Vorlesung Algebra und Zahlentheorie und ihre Didaktik.

Kapitel I Die natürlichen Zahlen.

I.1. Geschichte

- Ein paar Ausführungen zur Geschichte der natürlichen Zahlen.
  - Mengen zu vergleichen (einzeln – viele, gleichviele) ist schon im Tierreich zu finden. (Küken)
  - Mit der Sesshaftigkeit (Ackerbau und Viehzucht) wuchs das Bedürfnis nach genaueren Angaben von Beziehungen zwischen Quantitäten
    ⇝ Das Verständnis von natürlichen Zahlen (vor 10000 Jahren)
  - Notwendigkeit und Forscherdrang
    ⇝ elementare Zahlentheorie (Pythagoras, Euklid)

I.2. Peano-Axiome

Es seien
- S eine Menge
- $\mathbb{C}$ eine Menge mit $S \subseteq \mathbb{C}$
- $0 \in \mathbb{C}$
- $()^* : S \longrightarrow \mathbb{C}$ eine Abbildung

Wir bezeichnen s^* als den Nachfolger von s.
Die Peano-Axiome sind die folgenden:

(P1) $0 \in S$

(P2) Für jedes $s \in S$ ist der Nachfolger auch ein Element von S

(P3) 0 hat keinen Nachfolger

(P4) $s_1^* = s_2^* \Rightarrow s_1 = s_2$
(Injektivität der Abbildung $()^*$)

(P5) Für $T \subseteq S$ gilt das Induktionsprinzip, d.h. aus

- $0 \in T$ und
- $t \in T \Rightarrow t^* \in T$

folgt $T = S$.

Bem: 1) Es gibt ein Modell für die Peano-Axiome.

Bsp: Die kleinste (bzgl. $\subseteq$) Teilklasse K von $\mathbb{V}$, die
- $\emptyset$ enthält und
- die das folgende erfüllt:
  $x \in K \Rightarrow x \cup \{x\} \in K$.

Wir nehmen jetzt einfach ein Modell $(S, ()^*, 0)$ und bezeichnen dieses einfach mit $(\mathbb{N}_0, ()^*, 0)$. $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$ heißt die Menge der natürlichen Zahlen.

Satz 1:
Prinzip der vollständigen Induktion:

Es sei $(A(n))_{n \in \mathbb{N}_0}$ eine Folge von Aussagen, sodass
1) (Induktionsanfang) $A(0)$ gilt, und
2) (Induktionsschritt) $A(n^*)$ gilt, wenn $A(n)$ gilt.

Dann gilt $A(n)$ für alle $n \in \mathbb{N}_0$.

Beweis: Setze $T := \{n \in \mathbb{N}_0 \mid A(t) \text{ ist wahr}\}$
Dann haben wir: $0 \in T$
$t \in T \Rightarrow t^* \in T$
Aus dem Induktionsprinzip (PS) folgt $T = \mathbb{N}_0$ □

Die einfachste Anwendung von Satz 1 ist
Satz 2: Jedes Element aus $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$ ist ein Nachfolger eines Elementes aus $\mathbb{N}_0$.

Bew.: $A(n) :=$ "Wenn $n \neq 0$, dann ist n Nachfolger eines Elementes von $\mathbb{N}_0$"

(IA) $A(0)$ ist wahr, da 0 nicht ungleich 0 ist.

(IB) IV: Es sei $A(n)$ wahr.
IB: $A(n^*)$ ist wahr.
Bew.: n^* ist der Nachfolger von n, also ist $A(n^*)$ wahr. □

(Hier haben wir die Induktionsvoraussetzung nicht gebraucht.)

Satz 1 $\Rightarrow$ $A(n)$ stimmt für alle $n \in \mathbb{N}_0$ $\square$

I 3 Strukturen auf $\mathbb{N}_0$

Ⓐ **Addition** Wir suchen eine Abbildung

$+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ mit den uns vertrauten Eigenschaften.

Def 3: a) $n + 0 := n$ und b) $n + m^* := (n+m)^*$

Dies definiert eine Abbildung $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, da

1) $n + m^*$ wohldefiniert ist, da m^* nach (P4) keinen zweiten Vorgänger hat, und
2) $+$ nach Satz 2 für alle Elemente aus $\mathbb{N}_0 \times \mathbb{N}_0$ definiert ist, und
3) die Bilder nach (P2) in $\mathbb{N}_0$ liegen.

(Das ist die halbe Wahrheit, siehe Serie 1 Aufgabe 2.)

Satz 4: $+$ ist kommutativ

Der Beweis benötigt ein Lemma

Lemma 5: Für alle $n, m \in \mathbb{N}_0$ gilt $n^* + m = (n+m)^*$.

Bew: mittels vollst. Induktion über m bei festem n.

(IA): $m = 0$: $n^* + 0 \underset{3a)}{=} n^* \underset{3a)}{=} (n+0)^*$

(IS) IV: $n^* + m = (n+m)^*$

IB: $n^* + m^* = (n + m^*)^*$

Bew.: $n^* + m^* \underset{3c)}{=} (n^* + m)^* \underset{IV}{=} ((n+m)^*)^*$

$\underset{3c)}{=} (n + m^*)^*$ □

Satz 1 $\Rightarrow$ Beh. von Lemma 5. □

Bew von Satz 4:

Teil 1: Wir zeigen durch vollst. Induktion
$n + 0 = 0 + n$.

(IA) $0 + 0 = 0$

(IS) $n^* + 0 \underset{3a)}{=} n^* \underset{3a)}{=} (n+0)^* \underset{IV}{=} (0+n)^*$

$\underset{3b)}{=} 0 + n^*$

Teil 2: Wir beweisen Satz 4 durch vollst. Induktion nach m.

$A(m) :=$ "Für alle $n \in \mathbb{N}_0$ gilt $n+m = m+n$."

(IA) $A(0)$ ist wahr nach Teil 1.

(IS) IV: $A(m)$ ist wahr
IB: $A(m^*)$ — " — .

Bew: $n + m^* \underset{3c)}{=} (n+m)^* \underset{IV}{=} (m+n)^*$

$\underset{Lem\,5}{=} m^* + n$. □

Satz 1 $\Rightarrow$ Beh. □.

Satz 6: + ist assoziativ.

Bew.: ÜA.

Bem: Wir haben $n^* = (n+0)^* \overset{3e)}{=} n + 0^*$

Wir setzen $1 := 0^*$. Damit haben wir $n^* = n+1$.

Weitere Übungsaufgaben: Es seien $n, m \in \mathbb{N}_0$

A1: Wenn $n + m = n$, dann $m = 0$.

A2: Wenn $n + m = 0$, dann $n = m = 0$.
(Vorsicht: Hier wird $n, m \in \mathbb{N}_0$ verwendet. Für ganze Zahlen wäre A2 falsch.)

(M) Multiplikation auf $\mathbb{N}_0$

Def 7: $n \cdot 0 := 0$, $n \cdot m^* := n \cdot m + n$.

Satz 8:
- $\cdot$ ist wohldefiniert.
- $\cdot : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ ist kommutativ, assoziativ und erfüllt mit $+$ die Distributivgesetze: $n(m_1 + m_2) = nm_1 + nm_2$, $(n_1 + n_2)m = n_1 m + n_2 m$.

Bew: Übungsaufgabe auf dem 1. Zettel.

I.4. Ordnungsrelation auf $\mathbb{N}_0$

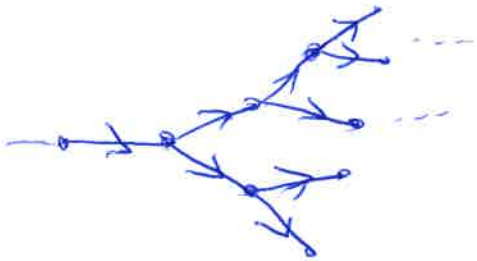
Binäre Relationen spielen zum Beispiel eine Rolle, wenn man

a) Elemente mit einer gleichen Eigenschaft zusammenfassen möchte, oder

b) Elemente anordnen möchte.

Hier interessieren wir uns nur für Ordnungsrelation (Punkt b)). Äquivalenzrelationen (Punkt a)) betrachten wir später.

Bsp: Betrachten wir einen gerichteten Baum



B

$E :=$ Menge der Ecken von B.

R_B sei die folgende Relation:
$e_1 \in E$ soll in Relation zu $e_2 \in E$ stehen, falls der eindeutig bestimmte Pfad von e_1 nach e_2 in Richtung e_2 gerichtet ist.

Hierbei ist ein Pfad von e_1 nach e_2 eine Folge von Ecken

$$e_1 = x_1, x_2, \dots, x_m = e_2$$

so dass für alle $1 \leq i < m$ das Folgende gilt:

- $x_i \neq x_{i+1}$, und
- $x_i \neq x_{i+2}$, falls $i+1 < m$ ist.

Bem: Pedantisch gesehen, haben wir $i < m$ noch garnicht definiert.
→ Das machen wir in diesem Abschnitt.

Def 8: Es sei M eine Menge. Eine Klasse R heißt binäre Relation auf M, falls R eine Teilklasse von $M \times M$ ist.

Es sei nun R eine solche. R heißt

(R1) reflexiv, falls für alle $x \in M$ $(x,x) \in R$ gilt,

(R2) transitiv, falls für alle $x,y,z \in M$ aus $(x,y), (y,z) \in R$ $(x,z) \in R$ folgt.

(R3) antisymmetrisch, falls für alle $x,y \in M$ aus $(x,y), (y,x) \in R$ $x = y$ folgt.

Ordnungsrelation, falls sie (R1) (R2) und (R3) erfüllt, und
totale Ordnungsrelation, falls sie eine Ordnungsrelation ist, in der je zwei Elemente x,y aus M vergleichbar sind, d.h. $(x,y) \in R$ oder $(y,x) \in R$ gilt.

Wir schreiben auch xRy für $(x,y) \in R$.
Man nennt eine Ordnungsrelation auch eine Ordnung, und im totalen Fall Totalordnung

Wir definieren die folgende binäre Relation auf $\mathbb{N}_0$:

$$\leq := \{(n, n+\ell) \mid n, \ell \in \mathbb{N}_0\}$$

also: $n_1 \leq n_2 \iff \exists_{\ell \in \mathbb{N}_0}: n_2 = n_1 + \ell$.

Satz 9: $\leq$ ist eine Totalordnung auf $\mathbb{N}_0$.

Beweis: (ÜA) Hinweis: Nutzen Sie A1 und A2, um die Antisymmetrie zu zeigen.

Für das Adjektiv total fixieren Sie n und zeigen Sie dass

$A(m) :=$ "$m \leq n$ oder $m > n$"

für jedes m wahr ist. □

Def 10: Es sei R eine Ordnung auf M.
Ein Element $x \in M$ heißt größtes (kleinstes) Element bzgl. R, wenn für jedes $y \in M$ $y \leq x$ ($x \leq y$) gilt.

Wir bezeichnen $\mathbb{N}^{\leq n} = \{m \in \mathbb{N} \mid m \leq n\}$
und $\mathbb{N}_0^{\leq n} := \mathbb{N}^{\leq n} \cup \{0\}$.

Wir setzen $1 := 0^*$, $2 := 1^*$, $3 := 2^*$, ...
Das folgende Lemma besagt, dass wir $\mathbb{N}^{\leq n} = \{1, 2, 3, \ldots, n\}$ schreiben können

Lemma 11: Für $x, n \in \mathbb{N}_0$ gilt, wenn $n \leq x \leq n^*$, dann $x = n$ oder $x = n^*$.

Beweis: (ÜA) □

Def 12: Eine ~~nichtleere~~ Menge T heißt endlich falls sie leer ist oder falls ein $n \in \mathbb{N}$ und eine injektive Abbildung $\varphi: T \to \mathbb{N}^{\leq n}$ existieren.

Bem: Die Teilmenge einer endlichen Menge ist endlich.

Satz 13: Es sei T eine nichtleere endliche Menge. Dann existiert ein $m \in \mathbb{N}$ und eine Bijektion $\psi: T \to \mathbb{N}^{\leq m}$. (Wir schreiben auch $T \simeq \mathbb{N}^{\leq m}$.

Bezeichnung: $|T| := m$, $|\emptyset| = 0$. Mächtigkeit von T.

Beweis: (ÜA) Hinweis: Betrachte

$A(n)$ = " Für alle endlichen ~~Teilmengen~~ Mengen T und Injektionen $\varphi: T \to \mathbb{N}^{\leq n}$ gilt die Aussage des Satzes"

Führe eine Induktion nach n und nutze Lemma 11 für den Induktionsschritt. □

Satz 14: Jede endliche nichtleere Teilmenge von $\mathbb{N}_0$ hat ein kleinstes und ein größtes Element.

Bew: (IA) $|T| = 1 \Rightarrow T \simeq \mathbb{N}^{\leq 1} \underset{\text{Lem 11}}{=} \{1\}$

$\Rightarrow T = \{t\} \Rightarrow t$ ist größtes und kleinstes Element von T.

(IS) $|T| = n+1 \Rightarrow T \overset{\varphi}{\simeq} \mathbb{N}^{\leq n+1}$

$\Rightarrow \exists\, t_0 \in T: \varphi(t_0) = n+1$

$\Rightarrow T \setminus \{t_0\} \simeq \mathbb{N}^{\leq n}$

$\exists V \Rightarrow$ $T \setminus \{t_0\}$ hat ein größtes und kleinstes Element.
Vergleiche diese Element mit t_0.
$\Rightarrow$ T hat ein größtes und ein kleinstes Element. □

Satz 15 (Satz vom kleinsten Element)
Es sei $T \subseteq \mathbb{N}_0$ nichtleer. Dann hat T ein kleinstes Element.

Bew.: Wähle ein $n \in T$. Dann ist $n = 0$ oder $T \cap \mathbb{N}^{\leq n}$ eine nichtleere endliche Menge.

In beiden Fällen hat T ein kleinstes Element. Im zweiten Fall wegen Satz 14. □

I 5. Die ganzen Zahlen und Teilbarkeiten

Def 16: $\mathbb{Z} := (\{0,1\} \times \mathbb{N}) \cup \mathbb{N}_0$

Wir setzen die Addition und die Multiplikation von $\mathbb{N}_0$ auf $\mathbb{Z}$ wie folgt fort.

1) $(0,n_1) + (0,n_2) := (0, n_1+n_2)$

$n_2 + (0,n_1) := (0,n_1) + n_2 := \begin{cases} \ell, \text{ o.d. } n_1+\ell = n_2, \\ \quad \text{falls } n_1 \geq n_2 \\ (0,\ell), \text{ o.d. } n_2+\ell = n_1 \\ \quad \text{falls } n_2 < n_1 \end{cases}$

2) $(0,n_1)\cdot n_2 := \begin{cases} (0, n_1 n_2), & \text{falls } n_2 > 0 \\ 0, & \text{falls } n_2 = 0 \end{cases}$

$(0,n_1)(0,n_2) := n_1 n_2$

Satz 17: $(\mathbb{Z}, +, \cdot)$ sind die Strukturen $+$ und $\cdot$ kommutativ und assoziativ, erfüllen die Distributivgesetze

$$z_1(z_2+z_3) = z_1 z_2 + z_1 z_3$$
$$(z_1+z_2)z_3 = z_1 z_3 + z_2 z_3$$

und 0 ist das neutrale Element bzgl. $+$ ($0 + z = z + 0 = z$)
und 1 ist das neutrale Element bzgl. $\cdot$ ($1 \cdot z = z \cdot 1 = z$).

In $\mathbb{Z}$ hat $z \in \mathbb{Z}$ ein eindeutig bestimmtes Inverses bzgl. der Addition. Es ist das Element

$$\begin{cases} n, & \text{falls } z = (0,n) \\ 0, & z = 0 \\ (0,n), & \text{falls } z = n \in \mathbb{N}. \end{cases}$$

Die Totalordnung $\leq$ auf $\mathbb{N}_0$ wird auf die übliche Weise nach $\mathbb{Z}$ zu einer Totalordnung fortgesetzt. Wir schreiben also ab jetzt $-n$ für $(0,n)$ und können nun in $\mathbb{Z}$ rechnen, wie wir es gewohnt sind.

Teilbarkeiten:

Def 18: Wir sagen, dass eine ganze Zahl a eine andere ganze Zahl b teilt $(a \mid b)$ falls eine ganze Zahl c existiert, s.d. $b = c \cdot a$.

Satz 19:
1) $a \mid b$ und $b \mid c \Rightarrow a \mid c$
2) $a \mid b_1$ und $a \mid b_2 \Rightarrow a \mid b_1 + b_2$
3) $a_1 \mid b_1$ und $a_2 \mid b_2 \Rightarrow a_1 a_2 \mid b_1 \cdot b_2$
4) Jedes Element aus $\mathbb{Z}$ teilt 0
5) 0 teilt nur die 0.

Bew: 2) $a \mid b_1 \wedge a \mid b_2 \Rightarrow \exists\, c_1, c_2 \in \mathbb{Z} : a c_i = b_i$

$\Rightarrow a(c_1 + c_2) = a c_1 + a c_2 = b_1 + b_2$

$\Rightarrow a \mid b_1 + b_2$.

Der Rest ist Übungsaufgabe. □

Um uns von $\mathbb{Z}$ auf $\mathbb{N}_0$ zurückbewegen zu können, benötigen wir die Betragsabbildung.

$$|\cdot| : \mathbb{Z} \longrightarrow \mathbb{N}_0 \qquad |a| := \begin{cases} a, & a \in \mathbb{N}_0 \\ -a, & a \notin \mathbb{N}_0. \end{cases}$$

Einschub: **Bem 17:** Es seien $z, z_1, z_2 \in \mathbb{Z}$. Dann gelten

1) $-(-z) = z$

2) $(-z_1)(+z_2) = -z_1 z_2$, $(-z_1)(-z_2) = z_1 z_2$

3) $z < 0 \Leftrightarrow -z > 0$

4) $z_1 > z_2 \Leftrightarrow z + z_1 > z + z_2$

5) Es seien $z_1, z_2 \in \mathbb{N}_0$ und $z \in \mathbb{N}$, dann gilt

$$z_1 z < z_2 z \Leftrightarrow z_1 < z_2$$

Bew.: 1) $+(-z) + z = 0$ ($-z$ additive Inverse von z) $\Rightarrow z$ ist die additive Inverse von $(-z)$

$\Rightarrow -(-z) = z$

2) $(-z_1) z_2 + z_1 z_2 = ((-z_1) + z_1) z_2$ (Distr.)

$= 0 \cdot z_2 = 0$ (add. Inv.)

$\Rightarrow (-z_1) z_2$ ist die additive Inverse von $z_1 z_2$

$\Rightarrow (-z_1) z_2 = -z_1 z_2$

3) $z < 0 \Rightarrow \exists\, s \in \mathbb{N}_0,\ s \neq 0 :\ z + s = 0$

$\Rightarrow \exists_{s \in \mathbb{N}_0,\, s \neq 0} :\ 0 + s = (-z) + z) + s$

$= (-z) + (z + s) = -z + 0 = -z$

$\Rightarrow 0 < -z$

$\Leftarrow$: analog

4) ü.A. (analog zu 3)) 5) ü.A

Differenz: $z_1, z_2 \in \mathbb{Z}$

$$z_1 - z_2 := z_1 + (-z_2)$$

$$= z \text{ mit } z_2 + z = z_1.$$

Bem 19: $\forall z, z_1, z_2 \in \mathbb{C}$:

1) $|z| = 0 \Leftrightarrow z = 0$

2) $|z_1 z_2| = |z_1||z_2|$

3) $|z_1 + z_2| \leq |z_1| + |z_2|$

Beweis: 1) $|0| = 0$, Sei $|z| = 0 \Rightarrow$

$\max\{z, -z\} = 0 \Rightarrow z = 0 \vee -z = 0$

$\Rightarrow z = 0 \vee z = -(-z) = -0 = 0$ (Bem 17) $\Rightarrow z \in 0$

$\Rightarrow -0 = 0$

2) $|z_1 z_2| = |-z_1 z_2| = |(-z_1) z_2|$

$\Rightarrow |z_1 z_2| = \big||z_1| z_2\big| = \big||z_1||z_2|\big| \leq |z_1||z_2|$

(= analog; $\leq$: $|z_1||z_2| \in \mathbb{N}_0$)

3) 1. Fall: $|z_1 + z_2| = z_1 + z_2$

$\Rightarrow |z_1| + |z_2| \geq z_1 + |z_2| \geq z_1 + z_2 = |z_1 + z_2|$

($|z_i| \geq z_i$; Bem 17)

2. Fall $|z_1 + z_2| = -(z_1 + z_2)$:

$\Rightarrow |z_1| + |z_2| = |-z_1| + |z_2| \geq (-z_1) + (-z_2)$ (Fall 1)

$= (-1) z_1 + (-1) z_2$ (Bem 17)

$= (-1)(z_1 + z_2) = -(z_1 + z_2)$. (Distr., Bem 17)

$= |z_1 + z_2|$. ∎

Bem 26: $n, m \in \mathbb{N}$ ... $n \mid m$, etwa $nl = m$ mit $l \in \mathbb{Z}$. Dann

1) $l \in \mathbb{N}$

2) $n \leq m$

Bew.: 1) Ann.: $l \notin \mathbb{N}$ $\overset{\text{Def. von } \mathbb{Z}}{\Rightarrow}$ $-l \in \mathbb{N}$, $\vee\, l = 0$;

$n \neq 0 \Rightarrow l \neq 0$;

Also $-m = n(-l) \in \mathbb{N}_0$

$\Rightarrow$ $m, -m \in \mathbb{N}_0$ und $m + (-m) = 0$

$\overset{\text{A.2}}{\Rightarrow}$ $m = 0$ ↯

2) Aus 1) folgt $l \in \mathbb{N}$.

$\overset{\text{Lemma 11}}{\Rightarrow}$ $l \geq 1 \Rightarrow n = n \cdot 1 \leq n \cdot l = m$ □

Einschub Ende

Satz 20: Jede ganze Zahl $a \neq 0$ hat höchstens $2|a|$ Teiler.

Beweis: 1) Aus $x \mid a$ folgt $|x| \leq |a|$:

$\exists\, y \in \mathbb{Z}: \; xy = a$. Also $|a| = |x||y|$.

$a \neq 0 \Rightarrow y \neq 0 \Rightarrow |y| > 0 \underset{\text{Lem 11}}{\Rightarrow} |y| \geq 1$

$\Rightarrow |y| - 1 \in \mathbb{N}_0$

Also gilt $|a| = |x| + \underbrace{|x|(|y|-1)}_{\in \mathbb{N}_0} \overset{\text{Def}\geq}{\geq} |x|$

2) $0 \neq a$ und 1) $\Rightarrow$ Wir haben folgende Injektion $\{x \mid a \mid x \in \mathbb{Z}\} \hookrightarrow \mathbb{N}_{\leq 2|a|}$

$$x \longmapsto \begin{cases} x, & x > 0 \\ |a| + |x|, & x < 0. \end{cases}$$

□

Wir definieren $T(a) := \{x \in \mathbb{Z} \mid x \mid a\}$

$V(a) := \{x \in \mathbb{Z} \mid a \mid x\}$ $\quad (\mathbb{Z} - \{0\} = \mathbb{Z}^\times)$

Def 21: 1) Für $(a,b) \in (\mathbb{Z} \times \mathbb{Z} - \{0\})^{\mathbb{Z}^\times}$ ist der Schnitt

$T(a) \cap T(b) \cap \mathbb{N}$ eine nichtleere endliche Menge (nichtleer da $1 \in \ldots$). Also besitzt sie ein größtes Element $g = ggT(a,b)$, den <u>größten gemeinsamen Teiler</u>

Wir setzen $ggT(0,0) := 0$.

2) Nach Satz 15 besitzt $V(a) \cap V(b) \cap \mathbb{N}_0$ ein kleinstes Element, das kleinste gemeinsame Vielfache von a und b.

Wir schreiben $\mathrm{kgV}(a,b)$.

Um die Division mit Rest für $\mathbb{Z}$ zu beweisen benötigen wir das Archimedische Axiom, das schon Eudoxus von Knidos bekannt war. Wir formulieren es hier für $\mathbb{N}$.

Satz 22: (Archimedisches Axiom) Es seien n und m natürliche Zahlen. Dann existiert eine natürliche Zahl a, so dass $am > n$.

Bew: Wähle $a = n+1$

$$\Rightarrow \quad am = n + n\cdot 1 + n(m-1) \geq n + n \overset{n>0}{>} n.$$

□

Satz 23: (Division mit Rest)
Für $(z,m) \in \mathbb{Z} \times \mathbb{N}$ gibt es genau ein Paar $(q,r) \in \mathbb{Z} \times \mathbb{N}_0^{\leq m-1}$ für das

die Gleichung $n = qm + r$ gilt.

Bew: Nach Satz 22 gibt es ein $a \in \mathbb{N}$, s.d. $am > |z|$ ist, und wenn die Aussage für $(am+z, m)$ bewiesen ist, so

ist sie auch für (z,m) bewiesen.

Also können wir ohne Einschränkung der Allgemeinheit ($\mathbb{E}$) annehmen, dass z positiv ist.

Nach Satz 22 ist die Menge

$$M := \{ a \in \mathbb{N}_0 \mid (a+1)m > z \}$$

nichtleer. Also existiert $q := \min M$ nach Satz 15.

$$\Rightarrow \quad (q+1)m > z \geq qm. \text{ und}$$

somit $\quad 0 \leq r := z - qm < m.$

Das beweist die Existenz

Eindeutigkeit: (Übungsaufgabe) $\square$

Satz 24 (Lemma von Bézout) Der größte gemeinsame Teiler zweier ganzer Zahlen z_1, z_2 besitzt eine Darstellung der Form

$$ggT(z_1, z_2) = a z_1 + b z_2$$

für geeignete $a, b \in \mathbb{Z}$.

Beweis: Wir führen eine Induktion nach $m := |z_1| + |z_2|$

(IA) $(m=0) \quad \Rightarrow \quad z_1 = z_2 = 0$ und $ggT(z_1, z_2) = 0$.
Wir haben $0 = 1 \cdot 0 + 1 \cdot 0$.

(IS) IV: Die Aussage richtig für alle $m \leq n$.

IB: Die Aussage stimmt für $m = n+1$.

Beweis: 1) Falls $z_1 \mid z_2$, dann haben wir $|z_1| = ggT(z_1, z_2)$

$= a z_1$ für ein $a \in \{\pm 1\}$.

Analog für $z_2 \mid z_1$

2) Nach 1) können wir uns auf $|z_1| > |z_2| \neq 0$ beschränken.

Nach Satz 23 existiert $(q, r) \in \mathbb{Z} \times \mathbb{N}_0^{<|z_2|}$, so dass

$$z_1 = q z_2 + r$$

$$\Rightarrow ggT(z_1, z_2) = ggT(z_2, r) =: t$$

und $|z_1| + |z_2| > |z_2| + |r|$

$\overset{IV}{\Rightarrow} \exists\, a, b \in \mathbb{Z}$:

$$t = a z_2 + b r$$

$$= (a - bq) z_2 + b z_1. \qquad \square$$

Der Beweis des letzten Satzes enthält,

wenn auch versteckt, einen Algorithmus um den ggT zweier ganzer Zahlen zu berechnen und Bézoutkoeffizienten zu ermitteln.

Euklidischer Algorithmus:

Es seien n, m natürliche Zahlen.
(Man kann sich immer auf diesen Fall zurückziehen)
Seke $n_0 := n$ und $m_0 := m$

$$n_0 = q_0 m_0 + r_0 \qquad n_1 := m_0 \quad m_1 := r_0$$
$$n_1 = q_1 m_1 + r_1 \qquad n_2 := m_1 \quad m_2 := r_1$$
$$\vdots$$

Stopp, wenn $r_\ell = 0$.

Gebe m_ℓ aus.

Wir haben $r_0 > r_1 > r_2 > \dots$ und dieser Algorithmus terminiert nach Satz 15.
Angenommen in Zeile ℓ_0, also $r_{\ell_0} = 0$ und $m_{\ell_0} | n_{\ell_0}$

Dann haben wir: $ggT(n_0, m_0) = ggT(n_1, m_1) = \dots$
$= ggT(n_{\ell_0}, m_{\ell_0}) = m_{\ell_0}$.

Bsp: $ggT(1085, 372) = ?$

$$1085 = 2 \cdot 372 + 341$$
$$372 = 1 \cdot 341 + 31$$
$$341 = 11 \cdot 31 + 0$$
$$\Rightarrow ggT(1085, 372) = 31$$

Bézoutkoeffizienten: $31 = -341 + 372 = -1085 + 3 \cdot 372$.
$a = -1$ und $b = 3$ funktionieren.

Primzahlen und der Fundamentalsatz der Arithmetik.

Def 2.5: Eine natürliche Zahl heißt Primzahl, wenn sie genau 2 Teiler in $\mathbb{N}$ hat.

Bem: Nach obiger Def. ist 1 keine Primzahl.

Def 2.5 ist äquivalent zu einer Eigenschaft, die es ermöglicht, den Begriff prim auf andere Zahlbereiche zu verallgemeinern.

Satz 2.6: Es sei n eine natürliche Zahl >1.
Dann sind äquivalent

1° n ist eine Primzahl
2° Für alle $a, b \in \mathbb{Z}$ gilt
$(n \mid ab \Rightarrow n \mid a$ oder $n \mid b)$

Beweis: $2° \Rightarrow 1°$: Es sei $m \overset{\in \mathbb{N}}{}$ ein Teiler von n.

$\Rightarrow \exists \ell \in \mathbb{N}: m\ell = n$

$\overset{2°}{\Rightarrow} n \mid m$ oder $n \mid \ell$

$\overset{\uparrow}{\Rightarrow}$ $m \leq n \leq m$ oder $\ell \leq n \leq \ell$
$m\ell = n$

$\Rightarrow m = n$ oder $(n = \ell$ und $(m-1)n = 0)$

$\overset{\uparrow}{\Rightarrow} m = n$ oder $m - 1 = 0$
$n \neq 0$

$1^\circ \Rightarrow 2^\circ$ Es seien $a, b \in \mathbb{Z}$, s.d. $n \mid ab$.
Im Fall $a=0$ oder $b=0$ wären wir fertig, da $n \mid 0$.
z.z. $n \mid a \vee n \mid b$.
Nach Satz 24 existieren $c, d \in \mathbb{Z}$, s.d.

$$ggT(n,a) = c \cdot n + d \cdot a.$$

Wenn $n \nmid a$, dann muss $ggT(n,a) = 1$ sein, da n nur die Teiler 1 und n in $\mathbb{N}$ hat.

$$\Rightarrow \quad 1 = c \cdot n + da \qquad | \cdot b$$
$$\Rightarrow \quad b = b \cdot c \cdot n + dab$$
$$\Rightarrow \quad n \mid b. \qquad \square$$

$n \mid ab$

Elemente in $\mathbb{Z}$, die 2° erfüllen heißen Primelemente.

Der nächste Satz besagt, dass man jede natürliche Zahl durch Primzahlen beschreiben kann.
Das ermöglicht oft Probleme, die von $\mathbb{N}$ abhängen, in Probleme aufzuteilen, die nur von einer Primzahl abhängen.
Die Idee mathematische Objekte in Objekte zu zerlegen, die nicht mehr weiter zerlegt werden können, zieht sich durch die gesamte Mathematik.

Satz 27: (Fundamentalsatz der Arithmetik)
Jede natürliche Zahl ≥ 2 ist ein Produkt von Primzahlen, und diese Produktdarstellung ist eindeutig bis auf Vertauschung der Faktoren.

Lemma 28: Es sei $n \in \mathbb{N}$ $n \geq 2$. Dann existiert eine Primzahl p, die n teilt.

Beweis: $\{a \in \mathbb{N} \mid a \mid n \text{ und } a \geq 2\}$ ist nichtleer und hat also ein kleinstes Element nach Satz 15.

Beh: p ist eine Primzahl.

Bew: Wenn $m \in \mathbb{N}^{\geq 2}$ p teilt, dann $m \mid n$ und somit $m \geq p$ nach Def. des kleinsten Elementes einer Menge. Also $m \leq p \leq m$

($m \mid p$, Beide $\in \mathbb{N}$, Satz 20.1)

$\Rightarrow m = p$. Also hat p genau 2 Teiler □

Bew von Satz 27: Induktion über n.

(IA) **$n = 2$:** 2 ist eine Primzahl, da in $\mathbb{N}^{\leq 2}$ genau 2 Elemente liegen.

(IS) **IV:** Die Aussage des Satzes gelte für alle $m \leq n$.

IB: Die Aussage gilt für $n+1$.

Bew: Wenn $n+1$ eine Primzahl ist, dann sind wir fertig. Andernfalls ist der kleinste Teiler p von $n+1$ in $\mathbb{N}^{\geq 2}$ eine Primzahl

nach Satz 28. Also $\exists\, m \in \mathbb{N}: 1+n = p\,m \geq 2m = m+m \geq 1+m$
$\Rightarrow m \leq n. \Rightarrow$ m hat eine Primfaktorzerlegung

$$m = p_1 \cdots p_t \quad \Rightarrow \quad 1+n = p \cdot p_1 \cdots p_t$$

<u>Eindeutigkeit</u>: Aus $p \cdot p_1 \cdots p_t = 1+n = p_1' \cdots p_s'$ (*)

folgt $p \mid p_1' \cdots p_s' \overset{26,2^0}{\Rightarrow} \exists_i : p \mid p_i'$

$\Rightarrow$ (↑ $p > 1$, p_i' prim) $p = p_i'$

$\overset{(*)}{\Rightarrow}$ $p\,(m - p_1' \cdots \widehat{p_i'} \cdots p_s') = 0$

$\Rightarrow$ (↑ Nullteilerfreiheit von $\mathbb{Z}$) $m = p_1' \cdots \widehat{p_i'} \cdots p_s'$.

$\overset{\text{IV}}{\Rightarrow}$ $(p_1, \ldots, p_t)$ und $(p_1', \ldots, \widehat{p_i'}, \ldots, p_s')$

können durch Vertauschung der Koordinaten übereinstimmend gemacht werden.

$\Rightarrow$ Entsprechendes gilt für $(p, p_1, \ldots, p_t)$ und $(p, p_1', \ldots, \widehat{p_i'}, \ldots, p_s')$.

□

Euklid wusste schon 300 v. Chr. dass unendlich viele Primzahlen existieren

Satz 29 (Euklid) Es gibt so viele Primzahlen.

Bew: Angenommen nicht, d.h. $p_1, \dots, p_e$ seien die einzigen Primzahlen

Dann kann $n := p_1 \cdots p_e + 1$ keine Primzahl sein, da $n > p_i$. Ausserdem gelt $p_i \nmid n$, da $p_i \nmid 1$.

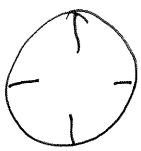
Nach Lemma 28 wird n durch eine Primzahl geteilt. Diese kann nach Obigem nicht eines der p_i sein. Widerspruch. □

Kapitel II

Restklassen und diophantische Gleichungen

Wenn man Elemente einer Menge, die eine gewisse Eigenschaft teilen, zusammenfassen will, dann verwendet man Äquivalenzrelationen.

Bsp (Uhr) Zwei Zeiten seien äquivalent (werden in einer Menge zusammengefasst), falls sie den gleichen Minutenstand haben



$11:35 \sim 9:35$

Vorteil: Wenn man nur an den Minuten interessiert ist, dann kann man bei der Addition und bei der Multiplikation die Stunden komplett ignorieren.

Bsp: $11:35 + 2:46 = 13:00 + 1:21$
$\sim 0:21$

$9:35 + 8:46 = 17:00 + 1:21$
$\sim 0:21$

Also man hätte die Stunden gleich am Anfang ignorieren können.

