Technische Universität Dresden

Skript:

Algebra

Verfasser Franziska Kühn

Daten Prof. Bernhard Ganter
Sommersemester 2010
Grundstudium

Inhaltsverzeichnis

1 Begriffsverbände

- Ein *formaler Kontext* (G,M,I) besteht aus Mengen G, M sowie einer Relation $I \subseteq G \times M$. Man nennt die Elemente von G die Gegenstände und die von M die Merkmale des formalen Kontext.
- Man liest gIm als „der Gegenstand hat das Merkmal m“, gIm bedeutet dasselbe wie $(g, m) \in I$.
- Die *Ableitungsoperatoren*: Ist (G,M,I) ein formaler Kontext, so definiert man für $A \subseteq G$:

  $$A' := \{m \in M | gIm \,\text{für alle}\, g \in A\}$$

  und für $B \subseteq M$

  $$B' := \{g \in G | gIm \,\text{für alle}\, m \in B\}$$

- Hilfssatz: Für jeden formalen Kontext (G,M,I) und für alle A, A_1, $A_2 \subseteq G$, B, B_1, $B_2 \subseteq M$ gilt:
  1. $A_1 \subseteq A_2 \Rightarrow A_2' \subseteq A_1'$ und $B_1 \subseteq B_2 \Rightarrow B_2' \subseteq B_1'$
  2. $A \subseteq A''$ und $B \subseteq B''$
  3. $A' = A'''$ und $B' = B'''$
  4. $A \subseteq B' \Leftrightarrow B \subseteq A'$
- (A,B) heißt *formaler Begriff* von (G,M,I) $:\Leftrightarrow A \subseteq G$, $B \subseteq M$, $A' = B$, $A = B'$. Man nennt A den Umfang und B den Inhalt des formalen Begriffs (A,B).
- Die Menge $\mathcal{B}(G, M, I)$ aller formalen Begriffe von (G,M,I) kann auf folgende Weise geordnet werden:

  $$(A_1, B_1) \leq (A_2, B_2) :\Leftrightarrow A_1 \subseteq A_2$$

  Man sagt dann, (A_1, B_1) sei ein *Unterbegriff* von (A_2, B_2) und (A_2, B_2) ein *Oberbegriff* von (A_1, B_1).
- Die Menge aller Begriffe von (G,M,I), so geordnet, wird mit $\underline{\mathcal{B}}$(G,M,I) bezeichnet und *Begriffsverband* von (G,M,I) genannt.

- Erstellen eines Liniendiagramms zu einem formalen Kontext:

  1. Lege eine Liste von Begriffsumfängen an. In dieser Liste wird zunächst für jedes Merkmal $m \in M$ der Merkmalumfang $\{m\}'$ eingetragen. Dabei sind Doppeleintragungen zu vermeiden.
  2. Von je zwei Mengen dieser Liste bilde den Durchschnitt. Wenn sich dabei eine Menge ergibt, die noch nicht in der Liste steht, dann füge sie zur Liste hinzu. Mit der erweiterten Liste kann weitergearbeitet werden wie zuvor.
  3. Wenn für je zwei Mengen in der Liste auch der Durchschnitt der beiden Mengen in der Liste steht, dann erweitere die Liste um die Meng G, sofern diese noch nicht in der Liste steht. Danach enthält die Liste alle Begriffsumfänge.
  4. Berechne zu jedem Begriffsumfang A in der Liste den zugehörigen Begriffsinhalt A' und erhalte so eine Liste aller Begriffe.
  5. Lege ein Blatt Papier bereit und zeichne für jeden Begriff einen kleinen Kreis darauf, und zwar so, dass der Kreis für einen Begriff stehts höher gezeichnet wird als die Kreise für seine echten Unterbegriffe.
  6. Verbinde den Kreis für einen Begriff jeweils mit den Kreisen seiner unteren Nachbarn.
  7. Beschrifte mit den Merkmalnamen: Trage jeweils das Merkmal m am Merkmalbegriff $(\{m\}', \{m\}'')$ ein.
  8. Beschrifte mit den Gegenstandsnamen: Trage jeweils den Gegenstand g am Gegenstandsbegriff $(\{g\}'', \{g\}')$ ein.

- Hilfssatz: Für jede Teilmenge $A \subseteq G$ ist (A",A') ein formaler Begriff und jeder Begriff von (G,M,I) ist von dieser Form. (Entsprechend dual)

  Beweis:

  1. $A'' \subseteq G$, $A' \subseteq M$ ist klar für $A \subseteq G$. Außerdem:

     $$(A'')' = A' \qquad (A')' = A''$$

     Also (A",A') formaler Begriff.
  2. Ist (A,B) formaler Begriff, dann ist $A \subseteq G$, $B = A'$ und $A = B' = (A')' = A''$, also (A,B) = (A",A').

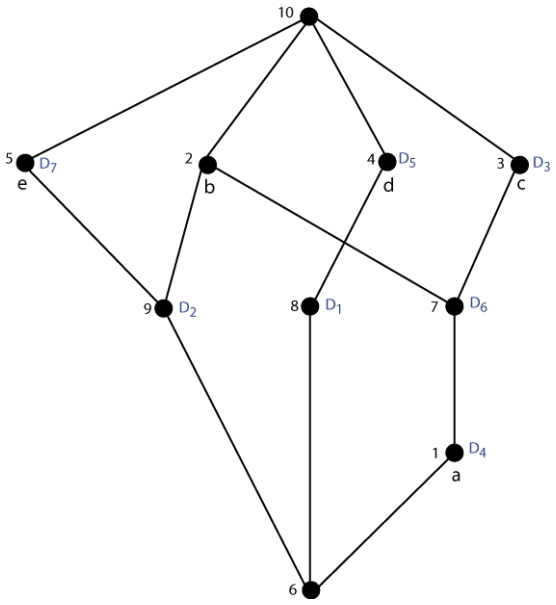
- Beispiel: gegebener formaler Kontext:

	a	b	c	d	e
D_1		√		√	
D_2		√			√
D_3			√		
D_4	√	√	√		
D_5				√	
D_6		√	√		
D_7					√

  Liste der Begriffsumfänge bzw. Inhalte:

	Begriffsumfang	Inhalt
1	$\{a\}' = \{D_4\}$	$\{a, b, c\}$
2	$\{b\}' = \{D_1, D_2, D_4, D_6\}$	$\{b\}$
3	$\{c\}' = \{D_3, D_4, D_6\}$	$\{c\}$
4	$\{d\}' = \{D_1, D_5\}$	$\{d\}$
5	$\{e\}' = \{D_2, D_7\}$	$\{e\}$
6	$\{a\}' \cap \{d\}' = \emptyset$	$\{a, b, c, d, e\}$
7	$\{b\}' \cap \{c\}' = \{D_4, D_6\}$	$\{b, c\}$
8	$\{b\}' \cap \{d\}' = \{D_1\}$	$\{b, d\}$
9	$\{b\}' \cap \{e\}' = \{D_2\}$	$\{b, e\}$
10	$\{D_1, \ldots, D_7\}$	$\emptyset$

Liniendiagramm:



- Eine *Ordnung* auf S ist eine Relation $R \subseteq S \times S$, die reflexiv, transitiv, antisymmetrisch ist. (S,R) ist dann eine geordnete Menge.
- Sind x,y Elemente einer geordneten Menge $(S, \leq)$, dann ist x ein *unterer Nachbar* von y, falls $x < y$ ist, aber kein Element z existiert mit $x < z < y$.
- Für $g \in G$ ist $(\{g\}'', \{g\}')$ der zugehörige *Gegenstandsbegriff*, für $m \in M$ ist $(\{m\}', \{m\}'')$ der zugehörige *Merkmalbegriff*.
- Hilfssatz: Es sei (G,M,I) ein formaler Kontext und $A_1, A_2 \subseteq G$. Dann gilt:

$$(A_1 \cup A_2)' = A_1' \cap A_2'$$

Beweis:

$$\begin{aligned} m \in (A_1 \cup A_2)' &\Leftrightarrow \forall g \in A_1 \cup A_2 : gIm \\ &\Leftrightarrow \forall g \in A_1 : gIm \wedge \forall g \in A_2 : gIm \\ &\Leftrightarrow m \in A_1' \cap A_2' \end{aligned}$$

- Hilfssatz: Sind (A,B) und (C,D) formale Begriffe eines Kontextes (G,M,I), dann sind auch $(A \cap C, (B \cup D)'')$ und $((A \cup C)'', B \cap D)$ formale Begriffe von (G,M,I).

$(A \cap C, (B \cup D)'')$ ist dann der größte gemeinsame Unterbegriff von (A,B) und (C,D). Dual ist $((A \cup C)'', B \cap D)$ der kleinste gemeinsame Oberbegriff von (A,B) und (C,D).

Notation:

$$\begin{aligned}(A,B) \wedge (C,D) &:= (A \cap C, (B \cup D)'') \\ (A,B) \vee (C,D) &:= ((A \cup C)'', B \cap D)\end{aligned}$$

Sprechweise: $\wedge$ heißt *Schnitt/Infimum*, $\vee$ *Verbindung/Supremum*.

Die Operationen $\vee$ und $\wedge$ sind beide assoziativ, kommutativ und idempotent, außerdem gelten die Verschmelzungsgesetze:

$$x \vee (x \wedge y) = x = x \wedge (x \vee y)$$

Eine algebraische Struktur mit diesen Eigenschaften ist ein *Verband*.

Beweisidee:

– Wir zeigen, dass $(A \cap C, (B \cup D)'')$ ein Begriff von (G,M,I) ist. Dazu muss nachgewiesen werden: $A \cap C \subseteq G$ (klar), $(B \cup D)'' \subseteq M$ (klar), $(A \cap C)' = (B \cup D)''$, $(B \cup D)'')' = A \cap C$. Dazu: Wegen $A = B'$ und $C = D'$ gilt mit dem zuvor bewiesenen Hilfssatz:

$$\begin{aligned}A \cap C &= B' \cap D' = (B \cup D)' \\ \Rightarrow (A \cap C, (B \cup D)'') &= ((B \cup D)', (B \cup D)'')\end{aligned}$$

ist ein formaler Begriff.

2 Arithmetik

- $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$, die natürlichen Zahlen. Sie bilden mit der Addition und der Multiplikation einen kommutativen Halbring, der dazu noch durch

  $$a \leq b :\Leftrightarrow \exists k \in \mathbb{N} : a + k = b$$

  verträglich geordnet ist.

- Satz: Die natürlichen Zahlen sind *wohlgeordnet*. Jede nichtleere Menge natürlicher Zahlen hat ein kleinstes Element. Dies ist eine Form des Induktionsprinzips.

- Seien $a, b \in \mathbb{N}$, $b > 0$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$ mit

  $$q \cdot b + r = a$$

  und $r < b$. Man schreibt dafür

  $$\begin{aligned} a \operatorname{div} b &:= q \\ a \mod b &:= r \end{aligned}$$

  Benutzt man die Gauss-Klammer, so hat man

  $$a \operatorname{div} b = \left\lfloor \frac{a}{b} \right\rfloor \qquad a \mod b = a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b$$

- Die *Teilbarkeitsrelation* auf $\mathbb{N}$

  $$a|b :\Leftrightarrow \exists k \in \mathbb{N} : a \cdot k = b$$

  lässt sich für $a > 0$ so schreiben:

  $$a|b \Leftrightarrow b \mod a = 0$$

- Eine natürliche Zahl p ist ist eine *Primzahl* , wenn sie größer als 1 ist und nur durch sich selbst und 1 teilbar ist.

  Merke:

  - 1 ist keine Primzahl.
  - Jede natürliche Zahl teilt 0.
  - Wenn a ein Teiler von b ist und $b > 0$, dann ist $a \leq b$.
  - Teilt a sowohl b_1 als auch b_2, dann auch $b_1 + b_2$ und $b_1 - b_2$.

- Hilfssaz: Jede natürliche Zahl > 1 ist durch eine Primzahl teilbar.

  Beweis:

  Die Menge G aller natürlichen Zahlen > 1, die nicht durch eine Primzahl teilbar ist, ist leer oder enthält ein kleinstes Element k. Entweder ist k eine Primzahl (Widerspruch) oder k hat einen Teiler mit $1 < t < k$. t muss durch eine Primzahl teilbar sein, weil $t \notin G$. Aus $p|t|k$ folgt $p|k$. Widerspruch!

- Satz: Es gibt unendlich viele Primzahlen.

  Beweis:

  Angenommen, es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_n$. Die Zahl

  $$m := \left(\prod_{i=1}^{n} p_i\right) + 1$$

  ist nach Hilfssatz durch eine Primzahl p teilbar. Wäre $p \in \{p_1, \ldots, p_n\}$, dann wäre auch $\prod p_i$ durch p teilbar und damit auch $m - \prod p_i = 1$. Widerspruch!

- Hilfssatz: Ist p eine Primzahl, dann existiert zu jeder kleineren natürlichen Zahl $r > 0$ eine Zahl s mit der Eigenschaft, dass $r \cdot s - 1$ durch p teilbar ist.

