N$
  $\mathrm{Char}(\mathbb{Z}/(N)) = |\,\mathrm{Bild}(f)| = |\,\mathrm{Bild}(\pi_N)| \overset{\pi_N surj.}{=} N$
- **Körper $\Leftrightarrow$ N prim**

  "$\Rightarrow$" Charakteristik Primzahl (0 geht nicht)

"⇐" Ginge besser (und konstrukiver) mit dem Euklidischen Algorithmus, dieser wurde aber hier nicht vorgestellt.

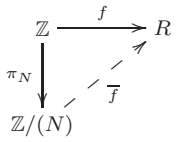
Sei $\overline{a} \in \mathbb{Z}/(N)$, $\overline{a} \neq \overline{0}$.
$\hat{\overline{a}} : \mathbb{Z}/(N) \mapsto \mathbb{Z}(N) : \overline{x} \mapsto \overline{a} * \overline{x}$ Homomorphismus bezüglich $+$
Eigentlich brauchen wir Surjektivität, in diesem Fall reicht es die Injektivität zu beweisen, da bei Endlichkeit(?) diese beiden Äquivalent sind.
Sei $\overline{ax} = \overline{ax} = \overline{0}$, d.h. $ax \sim 0$, d.h. $N \mod ax$. Da N Primzahl gilt $\underbrace{N \mod a}_{\Rightarrow \overline{a}=\overline{0}\ \lightning}$ oder $\underbrace{N \mod x}_{\Rightarrow \overline{x}=\overline{0}}$. Damit wird nur 0 auf $\overline{0}$ abgebildet, damit ist es injektiv.
Also $\text{Kern}(\hat{\overline{a}}) = \{\overline{0}\}$, $\hat{\overline{a}}$ injektiv. Da $\mathbb{Z}/(N)$ endlich, ist $\hat{\overline{a}}$ auch surjektiv.
Insbesondere $\exists \overline{x} \in \mathbb{Z}/(N) : \overline{ax} = \hat{\overline{a}}(\overline{x}) = \overline{1}$

Satz 9.4: Abbildungen zwischen Restklassensystemen

R kommutativer Ring mit 1.
Dann gibt es höchstens einen Homomorphismus $\mathbb{Z}/(N) \mapsto R$
Es gibt (genau) einen Homomorphismus $\Leftrightarrow \text{Char}(R) \mod N$

Beweis:

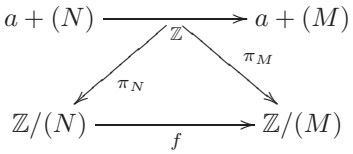
- **Eindeutigkeit**
  $f, g : \mathbb{Z}/(N) \mapsto R$ Homomorphismus.
  $\Rightarrow f \circ \pi_N, g \circ \pi_N : \mathbb{Z} \mapsto R$ Homomorphismen
  $\Rightarrow f \circ \pi_N = g \circ \pi_N$, da π_N surjektiv folgt $f = g$.
  (von $\mathbb{Z}$ gibt es nur einen Homomorphismus in Ring mit 1)
- **Existenz**
  Setze $\text{Char}(R) = p$. Gelte $p \mod N$. $f : \mathbb{Z} \mapsto R$ sei der eindeutig bestimmte Homomorphismus. Definiere $\overline{f} : \mathbb{Z}/(N) \mapsto R : \overline{f}(\overline{a}) = f(a)$.



- $\overline{f}$ **wohldefiniert** Sei $\overline{a} = \overline{a'}$. Zu Zeigen: $f(a) = f(a')$.
  $a - a' = k * N$, $N = l * p$. $f(a) - f(a') = f(a - a') = f(k * n * 1) = f * N * \underbrace{1}_{\text{in } R} = k * l * \underbrace{(p * 1)}_{=0} = 0$
  $\overline{f}(\overline{a}(\overset{+}{*})\overline{b}) = \overline{f}(\overline{a(\overset{+}{*})b}) = f(a(\overset{+}{*})b) = \overline{f}(\overline{a}(\overset{+}{*})\overline{f}(\overline{b})$
  $\overline{f}(\overline{1}) = f(1) = 1$
- **2. Teil** Es gebe einen Homomorphismus $f : \mathbb{Z}/(N) \mapsto R$.
  $f \circ \pi_N : \mathbb{Z} \mapsto R$ ist der eindeutig bestimmte Homomorphismus von $\mathbb{Z}$ nach R.
  $\text{Char}(R) = |\,\text{Bild}(f \circ \pi_N)| = |\,\text{Bild}(f)| \leq |\mathbb{Z}/(N)| = N$
  $p = \text{Char}(R) \neq 0$. Division mit Rest: $N = qp + r$. Zu Zeigen: $r = 0$.
  $(f \circ \pi_N)(r) = r * 1 = (N - qp) * 1 = \underbrace{N * 1}_{\substack{=0 \\ (1)}} - q * \underbrace{p * 1}_{\substack{=0 \\ (2)}} = 0$
  (1): $N * 1 = (f \circ \pi_N)(N) = f(\overline{N}) = f(\overline{0}) = 0$
  (2): $\text{Char}(R) = p$
  $0 \leq r < p$, wegen Minimalität von p gilt: $r = 0$

$M \mod N$, $\mathbb{Z}/(N) \mapsto \mathbb{Z}/(M)$ Homomorphismus

$M \mod N$ Was tut dieser Homomorphismus? Notation: $z + (N)$



ist kommutativ wegen Eindeutigkeit und Homomorphieeigenschaften.
$f(a+(N)) = f \circ \pi_N(a) = \pi_M(a) = a+(M)$

Seien $a, b \in \mathbb{N}_1$. $G := \{c \in \mathbb{N}_1 | c \mid a \wedge c \mid b\}$ Menge der gemeinsamen Teiler. Weil $c \leq \min(a,b)$ ist G endlich.
Weil $1 \in G$ ist G nicht-leer. Damit enthält G ein größtes Element:
Der größte gemeinsame Teiler $=:$ ggT(a,b).
Wenn a, b Teilerfremd sind, gilt $G = \{1\}$.

Satz 9.5: chinesischer Restsatz (!)

Sei $2 \leq N = KL$, ggT$(K,L) = 1$.
Dann gelten

- $\exists x, y \in \mathbb{Z} : 1 = xK + yL$
- Die kanonische Abbildung $\phi : \mathbb{Z}/(N) \mapsto \mathbb{Z}/(N) \times \mathbb{Z}/(N)$:
  $a+(N) \mapsto (a+(K), a+(L))$ ist Isomorphismus.

Dies bedeutet es ist egal, wo ich rechne. Gleichungen kann ich z.B. statt in $\mathbb{Z}/(N)$ mit i.A. deutlich weniger Aufwand in $\mathbb{Z}/(K)$ und $\mathbb{Z}/(L)$ lösen und die Ergebnisse mit einem logischen und verknüpfen.

Beweis: (b), unter Vorraussetzung (a)
$|\mathbb{Z}/(N)| = N = |\mathbb{Z}/(K) \times \mathbb{Z}/(L)| = |\mathbb{Z}/(K)| * |\mathbb{Z}/(L)| = K * L = N$
Daher genügt es zu zeigen: Injektiv oder Surjektiv
Beweis der Surjektivität: Wir suchen einen Repräsentanten zu $\mathbb{Z}/(K) \times \mathbb{Z}/(L) \ni (u+(K), v+(L))$
$= u(q+(K), 0+(L)) + v(0+(K), 1+(L))$.
$\phi((1-xK)+(N)) = ((1-xK)+(K), yL+(L)) = (1+(K), 0+(L))$
$\phi((1-yL)+(N)) = (xK+(K), (1-yL)+(L)) = (0+(K), 1+(L))$
$\phi(u(1-xK)+v(1-yL)) = (u+(K), v+(L))$ $\surd$

$\phi^{-1}(u+(K), v+(L)) = (u(1-xK)+v(1-yL))+(N)$ mit $1 = xK + yL$.
(Wichtig) Damit hat man mit oben eine explizite (Um-)Rechnung!

Beweis (a): Allgemeiner durch folgenden Satz mit $w = 1$.

Satz 9.6: Charakterisierung des ggT

Seien $u, v \in \mathbb{N}_1$. Es gibt eine größte natürliche Zahl $g \in \mathbb{N}$, welche u, v beide teilt. (größter gemeinsamer Teiler, $ggT(u,v)$) Sei $w \in \mathbb{N}_1$. Dann gilt:
$w = g \Leftrightarrow \{xu + yv | x, y \in \mathbb{Z}\} = \mathbb{Z} * w$.

Beweis:
(Reihenfolge wichtig!)

"$\Rightarrow$" $\exists a, b \in \mathbb{Z} : u = aw \wedge v = bw$. Seien $x, y \in \mathbb{Z} \Rightarrow xu + yv = (xa + yb)w$. ($\subseteq$)
Setze vorraus: $w = xu + yv$; $x, y \in \mathbb{Z}$. Sei $t \in \mathbb{Z} \Rightarrow tw = txu + tyv$. ($\supseteq$)
Zu Zeigen: $\exists x, y \in \mathbb{Z} : w = xu + yv$.
Wegen $w = g$: a, b haben nur 1 als gemeinsamer Teiler. (Sei $a = a_1 * c$; $b = b_1 * c$. Es folgt $u = a_1(cw)$, $v = b_1(cw)$. d.h. cw gemeinsamer Teiler, $cw > w$. $w = ggT(u,v) \Rightarrow c = 1$)
Falls $1 = xa + yb : w = x(aw) + y(bw) = xu + yv$.
Also oBdA: $1 = ggT(u,v)$.
Nun mit Induktion:
$M = \{n \in \mathbb{N} | n = 0 \vee (n > 0 \wedge$ für $1 \leq r, s \leq n$, $1 = ggT(r,s)$ gibt es Darstellung $1 = xr + ys\}$.

Beweis:

$0 \in M$ $(\surd)$

$1 \in M$ $1 \leq r, s \leq 1 \Rightarrow r = s = 1 \Rightarrow 1 = 1r + 0s$ $(\surd)$

$n \in M \Rightarrow n + 1 \in M$

- Fall $r = 1$: $1 = 1r + 0s$
- Fall $s = 1$: $1 = 0r + 1s$
- Fall $r = s$: $\lightning$(r, s teilerfremd)
- Fall $r < s \leq n$ Induktion $(\surd)$
- Fall $s < r \leq n$ Induktion $(\surd)$
- Fall $1 < r < s = n + 1$, r, s teilerfremd.
  Division mit Rest durch r: $s = qr + t$, $0 \leq t < r$.
  Annahme: $t = 0$: $s = qr \Rightarrow 1 < r = ggT(r, s)$ $\lightning$
  Also $t \neq 0$. Wenn p gemeinsamer Teiler von r, t ist: $r = r_1 p$; $t = t_1 p \Rightarrow s = (qr_1 + t_1) * p$ d.h. p gemeinsamer Teiler von r, s, also $p = 1$.
  Also: $1 \leq t < r < n + 1$ Die Induktion gibt $1 = xr + yt = xr + y(s - qr) = (x - qy)r + ys$ $(surd)$
- Fall $1 < s < r = n + 1$, r, s teilerfremd: Analog.

"$\Leftarrow$" Wegen $\Rightarrow$ gilt: $\mathbb{Z} * g = \{xu + yv | x, y \in \mathbb{Z}\}$ Nach Voraussetzung: $\mathbb{Z} * w = \{xu + yv | x, y \in \mathbb{Z}\}$
$\Rightarrow \mathbb{Z} * g = \mathbb{Z} * w$ Insbesondere $w = w_1 * g$, $g = g_1 * w$.
$\Rightarrow w = (w_1 * g_1)w \Rightarrow w_1 * g_1 = 1$
$\underbrace{\Rightarrow}_{w_1, g_1 > 0}$ $w_1 = g_1 = 1$

Erinnerung: Was bedeutet das für den chinesischen Restsatz?
$\mathbb{Z}/(N) \overset{\cong}{\mapsto} \mathbb{Z}/(K) \times \mathbb{Z}/(L)$ K, L teilerfremd.
$a + (N) \mapsto (a + (K), a + (L))$ $q = x * K + y * L$
$(yLb + xKc) + (N) \leftarrow (b + (K), c + (L))$

$1 \leq u, v \in \mathbb{N}$, $g = ggT(u, v)$
$u = qv + r \Rightarrow g = ggT(v, r)$

$a_0, a_1 > a_2 > a_3 > ... > a_k = 0$
$a_i = q_i * a_{i+1} + a_{i+2}$, $0 \leq a_{i+2} < a_{i+1}$
$g = ggT(a_0, a_1) = ... = ggT(a_{k-2}, a_{k-1}) = a_{k-1}$
$a_{k-2} = q_{k-2} * a_{k-1} + a_k \Rightarrow a_{k-2} = q_{k-2} * a_{k-1}$
$a_{k-3} = q_{k-3} * a_{k-2} + \overbrace{a_{k-1}}^{=g}$
$\Rightarrow g = 1 * a_{k-3} - q_{k-3} * a_{k-2}$
...
$\Rightarrow g = x_i * a_i + y_i * a_{i+2}$ $a_{i-1} = q_{i-1} * a_i + a_{i+1}$
$\Rightarrow g = x_i * a_i + y_i * (a_{i-1} - q_{i-1} * a_i)$
$\Rightarrow g = y_i * a_{i-1} + (x_i - y_i * q_{i-1}) * a_i$
Dies hat eine ziemlich geringe Komplexität.
Beispiel: $g = \text{ggT}(7896, 1593)$

$$\begin{aligned} 7896 &= 4 * 1593 + 1524 \\ 1593 &= 1 * 1524 + 69 \\ 1524 &= 22 * 69 + 6 \\ 69 &= 11 * 6 + 3 \\ 6 &= 2 * 3 + 0 \end{aligned}$$

Durch Rückwärtsentwicklung kann man sich hieraus eine Darstellung der Zahl 3 als Linearkombination von 7896 und 1593 verschaffen:

$$\begin{aligned} 3 &= 1 * 69 - 11 * 6 \\ &= 1 * 69 - 11 * (1524 - 22 * 69) \\ &= 243 * 69 - 11 * 1524 \\ &= 243 * (1 * 1593 - 1 * 1524) - 11 * 1524 \\ &= 243 * 1593 - 254 * 1524 \\ &= 243 * 1593 - 254 * (1 * 7896 - 4 * 1593) \\ &= 1259 * 1593 - 254 * 7896 \end{aligned}$$