$11:35 + 2:46 \sim 0:35 + 0:46$
$= 1:21 \sim 0:21$

Dasselbe gilt für die Multiplikation:
(1 Stunde = 60 Minuten)

$(11 \cdot 60 + 35) \cdot (2 \cdot 60 + 46) \sim 35 \cdot 46$

$\sim (-25)(-14) = 25 \cdot 14 = 350 \sim -10$ (*)

Die komplizierte Variante wäre:

$(11 \cdot 60 + 35) \cdot (2 \cdot 60 + 46) = 695 \cdot 166$

$= 115370 = 1922 \cdot 60 + 50 \sim 50$.

$\rightsquigarrow$ (*) ist eine Rechenvereinfachung, wenn man nur an den Minutenzeiger denkt.

Def 30: Eine binäre Relation R auf M heißt symmetrisch, falls für jedes Paar $(x,y) \in M^2$ aus xRy auch yRx folgt. (R4)
R heißt Äquivalenzrelation, falls sie (R1), (R2), (R4) erfüllt, d.h. reflexiv, transitiv und symmetrisch ist.

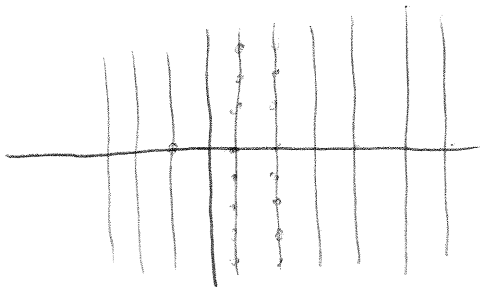
Bsp: 1) $"="\ := \{(x,x) \mid x \in M\}$ ist eine Äquivalenzrelation auf M.

2) Wir nennen z gerade, falls $2 \mid z$, ansonsten heißt z ungerade.

$\equiv_2 \ := \{(z_1, z_2) \in \mathbb{Z}^2 \mid 2 \mid z_1 - z_2\}$

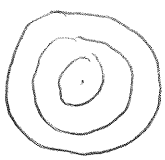
$\equiv_2$ ist eine Äquivalenzrelation.

3) $\{((z_1, z_2), (z_1', z_2')) \in \mathbb{Z}^2 \times \mathbb{Z}^2 \mid z_1 = z_1'\}$
ist eine Äquivalenzrelation auf $\mathbb{Z}^2$



4) Zwei Punkte $x, y \in \mathbb{R}^2$ seien bzgl. R_{Kreis} in Relation: $x R_{Kreis} y$, falls sie auf einem Kreis mit Mittelpunkt im Ursprung liegen.

R_{Kreis} ist eine Äquivalenzrelation.



(Der Kreis mit Radius 0 sei einfach ein Punkt)

Def 31: Es sei R eine Äquivalenzrelation auf M. Eine Teilmenge C von M heißt Äquivalenzklasse von R, falls

1) alle Elemente von C zueinander äquivalent sind ($\forall_{x,y \in C}: x R y$)
2) kein Element von $M \setminus C$ zu einem Element aus C äquivalent ist.

Wir bezeichnen mit M/R die Menge der Äquivalenzklassen von R.

Insbesondere haben wir $M/R \subseteq \mathcal{P}(M) = \{N \mid N \subseteq M\}$

Satz 32: Es sei R eine Äquivalenzrelation auf M. Dann gelten:

1) Für $C_1, C_2 \in M/R$ gilt: $C_1 = C_2 \vee C_1 \cap C_2 = \emptyset$
2) $\bigcup_{C \in M/R} C = M$

Bew: 1) Es sei $C_1 \cap C_2 \neq \emptyset$. Z.z. $C_1 = C_2$.

Wähle $x \in C_1 \cap C_2$.

„$\subseteq$": $y \in C_1 \overset{C_1 \text{ Äkl. } 1)}{\Rightarrow} y R x \overset{C_2 \text{ Äkl. } 2)}{\Rightarrow} y \in C_2$

Also $C_1 \subseteq C_2$, da y beliebig gewählt war.

„$\supseteq$" Analog

2) Es sei $x \in M$. Definiere $[x]_R := \{y \in M \mid y R x\}$.

Beh.: $[x]_R$ ist eine Äquivalenzklasse von R.

Bew.: 1) Wähle $y, z \in [x]_R$.
Dann $y R x R z \overset{(R2)}{\Rightarrow} y R z$

2) Wähle $y \in M \setminus [x]_R$ und $z \in [x]_R$.

Wenn $y R z$, dann $y R x$, da $z R x$ und (R2), also dann $y \in [x]_R$ ↯

□ □

$[x]_R$ heißt die Äquivalenzklasse von x bzgl. R.

Bem: Eine Teilmenge $T \subseteq \wp(M)$, die 32.1) und 32.2) erfüllt heißt <u>Partition</u> von M

Wir schreiben ab jetzt öfters $\sim$ statt R bei Äquivalenzrelationen.

Def 33: (Kongruenzrelation)

Es sei m eine ganze Zahl. Für $a, b \in \mathbb{Z}$ definieren wir

$$a \equiv_m b \iff_{\text{Def}} m \mid a - b,$$

oder anders geschrieben

$$\equiv_m := \{(z, z + m z') \mid z, z' \in \mathbb{Z}\}$$

$\equiv_m$ heißt die Kongruenzrelation modulo m auf $\mathbb{Z}$.

Statt $a \equiv_m b$ schreibt man auch $a \equiv b \bmod m$.

Bem: 1) Das Beispiel mit der Uhr ist $\equiv_{60}$. Analog können Sie sich auch das Beispiel $\equiv_{12}$ vorstellen.

2) Fixiere $5 \in \mathbb{Z}$. (nur für die Erklärung) Man $\equiv_5$ auch wie folgt beschreiben

$a \equiv_5 b$ genau dann, wenn a und b

bei der Division durch 5 mit Rest (Satz 23) den gleichen Rest erhalten. Das ist irreführend. Der Begriff „Rest" ist hier zu eng.

Besser müsste man sagen „den gleichen Rest in $\mathbb{N}_0^{<5}$ erhalten", um den Begriff Rest zu verallgemeinern.

„Ein Rest von a modulo m ist eine ganze Zahl, die man erhält, wenn man ein Vielfaches von m von a abzieht."
Also

$$\begin{aligned} 102 \text{ durch } 5 &= 20 \text{ Rest } 2 = 21 \text{ Rest } -3 \\ &= 0 \text{ Rest } 102 = 23 \text{ Rest } -13. \end{aligned}$$

Ziel sollte es für Vereinfachung von Rechnungen sein, einen betragsmäßig kleinen Rest zu finden.

$$99 \cdot 98 \equiv_{100} (-1)\cdot(-2) \equiv_{100} 2$$

Satz 34: $\equiv_m$ ist eine Äquivalenzrelation.

Bew: (R1) $a \in \mathbb{Z},\ a-a=0 \wedge m \mid 0 \Rightarrow a \equiv_m a$

(R2) $a,b,c \in \mathbb{Z},\ a \equiv_m b \equiv_m c$

$$\Rightarrow m \mid a-b \wedge m \mid b-c$$

$$\Rightarrow m \mid (a-b)+(b-c)$$

$$\Rightarrow m \mid a-c \Rightarrow a \equiv_m c$$

(R4) $a,b \in \mathbb{Z},\ a \equiv_m b \Rightarrow m \mid a-b$

$$\Rightarrow m \mid (a-b)\cdot(-1) = b-a \Rightarrow b \equiv_m a. \quad \square$$

Def 35: Wir schreiben $[a]_m$ für $[a]_{\equiv_m}$.

$$[a]_m + [b]_m := [a+b]_m$$

$$[a]_m \cdot [b]_m := [ab]_m$$

(ÜA) $+$ und $\cdot$ sind wohldefinierte Abbildungen von $\mathbb{Z}/\equiv_m \times \mathbb{Z}/\equiv_m$ nach $\mathbb{Z}/\equiv_m$, hängen also nicht von der Wahl der Repräsentanten a, b ab.

$$\left([a]_m = [a']_m \wedge [b]_m = [b']_m \Rightarrow [a+b]_m = [a'+b']_m \right)$$

bzw.

$$a \equiv_m a' \wedge b \equiv_m b' \Rightarrow a+b \equiv_m a'+b' \Big)$$

Satz 36: 1) $(\mathbb{Z}/\equiv_m, +)$ ist kommutativ, assoz. und hat ein neutrales Element.
Selbiges gilt für $(\mathbb{Z}/\equiv_m, \cdot)$.

2) zu jedem Element aus $\mathbb{Z}/\equiv_m$ gibt es eine Inverse bzgl. der Addition.

3) Es gelten die Distributivgesetze.

Bew: Es vererbt sich alles von $\mathbb{Z}$.

Assoziativität:

$$([a]_m + [b]_m) + [c]_m = [a+b]_m + [c]_m$$

$$= [(a+b)+c]_m \underset{\text{Ass. } \mathbb{Z}}{=} [a+(b+c)]_m$$

$$= [a]_m + [b+c]_m = [a]_m + ([b]_m + [c]_m)$$

usw. □

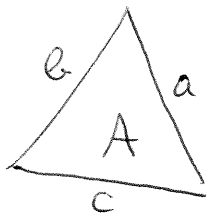
II 2 Diophantische Gleichungen

Eine polynomielle Gleichung mit ganzzahligen Koeffizienten, bei der nach ganzzahligen Lösungen gefragt wird, heißt

diophantische Gleichung.

Bsp: 1) $X = Y^2$, $X^2 - dY^2 = 1$ $(d \in \mathbb{N})$
Pellsche Gleichung.

2) ganzzahlige Heronsche Dreiecke:
Ein solches ist ein Dreick bei dem alle Seitenlängen und der Inhalt ganzzahlig sind.



$a, b, c, A \in \mathbb{N}$

Finde ein solches Dreieck $\Leftrightarrow$

Löse $A = \sqrt{\underbrace{\frac{(a+b+c)}{2}}_{s}(s-a)(s-b)(s-c)}$

$\Leftrightarrow$ Löse $16A^2 = (a+b+c)(b+c-a) \cdot (a+c-b)(a+b-c)$.

3) Fermatgleichung

$X^n + Y^n = Z^n \qquad n \geq 3.$

Restklassen können manchmal dabei helfen, um zu zeigen, dass eine diophantische Gleichung keine Lösung hat.

Bsp: 1) $X^2 + Y^2 = 8Z + 6$ hat keine Lsg.

Bew.: Ann. (x,y) ist eine Lösung.

Dann gilt $x^2 + y^2 \equiv_8 6$.

Welche Restklassen mod 8 sind Quadrate?

$0^2 \equiv_8 0$, $1^2 \equiv_8 1$, $2^2 \equiv_8 4$, $3^2 \equiv_8 1$, $4^2 \equiv_8 0$, $5^2 \equiv_8 1$

$6^2 \equiv_8 4$, $7^2 \equiv_8 1$,

$\Rightarrow \{[x]_8^2 \mid x \in \mathbb{Z}\} = \{[0]_8, [1]_8, [4]_8\}$

Nun: $0+0 \not\equiv 6 \bmod 8$

$0+1$ —"—

$0+4$ —"—

$1+1 \equiv 2 \not\equiv 6 \bmod 8$

$1+4 \equiv 5 \not\equiv 6$ —"—

$4+4 \equiv 0 \not\equiv 6$ —"—

$\Rightarrow$ Widerspruch dazu, dass (x,y) eine Lsg sein soll. □

2) Eine ganze Zahl der Form $3z+2$ ist kein Quadrat.

Satz 37 (Andrew Wiles)
"Großer Satz von Fermat" Es sei n eine natürliche Zahl größer als 2.
Die Fermat-Gleichung hat in $\mathbb{Z}^3$ nur Lösungen (x,y,z) mit $x \cdot y \cdot z = 0$.

Übungsaufgabe: Zeigen Sie, dass $X^3 - Y^3 = 8Y$ in $\mathbb{Z}^2$ nur die Lösung $(0,0)$ hat.
(Hinweis: Verwenden Sie Satz 37 für $n=3$.)

Bsp: Für welche Primzahlen p hat $X^2 + Y^2 = p$ eine Lösung?
$p=2$ hat eine $2 = 1^2+1^2$. Es sei $p>2$.
Ein Quadrat ist kongruent zu $0,1 \bmod 4$. Also hat die Gleichung für $p \equiv_4 3$ keine Lösung.
Später werden wir zeigen, dass die Gleichung für jedes $p \equiv_4 1$ eine Lösung hat. (z.B. $2^2+3^2=13$)
Wir benötigen dazu noch einige Grundlagen.

Wir schreiben $\mathrm{Lsg}_{\mathbb{Z}}$ (Gleichung) für die Menge der ganzzahligen Lösungen der gegebenen Gleichung.

Bsp: 1) Lineare diophantische Gleichungen

$$a_1 X_1 + \dots + a_n X_n \qquad a_i \in \mathbb{Z}$$

1a) $n=2$: $a_1 X_1 + a_2 X_2 = 0 \qquad a_1 a_2 \neq 0$

Wir dividieren durch $ggT(a_1, a_2)$ und können somit $ggT(a_1, a_2) = 1$ annehmen

Es sei $(x_1, x_2) \in \mathbb{Z}$ eine Lösung, dann

$$a_1 x_1 = -a_2 x_2 \overset{ggT(a_1,a_2)=1}{\Longrightarrow} a_1 \mid x_2 \wedge a_2 \mid x_1$$

$$\Rightarrow \exists\, z_1, z_2 \in \mathbb{Z}: \quad a_1 z_2 = x_2 \wedge a_2 z_1 = x_1$$

Aus $a_1 a_2 z_1 = -a_2 a_1 z_2$ folgt $z_1 = -z_2$, da $a_1 a_2 \neq 0$.

$$\Rightarrow (x_1, x_2) = (a_2 z_1, -a_1 z_1).$$

Paare dieser Form sind auch Lösungen.

$$\Rightarrow \mathrm{Lsg}(0 = a_1 X_1 + a_2 X_2) = \{(a_2 z_1 - a_1 z) \mid z \in \mathbb{Z}\}$$

falls $ggT(a_1, a_2) = 1$

1e) $7X + 3Y + 5Z = 0$

Es sei $(x,y,z) \in \mathbb{Z}^3$ eine Lsg.

$\Rightarrow \quad x - z \equiv 0 \mod 3$

$\Rightarrow \exists r \in \mathbb{Z} : \quad x = z + 3r$

Einsetzen: $7(z+3r) + 3y + 5z = 0$

$3(7r + y + 4z) = 0$

$\Rightarrow \quad y = -7r - 4z.$

Also $(x,y,z) = (z+3r, -7r-4z, z)$

Alle Tupel dieser Form sind auch eine Lösung (Nachprüfen!)

$\Rightarrow \quad \log_{\mathbb{Z}}(7X + 3Y + 5Z = 0)$

$= \{ (z+3r, -7r-4z, z) \mid z \in \mathbb{Z} \}$

2) Affine diophantische Gleichungen

$a_1 X_1 + \dots + a_n X_n = c \qquad a_i, c \in \mathbb{Z}.$

(ÜA) Wenn $\underline{x}$ eine Lösung ist, dann gilt $\log_{\mathbb{Z}}(-u-) = \underline{x} + \log_{\mathbb{Z}}(\sum_{i=1}^{n} a_i X_i = 0)$

Es sei $a_1 \cdot \dots \cdot a_n \neq 0.$

Suche nach einer ersten Lösung:

$t := ggT(a_1, \dots, a_n)$

Falls $t \nmid c$, dann gibt es keine Lösung.

Falls $t \mid c$, dann dividiere die Gleichung durch t.
Also können wir annehmen, dass $ggT(a_1, \dots, a_n) = 1$ ist.

Lemma von Bézout
$\Rightarrow \exists\, y_1, \dots, y_n \in \mathbb{Z} : \sum_{i=1}^{n} a_i y_i = 1$

$\Rightarrow (y_1 c, \dots, y_n c) \in \log_{\mathbb{Z}} \left(\sum_{i=1}^{n} a_i X_i = c \right)$.

Satz 38: Es seien a, m und c ganze Zahlen und $a \neq 0$. Dann sind äquivalent

1° $aX + mY = c$ hat eine Lösung
2° $aX \equiv c \mod m$ hat eine Lösung.
3° $t := ggT(a, m) \mid c$.

Im Falle der Lösbarkeit von $aX \equiv_m c$ ist die Lösungsmenge gleich

$$\bigcup_{i=0}^{t-1} \left[e\frac{c}{t} + i\frac{m}{t} \right]_m,$$ wobei e eine ganze Zahl ist, die $ea \equiv_m t$ erfüllt.

Beweis: 1° $\Rightarrow$ 2° $ax + my = c \Rightarrow ax \equiv_m c$.
2° $\Rightarrow$ 1° $ax \equiv_m c \Rightarrow \exists y \in \mathbb{Z} : ax = c + ym$
$\Rightarrow aX + mY = c$ hat eine Lösung
1° $\Rightarrow$ 3° $t \mid a \wedge t \mid m$
$\Rightarrow t \mid ax + my = c$
3° $\Rightarrow$ 1° Nach dem Lemma von Bézout

existieren $e, f \in \mathbb{Z}$: $ea + fm = t$.

$t \mid c \Rightarrow \exists\, d \in \mathbb{Z}$: $td = c$

$\Rightarrow \quad dea + dfm = c.$ □ (Äquivalenz)

Teil 2 des Satzes. Es sei $x \in \mathbb{Z}$ eine Lösung von $a\underline{X} \equiv c \mod m$.

$\Rightarrow \quad ax \equiv c \mod m \Rightarrow \quad \underset{\substack{\text{|||} \\ tx}}{eax} \equiv ec \mod m$

$\Rightarrow \quad x \equiv e\frac{c}{t} \mod \frac{m}{t}$

$\Rightarrow \quad x \equiv e\frac{c}{t} + i\frac{m}{t} \mod m$

für ein $i \in \mathbb{Z}$. Die $i \in \{0, \ldots, t-1\}$

reichen aus, ~~dan~~ da aus $t \mid i_1 - i_2$

$m \mid i_1\frac{m}{t} - i_2\frac{m}{t}$ folgt.

$\Rightarrow \quad x \in \bigcup_{i=0}^{t-1} \left[\frac{ec}{t} + i\frac{m}{t}\right]_m.$

Ein Element dieser Menge löst die Gleichung auch, da

$$a\left(e\frac{c}{t} + i\frac{m}{t}\right) \equiv t\frac{c}{t} + i\frac{am}{t}$$

$$\underset{t \mid a}{\equiv} \quad c + 0 \mod m. \qquad □$$

Der chinesische Restsatz

Es seien $a, c, m \in \mathbb{Z}$, $a m \neq 0$, $ggT(a, m) = 1$

Will man die Kongruenz $a\underline{x} \equiv c \bmod m$

lösen und der Modul m ist besonders groß, so kann es hilfreich sein, das Problem aufzuteilen

$$m = m_1 \cdots m_\ell \qquad ggT(m_i, m_j) = 1$$

für alle $i \neq j$

Nun löst man für jedes i die Kongruenz $a\underline{x}_i \equiv c \bmod m_i$, z.B. mittels $e_i \in \mathbb{Z}$, s.d. $e_i a \equiv 1 \bmod m_i$.

Wir erhalten modulo (m_i) eine eindeutige Lösung $\underline{x} = (x_1, \ldots, x_\ell)$ des Kongruenzgleichungssystems.

$(e_1, c_1 \ldots, e_\ell c)$

(Die Eindeutigkeit modulo (m_i) folgt aus Satz 38)

Der folgende Satz gibt im Beweis eine Konstruktion einer mod m Restklasse $[x]_m$, die

$$x \equiv x_i \bmod m \qquad i = 1, \ldots, \ell$$

erfüllt.

Dann ist $[x]_m$ die Lösungsmenge von $a\underline{x} \underset{m}{\equiv} c$.

Satz 39 (Chinesischer Restsatz)

Es seien $c_1, \dots, c_\ell, m_1, \dots, m_\ell$ ganze Zahlen, so dass $m_1 \cdots m_\ell \neq 0$ und so dass m_i und m_j für $i \neq j$ teilerfremd sind.

Dann hat das Kongruenzsystem

$$X \equiv c_i \mod m_i \quad i = 1, \dots, \ell$$

genau eine Lösung modulo m.

Bew: (vollst. Induktion über ℓ)

(IA) $\ell = 1$: $[c_1]_m$ ist die Lösungsmenge von $X \equiv c_1 \mod m$.

(IS) IV: $X \equiv c_i \mod m_i$, $i = 1, \dots, \ell - 1$ hat mod $\hat{m}$ eine eindeutige Lösung, etwa $\hat{x}$. ($\hat{m} := m_1 \cdots m_{\ell-1}$)

IB: Das Kongruenzsystem $X \equiv c_i \mod m_i$, $i = 1, \dots, \ell$ hat mod m eine eindeutige Lösung.

Bew: $\operatorname{ggT}(\hat{m}, m_\ell) = 1$

Lemma von Bézout $\Rightarrow \exists\, e, f \in \mathbb{Z}$:

$$e\hat{m} + f m_\ell = 1$$

Setze

$$x := \hat{x} f m_\ell + c_\ell e \hat{m}$$

Dann gilt:

$x \equiv c_\ell \bmod m_\ell$ und

$x = \hat{x} \equiv c_i \bmod m_i$ für $i = 1, \dots, \ell-1$.

Eindeutigkeit: Es sei x' eine Lösung mod m

$\Rightarrow \quad x - x' \equiv 0 \bmod m_i \quad i = 1, \dots, \ell$

$\Rightarrow \quad m \mid x - x' \Rightarrow x \equiv x' \bmod m.$

↑ $\gcd(m_i, m_j) = 1$, für $i \neq j$ und (ÜA)

□

□

Bsp.: $\overline{X} \equiv 2 \bmod 11$

$X \equiv 5 \bmod 7$

$X \equiv 3 \bmod 8.$

Die Lösungsmethode mit Bézout ist etwas aufwendig.

$\overline{X} \equiv_{11} 2 \qquad X \equiv_7 5 \qquad (1)$

Euklidischer Algorithmus

$\Rightarrow \quad 2 \cdot 11 - 3 \cdot 7 = 1$

$\hat{x} := -2 \cdot 3 \cdot 7 + 5 \cdot 2 \cdot 11 = -42 + 110$

$= 68 \equiv_{77} -9$

$\Rightarrow$ ↑ Bew. Satz 39 $\hat{x} \bmod 77$ ist eindeutige Lösung mod 77 von (1)

$$\begin{aligned} x &\equiv -9 \mod 77 \\ x &\equiv 3 \mod 8 \end{aligned} \qquad (2)$$

Eukl. Alg. $\Rightarrow \quad 29 \cdot 8 - 3 \cdot 77 = 1$

$\Rightarrow$ Die mod 616 ($= 8 \cdot 7 \cdot 11$) Restklasse von

$\uparrow$ Satz 39

$$\begin{aligned} x &= -3 \cdot 3 \cdot 77 + (-9) \cdot 8 \cdot 29 \\ &= -2781 \equiv_{616} 299 \end{aligned}$$

ist die, mod 616 eindeutig bestimmte Lösung von (2)

und damit auch vom Ausgangsproblem.

Probe:
$$\begin{aligned} 299 &\equiv -31 \equiv (-1)(-2) \equiv 2 \mod 11 \\ 299 &\equiv +19 \equiv 5 \mod 7 \\ 299 &\equiv -21 \equiv \underbrace{(-1)(-3)}_{3} \mod 8 \end{aligned}$$

✓

Das war recht aufwendig, insbesondere die Berechnung der Bézoutkoeffizienten.

Bessere Methode: x sei eine Lsg.

$$x \equiv_{11} 2 \quad \Rightarrow \quad \exists r \in \mathbb{Z}: \; x = 11 \cdot r + 2$$

$$\Rightarrow \quad 2 + 11 \cdot r \equiv_7 5 \quad \wedge \quad 2 + 11 r \underset{8}{\equiv} 3$$

$$\Leftrightarrow \quad 4r \equiv_7 3 \quad \wedge \quad 3r \equiv_8 1$$

$$\Leftrightarrow \quad r \equiv_7 6 \equiv_7 -1 \quad \wedge \quad r \underset{8}{\equiv} 3$$

$r = 7s - 1$

Einsetzen $\Rightarrow \quad -s \equiv_8 4 \Leftrightarrow \quad s \equiv_8 4$

Wähle $s := 4 \Rightarrow r = 27 \Rightarrow x = 299.$

$[299]_{616}$ ist Lösungsmenge.

Zusatz: g-adische Zahlen

Satz 1: Es seien $z \neq 0$ eine ganze Zahl und $g \in \mathbb{N}^{>1}$. Dann existiert genau ein Paar $(\varepsilon, m) \in \{\pm 1\} \times \mathbb{N}_0$ und genau ein Tupel $(a_0, \dots, a_m) \in \mathbb{N}_0^{<g}$ mit $a_m \neq 0$, s.d.

$$z = \varepsilon \left(a_0 + a_1 g + a_2 g^2 + \dots + a_m g^m \right)$$

Hierbei ist $\varepsilon = 1 \iff z \in \mathbb{N}_0$

Bsp: $g = 10$: Dezimaldarstellung

$$22578 = 8 + 7 \cdot 10 + 5 \cdot 10^2 + 2 \cdot 10^3 + 2 \cdot 10^4$$

$g = 2$: Binärdarstellung

$$19 = 1 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$$

$$= 10011_2$$

Also $19_{10} = 10011_2$

$g = 7$: $23 = 2 \cdot 7^0 + 1 \cdot 7^1 + 1 \cdot 7^2$

$$23_{10} = 112_7$$

Beweis: Existenz:

Induktion über $|z| \neq 0$

IA) $|z| < g$ ✓ $\quad m=0$, $a_0 = |z|$

$\varepsilon = 1$, falls $z > 0$

$\varepsilon = -1$, " $z < 0$

IS) $|z| \geq g$.

Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{N} \times \mathbb{N}_0^{<g}$:

$|z| = qg + r$

$\Rightarrow \quad |q| = q < |z|$

$\Rightarrow$ IV q hat eine g-adische Darstellung

$$q = \sum_{i=0}^{m'} a_i' g^i$$

$$\Rightarrow |z| = \sum_{i=1}^{m'+1} a_{i-1}' g^i + r$$

Setze $a_i := \begin{cases} a_{i-1}', & \text{falls } i \in \{1, \dots, m'+1\} \\ r, & \text{falls } i = 0. \end{cases}$

Eindeutigkeit:

Falls $\varepsilon \underbrace{\sum a_i g^i}_{>0} = \varepsilon' \underbrace{\sum a_i' g^i}_{>0} = z \neq 0$

$\Rightarrow \quad \varepsilon = \varepsilon'$

↑

Beide Seiten haben das selbe VZ wie z.

Also $\sum_{i=0}^{m} a_i g^i = \sum_{i=0}^{m'} a'_i g^i$ (*) Es $m \geq m'$

$\Rightarrow \forall_{j=0,\dots,m'}$: $\sum a_i g^i \equiv_{g^j} \sum a'_i g^i$

$\sum_{i=0}^{j-1} a_i g^i$ $\quad$ $\sum_{i=0}^{j-1} a'_i g^i$

$< g^j$ $\quad$ $\in \mathbb{N}_0 < g^j$

≥ 0

$\Rightarrow$ $\forall_{j=0,\dots,m'}$: $a_j = a'_j$.

Rechte Seite in (*) von der linken Seite abziehen $\Rightarrow$ $\sum_{j=m'+1}^{m} a_i g^i = 0$

ist > 0, falls $m > m'$, da $a_m \neq 0$ und $a_i g^i \geq 0$.

$\Rightarrow$ $m = m'$. $\square$

Anwendung des chinesischen Restsatzes in der Computerarithmetik:

Addition und Mult. großer Zahlen, d.h.
Zahlen $\in \mathbb{N}_0^m$ mit $m \approx 2^{128}$.
↑
Bsp.

Betrachte $m_1 = 2^{32}-1$, $m_2 = 2^{32}-3$
$m_3 = 2^{32}-5$, $m_4 = 2^{32}-9$
(paarweise teilerfremd.)

Operation: $n_1, n_2 \in \mathbb{N}_0^m$

$\rightsquigarrow$ Addiere n_1 und n_2 mod m_i $i = 1,\dots,4$.

$\rightsquigarrow$ Erhalte $n_1 + n_2$ mod m
↑
chinesischer Restsatz

$\rightsquigarrow$ Wenn $n_1 + n_2 < m$, erhalten wir das Ergebnis.

Zusatz: Pythagoräische Zahlentripel

Def 22: Ein -11- ist ein Tripel natürlicher Zahlen, die als Seitenlängen eines rechtwinkligen Dreiecks vorkommen.

Satz 23 (Indische Formeln)

$$\log_{\mathbb{Z}}(X^2+Y^2=Z^2)$$

$$= \left\{(x,y,z)\in\mathbb{Z}^3 \;\middle|\; \{|x|,|y|\}=\{2ab,\ a^2-b^2\},\ |z|=a^2+b^2,\ a,b\in\mathbb{N}_0 \text{ mit } a\geq b.\right\}=:L$$

Beweis: Es sei $(x,y,z)\in\mathbb{Z}^3$. Es ist eine Lösung $\Leftrightarrow$ $(|x|,|y|,|z|)$ eine Lösung ist

$\Rightarrow$ OE sei $(x,y,z)\in\mathbb{N}_0^3$ eine Lösung.

Teil 1: z.z. $2\mid xy$

Ann. $2\nmid xy \Rightarrow x^2+y^2 \equiv_4 1+1 \equiv_4 2$

$\Rightarrow 2\mid z^2 \Rightarrow 2\mid z \Rightarrow 4\mid z^2 \Rightarrow 0\equiv_4 z^2 \equiv_4 x^2+y^2 \equiv_4 2$ ↯

(↑ 2 prim zahl)

Teil 2: $(0,0,c) \in L$ (nehme $a=0=e$)

Also betrachten wir $(x,y,z) \in \mathbb{N}_0^3$ mit $(x,y,z) \neq (0,0,0)$. Es sei $t := ggT(x,y,z) \in \mathbb{N}$

$\Rightarrow$ $\frac{x}{t}, \frac{y}{t}$ sind teilerfremd, da jeder Primzahl p, die $\frac{x}{t}$ und $\frac{y}{t}$ teilt, auch $\frac{z}{t}$! aber eine solche Primzahl p kann es nicht geben, da $ggT(\frac{x}{t}, \frac{y}{t}, \frac{z}{t}) = 1$.

analog $ggT(\frac{y}{t}, \frac{z}{t}) = ggT(\frac{x}{t}, \frac{z}{t}) = 1$.

$\Rightarrow$ OE können wir $ggT(x,y) = ggT(y,z) = ggT(x,z) = 1$ annehmen.

$(\frac{x}{t}, \frac{y}{t}, \frac{z}{t}) \in \mathbb{Z}$

Weiter $2 \mid xy \Rightarrow 2 \mid x \vee 2 \mid y$. OE gelte $2 \mid y$

$\Rightarrow$ $ggT(x,y) = 1 = ggT(z,y)$ $2 \nmid x \wedge 2 \nmid z$.

$\Rightarrow$ $2 \mid \underbrace{x+z}_{=:2c} \wedge 2 \mid \underbrace{z-x}_{=:2d} \Rightarrow z = c+d \wedge x = c-d$

$\Rightarrow y^2 = z^2 - x^2 = (c+d)^2 - (c-d)^2 = 4dc$.

$ggT(c,d) \mid ggT(x,z) = 1 \Rightarrow$ d und c sind $(\frac{y}{2})^2 = cd$ Quadratzahlen.

$\Rightarrow \exists_{a,b \in \mathbb{N}_0} : c = a^2 \wedge d = b^2$ Also

$z = a^2 + b^2 \wedge x = a^2 - b^2 \wedge y = 2ab.$

Aus $x \geq 0$ folgt $a^2 \geq b^2 \Rightarrow (a-b)(a+b) \geq 0$

$a + b > 0$, da $a, b \in \mathbb{N}_0$ und $(a,b) \neq (0,0)$, da $(x,y,z) \neq (0,0,0)$

$\Rightarrow$ $a - b \geq 0$, da sonst $(\ )\cdot(\ ) < 0$
$(\ )\cdot(\ ) \geq 0$

Widerspruch.

Also $a \geq b$. $\square$

Zusatz: Das Auswahlaxiom

In S.2.3. hatten wir die Widerspruchsmethode mit Unendlichem Abstieg.

Man hat ein ganzzahliges Problem gegeben, (z.B. $X^3+Y^3=Z^3 \wedge XYZ \neq 0$.)

Es sei $L \subseteq \mathbb{Z}^3$ die Menge der Lösungen des Problems. Wir betrachten $h(\underline{z}) := |z_1| + |z_2| + |z_3|$

Angenommen man kann zeigen, dass gilt

(*) $\forall_{\underline{z} \in L} : \quad \emptyset \neq L \cap \{\underline{\tilde{z}} \in \mathbb{Z}^3 \mid h(\underline{\tilde{z}}) < h(\underline{z})\}$

Beh: Dann ist L leer.

Beweis: Annahme $L \neq \emptyset \Rightarrow M := h(L) \neq \emptyset$.

Wähle $m_0 \in M$. Wir brauchen $f: \mathbb{N}_0 \to \mathbb{N}_0$ strikt ordnungsumkehrend.

1) Für $m \in M$ gilt: $M \cap \mathbb{N}^{<m} \neq \emptyset$.

Beweis: $m \in M \Rightarrow \exists \underline{z} \in L : h(\underline{z}) = m$.

$\overset{(*)}{\Rightarrow} \exists \underline{\tilde{z}} \in L : h(\underline{\tilde{z}}) < h(\underline{z})$. Also

$h(\underline{\tilde{z}}) \in M \cap \mathbb{N}^{<m}$. □

Wählen Sie $g: M \to M$, o.d. $g(m) < m$

(Aber warum geht das?)

Rekursionssatz (S.12.2.) $\Rightarrow \exists f: \mathbb{N}_0 \to M: f(0) = m_0$ ∧

$\forall n \in \mathbb{N}_0: f(n+1) = g(f(n))$

Dann gilt $f(n+1) = g(f(n)) < f(n)$ für alle $n \in \mathbb{N}_0$

Mit vollst. Induktion zeigt man $f(n+l) < f(n)$ $\forall_{n \in \mathbb{N}_0} \forall_{l \in \mathbb{N}}$

$\Rightarrow$ Widerspruch zu S.2.3.1. □

Def 7.4: Es sei M eine Menge.

$$\text{Auswahl}(M) :\Leftrightarrow \forall_{G: I \to \mathcal{P}(M) \setminus \{\emptyset\}} \exists_{g: I \to M} \forall_{i \in I}: g(i) \in G(i)$$

Wir können obiges g aufgrund des folg. Satzes finden

Satz 7.5: Für jede Teilmenge M von $\mathbb{N}_0$ gilt Auswahl(M).

Beweis: Für $M = \emptyset$ ist nichts zu zeigen.

Es sei $M \in \mathcal{P}(\mathbb{N}_0) \setminus \{\emptyset\}$, und es sei

$G: I \to \mathcal{P}(M) \setminus \{\emptyset\}$ gegeben.

Definiere $g(i) := \min G(i)$. (Satz 15) □

Auswahlaxiom (AC): Für alle Mengen M gilt Auswahl(M).

Dazu äquivalente Axiome

Def Z6: Es sei $f: M \to N$ eine Abbildung. Eine Abbildung $g: N \to M$ heißt

- Rechtsinverse von f, falls $f \circ g = id_N$ ist.
- Linksinverse von f, falls $g \circ f = id_M$ ist.

Axiom von der Existenz von Rechtsinversen: (AER)

$\forall f: M \to N$ surjektiv: f besitzt eine Rechtsinverse.