  Beweis:

  Sei r eine Zahl mit $1 < r < p$. Die Behauptung sei richtig für jede Zahl r_0 mit $0 < r_0 < r$. Es sei nun $r_0 := p \mod r$ und $k = p \operatorname{div} r$. Weil r_0 kleiner als r ist, muss es eine Zahl t geben für die $r_0 \cdot t - 1$ durch p teilbar ist, also $t \cdot r_0 - 1 = v \cdot p$ für ein v gilt. Dann ist

  $$\begin{aligned}(p-1)\cdot t \cdot k \cdot r &= (p-1)\cdot t \cdot (p - r_0)\\ &= (p-1)\cdot t \cdot p - (p-1)\cdot t \cdot r_0\\ &= p \cdot t \cdot (p-1) - (p-1)\cdot(v\cdot p + 1)\\ &= p \cdot t \cdot (p-1) - p\cdot(v\cdot p+1) + (v\cdot p + 1)\\ &= p\cdot(t\cdot(p-1) - (v\cdot p + 1) + v) + 1\end{aligned}$$

  Also erfüllt $s := t \cdot k \cdot (p-1)$ die Behauptung.

- Hilfssatz: Teilt eine Primzahl p ein Produkt zweier natürlicher Zahlen r_1 und r_2, die beide kleiner sind als p, dann ist eine davon gleich 0.

  Beweis:

  Angenommen, r_1 und r_2 sind beide > 0. Dann gibt es Zahlen s_1, s_2 mit der Eigenschaft, dass $r_1 \cdot s_1 - 1$ und $r_2 \cdot s_2 - 1$ durch p teilbar sind. Damit ist auch $(r_1 \cdot s_1 - 1)\cdot(r_2 \cdot s_2 - 1)$ durch p teilbar,

  $$\begin{aligned} w &:= (r_1 \cdot s_1 - 1)\cdot(r_2 \cdot s_2 - 1)\\ &= r_1 \cdot s_1 \cdot r_2 \cdot s_2 - r_1 \cdot s_1 - r_2 \cdot s_1 + 1\\ &= \underbrace{r_1 \cdot s_1 \cdot r_2 \cdot s_2 - (r_1 \cdot s_1 - 1) - (r_2 \cdot s_2 - 1)}_{=:z} - 1\end{aligned}$$

  Es gilt $p|z$ und $p|w$, also $p|z - w$ mit $z - w = 1$. Widerspruch!

- Hilfssatz: Teilt eine Primzahl p ein Produkt natürlicher Zahlen, dann teilt sie einen der Faktoren.

- Hilfssatz: Teilt eine Primzahl p ein Produkt zweier natürlicher Zahlen, dann teilt sie einen der beiden Faktoren.

  Beweis:

  Wenn $p|a \cdot b$, dann hat man wegen

  $$\begin{aligned} a &= p\cdot(a \operatorname{div} p) + a \mod p\\ b &= p\cdot(b \operatorname{div} p) + b \mod p\end{aligned}$$

  auch $p|(a \mod p)(b \mod p)$, also $a \mod p = 0$ oder $b \mod p = 0$ wegen letzten Hilfssatz.

- Satz: (Fundamentalsatz der Arithmetik) Jede natürliche Zahl $u > 0$ kann auf genau eine Weise als ein Produkt

$$u = \prod_{i=1}^{k} p_i^{\alpha_i}$$

geschrieben werden, wobei k eine natürliche Zahl ist, $p_1, \ldots, p_k$ Primzahlen und $\alpha_1, \ldots, \alpha_k$ positive natürliche Zahlen sind. Man nennt den Produktterm die *kanonische Darstellung* der Zahl u. Für das leere Produkt (d.h. für $k = 0$) wird der Wert 1 vereinbart.

Beweis:

Existenz: Sei n eine natürliche Zahl > 1 mit der Eigenschaft, dass jede kleinere Zahl eine kanonische Darstellung besitzt. Wenn n eine Primzahl ist, dann ist $n = n^1$ die kanonische Darstellung. Ist $n = a \cdot b$ mit $a, b > 1$, so erhält man eine kanonische Darstellung von n aus der kanonischen Darstellung von a und b:

$$n = a \cdot b = \left(\prod_{i=1}^{r} p_i^{\alpha_i} \right) \cdot \left(\prod_{j=1}^{s} q_j^{\beta_j} \right)$$

Ergibt durch Umsortieren eine kanonische Darstellung von n.

Eindeutigkeit: Für alle $m < n$ existiere eine eindeutige Darstellung.

$$\prod_{i=1}^{r} p_i^{\alpha_i} = n = \prod_{k=1}^{s} q_i^{\beta_i}$$

Wähle $p \in \{p_1, \ldots, p_r\}$. Dann ist die Zahl

$$\frac{1}{p} \cdot \prod_{i=1}^{r} p_i^{\alpha_i} = \frac{n}{p} = \frac{1}{p} \cdot \prod_{k=1}^{s} q_i^{\beta_i}$$

kleiner als n, besitzt also eine eindeutige Darstellung.

- Hilfssatz: Die Teiler einer natürlichen Zahl u mit der kanonischen Darstellung

$$u = \prod_{i=1}^{k} p_i^{\alpha_i}$$

sind genau die Zahlen der Form

$$\prod_{i=1}^{k} p_i^{\beta_i}$$

wobei β_i natürliche Zahlen sind mit $0 \leq \beta_i \leq \alpha_i$ für $i = 1, \ldots, k$.

Beispiel: $240 = 2^4 \cdot 3 \cdot 5$

- Korollar: Die Anzahl der Teiler einer Zahl n mit der kanonischen Darstellung $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ ist

$$\prod_{i=1}^{r} (\alpha_i + 1)$$

- Beispiele:

1. Wieviele durch 6 teilbare Zahlen mit genau 6 Teilern gibt es?
   Anzahl der Teiler $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1)$ soll 6 sein, also folgt $k \leq 2$. Wegen Teilbarkeit durch 6 folgt:

$$n = 2^2 \cdot 3 = 12 \qquad n = 2 \cdot 3^2 = 18$$

   sind einzige Lösungen.

2. Teilerdiagramm der Zahl 240: Die Menge aller Teiler von 240, geordnet durch die Teilbarkeit.

- Sind $\prod_{i=1}^{k} p_i^{\beta_i}$ und $\prod_{i=1}^{k} p_i^{\gamma_i}$ Teiler der natürlichen Zahl $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, dann ist der *größte gemeinsame Teiler* der Zahlen gleich

$$\prod_{i=1}^{k} p_i^{\min\{\beta_i,\gamma_i\}}$$

und das *kleinste gemeinsame Vielfache* gleich

$$\prod_{i=1}^{k} p_i^{\max\{\beta_i,\gamma_i\}}$$

- Satz: Für jede natürliche Zahl $n > 0$ gilt: Die menger aller Teiler von n bildet mit den Operationen

$$\begin{aligned} s \wedge t &:= ggT(s,t) \\ s \vee t &:= kgV(s,t) \end{aligned}$$

einen Verband, d.h. es gelten die Gleichungen

1. $s \wedge s = s$ und $s \vee s = s$
2. $r \wedge (s \wedge t) = (r \wedge s) \wedge t$ und $r \vee (s \vee t) = (r \vee s) \vee t$
3. $s \wedge t = t \wedge s$ und $s \vee t = t \vee s$
4. $s \wedge (s \vee t) = s$ und $s \vee (s \wedge t) = s$
5. Diese Verbände sind sogar distributiv, d.h. es gelten auch

$$r \wedge (s \vee t) = (r \wedge s) \vee (r \wedge t) \qquad r \vee (s \wedge t) = (r \vee s) \wedge (r \vee t)$$

Beweis: Folgt aus entsprechenden Eigenschaften von min, max

3 Axiomatik

- Man legt Regeln für den Umgang mit den untersuchten Objekten fest (Axiome genannt) und untersucht nur noch, was aus diesen Regeln folgt. Ein solches Axiomensystem für die Arithmetik wurde von R. Dedekind sprachlich formuliert und dann von G. Peano formalisiert, die Peano-Axiome:

  1. Zu jeder natürlichen Zahl n gibt es genau eine natürliche Zahl n^+, genannt der Nachfolger von n.
  2. Aus $n^+ = m^+$ folgt stets n=m, d.h. jede natürliche Zahl ist Nachfolger von höchstens einer natürlichen Zahl.
  3. Es gibt eine natürliche Zahl, 0 genannt, die nicht Nachfolger einer natürlichen Zahl ist.
  4. Ist S eine Menge von natürlichen Zahlen, welche die Zahl 0 enthält und die die Eigenschaft hat, dass mit $n \in S$ stets auch $n^+ \in S$ gilt, dann ist S die Menge aller natürlichen Zahlen. (Induktionsaxiom)

- Modell der Peano-Axiome: Wir definieren für Mengen

  $$S^+ := S \cup \{S\}$$

  Betrachte die Folge $\emptyset, \emptyset^+, \emptyset^{++}, \ldots$, genauer

  $$\emptyset, \{\emptyset\}, \{\emptyset\{\emptyset\}, \{\emptyset\{\emptyset, \{\emptyset\}\}\}, \ldots$$

  Man benötigt ein eigenes Axiom der Mengenlehre um sicherzustellen, dass auch die Menge

  $$\mathbb{N} := \{\emptyset, \emptyset^+, \ldots\}$$

  existiert. In diesem Fall ist $0 := \emptyset$ und $n+1 := \{1, \ldots, n\}$. Jede natürliche Zahl ist gleich der Menge aller echt kleineren natürlichen Zahlen.

- Ein Beweis der Widerspruchsfreiheit der elementaren Arithmetik wurde 1936 von Genzen angegeben.

- Definition von Addition, Multiplikation und einer Ordnung:

  $$\begin{aligned} n + 0 &:= n \qquad & n + m^+ &:= (n+m)^+ \\ n \cdot 0 &:= 0 \qquad & n \cdot m^+ &= n \cdot m + n \\ n \leq m &\Leftrightarrow \exists k \in \mathbb{N}_0 : n + k = m \end{aligned}$$

- Vier schwerwiegende Fragen:

  1. Ist das angegebene Modell (bis auf Isomorphie) das einzig mögliche? (Ist Peanos Axiomensystem kategorisch?)
  2. Kann das Induktionsaxiom durch ein einfacheres ersetzt werden, genauer: Kann man ein Axiomensystem erster Stufe für die natürlichen Zahlen angeben? (Das Induktionsaxiom ist nicht in Logik erster Stufe formuliert, weil über Mengen quantifiziert wird.)

3. Kann man noch Axiome hinzunehmen, die aus den angegebenen weder beweisbar noch widerlegbar sind? (Vollständigkeit)
4. Reichen die natürlichen Zahlen zum Zählen aus?

Antworten:

1. Ja.
2. Nach einem Satz (von Skolem) aus der mathematischen Logik gibt es zu jeder unendlichen mathematischen Struktur eine weitere, die zu ihr elementar äquivalent, aber nicht isomorph ist. Zwei Strukturen heißen elementar äquivalent, wenn in ihnen genau die gleichen Sätze der Logik erster Stufe gelten. Es gibt also „Nonstandard natürliche Zahlen“, d.h. eine mathematische Struktur, in der genau die gleichen Regeln erster Stufe gelten wie in den natürlichen Zahlen, die aber nicht zu $\mathbb{N}$ isomorph ist.
3. Der Gödelsche Unvollständigkeitssatz sagt (insbesondere), dass es für jedes endliche Axiomensystem der natürlichen Zahlen Aussagen gibt, die wahr, aber nicht aus den Axiomen beweisbar sind. Die Theorie der natürlichen Zahlen ist unvollständig.
4. Die Frage „Wieviele natürliche Zahlen gibt es?“ hat als Antwort offenbar keine natürliche Zahl. Georg Cantor hat gezeigt, dass man sinnvoll unendliche Zahlen einführen und benutzen kann.

- Wie kommt man von $\mathbb{N}$ zu $\mathbb{Z}$? Bei der soliden mathematischen Konstruktion geht man so vor: Man bildet zunächst $\mathbb{N}_0 \times \mathbb{N}_0$ und faktorisiert nach einer geeigneten Äquivalenzrelation.

- $\mathbb{N}$ ist ein kommutativ angeordneter Halbring mit Eins. Aus den natürlichen Zahlen konstruiert man den Ring $\mathbb{Z}$ der ganzen Zahlen: Sei zunächst $\mathbb{N} \times \mathbb{N}$ die Menge aller Paare natürlicher Zahlen und faktorisiert nach der Äquivalenzrelation

$$(u, v)\Delta(x, y) :\Leftrightarrow u + y = v + x$$

Die Äquivalenzrelation nennt man die ganzen Zahlen. Beachte:

$$(u, v)\Delta(x, y) \Leftrightarrow u - v = x - y$$

Auf den Äquivalenzklassen definiert man:

$$\begin{aligned} (u, v)/_\Delta + (x, y)/_\Delta &:= (u + x, v + y)/_\Delta \\ (u, v)/_\Delta \cdot (x, y)/_\Delta &:= (u \cdot x + v \cdot y, u \cdot y + v \cdot x)/_\Delta \\ (u, v)/_\Delta \leq (x, y)/_\Delta &:\Leftrightarrow u + x \leq v + y \end{aligned}$$

Diese sind wohldefiniert. Man hat eine zusätzliche einstellige Operation $-$, welche durch

$$-(x, y)/_\Delta := (y, x)/_\Delta$$

definiert ist.