Beispiel zum chinesischen Restsatz:
Sei $N = KL$ mit $ggt(K, L) = 1$
$\mathbb{Z}/(N) \overset{\cong}{\mapsto} \mathbb{Z}/(K) \times \mathbb{Z}/(L)$
Leicht zu beweisende Erweiterung des chinesischen Restsatzes:
Falls $N = K_1 * ... * K_r$ paarweise teilerfremd sind:
$\mathbb{Z}/(N) \overset{\cong}{\mapsto} \mathbb{Z}/(K_1) \times ... \times \mathbb{Z}/(K_r)$
Man kann N immer darstellen als $N = p_1^{k_1} * ... * p_r^{k_r}$, wobei $p_1, .., p_r$ Primzahlen sind.
Das heisst es gibt einen Isomorphismus $\mathbb{Z}/(N) \overset{\cong}{\mapsto} \prod_{i=1}^{r} \mathbb{Z}/(p_i^{k_i})$
Da $\mathbb{Z}/(N)$ ein kommutativer unitärer Ring ist folgt das $\mathbb{Z}/(N)^\times$ ein abelsche Gruppe bezüglich der Multiplikation ist.
Da ein Isomorphismus $\mathbb{Z}/(N) \overset{\cong}{\mapsto} \prod_{i=1}^{r} \mathbb{Z}/(p_i^{k_i})$ vorliegt werden Einheiten wieder auf Einheiten abgebildet:
$\mathbb{Z}/(N)^\times \overset{\cong}{\mapsto} \prod_{i=1}^{r} \mathbb{Z}/(p_i^{k_i})^\times$
Zur Erläuterung:
Seien a, b Einheiten eines kommutativen unitären Ringes R_1 und sei f ein Isomorphismus in einen anderen kommutativen unitären Ring R_2, so gilt:
$f(1_{R_1}) = f(1_{R_1} * 1_{R_1}) = f(1_{R_1}) * f(1_{R_1})$
$\Rightarrow f(1_{R_1}) = 1_{R_2}$
(Begründung: $1 = 1 * 1' = 1'$ d.h. es kann in einem kommutativen unitären Ring nur ein Einselement geben)
Aus dieser Überlegung folgt:
$1_{R_2} = f(1_{R_1}) = f(a * b) = f(a) * f(b)$
D.h. ist a eine Einheit in R_1 so ist $f(a)$ Einheit in R_2.
Mit einem analogen Argument zeigt man dass durch f^{-1} jede Einheit in R_2 auf eine Einheit in R_1 abgebildet wird.
Deswegen kann man den allgemeinen Isomorphismus auch auf die Einheiten von Urbild- und Bildring einschränken.
Nun ist es interessant, wieviele Einheiten es in $\mathbb{Z}/(N)$ gibt.

Definition 9.7: Euler'sche φ-Funktion

$\varphi : \mathbb{N}_2 \to \mathbb{N} : N \mapsto |\mathbb{Z}/(N)^\times|$

Korollar 9.8:

Sei $N = KL, 1 = ggT(K, L), 2 \leq K, L$
$\Rightarrow \varphi(N) = \varphi(K) * \varphi(L)$
Begründung:
$|\mathbb{Z}/(N)^\times| = |\mathbb{Z}/(K)^\times \times \mathbb{Z}/(L)^\times| = |\mathbb{Z}/(K)^\times| * |\mathbb{Z}/(L)^\times|$
D.h. $\varphi(N) = \varphi(p_1^{k_1}) * ... * \varphi(p_r^{k_r})$

Satz 9.9:

Sei $1 \leq a < N$. Dann gilt:
$a + (N) \in \mathbb{Z}/(N)^\times \Leftrightarrow 1 = ggT(a, N)$

Beweis:
Sei $g = ggT(a, N) \Rightarrow \exists x, y \in \mathbb{Z} : g = x * a + y * N$
„$\Leftarrow$“

$$\begin{aligned} x*a+y*N+(N) &= 1+(N) \\ x*a+(N) &= 1+(N) \\ x*a+(N) &= (x+(N))*(a+(N)) \end{aligned}$$

„⇒“
Zu $a+(N)$ gibt es nach Voraussetzung $x+(N)$ mit
$1+(N)=(a+(N))*(x+(N))=(a*x)+(N)$
$\Rightarrow 1-ax=y*N$ für ein $y\in\mathbb{Z}$
$\Rightarrow 1=a*x+y*N$
$\Rightarrow 1=ggT(a,N)$
Hinweis: Benutze bei dem letzten Schluss die Richtung „⇐“ des Satzes über die Charakterisierung des ggT.
(Tipp: $1=ax+yN\Rightarrow t=t*(ax+yN)=(ta)x+(ty)N\forall t\in\mathbb{Z}$)

Satz 9.10:

$\varphi(p^r)=(p-1)-p^{r-1}$, p Primzahl, $1\leq r\in\mathbb{N}$

Beweis:
$\mathbb{Z}/(p^r)^\times=\{a+(p^r)|1\leq a<p^r\wedge ggT(a,p^r)=1\}$
Es geht also um die Menge $\{1,...,p^r-1\}$
Betrachtet man zunächst welche Elemente in dieser Menge nicht teilerfremd zu p^r sind so findet man als Antwort die Menge der Vielfachen der Primzahl p bis $p^r-p:\{1*p,2*p,...,(p^{r-1}-1)*p\}$
Also ist $\varphi(p^r)=(p^r-1)-(p^{r-1}-1)=p^r-p^{r-1}=(p-1)*p^{r-1}$
q.e.d.

Beispiel: Nullstellenberechnung von Polynomen in $\mathbb{Z}/(N)$
Sei $P_N\in\mathbb{Z}/(N)[X_1,...,X_r]$
Dann hat das Polynom P_N folgende Gestalt:
$\sum a_{i_1,...,i_r}+(N)*X_1^{i_1}*...*X_r^{i_r}$
Gesucht: $(\alpha_1+(N),...,\alpha_r+(N))$ mit
$\sum a_{i_1,...,i_r}+(N)*(\alpha_1+(N))^{i_1}*...*(\alpha_r+(N))^{i_r}=0$
Der Trick den man heranzieht um dieses Polynom in $\mathbb{Z}/(N)$ zu lösen ist, dass man es in zwei Polynome jeweils eines in $\mathbb{Z}/(K)$ und $\mathbb{Z}/(L)$ aufspaltet und dort jeweils das Nullstellenproblem der neuen Polynome im neuen, kleineren Ring löst. Hat man dort die Lösung so transformiert man diese über den Isomorphismus des chinesischen Restsatzes wieder zurück nach $\mathbb{Z}/(N)$ und erhält so Lösungen des Ausgangspolynoms.
Die zwei neuen Polynome lauten:
$P_K=\sum(a_{i_1,...,i_r}+(K))*X_1^{i_1}*...*X_r^{i_r}$
P_L definiert man analog.
$(\beta_1+(K),...,\beta_r*(K))$ sei Nullstelle von P_K und $(\gamma_1+(L),...,\gamma_r*(L))$ sei Nullstelle von P_L.
$(\alpha_1+(N),...,\alpha_r*(N))$ ist Nullstelle von P_N falls
$\alpha_i+(N)\mapsto(\beta_i+(K),\gamma_i+(L))$

Beispiel: Zahlenbeispiel zur Nullstellenberechnung von Polynomen in $\mathbb{Z}/(N)$
Sei $N=825=3*5^2*11$ also $K=3,L=5^2,M=11$.
Wir verwenden also eine Form der Erweiterung des chinesischen Restsatzes:
$\mathbb{Z}/(N)\overset{\cong}{\mapsto}\mathbb{Z}/(K)\times\mathbb{Z}/(L)\times\mathbb{Z}/(M)$
Das Polynom das wir betrachten werden ist ein Polynom in $\mathbb{Z}/(825)[X]$
Wir suchen die Nullstellen folgender Gleichung: $X^2+X+1=0$
Wir wollen die Lösungen in $\mathbb{Z}/(825)$ finden.
Die Brute-Force Methode wäre es jetzt alle 825 Zahlen einzusetzen und auszuprobieren bei welcher Einsetzung 0 herauskommt. Das mag für kleine Zahlen praktikabel sein(wenn man denn gerade einen Rechner parat hat, ansonsten nämlich auch nicht - viel Spass beim Rechnen). Aber für große N ist es effizienter auch auf Rechenmaschinen solche Gleichungen mit Hilfe des chinesischen Restsatzes wie folgt zu vereinfachen:
1. Schritt: Suche Lösungen in $\mathbb{Z}/(3)$.
Da kein Koeffizient des Polynoms größer oder gleich 3 ist muss keine Anpassung dieser modulo 3 vorgenommen werden. Wir rechnen das Polynom für die drei Elemente des kommutativen

unitären Ringes aus:
$0^2 + 0 + 1 = 1$
$1^2 + 1 + 1 = 3$ 2 ist also eine Lösung in $\mathbb{Z}/(3)$!
$2^2 + 2 + 1 = 7$
2. Schritt: Suche Lösungen in $\mathbb{Z}/(5)$
Warum suchen wir nach Lösungen in $\mathbb{Z}/(5)$?
Es gilt $25 + (5) = 0 + (5)$, d.h. 5 mod 25. Deswegen gibt es einen Homomorphismus von $\mathbb{Z}/(25)$ nach $\mathbb{Z}/(5)$ wie in einem Satz weiter vorne in diesem Dokument bereits diskutiert. D.h. jede Lösung von $P_{25} = 0$ in $\mathbb{Z}/(25)$ hat als Bild unter diesem Homomorphismus eine Lösung von $P_5 = 0$ in $\mathbb{Z}/(5)$. Man kann jetzt zwei Sachverhalte schließen. Zum einen, wenn man keine Lösungen in $\mathbb{Z}/(5)$ von $P_5 = 0$ findet, so kann es auch keine Lösungen von $P_{25} = 0$ in $\mathbb{Z}/(25)$ geben. Andererseits findet man Lösungen von $P_5 = 0$ in $\mathbb{Z}/(5)$, so braucht man nur noch Elemente $a + (25) \in \mathbb{Z}/(25)$ betrachten, für die $a + (5) = L + (5)$ ist für alle Lösungen $L \in \mathbb{Z}/(5)$.
Die Ergebnisse für $\{0, 1, 2\}$ sind dieselben wie im 1. Schritt, da die Koeffizienten sich von P_3 im Vergleich zu P_5 nicht ändern. Grund: Sie sind alle kleiner als 5.
$4^2 + 4 + 1 = 21$
$5^2 + 5 + 1 = 31$
Man erkennt dass es in $\mathbb{Z}/(5)$ keine Lösungen von $P_5 = 0$ gibt. Deswegen gibt es auch keine Lösungen von $P_{25} = 0$ in $\mathbb{Z}/(25)$. Da aber der chinesische Restsatz ein Isomorphismus ist der für jede Lösung von $P_{825} = 0$ eine Lösung in jeweils $P_3 = 0$, $P_{25} = 0$ und $P_{11} = 0$ generiert, kann $P_{825} = 0$ keine Lösungen in $\mathbb{Z}/(825)$ haben.

Beispiel: Zweites Zahlenbeispiel zur Nullstellenberechnung von Polynomen in $\mathbb{Z}/(N)$

Wieder suchen wir nach Lösungen in $\mathbb{Z}/(825)$, dieses mal aber von
$X^2 + 473 * X + 376 = 0$
1. Schritt: Lösungen in $\mathbb{Z}/(3)$
Zuerst werden die Koeffizienten des Polynoms nach $\mathbb{Z}/(3)$ transferiert. $P_3 : X^2 + 2 * X + 1$
$0^2 + 2 * 0 + 1 = 1$
$1^2 + 2 * 1 + 1 = 1$
$2^2 + 2 * 2 + 1 = 9$ (Lösung)
Es folgt dass $2 + (3)$ eine Lösung von $P_3 = 0$ ist.
2. Schritt: Lösungen in $\mathbb{Z}/(5)$
$P_5 : X^2 + 3 * X + 1$
Da P_3 und P_5 nicht identisch sind müssen alle Werte neu berechnet werden.
$0^2 + 3 * 0 + 1 = 1$
$1^2 + 3 * 1 + 1 = 5$ (Lösung)
$2^2 + 3 * 2 + 1 = 11$
$3^2 + 3 * 3 + 1 = 19$
$4^2 + 3 * 4 + 1 = 29$
Es folgt dass $1 + (5)$ eine Lösung von $P_5 = 0$ ist.
Wenn wir nun also die Lösungen von P_{25} finden wollen müssen wir nur noch solche $a + (25) \in \mathbb{Z}/(25)$ betrachten, für die gilt: $a + (5) = 1 + (5)$. Das sind nur noch die folgenden 5 Elemente von $\mathbb{Z}/(25)$:
$P_{25} : X^2 + 23 * X + 1$ $1^2 + 23 * 1 + 1 = 25$ (Lösung)
$6^2 + 23 * 6 + 1 = 175$ (Lösung)
$11^2 + 23 * 11 + 1 = 375$ (Lösung)
$16^2 + 23 * 16 + 1 = 256 + 230 + 138 + 1 = 625$ (Lösung)
$21^2 + 23 * 21 + 1 = 441 + 483 + 1 = 925$ (Lösung)
Es folgt dass $1 + (25), 6 + (25), 11 + (25), 16 + (25), 21 + (25)$ Lösungen von $P_{25} = 0$ sind.
3.Schritt: Lösungen in $\mathbb{Z}/(11)$
$P_{11} : X^2 + 2$
$0^2 + 2 = 2$

$1^2 + 2 = 4$
$2^2 + 2 = 6$
$3^2 + 2 = 11$ (Lösung)
$4^2 + 2 = 18$
$5^2 + 2 = 27$
$6^2 + 2 = 38$
$7^2 + 2 = 51$
$8^2 + 2 = 66$ (Lösung)
STOP. $\mathbb{Z}/(11)$ ist ein Körper und Polynome zweiten Grades haben über einem Körper maximal 2 Nullstellen.
Es folgt dass $3 + (11), 8 + (11)$ Lösungen von $P_{11} = 0$ sind.
Jetzt müssen die Lösungen in den kleineren Restklassenringen $\mathbb{Z}/(3)$, $\mathbb{Z}/(25)$ und $\mathbb{Z}/(11)$ noch mit Hilfe des chinesischen Restsatzes in Lösungen von P_{825} in $\mathbb{Z}/(825)$ überführt werden.
Bei der Rückübersetzung muss allerdings ein kleiner Trick angewandt werden.
Wir leiten zunächst die Umkehrabbildung des Isomorphismus
$\mathbb{Z}/(N) \overset{\cong}{\mapsto} \mathbb{Z}/(K) \times \mathbb{Z}/(L) \quad (K, L$ teilerfremd)
her. Da $ggT(K, L) = 1$ folgt dass man $x, y \in \mathbb{Z}$ findet, so dass gilt:
$1 = xK + yL$
Will man, wenn man $Z + (K) = a \wedge Z + (L) = b$ erhalten, so ist die Behauptung dass man dies mit $Z = xK * b + yL * a$ erreicht.