Def Z7: Es sei $(M, \leq)$ geordnet. Wir nennen eine total geordnete Menge auch Kette.

Es sei $N \subseteq M$ und $x \in M$.

x heißt obere Schranke von N, falls

$\forall y \in N: y \leq x$.

Wenn x ein kleinstes Element unter allen oberen Schranken von N ist, so bezeichnen wir $x = \sup N$.

analog untere Schranke von N und $\inf(N)$.

2) x heißt maximales Element von M, falls kein Element von M größer ist.

3) — " — minimales — " — kleiner ist.

4) $(M, \leq)$ heißt induktiv geordnet, falls $M \neq \emptyset$ ist und jede Kette $N \subseteq M$ in M eine obere Schranke besitzt.

Axiom (Zornsches Lemma) (AZL):
Jede induktiv geordnete Menge besitzt ein maximales Element.

Satz 2.8: $(AC) \Leftrightarrow (AER) \Leftrightarrow (AZL)$.

Beweis $(AC) \Rightarrow (AER)$: $f: M \twoheadrightarrow N$.

$\Rightarrow \forall_{y \in N}: f^{-1}(\{y\}) = \{x \in M \mid f(x) = y\} \neq \emptyset$

$(AC) \Rightarrow \exists_{g: N \to M}: \forall_{y \in N}: g(y) \in f^{-1}(\{y\})$

$\Rightarrow f \circ g = id_N$

$(AER) \Rightarrow (AC)$: (Übungsaufgabe)

(AZL) ⇒ (AC): Es sei $G: I \to \mathcal{P}(M) \setminus \{\emptyset\}$ gegeben. $\mathcal{M} = \{ (J, f) \mid J \subseteq I,\ f: J \to M,\ \forall i \in J: f(i) \in G(i) \}$

Definiere: $(J_1, f_1) \leq (J_2, f_2) \Leftrightarrow_{\text{def}} J_1 \subseteq J_2 \wedge f_2|_{J_1} = f_1$.

Es sei $\mathcal{N} \subseteq \mathcal{M}$ eine Kette. Definiere $J_0 = \bigcup_{\exists f: (J,f) \in \mathcal{N}} J$ und $f_0: J_0 \to M$ durch $f_0|_J := f$ für alle $(J, f) \in \mathcal{N}$. f_0 ist wohldefiniert. (üA)

(J_0, f_0) ist eine obere Schranke von $\mathcal{N}$ per Definition.

$\mathcal{N}$ beliebig ⇒ $\mathcal{M}$ ist induktiv geordnet

(AZL) ⇒ $\exists (\hat{J}, \hat{f}) \in \mathcal{M}$: $(\hat{J}, \hat{f})$ maximales Element

Annahme $\hat{J} \subsetneq I$ ⇒ $\exists i_0 \in I \setminus \hat{J}$. Wähle $x_0 \in G(i_0)$

Definiere $\tilde{f}(i_0) := x_0$ und $\tilde{f}|_{\hat{J}} := \hat{f}$.

⇒ $(\hat{J}, \hat{f}) \subsetneq (\tilde{J}, \tilde{f})$ ↯ zur Maximalität.

Also $I = \hat{J}$. Damit ist (AC) gezeigt.

(AC) ⇒ (AZL) ohne Beweis □

Kapitel III Algebraische Strukturen

Wir haben im Wesentlichen durch Rechnen mit + und · gesehen, dass sich die Elemente von $\mathbb{Z}$ als Produkte unzerlegbarer Elemente schreiben lassen, und das eindeutig bis auf Multiplikation mit ± 1. ($-p, p$ Primzahl sind in $\mathbb{Z}$ auch unzerlegbar, siehe Def 8.3)
Eine solche Zerlegungseigenschaft vereinfacht Rechnungen und Beweise und führt zu

schnellen einfachen Agorithmen in Computeralgebrasystemen (Chinesischer Restsatz).

Es stellt sich also die Frage inwieweit diese Zerlegungseigenschaft von den üblichen Eigenschaften (Kommutativität, Assoziativität, Distributivgesetze, etc) von + und · abhing.

Deshalb studieren wir in diesem Kapitel Mengen mit Strukturen.

III 1. Halbgruppen und Gruppen

Hier beschäftigen wir uns nur mit Mengen mit einer Struktur

Def 40: Es sei M eine Menge.
Eine Struktur auf M ist eine Abbildung
$* : M \times M \longrightarrow M$.
Ein Paar $(M, *)$ bestehend aus einer Menge M und einer Struktur auf M heißt Magma

Bsp: Eine Struktur auf M ist nichts anderes als dass sie zwei Elementen aus M wieder ein Element aus M zuordnet. Da gibt es viele Beispiele:

$(\mathcal{P}(M), \cap)$ $\quad \cap : \mathcal{P}(M) \times \mathcal{P}(M) \longrightarrow \mathcal{P}(M)$
$(A, B) \longmapsto A \cap B = \{x \in M \mid x \in A \wedge x \in B\}$

$(\mathcal{P}(M), \setminus)$ $\quad \setminus : \mathcal{P}(M) \times \mathcal{P}(M) \longrightarrow \mathcal{P}(M)$
$(A, B) \longmapsto A \setminus B = \{x \in M \mid \begin{smallmatrix} x \in A \\ x \notin B \end{smallmatrix} \wedge\}$

$(\mathbb{Z}, \text{power})$ $\quad \text{power} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
$\text{power}(a, b) = a^{|b|}$

$(\mathbb{Z}, *)$ $\quad * : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
$(z_1, z_2) \longmapsto z_1^2 \cdot z_2^3$

$(\mathbb{Z}, ggT)$

$(\mathbb{Z}, kgV)$

Def 41: Ein Magma $(M, *)$ heißt Halbgruppe, falls $*$ assoziativ ist, d.h.

$$\forall_{a,b,c \in M}: (a * b) * c = a * (b * c)$$

$*$ heißt abelsch (oder auch kommutativ) falls $\forall_{a,b \in M}: a * b = b * a$.

$e \in M$ rechtsneutral falls $x * e = x$ für alle $x \in M$

linksneutral falls $e * x = x$ für alle $x \in M$.

neutral falls $e * x = x * e = x \; \forall_{x \in M}$.

Ein Magma $(M, *)$ heißt Monoid, falls es eine Halbgruppe ist, die ein neutrales Element besitzt.

Bem: Zwei neutrale Elemente eines Magmas stimmen überein.

Bew: $e_1, e_2 \in M$ seien neutrale Elemente.

$$\Rightarrow \; e_1 = e_1 * e_2 = e_2$$

(e_2 neutr. El. bzw. e_1 neutr. Element) ∎

Bsp: 1) $(\mathbb{N}, +)$ ist eine abelsche Halbgruppe. $(\mathbb{N}, \cdot)$ und $(\mathbb{N}_0, +)$ sind abelsche Monoide, wie auch $(\mathbb{Z}, \cdot)$ und $(\mathbb{Z}, +)$.

2) $(\mathcal{P}(M), \cap)$, $(\mathcal{P}(M), \cup)$, $(\mathcal{P}(M), \Delta)$ mit

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

sind abelsche Monoide.

Bew. für $(\mathcal{P}(M), \cup)$: $A, B, C \in \mathcal{P}(M)$, d.h. $A, B, C \subseteq M$.

Ass:
$$\begin{aligned}(A \cup B) \cup C &= \{x \mid x \in A \cup B \vee x \in C\} \\ &= \{x \mid (x \in A \vee x \in B) \vee x \in C\} \\ &= \{x \mid x \in A \vee (x \in B \vee x \in C)\} \\ &= \{x \mid x \in A \vee x \in B \cup C\} = A \cup (B \cup C)\end{aligned}$$

Kom.: Analog $A \cup B = B \cup A$

Neutr. El.: $E := \emptyset$ $\quad E \cup A = \emptyset \cup A = A$

Kom. $\rightarrow$ $=$

$A \cup E$. $\square$

3) $(\mathbb{Z}, *)$ mit $z_1 * z_2 = z_1^2 z_2^3$

ist nicht ~~assoziativ~~ abelsch: $1 * 2 = 8$

$2 * 1 = 4$,

nicht assoziativ:

$(1 * 2) * 2 = 8 * 2 = 2^6 \cdot 2^3 = 2^9$

$1 * (2 * 2) = 1^2 \cdot (2^2 \cdot 2^3)^3 = 2^{15}$,

und hat kein neutrales Element. ($\neq A$).

4) $M \neq \emptyset$, dann ist $(\mathcal{P}(M), \setminus)$

weder abelsch noch assoziativ,

hat kein linksneutrales Element, aber ein rechtsneutrales Element $\emptyset$.

Jetzt kommen wir zum zentralen Begriff des Abschnittes, der Gruppe.

Eine Gruppe hält die Symmetrien eines Problems fest.

Bsp: 1) Kurvendiskussion:

- $f: \mathbb{R} \to \mathbb{R}$ sei achsensymmetrisch zur y-Achse. $f(x) = f(-x) \; \forall x \in \mathbb{R}$.

Dann reicht es aus f auf $\mathbb{R}^{\geq 0}$ zu studieren.

Weis man etwas über $f|_{\mathbb{R}^{\geq 0}}$, so weis man das Entsprechende über $f|_{\mathbb{R}^{\leq 0}}$.

z.B. Ist f in 1 differenzierbar, so ist f in -1 — " —.

Aus $f'(1) = 3$ folgt $f'(-1) = -3$

Die Symmetrie die dafür verantwortlich ist $f|_{\mathbb{R}^{\geq 0}}$ und $f|_{\mathbb{R}^{\leq 0}}$ als "äquivalent" anzusehen, ist die Abbildung

$$a: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$a(x,y) = (-x,y)$$

- Selbe Idee für die Punktsymmetrie in $(0,0)$.

  Symmetrie: $\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ $\varphi(x,y) = (-x,-y)$

  Drehung um 180°.

2) Eine Baufirma baut eine Siedlung mit 10 Wohnblöcken $B1, \ldots, B10$. Jeder Block hat 5 Wohnungen, wobei jede der 5 Wohnungen einen anderen Zuschnitt hat. Bi wird eine Kopie von $B1$. $B1$ ist fertig, $B2 - B10$ aber noch nicht.

Ein Wohnungsbauinteressent kann die Wohnungen in $B1$ besichtigen, um

um alle vorhandenen Zuschnitte kennenzulernen.

Was sind hier die Symmetrien?

Es sind die Abbildungen, die die 50 Wohnungen vertauschen und dabei den Zuschnitt erhalten.

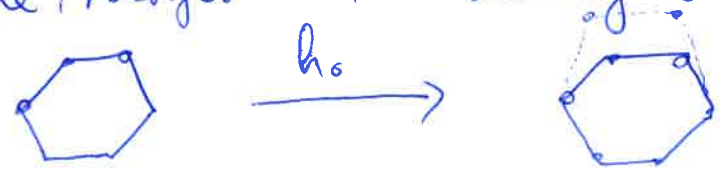
Wir interessieren uns in diesem Abschnitt für die Symmetrien,

nicht für die Wohnungen.

3) Wir suchen jede Abbildung

die Kanten auf Kanten abbildet und injektiv ist. Ausserdem soll der Abstand von Punkten auf einer Kante erhalten bleiben.

Eine mögliche Abbildung wäre



Eine weitere erhält man, wenn man zuerst das Hexagon um 60° dreht und dann h_0 anwendet.

Wenn man sich nur dafür interessiert, wie man A in B hineinlegen kann, dann sollte man die Drehung ignorieren; man sagt "die Symmetrien des Hexagons rausfaktorisieren".

Dazu muss man aber die Symmetrien kennen ⇝ Begriff der Symmetriegruppe des Hexagons.

Def. 42: Es sei $(M,*)$ ein Monoid. $b \in M$.
Ein Element a von M heißt das
- Rechtsinverse von b, falls $b*a = e$
- linksinverse von b, falls $a*b = e$.
- Inverse von b, falls $a*b = b*a = e$.

$(M,*)$ heißt Gruppe falls jedes Element von M ein Inverses besitzt.

Bem: Es sei $(M,*)$ ein Monoid. Wenn $a \in M$ ein linksinverses und ein Rechtsinverses hat, dann stimmen diese überein.

Bew.: $a_1, a_2 \in M$: $a_1 * a = e = a * a_2$

$$\Rightarrow \quad a_1 * (a * a_2) \overset{\text{Ass} \rightarrow}{=} (a_1 * a) * a_2 \overset{a_1 \text{ LI} \rightarrow}{=} e * a_2 \overset{e \text{ neutr. El.} \rightarrow}{=} a_2$$

a_2 RI; e neutr. El.

□

Wir bezeichnen das Inverse eines Elementes a, falls existent, mit a^{-1}.

Satz 43: In einer Gruppe $(G, *)$ hat die Gleichung $a * x = b$ $(a, b \in G)$ genau eine Lösung, nämlich $x := a^{-1} * b$.

Beweis: Ex: $a * (a^{-1} * b) \underset{\text{Ass}}{=} (a * a^{-1}) * b = e * b = b$ (inv., neutr. El.)

Eindeutigkeit: Es sei x' eine zweite Lösung. $\Rightarrow a * x' = b = a * x$

$\Rightarrow a^{-1} * (a * x') = a^{-1} * (a * x)$

$(a^{-1} * a) * x' \quad (a^{-1} * a) * x$

$e * x' \quad e * x$

$x' \quad x$ □

Zurück zu den Beispielen:

zu 1) sind $(\{id_{\mathbb{R}^2}, \text{Spiegelung an der Y-Achse}\}, \circ)$

und $(\{id_{\mathbb{R}^2}, \text{Drehung um } 180°\}, \circ)$

die Gruppen, wobei $\circ$ die Verknüpfung von Abbildungen ist.

Jedes Gruppenelement erfüllt hier $g \circ g = id$ und $id_{\mathbb{R}^2}$ ist das neutrale Element für beide Gruppen.

Zu Bsp 2) Wir beschreiben die Wohnungen wie folgt

(i,j) $\quad j$ – Wohnungsnummer $\quad j \in \{1,\dots,5\}$
$\quad\quad i$ – Blocknummer $\quad i \in \{1,\dots,10\}$

D.d. „(i_1,j_1) und (i_2,j_2) haben dasselbe Zuschnitt" $\Leftrightarrow$ $j_1 = j_2$"

Der Wohnblock B_i ist also $\{(i,1),\dots,(i,5)\}$
Die Menge der Wohnungen ist $M = \{(i,j) \mid i \in \mathbb{N}^{\leq 10}, j \in \mathbb{N}^{\leq 5}\}$
Die zuschnittserhaltenen Bijektionen von M sind die Abbildungen $g: M \to M$, welche für jedes $j \in \mathbb{N}^{\leq 5}$

$$g(\mathbb{N}^{\leq 10} \times \{j\}) \subseteq \mathbb{N}^{\leq 10} \times \{j\}$$

erfüllen. $G_{2)} = \{g \in \mathrm{Bij}(M) \mid g(i,j) \in \mathbb{N}^{\leq 10} \times \{j\} \; \forall_{j \in \mathbb{N}^{\leq 5}}\}$

Wir werden gleich zeigen, dass $G_{2)}$ eine Gruppe ist.

zu 3) Das Beispiel lässt sich allgemeiner betrachten.

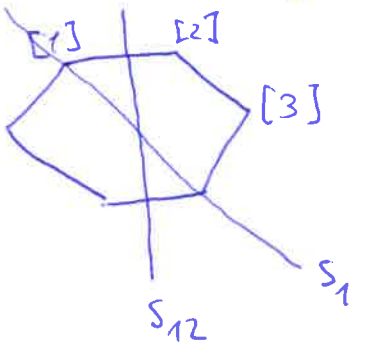
Def 43: Ein <u>Graph</u> ist ein Paar (E,K), bestehend aus einer nichtleeren Menge E („Menge der Ecken") und einer Teilmenge K von $\mathcal{P}(E)$. („Menge der Kanten"), so dass jedes Element von K $1 \leq |k| \leq 2$ erfüllt. Es sei (E,K) ein Graph.
Eine bijektive Abbildung $\varphi: E \to E$ heißt Automorphismus von (E,K), falls für alle $e_1, e_2 \in E$ gilt:

$$\{e_1,e_2\} \in K \Leftrightarrow \{\varphi(e_1),\varphi(e_2)\} \in K.$$

Sie zeigen in der 5. Serie, dass
$\mathrm{Aut}(E,K) := \{ f : E \to E \mid f \text{ ist ein Automorphismus von } (E,K) \}$

mit der Komposition von Abbildungen eine Gruppe bildet. $(\mathrm{Aut}(E,K), \circ)$ heißt „Automorphismengruppe von (E,K)".

Bsp: $E = \mathbb{Z}/\equiv_6$, $K := \{ \{ [z]_6, [z+1]_6 \} \mid z \in \mathbb{Z} \}$



(Ü A) $\mathrm{Aut}(E,K) =$

$\{ d_{0°}, d_{60°}, d_{120°}, d_{180°}, d_{240°}, d_{300°}, s_1, s_{14}, s_2, s_{23}, s_3, s_{34} \}$

Bsp 44: Es sei $M \neq \emptyset$ eine Menge. Dann ist $(\mathrm{Bij}(M), \circ)$ eine Gruppe.

Diese Gruppe heißt auch die symmetrische Gruppe von M, die man auch mit $\mathrm{Sym}(M)$ bezeichnet.

Beweis: Wohldefiniertheit von $\circ$: $f_1, f_2 \in \mathrm{Bij}(M)$

z.z. $f_1 \circ f_2$ ist bijektiv

$(f_1 \circ f_2)(x) = (f_1 \circ f_2)(x') \Rightarrow f_1(f_2(x)) = f_1(f_2(x'))$

$\Rightarrow f_2(x) = f_2(x') \Rightarrow x = x'$

($\Rightarrow$: f_1 injektiv; f_2 injektiv)

Also ist $f_1 \circ f_2$ injektiv.

Surjektivität: Wähle ein $Y \in M$.

$\Rightarrow$ $\exists z \in M : f_1(z) = Y$

f_1 surjektiv

$\Rightarrow$ $\exists x \in M : f_2(x) = z$

f_2 surjektiv

$\Rightarrow$ $f_1(f_2(x)) = f_1(z) = Y$.

$f_1(z) = Y$

Also $f_1 \circ f_2$ ist surjektiv.

Assoziativität z.z. $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$

$$\begin{aligned}(f_1 \circ (f_2 \circ f_3))(x) &= f_1((f_2 \circ f_3)(x)) \\ &= f_1(f_2(f_3(x))) \\ &= (f_1 \circ f_2)(f_3(x)) \\ &= ((f_1 \circ f_2) \circ f_3)(x)\end{aligned}$$

x beliebig $\Rightarrow$ $f_1 \circ f_2 \circ f_3 = (f_1 \circ f_2) \circ f_3$

neutrales Element:

z.z. $id_M \circ f = f \circ id_M = f \quad \forall f \in Bij(M)$

$$(id_M \circ f)(x) = id_M(f(x)) = f(x)$$

$$(f \circ id_M)(x) = f(id_M(x))$$

x bel. $\Rightarrow$ Beh.

$\exists$ eine Inverse zu $f \in Bij(M)$. Wähle ein $f \in Bij(M)$

$h : M \to M$ sei def. durch $h(x) = y$, falls $f(y) = x$

h ist wohldefiniert, denn es ein y existiert, da f surjektiv ist (+ Auswahlaxiom) und y durch x eindeutig bestimmt ist, da f injektiv ist.

$(h \circ f)(y) = h(f(y)) = y$
(↑ Def von h)

$\Rightarrow h \circ f = id_M$ und h ist surjektiv

$(f \circ h)(y) = f(h(y)) = y$
(↑ Def. von h)

$\Rightarrow f \circ h = id_M$ und h ist injektiv.

Also $h \in Bij(M)$ und h ist eine Inverse von f. □

Def 45: Es sei $(G, *)$ eine Gruppe.
H heißt Untergruppe von $(G, *)$ falls $(H, *|_{H \times H})$ eine Gruppe ist. (insbesondere $*(H \times H) \subseteq H$)

Untergruppenkriterium:

Satz 46: Es sei $(G, *)$ eine Gruppe und $H \subseteq G$ nichtleer. Dann sind äquivalent

1° H ist eine Untergruppe von G.

2° $\forall h_1, h_2 \in H: h_1^{-1} h_2 \in H$.

3° $\forall h_1, h_2 \in H: h_1 h_2 \in H$ und $h_1^{-1} \in H$.

Beweis: $1° \Rightarrow 3°$. $(H, *|_{H\times H})$ ist eine Untergruppe von $(G, *) \Rightarrow *(H\times H) \subseteq H$.
also $\forall h_1, h_2 \in H : h_1 * h_2 \in H$.

- Es sei $h \in H$. h^{-1} ist das Inverse von h in G, also bzgl. e_G.
$(H, *|_{H\times H})$ ist eine Gruppe, also besitzt ein Inverses $h^{-1,H}$ von h bzgl. $*|_{H\times H}$. Also

$$h * h^{-1} = h^{-1} * h = e_G$$

$$h * h^{-1H} = h^{-1H} * h = e_H.$$

Es reicht $e_G = e_H$ zu zeigen, denn dann folgt nach Satz 43 $h^{-1} = h^{-1H}$.

$$e_H * e_G = e_H = e_H * e_H \overset{\text{Satz 43}}{\Rightarrow} e_G = e_H.$$

(e_G neutr. El in G; e_H neutr. El in H)

Also haben wir $h^{-1} = h^{-1H}$ und somit

$$h^{-1} = h^{-1H} \in H.$$

$3° \Rightarrow 2°$ einfach.

$2° \Rightarrow 1°$ Vorbereitung: Wir zeigen $e_G \in H$.
$H \neq \emptyset \Rightarrow \exists h \in H$. $2° \Rightarrow e_G = h^{-1} * h \in H$.

- $* (H \times H) \subseteq H$: $h_1, h_2 \in H$

  $\Rightarrow h_1^{-1} = h_1^{-1} * e_G \in H$, $h_2 \in H$

  $\Rightarrow (\underbrace{h_1^{-1}}_{h_1})^{-1} * h_2 \in H$

- Assoziativität: wird von $(G, *)$ vererbt.
- neutrales Element: $e_G \in H$ und damit hat H ein neutrales Element: $e_H := e_G$
- Ex. des Inversen eines Elementes von H.
  $h \in H$. Betrachte h^{-1}, die Inverse von h in G.

  $\Rightarrow h^{-1} * h = h * h^{-1} = e_G = e_H$ (↑ Def von e_H)

  Außerdem gilt

  $h^{-1} = h^{-1} * e_G \in H$. □

Aus dem Untergruppenkriterium folgt jetzt leicht, dass G_{f_2} und G_{f_3} Gruppen sind

z.B. für G_{f_2}: $(\mathrm{Bij}(\mathbb{N}), \circ)$ ist eine Gruppe.

$g_1, g_2 \in G_{f_2} \Rightarrow g_2(\mathbb{N}^{\leq 10} \times \{f\}) \subseteq \mathbb{N}^{\leq 10} \times \{f\}$

$\forall i \in \mathbb{N}^{\leq 5}$

$\Rightarrow (g_1 \circ g_2)(\mathbb{N}^{\leq 10} \times \{f\})$

$g_1 \in G_{f_2}$ ⇑

$= g_1(g_2(\mathbb{N}^{\leq 10} \times \{i\}))$

$\subseteq g_1(\mathbb{N}^{\leq 10} \times \{i\})$

$\forall i \quad \{i\} \times \mathbb{N}^{\leq 10} \subseteq \mathbb{N}$ ⇑

z.z. $g_1^{-1}(\mathbb{N}^{\leq 10} \times \{j\}) \subseteq \mathbb{N}^{\leq 10} \times \{j\}$.

Wähle $(i_1, j_1) \in M$ mit $g_1(i_1, j_1) = (i_2, j)$

$g_1(i_1, j_1) \in \mathbb{N}^{\leq 10} \times \{j_1\} \Rightarrow j_1 = j$

$\Rightarrow g_1^{-1}(i_2, j) = (i_1, j) \in \mathbb{N}^{\leq 10} \times \{j\}$.

$\Rightarrow g_1^{-1}(\mathbb{N}^{\leq 10} \times \{j\}) \subseteq \mathbb{N}^{\leq 10} \times \{j\}$ □

Def 47: Es seien $(M_1, *_1)$ und $(M_2, *_2)$ zwei Magmen. Eine Abbildung $\varphi: M_1 \to M_2$ heißt Homomorphismus, falls $\forall x, y \in M_1: \varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$.

Sind M_1 und M_2 Gruppen, so heißt φ ein Gruppenhomomorphismus.

Satz 48 (Übungsaufgabe): Es sei $\varphi: G_1 \to G_2$ ein Gruppenhomomorphismus, dann gilt $\varphi(e_1) = e_2$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Bsp: $(\mathbb{Z}, +) \xrightarrow{\pi} (\mathbb{Z}/\equiv_6, +)$

$z \longmapsto [z]_6$ ist ein Gruppenhomomorphismus.

$\pi(z_1 + z_2) = [z_1 + z_2]_6 \overset{\text{Def. +}}{=} [z_1]_6 + [z_2]_6$

$= \pi(z_1) + \pi(z_2)$

Untergruppen definieren eine Äquivalenzrelation auf Gr
$H \leq Gr$ heißt ab jetzt "Ht ist UGr von Gr."

Def: $H \leq G; \sim_H := \{(g_1, g_2) \mid g \in G, h \in H\}$, also

$$g_1 \sim_H g_2 \iff \exists h \in H : g_2 = g_1 h$$

$$\iff g_2 \in g_1 H.$$

$$\iff g_1^{-1} g_2 \in H \iff g_1^{-1} g_2 H = H$$

$$\iff g_1 H = g_2 H.$$

Wir bezeichnen gH als
Linksnebenklasse von H nach g.

$\sim_H$ ist eine Äquivalenzrelation mit
Äquivalenzklassen

$$gH \,, g \in Gr.$$

Die Faktormenge $Gr/\sim_H$ bezeichnen
wir mit Gr/H, also $Gr/H = \{gH \mid g \in Gr\}$

Bsp: $\equiv_m$ ist das selbe wie $\sim_{m\mathbb{Z}}$
auf $\mathbb{Z}$.

$$x \equiv_m y \iff m \mid x-y \iff x-y \in m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$$

$$\iff -x+y \in m\mathbb{Z} \iff x \sim_{m\mathbb{Z}} y$$

Also ist $\mathbb{Z}/\equiv_m \;=\; \mathbb{Z}/\sim_{m\mathbb{Z}} \;=\; \mathbb{Z}/m\mathbb{Z}$

Satz 48A: (direktes Produkt von Magmen)

Es sei $((M_i, *_i))_{i \in I}$ eine Familie von Magmen.

Auf dem kartesischen Produkt

$$\bigtimes_{i \in I} M_i := \{(x_i)_{i \in I} \mid \forall_{i \in I}: x_i \in M_i\}$$
$$\subseteq \mathrm{Abb}\left(I, \bigcup_{i \in I} M_i\right)$$

gibt es genau eine Struktur $*$, sodass alle kanonischen Projektionen

$$\pi_j : \bigtimes_{i \in I} M_i \longrightarrow M_j$$
$$\pi_j((x_i)_{i \in I}) := x_j$$

Homomorphismen sind.

Wir bezeichnen $\left(\bigtimes_{i \in I} M_i, *\right) =: \prod_{i \in I} (M_i, *_i) =: \prod_{i \in I} M_i$

das direkte Produkt von $(M_i)_{i \in I}$.

Es sei $(M', *')$ ein Magma.
Eine Abb. $f : M' \longrightarrow \prod_{i \in I} M_i$ ist genau dann ein Homomorphismus, wenn für alle $i \in I$ die Abbildung $\pi_i \circ f$ ein Homomorphismus ist.

Beweis: Def. $(x_i)_{i\in I} * (y_i)_{i\in I} := (x_i *_i y_i)_{i\in I}$.

Dann gilt $\pi_k((x_i)_i * (y_i)_i) = \pi_k((x_i *_i y_i)_i)$

$= x_k *_k y_k = \pi_k((x_i)_i) *_k \pi_k((y_i)_i)$.

Es sei $*'$ eine weitere Struktur, so, dass alle π_k Homomorphismen sind. Wähle $(x_i)_{i\in I}, (y_i)_{i\in I}$

$(z_i)_{i\in I} := (x_i)_{i\in I} *' (y_i)_{i\in I}$

$\Rightarrow \forall_{k\in I}: z_k = \pi_k((z_i)_{i\in I}) \overset{\pi_k \text{ Homom.}}{=} \pi_k((x_i)_i) *_k \pi_k((y_i)_i)$

$= x_k *_k y_k$

2) Wenn f ein Homom. ist, dann ist $\pi_k \circ f$ ein Homom., der das Komposition zweier — " — ein Homomorphismus ist.

Umgekehrt: Es seien alle $\pi_k \circ f$ Homomorphismen. $x', y' \in M'$

$f(\overbrace{x' *' y'}^{z'})$ $\quad f(x') \quad f(y')$

$!!$ $\quad !! \quad !!$

$(z_i)_{i\in I}$ $\quad (x_i)_{i\in I} \quad (y_i)_{i\in I}$

$\Rightarrow \pi_k \circ f(z') = z_k$

$(\pi_k \circ f)(x') *_k (\pi_k \circ f)(y') = x_k *_k y_k$. !

$$\Rightarrow \quad f(z') = f(x' * y') = (z_i)_{i\in I} = (x_i *_i y_i)_{i\in I}$$
$$= (x_i)_{i\in I} * (y_i)_{i\in I} = f(x') * f(y'). \qquad \square$$

Bem 48B: Wenn alle M_i Monoide sind, dann ist $\prod M_i$ ein Monoid. Das selbe für Gruppen.

Bew. · Assoziativität:

$$((x_i) * (y_i)) * (z_i) = (x_i *_i y_i)_i * (z_i)_i$$
$$= ((x_i *_i y_i) *_i z_i)_i = (x_i *_i (y_i *_i z_i))_i$$
$$= (x_i)_{i\in I} * ((y_i)_{i\in I} * (z_i)_{i\in I}).$$

↑ analog zurück

· $(e_i)_{i\in I}$ ist das neutrale Element.

$$(x_i)_i * (e_i)_i \overset{\text{Def.}}{=} (x_i *_i e_i)_i = (x_i)_i = (e_i *_i x_i)_i$$

↑ neutr. Elt

$$= (e_i)_i * (x_i)_i$$

↑ analog zurück

· Im Fall von Gruppen: Inverse: $(x_i)_{i\in I} \in \prod_{i\in I} G_i$

$$(x_i^{-1})_i * (x_i)_i = (x_i^{-1} *_i x_i)_i$$
$$= (e_i)_{i\in I} = (x_i)_{i\in I} * (x_i^{-1})_{i\in I}$$

↑ analog zurück

$\square$

Schreibweise: Wenn $I = \mathbb{N}^{\leq 2}$, dann schreiben wir auch $(M_1 *_1 M_2) \times (M_1 *_2 M_2) \times \ldots$

Bsp:

1) $\prod_{i \in I} (\mathbb{Z}, +)$

2) $(\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$

$(z_1, [z_2]_2) + (z_1', [z_2']_2) := (z_1 + z_1', [z_2 + z_2']_2)$

3) $(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, +)$

$([z_1]_{m_1}, \ldots, [z_n]_{m_n}) + ([z_1']_{m_1}, \ldots, [z_n']_{m_n})$

$:= ([z_1 + z_1']_{m_1}, \ldots, [z_n + z_n']_{m_n})$.

4) $(\mathbb{Z}, +) \times (\mathbb{Z}, \cdot)$

$(z_1, z_2) \odot (z_1', z_2') := (z_1 + z_1', z_2 \cdot z_2')$

Def: Ein Gruppenhomomorphismus $f: G_1 \to G_2$ heißt
- —"— monomorphismus, falls f injektiv ist
- Gruppenepimorphismus, falls f surjektiv ist
- —"— isomorphismus, falls f bijektiv ist. $\cong$

$\ker(f) = \{ g \in G_1 \mid f(g) = e_2 \}$ Kern von f.

$\operatorname{im}(f) = f(G_1) = \{ f(g) \mid g \in G_1 \}$ Bild, bzw. Image von f.

Satz 49: (1. Isomorphiesatz) Es sei $f: G_1 \to G_2$ ein Gruppenhomomorphismus. Dann sind $f(G_1)$ und $\ker(f)$ Untergruppen von G_2 bzw. G_1.

Des weiteren ist $(G_1/\ker(f), *)$ def. durch $[g] \cdot [h] := [gh]$ eine Gruppe und

$$G_1/\ker(f) \cong \operatorname{im} f$$

[$\cong$ bedeutet, dass ein Isomorphismus von $G_1/\ker(f)$ nach $\operatorname{im} f$ existiert]

Bsp: Es sei m eine natürliche Zahl und $\zeta := e^{i\frac{2\pi}{m}}$.

$\mu_m(\mathbb{C}) := \{\zeta^j \mid j \in \mathbb{Z}\} = \{x \in \mathbb{C}^\times \mid x^m = 1\}$

ist die Menge der m-ten Einheitswurzeln.

Dann ist $(\mu_m(\mathbb{C}), \cdot)$ eine Gruppe. (ÜA),

und $\varphi : (\mathbb{Z}, +) \longrightarrow (\mu_m(\mathbb{C}), \cdot)$, $\varphi(z) = \zeta^z$

ein Gruppenepimorphismus.

- Surjektiv ✓
- $\varphi(z_1 + z_2) = \zeta^{z_1 + z_2} = \zeta^{z_1} \cdot \zeta^{z_2}$
  $= \varphi(z_1)\,\varphi(z_2)$

Der Kern von φ ist

$$\begin{aligned}\ker\varphi &= \{z \in \mathbb{Z} \mid \varphi(z) = 1\} \\ &= \{z \in \mathbb{Z} \mid e^{i\frac{2\pi}{m}z} = 1\} \\ &= \{z \in \mathbb{Z} \mid m \mid z\} \\ &= \{mz \mid z \in \mathbb{Z}\} = m\mathbb{Z}\end{aligned}$$

Satz 49 $\Rightarrow$ $\mathbb{Z}/m\mathbb{Z} \cong \mu_m(\mathbb{C})$ über φ.

Für den Beweis von Satz 49 benötigen wir ein Lemma und eine Definition.

Def 50: $H \leq G$ heißt <u>Normalteiler</u>, falls für alle $g \in G$ die Menge gHg^{-1} mit H übereinstimmt. Wir schreiben $H \trianglelefteq G$.

<u>Lemma 51:</u> Es sei G eine Gruppe und H ein Normalteiler von G. Dann ist

$$\left(G/H, *\right), \quad [g_1] * [g_2] := [g_1 * g_2]$$

eine Gruppe, die "Faktorgruppe von G nach H".

<u>Bew:</u> Wohldefiniertheit.

z.z. $\left(g_1 H = g_1' H \text{ und } g_2 H = g_2' H \right.$

$\left. \Rightarrow g_1 g_2 H = g_1' g_2' H\right)$

<u>Bew:</u>

$$g_1 g_2 H \underset{\uparrow}{=} g_1 g_2' H \underset{\uparrow}{=} g_1 H g_2'$$

$[g_2] = [g_2']$; H Normalteiler v. G

$$\underset{\uparrow}{=} g_1' H g_2' \underset{\uparrow}{=} g_1' g_2' H \quad \square$$

$g_1 H = g_1' H$; H NT von G

Assoziativität wird von G geerbt.

Neutrales Element: $[e] = eH = H$

Existenz des Inversen zu $[g]$:

Nehme das Inverse g^{-1} von g in G_1.

$\Rightarrow [g^{-1}] * [g] = [g^{-1} * g] = [e]$

(Def. $\uparrow$ $\#$ $\uparrow$ Def Inverse von g.)