- Die Menge $\mathbb{Z}$ aller ganzen Zahlen bildet mit diesen Operationen und der Ordnung einen angeordneten kommutativen Ring mit Eins.

- Die Kommutativität der Addition ist in einem kommutativen Ring mit Eins automatisch gegeben durch:

$$\begin{aligned} a + a + b + b = a \cdot (1 + 1) + b \cdot (1 + 1) &= (a + b) \cdot (1 + 1) = (a + b) + (a + b) \\ \Rightarrow -a + a + a + b + b &= -a + a + b + a + b \\ \Rightarrow a + b + b - b &= b + a + b - b \\ \Rightarrow a + b &= b + a \end{aligned}$$

Die natürlichen Zahlen sind dabei in $\mathbb{Z}$ eingebettet: $n \mapsto (n, 0)/_\Delta$ (ist eine strukturerhaltende Einbettung von $\mathbb{N}$ in $\mathbb{Z}$).

- Verzweigung im Zahlensystem:
  1. zu den Körpern $\mathbb{Q}, \mathbb{A}, \mathbb{R}, \mathbb{C}$
  2. zur modularen Arithmetik
- Von $\mathbb{Z}$ zum Körper $\mathbb{Q}$ der rationalen Zahlen kommt man durch eine ähnliche Konstruktion: Man bildet die Menge $\mathbb{Z} \times \mathbb{N}\backslash\{0\}$, nennt deren Elemente *Brüche* und notiert $\frac{z}{n}$ statt (z, n). Darauf wird wieder eine Äquivalenzrelation $\sim$ eingeführt:

$$\frac{u}{v} \sim \frac{x}{y} :\Leftrightarrow u \cdot y = v \cdot x$$

  Die Klassen dieser Äquivalenz nennt man Bruchzahlen oder *rationale Zahlen*. Addition, Multiplikation, Ordnung und multiplikativ inverse Elemente werden wie bekannt eingeführt, Definitionen sind mit $\sim$ verträglich:

$$\begin{aligned} \frac{x}{y} + \frac{u}{v} &= \frac{x \cdot v + y \cdot u}{y \cdot v} \\ \frac{x}{y} \cdot \frac{u}{v} &= \frac{x \cdot u}{y \cdot v} \qquad \left(\frac{z}{n}\right)^{-1} = \frac{\frac{z}{|z|} \cdot n}{|z|} \qquad (z \neq 0) \\ \frac{x}{y} \leq \frac{u}{v} &:\Leftrightarrow x \cdot v \leq u \cdot y \end{aligned}$$

  Die so eingeführten rationalen Zahlen bilden einen (angeordneten) kommutativen Körper. Die rationalen Zahlen reichen aber nicht zur Beschreibung der in der Anschauungsgeometrie auftretenden Längen. Die Länge der Diagonale eines Quadrates der Seitenlänge 1 ist nicht rational, d.h. $\sqrt{2}$ ist nicht rational.

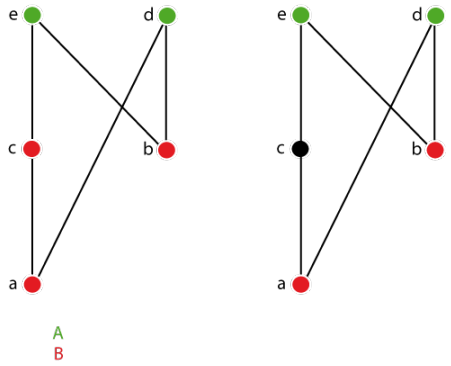
  Beweis:

  – Annahme es gäbe teilerfremde ganze Zahlen mit $\frac{a}{b} = \sqrt{2} \Leftrightarrow a^2 = 2b^2$. Dabei darf angenommen werden, dass a, b nicht gleichzeitig gerade sind. Weil a^2 durch 2 teilbar ist, muss a durch 2 teilbar sein und deshalb a^2 durch 4 teilbar. Damit ist auch b gerade. Widerspruch!

  Die rationen Zahlen reichen also nicht aus und man kann nach Körpererweiterungen von $\mathbb{Q}$ fragen, welche $\sqrt{2}$ enthalten.
- Die Menge aller *algebraischen Zahlen*, d.h. derjenigen komplexen Zahlen, die Nullstellen von Polynomen mit rationalen Koeffizienten sind, bilden einen Körper. Nicht-algebraische Zahlen heißen *transzendent* (z.B. e, π). Es gibt überabzählbar viele transzendente Zahlen, d.h. die algebraischen Zahlen sind abzählbar.

Einschub: Schnitte einer geordneten Menge

- Sei $(P, \leq)$ eine geordnete Menge, d.h. $\leq \subseteq P \times P$ ist eine transitive, reflexive und antisymmetrische Relation auf P (eine *Ordnung*).
- Ein Schnitt einer geordneten Menge $(P, \leq)$ ist ein Paar (A,B) von Teilmengen von P, dass die folgenden Eigenschaften erfüllt:
  1. Jedes Element von A ist $\leq$ jedem Element von B.
  2. A und B sind bzgl. dieser Bedingung maximal.
- Beispiel:



Links: Kein Schnitt, weil $c \not\leq d$; rechts: Schnitt

- Behauptung: Die Schnitte einer geordneten Menge $(P, \leq)$ sind genau die formalen Begriffe des formalen Kontextes $(P, P, \leq)$. Für eine Menge A von Gegenständen:

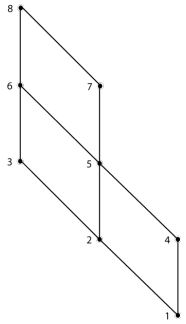
$$A^{\leq} = \{m \in P | \forall a \in A : a \leq m\}$$

d.h. $A^{\leq}$ ist die Menge aller oberen Schranken von A. Dual ist für eine Menge B von Merkmalen

$$B^{\leq} = \{g \in P | \forall b \in B : g \leq b\}$$

d.h. $B^{\leq}$ ist die Menge aller unteren Schranken von B. (A,B) ist ein formaler Begriff von $(P, P, \leq) \Leftrightarrow A \subseteq P$, $B \subseteq P$, $A' = B$, $B' = A \Leftrightarrow A, B \subseteq P$, A besteht aus allen unteren Schranken von B, B aus allen oberen Schranken von A. $\Leftrightarrow$ (A,B) ist ein Schnitt von $(P, \leq)$.

- Beispiel: Alle Schnitte von obigem Beispiel



mit

	Begriffsumfang	Inhalt
1	$\emptyset$	a,b,c,d,e
2	a	a,c,d,e
3	a,c	c,e
4	b	b,d,e
5	a,b	d,e
6	a,b,c,e	e
7	a,b,d	d
8	a,b,c,d,e	$\emptyset$

- Beobachtung: Ist $(P, \leq)$ eine geordnete Menge, $a \in P$,

$$\begin{aligned} \downarrow a &:= \{p \in P | p \leq a\} \\ \uparrow a &:= \{p \in P | a \leq p\} \end{aligned}$$

dann ist $(\downarrow a, \uparrow a)$ ein Schnitt von $(P, \leq)$. Die Menge $\{(\downarrow p, \uparrow p); p \in P\}$ ist mit der induzierten Ordnung ordnungsisomorph zu $(P, \leq)$, die Abbildung $p \mapsto (\downarrow p, \uparrow p)$ ist eine Ordnungseinbettung.

- $\mathcal{B}(P, P, \leq)$, die Dedekind-McNeillsche-Vervollständigung von $(P, \leq)$ ist der kleinste vollständige Verband, der $(P, \leq)$ ordnungsisomorph enthält.

Von $\mathbb{Q}$ zu $\mathbb{R}$

- 1888 hat Richard Dedekind eine ernste formale Konstruktion der reellen Zahlen aus den rationalen angegeben:
$$\mathbb{R} \cup \{\infty, -\infty\} \cong \mathcal{B}(\mathbb{Q}, \mathbb{Q}, \leq)$$
Die Schnitte der geordneten Menge $(\mathbb{Q}, \leq)$ nennt man *Dedekindsche Schnitte*. Kennt man die reellen Zahlen bereits, dann kann man die Dedekindschen Schnitte einfach beschreiben: Zu jedem $r \in \mathbb{R} \cup \{\pm\infty\}$ ist
$$(\{q \leq r | q \in \mathbb{Q}\}, \{q \geq r | q \in \mathbb{Q}\})$$
ein Schnitt.

- $\mathcal{F} := \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$ ist eine linear geordnete menge mit 4 Elementen, die selber Mengen sind und deren Vereinigung gleich $\{a, b, c\}$ ist. Die Menge
$$\{\{q \in \mathbb{Q} | q \leq r\} | r \in \mathbb{R}\}$$
ist eine geordnete Menge mit überabzählbar vielen Elementen, deren Vereinigung gleich $\mathbb{Q}$, also abzählbar ist.

- Auf der Menge der Dedekindschen Schnitte (ohne $\pm\infty$) kann man die algebraischen Operationen $+, -, \cdot, /$ einführen. Die Menge $\mathbb{R}$ der reellen Zahlen wird dadurch zu einem angeordneten Körper, der die rationen Zahlen (und damit auch $\mathbb{Z}, \mathbb{N}$) enthält. $\mathbb{R}$ und $\mathbb{Q}$ sind sogar *archimedisch angeordnet*, d.h. zu jeder reellen Zahl r gibt es eine natürliche Zahl n mit $r \leq n$.

- Achtung: Die Bedingung „archimedisch angeordnet“ greift auf die natürlichen Zahlen und damit auf das Induktionsaxiom zurück. Nichtstandard-reelle Zahlen sind zu den reellen Zahlen elementar äquivalent.

Von $\mathbb{R}$ zu $\mathbb{C}$

- Man kann die komplexen Zahlen auf viele Weisen einführen:

  1. Als Vektorraum aller Paare reeller Zahlen, versehen mit der Multiplikation
  $$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$
  Einprägsamer ist es die Standardbasis mit abkürzenden Namen zu versehen:
  $$\mathbf{1} := (1, 0)^T \qquad \imath := (0, 1)^T$$
  und die Multiplikation für die Basis festzulegen:
  $$\mathbf{1} \cdot \mathbf{1} = 1 \qquad \mathbf{1} \cdot \imath = \imath \cdot \mathbf{1} = \imath \qquad \imath \cdot \imath = -\mathbf{1}$$
  Mit Hilfe der Körpergesetze erhält man die Multiplikation wie allgemein angegeben:
  $$\begin{aligned} (a, b) \cdot (c, d) &= (a \cdot \mathbf{1} + \imath \cdot b) \cdot (c \cdot \mathbf{1} + \imath \cdot d) \\ &= (ac - bd) \cdot \mathbf{1} + \imath \cdot (ad + bc) \end{aligned}$$

  2. Als Faktorring des Polynomrings $\mathbb{R}[x]$ nach dem Modulpolymom $x^2 + 1$. Die Multiplikation ist die Polynommultiplikation modulo $x^2 + 1$. Jede Restklasse enthält genau ein Polynom vom Grad ≤ 1, also genau ein Polynom der Form $a \cdot x + b$. Dieses repräsentiert die komplexe Zahl $b + \imath \cdot a$:
  $$\begin{aligned} (aX + b) \cdot (cX + d) &= acX^2 + (ad + bc)X + bd \\ &\equiv -ac + bd + (ad + bc) \cdot X \end{aligned}$$

3. Man kann $\mathbb{C}$ auch einführen als die Menge aller reellen 2×2-Matrizen der Form

$$A := \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad (a, b \in \mathbb{R})$$

Addition und Multiplikation sind dann genau die Matrix-Addition bzw. Multiplikation:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bc \end{pmatrix}$$

Wegen $\det A = a^2 + b^2 \neq 0$ für $(a, b) \neq (0, 0)$ hat jede solche Matrix eine Inverse (außer $A = 0$) die die gleiche Form hat.

- Der Körper $\mathbb{C}$ der komplexen Zahlen ist *algebraisch abgeschlossen*. Das besagt der Fundamentalsatz der Algebra: Jedes nichtkonstante Polynom mit komplexen Koeffizienten hat eine Nullstelle.
- Verloren geht die Ordnung: Es gibt keine mit der komplexen Multiplikation verträgliche Ordnung von $\mathbb{C}$.
- Sehr reizvoll, aber nicht Gegenstand der Vorlesung, ist das Studium der komplexen ganzen Zahlen $a + \imath b$ mit $a, b \in \mathbb{Z}$ (*Gaußsche ganze Zahlen*). Viele Fragen über ganze Zahlen stellen sich dafür neu, z.B. die nach den Gaußschen primzahlen: 3 ist prim, aber 5 nicht wegen $5 = (2 + \imath) \cdot (2 - \imath)$.
- Die komplexen Zahlen vom Betrag 1 sind gegen die Multiplikation abgeschlossen. Unter diesen Zahlen findet man für jede natürliche Zahl $n > 0$ die n verschiedenen n-ten Einheitswurzeln

$$e^{\frac{k}{n} \cdot 2\pi\imath} \qquad k \in \{0, \ldots, n-1\}$$

4 Gruppoide

- Gruppoide $(P, \circ)$, die den Gleichungen $(^*)$

$$\begin{aligned} x \circ x &= x \\ x \circ y &= y \circ x \\ x \circ (x \circ y) &= y \end{aligned}$$

  genügen, nennt man *Squags* (Steinersche Quasigruppen).