Beweis:

$$\begin{aligned} Z + (K) &= xK * b + yL * a + (K) \\ &= (xK * b + (K)) + ((yL * a) + (K)) \\ &= yL * a + (K) \\ &= (yL + (K)) * (a + (K)) \\ &= a + (K) \end{aligned}$$

Die letzte Gleichung erhält man wenn man sich überlegt was herauskommt wenn man die Gleichung $1 = xK + yL$ auf beiden Seiten modulo K nimmt.
Exakt analoge Überlegungen zeigen dass $Z + (L) = b$ sein muss.

Es bleibt nach dieser Erläuterung also nur $x, y \in \mathbb{Z}$ zu bestimmen für die $1 = xK + yL$ ist. Dann ist die Umkehrabbildung des chinesischen Restsatzes wie folgt:
$f^{-1}((a + (K), b + (L))) = xK * b + yL * a$
(Wobei f der Isomorphismus des chinesischen Restsatzes ist)
Da wir jetzt aber bloß eine Rückübersetzung für den Standard-Isomorphismus des chinesischen Restsatzes beherrschen, müssen wir die Rücktransformation unserer gefundenen 3-Tupel Nullstellen etwas anders machen.
Wir betrachten dabei die zwei Isomorphismen:
$\mathbb{Z}/(75) \overset{\cong}{\mapsto} \mathbb{Z}/(3) \times \mathbb{Z}/(25)$ und
$\mathbb{Z}/(825) \overset{\cong}{\mapsto} \mathbb{Z}/(75) \times \mathbb{Z}/(11)$ Für den ersten Isomorphismus ist $1 = (-8) * 3 + 1 * 25$. D.h. die Rückübersetzung findet mittels $f^{-1}((a + (3), b + (25))) = (-8) * 3 * b + 1 * 25 * a + (75)$ statt.
Für den zweiten Isomorphismus ist $1 = 5 * 75 + (-34) * 11$. D.h. die Rückübersetzung findet mittels $f^{-1}((c + (75), d + (11))) = 5 * 75 * d + (-34) * 11 * c + (75)$ statt.
Wendet man also die zweite Rückübersetzung nach der ersten an, so erhält man:
$f^{-1}((a+(3), b+(25), c+(11))) = 375*c+(-374)*(-24*b+25*a)+(825) = 550*a+726b+375c+(825)$
Durch Einsetzen der bereits errechneten Lösungen für a, b, c in allen möglichen Kombinationen erhält man alle Lösungen im Ausgangsring $\mathbb{Z}/(825)$.

Exemplarisch wird eine Lösung berechnet:
Zu $(2+(3), 6+(25), 3+(11)) \in \mathbb{Z}/(3) \times \mathbb{Z}/(25) \times \mathbb{Z}/(11)$ gehört die Lösung
$550 * 2 + 726 * 6 + 375 * 3 + (825) = 1100 + 4356 + 1125 + (825) = 6581 + (825) = 806 + (825)$
Man kann dies durch Einsetzen in das Ausgangspolynom verifizieren.

3 Diophantische Gleichungen / Ungleichungen

Einführung

Die grundsätzliche Fragen in diesem Teil ist die Lösbarkeit und die Lösungsmenge einer Gleichung / eines Gleichungssystems. Wichtig hierfür ist es, wo wir denn eigentlich suchen. Die grundlegenden Dinge, die wir behandeln werden:

(a) lineare Gleichungssysteme
$A * x = b \quad A \in \mathbb{Z}^{k \times l}, b \in \mathbb{Z}^k$
(Hier: $\text{rang}(A) = \text{rang}(erw)$ nicht hinreichend!)

(b) Polynome
$3 * x - 1 = 0$ ist lösbar in $\mathbb{Q}$, nicht aber in $\mathbb{Z}$.
$x^4 - 2 = 0$ hat keine Lösung in $\mathbb{Z}$, $\mathbb{Q}$. 2 Lösungen in $\mathbb{R}$. In $\mathbb{C}$ gibt es sogar 4 Lösungen.

Wir suchen hier ganzzahlige Lösungen und Lösungen in Restklassenringen. Wir beschränken uns auf ganzzahlige Koeffizienten.

Beispiel Restklassenring:

$P \in \mathbb{Z}[X_1, ..., X_r] = \sum \alpha_{i_1,...,i_r} * (X^{i_1} * ...X^{i_r})$
$2 \leq N \in \mathbb{N}$: $\pi : \mathbb{Z} \mapsto \mathbb{Z}/(N)$.
$\pi(P) = \sum \pi(\alpha_{i_1,...,i_r}) * (X^{i_1} * ...X^{i_r}) \in \mathbb{Z}/(N)[X_1, ..., X_r]$
Sei $(a_1, ..., a_r) \in \mathbb{Z}^r$ Lösung von P. Dann ist $(\pi(a_1), ..., \pi(a_r)) \in \mathbb{Z}/(N)^r$ Lösung von $\pi(P)$.

Beispiel $x^2 - 2$:

(hat keine (rationale) Lösung in $\mathbb{Q}$)
Annahme: $q \in \mathbb{Q}$ Lösung: $q = \frac{k}{l}$, $1 \leq l \in \mathbb{N}$, $1 = \text{ggT}(k, l)$
$\frac{k^2}{l^2} - 2 = 0$, d.h. $k^2 - 2l^2 = 0$
$\pi : \mathbb{Z} \mapsto \mathbb{Z}/(3)$ Modulo 3
$(k + (3))^2 = 2 * (l + (3))^2$
Quadratisch in $\mathbb{Z}/(3)$ $(0 + (3))^2 = 0 + (3)$, $(1 + (3))^2 = 1 + (3)$, $(2 + (3))^2 = 1 + (3)$
$\Rightarrow l + (3) = 0 + (3) = k + (3)$
$\Rightarrow 3 \mid l \wedge 3 \mid k$ ↯(teilerfremd)
Nachfolgend werden wir relativ einfache Diophantische Gleichungen behandeln.

3.1 Lineare Diophantische Gleichungen

Wir suchen ganzzahlige Lösungen, wir benutzen dabei die Ergebnisse aus der linearen Algebra für $\mathbb{Q}$.
Sei M die Lösungsmenge von $A * x = b$ in $\mathbb{Z}^l$,
Sei L die Lösungsmenge von $A * x = 0$.
Es folgt: (Falls $M \neq \emptyset$) $M = a + L$, $a \in M$ beliebig. (a: partikuläre Lösung)
Fragen: (vollständig beantwortbar)

- Lösbarkeit?
- Bestimmung einer partikulären Lösung?
- Bestimmung aller Lösungen von A*X = 0?

Bezeichnungen:

L Lösungsmenge (im umgebenen System)

$L_{\mathbb{Q}}$ Lösungsmenge von $A * X = 0$ in $\mathbb{Q}^l$

$\mathbb{Z}^l \subseteq \mathbb{Q}^l$, $L = L_{\mathbb{Q}} \sup \mathbb{Z}^l$ L Untergruppe von $\mathbb{Z}^l$.

Satz 1.1: $L_{\mathbb{Q}}$ ist der von L erzeugte lineare Unterraum

$L_{\mathbb{Q}}$ ist der von L erzeugte lineare Unterraum.

Beweis:
Sei $(a_1, ..., a_l) \in L_{\mathbb{Q}}$. $a_1 = \frac{b_1}{c}$, ..., $a_l = \frac{b_l}{c}$ (gleicher Teiler!) $1 \leq c \in \mathbb{N}$.
Es folgt $(b_1, ..., b_l) \in L$, $(a_1, ..., a_l) = \frac{1}{c}(b_1, ..., b_l)$

Definition 1.2: Rang: $\mathrm{rg}(G)$

(Ersatz für Dimensionsbegriff der linearen Algebra)
Sei $G \subseteq \mathbb{Q}^l$ eine Untergruppe.
Dann ist $\mathrm{rg}(G) = dim_{\mathbb{Q}} < G >$ ist der Rang von G.
$< G >$: von G erzeugter linearer Unterraum von $\mathbb{Q}^l$.
G ist frei, falls sie eine Basis hat. d.h. eine Folge $(b_1, ..., b_r)$ mit:

- $b_1, ..., b_r$ in $\mathbb{Q}^l$ linear unabhängig.
- G wird von $b_1, ..., b_r$ erzeugt.

Nicht jede Untergruppe von $\mathbb{Q}^l$ hat eine Basis. $\mathbb{Q}$ als Gruppe hat keine Basis!

Beispiel:

$\mathbb{Z}^l$ ist frei vom Rang l: Die kanonische Basis.

Beispiel:

$(6, 10)$, $(10, 15)$, $(30, 40)$ erzeugen Untergruppe G von $\mathbb{Z}^2$.
$\mathrm{rg}(G) = 2$
frei: G hat Basis $(2, 0)$, $(0, 5)$!
$(6, 10) = 3 * (2, 0) + 2 * (0, 5)$ ...
Darstellung von $(2, 0)$, $(0, 5)$ als Linearkombination von $(6, 10)$, $(10, 15)$, $(30, 40)$!
$(2, 0) = 2 * (6, 10) - 4 * (10, 15) + (30, 40)$
$(0, 5) = 3 * (10, 15) - (30, 40)$

Satz 1.3: Jede Untergruppe $G \subseteq \mathbb{Z}^l$ ist frei.

$l \in \mathbb{N}$, $G \subseteq \mathbb{Z}^l$ Untergruppe. Dann ist G frei.

Beweis: Induktion nach l

$l = 0$ $\surd$

$l = 1$ $G = \{0\}$ $\surd$, Basis: $\{\}$
$G \neq \{0\}$. In G gibt es eine positive Zahl. Sei g_0 die kleinste positive Zahl in G.
Behauptung: g_0 ist Basis von G. Zu Zeigen: g_0 erzeugt G.
Sei $g \in G$. Division mit Rest: $g = qg_0 + r$, $0 \leq r < g_0$. $r = g - qg_0 \in G$. Aus der Minimalität von g_0 folgt $r = 0$.

$l \rightsquigarrow l + 1$ Falls $G \subseteq \mathbb{Z}^l \times \{0\}$ (praktisch in $\mathbb{Z}^l$ enthalten): Nach Induktion ist G frei.
Sei $G \not\subseteq \mathbb{Z}^l \times \{0\}$. $\pi : \mathbb{Z}^{l+1} \mapsto \mathbb{Z}$ Projektion auf die letzte Komponente. Daraus folgt: $\pi[G] \subseteq \mathbb{Z}$ ist nicht $\{0\}$.
Fall $l = 1$ zeigt: $\pi[G]$ hat Basis, etwa $\alpha \in \mathbb{Z}$ (theoretisch vorraussetzbar: $\alpha > 0$) $\alpha = \pi(\beta)$, $\beta \in G$.
Setze $H = G \sup(\mathbb{Z}^l \times \{0\})$ (Untergruppe von $\mathbb{Z}^l$). Nach Induktion: Es gibt eine Basis $\gamma_1, ..., \gamma_r$. Dann ist
$\underbrace{\gamma_1, ..., \gamma_r}_{\text{linear unabhängig}}$, β Basis von G!
β ist nicht als Kombination von γ_i darstellbar, da $\forall i : \gamma_i = (..., 0)$, aber $\beta = (..., x)$ mit $x \neq 0$.
Damit ist $\gamma_1, ..., \gamma_r, \beta$ linear unabhängig.

G wird erzeugt: Sei $g \in G \Rightarrow \pi(g) = z\alpha$, $z \in \mathbb{Z}$
$\Rightarrow \pi(g - z\beta) = 0 \Rightarrow g - z\beta \in (G \sup \mathbb{Z}^l \times \{0\}) = H \Rightarrow g - z\beta = t_1\gamma_1 + ... + t_r\gamma_r$.

Beispiel:

$\mathbb{Z}^2 : (6, 10), (10, 15), (30, 40)$ erzeugen Untergruppe G von $\mathbb{Z}^2$.
$\pi[G] \subseteq \mathbb{Z}$ erzeugt von $10, 15, 40$. $\text{ggT}(10, 15, 40) : \overset{\alpha}{5} = 15 - 10$
$\pi(\underbrace{(10, 15) - (6, 10)}_{\substack{(4,5) \\ \beta}}) = \overset{\alpha}{5}$

Erzeugendensystem für $H = G \sup(\mathbb{Z} \times 0)$:
$\underbrace{(-2, 0) = (6, 10) - 2(4, 5); \quad (-2, 0) = (10, 15) - 3(4, 5); \quad (-2, 0) = (30, 40) - 8(4, 5)}_{\text{letzte Komponente 0, zusammen erzeugen sie H}}$
$+2 = \text{ggT}(-2, -2, -2) \Rightarrow (2, 0)$ Basis für $H \Rightarrow (2, 0), (4, 5)$ Basis für G.

Lemma 1.4: Homogenes diophantisches Gleichungssystem

$A * x = 0$, $A \in \mathbb{Z}^{k \times l}$, L Lösungsmenge.
Dann gilt $L \subseteq \mathbb{Z}^l$ ist freie (abelsche) Gruppe von Rang: $l - \underbrace{\text{Rang}\,(A)}_{lin.Alg.}$

Das algorithmische Problem ist nun: Basisberechnung.
Für den nachfolgenden Satz brauchen wir eine passende (rekursive) Definition vom ggT (für mehr als ein Parameter):
$\text{ggT}(0, 0) = 0$
a, b nicht beide 0: $\text{ggT}(a, b) = \sup\{n \in \mathbb{N} | n \mid a \wedge n \mid b\}$
$\text{ggT}(a_1, ..., a_r) = \text{ggT}(\text{ggT}(a_1, ..., a_{r-1}), a_r)$
Als Erinnerung den **Satz I.9.6**: Für $1 \leq a, b \in \mathbb{N}$ gilt: $\{ua + vb | u, v \in \mathbb{Z}\} = \mathbb{Z} * \text{ggT}(a, b)$, verallgemeinert: $a_1, ..., a_r \in \mathbb{Z}$: $\{u_1a_1, ..., u_r, a_r | u_i \in \mathbb{Z}\} = \mathbb{Z} * \text{ggT}(a_1, ..., a_r)$

Satz 1.5:

$a_1X_1 + ... + a_lX_l = b$ ist lösbar $\Leftrightarrow \text{ggT}(a_1, ..., a_l) \mid b$.