$[g] * [g^{-1}] = [g * g^{-1}]$ $\square$

Beweis von Satz 49: a) $\ker(f)$ ist eine Untergruppe von G_1 nach dem Untergruppenkriterium.

z.z. $(g_1, g_1' \in \ker(f) \Rightarrow g_1^{-1} g_1' \in \ker(f))$ und $\ker(f) \neq \emptyset$:

- $f(e_1) = e_2 \Rightarrow \ker(f) \ni e_1$
- $g_1, g_1' \in \ker(f) \Rightarrow$

$$f(g_1^{-1} g_1') = f(g_1^{-1}) f(g_1') = f(g_1)^{-1} f(g_1')$$

(Gruppenhom. $\uparrow$, S. 48 $\uparrow$)

$$= e_2^{-1} e_2 = e_2 e_2 = e_2$$

($\uparrow$ $g_1, g_1' \in \ker(f)$; $\uparrow$ $e_2^{-1} = e_2$)

$\Rightarrow g_1^{-1} g_1' \in \ker(f)$.

b) $\ker(f)$ ist ein NT von G_1

$g_1 \in G_1$, z.z. $g_1 \ker(f) g_1^{-1} = \ker(f)$.

Es reicht „$\subseteq$" zu zeigen. (Begründen Sie warum!)

$h \in \ker(f) \Rightarrow f(g_1 h g_1^{-1}) = f(g_1) f(h) f(g_1)^{-1}$

$= f(g_1) e_2 f(g_1)^{-1} = f(g_1) f(g_1)^{-1} = e_2.$

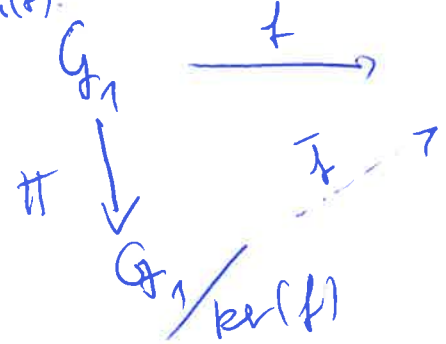
($h \in \ker(f)$)

$\Rightarrow g_1 h g_1^{-1} \in \ker(f)$

Also „$\subseteq$" stimmt.

Lemma 5.1 $\Rightarrow$ $G_1/\ker(f)$ ist eine Gruppe.

z.z. $G_1/\ker(f) \cong \mathrm{im}(f)$.



$\bar{f}([g_1]) := f(g_1)$

$\bar{f}$ ist wohldefiniert:

$[g_1] = [g_1'] \Rightarrow \exists_{h \in \ker(f)} : g_1 = g_2 h \Rightarrow f(g_1) = f(g_2) f(h)$

$= f(g_2) e_2$

$= f(g_2)$

$\bar{f}$ ist ein Gruppenhomomorphismus:

$\bar{f}([g_1][g_1']) = \bar{f}([g_1 g_1']) = f(g_1 g_1')$

$\bar{f}([g_1]) \bar{f}([g_1']) = f(g_1) f(g_1')$

$\mathrm{im}\,\bar{f} = \mathrm{im}\, f$ nach Definition von $\bar{f}$

$\ker \bar{f} = \{[g_1] \mid \bar{f}([g_1]) = e_2\} = \{[g_1] \mid f(g_1) = e_2\}$

$$= \{ [g_1] \mid g_1 \in H \} = \{ g_1 H \mid g_1 \in H \}$$
$$= \{ H \}.$$

$\Rightarrow \bar{f}$ ist injektiv. □

In den Übungsaufgaben beweisen Sie den 2. und den 3. Isomorphiesatz.

Satz 52: (2. und 3. Isomorphiesatz)

2. Isomorphiesatz: Es seien G eine Gruppe, H_1 und H_2 Normalteiler von G, s.d. $H_1 \leq H_2$.

Dann gilt $\left(G/H_1\right) \Big/ \left(H_2/H_1\right) \cong G/H_2$

über einen kanonischen Isomorphismus.

3. Isomorphiesatz: Es sei G eine Gruppe und $H_1, H_2 \leq G$, sodass H_1 die Gruppe H_2 normalisiert, d.h. für alle $h_1 \in H_1$ gilt $h_1 H_2 h_1^{-1} = H_2$.

Dann gibt es einen kanonischen Isomorphismus

$$H_2 / (H_1 \cap H_2) \xrightarrow{\sim} H_1 H_2 / H_1.$$

$\left(H_1 H_2 = \{ h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2 \} \right.$

$$[[z]_6]_{3\mathbb{Z}/6\mathbb{Z}} \longmapsto [z]_3$$

Bspi 1) $\dfrac{\mathbb{Z}/6\mathbb{Z}}{3\mathbb{Z}/6\mathbb{Z}} \cong \dfrac{\mathbb{Z}}{3\mathbb{Z}}$

2) $\dfrac{10\mathbb{Z}}{10\mathbb{Z}\cap 6\mathbb{Z}} \cong \dfrac{10\mathbb{Z}+6\mathbb{Z}}{6\mathbb{Z}}$

$$[z]_{10\mathbb{Z}\cap 6\mathbb{Z}} \longmapsto [z]_6$$

Allgemeiner gilt

Satz 53: Es seien $m_1,\dots,m_n \in \mathbb{Z}\setminus\{0\}$. Dann gelten

1) $\bigcap_{i=1}^{n} m_i\mathbb{Z} = kgV(m_1,\dots,m_n)\,\mathbb{Z}$

2) $\sum_{i=1}^{n} m_i\mathbb{Z} \underset{\text{Def}}{=} \{x_1+\dots+x_n \mid x_i \in m_i\mathbb{Z},\ i=1,\dots,n\}$

$$\underset{\text{Beh}}{=} ggT(m_1,\dots,m_n)\,\mathbb{Z}$$

3) Für ganze Zahlen m, m' mit $mm' \neq 0$ gilt

$$\frac{m\mathbb{Z}}{kgV(m,m')\mathbb{Z}} \cong \frac{m\mathbb{Z}+m'\mathbb{Z}}{m'\mathbb{Z}}$$

$$\| $$

$$\frac{ggT(m,m')\mathbb{Z}}{m'\mathbb{Z}}$$

Bew: 1) „$\subseteq$" $x \in \bigcap_{i=1}^{n} m_i\mathbb{Z} \Rightarrow \forall_{i\in\mathbb{N}\le n}: m_i \mid x$

$$\underset{(\text{ÜA})}{\Rightarrow} kgV(m_1,\dots,m_n) \mid x$$

$$\Rightarrow x \in kgV(m_1,\dots,m_n)\,\mathbb{Z}$$

„$\supseteq$" $x \in kgV(m_1,\dots,m_n)\,\mathbb{Z} \Rightarrow \forall_{i\in\mathbb{N}\le n}:$

$m_i \mid kgV(\dots) \mid x$.

$\Rightarrow \quad x \in \bigcap_{i=1}^{n} m_i \mathbb{Z}$

2) „$\subseteq$" $\quad x \in \sum_{i=1}^{n} m_i \mathbb{Z} \Rightarrow \exists (x_1, \dots, x_n) \in m_1\mathbb{Z} \times \dots \times m_n \mathbb{Z}$:
$x = x_1 + \dots + x_n$

Für jedes $i \in \{1, \dots, n\}$ gilt $ggT(m_1, \dots, m_n) \mid m_i \mid x_i$

$\Rightarrow ggT(m_1, \dots, m_n) \mid x \Rightarrow x \in ggT(m_1, \dots, m_n)\mathbb{Z}$

„$\supseteq$" $x \in \underbrace{ggT(m_1, \dots, m_n)\mathbb{Z}}_{=:t} \Rightarrow \exists\, y \in \mathbb{Z} : x = ty$

Lemma von Bézout $\Rightarrow \exists\, a_1, \dots, a_n \in \mathbb{Z} : \sum a_i m_i = t$

$\Rightarrow x = \sum_{i=1}^{n} y a_i m_i \in \sum_{i=1}^{n} m_i \mathbb{Z}$.

$y a_i m_i \in m_i \mathbb{Z}$

3) 3. Isomorphiesatz $\Rightarrow \quad \dfrac{m\mathbb{Z}}{m\mathbb{Z} \cap m'\mathbb{Z}} \simeq \dfrac{m\mathbb{Z} + m'\mathbb{Z}}{m'\mathbb{Z}}$

1) $\quad \dfrac{m\mathbb{Z}}{kgV(m,m')\mathbb{Z}}$

2) $\quad \dfrac{ggT(m,m')\mathbb{Z}}{m'\mathbb{Z}}$.

□

Der letzte Satz führt uns zur Erzeugung von Untergruppen $\sum_{i=1}^{n} m_i \mathbb{Z}$ ist die von $m_1, \dots, m_n$ erzeugte Untergruppe von $\mathbb{Z}$. Wir definieren den allgemeinen Begriff:

Def 54: Es sei Y eine Teilmenge einer Gruppe G. Wir bezeichnen mit $\langle Y \rangle$ die kleinste Untergruppe von G, die Y enthält.

bzgl. $\subseteq$

Eine Gruppe G heißt endlich erzeugt, falls eine endliche Teilmenge $Y \subseteq G$ existiert, s.d. $\langle Y \rangle = G$.
Falls sogar $|Y| = 1$ möglich ist, so heißt G zyklisch.

Satz 54: Es sei G eine Gruppe und $Y \subseteq G$.

1) $\langle Y \rangle$ existiert und ist damit eindeutig bestimmt, nach der Eigenschaft eines kleinsten Elementes

2) $\langle Y \rangle = \{ g_1^{\pm 1} \cdot g_2^{\pm 1} \cdots g_n^{\pm 1} \mid n \in \mathbb{N}_0, g_1, \ldots, g_n \in Y \}$

(Wir definieren das leere Produkt ($n=0$) als e)

Bew: 1) $H := \bigcap_{\substack{H' \leq G \\ Y \subseteq H'}} H'$ ist eine Untergruppe von G nach dem Untergruppenkriterium.

Es sei $H' \leq G$ mit $Y \subseteq H'$. Dann ist H' am Schnitt beteiligt. Also $H \subseteq H'$, und somit ist H das kleinste Element von $\{ H' \leq G \mid Y \subseteq H' \}$ bzgl. $\subseteq$.

2) Übung $\Rightarrow$ $\{ g_1^{\pm 1} \cdots \} =: L$ ist eine Untergruppe von G.

$\langle Y \rangle$ kleinste Gpe. $\subseteq$ und $Y \subseteq$

$Y \subseteq L \Rightarrow \langle Y \rangle \subseteq L$

z.z. „$\supseteq$" $x = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} \in L$, $g_i \in Y$, $\varepsilon_i \in \{\pm 1\}$, $n \in \mathbb{N}_0$

$g_i \in Y \wedge \langle Y \rangle \leq G$

$\Rightarrow x = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} \in \langle Y \rangle$

Satz 46

x beliebig $\Rightarrow$ $L \subseteq \langle Y \rangle$ □

Die Konstruktion von $\mathbb{Q}$

Wir möchten durch ganze Zahlen teilen, ausser durch Null.

$(\mathbb{Z} - \{0\}, \cdot)$ ist ein abelscher Monoid. Wir brauchen eine abelsche Gruppe $(G, \cdot)$ die $\mathbb{Z} - \{0\}$ enthält.

Am besten nicht zu groß, also idealerweise

$\langle \mathbb{Z} - \{0\} \rangle = G$.

Problemstellung: Gegeben sei ein abelscher Monoid $(M, *)$. Kann man eine Gruppe konstruieren $(G, *)$, sodass $M \xrightarrow{\varphi} G$ und

$\langle \varphi(M) \rangle = G$.

Antwort: Im Allgemeinen nicht. Es fehlt noch eine Voraussetzung.

In einer Gruppe gilt die Kürzungseigenschaft

$g_1 g' = g_2 g' \Rightarrow g_1 = g_2$. Diese muss M auch erfüllen.

Def: Es sei $(M,*)$ ein Magma.
$a \in M$ heißt linksregulär (bzw. linkskürzbar) falls $\forall_{b,c \in M}: (ab = ac \Rightarrow b = c)$
Analog rechtsregulär bzw. rechtskürzbar.
a heißt regulär bzw. kürzbar, falls es links- und rechtsregulär ist.
$(M,*)$ heißt linksregulär, falls jedes Element aus M linksregulär ist. usw.

Satz 55: Es sei $(M,*)$ ein regulärer abelscher Monoid. Dann gibt es eine Gruppe $(G,*_G)$ und einen injektiven Homomorphismus

$$M \xhookrightarrow{\varphi} G,$$

s.d. $\langle \varphi(M) \rangle = G$.

Bew.: Wir definieren eine Äquivalenzrelation auf $M \times M$.

$$(a_1,b_1) \sim (a_2,b_2) \underset{\text{Def.}}{\Leftrightarrow} a_1 b_2 = a_2 b_1$$

Das ist eine Äquivalenzrelation

(R1) ✓

(R2) ✓

(R4) $(a_1,b_1) \sim (a_2,b_2) \sim (a_3,b_3)$

$\Rightarrow a_1 b_2 = a_2 b_1 \wedge a_3 b_2 = a_2 b_3$

$\Rightarrow a_1 b_2 a_2 b_3 = a_2 b_1 a_3 b_2$

abelsch ↓

$\Rightarrow a_1 b_3 (a_2 b_2) = a_3 b_1 (a_2 b_2)$

$\Rightarrow$ ↑ Kürzen $\quad a_1 b_3 = a_3 b_1 \Rightarrow (a_1, b_1) \sim (a_3, b_3)$

$G := M \times M / \sim$

$*_G : G \times G \longrightarrow G$ sei definiert durch

$$[(a_1, b_1)]_\sim *_G [(a_2, b_2)]_\sim := [(a_1 a_2, b_1 b_2)]_\sim$$

(ÜA): $(G, *_G)$ ist eine abelsche Gruppe.

Ref. $\varphi: M \longrightarrow G$ via $\varphi(a) := [(a, e)]_\sim$

$\Rightarrow \varphi$ ist ein injektiver Homomorphismus (ÜA)

z.z. $\langle \varphi(M) \rangle = G$.

$$[(a, b)]_\sim = [(a, e)]_\sim *_G [(e, b)]_\sim$$
$$= [(a, e)]_\sim *_G [(b, e)]^{-1}_\sim$$
$$= \varphi(a) *_G \varphi(b)^{-1}$$

Satz 54 $\Rightarrow \langle \varphi(M) \rangle = G$. □

Das G aus Satz 55 heißt Quotientengruppe von $(M, *)$ und wird mit $Q(M)$ bezeichnet.

Man schreibt statt $[(a, b)]_\sim$ auch einfach $\frac{a}{b}$.

Bsp: $\mathbb{Q}^\times := \mathbb{Q}(\mathbb{Z}\setminus\{0\})$

Wir wollen die Null hinzufügen aber auch als Bruch sehen.

$\rightsquigarrow$ Betrachte die Relation $\sim$ auf $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$

$$\mathbb{Q} := \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})/\sim$$

$$= \mathbb{Q}(\mathbb{Z}\setminus\{0\}) \dot\cup \left\{\tfrac{0}{1}\right\}$$

Addition $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$.

Satz 56: $(\mathbb{Q}, +)$ und $(\mathbb{Q}^\times, \cdot)$ sind abelsche Gruppen, es gelten die Distributivgesetze und $1 \cdot \frac{a}{b} = \frac{a}{b}$ für alle $\frac{a}{b} \in \mathbb{Q}$.

Bew.: (Ü A). □

III 2. Endliche Gruppen.

Def 57: Es seien G eine Gruppe und $g \in G$ und $H \leq G$.

a) $\operatorname{ord}(G) := |G|$ heißt die Ordnung von G.

b) $(G:H) := |G/H|$ heißt der Index von H in G.

c) G heißt endliche Gruppe, falls $\operatorname{ord}(G) \in \mathbb{N}$.

d)
$$\operatorname{ord}(g) := \begin{cases} \min\{n \in \mathbb{N} \mid g^n = e\}, \text{ falls die Menge nicht leer ist} \\ \infty, \text{ sonst.} \end{cases}$$

Satz 58 (Satz von Lagrange)

Es seien G eine Gruppe und $H \leq G$. Falls H und G/H endlich sind, so ist G endlich und es gilt

$$\operatorname{ord}(G) = (G:H)\operatorname{ord}(H).$$

Def: Es sei R eine Äquivalenzrelation auf M.
Ein Repräsentantensystem von R bzw. M/R ist eine Menge $N \subseteq M$, sodass

(RS1) $\forall a \in M \; \exists b \in N : aRb$

(RS2) $\forall b_1, b_2 \in N : (b_1 \sim b_2 \Rightarrow b_1 = b_2)$

Nach dem Auswahlaxiom kann man zu jeder Äquivalenzrelation ein Repräsentantensystem finden.

Bew. von Satz 58: Wir wählen ein Repräsentantensystem von G/H: $\{g_i \mid i \in I\}$.

Die Abbildung

$$\{g_i \mid i \in I\} \times H \xrightarrow{\varphi} G$$
$$(g_i, h) \longmapsto g_i h$$

ist eine Bijektion

Bew: Surjektivität: $g \in G \overset{(RS1)}{\Rightarrow} \exists i_0 \in I : g_{i_0} \sim_H g$

Also $g_{i_0} H = gH \Rightarrow \exists h \in H : g = g_{i_0} h$.

$\Rightarrow \varphi(g_{i_0}, h) = g$

Injektivität folgt aus (RS2) (Übung) $\square$

Wir haben also

$$G \xrightarrow[\varphi^{-1}]{\sim} \{g_i \mid i \in I\} \times H \xrightarrow{\sim} \underbrace{\{g_i H \mid i \in I\}}_{\text{RS}} \times H \xrightarrow{\sim} \frac{G}{H} \times H$$

$\downarrow$ $S \leftarrow$ Def. Mächtigkeit

$$\mathbb{N}^{\leq |\frac{G}{H}| \cdot |H|} \xleftarrow[\text{ÜA}]{\sim} \mathbb{N}^{= |\frac{G}{H}|} \times \mathbb{N}^{= |H|}$$

$\square$

$\Rightarrow |G| = |\frac{G}{H}| \cdot |H|$.

↑ Def. der Mächtigkeit einer Menge

Korollar 59: $|H| \mid |G|$, falls G endlich ist.

Übungsaufgabe 60: $\operatorname{ord}(g) = \operatorname{ord}(\langle \{g\} \rangle)$

↑ Wir lassen im Folgenden die Klammern $\{,\}$ weg.

Satz 61 (Satz von Euler) Es sei G eine endliche Gruppe. Dann gilt für $g \in G$:

$$g^{\operatorname{ord}(G)} = e.$$

Beweis: Nach 60 gilt $\operatorname{ord}(g) = \operatorname{ord}(\langle g \rangle)$

und aus Korollar 59 folgt $\operatorname{ord}(\langle g \rangle) \mid \operatorname{ord}(G)$.

$\Rightarrow \exists\, m \in \mathbb{N}$:

$$\operatorname{ord}(g)\, m = \operatorname{ord}(G)$$

$$\Rightarrow g^{\operatorname{ord}(G)} = (g^{\operatorname{ord}(g)})^m \overset{\text{Def. von ord}(g)}{=} e^m = e$$

$\square$

Beispiel: 1) $\mathrm{ord}(\mathbb{Z}/m\mathbb{Z}) = m$, da $\{1, \dots, m\}$ ein Repräsentantensystem von $\mathbb{Z}/m\mathbb{Z}$ ist.

2) $\mathfrak{S}_n := (\mathrm{Bij}(\underline{n}), \circ)$ heißt die symmetrische Gruppe vom Grad n.

$\mathrm{ord}(\mathfrak{S}_n) = n!$

Ein Element σ von $\mathfrak{S}_n$ heißt Permutation und kann wie folgt geschrieben werden

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

Ein Paar $i < j$ mit $\sigma(i) > \sigma(j)$ heißt Inversion von σ.

$$\mathrm{inv}(\sigma) := |\{ i, j \in \underline{n} \mid i < j \wedge \sigma(i) > \sigma(j) \}|$$

Die Gruppe

$$A_n := \{ \sigma \in \mathfrak{S}_n \mid 2 \mid \mathrm{inv}(\sigma) \}$$

heißt die alternierende Gruppe vom Grad n.

$(\mathfrak{S}_n : A_n) = 2$.

Satz 62: Es sei G eine zyklische Gruppe. Dann existiert ein $n \in \mathbb{N}_0$, sodass G isomorph zu $\mathbb{Z}/n\mathbb{Z}$ ist.

$\left[\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z} \right]$

Beweis: $G = \langle g \rangle = \{ g^i \mid i \in \mathbb{Z} \}$ für ein $g \in G$.

1. Fall: $\operatorname{ord}(G) < \infty$ $\quad n := \operatorname{ord}(G)$

Die Abbildung

$$\varphi : G \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$\varphi(g^i) := [i]_n$$

ist wohldefiniert:

$$g^i = g^j \Rightarrow g^{i-j} = e \Rightarrow \operatorname{ord}(g) \mid i-j$$

ist

$$\Rightarrow n = |G| = |\langle g \rangle| = \operatorname{ord}(g) \mid i-j$$

$$\text{d.h. } |\langle g \rangle| = \operatorname{ord}(g)$$

$$\Rightarrow [i]_n = [j]_n.$$

und ein Gruppenisomorphismus:

- $\varphi(g^i g^j) = [i+j]_n = [i]_n + [j]_n = \varphi(g^i) + \varphi(g^j)$
- $\psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$, $\psi([i]_n) = g^i$, ist eine wohldefinierte Inverse von φ.

Fall 2: $\operatorname{ord}(G) = \infty$

$\varphi: G \to \mathbb{Z} \cong \mathbb{Z}/0\mathbb{Z}$, $\varphi(g^i) := i$. Gleicher Beweis wie im Fall 1. □

Allgemeiner kann man zeigen:

Satz 63: Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem Produkt von zyklischen Gruppen; also folglich nach Satz 62 zu einem Produkt der Form

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$

$m_1, \ldots, m_n \in \mathbb{N}_0$.

Bsp: 1) Es sei $(M, *)$ ein Monoid. Dann ist

$M^\times := \{ g \in M \mid g \text{ besitzt eine Inverse in } M \}$ eine Gruppe. (Ü A)

2) $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ ist ein abelscher Monoid.

Beh: $(\mathbb{Z}/m\mathbb{Z})^\times = \{ [z]_m \mid z \in \mathbb{Z},\ \operatorname{ggT}(z, m) = 1 \}$

Bew: Folgt aus dem Lemma von Bézout. □

Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$

$$\varphi(n) := \operatorname{ord}\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right)$$

heißt Eulersche Phi-Funktion.

Satz 6.1 $\Rightarrow \forall\, z \in \mathbb{Z}$ $ggT(z,n)=1$:

$$z^{\varphi(n)} \equiv 1 \mod n.$$

Aus dem chinesischen Restsatz folgt

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \simeq \left(\mathbb{Z}/p_1^{\nu_1}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_\ell^{\nu_\ell}\mathbb{Z}\right)^\times$$

für $n = p_1^{\nu_1} \cdots p_\ell^{\nu_\ell}$ $\quad ggT(p_i, p_j)=1$ für $i \neq j$

p_i prim.

$$\Rightarrow \quad \varphi(n) = \varphi(p_1^{\nu_1}) \cdots \varphi(p_\ell^{\nu_\ell})$$

Die Anzahl der zu p teilerfremden Restklassen in $\mathbb{Z}/p^\nu\mathbb{Z}$ ist $p^\nu - p^{\nu-1}$.

$$\Rightarrow \quad \varphi(n) = (p_1^{\nu_1} - p_1^{\nu_1-1}) \cdots (p_\ell^{\nu_\ell} - p_\ell^{\nu_\ell-1}).$$

$$= p_1^{\nu_1-1} \cdots p_\ell^{\nu_\ell-1} (p_1-1) \cdots (p_\ell-1).$$

Der kleine Satz von Fermat: $z \in \mathbb{Z}$, $p \in \mathbb{N}$ Primzahl, s.d. $ggT(z,p)=1$. Dann gilt $z^{p-1} \equiv 1 \mod p$.

Beweis: $[z]_p \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, da $ggT(z,p)=1$.

Satz von Euler $\Rightarrow$ $\left([z]_p\right)^{p-1} = [1]_p \Rightarrow [z^{p-1}]_p = [1]_p$

$1 \,\hat{=}\, \operatorname{ord}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^\times\right) = p-1$ $\square$

Zusatz: Die Signumfunktion der symmetrischen Gruppe vom Grad n

Def 2.11: 1) Eine Permutation $\sigma \in S_n$ heißt (auch k-Zykel) k-Zyklus, falls paarweise verschiedene Elemente $a_1, \dots, a_k \in \mathbb{N}^{\leq n}$ existieren, so dass

$$\sigma(b) = \begin{cases} a_{i+1} & b = a_i \text{ mit } i < k \\ a_1 & b = a_k \\ b & b \notin \{a_1, \dots, a_k\} \end{cases}$$

gilt. Wir schreiben auch $(a_1\ a_2\ a_3 \dots a_k)$ für den k-Zyklus σ und

$\text{Bahn}(\sigma) = \{b \in \mathbb{N}^{\leq n} \mid \sigma(b) \neq b\}$ heißt dessen Bahn.

2) Es sei $\sigma \in S_n$. $b \in \mathbb{N}^{\leq n}$ heißt Fixpunkt von σ, wenn $\sigma(b) = b$. $\text{Fix}(\sigma) = \{a \in \mathbb{N}^{\leq n} \mid \sigma(a) = a\}$

Satz 2.12: Es sei σ eine Permutation von $\mathbb{N}^{\leq n}$.
Dann existieren (nicht-triviale) Zyklen $\tau_1, \dots, \tau_\ell$, s.d.

$\sigma = \tau_1 \circ \dots \circ \tau_\ell$ und $\text{Bahn}(\tau_i) \cap \text{Bahn}(\tau_j) = \emptyset$

für alle $i, j \in \mathbb{N}^{\leq \ell}$ mit $i \neq j$.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Bew: Existenz: Induktion über $|Fix(\sigma)|$

(IA): $|Fix(\sigma)| = n \Rightarrow \sigma = id_{\mathbb{N}^{\leq n}}$

$id_{\mathbb{N}^{\leq n}}$ ist das Produkt von 0 Zyklen.
(0 Fixen)

(IS)

$|Fix(\sigma)| < n$. Es sei $a \in \mathbb{N}^{\leq n}$ ein Element von $\mathbb{N}^{\leq n} \setminus Fix(\sigma)$.

$\rho := \sigma \circ (a\ \sigma(a))$ hat mehr Fixpunkte als σ, da $\rho(\sigma(a)) = \sigma(a)$, d.h. $|Fix(\rho)| > |Fix(\sigma)|$

$\overset{IV}{\Rightarrow} \exists \tau_1, \dots, \tau_\ell$ nicht-triviale Zyklen mit p.w. disj. Bahnen: $\rho = \tau_1 \circ \dots \circ \tau_\ell$

1. Fall $\left(\bigcup_{i=1}^{\ell} Bahn(\tau_i)\right) \cap \{a, \sigma(a)\} = \emptyset$:

$\Rightarrow \sigma = \tau_1 \circ \dots \circ \tau_\ell \circ (a\ \sigma(a))$ mit p.w. disjunkten Bahnen.

2. Fall: o.E. $Bahn(\tau_1) \cap \{a, \sigma(a)\} \neq \emptyset$:

$\Rightarrow a \in Bahn(\tau_1)$, da $\sigma(a) \notin Fix(\rho)$

$\exists e_1, \dots, e_m$ ($= a$): $\tau_1 = (e_1 \dots e_m)$

Also ist $\tilde{\tau}_1 := \tau_1 \circ (a\ \sigma(a)) = (e_1 \dots e_m\ \sigma(a))$ ein $m+1$-Zyklus, dessen Bahn disjunkt zu den Bahnen von $\tau_2, \dots, \tau_\ell$ ist, da $\sigma(a) \in Fix(\rho)$.

$\Rightarrow \sigma = \varphi \circ (\varphi_\sigma(a)) = \tau_2 \circ \cdots \circ \tau_\ell \circ \tau_1 \circ (a\ \sigma(a))$

$= \tau_2 \circ \cdots \circ \tau_\ell \circ \tilde{\tau}_1$

□ Existenz.

Eindeutigkeit. $\tau_1 \circ \cdots \circ \tau_\ell = \sigma = \tau'_1 \circ \cdots \circ \tau'_{\ell'}$ $\overset{\text{da Fix}(\sigma) = \{\}}{\Rightarrow} \ell' = 0$ falls $\ell = 0$

IS $(\ell > 0)$: Für $a \in \text{Bahn}(\tau_1)$ gilt $\text{Bahn}(\tau_1) = \{\tau_1^i(a) \mid i \in \mathbb{Z}\}$

$= \{\sigma^i(a) \mid i \in \mathbb{Z}\}$.

Aus $\sigma(a) \neq a$ folgt, dass ein Index i existiert, sodass

$a \in \text{Bahn}(\tau_j^i)$ ist.

$\Rightarrow$ $\text{Bahn}(\tau_j^i) = \{\sigma^i(a) \mid i \in \mathbb{Z}\} = \text{Bahn}(\tau_1)$,

und $\tau_j^i(\sigma^i(a)) = \sigma(\sigma^i(a)) = \tau_1(\sigma^i(a))$

($\tau_j = \sigma|_{\text{Bahn}(\tau_j)}$; $\uparrow$ analog)

$\Rightarrow$ $\tau_j^i = \tau_1$.

$\Rightarrow$ $\tau_2 \circ \cdots \circ \tau_\ell = \tau'_1 \circ \cdots \circ \underset{\wedge}{\tau_j^i} \circ \cdots \circ \tau'_{\ell'}$

$\underline{\text{IV}} \Rightarrow \ell = \ell' \wedge \exists\, \varphi : \{2, \ldots, \ell\} \to \{1, \ldots, \ell'\} \setminus \{j\}$:

$\forall_{i=2,\ldots,\ell} : \tau_i = \tau'_{\varphi(i)}$.

Also gilt $\{\tau_1, \ldots, \tau_\ell\} = \{\tau'_1, \ldots, \tau_{\ell'}\}$. □

Bez 2.13: Die Zerlegung $\sigma = \tau_1 \circ \cdots \circ \tau_\ell$, $\text{Bahn}(\tau_i) \cap \text{Bahn}(\tau_j) = \{\}$ $\forall_{i \neq j}$ heißt Zykelzerlegung von σ.

Def 2.14: Die Abbildung $\text{sgn} : S_n \to \{\pm 1\}$ die über die Zykelzerlegung $\sigma = \tau_1 \circ \cdots \circ \tau_\ell$

durch $\operatorname{sgn}(\sigma) = \prod_{i=1}^{k} (-1)^{|\text{Bahn}(\tau_i)|-1}$ definiert ist -91-
heißt Signumfunktion auf S_n

Ü1 Z15:

$\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ ist ein Gruppenhomomorphismus und es gilt

$$\operatorname{sgn}(\sigma) = (-1)^{\text{inv}(\sigma)}$$

Bsp:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 7 & 8 & 4 & 5 & 6 \end{pmatrix} = (1\,2\,3) \circ (4\,7\,5\,8\,6)$$

$$\operatorname{sgn}(\sigma) = (-1)^2 \cdot (-1)^4 = 1 \cdot 1 = 1.$$

$$\text{inv}(\sigma) = |\{(1,3), (2,3), (4,6), (4,7), (4,8), (5,6), (5,7), (5,8)\}| = 8$$

$$(-1)^8 = 1.$$

Zusatz: RSA (Rivest, Shamir, Adleman);

Person A möchte an die Person B eine verschlüsselte Nachricht senden.

B hat zwei Schlüssel: - einen geheimen zum Entschlüsseln von Nachrichten (S)
- einen öffentlichen zum Verschlüsseln von Nachrichten. (T)

[A]

N zu sendende Nachricht.

[B]

(S,T) Schlüssel

Schritte:
- B schickt T zu A
- A verschlüsselt N, bildet also T(N).
- A schickt T(N) zu B.
- B entschlüsselt T(N) mittels S.

RSA: ist eine besondere Wahl der Schlüssel:

n sei eine natürliche Zahl, die Produkt zweier großer Primzahlen ist. $n = q \cdot p \quad p \neq q$

p und q sollten eine ähnliche Größenordnung haben.

- e sei eine natürliche Zahl $1 < e < \varphi(n) = (p-1)(q-1)$

o.d. $ggT(e, \varphi(n)) = 1$.

• $d \in \mathbb{N}$ s.d. $ed \equiv_{\varphi(n)} 1$ (Kann man mit dem

erweit. Alg. berechnen.

Seien $T := (n, e)$ und $S := (d)$

Verschlüsselung: $N \in \mathbb{N}_0^{<n}$ Nachricht.

$T(N) := a \in \mathbb{N}_0^{<n}$ mit

$a \equiv N^e \bmod n$

Entschlüsselung: $T(N)^d \equiv N \bmod n$.

Bsp: $n = 5 \cdot 11$ $\varphi(n) = 4 \cdot 10 = 40$.

$e = 3$, $d = 27 \equiv_{40} -13$

$\left[3 \cdot (-13) \equiv_{40} -39 \equiv_{40} 1 \right]$

$S := (27)$, $T = (55, 3)$

A will die Nachricht 42 versenden.

B gibt A den öffentlichen Schlüssel T.

A verschlüsselt: $T(N) \equiv 42^3 \mod 55$

$42^3 \equiv 6^3 \cdot 7^3 \equiv 216 \cdot 343 \equiv (-4)\cdot(13)$

$\equiv -52 \equiv 3 \mod 55$

Also $T(N) = 3$, da $T(N) \in \mathbb{N}_0^{<55}$.

B entschlüsselt: $3^{27} \equiv_{55} X$

$\Leftrightarrow X \equiv_5 (-2)^{27} \equiv_5 (-1)^{13} \cdot (-2) \equiv_5 2$

$1X \equiv_{11} 3^{27} \equiv_{11} (3^{10})^2 \cdot 3^7 \equiv_{11} 3^7$

Kleiner Fermat

$\equiv_{11} (-2)^3 \cdot 3 \equiv_{11} 3 \cdot 3 \equiv_{11} -2$

Lösen: $X = 11 \cdot r - 2 \equiv_5 r - 2 \Leftrightarrow r \equiv_5 -1$

$\mathbb{Z}/5$

2

Sehe $X = -11 - 2 = -13 \equiv_{55} 42$

Wir suchen den Rest mod 55, der in $\mathbb{N}_0 \leq 41$ liegt. Also ist 42 die Nachricht.

III 3. Ringe und Körper.

III 3.1. Erste Definitionen und Beispiele

Nun betrachten wir das Zusammenspiel von zwei Strukturen $+$ und $\cdot$.

Erinnern Sie sich an $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ und auch $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Def 64: 1) Ein Tripel $(R, +, \cdot)$ bestehend aus einer abelschen Gruppe $(R, +)$ und einer Halbgruppe $(R, \cdot)$, sodass die Distributivgesetze gelten:

$$x(y_1 + y_2) = xy_1 + xy_2$$
$$(y_1 + y_2)x = y_1x + y_2x,$$

heißt Ring. 0_R bezeichnet das neutrale Elt. von $(R, +)$.

2) Ist $(R, +, \cdot)$ ein Ring und $(R, \cdot)$ ein Monoid, dann heißt R ein unitärer Ring, falls $R \neq \{0_R\}$ ist.

Wir bezeichnen das neutrale Element von $(R, \cdot)$ als Einselement und schreiben 1_R. Man sagt auch Ring mit Eins.

3) Ein Ring heißt kommutativ, falls $(R, \cdot)$ abelsch ist.