- 1841, Kirkman: Schulmädchenproblem. 15 Mädchen gehen in Dreierreihen jeden Tag zur Schule. Während einer Woche soll kein Mädchen zweimal mit einem anderen in der gleichen Reihe gehen.

  Beobachtung: Es gibt $\binom{15}{2} = 105$ Möglichkeiten Zweimengen von Mädchen. Jede Dreierreihe enthält drei Zweiermengen. Der Wochenplan benötigt $7 \cdot 5$ Dreierreihen und deckt damit $7 \cdot 5 \cdot 3 = 105$, also alle möglichen Dreierreihen ab.

  Konsequenz: Jedes Mädchen geht (in einer Woche) mit jedem anderen Mädchen genau einmal in der gleichen Reihe.

  Auf der Menge P der Mädchen definieren wir eine Multiplikation $\circ$ wie folgt:

$$\begin{aligned} \forall a \in P : a \circ a &= a \\ a \circ b &= c \Leftrightarrow \{a, b, c\} \text{ repräsentiert Dreierreihe} \end{aligned}$$

  Erfüllen $(^*)$. Beobachtung: jede Lösung des kirkmanschen Schulmädchenproblems führt auf eine Squag.

- Konstruktion einer Squag für zweielementige Menge P:

$$a, b, a \circ a, b \circ b, b \circ a, a \circ b, \ldots$$

  (Terme zur gegebenen Signatur und Variablenmenge) Die *Termalgebra* wird nach der von den definierten Gleichungen erzeugten Gleichungstheorie faktorisiert und man erhält eine *freie Algebra*.

- Wir suchen Modelle dieser Gleichungsbasis,also algebraische Strukturen $(A, \circ)$ vom Typ $(^*)$, die all diese Gleichungen erfüllen.

  1. freie Konstruktion: $A = \{a, b, a \circ b\}$

$\circ$	a	b	$a \circ b$
a	a	$a \circ b$	b
b	$a \circ b$	b	a
$a \circ b$	b	a	$a \circ b$

     Der Prozess führt im Allgemeinen zu einem unendlich großen Modell, z.B. für dreielementige Trägermenge. Die Struktur

$\circ$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	1

erfüllt die Gleichungen. Hier ist $a \circ b = 2 \cdot (a + b) \bmod 3$.

Wir nehmen noch die Gleichung

$$x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$$

hinzu. Für obiges Beispiel:

$$\begin{aligned} x \circ (y \circ z) &= 2 \cdot (2x + 2(y + z)) \mod 3 \\ &= 2x + y + z \\ (x \circ y) \circ (x \circ z) &= 2(2(x + y) + 2(x + z)) = 4x + 4y + 4x + 4z \\ &= 2x + y + z \mod 3 \end{aligned}$$

2. Modell: AG(2,3), affine Geometrie mit 2 Elementen über $\mathbb{Z}_3$. Man kann ein direktes Produkt bilden:
$$(a, b) \circ (c, d) := (a \circ c, b \circ d)$$
Bei Bildung direkter Produkte bleibt die Gültigkeit von Gleichungen erhalten.
3. Modell: PG(2,2), projektive Geometrie mit 2 Elementen der Dimension 2

- Es gibt n-elementige Squags für jedes $n \equiv 1$ oder 3 mod 6: $1, 3, 7, 9, 13, 15, \ldots$

Einschub: Codierung

- Dreimaliges Wiederholen einer Nachricht liefert einen 1-Fehler-korrigierenden (12,4)-Code, d.h. 12 Zeichen für 4 Zeichen Information.
- Einen 1-Fehler-korrigierenden binären (7,4)-Code erhält man als Kern der Matrix GF(2),

$$\begin{aligned} H_3 &:= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ C &:= \{v \in \{0,1\}^7 | H_3 \cdot v = 0\} \end{aligned}$$

Es gilt: $\dim C = 7 - 3 = 4$. Somit $|C| = 16$. Die Vektoren des Kerns können als 1-Fehler-korrigierender (7,4)-Code verwendet werden. Beispiel:

$$\begin{aligned} v &= \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ \Rightarrow H_3(v + e_5) &= \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = H_3 \cdot v + H_3 \cdot e_5 \end{aligned}$$

also Fehler an 5. Koordinate.

5 Rechnen Modulo n

- Im Folgenden sei $\mathbb{Z}_n := \{0, \ldots, n-1\}$. Die Abbildung

$$z \mapsto z \mod n = z - \left\lfloor \frac{z}{n} \right\rfloor \cdot n \qquad (n \geq 1)$$

bildet jede ganze Zahl nach $\mathbb{Z}_n$ ab. Wir nennen zwei Zahlen y, z *kongruent modulo* n, falls $y \mod n = z \mod n$. Der Einfachheit halber wird dies mit $y \equiv z$ (mod n) abgekürzt. Beispiel:

$$131 \cdot 76 + 9 \equiv 5 \cdot 6 + 2 \equiv 32 \equiv 4 \qquad (\mod 7)$$

Auf der Menge $\mathbb{Z}_n$ kann man eine Addition, eine Subtraktion und eine Multiplikation wie folgt definieren:

$$\begin{aligned} (a, b) &\mapsto (a + b) \mod n \\ (a, b) &\mapsto (a - b) \mod n \\ (a, b) &\mapsto (a \cdot b) \mod n \end{aligned}$$

Mit diesen Operationen wird $\mathbb{Z}_n$ zu einem kommutativen Ring mit Eins, d.h. $(\mathbb{Z}_n, +, -, 0)$ ist eine (abelsche) Gruppe, $\cdot$ ist kommutativ, distributiv über $+$ und hat 1 als neutrales Element.

- Satz: Für $n > 1$ ist $\mathbb{Z}_n := (\mathbb{Z}_n, +, -, \cdot)$ ein kommutativer Ring mit Eins und die Abbildung $z \mapsto z \mod n$ ist ein surjektiver Ringhomomorphismus.

- Für das praktische Rechnen modulo n bedeutet dies, dass in $\mathbb{Z}$ gerechnet werden kann und zwischendurch, jedenfalls aber am Schluß, modulo n reduziert wird.

- Teilbarkeitsregeln:

  1. Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist, d.h.

$$n = \sum_{i=0}^{k} z_i \cdot 10^i \qquad (z_i \in \mathbb{Z}_{10})$$

  ist genau dann durch 9 teilbar, wenn $q := \sum_{i=0}^{k} z_i$ durch 9 teilbar ist.

  Wegen $10 \equiv 1 \pmod 9$ gilt $10^i \equiv 1 \pmod 9$ für jedes $i \in \mathbb{N}$ und damit

$$\sum_{i=0}^{k} z_i \cdot 10^i \equiv \sum_{i=0}^{k} z_i \qquad (\mod 9)$$

  2. Eine natürliche Zahl ist genau dann durch 11 teilbar, wenn die Differenz der alternierenden Quersumme durch 11 teilbar ist. Der Grund dafür ist, dass $10 \equiv -1 \pmod{11}$ ist.

  Beispiel: 1327419, dann $(1 + 2 + 4 + 9) - (3 + 7 + 1) = 16 - 11 = 5$, also nicht durch 11 teilbar.

3. Teilbarkeit durch 7 im Oktalsystem

$$n = \sum_{i=0}^{k} z_i \cdot 8^i \qquad (z_i \in \mathbb{Z}_8)$$

Eine Oktalzahl ist genau dann durch 7 teilbar, wenn ihre Quersumme durch 7 teilbar ist. (siehe (1))

Beispiel: Oktalzahl 3732 (Dezimal: 2010) ist nicht durch 7 teilbar, sondern um eins größer als eine durch 7 teilbare Zahl.

4. Teilbarkeit durch 37: Man stellt fest, dass 37,74,111 durch 37 teilbar sind, also auch 999 durch 37 teilbar, also $1000 \equiv 1 \pmod{37}$. Jede natürliche Zahl n ist modulo 37 kongruent zur Summe der „Dreierblöcke“

$$z_j + 10 \cdot z_{j+1} + 100 z_{j+2} \qquad j \equiv 0 \mod 3$$

Beispiel: 1234567890, dann $1 + 234 + 567 + 890 = 1692$, $1 + 692 = 693$. 693 ist nicht durch 37 teilbar, also auch nicht 1234567890.

- Algorithmen zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen:

1. Algorithmus „Wechselwegnahme“, am Beispiel der Zahlen 238, 154:

154	238
154	84 = 238-154
70	84
70	14
56	14
42	14
28	14
14	14
14	0

Also ist der größte gemeinsame Teiler 14.

2. Euklidischer Algorithmus:

```
Input: m,n (m>=n)
while n != 0 do
(m,n) := (n, m \mod n)
Output: "ggT = " m
```

Beispiel: 238, 154

m	n
238	154
154	84
84	70
70	14
14	0

- Satz: Zu je zwei natürlichen Zahlen m, n gibt es ganze Zahlen α, β mit ggT(m,n) = $\alpha \cdot m + \beta \cdot n$.

Beispiel:

$$\begin{aligned} 84 &= 238 - 154 \qquad 70 = 154 \qquad 14 = 84 - 70 \\ 14 &= 238 - 154 - (154 - 84) = 238 - 154 - (154 - (238 - 154)) \\ &= 2 \cdot 238 - 3 \cdot 154 \end{aligned}$$

Die Berechnung dieser Zahlen α und β wird immer dann benötigt, wenn modulo n „dividiert“ werden soll.

Gruppen: Satz von Lagrange

- Eine Untergruppe einer Gruppe $(G, \circ, ^{-1}, e)$ ist eine Teilmenge $U \subseteq G$, die gegen die fundamentalen Operationen abgeschlossen ist, d.h. für die gilt

$$x, y \in U \Rightarrow x \circ y \in U \qquad x \in U \Rightarrow x^{-1} \in U \qquad e \in u$$

- Ist $(G, \circ, ^{-1}, e)$ eine Gruppe, $U \subseteq G$ eine Untergruppe und $g \in G$, dann heißt

$$g \circ U := \{g \circ u | u \in U\}$$

  die *Linksnebenklasse* von U durch g.

- Hilfssatz: Je zwei verschiedene Linksnebenklasse einer Untergruppe sind disjunkt.

  Beweis:

  – Seien $g \circ U$, $h \circ U$ Linksnebenklassen von U. Sei $x \in (g \circ U) \cap (h \circ U)$. Dann existieren Elemente $u_1, u_2 \in U$ mit $x = g \circ u_1 = h \circ u_2$ und es folgt

$$h = g \circ \underbrace{u_1 \circ u_2^{-1}}_{\in U} \in g \circ U$$

    Für ein beliebiges Element $h \circ U$ existiert jeweils ein $u \in U$ mit

$$y = h \circ u = g \circ (u_1 \circ u_2^{-1}) \circ u \in g \circ U$$

    Also $g \circ U \supseteq h \circ U$. Analoge Argumentation: $g \circ U \subseteq h \circ U$. Also $g \circ U = h \circ U$.

- Hilfssatz: Die Abbildung $u \mapsto g \circ u$ ist eine Bijektion von U auf $g \circ U$. Insbesondere gilt $|U| = |g \circ U|$.

  Beweis:

  – Surjektivität ist klar. Injektivität: Aus $g \circ u_1 = g \circ u_2$ folgt

$$g^{-1} \circ g \circ u_1 = g^{-1} \circ g \circ u_2 \Leftrightarrow u_1 = u_2$$

- Hilfssatz: Jedes Element von G liegt in einer Nebenklasse von U.

- Satz von Lagrange: Ist U eine Untergruppe von einer endlichen Gruppe G, dann ist $|U|$ stets ein Teiler von $|G|$.

  (Äquivalent: Die Ordnung einer Untergruppe ist stets ein Teiler von der Gruppenordnung (für endliche Gruppen), mit „Ordnung“ wird hierbei die „Anzahl der Elemente“ bezeichnet.)

  Ist $(G, \circ, ^{-1}, e)$ eine Gruppe und $g \in G$, dann bilden die Potenzen von g eine (kommutative) Untergruppe. Solche Untergruppen nennt man *zyklisch*. Die Anzahl der Elemente einer von g erzeugten zyklischen Gruppe ist entweder unendlich oder gleich der kleinsten Zahl $n > 0$ mit $g^n := g \circ g \circ \ldots \circ g = e$. Man nennt diese Zahl die *Ordnung von g*.

- Korollar: In einer endlichen Gruppe ist die Ordnung jedes Elements ein Teiler der Gruppenordnung.

Einheiten Modulo n

- Es soll gelten: (Division modulo 6)

  1. 2 geteilt durch 2 soll 1 sein.

2. 0 geteilt durch 2 soll 0 sein.

Das führt dann zu

$$3 \equiv 3 \cdot \frac{2}{2} \equiv \frac{3 \cdot 2}{2} \equiv \frac{0}{2} \equiv 0$$

also auf einen Widerspruch. Es gibt keine Möglichkeit modulo 6 eine halbwegs vernünftige Division durch 2 einzuführen.