Beweis:

"⇒" Sei $(x_1, ..., x_l) \in \mathbb{Z}^l$ eine Lösung. Es folgt $x_1a_1 + ... + x_la_l$ ist Linearkombination von $a_1, ..., a_l$. d.h. $b = x_1a_1 + ... + x_la_l = \mathbb{Z} * \text{ggT}(a_1, ..., a_l)$

"⇐" Sei $b = z * \text{ggT}(a_1, ..., a_l) \in \{u_1a_1 + ... + u_la_l | u_i \in \mathbb{Z}\}$. d.h. $\exists x_1, ..., x_l : b = x_1a_1 + ... + x_la_l$

Nachfolgend eine lange Darstellung/Beispiel, die im Manuskript als Satz steht, wie man eine Lösung eigentlich bestimmt.

Eine Lösung bestimmen

oBdA $a_1, ..., a_l \neq 0$, $b \neq 0$.

$$\begin{aligned} g_1 &= a_1 \\ g_2 &= \text{ggT}(a_1, a_2) \\ &... \\ g = g_l &= \text{ggT}(a_1, ..., a_l) \end{aligned}$$

Dividiere b mit Rest durch g: $b = qg + r$.
Wenn $r \neq 0$: unlösbar.
Wenn $r = 0$: lösbar.
Falls $g = u_1a_1 + ... + u_la_l \Rightarrow b = (qu_1)a_1 + ... + (qu_l)a_l$
Wie geht es nun algorithmisch? Unser Wunsch ist es eine Basis der Lösungsgruppe anzugeben.

$$\begin{aligned} g_1 &= x_{11}a_1 \\ g_2 &= x_{21}a_1 + x_{22}a_2 \\ g_3 &= zg_2 + ta_3 \\ &... \\ g = g_l &= x_{l1}a_1 + ... + x_{ll}a_l \end{aligned}$$

Löse $a_1x_1 + ... + a_lx_l = 0$: Basis der Lösungsmenge.
$a_1, ..., a_l = 0$: trivial, Lösung=$\mathbb{Z}^l$
Setze $J = \{i | a_i \neq 0\}$, $K = \{i | a_i = 0\}$ Trennung in 2 Gruppen
$\sum_{i \in K} a_ix_i = 0 : \mathbb{Z}^l$
$\sum_{i \in J} a_ix_i = \{x_j \in \mathbb{Z}^J | x_j \text{ ist Lösung}\} \times \mathbb{Z}^K$.
Daher genügt es vorrauszusetzen, dass $a_1, ..., a_l \neq 0$. Also sei ab jetzt $a_1, ..., a_l \neq 0$.
Suche in $\mathbb{Z}^2$ Lösung (x_1, x_2) von $a_1x_1 + a_2x_2 = 0$ (Damit ist $(x_1, x_2, 0..., 0)$ Lösung von $a_1x_1 + ... + a_lx_l = 0$) Lösungsmenge $L_2 \subseteq \mathbb{Z}^2$. Freie Untergruppe mit rg = 1.

$(x_1, x_2) \in L_2 \Rightarrow a_1x_1 = -a_2x_2$ ist gemeinsames Vielfaches von a_1, a_2.
k_2: kleinstes gemeinsames Vielfaches (Produkt/ggT)
Schreibe $k_2 = za_1 = ta_2 \Rightarrow za_1 + (-t)a_2 = 0$, d.h. $(z, -t) \in L_2$.
Basis von L_2! Sei $(x_1, x_2) \in L_2$. Es folgt $a_1x_1 = -a_2x_2 = uk_2 = uza_1 = uta_2 \Rightarrow x_1 = uz$, $x_2 = -ut$. d.h. $(x_1, x_2) = u(z, -t)$
L_3: Lösungsmenge von $a_1x_1 + a_2x_2 + a_3x_3$
$k_3 = \text{kgV}(g_2, a_3) = z'g_2 = t'a_3 = z'(x_{21}a_1 + x_{22}a_2) = t'a_3$
$(z'x_{21}, z'x_{22}, -t') \in L_3$
Strukturell: 2 Basis-Elemente
In der dritten Komponente einerseits 0, andererseits ungleich null, dann sind diese beiden Vektoren linear unabhängig.
$L_2 \times \{0\} \subseteq L_3$, $(z, -t, 0)$, $(z'x_{21}, z'x_{22}, -t')$ Basis von L_3.

Darstellbarkeit Sei $(x_1, x_2, x_3) \in L_3$. $x_1a_1 + x_2a_2 + x_3a_3 = 0$, d.h.

$\underbrace{x_1a_1 + x_2a_2}_{\text{Vielfaches von } g_2} = \underbrace{-x_3a_3}_{\text{VF von } a_3} = u'k_3$

$-x_3a_3 = u'k_3 = u't'a_3 \Rightarrow x_3 = -u't'$

$u'(z'x_{21}, z'x_{22}, -t') - (x_1, x_2, x_3) \in L_3$

$= (u'z'x_{21} - x1, u'z'x_{22} - x2, 0)$, d.h. $(u'z'x_{21} - x1, u'z'x_{22} - x2) \in L_2$

$\Rightarrow = v(z, -t)$

$(x_1, x_2, x_3) = u'(z'x_{21}, z'x_{22}, -t') - v(z, -t, 0)$

Ab nun wird iteriert (L_4 usw).

Induktiver Beweis, dass Untergruppe Linear Unabhängig.

$G \subseteq \mathbb{Z}^l$, $\pi : \mathbb{Z}^l \mapsto \mathbb{Z}$

$\pi[G] * \alpha$; $\alpha = \pi(\beta)$

$G \sup(\mathbb{Z}^{l-1} \times \{0\}) = H$: $\gamma_1, ..., \gamma_r$

$\gamma_1, ..., \gamma_r, \beta$ Basis von G

Das ist nun andersherum aufgezäumt gewesen:

$\left.\begin{array}{l} L_2 \subseteq \mathbb{Z}^2 \\ L_3 \subseteq \mathbb{Z}^3 \end{array}\right\}$ von allen die letzte Komponente angeschaut, so klein wie möglich von unten aufgebaut

Es fehlt nun wie man homogenes Gleichungssystem lösen kann, dies ist zurückführbar auf obriges. (Oder mit dem Durchschnitt der Lösungsräume)

$A * x = 0$ Zeilen von A: $a_1, ..., a_k$

Bestimme Lösungen von $a_1x = 0$: M_1

Bestimme Lösungen von $a_2x = 0$ in M_1: M_2

... (iteriert)

M_1 frei mit $\operatorname{rg} l - 1$, Basis $v_1, ..., v_{l-1}$,

d.h. $\mathbb{Z}^{l-1} \overset{\cong}{\mapsto} M_1$: $(z_1, ..., z_{l-1}) \mapsto z_1v_1 + ... + z_{l-1}a_{l-1}$

$$a_2 * \overbrace{\begin{pmatrix} & & \\ v_1, ..., v_{l-1} & & \\ & & \end{pmatrix}}^{B} * \begin{pmatrix} z_1 \\ ... \\ z_{l-1} \end{pmatrix} = 0$$

Aufgabe: Löse:

$(a_2(v_1, ..., v_{l-1})) * x = 0$: $M_2' \subseteq \mathbb{Z}^{l-1}$

$(a_3(v_1, ..., v_{l-1})) * x = 0$

...

Basis von M_2': $w_1, ..., w_{l-2}$

Basis von M_2: $Bw_1, ..., Bw_{l-2}$

3.2 Quadratische Reziprozität

Einführung

Die quadratische Reziprozität ist einer der Perlen der Zahlentheorie. Entdeckt wurde sie vor rund 200 Jahren von Gauss.
Wenn man die diophantischen Gleichungen richtig allgemein behandeln will, ist dies extrem kompliziert.
Hier haben wir wieder ganzzahlige Koeffizienten, diesmal aber mit Gleichungen: $x_1^2 + ax_2 = b$; $a, b \in \mathbb{Z}$
$(x_1, x_2) \in \mathbb{Z}^2$ Lösung $\Leftrightarrow x^2 - b = -ax_2$
Fall $a = 0$: Löse $x_1^2 = b$. Wenn $b < 0$ gibt es keine Lösung. Bei $b \geq 0$ berechnet man $\sqrt{b}$ in $\mathbb{R}$. Wenn nun $\sqrt{b} \in \mathbb{Z}$ sind $\sqrt{b}$,-$\sqrt{b}$ Lösungen.
Fall $a \neq 0$: (Generalvorraussetzung)
$x_1^2 + ax_2 = b \Leftrightarrow x_1^2 - a(-x_2) = b$. (Wenn negative Lösung, dann gibt es auch die positive Lösung), daher oBdA: $a \geq 1$
Fall $a = 1$: x_1 beliebig, setze $x_2 = -x_1^2 + b$. Dies ist immer lösbar, die Lösungsmenge ist klar.
Ab jetzt $a \geq 2$:
$x_1^2 - b = -ax_2$ hat Lösung $\Leftrightarrow \exists x_1 : x_1^2 - b \in \mathbb{Z} * a \Leftrightarrow$ In $\mathbb{Z}/(a)$:$(x_1 + (a))^2 = b + (a)$

Definition 2.1: Quadratischer (Nicht-)Rest

$2 \leq a \in \mathbb{N}$, $b \in \mathbb{Z}$
b ist quadratischer Rest modulo a, wenn $b + (a)$ in $\mathbb{Z}/(a)$ ein Quadrat ist.
Ansonsten heißt b quadratischer Nichtrest.

Vereinfachung

Mit dem chinesischen Restsatz gilt für $a = p_1^{k_1} * ... * p_r^{k_r}$ (Primfaktorzerlegung)
$\mathbb{Z}/(a) \overset{\cong}{\mapsto} \mathbb{Z}/(p_1^{k_1}) \times ... \times \mathbb{Z}/(p_r^{k_r})$ b ist quadratischer Rest modulo a
$\Leftrightarrow b$ quadratischer Rest modulo $p_i^{k_i}$ für alle i.
Problem noch: Primfaktorzerlegung, diese wird aber später unnötig werden...
Sei $a = p^k$, p Primzahl, $k \geq 1$.
Falls $b = xa$, d.h. $b + (a) = 0 + (a) = (0 + (a))^2$: quadratischer Rest
p nicht teilerfremd zu b wird auf Teilerfremdheit zurückgeführt.
Falls b kein Vielfaches von a: Sei $p \mid b$, d.h. $b = p^l * c$, $0 < l < k$, ggT$(c, p) = 1$.
Falls b quadratischer Rest modulo a: $\exists x, y \in \mathbb{Z}$: $x^2 + ay = b \Leftrightarrow x^2 = \underbrace{b - ay}_{\text{VF von } p^l \text{ nicht von } p^{l+1}}$
Maximale p-Potenz, die x^2 teilt: gerade $\Rightarrow l = 2 * m$; $x = p^m * z$, $p \not| z$
$z^2 = (\frac{x}{p^m})^2 = \frac{x^2}{p^l} = c - p^{k-l}y \Rightarrow c$ quadratischer Rest modulo p^{k-l}
Die Argumente sind umdrehbar, die Aussage wird später verstärkt. Theoretisch ist dies alles relativ befriedigend, aber zum richtigen Rechnen ist es noch nicht besonders gut geeignet.
c quadratischer Rest mit $p^{k-l} \Leftrightarrow b$ quadratischer Rest modulo $p^k = a$
Noch zu behandeln: b, a **teilerfremd**
Ab hier fängt die Theorie von Gauss an, vorheriges war nur Vorgeplänkel...

Satz 2.2:

$a = p^k$, $b \in \mathbb{Z}$ teilerfremd zu a.

(a) $p = 2$ b quadratischer Rest modulo $a \Leftrightarrow b \equiv 1 (\mathrm{mod}\, 2^\mu)$ mit $\mu = \min\{3, k\}$.

(b) p **ungerade** b quadratischer Rest modulo $a \Leftrightarrow b$ quadratischer Rest modulo p

Beweis: (a)

"$\Rightarrow$" Schreibe $b = x^2 + 2^k y$. p, b teilerfremd. b ungerade $\Rightarrow x$ ungerade, $x = 4 * z + t$ mit $t = 1$ oder $t = 3$
$\Rightarrow x^2 = 16z^2 + 8z + t + t^2 \equiv t^2 (\mathrm{mod}\, 8) = \begin{cases} 1 \\ 9 \equiv 1 (\mathrm{mod}\, 8) \end{cases}$
Falls $k \geq 3$: $b \equiv x^2 \equiv 1 (\mathrm{mod}\, 8)$, $8 = 2^3 = 2^\mu$
Falls $k \leq 2$: $b + (8) = 1 + (8)$
$k \leq 3$: $\mathbb{Z}/(2^3) \mapsto \mathbb{Z}/(2^k)$: $k + (2^k) = 1 + (2^k)$
$b \equiv 1 (\mathrm{mod}\, 2^k)$, $2^k = 2^\mu$

"$\Leftarrow$" $b + (2^\mu) = 1 + (2^\mu)$, Induktion nach k.