4) Ein Ring $(K,+,\cdot)$ heißt Körper falls $(K\setminus\{0\},\cdot)$ eine abelsche Gruppe ist.

Bezeichnung: Wenn $(R,+,\cdot)$ ein unitärer Ring ist, so bezeichnet $R^\times$ die Menge aller in $(R,\cdot)$ invertierbaren Elemente, auch Einheiten genannt.

Beispiele 65: 1) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ $(\mathcal{P}(M),\Delta,\cap)$ sind kommutative Ringe mit Eins.

2) $(\mathbb{Q},+,\cdot)$ ist ein Körper.

3) $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ ist ein Körper

$\Leftrightarrow$ $|m|$ ist eine Primzahl.

Beweis von 3): „$\Rightarrow$" Körpereigenschaft

$\Rightarrow (\mathbb{Z}/m\mathbb{Z})^\times = \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$

$\Rightarrow \forall z\in\mathbb{Z}: (m\nmid z \Rightarrow ggT(m,z)=1)$

$\Rightarrow m\neq 0$ und $|m|$ hat keinen Teiler $t\in\mathbb{N}$, o.d. $1<t<|m|$.

$\Rightarrow |m|=1 \vee |m|$ ist eine Primzahl.

Fall $|m|=$ Primzahl ✓

Fall $|m|=1$: $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\}$

Ein Körper hat mindestens zwei Elemente. $\Rightarrow$ ↯

„⇐" Ist $|m|$ ein Primzahl so gilt $(\mathbb{Z}/m\mathbb{Z})^\times = \{[z]_m \mid z \in \mathbb{Z}, \operatorname{ggT}(z,m)=1\}$

$\Vert$ ← Primzahl.

$\mathbb{Z}/m\mathbb{Z} \setminus \{[0]_m\} = \{[z]_m \mid z \in \mathbb{Z}, m \nmid z\}$

Die restlichen Eigenschaften folgen aus 1). □

Def 66: Eine Abbildung $f: (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ heißt Ringhomomorphismus, falls

$$f(x+y) = f(x) + f(y) \quad \text{und}$$
$$f(x \cdot y) = f(x) \cdot f(y)$$

für alle $x, y \in R_1$.

Ein Ringhomomorphismus $f: R_1 \to R_2$ heißt
- Ringepimorphismus, falls f surjektiv ist
- Ringmonomorphismus, falls f injektiv ist
- Ringisomorphismus falls f bijektiv ist.
- unitär, falls R_1 und R_1 unitär sind und $f(1_{R_1}) = 1_{R_2}$ gilt.
- Körperhomomorphismus, falls R_1 und R_2 Körper sind $f(1_{R_1}) = 1_{R_2}$ gilt.

Satz 67: Es sei $(K,+,\cdot)$ ein endlicher Körper. Dann existiert eine Primzahl p sodass $(\mathbb{Z}/p\mathbb{Z},+,\cdot)$ ein Unterkörper von $(K,+,\cdot)$ ist, bis auf Isomorphie. Es gilt $|K| = p^{(\dim_{\mathbb{Z}/p\mathbb{Z}} K)}$.

Bem: Man K als $\mathbb{Z}/p\mathbb{Z}$ Vektorraum ansehen $\dim_{\mathbb{Z}/p\mathbb{Z}} K$ ist die entsprechende Dimension.

Def 68 Es sei R ein unitärer Ring

- Wenn $n 1_R \neq 0_R$ für alle $n \in \mathbb{N}$ so definieren wir $\mathrm{char}(R) = 0$
- Wenn ein $n \in \mathbb{N}$ mit $n 1_R = 0_R$ existiert, dann setzen wir $\mathrm{char}(R) = \min\{n \in \mathbb{N} \mid n 1_R = 0_R\}$

$\mathrm{char}(R)$ heißt die Charakteristik von R.

Beweis: $(K,+,\cdot)$ ist ein Körper $\Rightarrow$ $\mathrm{char}(K) = 0$ oder Primzahl p.

K endlich $\Rightarrow$ $\mathrm{char}(K) = p$ Primzahl.

$\mathbb{Z}/p\mathbb{Z} \to K$.

$[z]_p \mapsto z \cdot 1_K$ Körpermonomorphismus.

$\Rightarrow$ K ist ein $\mathbb{Z}/p\mathbb{Z}$ - Vektorraum

$\Rightarrow$ $K \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p\mathbb{Z}}_{=: n}$

$\rightarrow$ $|K| = p^n$ $\square$

Ein weiterer wichtiger Ring ist der Polynomring in einer Variablen über einem kommutativen Ring R mit 1. (Denken Sie an $\mathbb{Z}[X]$.)

Def 69: Es sei ein kommutativer Ring R mit Eins gegeben.
Ein unitärer kommutativer Ring S heißt Polynomring über R in einer Variablen, falls

(P1) $\exists$ $R \hookrightarrow S$ Ringmonomorphismus mit $1_R \longmapsto 1_S$

(Wir denken uns $R \subseteq S$ mit $1_R = 1_S$)

(P2) $\exists X \in S$: $1, X, X^2, X^3, \dots$ ist eine R-Basis von S, d.h.

(B1) $\forall s \in S \; \exists n \in \mathbb{N} \; \exists r_1, \dots, r_n \in R$:

$$\sum_{i=1}^{n} r_i X^i = s$$

(B2) $\forall n \in \mathbb{N} \; \forall r_1, \dots, r_n \in R$ Wenn $\sum r_i X^i = 0 \Rightarrow \forall i \in \mathbb{N}, i \le n : r_i = 0$.

Wir schreiben $S = R[X]$

So einen Ring S können wir immer finden:

$$S := \{ (a_i)_{i \in \mathbb{N}_0} \mid a_i \in R, a_i = 0 \text{ für fast alle } i \}$$

(d.h. alle bis auf endlich viele)

$$(a_i)_{i \in \mathbb{N}_0} + (b_i)_{i \in \mathbb{N}_0} := (a_i + b_i)_{i \in \mathbb{N}_0}$$

$$(a_i)_{i \in \mathbb{N}_0} \cdot (b_i)_{i \in \mathbb{N}_0} := \left(\sum_{\substack{j+\ell = i \\ j,\ell \in \mathbb{N}}} a_j b_\ell \right)_{i \in \mathbb{N}_0}$$

Bsp: $(0,1,1,0,1,0,0,\ldots) \cdot (1,0,1,1,0,1,0,0,\ldots)$

$= (0, 0\cdot 0 + 1\cdot 1, 0\cdot 1 + 1\cdot 0 + 1\cdot 1, 0\cdot 1 + 1\cdot 1 + 1\cdot 0 + 0\cdot 1,$

$0\cdot 0 + 1\cdot 1 + 1\cdot 1 + 0\cdot 0 + 1\cdot 1, 0\cdot 1 + 1\cdot 0 + 1\cdot 1 + 0\cdot 1 + 1\cdot 0 + 0\cdot 1,$

$0\cdot 0 + 1\cdot 1 + 1\cdot 0 + 0\cdot 1 + 1\cdot 1 + 0\cdot 0 + 0\cdot 1, \ldots)$

$= (0,1,1,1,3,1,2,2,0,1,0,0,\ldots)$

$X := (0,1,0,0,\ldots)$

$1_S = (1,0,0,0,\ldots)$

Bedeutung: Unter anderem sind Polynomringe zur Konstruktion von neuen Ringen wichtig.

Beispiel: Wir wollen $\mathbb{Z}$ zu einem Ring T erweitern, s.d. T eine Quadratwurzel von -1 enthält. $P, Q \in \mathbb{Z}[X]$

$$P \sim_{X^2+1} Q \underset{\text{Def}}{\Leftrightarrow} X^2+1 \mid P-Q$$

(d.h. $\exists\, P' \in \mathbb{Z}[X]$: $(X^2+1)P' = P-Q$).

$\left(\mathbb{Z}[X]/\sim_{X^2+1}, +, \cdot\right)$ "enthält" $\mathbb{Z}$ via

$$\mathbb{Z} \hookrightarrow \mathbb{Z}[X]/\sim_{X^2+1}$$

$$z \longmapsto [z]_\sim = z \cdot [1]_\sim$$

und $[X]_\sim^2 = [X^2]_\sim = [-1]_\sim = -[1]_\sim$,

wobei $+$ und $\cdot$ wie üblich definiert sind.

Dieses Verfahren enthält zwei Schritte

1. Schritt: Bilde $\mathbb{Z}[X]$
2. Schritt: Gegeben eine "schöne" Äquivalenzrelation $\sim$, dann ist $\mathbb{Z}[X]/\sim$ ein Ring.

Im nächsten Abschnitt studieren wir Schritt 2 für beliebige kommutative Ringe mit 1.

Zusätzlicher Hinweis zum RSA:

Person A kennt die Primzahlen p und q nicht und ist nicht in der Lage p und q aus n zu bestimmen. Deshalb kann A

$N^e \equiv T(N) \bmod n$ nicht mit dem System ($N^e \equiv_p T(N)$ und $N^e \equiv_q T(N)$) berechnen $\not\Rightarrow$

Person B dagegen kann es, da B die Primzahlen p und q kennt.

Zum Bsp: $N = 42$. $T = (5, 5, 3)$

A berechnet $42^3 \equiv_{55} (-13)^3 \equiv_{55} -169 \cdot 13$

$\equiv_{55} (-4) \cdot 13 \equiv_{55} -52 \equiv_{55} 3$

entschlüsselt mit $S(d) = (27)$

$3^{27} \equiv_{55} N$ mittels Lösen des Systems

($N \equiv_5 3^{27} \equiv_5 (-2)^{27} \equiv_5 (-1)^{13}(-2) \equiv_5 2$

$\wedge \quad N \equiv_{11} 3^{27} \equiv_{11} (-2)^{13} \cdot 3 \equiv (-2)^{10}(-2)^3 \cdot 3$

$\equiv_{11} 1 \cdot (-2)^3 \cdot 3 \equiv_{11} -24 \equiv_{11} -2$)

$\Rightarrow$ klare Lösung

Wichtiges Beispiel zu Ringen (Zusatz)

Es sei R ein kommutativer Ring. $n \in \mathbb{N}$

Ein Gruppenhomomorphismus $f: (R^n, +) \longrightarrow (R^n, +)$ heißt R-linear, falls für jedes $r \in R$ und $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in R^n$ die Gleichung $f(r \cdot x) = r f(x)$ gilt, wobei $r \cdot x = \begin{pmatrix} r x_1 \\ \vdots \\ r x_n \end{pmatrix}$ definiert ist.

Bez 16: $\mathrm{Hom}_R(R^n, R^n) := \{ f \in \mathrm{Hom}_{\text{Gruppen}}((R^n,+),(R^n,+)) \mid f \text{ ist } R\text{-linear} \}$

$\| \cdot$

$\mathrm{End}_R(R^n)$.

Def 17: Wir bezeichnen $M_n(R) = \underbrace{R^n \times \cdots \times R^n}_{n \text{ mal}}$

die Menge der $n \times n$ Matrizen mit Einträgen in R. Auf $M_n(R)$ haben wir eine Addition

$$+ : \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{n1}+b_{n1} & \cdots & a_{nn}+b_{nn} \end{pmatrix}$$

und eine Multiplikation

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{n1} & & a_{nn} \end{pmatrix} \circ \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ b_{n1} & & b_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}$$

mit $c_{ij} := \sum_{k=1}^{n} a_{ik} b_{kj}$.

Bsp: In $M_2(\mathbb{Z})$:

$$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}$$

Insbesondere ist $(M_2(\mathbb{Z}), \cdot)$ nicht abelsch.

Satz 18: Es sei R ein kommutativer unitärer Ring. Dann sind $(M_n(R), +, \cdot)$ und $(\mathrm{End}_R(R^n), +, \circ)$ zueinander isomorphe unitäre Ringe.

Beweis: 1) $(M_n(R), +, \cdot)$ ist ein unitärer Ring:

- $(M_n(R), +)$ ist als direktes Produkt von abelschen Gruppen eine abelsche Gruppe.
- $(M_n(R), \cdot)$ ist assoziativ:

$$(A \cdot B) \cdot C = D$$

$$A \cdot (B \cdot C) = E$$

mit $d_{ij} = \sum_{\ell} \left(\sum_{k} a_{ik} b_{k\ell} \right) c_{\ell j}$

$$e_{ij} = \sum_{k} a_{ik} \left(\sum_{\ell} b_{k\ell} c_{\ell j} \right)$$

$$\Rightarrow \quad d_{ij} = \sum_{\ell} \sum_{k} (a_{ik} b_{k\ell}) c_{\ell j} \qquad \text{(Distrib.)}$$

$$= \sum_{\ell} \sum_{k} a_{ik} (b_{k\ell} c_{\ell j}) \qquad \text{(R_1) assoziativ}$$

$$= \sum_{k} \sum_{\ell} a_{ik} (b_{k\ell} c_{\ell j}) = \sum_{k} a_{ik} \left(\sum_{\ell} b_{k\ell} c_{\ell j} \right) \qquad \text{Distr.}$$

+ abelsch und an. $= e_{ij}$.

- $I_n = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ ist das neutrale Element bezüglich $\cdot$.
- Distributivgesetz:

$$(A+B)C = \left(\sum_{k} (a_{ik} + b_{ik}) c_{kj} \right)_{i,j}$$

$$= \left(\sum_{k} a_{ik} c_{kj} + b_{ik} c_{kj} \right)_{i,j}$$

$$= \left(\sum_{k} a_{ik} c_{kj} \right)_{i,j} + \left(\sum_{k} b_{ik} c_{kj} \right)_{i,j}$$

$$= AC + BC$$

analog $\quad CA + CB = C(A+B)$

2) $(\mathrm{End}_R(R^n), +, \circ)$ ist ein unitärer Ring

$((f+g)(x) := f(x) + g(x))$

- $(\mathrm{End}_K(K^4), +)$ ist eine abelsche Gruppe.
  (Übungsaufgabe)
- $(\mathrm{End}_K(K^4), \circ)$ ist ein Monoid
  völlig analog zum Beweis zu Bsp 44.
- Distributivgesetze:
  - $((f+g)\circ h)(x) = (f+g)(h(x)) \overset{\text{Def von } +}{=} f(h(x)) + g(h(x))$
    $= f\circ h(x) + (g\circ h)(x)$.
    $\times$ bel. $\Rightarrow (f+g)\circ h = (f\circ h) + (g\circ h)$

  und
  $(h\circ(f+g))(x) = h((f+g)(x)) = h(f(x)+g(x))$
  $\overset{h \text{ ist additiv}}{=} h(f(x)) + h(g(x)) = (h\circ f)(x) + (h\circ g)(x)$
  $= (h\circ f + h\circ g)(x)$

3) Isomorphie Übungsaufgabe in der neuen Serie. □

III 3.2 Ideale

Ab jetzt: Alle Ringe, die wir von jetzt an betrachten, sind kommutativ. Deshalb lassen wir ab jetzt das Attribut kommutativ bei Ringen weg. (in der VL)

Def 70: Es sei R ein Ring. Eine Teilmenge J von R heißt Ideal, falls $(J,+)$ eine Untergruppe von $(R,+)$ ist und für jedes $r \in R$ und jedes $x \in J$ das Produkt $r \cdot x$ ein Element von J ist.

Bsp 70: 1) $m\mathbb{Z}$ ist ein Ideal von $\mathbb{Z}$, denn $(m\mathbb{Z},+) \leq (\mathbb{Z},+)$ und $\forall z \in \mathbb{Z}$ und $mz' \in m\mathbb{Z}$ gilt:

$$z \cdot mz' = mzz' \in m\mathbb{Z}.$$

2) Bsp. 1) gilt viel allgemeiner. R sei ein Ring. Für $r \in R$ ist $rR = \{rr' \mid r' \in R\}$ ein Ideal von R.

Beweis: $J := rR$.

a) $(J,+)$ ist eine UG von $(R,+)$: $J \neq \emptyset$, da $0_R = r \cdot 0_R \in J$.

$x = rr_1, y = rr_2 \in J \Rightarrow x - y = r(r_1 - r_2) \in rR = J$

UG-Kriterium $\Rightarrow$ Beh.

b) Für $r_0 \in R$ und $x = rr_1 \in rR = J$ gilt

$$r_0 x = r_0(rr_1) = (r_0 r) r_1 = (rr_0) r_1 = r(r_0 r_1) \in rR = J.$$

a) & b) $\Rightarrow$ J ist ein Ideal von R. □

3) $R = (\mathcal{P}(M), \triangle, \cap)$ ist ein Ring mit Eins. ($1_R = M$). Es sei $N \subseteq M$.

Dann gilt $\mathcal{P}(N)$ ist ein Ideal von R.

Bew: a) Wir zeigen erst einmal, dass
$(\mathcal{P}(M), \triangle, \cap)$ ein kommutativer Ring ist.

- $(\mathcal{P}(M), \triangle)$ ist eine Gruppe nach S. 5.1.1
- $(\mathcal{P}(M), \cap)$ ist ein Monoid, da

$$(A \cap B) \cap C = \{x \mid x \in A \cap B \wedge x \in C\}$$
$$= \{x \mid (x \in A \wedge x \in B) \wedge x \in C\}$$
$$= \{x \mid x \in A \wedge (x \in B \wedge x \in C)\}$$
$$= A \cap (B \cap C)$$

und $A \cap M = A = M \cap A$.

- $(\mathcal{P}(M), \cap)$ ist abelsch, da „1" kommutativ ist.
- Distributivgesetze.

z.Z. $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$ und
$C \cap (A \triangle B) = (C \cap A) \triangle (C \cap B)$.

Die zweite Gleichung folgt aus der ersten, da „$\cap$" abelsch ist. Wir zeigen die erste Gleichung:

„$\subseteq$": $x \in (A \triangle B) \cap C \Rightarrow x \in (A \setminus B) \cup (B \setminus A) \wedge x \in C$.

Fall $x \in A \setminus B$: Aus $x \in C \wedge x \in A \setminus B$ folgt $x \in A \cap C$
„ $x \in C \wedge x \notin B$ „ $x \notin B \cap C$

Also $x \in (A \cap C) \setminus (B \cap C) \subseteq (A \cap C) \triangle (B \cap C)$

Fall $x \in B \setminus A$: analog zum obigen Fall.

„$\supseteq$": $x \in (A \cap C) \triangle (B \cap C) \Rightarrow x \in (A \cap C) \setminus (B \cap C)$
oder $x \in (B \cap C) \setminus (A \cap C)$.

O.E. sei $x \in (A \cap C) \setminus (B \cap C)$.
$\Rightarrow x \in A \cap C \Rightarrow x \in A \wedge x \in C$.
Aus $x \notin B \cap C$ und $x \in C$ folgt $x \notin B$.

Also $x \in A \setminus B$ und $x \in C$. Also $x \in (A \triangle B) \cap C$.

b) Nun zeigen wir, dass $\mathcal{P}(N)$ ein Ideal von $(\mathcal{P}(M), \Delta, \cap)$ ist.

- $(\mathcal{P}(N), \Delta)$ ist eine Gruppe nach S. 5.1.1. und $\mathcal{P}(N) \subseteq \mathcal{P}(M)$. Also ist $(\mathcal{P}(N), \Delta)$ eine UG von $(\mathcal{P}(M), \Delta)$.
- Für $A \in \mathcal{P}(M)$ und $B \in \mathcal{P}(N)$ gilt: $A \cap B \subseteq B \subseteq N$. Also $A \cap B \in \mathcal{P}(N)$.

Damit ist $\mathcal{P}(N)$ ein Ideal von $\mathcal{P}(M)$. □

3) $(X^2+1) \trianglelefteq \mathbb{Z}[X]$ ist ein Ideal von $\mathbb{Z}[X]$.

Bem 71: Es sei R ein Ring und J ein Ideal von R. $(J,+)$ ist eine Untergruppe von $(R,+)$ und $(R,+)$ ist abelsch. Also $(J,+)$ ist ein Normalteiler von $(R,+)$. Folglich ist $(R/J, +)$ eine Gruppe.

WH zur Def von $(R/J, +)$: Wir haben die folgende Äquivalenzrelation auf R: $x \sim_J y \Leftrightarrow_{def} x - y \in J$

$[x]_J := \{x' \in R \mid x' \sim_J x\}$ ist die Äquivalenzklasse von x.

$= x + J$

$R/J = \{[x]_J \mid x \in R\}$

$[x]_J + [y]_J := [x+y]_J$ ist wohldef. da $(J,+) \trianglelefteq (R,+)$.

Wir schreiben auch $\equiv_J$ für $\sim_J$

Bsp: $R = \mathbb{Z}$, $J = 3\mathbb{Z}$. $R/J = \mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$

Satz 7.2: Es sei R ein Ring und J und I Ideale von R. Dann gelten:

1) $(J, +, \cdot)$ ist ein Ring.
2) $J \cap I$ und $J + I$ sind Ideale.
3) $\left(R/J, +_{R/J}, \cdot_{R/J}\right)$ mit $[x]_J \cdot_{R/J} [y]_J := [xy]_J$ ist ein kommutativer Ring.

Vorsicht: $[x]_J = x + J$. Die Mengen

$[x]_J \cdot_{R/J} [y]_J = [xy]_J$ und

$(x+J)\cdot(y+J) = \{x'y' \mid x' \in x+J,\ y' \in y+J\}$

sind oftmals verschieden.

Bsp: $[2]_4 \cdot_{\mathbb{Z}/4\mathbb{Z}} [2]_4 = [4]_4 = [0]_4 = 4\mathbb{Z}$

$(2+4\mathbb{Z})\cdot(2+4\mathbb{Z}) = \{(2+4z_1)(2+4z_2) \mid z_1, z_2 \in \mathbb{Z}\}$

$\subseteq 4 + 8\mathbb{Z} \subsetneq 4\mathbb{Z}$. ⌟

Bez: $\left(R/J, +_{R/J}, \cdot_{R/J}\right)$ heißt der Faktorring von R modulo J.

Wir lassen im Folgenden das Subscript R/J weg.

Beweis von Satz 7.2:

1) $(J,+) \leq (R,+)$ da J ein Ideal ist. Des Weiteren ist $+$ abelsch

$\forall x, y \in J: xy \in J$ -11-

- $(J,\cdot)$ ist assoziativ, weil $(R,\cdot)$ assoziativ ist.
- $(J,+,\cdot)$ erfüllt die Distributivgesetze, da $(R,+,\cdot)$ diese erfüllt

Also ist $(J,+,\cdot)$ ein Ring.

2) Wir zeigen hier nur, dass $J \cap \mathcal{Y}$ ein Ideal ist. Der Schnitt von UG von $(R,+)$ ist wieder eine UG von $(R,+)$. Also ist $(\mathcal{Y} \cap J, +)$ eine UG von $(R,+)$. Für $r \in R$ und $x \in J \cap \mathcal{Y}$ gilt

$r \in R \wedge x \in J \wedge x \in \mathcal{Y}$.

Also $rx \in J$ und $rx \in \mathcal{Y}$, da J und $\mathcal{Y}$ Ideale sind. Also $rx \in J \cap \mathcal{Y}$.

3) Wir wissen schon, dass $\left(\frac{R}{J},+\right)$ eine abelsche Gruppe ist

- $\left(\frac{R}{J},\cdot\right)$ ist eine wohldef. abelsche Halbgruppe.

Wohldefiniertheit von „$\cdot$“: Es sei $x \sim_J x'$ und

$$y \sim_J y' \overset{\text{Def. } \sim_J}{\Longrightarrow} x - x', y - y' \in J$$

$$\Rightarrow xy - x'y' = x(y-y') + y'(x-x') \in J$$

(J Ideal)

$$\overset{\text{Def. } \sim_J}{\Longrightarrow} xy \sim_J x'y' \Rightarrow [xy]_J = [x'y']_J.$$

Die Assoziativität von „·" ist eine einfache Übung. Analog die Kommutativität.

- Distributivgesetz. $\left(\frac{R}{J}, \cdot\right)$ ist kommutativ. Deshalb reicht es ein Distributivgesetz zu zeigen.

$$[x]_J([y]_J + [z]_J) \overset{\text{Def +}}{=} [x]_J [y+z]_J$$

$$\overset{\text{Def.}}{=} [x(y+z)]_J \overset{\text{Distr.}}{=} [xy + xz]_J \overset{\text{Def +}}{=} [xy]_J + [xz]_J$$

$$\overset{\text{Def.}}{=} [x]_J [y]_J + [x]_J [z]_J \qquad \square$$

Bsp: 1) Übungsaufgabe $\frac{\mathcal{P}(M)}{\mathcal{P}(N)} \cong \mathcal{P}(M \setminus N)$ für alle $N \subseteq M$.

2) $$\frac{\mathbb{Z}[X]}{(X^2+1)\mathbb{Z}[X]} = \frac{\mathbb{Z}[X]}{\sim_{X^2+1}}$$

da für $P, Q \in \mathbb{Z}[X]$ gilt:

$$P \underset{X^2+1}{\sim} Q \overset{\text{Def } \sim_{X^2+1}}{\Leftrightarrow} X^2+1 \mid P-Q$$

$$\Leftrightarrow \exists\, S \in \mathbb{Z}[X] : (X^2+1) \cdot S = P-Q$$

$$\Leftrightarrow P - Q \in (X^2+1)\mathbb{Z}[X]$$

$$\overset{\text{Def } \sim_{(X^2+1)\mathbb{Z}[X]}}{\Leftrightarrow} P \sim_{(X^2+1)\mathbb{Z}[X]} Q.$$

3) $m(\mathbb{Z}[X])$ ist ein Ideal von $\mathbb{Z}[X]$ und es gilt $\dfrac{\mathbb{Z}[X]}{m(\mathbb{Z}[X])} \cong \dfrac{\mathbb{Z}}{m\mathbb{Z}}[X]$

Bew: $\Phi : \dfrac{\mathbb{Z}[X]}{m\mathbb{Z}[X]} \longrightarrow \dfrac{\mathbb{Z}}{m\mathbb{Z}}[X]$.

$\Phi([P]_{m\mathbb{Z}[X]}) := \overline{P}$

mit $\overline{\sum_{i=0}^{\ell} z_i X^i} := \sum_{i=0}^{\ell} [z_i]_m X^i$.

(Wir nehmen von den Koeffizienten von P die Restklassen mod m.)

- Φ ist wohldef: $m(\mathbb{Z}[X]) = \{mQ \mid Q \in \mathbb{Z}[X]\}$

$= \{\sum_{i=0}^{\ell} m a_i X^i \mid \ell \in \mathbb{N}_0,\ a_i \in \mathbb{Z}\}$

$= \{Q \in \mathbb{Z}[X] \mid$ Alle Koeff. von Q sind durch m teilbar.$\}$

Es seien $P_1, P_2 \in \mathbb{Z}[X]$ mit $P_1 \equiv P_2 \bmod m\mathbb{Z}[X]$

$\Rightarrow P_1 - P_2 \in m(\mathbb{Z}[X]) \Rightarrow$ Alle Koeff von $P_1 - P_2$ sind durch m teilbar. $\Rightarrow \overline{P_1} - \overline{P_2} = \overline{P_1 - P_2} = 0 \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}[X]$

$\Rightarrow \overline{P_1} = \overline{P_2}$. Also ist Φ wohldefiniert.

(↑ Def.)

- Φ ist ein Ringhomomorphismus:

$$P = \sum_{i=0}^{\ell} a_i X^i \,, \quad Q = \sum_{i=0}^{t} b_i X^i$$

Setze $a_i = 0$ für $i > \ell$ und $b_i = 0$ für $i > t$.

$\Rightarrow$ sei $\ell = t$.

$$\Phi([P] + [Q]) = \Phi([P+Q]) = \overline{P+Q}$$

$$= \overline{\sum_i (a_i + b_i) X^i} = \sum_i [a_i + b_i]_m X^i$$

$$= \sum_i ([a_i]_m + [b_i]_m) X^i = \sum_i [a_i]_m X^i + \sum_i [b_i]_m X^i$$

$$= \overline{P} + \overline{Q} = \Phi(P) + \Phi(Q)$$

$$\Phi([P][Q]) = \Phi([PQ]) = \overline{PQ} = \sum_i \sum_{s+t=i} a_s b_t X^i$$

$$= \sum_i \sum_{s+t=i} [a_s b_t]_m X^i = \left(\sum_s [a_s]_m X^s\right) \cdot \left(\sum_t [b_t]_m X^t\right)$$

$$= \overline{P}\,\overline{Q} = \Phi(P)\,\Phi(Q)$$

- Φ ist surjektiv, da $\forall_\ell \; \forall_{[a_i]_m \in \mathbb{Z}/m\mathbb{Z}}$ gilt

$$\sum [a_i]_m X^i = \Phi([\textstyle\sum a_i X^i])$$

- Φ ist injektiv, da $\ker(\Phi) = \{[P] \mid \Phi([P]) = 0\}$

$$= \{[P] \mid \overline{P} = 0 \in \mathbb{Z}/m\mathbb{Z}[X]\}$$

$$= \{[P] \mid \text{alle Koeffizienten von } P \text{ liegen in } [0]_m\}$$

$$= \{[P] \mid \text{— 4 —} \quad \text{sind durch } m \text{ teilbar}\}$$

$= \{[p] \mid p \in m(\mathbb{Z}[X])\} = \{[0]\}$ □

↑ siehe Anfang

Satz 73: (Isomorphiesätze) R sei ein Ring. I, I_1, I_2 seien Ideale von R. S sei ein weiterer Ring

1. Isomorphiesatz: Es sei $f: R \to S$ ein Ringhomomorphismus. Dann ist

$$\ker(f) = \{r \in R \mid f(r) = 0_S\}$$

ein Ideal von R und

$$R/\ker(f) \underset{\text{Ring}}{\cong} \operatorname{im}(f) \quad \text{via}$$

$$[x] \longmapsto f(x).$$

2. Isomorphiesatz: Wenn $I_1 \subseteq I_2 \subseteq R$, dann gilt

$$\frac{R/I_1}{I_2/I_1} \underset{\text{Ring}}{\cong} R/I_2.$$

3. Isomorphiesatz:

$$I_1/(I_1 \cap I_2) \underset{\text{Ring}}{\cong} (I_1 + I_2)/I_2.$$

Bew.: Übungsaufgabe. □

Jetzt kommen wir zur ersten Verallgemeinerung eines zahlentheoretischen Resultats aus Kapitel II.

Zur Erinnerung: (chin. Restsatz)

$$\mathbb{Z}/(m_1\mathbb{Z} \cap \dots \cap m_n\mathbb{Z}) \cong \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$$

$$[z] \longmapsto ([z]_{m_1}, \dots, [z]_{m_n})$$

Satz 74 (chinesischer Restsatz für Ringe):

Es seien I und J Ideale eines kommutativen Rings R, s.d. $I + J = R$.

Dann gilt $\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}$.

$$[r] \mapsto ([r]_I, [r]_J).$$

Beweis: Die Abbildung ist ein wohldefinierter Ringhomomorphismus (Übung)

Injektivität: wir call die map f.

$$\ker(f) = \{ [x]_{I \cap J} \mid [x]_I = [0]_I \wedge [x]_J = [0]_J \}$$

$$= \{ [x]_{I \cap J} \mid x \in I \wedge x \in J \}$$

$$= \{ [x]_{I \cap J} \mid x \in I \cap J \}$$

$$= \{ [0]_{I \cap J} \}$$

Surjektivität: $[r_1]_I \in \frac{R}{I}$ $[r_2]_J \in \frac{R}{J}$

$I + J = R \Rightarrow \exists\, x' \in I,\ y' \in J:$

$$x' + y' = 1_R.$$

$$x := r_2 x' + r_1 y'$$

$$\Rightarrow x + I = r_1 y' + I = r_1 y' + r_1 x' + I = r_1 + I$$

$$x + J = r_2 x' + J = r_2 x' + r_2 y' + J = r_2 + J.$$

□

Def 75: Es sei R ein Ring und $Y \subseteq R$.

$$\text{Ideal}(Y) = \bigcap_{\substack{J \text{ Ideal von } R \\ Y \subseteq J}} J$$

das kleinste Ideal von R bzgl. „$\subseteq$", das Y enthält.

Ein Ideal J heißt endlich erzeugt, falls $J = \text{Ideal}(Y)$ für eine endliche Teilmenge Y von J.

J heißt Hauptideal, falls $\exists x \in J : \text{Ideal}(\{x\}) = J$.

also $Rx = J$ (falls $1 \in R$). Statt $\text{Ideal}(\{x_1, \dots, x_n\})$ schreiben wir auch $(x_1, \dots, x_n)_R$, genauso $(Y)_R = \text{Ideal}(Y)$.

Wir wollen nun für Ideale das Pendant zu Primzahlen finden

Idee: Statt $p \in \mathbb{Z}$ Primzahl, stellen Sie sich

$(p)_{\mathbb{Z}} = p\mathbb{Z}$ vor.

$(p)_{\mathbb{Z}}$ hat besondere Eigenschaften.

Def 76: R sei ein Ring. Ein Ideal $\mathfrak{p} \subsetneq R$ von R heißt Primideal, falls

$\forall a, b \in R : (ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p})$

Ein Ideal $\mathfrak{m} \subsetneq R$ heißt Maximalideal, falls kein Ideal J von R existiert, s.d. $\mathfrak{m} \subsetneq J \subsetneq R$.

(M ist unter allen echten Idealen (d.h. $\neq R$) von R maximal bzgl. „$\subseteq$“) 109-4-

Satz 7.7: 1) Alle Ideale von $\mathbb{Z}$ haben die Form $m\mathbb{Z}$, $m \in \mathbb{Z}$.

2) $m\mathbb{Z}$ ist ein Primideal $\Leftrightarrow m = 0 \vee$ $|m|$ ist eine Primzahl.

3) $m\mathbb{Z}$ ist ein Maximalideal $\Leftrightarrow$ $|m|$ ist eine Primzahl.

Beweis: 1) Es sei J ein Ideal von $\mathbb{Z}$

Aus $z \in J$ folgt $-z \in J \Rightarrow J \cap \mathbb{N}_0 \neq \emptyset$.

Fall $J \cap \mathbb{N} = \emptyset \Rightarrow J = \{0\}$.

Fall $J \cap \mathbb{N} \neq \emptyset$. Es sei $m := \min(J \cap \mathbb{N})$

Beh: $J = m\mathbb{Z}$.

Bew: $\subseteq$ $z \in J$

↳ Seite 110

$\Rightarrow \exists\, q \in \mathbb{Z},\ r \in \mathbb{N}_0^{\leq m-1} : z = qm + r$

↑ Division mit Rest.

$\Rightarrow \quad r = z - qm \in J \ , \ 0 \leq r < m.$

$\Rightarrow \quad r = 0 \quad \Rightarrow \quad z \in m\mathbb{Z}.$

↑ $m = \min(J \cap \mathbb{N})$

„$\supseteq$" $\quad m \in J \ , \ J$ Ideal $\Rightarrow \mathbb{Z}m \subseteq J$.

2) Wenn $|m|$ eine Primzahl ist, folgt aus Satz 26, dass $m\mathbb{Z}$ ein Primideal ist.
$0\mathbb{Z} = \{0\}$ ist ein " , da $\mathbb{Z}$ nullteilerfrei ist ($ab = 0 \Rightarrow a = 0 \vee b = 0$)

Aus Satz 26 folgt auch, dass wenn $m\mathbb{Z} \neq \{0\}$ ein Primideal ist, dass dann $|m|$ eine Primzahl ist.

3) $\{0\}$ ist kein Maximalideal.
Es sei $m\mathbb{Z} \neq \{0\}$ ein Maximalideal und p eine Primzahl.

$\Rightarrow \quad m\mathbb{Z} \subseteq p\mathbb{Z} \subsetneq R \Rightarrow \quad m\mathbb{Z} = p\mathbb{Z}$

↑ Maximalideal

$\Rightarrow \quad m \mid p \quad \Rightarrow \quad |m| = 1 \vee |m| = p$

↑ p Primzahl.