- Man nennt eine Zahl $a \neq 0$ in einem Ring einen *Nullteiler*, wenn es eine Zahl $b \neq 0$ gibt mit $a \cdot b = 0$.
- Man kann das oben gegebene Beispiel leicht so verallgemeinern, dass klar wird: Eine Division durch einen Nullteiler kann nicht sinnvoll definiert werden.
- Man nennt eine Zahl a in einem Ring eine *Einheit*, wenn es eine Zahl b gibt mit $a \cdot b = 1$. Multiplikation mit b entspricht der Division durch a.

Einheiten und Nullteiler modulo n

- Satz: Für jedes Element $a \in \mathbb{Z}_n \backslash \{0\}$ ist entweder Nullteiler oder Einheit.
- Beispiel: Nullteiler in $\mathbb{Z}_{12}$:

$$\{2, 3, 4, 6, 8, 9, 10\}$$

Einheiten in $\mathbb{Z}_{12}$:

$$\{1, 5, 7, 11\}$$

- Satz: Ein Element $a \in \mathbb{Z}_n \backslash \{0\}$ ist genau dann eine Einheit modulo n, wenn ggT(a,n)= 1. Die Einheiten bilden bzgl. der Multiplikation eine Gruppe.

Beweis:

– Wenn $d := ggT(a, n) > 1$ ist, dann ist $\frac{n}{d} \in \mathbb{Z}_n$. Damit

$$a \cdot \frac{n}{d} = \frac{a \cdot n}{d} = \frac{a}{d} \cdot n \equiv 0 \mod n$$

und folglich a ein Nullteiler von $\mathbb{Z}_n$. Wenn $ggT(a, n) = 1$, dann gibt es Zahlen α, β mit $\alpha \cdot a + \beta \cdot n = 1$ (euklidischer Algorithmus). Daraus folgt

$$\begin{aligned} (\alpha \cdot a + \beta \cdot n) \mod n &= 1 \\ \Leftrightarrow ((\alpha \cdot a) \mod n + (\beta \cdot n) \mod n) \mod n &= 1 \\ \Leftrightarrow (\alpha \cdot a) \mod n &= 1 \\ \Leftrightarrow (\alpha \cdot \mod n) \cdot a \mod n &= 1 \end{aligned}$$

Folglich ist a eine Einheit.

- Dividieren durch Modulo n kann man nur durch Einheiten, d.h. durch diejenigen Elemente $a \in \mathbb{Z}_n \backslash \{0\}$ mit ggT(a,n)= 1. Ist a ein solches Element, dann findet man zu a einen Kehrwert, d.h. ein Element $b \in \mathbb{Z}_n$ mit $a \cdot b \equiv 1 \mod n$ wie folgt: Man findet ganze Zahlen α, β mit $\alpha \cdot a + \beta \cdot n = 1$ mit Hilfe des euklidischen Algorithmus und setzt $b := \alpha \mod n$.
- Beispiel: $n = 31, a = 3$

$$\begin{aligned} 1 &= -10 \cdot 3 + 1 \cdot 31 \\ \Rightarrow b &= -10 \mod 31 = 21 \end{aligned}$$

In der Tat gilt $21 \cdot 3 = 63 \equiv 1 \mod 31$.

- Wenn p eine Primzahl ist, dann ist jedes von Null verschiedene Element in $\mathbb{Z}_p$ Einheit und es gibt genau $p-1$ Einheiten. Nach dem Satz von Lagrange ergibt sich das Lemma von Fermat: Ist p eine Primzahl, dann gilt für jede nicht durch p teilbare Zahl a, dass $a^{p-1}-1 \equiv 0 \mod p$.

  Beweis vom Lemma von Fermat durch Anwenden des Satzes von Lagrange auf die Gruppe der Einheiten von $\mathbb{Z}_p$: Diese Gruppe hat $p-1$ Elemente. Damit $a^{p-1} \equiv 1 \mod p$. (siehe „Ordnung von g)

- Beispiel: Für $p = 11$ erhält man, dass die Zahlen $2^{10}-1, 3^{10}-1, \ldots, 10^{10}-1$ durch 11 teilbar sind.

- Man kann mit dem Lemma von Fermat zeigen, dass eine Zahl nicht prim ist.

  Beispiel: Wir zeigen, dass 35 nicht prim ist. Dazu berechnet man $2^{34} \mod 35$:

$$\begin{aligned} 2^{34} &= 2^{32} \cdot 2^2 = ((((2^2)^2)^2)^2)^2 \cdot 2^2 \\ &= ((((2^2)^2)^2)^2 \cdot 2)^2 = ((16^2)^2 \cdot 2)^2 \equiv (11^2 \cdot 2)^2 \equiv (16 \cdot 2)^2 \\ &\equiv (-3)^2 = 9 \qquad \mod 35 \end{aligned}$$

  (Rechenmethode: „Square and Multiply“)

- Die Verallgemeinerung des Lemmas von Fermat: Dazu benötigt man die Eulersche φ-Funktion. Für $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ (kanonische Darstellung) sei

$$\varphi(n) \quad := \quad n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

- Satz: $\varphi(n)$ gibt die Anzahl der Einheiten von $\mathbb{Z}_n$ an.

  Beweis:

  – Gegegen sei n, eine Primzahl p, die n teilt und eine Zahl $a \in \mathbb{Z}_n$ zufällig gewählt. Die Wahrscheinlichkeit, dass a durch p teilbar ist, ist $\frac{1}{p}$. Die Wahrscheinlichkeit, dass a nicht durch p teilbar ist, ist also $1 - \frac{1}{p}$. Wegen $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ ist also die Wahrscheinlichkeit, dass a durch keine Primzahl p_i teilbar ist

$$\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

  wegen der Unabhängigkeit der Ereignisse. Man erwartet also

$$n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

  Zahlen in $\mathbb{Z}_n$, die durch keine Primteiler von n teilbar sind.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(n)$		1	2	2	4	2	6	4	6	4	10	4	12

- Beispiel:

$$\varphi(24) = 24 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{3} = 8$$

- Das Lemma von Euler-Fermat: Ist a teilerfremd zu n, dann gilt $a^{\varphi(n)} \equiv 1 \mod n$.

- Beispiel: Was sind die letzten drei Ziffern von $(((7^7)^6)^5)^4$?

$$(((7^7)^6)^5)^4 = 7^{7\cdot 6\cdot 5\cdot 4} = 7^{840}$$

Es gilt: $\varphi(1000) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$. Damit:

$$\begin{aligned} 7^{840} &= 7^{400} \cdot 7^{400} \cdot 7^{40} \equiv 7^{40} = 7^{32} \cdot 7^8 \\ &= ((((7^2)^2 \cdot 7)^2)^2)^2 = (((16807)^2)^2)^2 \\ &\equiv ((807)^2)^2 \equiv (249^2)^2 \equiv 1^2 \equiv 1 \qquad \mod 1000 \end{aligned}$$

Kryptologie: RSA-Verfahren (Rivest, Shamir, Adleman)

- Das RSA-Verfahren ist ein Public-Key-Kryptoverfahren. Grundlegendes Prinzip:

  1. Der Empfänger der Nachricht wählt zwei große Primzahlen $p, q (> 10^{500})$, berechnet $n := p \cdot q$ und

$$\varphi(n) = \varphi(p \cdot q) = p \cdot q \cdot \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = (p-1) \cdot (q-1)$$

  2. Der Empfänger wählt eine Zahl e mit $1 < e < n$ so, dass e teilerfremd zu $\varphi(n)$ ist. Er berechnet das multiplikativ Inverse modulo $\varphi(n)$ von e und nennt dieses d ($\Rightarrow e \cdot d \equiv 1 \mod \varphi(n)$).
  3. Der Empfänger teilt dem Absender öffentlich die Zahlen n und e mit. Die übrigen Zahlen, also $p, q, d, \varphi(n)$ behält er geheim.
  4. Der Absender sendet die Nachricht in Form einer Zahlenfolge von Zahlen aus $\mathbb{Z}_n$. Er verschlüsselt jede solche Zahl m durch die Verschlüsselungsvorschrift $m \mapsto m^e \mod n$.
  5. Ein Angreifer, der die verschlüsselte Information m^e kennt, müsste daraus m berechnen (er kennt n, e). Es ist kein effizientes Verfahren dafür bekannt.
  6. Der Empfänger berechnet $(m^e)^d \equiv m^{e\cdot d} \equiv m^{k\cdot\varphi(n)+1}$ für ein $k \in \mathbb{N}$. Damit

$$m^{k\cdot\varphi(n)+1} = (m^{\varphi(n)})^k \cdot m \equiv 1^k \cdot m = m \qquad \mod n$$

     (falls m zu n teilerfremd).

- Die Berechnung der Langzahlpotenzen mit großen Exponenten ist kein Problem: Die Berechnung geschieht mit dem Square-and-Multiply-Verfahren. Weil Modulo n gerechnet wird, können alle Zwischenergebnisse klein gehalten werden.

6 Klassifikation endlicher Körper

- $\mathbb{Z}_p$, p prim, ist ein Körper. Es wird sich zeigen, dass das nicht alle endlichen Körper sind.
- Jeder Körper (endlich oder unendlich) hat eine *Charakteristik*. Darunter versteht man die kleinste Zahl χ mit
$$\underbrace{1+1+\ldots+1}_{\chi \text{ mal}} = 0$$
oder 0, falls es keine solche Zahl gibt.
- Satz: Die Charakteristik eines Körpers ist 0 oder eine Primzahl.

  Beweis:

  – Wenn $1+1+\ldots+1=0$ gilt und $n = k \cdot l$ ist, dann gilt auch
  $$0 = \underbrace{1+1+\ldots+1}_{n \text{ mal}} = \underbrace{(1+1+\ldots+1)}_{k \text{ mal}} \cdot \underbrace{(1+1+\ldots+1)}_{l \text{ mal}}$$
  also $k = 1$ oder $l = 1$ wegen Nullteilerfreiheit.
- Beispiel: $\mathbb{Q}, \mathbb{R}, \mathbb{A}$ haben Charakteristik 0, $\mathbb{Z}_p$ hat Charakteristik p.
- In einem Körper der Charakteristik $p \neq 0$ bilden die Vielfachen der 1, also $1, 1+1, \ldots, 1+1+\ldots+1$ (p-mal), einen Teilkörper mit p Elementen (den *Primkörper*).
- Satz: Es sei $\mathbb{E}$ ein Körper und $\mathbb{K} \subseteq \mathbb{E}$ ein Teilkörper. Dann kann man $\mathbb{E}$ als Vektorraum über $\mathbb{K}$ auffassen.
- Die Klassifikation der endlichen Körper baut auf auf die Klassifikation der endlichdimensionalen Vektorräume: Zu gegebenem Körper $\mathbb{K}$ und $n \in \mathbb{N}$ gibt es bis auf Isomorphie genau einen $\mathbb{K}$-Vektorraum der Dimension n, nämlich $\mathbb{K}^n$, den Vektorraum aller n-Tupel über $\mathbb{K}$.

  Ist V ein weiterer n-dimensionaler Vektorraum über $\mathbb{K}$ existiert eine Basis aus n Vektoren, in $\mathbb{K}^n$ wähle Einheitsbasis. Lineare Abbildung zwischen Basen ist Isomorphismus zwischen $\mathbb{K}^n$ und V.
- Insbesondere gilt: Wenn $\mathbb{E}$ als Vektorraum über dem Teilkörper $\mathbb{K}$ endlich-dimensional ist, dann muss die additive Gruppe von $\mathbb{E}$ isomorph zu der von $\mathbb{K}^n$ sein. Wenn $\mathbb{E}$ endlichdimensional ist, ist $\mathbb{E}$ auch endlich dimensional.
- Jeder Körper $\mathbb{K}$ hat einen kleinsten Teilkörper, den Primkörper. Dieser enthält das Element 1 und alle seine Vielfachen. Bei einem Körper der Charakteristik 0 ist der Primkörper isomorph zu $\mathbb{Q}$. Hat $\mathbb{K}$ Charakteristik $p \neq 0$, dann ist p eine Primzahl und der Primkörper von $\mathbb{K}$ hat genau p Elemente.
- Sei $\mathbb{K}$ endlich, dann hat Primkörper $\mathbb{P}$ p Elemente mit p Primzahl. Somit:
$$\mathbb{K} \cong \mathbb{P}^n \qquad |\mathbb{K}| = p^n$$
Die Anzahl der Elemente eines endlichen Körpers ist stets eine Primzahl.

- $\mathbb{Z}_p$, p prim, ist ein endlicher Körper. Möglich sind aber auch Körper mit $4, 8, 9, 16, \ldots$ Elementen.
- Wir versuchen einen Körper mit genau 4 Elementen zu konstruieren:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$+$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

  Vorüberlegungen:
  - $\mathbb{Z}_4$ ist kein Körper, denn $\mathbb{Z}_4$ ist wegen $2 \cdot 2 = 0$ nicht nullteilerfrei.
  - Die additive Gruppe eines möglichen vierelementigen Körpers muss isomorph zu $\mathbb{Z}_2^2$ sein, denn $4 = 2^2$.