- $k \leq 3$ $\mu = k$, also $b + (2^k) = b + (2^\mu) = 1 + (2^\mu) = (1 + (2^k))^2$.
- $k \rightsquigarrow k + 1$ Sei $b + (2^k) = (x + (2^k))^2 = x^2 + (2^k)$. Suche $y \in \mathbb{Z}$ mit
  $b + (2^{k+1}) = (x + 2^{k-1} * y)^2 + (2^{k+1})$. Sei $y \in \mathbb{Z}$ beliebig. $(x + 2^{k-1} y)^2 = x^2 + 2^k xy + 2^{2(k-1)} * y^2$
  b ungerade $\Rightarrow x$ ungerade. $x = 2z + 1$.
  $\Rightarrow = x^2 + 2^{k+1} zy + 2^k y + 2^{k+1} 2^{k-3} y^2 \equiv x^2 + 2^k y$ (modulo 2^{k+1})
  Suche y mit : $x^2 + 2^k y \equiv b$ (modulo 2^{k+1})
  $x^2 - b = u 2^k$, $u \in \mathbb{Z}$. Entweder $u = 2v$, oder $u = 2v + 1$
  - $u = 2v$**:** $x^2 - b = 2^{k+1} v \equiv 0$ (modulo 2^{k+1}) Setze $y = 0 \Rightarrow x^2 + 2^k y \equiv b$ (modulo 2^{k+1})
  - $u = 2v + 1$**:** $x^2 - b = 2^{k+1} v + 2^k \equiv 2^k$ (modulo 2^{k+1}) Setze $y = 1 \Rightarrow x^2 + 2^k y \equiv b$ (modulo 2^{k+1})
    $\Leftrightarrow x^2 - 2^k \equiv b$ (modulo 2^{k+1})

Beweis: (b)

"$\Leftarrow$" $\pi : \mathbb{Z}/(p^k) \mapsto \mathbb{Z}/(p)$ Ringhomomorphismus
$b + (p^k) = (c + (p^k))^2$; $b + (p) = (c + (p))^2$

"$\Rightarrow$" Induktion nach k

- $k = 1$ $\surd$
- $k \rightsquigarrow k + 1$ $b + (p^k) = x^2 + (p^k)$
  Modifikation von x:
  Suche $y \in \mathbb{Z}$ mit: $b + (p^{k+1}) = (x + p^k y)^2 + (p^{k+1})$ Sei $y \in \mathbb{Z}$ beliebig. Dann gilt
  $(x + p^k y)^2 = x^2 + 2p^k xy + p^{2k} y^2 \equiv x^2 + 2p^k xy$ (modulo p^{k+1})
  Suche $y \in \mathbb{Z}$ mit: $x^2 + 2p^k xy \equiv b$ (modulo p^{k+1})
  Schreibe: $x^2 - b = up^k$. $up^k = x^2 - b \equiv -2p^k xy$ (modulo p^{k+1})
  $\Rightarrow u \equiv -2xy$ (modulo p)
  Suche $y \in \mathbb{Z}$ mit: $u + 2xy \equiv 0$ (modulo p). Falls $2x + (p) \neq 0 + (p)$: Setze
  $y + (p) = \underbrace{(2x + (p))^{-}1}_{\text{darf}} * (-u + (p))$

Beispiel 9393 Quadratischer Rest modulo 10000?:

$10000 = 2^5 * 5^5$
9393 quadratischer Rest modulo 2^5? $\mu = 3 \Rightarrow 9393 \equiv 1 (\mathrm{mod}\, 8)$ $\surd$
9393 quadratischer Rest modulo 5^5?
$\Leftrightarrow$ 9393 quadratischer Rest modulo 5? $9393 \equiv 3 (\mathrm{mod}\, 5)$
$\Leftrightarrow$ 3 quadratischer Rest modulo 5?

z	z^2
0	0
1	1
2	4
3	4
4	1

0 kann eh nicht, da teilerfremd.

(Unter Beweis (b))
Es bleibt: b quadratischer Rest modulo p.
Es gibt es Gesetz, welches wir noch behandeln werden, welches nicht einfach zu sehen ist. Dieses wurde von Gauss mit 21 bewiesen (1797 im "Großes Werk")

Korollar 2.3:

$a = p^k$, $b = cp^l$, $0 < l < k$, $0 < b < a$ (Ansonsten Division mit Rest)
Dann gilt: b quadratischer Rest modulo $a \Leftrightarrow l = 2m$ und c quadratischer Rest modulo a.

Beweis:

"$\Leftarrow$" $c + (a) = x^2 + (a) \Rightarrow b + (a) = c * p^l + (a) = x * p^m)^2 + (a)$ ($\surd$)

"$\Rightarrow$" Für l gerade gezeigt, c ist quadratischer Rest modulo p^{k-l}.

Zu Zeigen: c quadratischer Rest modulo p^k.

p **ungerade** c quadratischer Rest modulo $p^{k-l} \Rightarrow c$ quadratischer Rest modulo $p \Rightarrow c$ quadratischer Rest modulo p^k

$p = 2$ **Falls** $k - l \geq 3$: c quadratischer Rest modulo 2^{k-l}, $\mu = 3 \Rightarrow c \equiv 1$ (modulo 2^μ) $\Rightarrow c$ quadratischer Rest modulo 2^k.

Falls $k - l = 1$: $0 < b = c * 2^{\overbrace{k-1}^{l}} < 2^k \Rightarrow c = 1 \Rightarrow c$ quadratischer Rest modulo $\overbrace{2^k}^{r}$

Falls $k - l = 2$: $0 < b = c * 2^{k-2} < 2^k$, c ungerade.
Entweder $c = 1$ quadratischer Rest modulo 2^k ($\surd$)
oder $c = 3$; 3 ist nicht quadratischer Rest modulo $2^2 = 2^{k-l}$ $\lightning$.

Quadratische Rest in $\mathbb{Z}/(p)$, p ungerade. Wie ist die Struktur von $\mathbb{Z}/(p)^\times$?

> **Pierre de Fermat**[1] (* Ende 1607 oder Anfang 1608 in Beaumont-de-Lomagne; Tod: 12. Januar 1665 in Castres) war ein französischer Mathematiker und Jurist.

Fermat'scher Satz: $x^n + y^n = z^n$: Gibt es eine nicht-triviale Lösung ($n \geq 3$)? Dieses Problem war bis 1990 offen.
Der nachfolgende kleine Fermat'sche Satz existiert in verschiedenen Formulierungen. In der Algebra-Vorlesung wird er viel allgemeiner gezeigt, dafür werden aber verschiedene Vorbereitungen nötig. Dadurch wird der eigentliche Beweis kürzer.
Jeder einzelne Schritt des Beweises offenbart interessante Eigenschaften für Körper...

Satz 2.4: kleiner Fermat'scher Satz (1640)

Die Gruppe $\mathbb{Z}/(p)^\times$ ist zyklisch, d.h. $\exists \alpha \in \mathbb{Z}/(p)^\times : \{\alpha, ..., \alpha^{p-1}\} = \mathbb{Z}/(p)^\times$.
α: primitives Element, bzw. primitive Restklasse

Beweis: 1. Schritt
Falls K Körper, $P \in K[X]$, $1 \leq \deg(P) = d$ ist, dann hat P in K höchstens d verschiedene Nullstellen.

Beweis:
Induktion nach d:

- $d = 1$ $\surd$
- $d \rightsquigarrow d + 1$ Annahme: Nullstellen $a_1, ..., a_{d+2}$ paarweise verschieden. $P = (X - a_{d+2}Q + R$ Division mit Rest (wie in der Schule: Polynomdivision), R ist konstant. $P(a_{d+2}) = 0$, $(a_{d+2} - a_{d+2}) * Q(a_{d+2}) + R = 0$, $\deg(Q) = d$, Nullstellen: $a_1, ..., a_{d+1}$
  $0 = P(a_i) = \underbrace{(a_i - a_{d+2})}_{\neq 0} * \underbrace{Q(a_i)}_{\Rightarrow = 0}, \quad 1 \leq i \leq d+1$
  $\Rightarrow Q(a_i) = 0$ $\lightning$Induktionsannahme

[1] http://de.wikipedia.org/wiki/Fermat

Beweis: 2. Schritt

Für alle $\alpha \in \mathbb{Z}/(p)^\times : \alpha^{p-1} = 1$. Seien $\beta_1, ..., \beta_{p-1}$ die Elemente von $\mathbb{Z}/(p)^\times$ Es folgt $\alpha\beta_1, ..., \alpha\beta_{p-1}$ sind Elemente von $\mathbb{Z}/(p)^\times$. Dann ist $\underbrace{\prod_i \beta_i}_{\neq 0} = \prod_i \alpha\beta_i = \alpha^{p-1} \prod_i \beta_i$. Es folgt: $1 = \alpha^{p-1}$.

Für jedes α: Gibt es eine kleinste positive Zahl r_α mit $\alpha^{r_\alpha} = 1$. r heißt Ordnung von α, $r = \text{ord}(\alpha)$
Es gilt $\alpha^s = 1 \Leftrightarrow r_\alpha \mid s$.

Beweis:

"$\Leftarrow$" $s = t * r_\alpha = \alpha^s = (\alpha^{r_\alpha})^t = 1^t = 1$

"$\Rightarrow$" Division mit Rest: $s = q * r_\alpha + t$, $0 \leq t < r_\alpha$
$1 = \alpha^s = (\alpha^{r_\alpha})^q * \alpha^t = \alpha^t$. Es folgt wegen der Minimalität von r_α: $t = 0$.

Es gilt: Für $n \in \mathbb{N}$: $r_{\alpha^u} \mid r_\alpha$.
Suche α mit Ordnungen $r_\alpha = p - 1$.

Beweis: 3. Schritt

Seien $\alpha, \beta \in \mathbb{Z}/(p)^\times$, $k = \text{kgV}(r_\alpha, r_\beta)$. Dann gibt es ein $\gamma \in \mathbb{Z}/(p)^\times$ mit $r_\alpha = k$.

Beweis:

Falls $k = r_\alpha$: $\gamma = \alpha$, falls $k = r_\beta$: $\gamma = \beta$. Ab jetzt also $k \neq r_\alpha, r_\beta$.
Mit $g = \text{ggT}(r_alpha, r_beta)$: $k = \frac{r_\alpha}{g} * r_\beta$: $r_{\alpha^g} = \frac{r_\alpha}{g}$, $k = \text{kgV}(r_{\alpha^g}, r_\beta)$.
Nach Ersetzen von α^g: oBdA r_α, r_β teilerfremd. Sei $\delta \in \mathbb{Z}/(p)^\times$ Potenz α und Potenz von β: $\delta = \alpha^u = \beta^v$.

$$\left.\begin{array}{l} r_\delta = r_{\alpha^u} \mid r_\alpha \\ r_\delta = r_{\beta^v} \mid r_\beta \end{array}\right\} r_\delta = 1 \Rightarrow 1 = \delta' = \delta$$

Setze $\gamma = \alpha * \beta$. Sei $\gamma^s = 1 \Rightarrow \alpha^s = \beta^{-s}$ Potenz von α und $\beta \Rightarrow \alpha^s = 1 = \beta^s$.
$\Rightarrow r_\alpha \mid s$, $r_\beta \mid s \Rightarrow k \mid s$
$\gamma^k = \alpha^k * \beta^k, \quad k = r_\alpha * t_\alpha, \quad k = r_\beta * t_\beta$
$\gamma^k = (\alpha^{r_\alpha})^{t_\alpha} * (\beta^{r_\beta})^{t_\beta} = 1$

Beweis: 4. Schritt

Annahme: Behauptung falsch.
Dann ist $\forall \alpha \in \mathbb{Z}/(p)^\times : r_\alpha < p - 1$
$\Rightarrow k = \text{kgV}\{r_\alpha | \alpha \in \mathbb{Z}/(p)^\times\} < p - 1$
$\Rightarrow \forall \alpha \in \mathbb{Z}/(p)^\times : \alpha^k - 1 = 0$
d.h.: $\forall \alpha \in \mathbb{Z}/(p)^\times : \alpha$ Wurzel von $X^k - 1$, damit haben wir mehr Nullstellen als Grad. ↯

Der Schritt 4 bedeutet, dass wir eines haben. Es gibt aber iA viele primitive α. Die Struktur ist zyklisch. Nun definieren wir uns einen Homomorphismus von $\mathbb{Z}$ auf die Gruppe ...
[Heiko: Die Domainen habe ich nicht genau genug mitgeschrieben, also Obacht!]
α primitiv, $\varphi : \mathbb{Z} \mapsto \mathbb{Z}/(p)^\times : z \mapsto \alpha^z$ ist ein Gruppenhomomorphismus. Dieser ist surjektiv, weil α primitiv ist.
$\text{Kern}(\varphi) = \mathbb{Z}(p-1)$
$\mathbb{Z}/(p-1) \overset{\cong}{\mapsto} \mathbb{Z}/(p)^\times$: $a + (p-1) \mapsto \alpha^a$ Gruppenisomorphismus (surjektiv + injektiv)
Damit gibt es $\frac{p-1}{2}$ Quadrate, $\frac{p-1}{2}$ nicht-Quadrate.
Sei $\beta \in \mathbb{Z}/(p)^\times$: Ist β Quadrat?
Falls $\beta = \alpha^a$, a gerade, $a = 2b$: $\beta = (\alpha^b)^2$
Falls $\beta = \alpha^a$, a ungerade, $a = 2b + 1$: $\beta = (\alpha^b)^2 * \alpha$
Annahme: $\beta = \gamma^2 \Rightarrow \alpha = (\gamma * (\alpha^b)^{-1})^2$ ↯(α primitiv)
α primitiv $\Rightarrow \alpha$ kein Quadrat
Annahme: $\alpha = \delta^2$, $\alpha^{\frac{p-1}{2}} \underbrace{=}_{p \text{ ungerade}} \delta^{p-1} = 1$ ↯

$\beta = \alpha^a$ ist iA schwer zu lösen, wenn man nur die Eingaben β, α hat! Dies wird als diskreter Logarithmus bezeichnet, es ist ein imminent schwieriges Problem, so schwer, dass es Basis für manch ein kryptographisches Verfahren ist.

Adrien-Marie Legendre[2] (* 18. September 1752 in Paris; Tod: 10. Januar 1833 ebenda) war ein französischer Mathematiker.

Definition 2.5: Legendre-Symbol

p ungerade Primzahl, $a \in \mathbb{Z}$, $p \not| a$

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ quadratischer Rest modulo } p \\ -1 & a \text{ quadratischer Nichtrest modulo } p \end{cases} \quad \text{(Legendre-Symbol)}$$

Mit diesem Symbol kann man rechnen.