$\Rightarrow \quad |m| = p.$

($m\mathbb{Z} \neq \mathbb{Z} \Rightarrow |m| \neq 1$)

Umgekehrt ist $p\mathbb{Z}$ ein Maximalideal

$p\mathbb{Z} \subseteq J \subsetneq \mathbb{Z} \Rightarrow n \mid p \Rightarrow n = 1 \vee n = p$

$J = n\mathbb{Z}$, $n > 0$; $n > 0$, p Primzahl

$\Rightarrow$ $n \neq 1$ da $n\mathbb{Z} \neq \mathbb{Z}$ $\quad n = p \Rightarrow J = p\mathbb{Z}$ $\square$

Beispiel: Ring der Gaußschen Zahlen

$\mathbb{Z}[i] = \mathbb{Z}[X] / (X^2+1)$ $\qquad i = \sqrt{-1}$

$13\mathbb{Z}$ ist ein Primideal in $\mathbb{Z}$, aber

$13\mathbb{Z}[i]$ ist kein n in $\mathbb{Z}[i]$.

da $13 = (3+2i)(3-2i)$, aber

$3+2i,\ 3-2i \notin 13\mathbb{Z}[i]$, da

$13 \nmid 3$.

Die Primideale von $\mathbb{Z}[i]$ sind

(0), $p\mathbb{Z}[i]$, p Primzahl $p \equiv_4 3$;

$(n \pm im)\mathbb{Z}[i]$, n^2+m^2 Primzahl.

Bsp: (Primideal und Maximalideal)

$$(X-3) \underset{\mathbb{Z}[X]}{\subsetneq} (X-3,7) \underset{\mathbb{Z}[X]}{\subsetneq} (X-7) \underset{\mathbb{Z}[X]}{}$$

a) $(X-3)_{\mathbb{Z}[X]}$ ist ein Primideal:

$Q \cdot P \in (X-3)\mathbb{Z}[X] \Rightarrow$

Polynomdivision $Q = (X-3)S + R \quad \deg R < 1$

$P = (X-3)T + U \quad \deg U < 1$

d.h. $R, U \in \mathbb{Z}$.

$X-3$ teilt $QP = (X-3)((X-3) + RT + SU) + RU$.

$\Rightarrow X-3 \mid RU. \Rightarrow 0 = RU(3) = R(3)U(3) = R \cdot U$

$\Rightarrow R = 0 \vee U = 0 \Rightarrow Q \in (X-3)\mathbb{Z}[X]$ $\quad \vee P \in (X-3)\mathbb{Z}[X]$

$R, U \in \mathbb{Z}$

$\mathbb{Z}$ ist nullteilerfrei

b) $(X-3,7)_{\mathbb{Z}[X]} = (X-3)\mathbb{Z}[X] + 7\mathbb{Z}[X]$ ist ein Maximalideal:

- z.z. $(X-3,7)_{\mathbb{Z}[X]} \neq \mathbb{Z}[X]$

Annahme "=": $1 = (X-3)S + 7T$

für geeignete $S, T \in \mathbb{Z}[X]$

$\Rightarrow 1 = (3-3)S(3) + 7 \cdot T(3) = 7 \cdot T(3)$

$\Rightarrow 7 \mid 1 \; \lightning$

- z.z. $\forall$ I Ideal von $\mathbb{Z}[X]$:

- $(X-3,7)_{\mathbb{Z}[X]} \subsetneq J \subsetneq \mathbb{Z}[X]$

Aus doch: Wähle $P \in J \setminus (X-3,7)_{\mathbb{Z}[X]}$

Division mit Rest

$\Rightarrow \exists_{S,R}\ P = (X-3)\cdot S + R \qquad \deg R < 1, \text{d.h.}$

$R \in \mathbb{Z}$

$P \notin (X-3,7)_{\mathbb{Z}[X]} \Rightarrow 7 \nmid R$

$\Rightarrow \quad (7,R)_{\mathbb{Z}} = 7\mathbb{Z} + R\mathbb{Z} = ggT(7,R)\mathbb{Z}$

$= 1\mathbb{Z}$

$\Rightarrow 1 \in (7,R)_{\mathbb{Z}} \subseteq J$

$\uparrow$

$R = P - (X-3)S \in J$

$\Rightarrow \mathbb{Z}[X] = \mathbb{Z}[X]\cdot 1 \subseteq J \subsetneq \mathbb{Z}[X]$ ↯ da $J \neq \mathbb{Z}[X]$

c) Die drei Ideale sind verschieden.

- $(X-3)_{\mathbb{Z}[X]} \subsetneq (X-3,21)_{\mathbb{Z}[X]}$ da jedes Polynom aus $(X-3)_{\mathbb{Z}[X]}$ 3 als Nullstelle hat, und 21 nicht 3 als Nullstelle hat.

- $(X-3,21)_{\mathbb{Z}[X]} \subsetneq (X-3,7)_{\mathbb{Z}[X]}$

da alle

Elemente P aus $(\mathbb{Z}-3, 17)_{\mathbb{Z}}[X]$ die Teilbarkeit $3 \mid P(0)$ erfüllen, aber $3 \nmid 7$.

Bsp: (zum chinesischen Restsatz:

z.z. $\mathbb{Q}[X]/(X^4+3X^2+2)_{\mathbb{Q}[X]} \cong \mathbb{Q}[X]/(X^2+1)_{\mathbb{Q}[X]} \times \mathbb{Q}[X]/(X^2+2)_{\mathbb{Q}[X]}$

$\{ J := (X^2+1)_{\mathbb{Q}[X]}, \; J = (X^2+2)_{\mathbb{Q}[X]}$

$J + J \ni 1$, da $X^2+2-(X^2+1)=1$.

chin. Restsatz $\Rightarrow \mathbb{Q}[X]/J\cap J \cong \mathbb{Q}[X]/J \times \mathbb{Q}[X]/J$.

z.z. $J \cap J = (X^4+3X^2+2)_{\mathbb{Q}[X]}$.

Begriff: Idealprodukt: $J \cdot_{Id} J = \{x_1 y_1 + \dots + x_\ell y_\ell \mid$

$\ell \in \mathbb{N} \wedge \forall i: x_i \in J \wedge y_i \in J\}$

Ü.A.: $J \cdot_{Id} J = J \cap J$, wenn $J + J \ni 1$

zurück zum Bsp:

Also $J \cap J = J \cdot_{Id} J = \{ x_1 y_1 + \dots + x_\ell y_\ell \mid$

$\ell \in \mathbb{N} \wedge \forall i: (X^2+1) \mid x_i \wedge X^2+2 \mid y_i\}$

$= (X^2+1)(X^2+2)_{\mathbb{Q}[X]}$

$= (X^4+3X^2+2)_{\mathbb{Q}[X]}$.

Anwendung: Die Gleichung

$X^2 + Y^2 = 21 Z^2$ hat keine Lösung in $\mathbb{Z}^3$.

Angenommen (x,y,z) wäre eine Lösung.

Wir teilen $ggT(x,y,z)$ raus, und können deshalb $ggT(x,y,z) = 1$ annehmen.

$$x^2 + y^2 = 21 z^2 = 3 \cdot 7 \cdot z^2$$

$x^2 + y^2 = (x+iy)(x-iy)$

$3\mathbb{Z}[i]$ ist ein Primideal in $\mathbb{Z}[i]$

$\Rightarrow$ $x+iy \in 3\mathbb{Z}[i]$ oder $x-iy \in 3\mathbb{Z}[i]$.

$\Rightarrow$ $3 \mid x \wedge 3 \mid y \Rightarrow 3^2 \mid x^2 + y^2 = 3 \cdot 7 z^2$

$\{1, i\}$ $\mathbb{Z}$-Basis von $\mathbb{Z}[i]$.

$\Downarrow$

$3 \mid z$

$\Leftarrow$

$3 \mid ggT(x,y,z)$

Widerspruch. $\Leftarrow$

Satz 78: Es sei R ein Ring mit 1. $I \subsetneq R$ sei ein Ideal

1) Jedes Maximalideal ist ein Primideal.
2) I ist ein Primideal $\Leftrightarrow$ R/I nullteilerfrei ist, d.h. $(a \cdot b = 0 \Rightarrow a = 0 \vee b = 0)$
3) I ist ein Maximalideas $\Leftrightarrow$ R/I ist ein Körper.

Beweis 2) „$\Rightarrow$“ $[x]\cdot[y]=[0]$

$\Rightarrow [xy]=[0] \Rightarrow xy\in J$

$\Rightarrow$ (↑ Primideal) $x\in J \vee y\in J$

$\Rightarrow [x]=[0] \vee [y]=[0]$.

„$\Leftarrow$“ $xy\in J \Rightarrow [xy]=[0]$

$\Rightarrow [x]\cdot[y]=[0] \Rightarrow [x]=[0] \vee [y]=[0]$

(↑ Nullteilerfreiheit)

$\Rightarrow x\in J \vee y\in J$.

3) „$\Rightarrow$“ $(R/J, +, \cdot)$ ist ein Ring mit Eins.

z.z. Es ist ein Körper, wenn J ein Maximalideal ist.

J sei ein Maximalideal.

$[x]\in R/J \setminus\{[0]\} \Rightarrow x\in R\setminus J$

$\Rightarrow Rx+J=\{rx+y \mid r\in R \wedge y\in J\}$ ist ein Ideal $\supsetneq J$

$\Rightarrow Rx+J=R \Rightarrow \exists\, r\in R, y\in J:\ rx+y=1_R$

(↑ J maximal)

$\Rightarrow rx-1_R\in J \Rightarrow [r]\cdot[x]=[1_R]$

$[x]\cdot[r]$

$\Rightarrow$ $(R/J, +, \cdot)$ ist ein Körper.

"$\Leftarrow$" z.z. J ist ein Maximalideal

$J \subseteq \mathcal{J} \subsetneq R$ Ideal, z.z. $\mathcal{J} = J$

Sei $x \in \mathcal{J}$. Annahme $x \notin J$

$\Rightarrow [x]_J \neq [0]_J \Rightarrow \exists\, [r]_J : [r]_J [x]_J = [1]_J$ (Körpereig.)

$\Rightarrow rx - 1 \in J \subseteq \mathcal{J}$

$\Rightarrow 1 = (1 - rx) + rx \in \mathcal{J}$

$x \in \mathcal{J}$

$\Rightarrow \mathcal{J} = R$. $\lightning$

$\Rightarrow$ Annahme ist falsch $\Rightarrow x \in J$

1) Körper sind nullteilerfrei

$\overset{3)1)2)}{\Rightarrow}$ 1). $\square$

Def: Ein Ring R mit 1 heißt Integritätsbereich, wenn er nullteilerfrei ist.

Bsp: $\mathbb{Z}[i]$ ist ein Integritätsbereich.

Bew: $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$

z.z. (X^2+1) ist ein Primideal.

$P, Q \in \mathbb{Z}[X]$ mit $P \cdot Q \in (X^2+1)_{\mathbb{Z}[X]}$

$\Rightarrow X^2+1 \mid PQ$, d.h. $\exists\, T \in \mathbb{Z}[X]$:

$(X^2+1) \cdot T = P \cdot Q$

Polynomdivision mit Rest:

$P = q \cdot (X^2+1) + r$

$Q = q' \cdot (X^2+1) + r'$

$q, q', r, r' \in \mathbb{Q}[X]$

$0 \leq \deg(r) <$ $\qquad \deg(X^2+1) = 2$

$0 \leq \deg(r') <$ $\qquad \deg(X^2+1) = 2$

$\vee\ r = 0$ oder $r' = 0$.

Wenn $r = 0$ oder $r' = 0$, dann sind wir fertig, da dann $X^2+1 \mid P$ oder $\mid Q$.

Anm: $r \neq 0$, $r' \neq 0$:

$r = aX + b \qquad r' = a'X + b'$

$X^2+1 \mid r \cdot r'$, da $X^2+1 \mid P \cdot Q$.

$\Rightarrow 2 = \deg(X^2+1) \leq \deg(r) + \deg(r') \leq 1+1 \leq 2.$

$\Rightarrow \deg(r) = \deg r' = 1$, also $a \cdot a' \neq 0$.

$\deg r \leq 1$

$\deg r' \leq 1$

$$\Rightarrow \quad aa'(X^2+1) = (aX+b)(a'X+b')$$

$$\Rightarrow \quad aa' = ab'X + a'bX + bb'$$

$$\Rightarrow \quad aa' = bb' \quad (1)$$

$$ab' + a'b = 0.$$

↑ Koeffizienten-Vergleich

$$aa' = bb'$$

$$\Rightarrow \quad 0 = a(ab' + a'b) \overset{\downarrow}{=} (a^2 + b^2)b'$$

$$\Rightarrow \quad (a^2+b^2) = 0, \text{ da } \mathbb{Z} \text{ nullteilerfrei ist.}$$

↑ $b' \neq 0$, da $bb' = aa' \neq 0$

$$\Rightarrow \quad a^2 = b^2 = 0 \Rightarrow a = b = 0 \quad \lightning$$

↑ $a^2, b^2 \in \mathbb{N}_0$; ↑ $\mathbb{Z}$ nullteilerfrei.

Im letzten Beweis haben wir eine Division mit Rest durchgeführt. Das ging, weil X^2+1 ein normiertes Polynom ist, d.h. der Leitkoeffizient ist 1.

$$P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$$

↑ Leitkoeffizient

P normiert $\overset{\text{Def}}{\Leftrightarrow}$ $a_n = 1$.

Bem: Ein Integritätsbereich R kann zu einem Körper $Q(R)$ erweitert werden, so dass R den Körper $Q(R)$ erzeugt, d.h.

$$\bigcap_{R \subseteq K \subseteq Q(R),\ K \text{ Körper}} K = Q(R),$$

oder anders gesagt $\forall x \in Q(R)\ \exists\, a \in R,\ b \in R \setminus \{0\}$:

$$x = \frac{a}{b}.$$

[Als Beispiel hatten wir schon die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ gesehen.]

Betrachte $(r,s) \sim (r',s') \Leftrightarrow_{\text{Def}} s'r = r's$ auf $R \times (R \setminus \{0\})$

$$R \times (R \setminus \{0\}) / \sim \;=: Q(R).$$

Addition auf $Q(R)$: $[(r,s)]_\sim + [(u,v)]_\sim := [(rv+us, sv)]_\sim$

Multiplikation: $[(r,s)]_\sim \cdot [(u,v)]_\sim := [(ru, sv)]_\sim$.

Man schreibt auch $\frac{r}{s}$ statt $[(r,s)]_\sim$.

Nachtrag zu Nullteilern

Def: Es sei R ein Ring. $a \in R$ heißt Nullteiler von R, falls ein $b \in R \setminus \{0\}$ existiert, so dass $ab = 0$. Wenn zusätzlich $a \neq 0$ gilt, so heißt a echter Nullteiler von R.

Bsp: $[0]_{15}, [3]_{15}, [5]_{15}, [6]_{15}, [9]_{15}, [10]_{15}, [12]_{15}$ sind alle Nullteiler von $\mathbb{Z}/15\mathbb{Z}$. Bsp: $[6]_{15} \cdot [5]_{15} = [0]_{15}$

III.3. Euklidische und Faktorielle Ringe.

Faktorielle Ringe: Existenz der Primfaktorzerlegungen

Euklidische Ringe: " der Division mit Rest.

Ref: (Primelemente)

Es sei R ein nullteilerfreier Ring und $x \in R \setminus (R^\times \cup \{0\})$.
x heißt Primelement von R, falls

$$\forall a,b \in R: (x \mid ab \Rightarrow x \mid a \vee x \mid b)$$

Bsp: 1) $n \in \mathbb{Z}$ ist ein Primelement $\Leftrightarrow$ $|n|$ ist eine Primzahl, nach Satz 26.

2) Ein Körper hat keine Primelemente.

3) (Ü A) Im $\mathbb{Z}[\sqrt{-5}]$: Alle 4 Faktoren von $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ sind keine Primelemente.

Def 79: Ein Integritätsbereich R heißt faktorieller Ring, falls jedes Element von $R \setminus (R^\times \cup \{0\})$ eine Produktzerlegung in Primelemente besitzt.

Satz 80: Es sei R ein faktorieller Ring und es seien $p_1, \dots, p_n, q_1, \dots, q_m$ Primelemente von R, s.d.

$$p_1 \cdots p_n = q_1 \cdots q_m.$$

Dann gilt $n = m$ und die Faktoren

sind bis auf Einheiten und Reihenfolge eindeutig bestimmt.

Beweis: $p_1 \mid q_1 \cdots q_m \overset{p_1 \text{ prim}}{\Longrightarrow} \exists j_1 : p_1 \mid q_{j_1}$

$\Rightarrow \exists x \in R : p_1 x = q_{j_1}$

$\Rightarrow$ (q_{j_1} prim) $q_{j_1} \mid x \vee q_{j_1} \mid p_1$

Fall: $q_{j_1} \mid x \Rightarrow \exists y \in R : q_{j_1} y = x$

$\Rightarrow q_{j_1} = p_1 x = p_1 y q_{j_1}$

$\Rightarrow q_{j_1}(1 - p_1 y) = 0$

$\Rightarrow$ (nullteilerfrei) $q_{j_1} = 0 \vee 1 = p_1 y$

$\Rightarrow$ ($q_{j_1} \neq 0$) $1 = p_1 y \Rightarrow p_1 \in R^\times$ ↯

Fall: $q_{j_1} \mid p_1 \Rightarrow \exists y \in R \quad q_{j_1} y = p_1$

$\Rightarrow q_{j_1} = p_1 x = q_{j_1} y x$

$\Rightarrow q_{j_1}(1 - yx) = 0 \Rightarrow yx = 1$ (wie oben)

$\Rightarrow x \in R^\times$

Teile p_1 aus $p_1 \cdots p_n = q_1 \cdots q_m$ raus und fahre induktiv fort. $\square$

Bsp: 1) $(\mathbb{Z}, +, \cdot)$ ist ein faktorieller Ring
2) jeder Körper ist ein faktorieller Ring.

Eine große Klasse faktorieller Ringe bilden die folgenden:

Def 81: 1) Ein Integritätsbereich R heißt Hauptidealring, falls jedes Ideal von R durch ein Element erzeugt wird, d.h.

$$\forall_{J \subseteq R \text{ Ideal}} : \exists_{x \in R} : Rx = J.$$

2) Ein Paar (R, N) heißt euklidischer Ring, falls

- R ein Integritätsbereich ist, und
- $N: R \longrightarrow \mathbb{Z} \cup \{-\infty\}$ eine Abbildung ist, sodass $N(R \setminus \{0\}) \subseteq \mathbb{Z}^{\geq m}$ für ein $m \in \mathbb{Z}$ und $N(0) < N(r) \; \forall_{r \in R \setminus \{0\}}$

sodass $\forall_{a \in R} \forall_{b \in R \setminus \{0\}}$

$$\exists\, q, r \in R : a = qb + r \wedge N(r) < N(b).$$

„Division mit Rest" N heißt „eukl. Bewertungsfunktion".

Bsp: 1) $\mathbb{Q}[X]$ ist ein euklidischer Ring.

$$N: \mathbb{Q}[X] \longrightarrow \mathbb{Z} \cup \{-\infty\}$$
$$N(P) := \deg(P).$$

2) $(K[X], \deg)$ K Körper ist ein euklidischer Ring.

Satz 82: Jeder euklidische Ring ist ein Hauptidealring.

Bew: Es sei (R, N) ein euklidischer Ring, und es sei I ein Ideal von R.

Fall $I = \{0\}$: I ist ein Hauptideal.

Fall $I \neq \{0\}$: Wähle $r \in I \setminus \{0\}$ mit minimaler Bewertung $N(r)$. z.z. $I = r \cdot R$.

Bew: „$\supseteq$": $r \in I \Rightarrow R \cdot r \subseteq I$

„$\subseteq$" $x \in I$. Division mit Rest

$\Rightarrow \exists\, q, s \in R$: $N(s) < N(r)$ und

$$x = q \cdot r + s$$

$\Rightarrow \quad s = x - qr \in I$

$\Rightarrow \quad s = 0$. Also $x = qr \in rR$. $\square$

$\uparrow$ $N(s) < N(r)$

Folgerung 83: Wenn K ein Körper ist, dann ist $K[X]$ ein Hauptidealring.

Satz 83: Jeder Hauptidealring ist ein faktorieller Ring.

Für den Beweis von Satz 83 benötigen wir eine Hilfsdefinition.

Def 83: Es sei R ein unitärer Ring. Ein Element $a \in R - (R^\times \cup \{0\})$ heißt irreduzibel (bzw. unzerlegbar), falls

$$\forall_{b,c \in R}: \left(a = b \cdot c \Rightarrow b \in R^\times \vee c \in R^\times\right)$$

Bsp: 1) Irreduzible Elemente und Primelemente sind in $\mathbb{Z}$ das selbe. (Folgt aus Satz 26)

2) In einem Integritätsbereich ist jedes Primelement irreduzibel (ü.A. S.10.4.1)

3) In $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X] / (X^2+5)\,\mathbb{Z}[X]$ ist das Element $(1+\sqrt{-5})$ irreduzibel aber nicht prim.

Bew.: a) $(1+\sqrt{-5})$ ist irreduzibel:

$$\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \mathbb{Z} + i\sqrt{5}\,\mathbb{Z}.$$

[Erinnerung: komplexe Konjugation.
$x+iy = \alpha \in \mathbb{C} = \mathbb{R}+i\mathbb{R}$. $\overline{\alpha} = x - iy$
"komplex Konjugierte zu α"

Eig: $\overline{\alpha}\,\overline{\beta} = \overline{\alpha\beta}$, $\alpha\overline{\alpha} = x^2+y^2$.
$N(\alpha) = \alpha\overline{\alpha}$ heißt die Norm von α.]

Zurück zum Beweis: Ansatz: $1+\sqrt{-5} = \alpha\beta$
$(\alpha = x_\alpha + i\sqrt{5}\,y_\alpha \;\wedge\; \beta = x_\beta + i\sqrt{5}\,y_\beta)$

$\Rightarrow 6 = N(1+\sqrt{-5}) = N(\alpha)\,N(\beta) = (x_\alpha^2 + 5y_\alpha^2)(x_\beta^2+5y_\beta^2)$

$x_\alpha^2 + 5y_\alpha^2 \equiv_5 0, 1, -1$.

$\Rightarrow$ —"— $\in \{1, 6\}$. Da bei $x_\alpha^2+5y_\alpha^2 = 1$ ∧ $x_\beta^2+5y_\beta^2 = 6$
↑
$x_\alpha^2+5y_\alpha^2 \mid 6$

Aus $x_\alpha^2+5y_\alpha^2 = 1$ folgt $y_\alpha = 0$ und $|x_\alpha| = 1$.
$\Rightarrow \alpha \in \{1, -1\} \subseteq \mathbb{Z}[\sqrt{-5}]^\times$

e) $1+\sqrt{-5}$ ist kein Primelement von $\mathbb{Z}[\sqrt{-5}]$

$(1+\sqrt{5})(1-\sqrt{-5}) = 2\cdot 3$

z.z. $1+\sqrt{-5} \nmid 2$ und $\nmid 3$.

Wir zeigen $\nmid 2$ und die Aussage $\nmid 3$ geht analog.

Ann: $1+\sqrt{-5} \mid 2 \Rightarrow \exists \alpha \in \mathbb{Z}[\sqrt{-5}] : \alpha \cdot (1+\sqrt{5}) = 2$

$\Rightarrow \quad 4 = \underbrace{N(\alpha)}_{\in \mathbb{Z}} \cdot 6 \Rightarrow \quad 3 \mid 2 \quad \lightning$

Lemma 84: In einem Hauptidealring sind alle irreduziblen Elemente prim und alle Primideale $\neq \{0\}$ maximal.

Bew: Es sei R ein Hauptidealring und $r \in R$ sei ein irreduzibles Element.

Schritt 1): $r \cdot R$ ist ein Maximalideal.

Bew: $(r)_R \subseteq J \subsetneq R$.

J ist ein Hauptideal $\Rightarrow \exists s \in R : J = (s)_R$

$r \in J = (s)_R \Rightarrow s \mid r \Rightarrow \exists t \in R : r = st$.

r irreduzibel $\Rightarrow s \in R^\times \checkmark \; t \in R^\times$.

$s \notin R^\times$, da $(s) = J \neq R$.

$\Rightarrow t \in R^\times \Rightarrow rR = stR = sR = J$.

J bel. $\Rightarrow (r)_R$ ist ein Maximalideal.

Schritt 2: z.z. r ist ein Primelement.

$(r)_R$ ist ein Maximalideal

$\Rightarrow$ $(r)_R - \{0\}$ Primideal

$\uparrow$ Satz 78

$\Rightarrow$ r ist ein Primelement $\square$

$\uparrow$

$r \neq 0$

Zweite Aussage des Lemmas: Es sei $\mathfrak{p}$ ein Primideal von R. R Hauptidealring $\times \{0\}$

$\Rightarrow \exists\, x \in \mathfrak{p} : (x)_R = \mathfrak{p}$.

$\mathfrak{p}$ ist prim $\overset{x \neq 0}{\Rightarrow}$ x ist prim $\underset{(\text{Ü A})}{\Rightarrow}$ x ist irreduzibel.

$\Rightarrow$ $\mathfrak{p} = (x)_R$ ist ein Maximalideal. $\square$

$\uparrow$ Schritt 1.

Beweis von Satz 82: Es sei R ein Hauptidealring.

z.z. R ist faktoriell.

Schritt 1: Jedes Element von $R - (R^\times \cup \{0\})$ besitzt einen irreduziblen Teiler:

Beweis: Ann. $a \in R - (R^\times \cup \{0\})$ besitzt keinen irreduziblen Teiler.

Betrachte $a = a_1 b_1 = \underbrace{a_2 b_2}_{a_1} b_1 = \underbrace{a_3 b_3}_{a_2} b_2 b_1 = \dots$

mit $a_i, b_i \notin R^\times \cup \{0\}$, $i \in \mathbb{N}$.

Das existiert nach Voraussetzung an a.

R HIR $\Rightarrow$ $(a_1, a_2, a_3, \dots)_R$ ist ein Hauptideal

also $= (r)_R$ für ein $r \in R$.

$\Rightarrow \exists_n \exists_{r_1, \dots, r_n \in R}$: $r = r_1 a_1 + \dots + r_n a_n$.

$a_n \mid a_{n-1} \mid a_{n-2} \mid \dots \mid a_2 \mid a_1 \Rightarrow r \in (a_n)_R$.

$\Rightarrow$ $(a_n)_R = (r)_R$.

$\uparrow$

$a_n \in (r)_R$

$\Rightarrow$ $\exists_{s \in R}$: $a_n s = a_{n+1}$

$\Rightarrow$ $a_{n+1} \in (r)_R = (a_n)_R$

$\Rightarrow$ $a_{n+1}(b_{n+1} s - 1) = 0$

$\uparrow$

$a_{n+1} b_{n+1} = a_n$

$a_{n+1} s = 1 \Rightarrow b_{n+1} \in R^\times$ ↯

$\Rightarrow$

$\uparrow$

$a_{n+1} \neq 0$, Nullteilerfreiheit

<u>Schritt 2:</u> Jedes Element $a \in R - (R^\times \cup \{0\})$ besitzt eine Primfaktorzerlegung.

<u>Bew:</u> Lemma 84 $\Rightarrow$ Eine Zerlegung in unzerlegbare Elemente reicht.

<u>Anw:</u> $a \in R - (R^\times \cup \{0\})$ hat keine derartige Zerlegung.

Also wieder $a = a_1 b_1 = \underbrace{a_2 b_2}_{a_1} b_1 = a_3 b_3 b_2 b_1 = \dots$ mit

b_i unzerlegbar (Schritt 1) und a_i nicht unzerl und nicht $\in R^\times$.

Selbes Argument wie in Schritt 1 $\Rightarrow \exists_{n \in \mathbb{N}} \beta_n \in R^\times$

Bsp 1) $\mathbb{Z}[i]$ ist euklidisch, also auch faktoriell.

Beweis: $N(\alpha) = \alpha\bar{\alpha}$

$\alpha = x_\alpha + i y_\alpha$, $\beta = x_\beta + i y_\beta \neq 0$ mit $N(\alpha) \geq N(\beta)$

$\gamma := \frac{\alpha}{\beta} = x_\gamma + i y_\gamma \in \mathbb{Q}[i]$, x_γ, y_γ Brüche

Wähle $z_1, z_2 \in \mathbb{Z}$, sodass $|x_\gamma - z_1| < \frac{1}{2}$

und $|y_\gamma - z_2| < \frac{1}{2}$

Setze $\delta := z_1 + i z_2$

$\Rightarrow \alpha = \beta\gamma = \beta\delta + \beta(\gamma - \delta)$

$N(\beta(\gamma - \delta)) = N(\beta) N(\gamma - \delta)$

$= N(\beta)(|x_\gamma - z_1|^2 + |y_\gamma - z_2|^2)$

$\leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) = N(\beta)\frac{1}{2} < N(\beta)$ ☐

2) Lemma 8.4 $\Rightarrow$ Primelement = irred. Polynom in $K[X]$ = maximalideal.

Bsp: $(X^3+3)_{\mathbb{Q}[X]}$ ist ein Maximalideal

da X^3+3 irreduzibel ist:

$X^3+3 = S \cdot T$. mit $\deg S \geq \deg T$

Fall $\deg(T) = 0 \Rightarrow T \in \mathbb{Q}^\times \subseteq \mathbb{Q}[X]^\times$

Fall $\deg(T) = 1 \Rightarrow X^3+3$ hat Nullstelle in $\mathbb{Q}$

also $\left(\frac{a}{b}\right)^3 + 3 = 0 \Rightarrow a^3 = -3b^3$

in $\mathbb{Z}$. Aber $3 \nmid \nu_3(3b^3) = 1 + 3\nu_3(b)$

und $3 \mid \nu_3(a^3) = 3\nu_3(a)$ ↯.

III.4. Konstruktion von $\mathbb{R}$ und $\mathbb{C}$

$$Abb(\mathbb{N},\mathbb{Q}) = \{(a_n)_{n\in\mathbb{N}} \mid a_n \in \mathbb{Q}\}$$

= Menge aller Folgen in $\mathbb{Q}$

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}}$$

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (a_n \cdot b_n)_{n\in\mathbb{N}}$$

z.B. $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \dots)$

$(1, 2, 3, 4, \dots)$

$(\frac{1}{2}, \frac{1}{3}, 0, -2, -\frac{3}{4}, 5, \dots)$

Auf $\mathbb{Q}$ haben wir den Betrag:

$$|\cdot|_{\mathbb{Q}} : \mathbb{Q} \longrightarrow \mathbb{Q}^{\geq 0} \qquad \left|\frac{a}{b}\right|_{\mathbb{Q}} := \frac{|a|_{\mathbb{Z}}}{|b|_{\mathbb{Z}}}$$

Cauchyfolgen: $(a_n)_{n\in\mathbb{N}} \in Abb(\mathbb{N},\mathbb{Q})$ heißt Cauchyfolge, falls

$$\forall_{N>0}\ \exists_{n_0\in\mathbb{N}}\ \forall_{n,m\geq n_0}: |a_n - a_m| \leq \frac{1}{N}$$

(Für n und m hinreichend groß haben a_n und a_m einen Abstand $\leq \frac{1}{N}$)

$$CF(\mathbb{Q}) := \{(a_n)_{n\in\mathbb{N}} \in Abb(\mathbb{N},\mathbb{Q}) \mid (a_n)_{n\in\mathbb{N}} \text{ Cauchyfolge}\}$$

Bsp: a) $\left(\frac{1}{2}, \frac{3}{4}, \frac{5}{6}, \frac{7}{8}, \frac{9}{10}, \dots\right)$

b) $\left(1, 1+\frac{1}{2}, 1+\frac{1}{2+\frac{1}{2}}, 1+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}, \dots\right)$

$= \left(1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \dots\right)$

c) $\left(1, \frac{1}{2}, -\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\right)$

d) $(1, 1, 1, 1, \dots)$

Eine Folge $(a_n)_{n\in\mathbb{N}}$ heißt <u>konvergent</u> gegen $a \in \mathbb{Q}$ falls

$$\forall_{N\in\mathbb{N}}\ \exists_{n_0\in\mathbb{N}}\ \forall_{n\geq n_0}: |a_n - a| \leq \frac{1}{N}.$$

Wir schreiben $\lim\limits_{n\to\infty} a_n = a$ ("Grenzwert" $:= a$)

Bsp: a) $\lim\limits_{n\to\infty} a_n = 1$

b) ? Man kann zeigen: $(a_n)_n$ hat keinen Grenzwert in $\mathbb{Q}$.

c) $\lim\limits_{n\to\infty} a_n = 0$

d) $\lim\limits_{n\to\infty} a_n = 1$.

Eine Folge $(a_n)_{n\in\mathbb{N}} \in \mathrm{Abb}(\mathbb{N}, \mathbb{Q})$ heißt <u>Nullfolge</u> falls $\lim\limits_{n\to\infty} a_n = 0$.

Satz 85: $M := \{ (a_n)_{/N} \in \mathrm{Abb}(\mathbb{N}, \mathbb{Q}) \mid \lim_{n\to\infty} a_n = 0 \}$ ist ein Maximalideal im Ring $CF(\mathbb{Q})$. Wir schreiben auch $NF(\mathbb{Q})$ für M.

Bew.: 1) (Ü A) $CF(\mathbb{Q})$ ist ein Ring mit 1.

2) $M \subseteq CF(\mathbb{Q})$, da jede konvergente Folge in $(\mathbb{Q}, |\cdot|)$ eine Cauchyfolge ist. (siehe Analysisvorlesung)

3) Idealeigenschaft: $(a_n)_{/N}, (b_n)_{/N} \in M$

$\Rightarrow \lim_{n\to\infty} (a_n - b_n) = \lim a_n - \lim b_n = 0 - 0 = 0$

- $M \ni (0)_{/N}$
- $(b_n)_{/N} \in CF(\mathbb{Q}) \wedge (a_n) \in M$

$\Rightarrow (a_n)_{/N} \cdot (b_n)_{/N} = (a_n b_n)_{/N}$ erfüllt

$|a_n b_n| \leq |a_n| \cdot B \xrightarrow{n\to\infty} 0$

($\uparrow$ CF sind beschränkt)

$\Rightarrow (a_n b_n)_N$ Nullfolge.

4) Maximalität: Es sei $(a_n)_{n\in\mathbb{N}} \in CF(\mathbb{Q}) \setminus M$

z.z. $\exists (b_n)_{n\in\mathbb{N}} \in CF(\mathbb{Q})$:

$$(1)_{n\in\mathbb{N}} \in (a_n b_n)_{n\in\mathbb{N}} + M.$$

[(i.t) $\Rightarrow$ Maximalität]

Wenn $(a_n)_{n\in\mathbb{N}} \notin M$, dann $\exists_{N\in\mathbb{N}}$ ∞-viele $n_j \in \mathbb{N}$: $\forall_j : |a_{n_j}| \geq \frac{1}{N}$

$(a_n)_{n\in\mathbb{N}} \in CF(\mathbb{Q}) \Rightarrow \exists_{n_0\in\mathbb{N}} \forall_{m,n\geq n_0}$:

$$|a_n - a_m| \leq \frac{1}{2N}$$

Wähle j_0 mit $n_{j_0} \geq n_0$.