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

  Tatsächlich ergeben diese Multiplikation und diese Addition eine Körperstruktur auf der vierelementigen Menge $\{0, 1, \alpha, 1+\alpha\}$.
- Satz: Die Anzahl der Elemente eines endlichen Körpers ist eine Primzahlpotenz. Zu jeder Primzahlpotenz q gibt es bis auf Isomorphie genau einen Körper mit q Elementen. Dieser wird mit $GF(q)$ bezeichnet (Galois-Field).

  Achtung: GF(p) und $\mathbb{Z}_p$ sind dasselbe, wenn p eine Primzahl ist, aber sonst nicht!
- Linear rückgekoppelte Schieberegister (Skizze!)

  Darstellung durch das Zustandspolynom und das Rückkopplungspolynom

$$\begin{aligned} c(x) &= 1 \cdot 1 + 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3 = 1 + x + x^3 \\ a(x) &= 1 + x + x^4 \end{aligned}$$

  Diese Polynome leben in $\mathbb{Z}_2[x]$, dem Ring aller Polynome in den Variablen x mit Koeffizienten aus $\mathbb{Z}_2$. Wie entsteht Zustandspolynom für neuen Takt?

$$\begin{aligned} c_1(x) &= 1 + 0 \cdot x + 1 \cdot x^2 + 0 \cdot x^3 = 1 + x^2 \\ c_2(x) &= 0 + 1 \cdot x^2 + 1 \cdot x^3 = x + x^3 = x \cdot c_1(x) \\ c_3(x) &= 1 + x + x^2 = x \cdot c_2(x) - a(x) \end{aligned}$$

  Somit: Ist das Schieberegister im Zustand $c(x)$, dann ist der Zustand einen Takt später gleich

$$c'(x) := \begin{cases} x \cdot c(x) & c_{n-1} = 0 \\ x \cdot c(x) - a(x) & c_{n-1} \neq 0 \end{cases} = x \cdot c(x) \mod a(x)$$

  für $c(x) = c_0 + c_1 \cdot x + \ldots + c_{n-1} \cdot x^{n-1}$.

7 Modulare Arithmetik mit Polynomen

- Ein *Polynom* in der Variable X mit Koeffizienten aus einem Körper $\mathbb{K}$ ist ein Ausdruck der Form
$$a_0 + a_1 \cdot X + \ldots + a_n \cdot X^n$$
wobei $n \in \mathbb{N}$, $a_i \in \mathbb{K}$, $a_n \neq 0$. Ein Polynom in X ist also eine formale Linearkombination von Potenzen aus X.

- Die Menge aller solchen Polynome wird mit $\mathbb{K}[X]$ notiert. Die a_i nennt man die Koeffizienten des Polynoms. Außer beim *Nullpolynom*, dessen Koeffizienten alle Null sind, gibt es stets einen *Leitkoeffizienten* $a_n \neq 0$, der unter allen von Null verschiedenen Koeffizienten den höchsten Index hat. Man nennt diesen Index den *Grad* des Polynoms. Das Nullpolynom hat den Grad $-\infty$. Den Grad eines Polynoms bezeichnet man mit grad(p). Ist der Leitkoeffizient gleich Eins, nennt man das Polynom *normiert*.

- Die Polynome in $\mathbb{K}[X]$ kann man auf die naheliegende Weise addieren, subtrahieren und multiplizieren. Mit diesen Operationen ist $\mathbb{K}[X]$ ein Ring und zugleich ein $\mathbb{K}$-Vektorraum.

- Sind f, g Polynome in $\mathbb{K}[X]$ und ist $n :=$ grad(f) $\geq$ grad(g) $=: m \geq 0$ und a_n (b_m) der Leitkoeffitienten von f (g), dann ist
$$f - \frac{a_n}{b_m} \cdot X^{n-m} \cdot g$$
ein Polynom, dessen Grad kleiner ist als der von f. Wiederholt man dies, erhält man schließlich ein Polynom, dessen Grad kleiner ist als der von g.

- Satz: Zu je zwei Polynomen $f, g \in \mathbb{K}[X]$ mit $g \neq 0$ existieren eindeutig bestimmte Polynome $q, r \in \mathbb{K}[X]$ mit
$$f = q \cdot g + r$$
und grad(g) > grad(r).

- Wie bei den ganzen Zahlen schreibt man dann
$$f \operatorname{div} g = q \qquad f \mod g = r$$
Wenn $f \mod g = 0$ ist, nennt man g einen *Teiler* von f. Analog zum Rechnen modulo n kann ein „Rechnen modulo einen Polynom“ eingeführt werden.

- In der elektronischen Realisierung ist diese modulare Arithmetik mit $\mathbb{Z}_2$-Polynomen viel einfacher als das Rechnen mit reellen Zahlen.

- Der Euklidische Algorithmus funktioniert auch für Polynome.

```
Input: m,n (grad(m)>=grad(n))
while n != 0 do
(m,n) := (n, m \mod n)
Output: "ggT = " m
```

Beispiel:

$$f(x) = x^4 - 2x^2 - 1 \in \mathbb{Q}[x] \qquad g(x) = x^3 - 3x + 2 \in \mathbb{Q}[x]$$

m	n	m mod n
$x^4 - 2x^2 - 1$	$x^3 - 3x + 2$	$x^2 - 2x - 1$
$x^3 - 3x + 2$	$x^2 - 2x - 1$	$2x^2 - 2x + 2$
		$2x + 4$
$x^2 - 2x - 1$	$2x + 4$	$-4x - 1$
		7
$2x + 4$	7	0
7	0	0

- Es gilt dann aber auch, dass
  1. Zwei Polynome aus $\mathbb{K}[X]$ einen größten gemeinsamen Teiler haben, dieser ist bis auf skalare Vielfache eindeutig bestimmt.
  2. Zu je zwei Polynomem f und g mit einem Polynom d als ggT existieren zwei Polynome α und β mit $\alpha \cdot f + \beta \cdot g = d$.
- Satz: Zu je zwei teilerfremden Polynomen f und p aus $\mathbb{K}[X]$ existiert ein Polynom $\alpha \in \mathbb{K}[X]$ mit $\alpha \cdot f \equiv 1 \mod p$, also ein Polynom, das $\mod p$ multiplikativ invers zu f ist.
- Folgerung: Wenn p in $\mathbb{K}[X]$ irreduzibel ist, dann ist $\mathbb{K}[X]/p$ ein Körper.

8 Körper zwischen $\mathbb{Q}$ und $\mathbb{C}$

- Es sei $\mathbb{K}$ ein Körper und $\mathbb{E}$ ein Erweiterungskörper von $\mathbb{K}$. Weiter sei $a \in \mathbb{E}\backslash\mathbb{K}$. $\mathbb{K}(a)$ bezeichne den kleinsten Teilköprer von $\mathbb{E}$, der sowohl a als auch $\mathbb{K}$ ganz enthält. Es gibt zwei Möglichkeiten:

  1. Die Folge der Potenzen von a (also $1, a, a^2, \ldots$) ist linear unabhängig über $\mathbb{K}$. Dann ist $\mathbb{K}(a)$ unendlich dimensional über $\mathbb{K}$. Man nennt das Element a in diesem Fall *transzendent über* $\mathbb{K}$. $\mathbb{K}[a]$ ist isomorph zu $\mathbb{K}[X]$, also kein Körper.
  2. Die Folge $1, a^1, a^2, \ldots$ der Potenzen von a ist linear abhängig. Dann gibt es ein kleinstes $n \in \mathbb{N}$, für das die Folge $1, a, \ldots, a^n$ linear abhängig ist. Es gibt dann also Elemente $a_0, \ldots, a_n \in \mathbb{K}$ mit
  $$\sum_{i=0}^{n} a_i \cdot a^i = 0$$
  und $a_n \neq 0$, d.h. es gibt ein Polynom $m \in \mathbb{K}[x]$,
  $$m(x) = \sum_{i=0}^{n} a_i \cdot x^i \qquad (a_n \neq 0)$$
  mit $m(a) = 0$. In diesem Fall ist a also eine Nullstelle eines nichttrivialen Polynoms mit Koeffizienten aus $\mathbb{K}$. Man nennt solche Elemente *algebraisch über* $\mathbb{K}$.

- Beispiele:

  1. $\mathbb{K} = \mathbb{Q}, a = \sqrt{2}$

     Die Folge $1, \sqrt{2}, 2, 2 \cdot \sqrt{2}, \ldots$ ist linear abhängig, denn
     $$-2 \cdot 1 + 0 \cdot \sqrt{2} + 1 \cdot 2 = 0$$
     Also Minimalpolynom von $\sqrt{2}$:
     $$m(x) = x^2 - 2$$
  2. $\mathbb{K} = \mathbb{Q}, a = e$

     Die Folge $1, e, e^2, \ldots$ ist linear unabhängig über $\mathbb{Q}$.

- Satz: Es sei $\mathbb{K}$ ein Teilkörper des Körpers $\mathbb{E}$ und $a \in \mathbb{E}$ algebraisch über $\mathbb{K}$. Dann gibt es genau ein normiertes Polynom $m_a \in \mathbb{K}[x]$ mit folgenden Eigenschaften:

  1. a ist eine Nullstelle von $m_a(x)$, d.h. es gilt $m_a(a) = 0$.
  2. Jedes Polynom in $\mathbb{K}[x]$, welches a als Nullstelle hat, ist durch $m_a(x)$ teilbar.
  3. $m_a(x)$ ist irreduzibel über $\mathbb{K}$.

  Beweis:

  1. Klar.

2. Teilbarkeit: Euklidischer Algorithmus (ggT hat a als Nullstelle. Widerspruch zur Minimalität!)
3. Man wählt als Minimalpolynom das normierte Polynom kleinsten Grades, das a als Nullstelle hat. Wäre $m_a(x)$ reduzibel, also

$$m_a(x) = f(x) \cdot g(x)$$

mit grad $f <$ grad m_a, grad $g <$ grad m_a, dann wäre

$$0 = m_a(a) = f(a) \cdot g(a) \Rightarrow f(a) = 0 \vee g(a) = 0$$

m_a wäre also nicht Polynom kleinsten Grades.

- Seien $\mathbb{K}, \mathbb{E}$ Körper mit $\mathbb{K} \subseteq \mathbb{E}$. Dann heißt $\mathbb{K}$ *Teilkörper* von $\mathbb{E}$, $\mathbb{E}$ *Erweiterungskörper* von $\mathbb{K}$. Wir fassen $\mathbb{E}$ als Vektorraum über $\mathbb{K}$ auf. Dann definiert man den *Grad der Körpererweiterung* durch

$$(\mathbb{E} : \mathbb{K}) := \dim_{\mathbb{K}} \mathbb{E}$$

- Satz: Sei $\mathbb{F}$ ein Erweiterungskörper von $\mathbb{K}$ und $\mathbb{E}$ ein Erweiterungskörper von $\mathbb{F}$. Dann gilt:

$$(\mathbb{E} : \mathbb{K}) = (\mathbb{E} : \mathbb{F}) \cdot (\mathbb{F} : \mathbb{K})$$

Beweis:

– Seien ohne Einschränkung $(\mathbb{E} : \mathbb{K}), (\mathbb{E} : \mathbb{F}), (\mathbb{F} : \mathbb{K}) < \infty$. Sei $B := \{b_1, \ldots, b_m\}$ Basis von $\mathbb{E}$ (als $\mathbb{F}$-Vektorraum), $C := \{c_1, \ldots, c_n\}$ Basis von $\mathbb{F}$ als $\mathbb{K}$-Vektorraum. Setze

$$D := \{b_i \cdot c_j | i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$$

Dann $|D| = m \cdot n$.

1. Lineare Unabhängigkeit von D:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} \cdot b_i \cdot c_j = 0$$

mit $\alpha_{ij} \in \mathbb{K}$. Dann:

$$\begin{aligned} \sum_{i=1}^{m} b_i \cdot \underbrace{\left(\sum_{j=1}^{n} \alpha_{ij} \cdot c_j \right)}_{\in \mathbb{F}} &= 0 \\ \Rightarrow \forall i \in \{1, \ldots, m\} : \sum_{j=1}^{n} \alpha_{ij} \cdot c_j &= 0 \\ \Rightarrow \forall i \in \{1, \ldots, m\}, \forall j \in \{1, \ldots, n\} : \alpha_{ij} &= 0 \end{aligned}$$

2. D ist Erzeugendensystem: Sei $e \in \mathbb{E}$ beliebig. Weil B Basis von $\mathbb{E}$ über $\mathbb{F}$ existieren $f_j \in \mathbb{F}$ mit

$$e = \sum_{j=1}^{m} f_j \cdot b_j$$

Da C Basis von $\mathbb{F}$ über $\mathbb{K}$ existieren $\alpha_{ij} \in \mathbb{K}$ mit

$$e = \sum_{j=1}^{m} b_j \cdot \left(\sum_{i=1}^{n} \alpha_{ij} \cdot c_i \right)$$

- Sei $\mathbb{E}$ Erweiterungskörper von $\mathbb{K}$, $a \in \mathbb{E}$. Bezeichne $\mathbb{K}[a]$ den von $\mathbb{K} \cup \{a\}$ erzeugten Ring. Dann

$$\mathbb{K}[a] = \{k_0 \cdot a^0 + k_1 \cdot a^1 + \ldots + k_n \cdot a^n | n \in \mathbb{N}, k_i \in \mathbb{K}\}$$

- Die Auswerteabbildung φ_a ist gegeben durch

$$\varphi_a : \mathbb{K}[x] \to \mathbb{K}[a], p(X) \mapsto p(a)$$

und ist ein surjektiver Ringhomomorphismus.