Lemma 2.6:

p wie oben

(a) $p \not| a \wedge a \equiv b (\text{modulo } p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(b) Wenn $a + (p)$ in $\mathbb{Z}/(p)^\times$ primitiv. $\Rightarrow \left(\frac{a}{p}\right) = -1$

(c) $p \not| a * b$ $(\Rightarrow p \not| a \wedge p \not| a) \Rightarrow \left(\frac{a*b}{p}\right) = \left(\frac{a}{p}\right) * \left(\frac{a}{p}\right)$

Beweis:

$a + (p) = \alpha^s$, $b + (p) = \alpha^t$, $a * b + (p) = \alpha^{s+t}$

Nachfolgend dasr langangekündigte Reziprozitätsgesetz, der Hauptteil ist (a). Bewiesen werden die einzelnen Teile später (mit Hilfe von Hilfssätzen)

Satz 2.7: Quadratisches Reziprozitätsgesetz

(a) p, q ungerade Primzahlen, $p \neq q$

$$\Rightarrow \left(\frac{p}{q}\right) * \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} * \frac{q-1}{2}} = \begin{cases} +1 & p \text{ oder } q \equiv 1 \text{ (modulo 4)} \\ -1 & p \text{ und } q \equiv 3 \text{ (modulo 4)} \end{cases}$$

(b) Erster Ergänzungssatz: p ungerade Primzahl

$$\Rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(c) Zweiter Ergänzungssatz: p ungerade Primzahl

$$\Rightarrow \left(\frac{2}{p}\right) = (-1)^{p^2-1}8 = \begin{cases} +1 & p \equiv 1, 7 \text{ (modulo 8)} \\ -1 & p \equiv 3, 5 \text{ (modulo 8)} \end{cases}$$

Beispiel:

9533 ungerade Primzahl

Frage: Ist 4785 quadratischer Rest modulo 9533? (4785 = 3*5*11*29)

Da $\left(\frac{\cdot}{\cdot}\right)$ homomorph bezüglich der Multiplikation ist, kann man diese Fragestellung vereinfachen:

[2] http://de.wikipedia.org/wiki/Legendre

$$\left(\frac{4785}{9533}\right) = \left(\frac{3}{9533}\right) * \left(\frac{5}{9533}\right) * \left(\frac{11}{9533}\right) * \left(\frac{29}{9533}\right)$$

$$\left(\frac{3}{9533}\right) * \left(\frac{9533}{3}\right) = (-1)^{\frac{9533-1}{2} * \frac{3-1}{2}} = +1$$

$$\Rightarrow \left(\frac{3}{9533}\right) = \left(\frac{9533}{3}\right) = \left(\frac{2}{3}\right) = \boxed{\text{-1}}$$

$$\left(\frac{5}{9533}\right) * \left(\frac{9533}{5}\right) = (-1)^{\frac{9533-1}{2} * \frac{5-1}{2}} = +1$$

$$\Rightarrow \left(\frac{5}{9533}\right) = \left(\frac{9533}{5}\right) = \left(\frac{3}{5}\right) = \boxed{\text{-1}}$$

$$\left(\frac{11}{9533}\right) = \left(\frac{9533}{11}\right) = \left(\frac{7}{11}\right)$$

$$\left(\frac{7}{11}\right) * \left(\frac{11}{7}\right) = -1$$

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2}{7}\right)^2 = \boxed{\text{-1}}$$

$$\left(\frac{29}{9533}\right) * \left(\frac{9533}{29}\right) = +1$$

$$\Rightarrow \left(\frac{29}{9533}\right) = \left(\frac{9533}{29}\right) = \left(\frac{21}{29}\right) = \underbrace{\left(\frac{3}{29}\right)}_{=-1} * \underbrace{\left(\frac{7}{29}\right)}_{=+1} = \boxed{\text{-1}}$$

$$\Rightarrow \left(\frac{4785}{9533}\right) = +1 \Rightarrow 4785 \text{ ist quadratischer Rest (modulo 9533)}$$

Unser Problem: Wir brauchen Primzahlen, verallgemeiner läßt sich dieses Verfahren aber zum Jakobi-Symbol (wo dann nur noch gefordert ist, daß ggT = 1. Dieses hat aber eine andere Interpretation (wenngleich wir in der gleichen Arithmetik damit arbeiten können).

Wenn $\epsilon, \delta \in \{+1, -1\}$ und $\epsilon \equiv \delta$ (modulo p ungerade), dann gilt $\epsilon = \delta$.

Satz 2.8: Euler-Kriterium

p ungerade Primzahl, $p \not| a$.

Dann gilt $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (modulo p)

Beweis:

Sei α primitive Klasse modulo p. $a + (p) = \alpha^r$

$\left(\frac{a}{p}\right) = \begin{cases} +1 & r \text{ gerade} \\ -1 & r \text{ ungerade} \end{cases}$

$(a + (p))^{\frac{p-1}{2}} = \alpha^{r * \frac{p-1}{2}}$

Falls r gerade, etwa $2 * s$: $\alpha^{r * \frac{p-1}{2}} = (\alpha^{p-1})^s = 1 + (p)$

Falls r ungerade, etwa $2 * s + 1$: $\alpha^{r * \frac{p-1}{2}} = \alpha^{\frac{p-1}{2}} = -1 + (p)$

Der 1. Ergänzungssatz folgt sofort, für den Rest brauchen wir noch das Gauß'sche Lemma.
Als erste Anwendung des Gauß'schen Lemmas, beweisen wir den 2. Ergänzungssatz.
Die verquere Beweisfolge liegt daran, daß uns mehrfach die Zeit ausging...

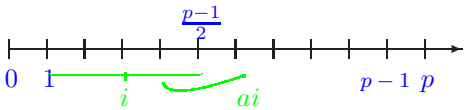
Beweis: 2.7 (b)

Wegen Euler-Kriterium gilt: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ modulo p

$(-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1(\text{modulo } 4) \\ -1 & p \equiv 3(\text{modulo } 4) \end{cases}$

$\Rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Lemma 2.9: Gauß'sches Lemma



p ungerade Primzahl, $a \in \mathbb{Z}$, $p \not| a$. Definiere:

$M = \{i | 1 \leq i \leq \frac{p-1}{2} \wedge (\exists k \in \mathbb{Z} : \frac{p-1}{2} < ai - rp \leq p-1)\}$

$\Rightarrow \left(\frac{a}{p}\right) = (-1)^{|M|}$

Beweis: 2.7 (c)

Gauß'sches Lemma mit $a = 2$: $\{1, ..., \frac{p-1}{2}\}$

$\{2 * 1, ..., 2 * \frac{p-1}{2}\}$ (Division mit Rest hier unnötig)

Wieviele Zahlen $2j$ liegen in $\{\frac{p-1}{2} + 1, ..., p-1\}$?

Wenn $\frac{p-1}{2}$ ungerade ist ($p \equiv 3$ modulo 8, oder $p \equiv 7$ modulo 8).

Damit sind $\frac{p-1}{2} + 1, \frac{p-1}{2} + 3, ..., p-1$ gerade Zahlen.

Die Anzahl dieser ist: $\frac{p+1}{4}$

Wenn $\frac{p-1}{2}$ gerade ist ($p \equiv 1$ modulo 8, oder $p \equiv 5$ modulo 8).

Damit sind $\frac{p-1}{2} + 2, \frac{p-1}{2} + 4, ..., p-1$ gerade Zahlen.

Die Anzahl dieser ist: $\frac{p-1}{4}$

Mit Gauß:

Für $p \equiv 3, 7$ modulo 8: $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}} = \begin{cases} -1 & 3 \\ +1 & 7 \end{cases}$

Für $p \equiv 1, 5$ modulo 8: $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} = \begin{cases} +1 & 1 \\ -1 & 5 \end{cases}$

Lemma 2.10: Gauß'sches Lemma

p ungerade Primzahl, $a \in \mathbb{Z}$, $\neg(p \mid a)$

$M = \{i | 1 \leq i \leq \frac{p-1}{2} \wedge \exists k \in \mathbb{Z} : \frac{p-1}{2} < a \cdot i - k \cdot p \leq p-1\}$

$\Rightarrow (\frac{a}{p}) = (-1)^{|M|}$

Beweis:

$\alpha := a + (p) \in \mathbb{Z}/(p)^\times$

$\widehat{\alpha} : \mathbb{Z}/(p)^\times \to \mathbb{Z}/(p)^\times : \beta \mapsto \alpha \cdot \beta$

Setze $N = \{1, ..., \frac{p-1}{2}\}$ M

Für $j \in N$: $s(j)$ Divisionsrest von $(a \cdot j)$ $mod(p)$

$\Rightarrow 1 \leq s(j) \leq \frac{p-1}{2}$

Für $j \in M$: r(j) Divisionsrest von $(a \cdot j)$ $mod(p)$

$\Rightarrow \frac{p-1}{2} < r(j) \leq p-1$

Erweiterung von $s : N \to \{1, ..., \frac{p-1}{2}\}$ zu

$s' : N \dot{\cup} M = \{1, ..., \frac{p-1}{2}\} \to \{1, ..., \frac{p-1}{2}\}$:

$s'(j) = \begin{cases} s(j) & , j \in N \\ p - r(j) & , j \in M \end{cases}$

$\Rightarrow 1 \leq s'(j) \leq \frac{p-1}{2}$

Behauptung: $\{s'(j)|1 \leq j \leq \frac{p-1}{2}\} = \{1, ..., \frac{p-1}{2}\}$

Beweis:

Injektivität von $s' : \{1, ..., \frac{p-1}{2}\} \to \{1, ..., \frac{p-1}{2}\}$
Es gilt drei Fälle zu unterscheiden.
1. Fall
$\forall j, k \in N : s'(j) = s'(k) \Rightarrow s(j) = s(k)$
$\Rightarrow \widehat{\alpha}(j + (p)) = \widehat{\alpha}(k + (p)) \Rightarrow \widehat{\alpha}$ ist injektiv $\Rightarrow j + (p) = k + (p) \Rightarrow j = k$
2. Fall
$\forall j, k \in M : s'(j) = s'(k) \Rightarrow r(j) = r(k)$
Analog zu Fall 1.
3. Fall
$j \in N, k \in M$, $s'(j) = s'(k)$
$a \cdot j = s(j) + u \cdot p = s'(j) + u \cdot p$, $(u \in \mathbb{Z})$
$a \cdot k = r(k) + v \cdot p = -s'(k) + (v + 1) \cdot p$, $(v \in \mathbb{Z})$
$a \cdot (j + k) = \underbrace{(s'(j) - s'(k))}_{=0} + (u + v + 1) \cdot p$
$\Rightarrow p \mid a \cdot (j + k)$
$\Rightarrow p \mid a \lightning \vee p \mid j + k$
$\Rightarrow p \leq j + k$
$\left.\begin{array}{l} j \leq \frac{p-1}{2} \\ k \leq \frac{p-1}{2} \end{array}\right\} \Rightarrow j + k \leq p - 1 \Rightarrow p \leq p - 1 \lightning$
Nun haben wir gezeigt das s' injektiv ist. Somit in diesem Fall auch surjektiv.

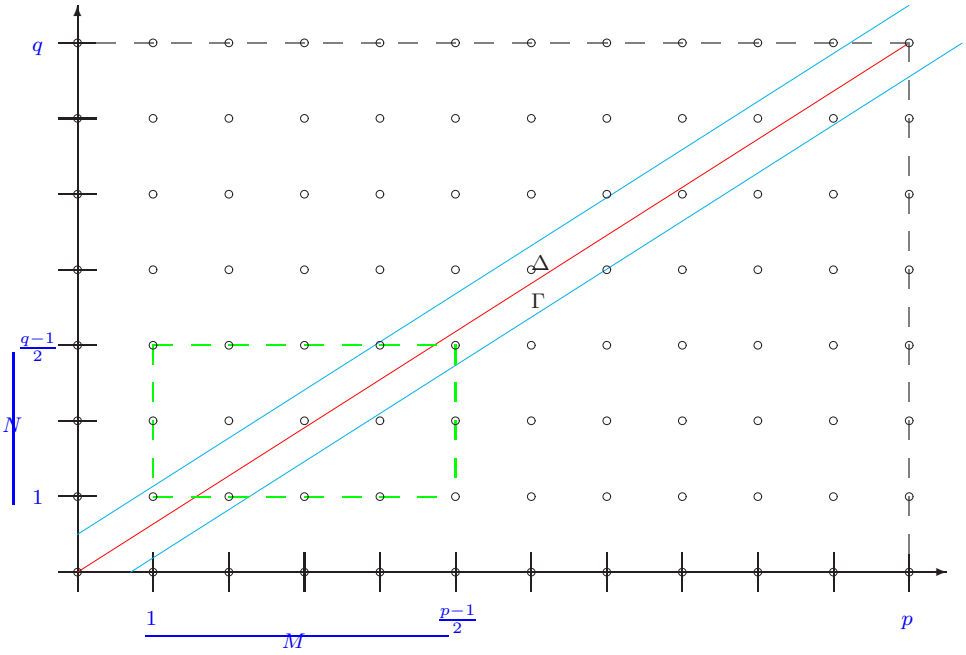
Damit erhalten wir:
$\prod_{i=1}^{\frac{p-1}{2}} i = \prod_{i=1}^{\frac{p-1}{2}} s'(i)$
$a^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j = \prod_{j=1}^{\frac{p-1}{2}} a \cdot j \equiv \prod_{j \in N} s(j) \prod_{j \in M} r(j) = \prod_{j \in N} s'(j) \prod_{j \in M} p - s'(j) \equiv$
$\equiv (-1)^{|M|} \cdot \prod_{j \in N} s'(j) \prod_{j \in M} s'(j) = (-1)^{|M|} \cdot \prod_{j=1}^{\frac{p-1}{2}} s'(j)$ (mod p)
Kürze mod(p) mit $\prod_{j=1}^{\frac{p-1}{2}} j$: $\underbrace{a^{\frac{p-1}{2}}}_{\equiv (\frac{a}{p})(SatzvonEuler)} \equiv (-1)^{|M|}$ (mod p)
$\Rightarrow (\frac{a}{b}) = (-1)^{|M|}$
q.e.d.