$\Rightarrow \forall_{n \geq n_{j_0}}$:

$$|a_n| = |a_{n_{j_0}} - (a_{n_{j_0}} - a_n)|$$

$$\geq \big| |a_{n_{j_0}}| - |a_{n_{j_0}} - a_n| \big| \geq |a_{n_{j_0}}| - |a_{n_{j_0}} - a_n|$$

$\uparrow$ zweite Δ Ungl.

$$\geq \frac{1}{N} - \frac{1}{2N} = \frac{1}{2N}$$

$$\Rightarrow \forall n \geq n_{j_0}: \quad |a_n| \geq \frac{1}{2N}$$

Setze $b_n := \begin{cases} 0, & \text{falls } n < n_{j_0} \\ \frac{1}{a_n}, & \text{falls } n \geq n_{j_0} \end{cases}$

(UA) $(b_n)_{/\mathcal{N}}$ ist eine Cauchyfolge.

Wir haben

$$(b_n a_n)_{/\mathcal{N}} = (1)_{/\mathcal{N}} + (\underbrace{-1, \ldots, -1}_{n_{j_0}-1}, 0, 0, \ldots)$$

$\in \mathcal{M}$ □

Satz 78 ↓ Satz 85 $\Rightarrow$ $\mathbb{R} := \dfrac{CF(\mathbb{Q})}{\mathcal{M}}$ ist ein Körper.

"Körper der reellen Zahlen"

$\mathbb{C} := \dfrac{\mathbb{R}[X]}{(X^2+1)}$ ist auch ein Körper, der "Körper der komplexen Zahlen".

Also haben wir $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Ordnung auf $\mathbb{R}$: $r = [(a_n)_{/\mathbb{N}}]$, $s = [(b_n)_{/\mathbb{N}}] \in \mathbb{R}$.

- Wir definieren $r > s \iff_{\text{def}} \exists_{n_0 \in \mathbb{N}} \forall_{n \geq n_0} : a_n - b_n > 0$.

- -"- $r \geq s \iff_{\text{def}} (r > s) \vee (r = s)$.

Wohin konvergiert $(1, 1+\frac{1}{2}, 1+\frac{1}{2+\frac{1}{2}}, \dots) =: (a_n)$ in $\mathbb{R}$?

Beh: $\lim_{n\to\infty} a_n = \sqrt{2}$, d. h. die positive reelle Zahl r, für die $r^2 = 2$ gilt.

Bew. (a_n) ist eine Cauchyfolge in $\mathbb{R}$ also auch konvergent, da $\mathbb{R}$ vollständig ist (Analysis VL).

$$a := \lim_{n\to\infty} a_n.$$

a_n erfüllt die Gleichung:

$$\frac{1}{a_{n+1}-1} = 1 + a_n.$$

$$\Leftrightarrow \quad 1 = (1+a_n)(a_{n+1}-1)$$

$$\Rightarrow 1 = \lim_{n\to\infty} 1 = \lim_{n\to\infty} (1+a_n) \lim_{n\to\infty} (a_{n+1}-1)$$

$$= (1+a)(a-1) = a^2 - 1$$

$$\Rightarrow \quad 2 = a^2 \Rightarrow a = \sqrt{2}. \quad \square$$

$\uparrow$ $a > 0$

Zusammenfassung zu Zahlbereichserweiterungen

alter Zahlbereich	Aufgabe	Konstruktion bzw Axiome	neuer Zahlbereich
"viel, weniger"	genauer Quantifizieren	Peano-Axiome	$\mathbb{N}_0$
$\mathbb{N}_0$	Wollen $a-b$ für $a<b$ bilden	$\sim$ auf $\mathbb{N}_0\times\mathbb{N}_0$ $(n_1,n_2)\sim(n_1',n_2') \Leftrightarrow n_1+n_2'=n_2+n_1'$	$\mathbb{Z}=\mathbb{N}_0\times\mathbb{N}_0/\sim$ „Quotientengruppe des Monoids $(\mathbb{N}_0,+)$"
$\mathbb{Z}$	Teilung durch $z\in\mathbb{Z}\setminus\{0\}$	$\sim$ auf $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ $(z_1,u_1)\sim(z_2,u_2)$ $\Leftrightarrow z_1u_2=z_2u_1$	$\mathbb{Q}=\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})/\sim$ Quotientenkörper von $(\mathbb{Q},\cdot)$
$\mathbb{Q}$	Lücken ziehen, nicht trivial, bzw. monoton wachsende beschränkte Folgen voll konvergent	Vervollständigung $\mathbb{Q}$ bezüglich $\lvert\cdot\rvert$	$\mathbb{R}=CF(\mathbb{Q})/NF(\mathbb{Q})$
$\mathbb{R}$	Lücken von Quadratwurzeln aus negativen ganzen Zahlen	Faktorisiere nach dem Maximalideal $(X^2+1)/\mathbb{R}[X]$	$\mathbb{C}=\mathbb{R}[X]/(X^2+1)_{\mathbb{R}[X]}$ $(X^2+1)_{\mathbb{R}[X]}$ ist maximal, da X^2+1 irreduzibel ist, das es keine Nullstelle in $\mathbb{R}$ hat. Lemma 8.4.

Zusatz: **Dedekindsche Schnitte**

Def Z19: Ein Paar (A,B) von nichtleeren disjunkten Teilmengen A und B von $\mathbb{Q}$ heißt Dedekindscher Schnitt, falls $A \dot\cup B = \mathbb{Q}$ und $\forall_{a\in A}\forall_{b\in B}\ a<b$. und A hat kein größtes Element.

Bsp Z20: $(\mathbb{Q}^{<\frac{3}{4}}, \mathbb{Q}^{\geq\frac{3}{4}})$

- $(\{x\in\mathbb{Q} \mid x\leq 0 \vee x^2<5\}, \{x\in\mathbb{Q}^{>0} \mid x^2>5\})$

$\mathrm{Ded}(\mathbb{Q}) := \{(A,B) \mid (A,B) \text{ ist ein Ded. Schnitt von } \mathbb{Q}\}$

Addition auf $\mathrm{Ded}(\mathbb{Q})$:

- $(A_1,B_1)+(A_2,B_2) := (A_1+A_2, \mathbb{Q}\setminus(A_1+A_2))$
- $(A_1+A_2 := \{a_1+a_2 \mid a_1\in A_1 \wedge a_2\in A_2\})$

Das neutrale Element bzgl. $+$ ist $(\mathbb{Q}^{<0}, \mathbb{Q}^{\geq 0})$

Vorzeichenfunktion:

$$VZ(A,B) := \begin{cases} 1, \text{ falls } (A,B) = (\mathbb{Q}^{<0}, \mathbb{Q}^{\geq 0}) \\ 1, \text{ falls } 0\in A \\ -1, \text{ falls } \mathbb{Q}^{<0}\cap B \neq \emptyset \end{cases}$$

Das additive Inverse Element zu (A,B) ist

$$-(A,B) = \Big(\underbrace{\{x\in\mathbb{Q} \mid \forall_{a\in A} : x+a<0\}}_{\tilde{A}}, \mathbb{Q}\setminus\tilde{A}\Big)$$

Multiplikation auf $\mathrm{Ded}(\mathbb{Q})$: Betrag: $|(A,B)| := VZ(A,B)(A,B)$

$$(A_1,B_1)(A_2,B_2) := \begin{cases} \Big(\underbrace{\mathbb{Q}^{<0} \cup (A_1\cap\mathbb{Q}^{\geq 0})\cdot(A_2\cap\mathbb{Q}^{\geq 0})}_{\tilde{A}}, \mathbb{Q}\setminus\tilde{A}\Big) & \text{falls } VZ=1 \text{ für beide} \\ VZ(A_1,B_1)\,VZ(A_2,B_2)\,|(A_1,B_1)|\,|(A_2,B_2)| & \text{allgemein.} \end{cases}$$

Ordnung auf $\mathrm{Ded}(\mathbb{Q})$: $(A_1,B_1)\geq(A_2,B_2) \Leftrightarrow VZ\big((A_1,B_1)+(A_2,B_2)\big)=1$

Satz (Ü A): $(\mathrm{Ded}(\mathbb{Q}),+,\cdot)$ ist ein unitärer Ring, welcher ringisomorph zu $\mathbb{R}$ ist.

Idee: $\Phi : \mathbb{R} \longrightarrow \mathrm{Ded}(\mathbb{Q})$

$$\Phi\big(\overbrace{[(a_n)_{/\mathbb{N}}]}^{r}_{N\in C(\mathbb{Q})}\big) :=$$

$$\Big(\underbrace{\{x\in\mathbb{Q} \mid \exists_{\substack{\varepsilon>0\\ \varepsilon\in\mathbb{Q}}} : \exists_{n_0\in\mathbb{N}} \forall_{n\geq n_0}\ x<a_n-\varepsilon\}}_{A_r},$$

$$\underbrace{\mathbb{Q}\setminus A_r}_{B_r}\Big)$$

$$\Phi : \mathbb{R} \longrightarrow \mathrm{Red}(\mathbb{Q})$$

$$\Phi\Big(\underbrace{\mathbb{C}_{(a_n)_{/\mathbb{N}}}}_{r}\Big) := \Big(\{x \in \mathbb{Q} \mid \exists \varepsilon \in \mathbb{Q}^{>0}\, \underbrace{\exists_{n_0 \in \mathbb{N}} \forall_{n \geq n_0}\, x < -\varepsilon + a_n}_{A_r}\},\ \underbrace{\mathbb{Q} \setminus A_r}_{B_r}\Big)$$

A_r hängt nicht von den Repräsentanten ab und die Beschränktheit von $(a_n)_{/\mathbb{N}}$ sorgt dafür, dass A_r und B_r nicht leer sind.

- Φ ist additiv: $\Phi(r_1 + r_2) = (A_{r_1+r_2}, B_{r_1+r_2})$

  - $A_{r_1} + A_{r_2} \subseteq A_{r_1+r_2}$ ist sehr einfach einzusehen.

  - „$\supseteq$": $x \in A_{r_1+r_2}$ $\qquad r_i = [(a_n^{(i)})_{/\mathbb{N}}]$

    $\Rightarrow \exists \varepsilon \in \mathbb{Q}^{>0}\ \exists_{n_0} \forall_{n \geq n_0}: \quad x < a_n^{(1)} - \varepsilon + a_n^{(2)}$.

    Für hinreichend großes n_1 gilt $-\frac{\varepsilon}{2} + a_{n_1}^{(i)} \in A_{r_i}$.

    $$x < -\varepsilon + a_{n_1}^{(1)} + a_{n_1}^{(2)} \in A_{r_1} + A_{r_2}$$

    $$\Rightarrow \uparrow \quad x \in A_{r_1} + A_{r_2}.$$

$A_{r_1} + A_{r_2}$ ist Teil eines Red. Schnittes.

- Φ ist multiplikativ:

$$\Phi(r_1 \cdot r_2) = (A_{r_1 r_2}, B_{r_1 r_2})$$

Es reicht positive reelle Zahlen zu betrachten.

Es gilt für $r > 0$: $0 \in A_r$.

Komplett analog zur Additivität zeigt man

$$\Phi(r_1 r_2) = \Phi(r_1)\,\Phi(r_2) \quad \text{für } r_1, r_2 \in \mathbb{R}^{>0}.$$

$\subseteq$: $(A_{r_1} \cap \mathbb{Q}^{>0}) \cdot (A_{r_2} \cap \mathbb{Q}^{>0}) \subseteq A_{r_1 r_2} \cap \mathbb{Q}^{>0}$ leicht

$\supseteq$: analog zu +Fall

Injektivität: $\Phi(r) = (\mathbb{Q}^{<0}, \mathbb{Q}^{\geq 0}) \Rightarrow A_r = \mathbb{Q}^{<0}$

Also $\forall_{x \in \mathbb{Q}^{<0}}\ \exists_{n_0}: \forall_{n \geq n_0}: x < a_n$

und $\forall_{x\ \mathbb{Q}^{\geq 0}}: \forall_{\varepsilon \in \mathbb{Q}^{>0}}\ \exists^{\infty}\text{vielen } n: x \geq a_n - \varepsilon$.

$(a_n)_{\mathbb{N}}$ ist eine CF Also $\forall_{x \in \mathbb{Q}^{\geq 0}} \forall_{\varepsilon \in \mathbb{Q}^{>0}} \exists_{n_0} \forall_{n \geq n_0}$:

$$\varepsilon + x \geq a_n.$$

Also $\forall_{\varepsilon > 0}\ \exists_{n_0} \forall_{n \geq n_0}: -\varepsilon < a_n < \varepsilon \Rightarrow \lim_{n \to \infty} a_n = 0$

Surjektivität: $(A, B) \in \mathrm{Ded}(\mathbb{Q})$.

Mittels Intervallschachtelung konstruiert man eine CF. $(a_n)_{\mathbb{N}}$, s.d. $\Phi([(a_n)_{\mathbb{N}}]) = (A, B)$.

IV Quadratische diophantische Gleichungen

IV 1. Quadratreste

$\mathbb{P} :=$ „Menge der Primzahlen".
Quadratreste sind sehr hilfreich, um diophantische Gleichungen zu analysieren.

$X^2 + Y^2 = 8Z^2$ hat keine Lösung in $(1,1,1) + 2\mathbb{Z}^3$.

Bew: Ann: $\exists (x,y,z) \in (1,1,1)+2\mathbb{Z}^3 : x^2+y^2 = 8z^2$

$\subseteq$ seien x,y,z teilerfremd.

Quadratestklassen: $\{[a]_8^2 \mid 2 \nmid a\} = \{[1]_8\}$ nachprüfen.

$$1^2 \equiv_8 3^2 \equiv_8 (-3)^2 \equiv_8 (-1)^2 \equiv_8 1$$

$$\Rightarrow \quad x^2+y^2 \equiv_8 2 \quad \Rightarrow \quad 2 \equiv_8 0 \;\lightning$$

$2 \nmid x$, $2 \nmid y$; $\quad \| \quad 8z^2 \equiv_8 0.$

□

In diesem Abschnitt geben wir eine allgemeine Formel dafür an, wann eine ganze Zahl z ein Quadratrest mod p (p Primzahl) ist.

Def: $a \in \mathbb{Z}$ heißt Quadratrest (auch quadratischer Rest) modulo m ($m \in \mathbb{N}$), falls $\exists\, x \in \mathbb{Z} : a \equiv_m x^2$.

Der erste Schritt ist durch den folgenden Satz gegeben:

Satz 86: $a \in \mathbb{Z}$, $p \in \mathbb{N}_{>2}$ Primzahl, $p \nmid a$. Dann sind äquivalent

1° a ist ein Quadratrest mod p

2° $a^{\frac{p-1}{2}} \equiv_p 1$.

Lemma 87: Es sei K ein Körper, dann ist jede endliche Untergruppe von $K^\times$ zyklisch.

Bew: $G \leq K^\times$ sei endlich.

Wähle $g_0 \in G$ mit $\operatorname{ord}(g_0)$ maximal.

z.z. $G = \langle g_0 \rangle$

Bew: "$\supseteq$" ✓

"$\subseteq$" $g \in G$. 1) z.z. $\operatorname{ord}(g) \mid \operatorname{ord}(g_0)$.

Ann.: $\operatorname{ord}(g) \nmid \operatorname{ord}(g_0)$.

$\Rightarrow \exists\, p$ Primzahl $\exists\, n \in \mathbb{N}_0$:

$p^{n+1} \mid \operatorname{ord}(g)$ aber $p^{n+1} \nmid \operatorname{ord}(g_0)$ und $p^n \mid \operatorname{ord}(g_0)$

$$\operatorname{ord}(g) = p^{\nu_p} \cdot \prod_{q \neq p} q^{\nu_q} \qquad (\nu_p \geq n+1)$$

g_1 (unter $\frac{\operatorname{ord}(g)}{p^{\nu_p}}$)

$\Rightarrow \quad \operatorname{ord}\left(g^{p^{\nu_p}}\right) = p^{\nu_p}$ ist teilerfremd zu $\operatorname{ord}(g_0^{p^n}) = \frac{\operatorname{ord}(g_0)}{p^n}$

$\Rightarrow \quad \operatorname{ord}(g_1 g_0^{p^n}) = p^{\nu_p} \cdot \frac{\operatorname{ord}(g_0)}{p^n} > p^n \frac{\operatorname{ord}(g_0)}{p^n}$

$\lightning$ $\operatorname{ord}(g_0)$

Also haben wir $\operatorname{ord}(g) \mid \operatorname{ord}(g_0)$ □

2) Schritt: z.z. $g \in \langle g_0 \rangle$.

1) $\Rightarrow \quad g \in \{x \in K \mid x^{\operatorname{ord}(g_0)} = 1\} =: R$

Letztere Menge hat aber höchstens $\operatorname{ord}(g_0)$ Elemente da K ein Körper ist. $\langle g_0 \rangle$ hat auch $\operatorname{ord}(g_0)$ viele Elemente und

$\langle g_0 \rangle \subseteq R \Rightarrow \langle g_0 \rangle = R$.

$\Rightarrow g \in R$. □

Bew. (Satz 86): Wenn $a \equiv_p x^2 \Rightarrow p \nmid x$ und

$a^{\frac{p-1}{2}} \equiv_p x^{p-1} \equiv_p 1$ nach dem kleinen Fermat.

Fall: a sei kein Quadratrest mod p.

Es sei $[h]_p$ ein zyklischer Erzeuger von $\mathbb{F}_p^\times$. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ Körper mit p Elementen.

$\Rightarrow \exists j \in \mathbb{N}_0 \leq p-2: \quad [h]_p^j = [a]_p$

$\Rightarrow \quad h^j \equiv_p a \quad \Rightarrow 2 \nmid j$

a ist kein Quadratrest mod p.

$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv_p h^{j\frac{p-1}{2}} \equiv_p -1$ da

$\left(p-1 \nmid j\frac{p-1}{2} \text{ und } \left(a^{\frac{p-1}{2}}\right)^2 \equiv_p 1 \right.$

$\left. \text{und } \mathbb{F}_p \text{ Körper} \right)$ □

Def 88: $a \in \mathbb{Z}$, p ungerade Primzahl, $ggT(a,p)=1$

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & a \text{ Quadratrest mod } p \\ -1, & \text{sonst.} \end{cases}$$

„Legendre-Symbol von a nach p"

Bsp: 1) $\left(\frac{2}{7}\right) = 1$ da $3^2 \equiv_7 2$

2) $\left(\frac{2}{13}\right) = -1$

3) $\left(\frac{1}{5}\right) = 1, \left(\frac{2}{5}\right) = -1, \left(\frac{3}{5}\right) = -1, \left(\frac{4}{5}\right) = 1$

Letztes Mal: $a \in \mathbb{Z}, p \in \mathbb{P}$

Wir hatten das Legendre-Symbol eingeführt.

Wir werden es jetzt ein wenig verallgemeinern, indem wir $p = 2$ und $p \mid a$ zulassen.

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & a \text{ quadr. Rest mod } p \wedge p \nmid a \\ 0, & p \mid a \\ -1, & a \text{ kein quadr. Rest mod } p. \end{cases}$$

Wir hatten Satz 86: $a \in \mathbb{Z}, p \in \mathbb{P}^{>2}$: $p \nmid a$:

$1^\circ \left(\frac{a}{p}\right) = 1$ und 2° $a^{\frac{p-1}{2}} \equiv_p 1$.

Folg 89: $a \in \mathbb{Z}, p \in \mathbb{P}^{>2}$: $\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$

Man beachte $1 \not\equiv_p -1$ für ungerades p, da $2 \nmid p$.

Bew: $p \mid a$: $a^{\frac{p-1}{2}} \equiv_p 0 = \left(\frac{a}{p}\right)$

$p \nmid a \wedge \left(\frac{a}{p}\right) = 1$: Satz 86 $\Rightarrow$ $a^{\frac{p-1}{2}} \equiv_p 1 = \left(\frac{a}{p}\right)$

$p \nmid a \wedge \left(\frac{a}{p}\right) = -1$: Satz 86 $\Rightarrow$ $a^{\frac{p-1}{2}} \not\equiv_p 1$

kleiner Fermat $\Rightarrow$ $[a]^{\frac{p-1}{2}}$ löst

$0 = X^2 - 1 = (X+1)(X-1)$ in $\mathbb{F}_p$.

$\mathbb{F}_p$ ist nullteilerfrei $\Rightarrow$ $[a]^{\frac{p-1}{2}} \in \{[1]_p, [-1]_p\}$

$\Rightarrow$ $[a]_p^{\frac{p-1}{2}} = [-1]_p \Rightarrow a^{\frac{p-1}{2}} \equiv_p -1 = \left(\frac{a}{p}\right)$.

$\uparrow$

$[a]_p^{\frac{p-1}{2}} \neq [+1]$

□

Bem 89: (erste Rechenregeln) $p \in \mathbb{P}$.

1) $a, b \in \mathbb{Z}$. a) Falls $a \equiv_p b$, so $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

e) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

2) Für $p > 2$ gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Bew: 1) a) Fall $p \mid a$: $b \equiv_p a$

$\equiv_p 0 \Rightarrow p \mid b$

$\uparrow$

$p \mid a$

somit $\left(\frac{b}{p}\right) = 0 = \left(\frac{a}{p}\right)$

Fall $p \nmid a$ und $\left(\frac{a}{p}\right) = 1$:

$\Rightarrow \exists x \in \mathbb{Z}$: $x^2 \equiv_p a \Rightarrow \exists x \in \mathbb{Z}$: $x^2 \equiv_p b \equiv_p a$

$\uparrow$ $a \equiv_p b$

$\not\equiv_p 0$

$\uparrow$

$p \nmid a$

$\Rightarrow \left(\frac{b}{p}\right) = 1$

Fall $p \nmid a$ und $\left(\frac{a}{p}\right) = -1$: Insbesondere ist $p > 2$, da $\left(\frac{a}{2}\right) \in \{0, 1\}$ und $\left(\frac{b}{p}\right) \neq -1$.

Dann folgt aus den obigen Fällen $\left(\frac{a}{p}\right) \neq -1$ ↯ □

c) $\underline{p = 2}$: $\left(\frac{a}{2}\right) \in \{0, 1\}$ und es gilt $\left(\frac{a}{2}\right) \equiv_2 a$. Also $\left(\frac{a}{2}\right)\left(\frac{b}{2}\right) \equiv_2 ab \equiv_2 \left(\frac{ab}{2}\right)$.

$\Longrightarrow$ $\left(\frac{a}{2}\right)\left(\frac{b}{2}\right) = \left(\frac{ab}{2}\right)$.

↑ Werte von $\left(\frac{*}{2}\right)$ sind nur 0 und 1.

$\underline{p > 2}$: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv_p a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv_p (ab)^{\frac{p-1}{2}}$

$\equiv_p \left(\frac{ab}{p}\right)$.

2) $p > 2$: $\left(\frac{-1}{p}\right) \equiv_p (-1)^{\frac{p-1}{2}}$ $\Longrightarrow$ $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ □

↑ $1 \neq_p -1$

Lemma (Gaußsches Kriterium) Sei $a \in \mathbb{Z}$, p Primzahl, $p \nmid a$.

Es sei $T := \left\{ [z]_p \mid 0 \neq z \leq \frac{p-1}{2} \right\}$

$$\mu(a,p) := \left| \left\{ [az]_p \mid [z]_p \in T \wedge [az]_p \notin T \right\} \right|$$

$$= \left| (-T) \cap ([a]T) \right|$$

Dann gilt $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$.

Beweis: $\forall z \in T$ gilt $[az]_p \in T \cup (-T)$.

also existiert $\varepsilon_z \in \{1, -1\} : \varepsilon_z [az]_p \in T$.

Die Abbildung

$$\begin{array}{ccc} T & \xrightarrow{f} & T \\ [z]_p & \longmapsto & \varepsilon_z [az]_p \end{array}$$

ist bijektiv:

Bew: Es reicht Injektivität zu zeigen, da T endlich ist.

$$f([z]) = f([z']) \Rightarrow \varepsilon_z az \equiv_p \varepsilon_{z'} az'$$

$$\Rightarrow p \mid a(\varepsilon_z z - \varepsilon_{z'} z')$$

$$\Rightarrow p \mid \varepsilon_z z - \varepsilon_{z'} z'$$

$p \nmid a$, p Primzahl

$\Rightarrow$ Falls $\varepsilon_z = \varepsilon_{z'}$ so $z \equiv_p z' \Rightarrow [z]_p = [z']_p$

Falls $\varepsilon_z = -\varepsilon_{z'}$ so $z \equiv_p -z' \Rightarrow z + z' \equiv_p 0$,

Das ist unmöglich mit $[z]_p, [z']_p \in T$. $\square$

$$\prod_{[z]_p \in T} [z]_p = \prod_{[z]_p \in T} [\varepsilon_z a z]_p = \prod_T [z]_p \prod_T [\varepsilon_z]_p \cdot [a]_p^{\frac{p-1}{2}}$$

$\uparrow$ f bijektiv, $f(T) = T$

$$\Rightarrow \quad [1]_p = [a]_p^{\frac{p-1}{2}} \cdot \prod_T [\varepsilon_z]_p$$

Dividiere durch $\prod_T [z]_p$

($\mathbb{F}_p^\times$ // Gruppe!)

$$\Rightarrow \quad [a^{\frac{p-1}{2}}]_p = \prod_T [\varepsilon_z]_p$$

$\Uparrow$

$[\varepsilon_z]_p^{-1} = [\varepsilon_z]_p$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv_p \prod_T \varepsilon_z = (-1)^{\mu(a,p)} \quad \square$$

Korollar 91: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ $\wedge$ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(1. Ergänzungssatz) (2. Ergänzungssatz.)

Beweis: Lemma 90 anwenden

$a = -1$: $\mu(a,p) = \frac{p-1}{2}$.

$a=2$:
$$\left\{ [2z] \in -T_p \;\middle|\; 1 \le z \le \frac{p-1}{2} \right\}$$
$$= \left\{ [2z] \;\middle|\; \frac{p-1}{4} < z \le \frac{p-1}{2} \right\}$$

$$\Rightarrow \mu(2,p) = \begin{cases} \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}, & \text{falls } \frac{p-1}{4} \in \mathbb{N} \\ \underbrace{\frac{p-1}{2} - \left(\frac{p-1}{4} - \frac{1}{2}\right)}_{\frac{p+1}{4}}, & \text{falls } \frac{p-1}{4} \notin \mathbb{N} \end{cases}$$

$$\overset{(IA)}{\equiv_2} \frac{p^2-1}{8} \qquad \square$$

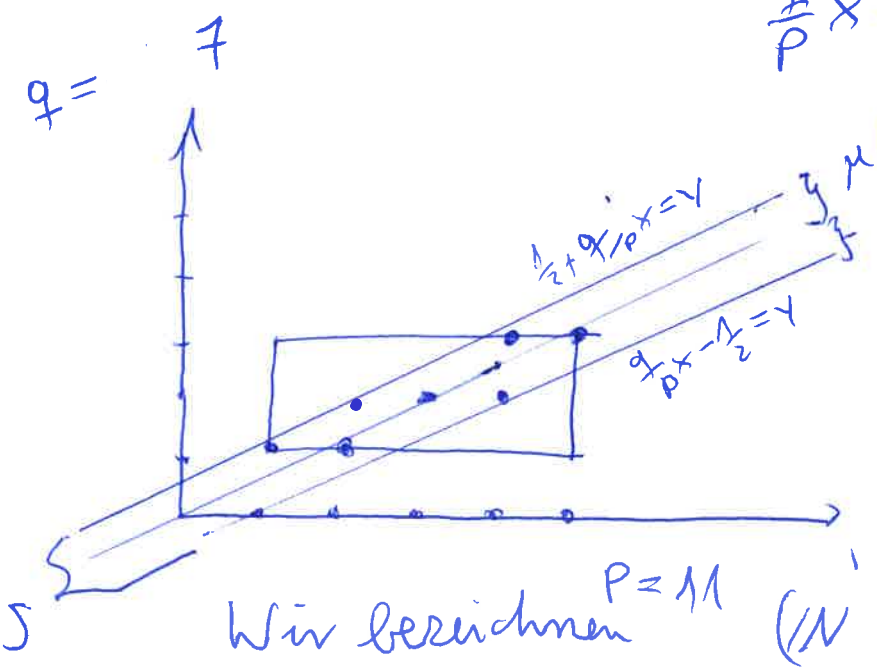
Satz 92: (Gauß) (quadratisches Reziprozitätsgesetz)

$p, q \in \mathbb{N}^{>2}$ seien verschiedene Primzahlen.
Dann gilt
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Beweis: $\mu(q,p)$: Wir interessieren uns für
$0 < x < \frac{p}{2}$ o.d. $[qx]_p \in -T_p$
also so dass $\exists y \in \mathbb{Z}$:
$$0 > qx - yp > -\frac{p}{2}$$
$$\left(\Leftrightarrow \frac{q}{p}x < y < \frac{q}{p}x + \frac{1}{2}\right)$$

$$\Rightarrow \mu(q,p) = \left| \left\{ (x,y) \in \mathbb{N}^{\frac{p-1}{2}} \times \mathbb{N}^{\frac{q-1}{2}} \;\middle|\; \frac{q}{p}x < y < \frac{q}{p}x + \frac{1}{2} \right\} \right|$$

Analog $\mu(p,q) = \left| \left\{ (x,y) \in \mathbb{N}^{\leq \frac{p-1}{2}} \times \mathbb{N}^{\leq \frac{q-1}{2}} \;\middle|\; \frac{q}{p}x - \frac{1}{2} < y < \frac{q}{p}x \right\} \right|$



Wir bezeichnen $\bigcup_{n=1}^{p=11} \left(\mathbb{N}^{\leq \frac{p-1}{2}} \times \mathbb{N}^{\frac{q-1}{2}}\right) + n$

Streifen $=: S$

Die Abbildung $(x,y) \overset{\varphi}{\longmapsto} \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$

erfüllt $\varphi(S) = S$.

φ ist die Punktspiegelung am Mittelpunkt des Rechtecks.

φ hat nur einen Fixpunkt, d.h. nur ein $(x_0, y_0) \in \mathbb{R}^2$: $\varphi(x_0, y_0) = (x_0, y_0)$, den Mittelpunkt des Rechtecks.

Mit φ bilden wir Paare von Punkten $s, \varphi(s)$: Genauer:

Def: $S_1, S_2 \in S$

$S_1 \sim S_2 \iff_{\text{Def}} \varphi(S_1) = S_2 \vee S_1 = S_2$

$\rightsquigarrow$ Äquivalenzrelation.

Die Äquivalenzklassen haben genau zwei Elemente, ausser die Klasse von (x_0, y_0), falls $(x_0, y_0) \in S$, d.h. falls $x_0, y_0 \in \mathbb{Z}$.

$\Rightarrow$ $|S|$ ist ungerade $\iff$ $x_0, y_0 \in \mathbb{Z} \iff \left(\frac{p+1}{4}, \frac{q+1}{4}\right) \in \mathbb{Z} \times \mathbb{Z}$

$\iff$ $q \equiv_4 3 \equiv_4 p$.

Also $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu(p,q)+\mu(q,p)}$

$= (-1)^{|S|} = \begin{cases} -1, & p \equiv_4 3 \equiv_4 q \\ 1, & \text{sonst} \end{cases}$

$= (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}}$ $\square$

$\uparrow$ nachrechnen

Bsp: 1) $\left(\frac{1001}{19}\right) = \left(\frac{13}{19}\right) = \left(\frac{19}{13}\right) = \left(\frac{6}{13}\right)$

($1001 \equiv_{19} 13$; $=$ mit Reziprozitätsgesetz)

$= \left(\frac{3}{13}\right)\left(\frac{2}{13}\right)$

$= \left(\frac{13}{3}\right)(-1) = \left(\frac{1}{3}\right)(-1)$ (Rez.)

$= 1 \cdot (-1) = -1.$

2) Zeigen Sie, dass die Kongruenz

$$x^2 + 7x \equiv 27 \mod 97$$

keine Lösung hat.

$$27 \equiv x^2 + 7x \equiv x^2 + 104x \equiv (x+52)^2 - 52^2 \mod 97$$

$\Leftrightarrow$ $2704 + 27 \equiv_{97} (x+52)^2$ ($2704 + 27 = 2731$)

Nicht lösbar $\Leftrightarrow$ $\left(\frac{2731}{97}\right) = -1.$

$$\left(\frac{2731}{97}\right) = \left(\frac{28 \cdot 97 + 15}{97}\right) = \left(\frac{15}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5}{97}\right)$$

$= \left(\frac{97}{3}\right)\left(\frac{97}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = 1 \cdot (-1) = -1.$

(Reziprozitätsgesetz) □

Def 93: (Das Jacobi-Symbol)

$a \in \mathbb{Z}$, $m \in \mathbb{N}_{>1}$. $m = \prod_{p \in \mathbb{P}} p^{\nu_p(m)}$.

Das Jakobisymbol ist wie folgt definiert:

$$\left(\frac{a}{m}\right) := \prod_{p \in \mathbb{P}} \left(\frac{a}{p}\right)^{\nu_p(m)}.$$

Erste Eigenschaften: $b, a \in \mathbb{Z}, n, m \in \mathbb{N}_{>2}$.

1) Wenn a ein quadr. Rest mod m und teilerfremd zu m ist, dann gilt $\left(\frac{a}{m}\right) = 1$

Die Umkehrung gilt nicht:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1,$$

aber 2 ist kein quadr. Rest mod 15, da

2 — " — mod 3 ist.

2) $\left(\frac{a}{m}\right) = 0 \iff \operatorname{ggT}(a, m) \neq 1$

3) Falls $a \equiv b \bmod \prod_{\substack{p \in \mathbb{P} \\ p \mid m}} p$ $\left(=: \operatorname{Rad}(m)\right)$

dann $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

Insbesondere folgt aus $a \equiv_m b$ die Flg $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

4) $\left(\frac{a}{m}\right)\left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right)$.

5) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$, falls $2 \nmid m$.

6) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$, falls $2 \nmid m$.

7) Für ungerade n, m gilt:

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

$$= \begin{cases} \left(\frac{m}{n}\right), & \text{falls } m \equiv_4 1 \text{ oder } n \equiv_4 1 \\ -\left(\frac{m}{n}\right), & \text{falls } m \equiv_4 3 \text{ oder } n \equiv_4 3. \end{cases}$$

Bew: 1) Aus $\operatorname{ggT}(a,m)=1$ folgt $\operatorname{ggT}(a,p)=1 \quad \forall_{p \in \mathbb{P}, p|m}$.

Wenn a ein quadr. Rest mod m ist, dann

ist —— n —— mod p $\forall_{p \in \mathbb{P}\, p|m}$.

$$\Rightarrow \left(\frac{a}{m}\right) = \prod_{\substack{p \in \mathbb{P} \\ p|m}} \left(\frac{a}{p}\right)^{\nu_p(m)} = \prod_{\substack{p \in \mathbb{P} \\ p|m}} 1 = 1.$$

2) Ü A.

3) $a \equiv b \bmod \operatorname{Rad}(m) \Rightarrow \bigwedge_{\substack{p \in \mathbb{P} \\ p|m}} a \equiv_p b \Rightarrow \bigwedge_{\substack{p \in \mathbb{P} \\ p|m}} \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$$\Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

4) folgt direkt aus dem Primzahlfall für m.