- Beispiel: $\mathbb{K} = \mathbb{Q}, \mathbb{E} = \mathbb{R}, a := \sqrt[3]{2}$,

$$\mathbb{Q}[\sqrt[3]{2}] = \{q_0 + q1 \cdot \sqrt[3]{2} + q_2 \cdot (\sqrt[3]{2})^2 | q_0, q_1, q_2 \in \mathbb{Q}\}$$

also $(\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}) = 3$, Basis $B = \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.

9 Unmöglichkeit geometrischer Konstruktionen

- Frage: Ist es möglich, die Zahl $\sqrt[3]{2}$ aus rationalen Zahlen und Quadratwurzeln mit Hilfe der arithmetischen Operationen darzustellen?

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2})(\sqrt{3}) \leq \ldots \leq \mathbb{C}$$

- Lösung: $\mathbb{Q} \leq \mathbb{Q}(\sqrt{a}) \leq \mathbb{E} \ni a$, damit

$$(\mathbb{E} : \mathbb{Q}) = (\mathbb{E} : \mathbb{Q}(a)) \cdot (\mathbb{Q}(a) : \mathbb{Q})$$

  nach Gradmultiplikationssatz. Wir zeigen noch:

$$(\mathbb{Q}(a) : \mathbb{Q}) = \operatorname{grad} m_a$$

  für $m_a \in \mathbb{Q}[x]$ Minimalpolynom von a, falls a algebraisch über $\mathbb{Q}$. $\mathbb{E}$ hat die Dimension 2^n mit $n \in \mathbb{N}$ über $\mathbb{Q}$, also auch $(\mathbb{Q}(a) : \mathbb{Q})$. Wegen $\operatorname{grad}(x^3 - 2) = 3$ für $a = \sqrt[3]{2}$ kann $\sqrt[3]{2}$ nicht wie gefordert dargestellt werden.

- Zutaten:
  - Ist $\mathbb{K}$ ein Teilkörper des Körpers $\mathbb{E}$, dann bezeichnet $(\mathbb{E} : \mathbb{K})$ den Grad der Körpererweiterung, d.h. die Dimension von $\mathbb{E}$ als $\mathbb{K}$-Vektorraum.
  - Gradmultiplikationssatz: Wenn $\mathbb{K} \leq \mathbb{F} \leq \mathbb{E}$ gilt

$$(\mathbb{E} : \mathbb{K}) = (\mathbb{E} : \mathbb{F}) \cdot (\mathbb{F} : \mathbb{K})$$

  - Ist $\mathbb{K} \leq \mathbb{E}$ und $a \in \mathbb{E}$ algebraisch über $\mathbb{K}$, dann ist $(\mathbb{K}(a) : \mathbb{K}) = \operatorname{grad} m_a$ mit a als Minimalpolynom $\in \mathbb{K}[x]$.
  - Ist $(\mathbb{E} : \mathbb{K})$ endlich, dann ist jedes Element von $\mathbb{E}$ algebraisch über $\mathbb{K}$. Insbesondere gilt: Entsteht $\mathbb{E}$ aus $\mathbb{K}$ durch Adjunktion (Hinzufügen) endlich vieler algebraischer Elemente, dann ist jedes Element von $\mathbb{E}$ algebraisch über $\mathbb{K}$.

    Wenn dabei jede einzelne Adjunktion zu einer Erweiterung vom Grad ≤ 2 führt, dann ist der Grad von $\mathbb{E}$ eine Potenz von 2. Jedes Minimalpolynom eines Elements aus $\mathbb{E}$ muss dann als Grad eine Potenz von 2 haben. Ein Element, dessen Minimalpolynom über $\mathbb{K}$ nicht Zweierpotenz-Grad hat, kann nicht zu $\mathbb{E}$ gehören!

Konstruktionen mit Zirkel und Lineal

- Es gibt zahlreiche unlösbare geometrische Konstruktionsaufgaben mit Zirkel und Lineal. Bekannt sind insbesondere:
  - Quadratur des Kreises
  - Dreiteilung des Winkels
  - Verdopplung des Würfels
- Gegeben sei eine Menge P von Punkten der Zeichenebene. Wir nennen einen Punkt *in einem Schritt aus P konstruierbar*, wenn er (nicht degenerierter) Schnittpunkt

1. zweier Geraden, oder
2. einer Geraden und eines Kreises, oder
3. zweier Kreise

ist, wobei diese Geraden jeweils durch zwei Punkte von P verlaufen und die Kreise jeweils einen Punkt von P als Mittelpunkt und als Radius den Abstand zweier Punkte aus P haben.

- Ein Punkt heißt *aus P konstruierbar*, wenn es eine Folge $p_1, \ldots, p_n$ von Punkten gibt mit $p = p_n$, für die gilt, dass p_i in einem Schritt aus $P \cup \{p_1, \ldots, p_{i-1}\}$ konstruierbar ist ($i = 1, \ldots, n$).
- Ein Punkt der Ebene heißt konstruierbar, wenn er aus der Menge $\{(0,1),(0,0)\}$ konstruierbar ist. Eine reelle Zahl heißt *konstruierbar*, wenn sie Koordinate eines konstruierbaren Punktes ist.
- Die Menge der konstruierbaren Punkte liegt dicht in der Zeichenebene. Jeder Punkt der Zeichenebene ist also Grenzwert einer konvergenten Folge konstruierbarer Punkte.
- Bemerkung: Jeder Punkt der Zeichenebene, dessen Koordinate konstruierbar ist, ist konstruierbar.
- Welche algebraischen Konstruktionen sind „konstruierbar“, d.h. unter welchen Operationen ist die Menge $\mathbb{K}$ aller konstruierbaren Zahlen abgeschlossen?
  - Addition, Subtraktion
  - Multiplikation, Division (Strahlensatz)
  - Wurzelziehen aus nichtnegativen Zahlen

  Also ist die Menge $\mathbb{K}$ aller konstruierbaren Zahlen ein Körper.
- Satz: Der Körper $\mathbb{K}$ aller konstruierbaren Zahlen ist der kleinste Teilkörper von $\mathbb{R}$, der gegen das Ziehen von Quadratwurzekn aus positiven Zahlen abgeschlossen ist.

  Beweis:
  - Bei jeder der drei Grundkonstruktionen lassen sich die Koordinaten der neu konstruierten Punkte als Lösungen höchstens quadratischer Gleichungen darstellen. Die neu gewonnen konstruierbaren Zahlen lassen sich deshalb mittels Addition, Subtraktion, Multiplikation, Division, Quadratwurzelziehen aus den alten gewinnen.
- Um zu zeigen, dass eine geometrische Aufgabe nicht mit Zirkel und Lineal lösbar ist, genügt es also zu zeigen, dass ihre Lösung eine nicht konstruierbare Zahl als Koordinate erfordert, d.h. eine Zahl, die nicht aus $\{0,1\}$ durch endlich viele Anwendungen der Körperoperationen und des Quadratwurzelziehens erhalten werden kann.
- Um zu zeigen, dass eine Zahl nicht konstruierbar ist, verwendet man meist die folgende notwendige Bedingung für Konstruierbarkeit:

  Satz: Der Grad des Minimalpolynoms einer beliebigen konstruierbaren Zahl ist eine Potenz von 2.
- Wenn also $r \in \mathbb{R}$ ein Minimalpolynom hat, dessen Grad keine Potenz von 2 ist (oder wenn r transzendent ist), dann ist r nicht konstruierbar.
- Man hat daraus:
  - Die Quadatur des Kreises mit Zirkel und Lineal ist nicht möglich, denn π ist transzendent über $\mathbb{Q}$ (Lindemann, 1882).
  - Die Verdopplung des Würfels mit Zirkel und Lineal ist unmöglich, denn ein Würfel vom doppelten Volumen des Einheitswürfels hat Seitenlänge $\sqrt[3]{2}$ und das Minimalpolynom von $\sqrt[3]{2}$ ist $x^3 - 2$.

– Die Dreiteilung des Winkels: Wir zeigen, dass es nicht möglich ist, einen Winkel von 20° mit Zirkel und Lineal aus $\{(0,0),(1,0)\}$ zu konstruieren. Könnten wir den Winkel konstruieren, dann auch ein Dreieck mit den Winkeln 20°,70°,90° und Hypothenusenlänge 2.

$$\beta = 2 \cdot \cos\left(\frac{\pi}{9}\right) \qquad \gamma := \cos\left(\frac{\gamma}{9}\right)$$

γ wäre dann konstruierbar. Es folgt:

$$\begin{aligned}
\cos(3\varphi) &= 4\cos^3(\varphi) - 3\cos\varphi \\
\Rightarrow \cos\left(\frac{\pi}{3}\right) &= 4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right) \\
\frac{1}{2} &= 4\gamma^3 - 3\gamma \\
\Rightarrow \frac{1}{2} &= \frac{1}{2}\beta^3 - \frac{3}{2}\beta \\
\Rightarrow \beta^3 - 3\beta - 1 &= 0
\end{aligned}$$

$x^3 - x - 1$ ist also das Minimalpolynom von β.

10
Anfänge der Galois-Theorie

Auflösung von Polynomialgleichungen durch Radikale

- Einfachster Fall: Gibt es eine p-q-Formel zur Bestimmung der Nullstellen beliebiger Polynome?

  Antwort: Es gibt Formeln zur Bestimmung der Nullstellen von Polynomen vom Grad ≤ 4, aber nicht für Grad ≥ 5 (N.H. Abel, 1824). Dabei „Formel“: Lösungsterm, der aus den Koeffizienten des Polynoms, den Körperoperationssymbolen, Konstanten und Radikalen aufgebaut ist (Radikal:n-te Wurzel, $n \in \mathbb{N}$).

- Wie bei den unlösbaren Konstruktionsaufgaben mit Zirkel und Lineal gilt auch hier: Die Unlösbarkeit der Aufgabe ist nicht darin begründet, dass man keinen Lösungsweg kennt, sondern beweisbar ist, dass es keine Lösung gibt.

- Die Beweisidee ist ähnlich wie bei den geometrischen Problemen. Ergibt sich eine Zahl z aus vorgegebenen Elementen eines Körpers $\mathbb{K}$ durch eine „Formel mit Radikalen“, dann gibt es eine endliche Folge von Körpererweiterungen

  $$\mathbb{K} = \mathbb{K}_0 \leq \mathbb{K}_1 \leq \ldots \leq \mathbb{K}_n$$

  mit $z \in \mathbb{K}_n$, wobei $\mathbb{K}_{i+1}$ durch Adjunktion einer m-ten Wurzel eines Elementes von $\mathbb{K}_i$ entsteht.

  (Zum Vergleich: Eine reelle Zahl z heißt (aus $\mathbb{Q}$) konstruierbar, wenn es eine Folge von Körpererweiterungen

  $$\mathbb{Q} =: \mathbb{K}_0 \leq \mathbb{K}_1 \leq \ldots \leq \mathbb{K}_n$$

  gibt, wobei $\mathbb{K}_{i+1}$ aus $\mathbb{K}_i$ durch Adjunktion einer Quadratwurzel eines Elements aus $\mathbb{K}_i$ entsteht. Notwendig dafür ist, dass das Minimalpolynom von z in $\mathbb{K}[x]$ existiert und als Grad eine Potenz von 2 hat.)

- Eine ähnliche notwendige Bedingung für die Auflösbarkeit einer Polynomgleichung durch Radikale liefert die Galois-Theorie. Jedem Polynom wird dabei eine Permutationsgruppe zugeordnet - die *Galois-Gruppe* des Polynoms.

- Betrachte einen Körper $\mathbb{K}$, einen Erweiterungskörper $\mathbb{E}$ von $\mathbb{K}$ und die Gruppe Aut $(\mathbb{E} : \mathbb{K})$ aller Körperautomorphismen von $\mathbb{E}$, die $\mathbb{K}$ punktweise festlassen. Wir bilden den formalen Kontext $(\mathbb{E}$,Aut $(\mathbb{E} : \mathbb{K}), I)$ mit $e \in \sigma :\Leftrightarrow e \in \mathbb{E}, \sigma \in$ Aut $(\mathbb{E} : \mathbb{K}, \sigma(e) = e$. Die formalen Begriffe dieses Kontextes sind von der Form $(\mathbb{F}, \sigma)$, wobei $\mathbb{F}$ ein Zwischenkörper $\mathbb{K} \leq \mathbb{F} \leq \mathbb{E}$ und σ eine Untergruppe von Aut $(\mathbb{E} : \mathbb{K})$.

  Sind a, b Fixpunkte eines Körperautomorphismus σ, dann auch $a \circ b$ mit $\circ \in \{+, -, \cdot, /\}$ (Division nur für $b \neq 0$),

  $$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$$

  d.h. die Menge aller Fixpunkte von σ ist ein (Teil-)Körper.