Satz 2.11: Reziprozitätsgesetz

p, q ungerade Primzahlen $p \neq q$
$\Rightarrow (\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Beweis:

$M = \{i|1 \leq i \leq \frac{q-1}{2} \wedge \exists k \in \mathbb{Z} : \frac{q-1}{2} < p \cdot i - k \cdot q \leq q - 1\}$
$\lambda = |M| \Rightarrow (\frac{p}{q}) = (-1)^{\lambda}$
$N = \{j|1 \leq j \leq \frac{p-1}{2} \wedge \exists l \in \mathbb{Z} : \frac{p-1}{2} < q \cdot j - l \cdot p \leq p - 1\}$
$\mu = |N| \Rightarrow (\frac{q}{p}) = (-1)^{\mu}$
Für $i \in M : \alpha(i)$ ist die Zahl mit $\frac{q-1}{2} < p \cdot i - \alpha(i) \cdot q \leq q - 1$
Für $j \in N : \beta(j)$ ist die Zahl mit $\frac{p-1}{2} < q \cdot j - \beta(i) \cdot p \leq p - 1$
Behauptung: $0 \leq \alpha(i) \leq \frac{p-3}{2}$
(Analog zeigt man $0 \leq \beta(j) \leq \frac{q-3}{2}$)
$p \cdot i - \alpha(i) \cdot q \leq q - 1 < q$
$\Rightarrow 0 < p \cdot i < (\alpha(i) + 1) \cdot q$
$\Rightarrow \alpha(i) + 1 \geq 1 \geq 0$
Annahme: $\alpha(i) \geq \frac{p-1}{2}$
$1 \leq i \leq \frac{q-1}{2} \Rightarrow p \leq p \cdot i \leq p \cdot \frac{q-1}{2}$
$p \cdot i - q \cdot \alpha(i) \leq p \cdot \frac{q-1}{2} - q \cdot \frac{p-1}{2} = \frac{pq}{2} - \frac{p}{2} - \frac{pq}{2} + \frac{q}{2} = \frac{q-p}{2} < \frac{q-1}{2} \lightning$



$L = \{\langle x, y\rangle \in \mathbb{Z} \times \mathbb{Z} | x \in M, y \in N\}$
$\varphi : M \to L : i \to (\alpha(i) + 1, i)$, $\Gamma := \varphi(M)$
$\psi : N \to L : j \to (j, \beta(j) + 1)$, $\Delta := \psi(N)$
Behauptung:
$\Gamma = \{(x, y) \in L | 0 < q \cdot x - p \cdot y \leq \frac{q-1}{2}\}$
$\Delta = \{(x, y) \in L | 0 < p \cdot y - q \cdot x \leq \frac{p-1}{2}\}$
$q \cdot x - p \cdot y = 0$ (Gerade: $y = \frac{q}{p} \cdot x$)
$q \cdot x - p \cdot y = \frac{q-1}{2}$ (Gerade: $y = \frac{q}{p} \cdot x - \frac{q-1}{2p}$)
Beweis für Γ
Sei $(x, y) \in \Gamma$, etwa $\varphi(i) = (x, y)$, $i \in M$
$\frac{q-1}{2} < p \cdot i - \alpha(i) \cdot q \leq q - 1$
$-\frac{q+1}{2} < p \cdot i - (\alpha(i) + 1) \cdot q + 1 \leq 0$
$0 < (\alpha(i) + 1) \cdot q - p \cdot i < \frac{q-3}{2} < \frac{q-1}{2}$
$\Rightarrow (\alpha(i) + 1, i) \in \Gamma$
Sei nun (x, y) ganzzahlig $\in L$, $0 < q \cdot x - p \cdot y \leq \frac{q-1}{2}$
$?x = \alpha(y) + 1$?
$-\frac{q+1}{2} < -\frac{q-1}{2} \leq p \cdot y - q \cdot x < 0$
$\Rightarrow \frac{q-1}{2} < p \cdot y - q \cdot (x - 1) \leq q - 1$
$\Rightarrow y \in M$, $\alpha(y) = x - 1$
$E = \Gamma \triangle \Delta$
$|E| = \underbrace{|\Gamma| + |\Delta|}$
verschiedene Seiten der Geraden
$|\Gamma| = |M| = \lambda$, $|\Delta| = |N| = \mu$
Definiere γ: $E \to \mathbb{Z}^2$: $(x, y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$
$1 \leq x \leq \frac{p-1}{2} \Rightarrow 1 \leq \frac{p+1}{2} - x \leq \frac{p-1}{2}$
$1 \leq \frac{q+1}{2} - y \leq \frac{q-1}{2}$
Behauptung: $\gamma(x, y) \in E$
$(x, y) \in \Gamma$, d.h. $-\frac{p-1}{2} < q \cdot x - p \cdot y \leq \frac{q-1}{2}$
d.h. $-\frac{p-1}{2} \leq q \cdot (\frac{p+1}{2} - x) - p \cdot (\frac{q+1}{2} - y) \leq \frac{q-1}{2}$??
Das mittlere ergibt:
$\frac{q-p}{2} - qx + py$
$\frac{q-p}{2} - \frac{q-1}{2} = -\frac{p-1}{2} \Rightarrow$ untere Abschätzung
$\frac{q-p}{2} + \frac{p-1}{2} = \frac{q-1}{2} \Rightarrow$ obere Abschätzung
$\gamma^2 = id_E \Rightarrow \gamma$ bijektiv
$z, t \in E$

$z\ t$, falls $z = t$ oder $\gamma(z) = t$
Das ist eine Äquivalenzrelation.
Menge der Äquivalenzklassen: $\overline{E}$
$E = \dot{\cup}_{C \in \overline{E}} C$
$\Rightarrow |E| = \sum_{C \in \overline{E}} |C|$
$\forall C \in \overline{E} : |C| = 1 \vee |C| = 2$
Falls $|C| = 1$: $(x, y) = C$

$$\left.\begin{array}{l} x = \frac{p+1}{2} - x \\ y = \frac{q+1}{2} - y \end{array}\right\} \Rightarrow \begin{array}{l} x = \frac{p+1}{4} \\ y = \frac{q+1}{4} \end{array} \in \mathbb{Z}$$

$$\Rightarrow \begin{array}{l} p \equiv 3 mod(4) \\ q \equiv 3 mod(4) \end{array}$$

Falls $p \equiv 1 mod(4)$ oder $q \equiv 1 mod(4)$:
$|E|$ gerade, d.h. $(-1)^{|E|} = +1$
Falls $p \equiv 3 mod(4)$ und $q \equiv 3 mod(4)$:
$|E|$ ungerade, d.h. $(-1)^{|E|} = -1$

3.3 Primzahltests

Einführung

Dieses Kapitel behandeln wir nicht erschöpfend, es gibt weitaus mehr, wirklich viel mehr darüber zu sagen. Es gibt hierzu eine spezielle Vorlesung "Primzahlen".
Die grundlegende Fragestellung ist die folgende:
$x \in \mathbb{N}$. Ist x Primzahl?
Diese Fragestellung hat weitreichende Konsequenzen, unter anderem basiert das RSA-Verfahren (Kryptographie) darauf, daß aus zwei sehr großen Primzahlen das Produkt gebildet wird und dieses ohne Gefahr veröffentlicht werden kann.
Es gibt ausser den hier vorgestellten auch definitive Verfahren, diese behandeln wir hier aber nicht.

Der einfachste Test

Der einfachste Test ist es natürlich, alle (Prim-)zahlen von 2 bis $\sqrt{x}$ auf Teilerfremdheit mit x zu prüfen. Bei genügend großen Primzahlen ist dieses Verfahren aber illusorisch schlecht.
Es reicht bis zu $\sqrt{x}$ zu testen, da für alle x gilt: $x = a * b \Rightarrow a \leq \sqrt{x} \vee b \leq \sqrt{x}$

Der Fermat-Test

Ein einfaches (semi-nichtentscheidbares) Verfahren für einen solchen Test, das schneller ist, basiert auf den kleinen Fermat'schen Satz: Sei n ungerade Primzahl, $1 \leq a \leq n-1$. Dann ist $a^{n-1} \equiv 1$ (modulo n)

Primzahltest
Gegeben: ungerade natürliche Zahl n
Aufgabe: Ist n Primzahl?

Verfahren:
Wähle zufälliges a mit $2 \leq a \leq n-1$.

(a) Berechne $g = \mathrm{ggT}(a, n)$
Falls $g \neq 1$: n keine Primzahl
Falls $g = 1$: n eventuell Primzahl

(b) Berechne $m = a^{n-1}$ (modulo n)
Falls $m \not\equiv 1$: n keine Primzahl
Falls $m \equiv 1$: n eventuell Primzahl

(c) Falls n eventuell Primzahl, iteriere das Verfahren mit anderen a.

Dieser Test ist kein definitiver Test; wenn man ihn hierzu missbrauchen will, ist er schlecht.

Carmichael-Zahlen

N keine Primzahl, für a mit $\mathrm{ggT}(a, N) = 1$ ist $a^{N-1} \equiv 1$ (modulo N)
Dies ist sehr schlecht für den Fermat-Test, man stelle sich zwei sehr große Primzahlen p, q vor mit $N = p * q$ und $p \neq q$.

Wie hoch ist die Wahrscheinlichkeit, daß der ggT-Test fehlschlägt (= Keine Entscheidung)?

a, N teilerfremd $\Leftrightarrow a + (N) \in \mathbb{Z}/(p)^\times$
$|\mathbb{Z}/(p)^\times| = \varphi(N) = (p-1)(q-1)$: Anzahl teilerfremder Zahlen
$(p * q - 1) - (p-1)(q-1) = p + q - 2$: Anzahl nicht-teilerfremder Zahlen

Relativer Anteil: $\frac{p+1-2}{p*q-1}$ sehr gering

Anmerkung: Es gibt nicht besonders viele, aber unendlich viele Carmichael-Zahlen. Bei einer Carmichael-Zahl ist mit dem Fermat-Test nicht (realistisch) feststellbar, ob eine Zahl x eine Primzahl ist.

Der Euler-Test

Verfahren:
Wähle zufälliges a mit $2 \leq a \leq n-1$.

(a) Berechne $g = \text{ggT}(a, n)$
Falls $g \neq 1$: n keine Primzahl
Falls $g = 1$: n eventuell Primzahl

(b) Berechne $e = a^{\frac{n-1}{2}} \in \{+1, -1\}$ (modulo n)
Falls $e \not\equiv \left(\frac{a}{n}\right)$: n keine Primzahl
Falls $e \equiv \left(\frac{a}{n}\right)$: n eventuell Primzahl

(c) Falls n eventuell Primzahl, iteriere das Verfahren mit anderen a.

Anmerkung: Es gibt bei diesem Verfahren keine "Carmichael-Zahlen", man kann sogar die Fehlerwahrscheinlichkeit beliebig klein wählen und so lange iterieren, bis diese erreicht ist. Dies ist ein probalistischer Test.

Nun haben wir aber ein **Problem:** Das Legrende-Symbol ist nur für prime n definiert, hier brauchen wir es aber für beliebige. Daher definieren wir nachfolgend das Jacobi-Symbol (gleiche Notation wie das Legrende-Symbol).
Für a, b teilerfremd, b ungerade, $b = \prod_{i=1}^{k} p_i^{r_i}$ gilt:

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{r_i}$$

Nun haben wir ein neues Problem: Wir haben für das Jacobi-Symbol haben wir noch keine Rechenregeln. Es gibt aber ein identisch formuliertes Reziprozitätsgesetz wie beim Legrende-Symbol. Daher brauchen wir auch keine explizite Primfaktorzerlegung, die aber für eine vernünftige Definition unabdingbar ist:

$$\left(\frac{a}{b}\right) * \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} * \frac{b-1}{2}}$$

3.4 Darstellung natürlicher Zahlen als Quadratsummen

Einführung

Gesucht sind die ganzzahligen Lösungen der folgenden Gleichung:

$$x_1^2 + x_2^2 + ... + x_n^2 = a$$

Für $a < 0$: Keine Lösung.
Für $a = 0$: $x_1 = x_2 = ... = x_n = 0$.
Also betrachten wir die Lösungen für $a > 0$. Im reellen ist dies sehr recht einfach lösbar, dieses Problem ist aber auch im ganzzahligen vollständig lösbar.

Zuerst kann man anmerken: Wenn $(x_1, ..., x_n)$ Lösung ist, dann sind alle Variationen von $(\pm x_1, ..., \pm x_n)$ Lösungen (2^n viele). Daher genügt es Lösungen für $\mathbb{N}^n$ zu betrachten.
Definieren wir also für n:

$$M_n := \{a \in \mathbb{N}_1 | \exists x_1, ..., x_n \in \mathbb{N} : a = x_1^2 + ... + x_n^2\}$$

Da 0 für beliebiges x_i erlaubt:

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq M_4 ...$$

M_1: Quadratzahlen
$M_1 \subsetneq M_2$: $5 = 1^2 + 2^2$, $8 = 2^2 + 2^2$, $10 = 1^2 + 3^2$
$M_2 \subsetneq M_3$: $6 = 1^2 + 1^2 + 2^2$, $11 = 1^2 + 1^2 + 3^2$, $12 = 2^2 + 2^2 + 2^2$
$M_4 \subsetneq M_4$: $7 = 1^2 + 1^2 + 1^2 + 2^2$, $15 = 1^2 + 1^2 + 2^2 + 3^2$

Satz 4.1: Satz von Lagrenge (Vier-Quadrate-Satz)

$M_4 = \mathbb{N}$

Lemma 4.2:

Sei p ungerade Primzahl. Dann gilt $\exists x, y, m \in \mathbb{N} : 0 < m < p \wedge 1 + x^2 + y^2 = mp$

Beweis: (nicht detailiert)
$M = \{0, ..., \frac{p-1}{2}\}$
$\varphi : M \mapsto \mathbb{Z}/(P) : x \mapsto x^2 + (p)$
$\psi : M \mapsto \mathbb{Z}/(P) : y \mapsto -1 - y^2 + (p)$
φ, ψ sind injektiv ($\surd$)

$$\left.\begin{array}{l} |\varphi[M]| = \frac{p+1}{2} \\ |\psi[M]| = \frac{p+1}{2} \end{array}\right\} \varphi[M] \cap \psi[M] \neq \emptyset$$

Wähle x, y mit $x^2 + (p) = -1 - y^2 + (p) \Rightarrow 1 + x^2 + y^2 = mp \equiv 0$ (modulo p)
Trivial gilt: $m > 0$, man kann abschätzen: $m < p$.

2. Nachfolgendes wurde sehr hektisch gemacht, ganz korrigieren konnte ich nicht, sehr wahrscheinlich sind Fehler vorhanden

Satz 4.3: M_2

$n \in M_2 \Leftrightarrow$ In der Primzerlegung $n = p_1^{r_1} * ... * p_k^{r_k}$ ist r_i gerade, falls $p_i \equiv 3$ (modulo 4).

Der Beweis ist methodisch interessant und wird noch nachgeschoben.

Satz 4.4: M_3

$n \in M_3 \Leftrightarrow n$ nicht von der Form $4^a(8b+7)$ ist für $a, b \in \mathbb{N}$

Der Beweis hierzu ist schwer und wird nicht gemacht.

Beweis: Satz 4.1

$$\left.\begin{array}{l} a = x_1^2 + x_2^2 + x_3^2 + x_4^2 \\ b = y_1^2 + y_2^2 + y_3^2 + y_4^2 \end{array}\right\} a * b = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

$$\left.\begin{array}{l} z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 = x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2 \\ z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \end{array}\right\} \text{nachrechnen.}$$

$2 = 1^2 + 1^2 + 0^2 + 0^2$

Es genügt also zu zeigen: Ungerade Primzahlen sind Summen von 4 Quadraten.