5) Für ungerade Zahlen s und t gilt:

$$\frac{s-1}{2} + \frac{t-1}{2} = \frac{st-1}{2} + \frac{(1-t)(s-1)}{2}$$

$$\equiv_2 \frac{st-1}{2}. \qquad (*)$$

Also $\left(\frac{-1}{m}\right) = \prod_{p \in \mathbb{P}} \left(\frac{-1}{p}\right)^{\nu_p(m)} = \prod_{p \in \Pi} \left(-1\right)^{\frac{p-1}{2}\nu_p(m)}$

$$\underset{(*)}{=} (-1)^{\frac{m-1}{2}}.$$

6) Komplett analog zu 5)

7) n und m seien ungerade und >2.

$$\left(\frac{n}{m}\right) = \prod_{p \in \mathbb{P}} \prod_{q \in \mathbb{P}} \left(\frac{q}{p}\right)^{\nu_q(n)\cdot\nu_p(m)}$$

$$= \prod_p \prod_q \left(\frac{p}{q}\right)^{\nu_q(n)\nu_p(m)} (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}\cdot\nu_q(n)\nu_p(m)}$$

$\uparrow$ Reziprozitätsgesetz

$$\underset{(*)}{=} \prod_p \left(\frac{p}{n}\right)^{\nu_p(m)} \cdot \prod_q (-1)^{\frac{p-1}{2}\nu_p(m)\frac{q-1}{2}\nu_q(n)}$$

$$= \prod_p \left(\frac{p}{n}\right)^{\nu_p(m)} \left((-1)^{\frac{p-1}{2}\cdot\nu_p(m)}\right)^{\frac{n-1}{2}}$$

$$\overset{(*)}{=} \left(\frac{m}{n}\right) \prod_p \left((-1)^{\frac{n-1}{2}}\right)^{\frac{p-1}{2}\cdot\nu_p(m)}$$

$$\overset{(*)}{=} \left(\frac{m}{n}\right) \left((-1)^{\frac{n-1}{2}}\right)^{\frac{m-1}{2}}$$

□

Mit dem Jacobi-Symbol kann man Legendre-Symbole einfacher ausrechnen.

Bsp: $\left(\frac{283}{331}\right) = -\left(\frac{331}{283}\right)$

$$= -\left(\frac{48}{283}\right) = -\left(\frac{2}{283}\right)^4 \cdot \left(\frac{3}{283}\right)$$

$$\overset{\uparrow}{=} -1 \cdot \left(\frac{3}{283}\right) = +\left(\frac{283}{3}\right)$$

$\uparrow$ ggT(2, 283) = 1 (Eine Null kann bei der Rechnung nicht auftreten, da 331 eine Primzahl ist und somit teilerfremd zu 283 ist.)

$$= \left(\frac{1}{3}\right) = 1.$$

331 ist eine Primzahl ⇒ 283 ist ein quadratischer Rest mod 331.

IV 2. Bsp für quadratische diophantische Gleichungen

IV 2.1. Lösungsstrategie über $\mathbb{Q}$

Def 94: Für $P \in R[X_1, \dots, X_n]$, R ein unitärer Ring, definieren wir dessen Grad wie folgt:

$$\deg(P) = \begin{cases} -\infty, & P = 0 \\ \max\{ i_1 + i_2 + \dots + i_n \mid a_{i_1 \dots i_n} \neq 0 \}, & \text{falls } P \neq 0 \end{cases}$$

wobei $P = \sum_{j_1, \dots, j_n \geq 0} a_{j_1 \dots j_n} X_1^{j_1} \cdots X_n^{j_n}$

Eine diophantische Gleichung

$P(X, Y, \dots) = 0$, $P \in \mathbb{Z}[X, Y, \dots]$

heißt quadratische diophant. Gleichung, falls $\deg P = 2$ gilt.

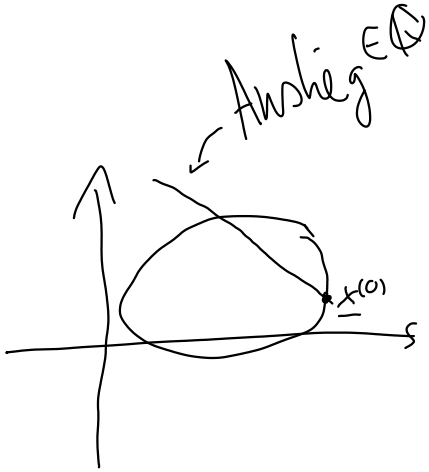
Lösungsstrategie zum Finden von rationalen Lösungen

95: • Finde eine erste rationale Lsg $\underline{x}^{(0)} \in \mathbb{Q}^3$

• Berechne für alle rationalen Richtungsvektoren $\underline{0} \neq \underline{v} \in \mathbb{Q}^n$ den zweiten Schnittpunkt der Geraden

$\{t\underline{v} + \underline{x}^{(0)} \mid t \in \mathbb{Q}\}$ mit der Menge

$\{\underline{x} \in \mathbb{Q}^n \mid P(x) = 0\}$



Bsp: $X^2 + XY + Y^2 = 7$. $(1,2) = \underline{x}^{(0)}$ ist eine erste Lsg.

Setze $t\underline{v} + \underline{x}^{(0)}$ ein mit $\underline{v} \neq \underline{0}$

$$(tv_1 + 1)^2 + (tv_1 + 1)(tv_2 + 2) + (tv_2 + 2)^2 = 7$$

$$\Rightarrow (t^2 v_1^2 + 2tv_1 + 1) + (t^2 v_1 v_2 + 2tv_1 + tv_2 + 2) + (t^2 v_2^2 + 4tv_2 + 4) = 7$$

$$\Rightarrow 0 = t\left(t(v_1^2 + v_1 v_2 + v_2^2) + 2v_1 + 2v_1 + v_2 + 4v_2\right)$$

Wir suchen $t \neq 0$.

$$\Rightarrow \quad t = \frac{-(4v_1 + 5v_2)}{v_1^2 + v_1 v_2 + v_2^2}$$

$\uparrow$

$v_1^2 + v_2^2 > -v_1 v_2$

für $\underline{v} \neq \underline{0}$.

[$v_1^2 + v_2^2 \geq 2|v_1||v_2| > |v_1||v_2|$, falls $v_1 \cdot v_2 \neq 0$.
$\geq -v_1 v_2$

$\Rightarrow v_1^2 + v_2^2 > 0 = -v_1 v_2$, falls $v_1 v_2 = 0$
und $\underline{v} \neq \underline{0}$]

Wir brauchen nur $\underline{v} \in \{(1,s), (0,1) \mid s \in \mathbb{Q}\}$

betrachten.

$$\Rightarrow \log_{\mathbb{Q}}(X^2 + XY + Y^2 = 7) =$$

$$\{(1,2) + (1,s) \cdot \frac{-(4+5s)}{1+s+s^2}, \overbrace{(1,-3)}^{(1,2)-5(0,1)} \mid s \in \mathbb{Q}\}$$

IV 2.2. Darstellung von natürlichen Zahlen als Quadratsummen

Satz 96: (Fermatscher 2-Quadrate Satz) Für $p \in \mathbb{P}$, $p \not\equiv_4 3$ existieren Zahlen $x, y \in \mathbb{N}_0$, so dass $x^2 + y^2 = p$.

Beweis: $2 = 1^2 + 1^2$. Deshalb betrachten wir nur noch $2 \nmid p$.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \quad , \text{da } p \equiv_4 1$$

$$\Rightarrow \exists u \in \mathbb{N} : u^2 \equiv_p -1 .$$

Wir betrachten die Terme $ux - y$ für $0 \le x < \lceil \sqrt{p} \rceil$ und $0 \le y < \lceil \sqrt{p} \rceil$

Das sind $(\lfloor p \rfloor + 1)^2 > p$ viele Terme

$\lceil \lfloor r \rfloor := \max [z \in \mathbb{Z} \mid z \le r] \rceil$

Also existieren $(x, y) \neq (x', y')$ mit $(*)$, so dass

$ux - y \equiv_p ux' - y'$

$\Rightarrow u(x - x') \equiv_p y - y'$. Setze $x_0 = x - x'$ und $y_0 = y - y'$

Dann gelten $-\lceil \sqrt{p} \rceil < -x' \le x_0 \le x' \le \lceil \sqrt{p} \rceil$

und $-\lceil \sqrt{p} \rceil < y_0 < \lceil \sqrt{p} \rceil$

und somit $0 < x_0^2 + y_0^2 < p+p = 2p$ (**)

$\uparrow$

$(x,y) \neq (x',y')$

Weiter gilt $x_0^2 + y_0^2 \equiv_p x_0^2 + u x_0^2 \equiv_p (1+u) x_0^2 \equiv_p 0$.

Also $p \mid x_0^2 + y_0^2$

$(**) \Rightarrow x_0^2 + y_0^2 = p$ $\square$

Folgerung 97: Es sei n eine natürliche Zahl, so dass für alle $p \in \mathbb{P} \cap [3]_4$ der Exponent $\nu_p(n)$ gerade ist. Dann ist n die Summe von zwei Quadratzahlen in $\mathbb{N}_0$.
Alle anderen nat. Zahlen sind nicht Summe von zwei Quadratzahlen.

Beweis: a) Es gilt $(a^2+b^2)(c^2+d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$

$= (ac - bd)^2 + (ad - bc)^2$ } (*)

$n = \left(\prod_{\substack{p \in \mathbb{P} \\ \wedge (p \equiv_4 1 \vee p = 2) \\ \wedge\, p \mid n}} p^{\nu_p(n)} \right) \cdot \tilde{n}^2 \qquad \tilde{n} \in \mathbb{N}$

$\Rightarrow$ (*) n ist die Summe von zwei Quadraten in $\mathbb{N}_0$.

b) Angenommen $n \in \mathbb{N}$ ist Summe zweier Quadratzahlen, etwa $n = x^2 + y^2$

Und es existiert eine Primzahl $p \equiv_4 3$, so dass $2 \nmid v_p(n)$. Wir setzen $t := ggT(x,y)$

$\frac{n}{t^2} = \left(\frac{x}{t}\right)^2 + \left(\frac{y}{t}\right)^2$ erfüllt auch die Eigenschaften, weshalb wir $ggT(x,y) = 1$ annehmen können.

$\Rightarrow$ $x^2 + y^2 \equiv_p 0$ und $p \nmid x$, da ansonsten $p \mid y$ und $p \mid ggT(x,y)$ gelten würde.

$\Rightarrow$ $[-1] = [y]^2 [x]^{-2}$ ist ein Quadrat in $\mathbb{F}_p$.

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

($p \equiv_4 3$)

Satz 98 (Drei-Quadrate-Satz von Gauß)

$n \in \mathbb{N}$ ist genau dann die Summe von 3 Quadratzahlen, wenn n nicht die Form $4^a(8k+7)$, $a, k \in \mathbb{N}_0$ hat.

Satz 99: (Vier-Quadrate Satz von Lagrange)
Jede natürliche Zahl ist Summe von 4 Quadraten in $\mathbb{N}_0$.

Bew: Wir brauchen nach Satz 98 nur $4^a(8b+7)$ behandeln.

$$4^a(8b+7) = 4^a(8b+6) + (2^a)^2$$
$$= x^2+y^2+z^2 + (2^a)^2$$

für geeignete $x,y,z \in \mathbb{N}_0$ nach Satz 98 □

Satz 22: $p \in \mathbb{P}$, $a, b \in \mathbb{N}$. Wenn p eine Darstellung der Form ax^2+by^2 mit $x,y \in \mathbb{N}_0$ besitzt, dann ist diese eindeutig, d.h. eine zweite Dg $au^2+bv^2=p$ erfüllt $(x,y)=(u,v)$ oder $(u,v)=(y,x)$.

Beweis: OE sei $a \le b$. Falls $p=a<b$, so ist $(1,0)$ die einzige Lsg.

Falls $p=a=b$ so sind $(1,0)$ und $(0,1)$ die einzigen Lösungen.

Also sei ab jetzt $a \le b < p$.

$$p = ax^2+by^2 = au^2+bv^2. \quad (\Rightarrow x,y,u,v \in \mathbb{N})$$

$$\Rightarrow p^2 = (ax^2+by^2)(au^2+bv^2) = a^2x^2u^2+b^2y^2v^2$$
$$+ab(x^2v^2+y^2u^2)$$
$$= (axu+byv)^2+ab(xv-yu)^2 \quad \} (*)$$
$$= (axu-byv)^2+ab(xv+yu)^2$$

$\operatorname{ggT}(x,y)=\operatorname{ggT}(u,v)=1$, da p eine Primzahl ist.

1. Fall $xv=yu$: $\operatorname{ggT}(x,y)=\operatorname{ggT}(u,v)=1$

$\Rightarrow x \mid u \wedge u \mid x \Rightarrow x=u$ ($\Rightarrow$ $\in \mathbb{N}$) $\Rightarrow v=y$ ($\Leftarrow$ $xv=yu$)

2. Fall $xv \neq yu$: $a(v^2x^2-y^2u^2) = (p-by^2)v^2-ay^2u^2$

$$= pv^2-(au^2+bv^2)y^2 = p(v^2-y^2).$$

$1 \le a < p \Rightarrow p \mid v^2x^2 - y^2u^2 \Rightarrow p \mid vx - yu \vee p \mid vx + yu$

Fall 2.a): $p \mid vx + yu$.

$$p^2 \ge ab(vx+yu)^2 \overset{a,b \ge 1}{\downarrow} \ge (vx+yu)^2 \ge p^2$$

$\uparrow$ $vx + yu > 0$

$\Rightarrow p = |vx + yu|$ und $a = b = 1$.

und $a \cdot u = b \cdot v$ (nach $*$)

Aus $xu = vy$ folgt $x \mid v$ und $v \mid x \Rightarrow v = x$

$\Rightarrow y = u$.

Fall 2.b) $p \mid vx - yu$ analog □

Anwendung (Primzahltests):

Def Z 23: Eine natürliche Zahl d heißt tauglich, falls jede natürliche Zahl $n > 1$, für die genau eine Darstellung der Form $x^2 + dy^2 = n$ existiert und diese auch noch $ggT(x,y) = 1$ erfüllt, eine Primzahl ist.

Bsp für taugliche Zahlen

1, 2, 3, 4, ..., 10

12, 13, 15, 16, 18,

21, und mehr. z.B. auch 1848.

Bsp: z.z. 977 ist eine Primzahl.

Wir betrachten die taugliche Zahl 7.

i) untersuche $x^2 + 7y^2 = 977$.

Damit das Sinn macht muss mindestens $\left(\frac{-7}{977}\right) = 1$ gelten.

$$\left(\frac{-7}{977}\right) = \left(\frac{-1}{977}\right)\left(\frac{7}{977}\right) = \left(\frac{977}{7}\right) = \left(\frac{-3}{7}\right)$$

$$= \left(\frac{-1}{7}\right)\left(\frac{3}{7}\right) = (-1)(-1)\left(\frac{7}{3}\right) = (-1)(-1) = 1. \quad \checkmark$$

Für eine Darstellung $x^2 + 7y^2 = 977$ muss $1 \leq y \leq 11$ gelten.

$977 - y^2$:

y	1	2	3	4	5	6	7	8	9	10
	976	949	914	865	802	725	634	529	410	277

$$\frac{11}{130}.$$

Die einzige auftretende Quadratzahl ist 529.

$\Rightarrow$ 977 ist eine Primzahl.

Bem: Euler zeigte mit 1848, dass

1851809 eine Primzahl ist.

V Konstruktion mit Zirkel und Lineal

Es werden geometrische Konstruktionsprobleme in algebraische Probleme umformuliert

Allg. Problemstellung: a) Wir betrachten die Gauß'sche Zahlenebene $\mathbb{R} \oplus \mathbb{R}i = \mathbb{C}$.

$Kr(M)$ = Menge der Kreise mit Mittelpunkt in M und Radius PQ für zwei $P, Q \in M$.

$Ger(M)$ = Menge der Geraden, die durch zwei verschiedene Punkte aus M verlaufen.

c) Konstruktion: $Konstr.(M) = M \cup \{P \in \mathbb{C} \mid P$ ist ein Schnittpunkt von zwei verschiedenen Elementen aus $Kr(M) \cup Ger(M)\}$

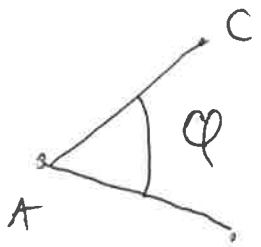
$M^{(0)} := M, \quad M^{(n+1)} := Konstr.(M^{(n)})$

$$\hat{M} = \bigcup_{n=0}^{\infty} M^{(n)}$$

b) Def: Ein Punkt $P \in \mathbb{C}$ heißt aus M konstruierbar mit Zirkel und Lineal, falls $P \in \hat{M}$.

d) Frage: Gegeben ein Punkt $P \in \mathbb{C}$, ist P konstruierbar aus M mit Zirkel und Lineal?

Man startet mit einem geometrischen Problem:
z.B. $M = \{A, B, C\} \subseteq \mathbb{C}$, o.d. A, B, C nicht kollinear sind, d.h. nicht auf einer Geraden liegen.



Kann man den Winkel $\varphi := \sphericalangle BAC$ dreiteilen mit Zirkel und Lineal?

Äquivalent formuliert: Ex. eine Gerade $g \in Ger(\hat{M})$, o.d. $\sphericalangle(\overline{AB}, g) = \frac{\varphi}{3}$ gilt?

Vorteil: $\hat{M}$ hat eine schöne algebraische Eigenschaft, falls $0, 1 \in M$.

Satz 100: $\hat{M}$ ist ein Unterkörper von $\mathbb{C}$, falls $0, 1 \in M$.

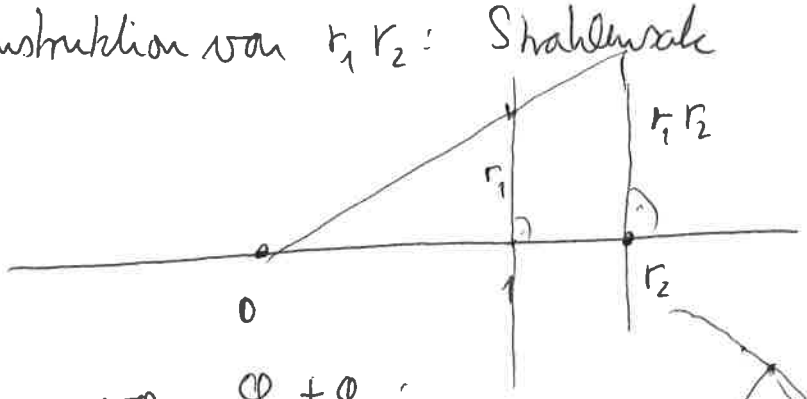
Beweis: 1) Addition: Konstruktion eines Parallelogramms.

2) $z \longmapsto -z$ Punktspiegelung an 0.

Also ist $(\hat{M}, +)$ eine UG von $(\mathbb{C}, +)$

3) $(z_1, z_2) \longmapsto z_1 \cdot z_2$: $z_1 = r_1 e^{i\varphi_1}$, $z_2 = r_2 e^{i\varphi_2}$

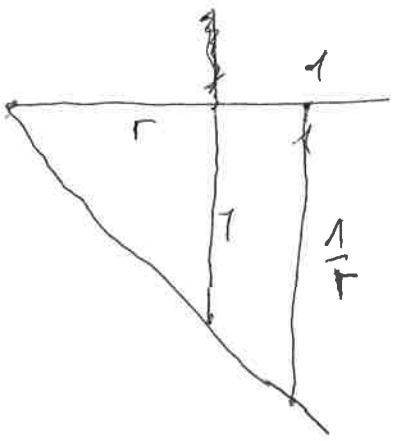
Konstruktion von $r_1 r_2$: Strahlensatz



— " — von $\varphi_1 + \varphi_2$:

4) $z \neq 0 \longmapsto z^{-1}$: $\quad r e^{i\varphi} \longmapsto \frac{1}{r} e^{-i\varphi}$

Konstr. von $\frac{1}{r}$:



Konstr. von $-\varphi$: (Übung) $\square$

Ab jetzt sei immer $\{0,1\} \subseteq \mathcal{U}$.

Wir wählen folgenden „Zweig" der Wurzel:

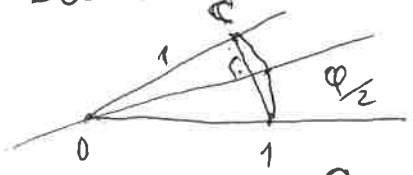
$z = r e^{i\varphi} \quad \varphi \in [0, 2\pi[, \; r \geq 0$.

$\sqrt{z} := \sqrt{r} \cdot e^{i\frac{\varphi}{2}}$.

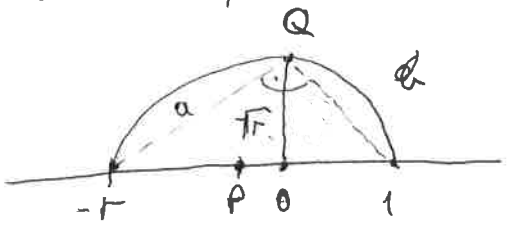
Satz 101: $\forall z \in \mathbb{C}: \left(z \in \hat{\mathcal{U}} \Rightarrow \sqrt{z} \in \hat{\mathcal{U}}\right)$

Bew: $z = r e^{i\varphi}$ Wir müssen $\frac{\varphi}{2}$ und $\sqrt{r}$ konstruieren

$\frac{\varphi}{2}$: Die Winkelhalbierende führen wir wie folgt durch:



$\sqrt{r}$:



Begründung $h := 0Q$

$(h^2+1) + (r^2+h^2) = a^2 + e^2$

$= (r+1)^2$

$\Leftrightarrow \quad 2h^2 = 2r \Leftrightarrow h^2 = r$.

$\square$

Def 102: Ein Unterkörper K von $\mathbb{C}$ heißt *quadratisch abgeschlossen*, falls für alle $z \in K$ die Wurzel von z ein Element von K ist.

Def 103: Ein Paar (L, K) bestehend aus einem Körper L und einem Unterkörper K heißt Körpererweiterung. Wir schreiben auch $L|K$.

Def 104: Es sei $L|K$ eine Körpererweiterung und S eine Teilmenge von L. Wir definieren

$$K(S) = \bigcap \tilde{K}$$

$\tilde{K}$ Unterkörper von L, der $K \cup S$ enthält

$K(S)$ heißt der *von S erzeugte Erweiterungskörper von K*.

Ber: $K \subseteq \mathbb{C}$ Unterkörper. Wir bezeichnen mit $\mathrm{Sqrt}(K)$ die Menge aller Quadratwurzeln von K, also $\{ z \in \mathbb{C} \mid z^2 \in K \}$.

Satz 105: Wir definieren $K_0^M = \mathbb{Q}(M \cup \overline{M})$

↑ komplexe Konjugation.

$$\overline{M} := \{ \bar{z} \mid z \in M \}$$

$$K_{n+1} := K_n(\mathrm{Sqrt}(K_n))$$

Beh: Es gilt $\hat{M} = \bigcup_{n=0}^{\infty} K_n^M$

Dieser Satz verschiebt das geometrische Problem „$P \in \hat{M}$?“ zum algebraischen Problem:

„Läßt sich P durch $\mathbb{Q}$, $M \cup \bar{M}$ und sukzessives Hinzunehmen von Quadratwurzeln erreichen?“

Bsp: 1) $M = \{0, 1, e^{i\varphi}\}$. Das Winkeldreiteilungsproblem ist für $\varphi = \frac{\pi}{2}$ lösbar:

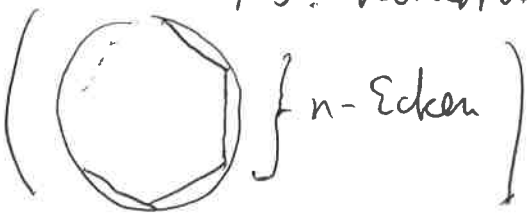
$$e^{i\frac{\pi}{6}} = \cos\left(\frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{i}{2}$$

Man kann zeigen, daß es für alle

$$\varphi \in \left\{ \frac{2\pi}{n} \mid n = 2^m p_1 \cdots p_e, \forall_{i \neq j}: p_i \neq p_k \in \mathbb{P}^{>3} \right.$$
$$\left. \text{o.d. } p_i - 1 \text{ eine Zweierpotenz ist} \right\}$$

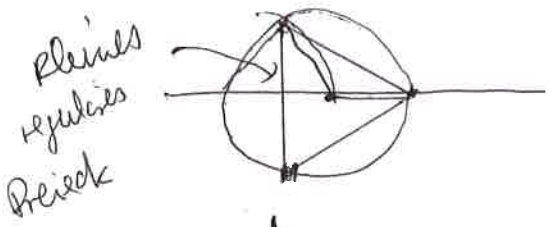
gelöst werden kann. Aber für $\varphi = 120°$ geht es zum Bsp nicht. Das hängt mit dem folgenden Problem zusammen.

2) $M = \{0, 1\}$. Konstruiere ein reguläres n-Eck

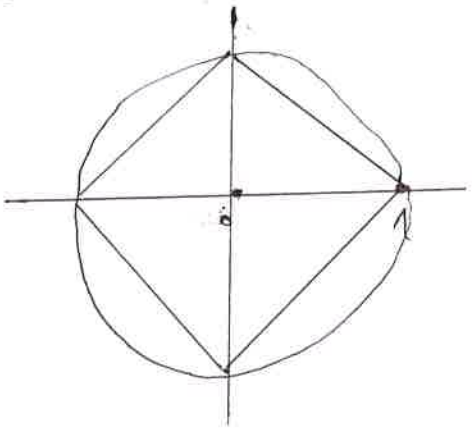


mit Zirkel und Lineal, wobei ein Kreis vorgegeben ist.

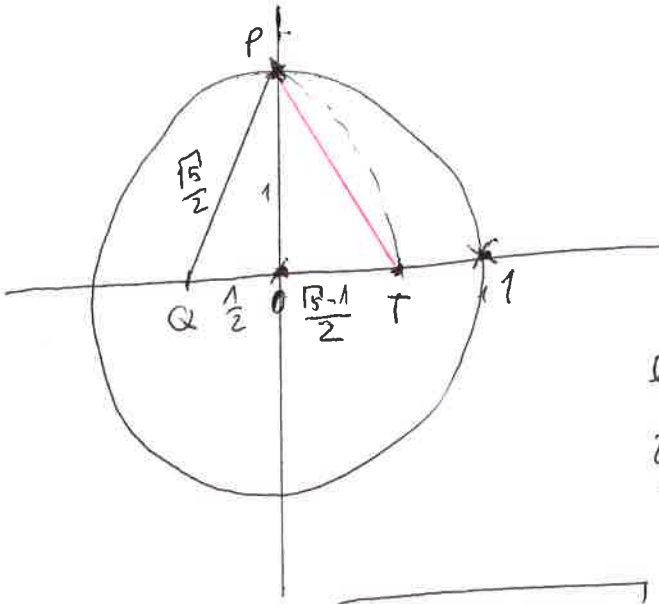
2a) $n=3$:



$n=4$:



$n=5$: Etwas komplizierter:



Wir tragen die rote Strecke 5 mal hintereinander auf den Kreis ab und erhalten ein reguläres 5-Eck.

Bem: • PT hat die Länge $\sqrt{1+\left(\frac{\sqrt{5}-1}{2}\right)^2} = \sqrt{\frac{10-2\sqrt{5}}{2}}$

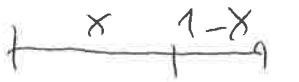
• Das Verhältnis $\frac{1}{OT} = \frac{1}{\frac{\sqrt{5}-1}{2}} = \frac{2(\sqrt{5}+1)}{4} = \frac{\sqrt{5}+1}{2}$

heißt der „Goldene Schnitt".

Man sagt, dass ein Punkt C eine Strecke $\overline{AB}$ im Goldenen Schnitt teilt, falls $C \in]A,B[$

Und $\dfrac{AB}{\max\{AC, CB\}} = \dfrac{\max\{AC, BC\}}{\min\{AC, BC\}}$ gilt

Und in diesem Fall ist das Verhältnis genau $\dfrac{\sqrt{5}+1}{2}$.



$$\frac{1}{x} = \frac{x}{1-x} \iff 1-x = x^2 \iff x^2+x-1=0$$

$$\underset{x>0}{\iff} \quad x = -\frac{1}{2} + \sqrt{\frac{5}{4}} = \frac{\sqrt{5}-1}{2}.$$

Also $$\frac{AB}{\max\{AC, CB\}} = \frac{1}{x} = \frac{1}{\frac{\sqrt{5}-1}{2}} = \frac{\sqrt{5}+1}{2}.$$

Wir zeigen auch algebraisch, dass ein regelläres 5-Eck mit Zirkel und Lineal konstruiert werden kann.

z.z. $e^{i\frac{2\pi}{5}} \in \hat{\mu}$. $\quad \frac{2\pi}{5} \hat{=} 72°$ $\quad \zeta = e^{i\frac{2\pi}{5}}$

$$0 = \zeta^5 - 1 = (\zeta-1)(\zeta^4+\zeta^3+\zeta^3+\zeta^2+\zeta^1+1)$$

$$\overset{\uparrow}{\underset{\zeta \neq 0}{\Rightarrow}} 0 = \sum_{i=0}^{4} \zeta^i = \zeta^2 + \zeta(\zeta^3+\zeta^2+1)+1 \qquad (*)$$

Weiter $(\zeta+\zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = \zeta^2 + \zeta^3 + 2$

$$\underset{(*)}{=} -\zeta - \zeta^{-1} + 1$$

Also $\zeta + \zeta^{-1}$ erfüllt X^2+X-1. $\overset{\zeta+\zeta^{-1}>0}{\Rightarrow}$ $\zeta+\zeta^{-1} = \frac{\sqrt{5}-1}{2}$.

$$\overset{(*)}{\Rightarrow} \quad \zeta^2 + \zeta^3 + 1 = -\zeta - \zeta^{-1} = \frac{1-\sqrt{5}}{2}$$

$$\overset{(*)}{\Rightarrow} \quad 0 = \zeta^2 + \zeta\left(\frac{1-\sqrt{5}}{2}\right) + 1$$

$$\Rightarrow \quad \zeta = -\frac{1-\sqrt{5}}{4} + \sqrt{\frac{-10-2\sqrt{5}}{16}}$$

$$\overset{\text{Satz 105}}{\Rightarrow} \quad \zeta \in \hat{\mu}.$$

Bew. von Satz 105: $K_\infty^M := \overset{\infty}{\underset{n=0}{\bigcup}} K_n^M \subseteq \hat{\mu}$, da $\hat{\mu}$ quadratisch abgeschlossen ist.

„$\supseteq$": $\mu \cup \bar{\mu} \subseteq K_\infty^M$. Wenn z_1, z_2, u_1, u_2 in K_∞ liegen, dann liegt auch der Schnittpunkt von

$$\{\lambda(z_2 - z_1) + z_1 \mid \lambda \in \mathbb{R}\} = g_{z_1, z_2}$$

und g_{u_1, u_2} in K_∞, da er durch Brüche mit z_1, z_2, u_1, u_2 geschrieben werden kann.

- Beim Schnitt eines Kreises mit einer Geraden müssen wir

$$|\lambda(z_2 - z_1) + z_1 - z_3|^2 = r$$

nach λ auflösen und erhalten, dass λ mit Quadratwurzeln, den Real und Imaginärteilen von z_i und mit r beschrieben werden kann.

Also liegen die Schnittpunkte wieder in K_∞^μ,
wenn $z_3, r_1 z_1, z_2 \in K_\infty^\mu$.
· Schnitt zweier Kreise (ü A). □

Satz 106: Die Quadratur eines Kreises (mit Zirkel und Lineal) ist nicht möglich

Def 107: $L|K$ Körpererweiterung, $[L:K] := \dim_K L$ „Grad von $L|K$".

Lemma 108: $L_1|L_2|L_3$ mit $[L_1:L_3] < \infty$.
Dann gilt $[L_1:L_3] = [L_1:L_2][L_2:L_3]$

Beweis: (Skizze) $x_1, \dots, x_s$ L_2-Basis von L_1

$y_1, \dots, y_t$ L_3-Basis von L_2

$\Rightarrow$ $x_1 y_1, \dots, x_1 y_t,$
$x_2 y_1, \dots, x_2 y_t$ ist eine L_3-Basis von L_1
$\vdots$
$x_s y_1, \dots, x_s y_t$

$\Rightarrow [L_1:L_3] = s \cdot t.$ □

Lemma 109: Es sei $\mu = \{0,1\}$ und $z \in \hat{\mu}$.
Dann ist $[\mathbb{Q}(z):\mathbb{Q}]$ endlich und gleich einer Zweierpotenz.

Beweis: $z \in \hat{\mu}$. Satz 105 $\Rightarrow \exists z_1, \dots, z_\ell$:

$z_1 \in \mathbb{Q}$, $z_2 \in \mathbb{Q}(\sqrt{z_1})$, $\dots$, $z_\ell \in \mathbb{Q}(\sqrt{z_1}, \dots, \sqrt{z_{\ell-1}})$

$\sqrt{z_1}$ $\sqrt{z_2}$ $\sqrt{z_\ell}$ &

$z \in \mathbb{Q}(\sqrt{z_1}, \dots, \sqrt{z_\ell})$.

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{z_1}) \subseteq \mathbb{Q}(\sqrt{z_1}, \sqrt{z_2}) \subseteq \dots \subseteq \mathbb{Q}(\sqrt{z_1}, \dots, \sqrt{z_\ell})$

Grad 2 Grad 2

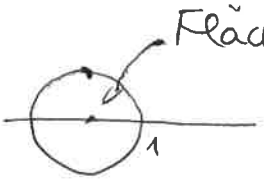
$\boxed{K(\sqrt{z}) = K \oplus K\sqrt{z} \text{ für } z \in K \text{ mit } \sqrt{z} \notin K}$

$\Rightarrow \quad [\mathbb{Q}(\sqrt{z_1}, \dots, \sqrt{z_\ell}) : \mathbb{Q}] = 2^\ell$

$\Rightarrow \quad [\mathbb{Q}(z) : \mathbb{Q}] \mid 2^\ell$ □

↑ Lemma 108

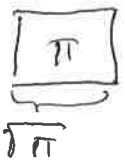
Beweis von Satz 106:



gegeben.

Annahme: Wir können ein Quadrat konstruieren, das den selben Flächeninhalt wie der Kreis hat.

$(\mu := \{a, 1+\})$



$\Rightarrow \sqrt{\pi} \in \hat{\mu} \Rightarrow \pi = \sqrt{\pi}^2 \in \hat{\mu}$

Lemma 109 $\Rightarrow \quad [\mathbb{Q}(\pi) : \mathbb{Q}] < \infty$.

$\Rightarrow \quad 1, \pi, \pi^2, \pi^3, \dots$ sind linear abhängig über $\mathbb{Q}$.

$\Rightarrow \exists\, p \in \mathbb{Q}[x] \setminus \{0\} : \; p(\pi) = 0.$ ↯

So ein Polynom gibt es nicht für π.

Man sagt π ist transzendent. □

Bem: Elemente aus $\mathbb{C}$, die Nullstellen von Polynomen aus $\mathbb{Q}[x] \setminus \{0\}$ sind, heißen algebraische Zahlen.

Satz 110: (Gauß) Ein reguläres 7-Eck lässt sich nicht mit Zirkel und Lineal konstruieren.

Beweis (Skizze): z.z. für $\mu = \{0,1\}$ gilt nicht $e^{i\frac{2\pi}{7}} \in \hat{\mu}$.

Annahme doch: Lemma 109 $\Rightarrow [\mathbb{Q}(e^{i\frac{2\pi}{7}}) : \mathbb{Q}]$ | Zweierpotenz

Fakt: $[\mathbb{Q}(e^{i\frac{2\pi}{n}}) : \mathbb{Q}] = \varphi(n)$ (φ - Eulersche φ-Funktion)

$\varphi(7) = 7 - 1 = 6$ keine Zweierpotenz $\lightning$ □

Man kann stärker zeigen

Satz 111: (Gauß) Ein reguläres n-Eck lässt sich genau dann mit Zirkel und Lineal konstruieren, wenn $\varphi(n)$ eine Zweierpotenz ist, also genau dann, wenn n die Form $n = 2^m \cdot p_1 \cdots p_\ell$

mit $p_j \neq p_i \in \mathbb{P}^{\geq 3}$ mit $p_i - 1$ Zweierpotenz hat.