Mit Lemma 4.2 gilt: $\exists m : 0 < m < p : \exists x, y : 1 + x^2 + y2 = m * p$

Also $\exists 0 < m < p : m * p$ Summe von 4 Quadraten. Wähle m minimal mit dieser Eigenschaft. Behauptung: $m = 1$

Annahme $m \neq 1$:

1. Fall: m gerade $m * p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ entweder 0,2 oder 4 davon ungerade

$x_1 + x_2 + x_3 + x_4$ gerade oder oBda x_1, x_2 gerade oder keiner Gerade.

Es folgt: $x_1 + x_2$; $x_1 - x_2$; $x_3 + x_4$; $x_3 - x_4$ in jedem Fall gerade.

$$\frac{m}{2} * p = \underbrace{\frac{x_1 + x_2}{2}}_{\in\mathbb{N}} + \underbrace{\frac{x_1 - x_2}{2}}_{\in\mathbb{N}} + \underbrace{\frac{x_3 + x_4}{2}}_{\in\mathbb{N}} + \underbrace{\frac{x_3 - x_4}{2}}_{\in\mathbb{N}}$$

↯Widerspruch zu m minimal.

2. Fall: m ungerade, $m \geq 3$ Falls $m \mid x_1, x_2, x_3, x_4$ ↯wegen Minimalität

Also m kein gemeinsamer Teiler von x_1, x_2, x_3, x_4.

Mit Division mit Rest (leicht abgeändert):

$x_i = a_i * m + y_i$; $|y_i| < \frac{m}{2}$

$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4 * (\frac{m}{2})^2 = m^2$

$\underbrace{y_1^2 + y_2^2 + y_3^2 + y_4^2}_{=l*m; 0<l<m} \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0$ (modulo m)

$$\left.\begin{array}{l} p * m = x_1^2 + x_2^2 + x_3^2 + x_4^2 \\ l * m = y_1^2 + y_2^2 + y_3^2 + y_4^2 \end{array}\right\} \text{siehe Anfang } \Rightarrow l * m^2 * p = z_1^2 + z_2^2 + z_3^2 + z_4^2 = m^2 * (l_1^2 + ... + l_4^2)$$

$(x_i = a_i * m + y_i) \Rightarrow z_1, ..., z_4$ sind Vielfaches von m

$z_i = l_i * m \Rightarrow l * p = l_1^2 + ... + l_4^2$ ↯m minimal

Als letztes kommen noch die Summen von 2 Quadraten, deren Satz härter zu beweisen ist, als der 4-Quadrate Satz. Der Hammer ist aber der 3-Quadrate- Satz, für den alleine schon etwas 3 Wochen einzurechnen wären... Der Beweis des 2-Quadrate-Satzes wird nicht vollständig in allen Einzelheiten durchgenommen.

Satz für M_2 (4.3 nochmal)

$n \in \mathbb{N}$ ist Summe von 2 Quadraten $\Leftrightarrow$ In der Primzerlegung $n = p_1^{k_1} * ... * p_r^{k_r}$ treten alle Primzahlen $p_i \equiv 3$ (modulo 4) mit geradem Exponenten auf.

Definition 4.5: $\mathbb{Z}$ adjungiert i

$\mathbb{Z}[i] := \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$ Ring der ganzen Gauß'schen Zahlen.

Beispiel: $n = a^2 + b^2 = (a + bi)(a - bi)$

$\bar{\cdot} : \mathbb{C} \mapsto \mathbb{C}$: $a + bi \mapsto a - bi$ Konjugation, hat Einschränkung auf $\mathbb{Z}[i]$.

$N : \mathbb{C} \mapsto \mathbb{R} : a + bi = z \mapsto z * \overline{z} = a^2 + b^2$ "Normabbildung"

Dies ist bis auf die Wurzel der euklidischer Abstand in $\mathbb{R}^2$

$N : \mathbb{Z}[i] \mapsto \mathbb{N} \subseteq \mathbb{Z}$ Einschränkung.

$N(zt) = N(z) * N(t)$ Homomorphie-Eigenschaft.

n ist Summe von 2 Quadraten $\Leftrightarrow n \in N[\mathbb{Z}[i]]$

Satz 4.6:

$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

Beweis: um zu sehen, wie die Normabbildung benutzt wird

"$\supseteq$" $\surd$

"$\subseteq$" Sei $z \in \mathbb{Z}[i]^\times$; $1 = zt$;
$1 = N(1) = \underbrace{N(z)}_{\in\mathbb{N}} * \underbrace{N(t)}_{\in\mathbb{N}} \Rightarrow a^2 + b^2 = N(z) = 1$, $z = a + bi$
$\Rightarrow = a = 0; b = \pm 1 \vee b = 0; a = \pm 1$

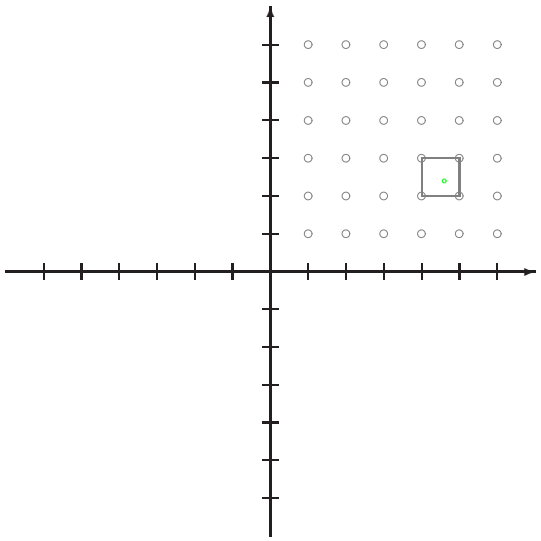
$\mathbb{Z}[i]$ ganz ähnlich zu $\mathbb{Z}$, Euklidischen Algorithmus, Primzahlen, ...
nachfolgend jeweils nur schwach gezeigt (soweit wir es halt brauchen)

Sachen hiernach habe ich mit einigem Abstand getext, hoffentlich mache ich keinen Fehler...
Zuerst beweisen wir, dass $\mathbb{Z}[i]$ ein nicht anordnenbarer euklidischer Ring ist (daher nutzen wir die Norm).

Satz 4.7: Euklidischer Ring

$z, t \in \mathbb{Z}[i]$, $t \neq 0 \Rightarrow \exists q, r \in \mathbb{Z}[i]: z = qt + r \wedge N(r) < N(t)$

Beweis:
$(N(z) < N(t) : \surd)$
Suche $q : N(z - qt) < N(t)$ Ausflug nach $\mathbb{C}$
$N(\frac{z}{t} - q) < N(\frac{t}{t}) = N(1) = 1$



(Es *gibt* eine Ecke mit Abstand < 1 zum Punkt)

Definition 4.8: π Primzahl

$\pi \in \mathbb{Z}[i]$, $\pi \neq 0$, $\pi \notin \mathbb{Z}[i]^\times$
π ist Primzahl, wenn gilt: $\pi \mid u * v \Rightarrow \pi \mid u \vee \pi \mid v$
Primzahl * Einheit = Primzahl (assoziiert)
$a, b \in \mathbb{Z}[i]$ assiziiert, falls es $\epsilon \in \mathbb{Z}[i]^\times$ gibt: $a = \epsilon b$
Partition der Primzahlen (durch Assoziiertheit) - wähle einen Repräsentanten aus jeder Partitionsmenge: Π
Teilweise hier Beweise

Satz 4.9: Hauptidealbereich

Seien $a_1, ..., a_r \in \mathbb{Z}[i] \Rightarrow \exists a \in \mathbb{Z}[i]$: $\mathbb{Z}[i] * a = \mathbb{Z}[i] * a_1 + ... + \mathbb{Z}[i] * a_r$
Vergleiche mit dem ggT in $\mathbb{Z}$.
Euklidischer Ring $\Rightarrow$ Hauptidealbereich $\mathbb{Z}, K[X], \mathbb{Z}[i]$. Es existieren wenige euklidische Ringe.
Das kommt in der Algebra-Vorlesung (aber auch in Computeralgebra!).

Satz 4.10: „Primfaktorzerlegung“

$0 \neq z \in \mathbb{Z}[i] \Rightarrow$ Es gibt eine bis auf die Reihenfolge der Faktoren eindeutige Weise der Darstellung $z = \epsilon\pi_1 * ... * \pi_r$; $\epsilon \in \mathbb{Z}[i]^\times$; $\pi_1, ..., \pi_r \in \Pi$

Beweis: Stichworte
Existenz: Induktion nach der Norm von z

$N(z) \leq n$ ok

$N(z) \leq n+1 \Rightarrow N(z) = n+1$, wenn z Primzahl: hinschreiben. Ansonsten $z = u * v$ (vgl. 4.10)
$N(z) = \underbrace{N(u)}_{\leq n} * \underbrace{N(v)}_{\leq n}$ mit Induktion.

Eindeutigkeit: $z = \epsilon * \pi_1 * ... * \pi_r = \rho * \sigma_1 * ... * \sigma_s$ obDa $r \leq s$
Induktion nach r:
Vorgehen: Einen Faktor wählen, kürzen, Induktionsannahme nutzen.
Siehe auch $\mathbb{Z}$.

Frage: Wie bestimmt man Primzahl in $\mathbb{Z}[i]$?

Lemma 4.11: $\overline{\pi}$ Primzahl

$\pi \in \mathbb{Z}[i]$ Primzahl $\Rightarrow \overline{\pi}$ Primzahl

Lemma 4.12: $N(\pi)$ einfache oder quadrat von Primzahl

$\pi \in \mathbb{Z}[i]$ Primzahl $\Rightarrow N(\pi) = p \vee N(\pi) = p^2$ mit p Primzahl in $\mathbb{Z}$

Beweis:
Sei $\pi * \overline{\pi} = N(\pi) = l * m$, $\text{ggT}(l, m) = 1 \overset{obDa}{\Rightarrow} \pi \mid l \vee \pi \mid m \Rightarrow \overline{\pi} \mid l$ $(l = \alpha * \pi \Rightarrow l = \overline{l} = \overline{\alpha} * \overline{\pi})$
Angenommen $\pi \mid m$: $1 = ul + vm \Rightarrow \pi \mid 1$ ↯
m müsste Einheit sein ↯
$N(\pi) = p^k$, $1 \leq k$
Angenommen $k \geq 3$: $\underbrace{\pi * \overline{\pi}}_{\text{2 Faktoren}} = N(\pi) = \underbrace{p^k}_{\text{min 3 Faktoren}}$ ↯

Lemma 4.13: Primzahlen berechenbar

$p \in \mathbb{N}$ Primzahl, dann ist p Primzahl in $\mathbb{Z}[i]$ oder p ist Produkt von zwei Primzahlen in $\mathbb{Z}[i]$, die zueinander konjugiert sind. (Nur ein Fall asso)
Wenn $p = \alpha * \beta$; $\alpha, \beta \notin \mathbb{Z}[i]^\times$ folgt α, β Primzahlen und zueinander konjugiert. (Damit sind Primzahlen ganz explizit berechenbar)

Beweis:
p keine Primzahl in $\mathbb{Z}[i]$
$p = \alpha * \beta$; $\alpha, \beta \notin \mathbb{Z}[i]^\times$
$p^2 = N(p) = N(\alpha) * N(\beta) \Rightarrow N(\alpha) = p \wedge N(\beta) = p$ (weil p in $\mathbb{Z}$ Primzahl)
$\Rightarrow p = \alpha * \overline{\alpha} = \beta * \overline{\beta}$
Behauptung α Primzahl, Annahme nicht: $\alpha = \alpha' * \alpha''$ $p = N(\alpha) = \underbrace{N(\alpha')}_{\neq 1} * \underbrace{N(\alpha'')}_{\neq 1}$ ↯

(... noch nachpolieren - keine Zeit, qed)

Satz 4.14: Fälle für p Primzahl

$p \in \mathbb{Z}$ Primzahl, nachfolgendes alle Fälle für Primzahlen in $\mathbb{Z}[i]$:

$$\begin{cases} p = 2 & 2 = \overbrace{(1+i)(1-i)}^{\text{Einziger Fall wo assoziiert ist}} = -i(1+i)^2 = N(1+i) \\ p \equiv 3 \mod 4 & p \text{ ist Primzahl in } \mathbb{Z}[i], N(p) = p^2 \\ p \equiv 1 \mod 4 & p = \underbrace{N(a+bi)}_{\text{größte Quadratzahl oft Realteil}} \quad \text{mit } 0 < |b| < a \end{cases}$$

Beweis:

(quadr. Reziproz.)

Fall 1: $\surd$

Fall 2: **Annahme p keine Primzahl:**
$\Rightarrow \exists \pi \in \mathbb{Z}[i]$ Primzahl: $p = \pi * \overline{\pi}$
$\pi = \alpha + \beta i \Rightarrow p = \alpha^2 + \beta^2$; $0 < \alpha, \beta < p$
In $\mathbb{Z}/(p)$: $\alpha^2 + (p) = -\beta^2 + (p) \Rightarrow \left(\frac{\alpha}{\beta}\right)^2 + (p) = (-1) + (p)$
$\Rightarrow \left(\frac{-1}{p}\right) = +1$ ↯(1. Ergänzungssatz zur Quadratischen Reziprozität)

Fall 3: nicht gemacht (wieder 1. Ergänzungssatz)

Der erste Ergänzungssatz hilft uns die Primzahl hier zu finden, er ist von einer ganz starken strukturellen Bedeutung.
(Annahme irgendeine PZ: PZ oder PZ^2 ...)

Als krönender Abschluss beweisen wir nun noch den Zwei-Quadrate-Satz:

Beweis: Zwei-Quadrate-Satz

„$\Rightarrow$“ $a = p_1^{k_1} * ... * p_r^{k_r}$;
$p_1, ..., p_s \equiv 3 \mod 4$;
$p_{s+1}, ..., p_r \not\equiv 3 \mod 4$;
$k_i = 2 * l_i$ für $i = 1, ..., s$
Für $i = 1...s$ gilt: $p_i^{k_i} = p_i^{2l_i} = N(p_i^{l_i})$.
Für $i = s+1...r$ gilt: $p_i = N(\pi_i)$.
Gemeinsam folgt: $a = N(p_1^{l_1} * ... * p_s^{l_s} * \pi_{s+1}^{k_{s+1}} * ... * \pi_r^{k_r}$

„$\Leftarrow$“ Sei $a = N(x) = N(\pi_1^{k_1} * ... * \pi_r^{k_r}) = N(\pi_1^{k_1}) * ... * N(\pi_r^{k_r})$
(entweder PZ oder quad. PZ)
$\Rightarrow N(\pi) = p^2, p$

Quintessenz - nicht leserlich *seufz*