- Analog: Für jedes $e \in \mathbb{E}$ bilden die Automorphismen, die e festlassen, eine Gruppe.

- Auf diese Weise ergibt sich eine Beziehung zwischen (einigen) Zwischenkörpern $\mathbb{K} \leq \mathbb{F} \leq \mathbb{E}$ und (einigen) Untergruppen $U \leq \text{Aut}\,(\mathbb{E} : \mathbb{K})$. Unter Zusatz-Voraussetzungen („galoissche Körpererweiterungen“) kommen dabei alle Zwischenkörper und Untergruppen vor. (galois = normal + separabel)

Normalteiler einer Gruppe

- Sei U eine Untergruppe einer Gruppe G. Die Links-Nebenklasse von U durch das Element $g \in G$ ist die Menge
$$g \circ U := \{g \circ u | u \in U\}$$
Eine Untergruppe U von G heißt ein *Normalteiler* von G $:\Leftrightarrow \forall g \in G : g \circ U = U \circ g$.

- In einer abelschen Gruppe ist jede Gruppe normal. Gleichbedeutend zu $g \circ U = U \circ g$ ist
$$g \circ U \circ g^{-1} = U$$

- Normalteiler sind deshalb besonders wichtige Untergruppen, weil sie in enger Beziehung zu den Gruppenhomomorphismen stehen: Normalteiler sind genau die Kerne von Homomorphismen.

- Satz: Ist $\varphi : G \to H$ ein Gruppenhomomorphismus von der Gruppe G in die Gruppe H und ist e das neutrale Element von H, dann ist
$$\varphi^{-1}(e) = \{g \in G : \varphi(g) = e\}$$
ein Normalteiler von G. Umgekehrt gibt es zu jedem Normalteiler N von G eine Gruppe H, einen Homomorphismus $\varphi : G \to H$ mit $\varphi^{-1}(e) = N$.

  Beweisidee:

  – Zu zeigen ist, dass $\varphi^{-1}(e)$ eine Untergruppe, sogar ein Normalteiler, ist. Für die Rückrichtung wird gezeigt, dass die Menge aller Nebenklassen $g \circ N$ eines Normalteilers eine Gruppe bildet und die Abbildung $g \mapsto g \circ N$ für $g \in G$ ein Homomorphismus mit der behaupteten Eigenschaft ist.

- Einschub aus Skript: Man kann die fundamentalen Operationen auf Teilmengen fortsetzen, indem man für $A, B \subseteq G$ definiert:
$$A \circ B := \{a \circ b | a \in A, b \in B\} \qquad A^{-1} := \{a^{-1} | a \in A\}$$
Man spricht auch von den *Komplexoperationen*. Sind dabei $A := g \circ N$, $B := h \circ N$ Nebenklasse desselben Normalteilers, dann sind auch die Ergebnisse Nebenklassen dieses Normalteilers, denn man hat
$$(g \circ N) \circ (h \circ N) = (g \circ h) \circ N \qquad (g \circ N)^{-1} = g^{-1} \circ N$$
Satz: Die Menge aller Nebenklasse eines Normalteilers N einer Gruppe G ist mit den Komplexoperationen selbst eine Gruppe.

  Das neutrale Element ist dabei N, die Inversabbildung ist $g \circ N \mapsto g^{-1} \circ N$. Man nennt diese Gruppe die *Faktorgruppe* der Grupe G nach dem Normalteiler N.

- Beispiel:

  1. $G := (\mathbb{Z}, +), N := 5\mathbb{Z}$
  Die Nebenklassen von N sind $0 + N, 1 + N, 2 + N, 3 + N, 4 + N$. Diese Nebenklassen bilden bzgl. der Komplexaddition eine Gruppe. Beispiel:
$$\begin{aligned}(1 + N) + (3 + N) &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} + \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\ &= \{\ldots, -6, -1, 4, 9, \ldots\} = 4 + N\end{aligned}$$
  Diese Gruppe ist isomorph zur Gruppe $(\mathbb{Z}_5, +)$. Deshalb wird oft statt $\mathbb{Z}_5$ auch $\mathbb{Z}_{/5\mathbb{Z}}$ geschrieben. Die Abbildung $a \mapsto a + N$ ist ein surjektiver Gruppenhomomorphismus mit dem Kern N.

- Beispiele nichtkommutativer Gruppen sind die symmetrischen Gruppen S_n ($n \geq 3$). Die symmetrische Gruppe S_n besteht aus allen Permuationen der Menge $\{0, \ldots, n-1\}$.
- Permutationen können auf unterschiedliche Weise geschrieben werden, z.B. durch Tafeln, Bilder, Matrizen, Zyklenschreibweise:

x	0	1	2	3	4
$\varphi(x)$	2	1	4	0	3

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad (0243)(1)$$

  Das Produkt (die Hintereinanderausführung) von Permutationen ist im Allgemeinen nicht kommutativ. Beispiel:

$$\varphi_1 = (012) \qquad \varphi_2 = (01)(2) \qquad \varphi_1 \circ \varphi_2 = (02) \qquad \varphi_2 \circ \varphi_1 = (12)$$

  Eine Sonderrolle spielen die *Transpositionen*, d.h. die Menge der Permutationen der Form (ab) mit $a \neq b$. Es gilt:

  1. Jede Permutation einer endlichen Menge kann als Produkt von Transpositionen geschrieben werden. (Transpostionen erzeugen die symmetrische Gruppe S_n, $n \in \mathbb{N}$).
  2. Jede Permutation einer endlichen Menge kann entweder als ein Produkt gerader vieler Transpositionen dargestellt werden oder als ein Produkt ungerade vieler Transpositionen. Man spricht von *geraden* und *ungeraden* Permutationen.

- Beispiel: $\varphi = (0326)(14)(5)$,
$$(0326) = (23)(26)(06)$$
  also ist φ eine gerade Permutation, $\varphi = (23)(26)(06)(14)$.
- Eine Permutation ist genau dann gerade, wenn in ihrer Darstellung als Produkt elementfremder Zyklen die Anzahl der Zyklen gerader Länge gerade ist.
- Jeweils die Hälfte aller Elemenge von S_n ist gerade bzw. ungerade ($n \geq 2$).
- Die Menge der geraden Permutationen der Menge $\{0, \ldots, n-1\}$ bildet eine Untergruppe A_n der symmetrischen Gruppe S_n. Sie wird die *alternierende Gruppe* auf n Elementen genannt und ist Normalteiler von S_n. Für $n \geq 4$ ist A_n nichtkommutativ.
- Beispiel: Wie sehen die zu $\varrho := (0326)(14)$ konjugierten Permutationen aus, d.h. die Permutationen der Form
$$\gamma \circ \varrho \circ \gamma^{-1}$$
  für $\gamma \in S_7$? Wir wenden $\gamma \circ \varrho \circ \gamma^{-1}$ auf das Element $\gamma(a)$, $a \in \{0, \ldots, 6\}$ an:
$$\gamma \circ \varrho \circ \gamma^{-1}(\gamma(a)) = \gamma \circ \varrho(\gamma^{-1}(\gamma(a))) = \gamma(\varrho(a))$$
  Die Zyklendarstellung von $\gamma \circ \varrho \circ \gamma^{-1}$ erhält man also, indem man in der Zyklendarstellung von ϱ jedes Elemnt a durch $\gamma(a)$ ersetzt.

  Beispiel:
$$\gamma = (02465) \Rightarrow \gamma \circ \varrho \circ \gamma^{-1} = (2345)(16)$$

Normalteiler und Auflösbarkeit von Gruppen

- Zusammenhang zur Galois-Theorie: Jedem Polynom $f \in \mathbb{K}[x]$ kann eine „Galoisgruppe von f“ zugeordnet werden. Es handelt sich um die Automorphismengruppe des Zerfällungskörpers von f. Man kann dann zeigen, dass die Polynomgleichung $f(x) = 0$ nur dann durch Radikale lösbar ist, wenn die Galoisgruppe von f auflösbar ist. Im fall des allgemeinen Polynoms n-ten Grades ist die Galois-Gruppe die symmetrische Gruppe S_n.

- Eine Gruppe G heißt auflösbar, wenn es eine absteigende Kette von Untergruppen

$$G =: G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

  gibt, derart, dass für alle $i < n$ die Gruppe G_{i+1} ein Normalteiler der Gruppe G_i ist und die Faktorgruppe G_i/G_{i+1} abelsch ist.

- Um etwas über die Auflösbarkeit der allgemeinen Polynomgleichung n-ter Ordnung zu erfahren, müssen wir also herausfinden, ob die symmetrischen Gruppen S_n auflösbar sind.

- Die Gruppen S_1, S_2 sind abelsch und damit auflösbar, $|S_1| = |\{\mathrm{id}\}| = 1, |S_2| = |\{(01), \mathrm{id}\}| = 2$.

- Die Gruppe S_3 hat sechs Elemente. Sie ist nicht kommutativ.

- Hilfssatz: Eine Untergruppe U einer endlichen Gruppe G, die halb soviele Elemente wie Gbesitzt, ist ein Normalteiler von G.

- Die Gruppe S_3 hat die Gruppe A_3 aller geraden Permutationen als Normalteiler. Wegen $A_3 \cong \mathbb{Z}_3$ ist $S_3 \supset A_3 \supset \{\mathrm{id}\}$, also S_3 auflösbar, denn

$$S_3/A_3 \cong \mathbb{Z}_2 \qquad A_3/\,\mathrm{id} \cong A_3 \cong \mathbb{Z}_3$$

- Die symmetrische Gruppe S_4 aller Permutationen der Menge $\{0, \ldots, 3\}$ hat 24 Elemente, davon sind 12 gerade und 12 ungerade. Die geraden Permutationen bilden die (nichtabelsche Gruppe) A_4. Darin liegt die Untergruppe V_4 aller Permutationen, die das Produkt von genau zwei elementfremden Transpositionen sind, zusammen mit der Identität.

$$V_4 = \{\mathrm{id}, (01)(23), (02)(13), (03)(12)\}$$

  Dies ist eine Untergruppe. Beispiel:

$$(01)(23) \circ (02)(13) = (03)(12)$$

  V_4 ist isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$ und ist deshalb abelsch.

- Behauptung: V_4 ist ein Normalteiler von A_4.

  Beweis: Ist $(ab)(cd) \in V_4$ und $\varphi \in A_4$ beliebig, dann ist

$$\varphi \circ (ab)(cd) = (\varphi(a)\varphi(b))(\varphi(c)\varphi(d)) \in V_4$$

- Beispiel: $\varphi \circ (01)(23) \circ \varphi^{-1}$ für $\varphi = (3210)$ ergibt

$$(3210) \circ (01)(23) \circ (0123) = (03)(12) = (30)(12) = (\varphi(0)\varphi(1))(\varphi(2)\varphi(3))$$

- Also $S_4 \supset A_4 \supset V_4 \supset \{\mathrm{id}\}$ mit

$$|S_4/A_4| = 2 \qquad |A_4/V_4| = 3 \qquad |V_4/\,\mathrm{id}\,| = 4$$

  (alle Faktorgruppen abelsch), also S_4 auflösbar.

- Hilfssatz: Es sei G eine Permutationsgruppe auf einer mindestens fünfelementigen Menge, die alle Dreierzyklen enthält. N sei ein Normalteiler von G mit abelscher Faktorgruppe. Dann enthält auch N alle Dreierzyklen.

  Beweis:

– Es sei φ der kanonische Homomorphismus von G auf G/N, also die Abbildung, die $g \in G$ auf die Nebenklasse $g \circ N$ abbildet. Beachte: Ein Element $g \in G$ gehört genau dann zu N, wenn $\varphi(g) = N$ ist.

– Nun sei (abc) ein beliebiger Dreierzyklus und e, f seien Elemente der Grundmenge mit $|\{a, b, c, e, f\}| = 5$. Man setze

$$x := \begin{pmatrix} e & b & a \end{pmatrix} \qquad y := \begin{pmatrix} a & f & c \end{pmatrix}$$

Das Bild des Elements $x^{-1}y^{-1}xy$ unter φ ist $\tilde{x}^{-1}\tilde{y}^{-1}\tilde{x}\tilde{y}$ wobei $\tilde{x} := \varphi(x), \tilde{y} := \varphi(y)$. Weil die Faktorgruppe nach Voraussetzung abelsch ist, ist das Bild gleich dem neutralen Element. Wir erhalten also, dass

$$\varphi((eba)^{-1}(afc)^{-1}(eba)(afc)) = \varphi((abc)(e)(f))$$

das neutrale Element der Faktorgruppe ist, also N, d.h. $(abc)(e)(f) \in N$.

- Satz: Für $n \geq 5$ ist die symmetrische Gruppe S_n nicht auflösbar.
- Korollar: Es gibt keine Formel zur Bestimmung der Nullstellen des allgemeinen Polynoms vom Grad ≥ 5, die aus Radikalausdrücken aufgebaut ist.

11 Zusatz-Vorlesungen

11.1 Primzahlen

- Wieviele Primzahlen gibt es? Unendlich viele! Es gibt dafür mehrere Beweise, darunter einer von L. Euler:

  Betrachte die Menge $A_m := \{1, \ldots, 2^m\}$ für $m \in \mathbb{N}$. Es sei q die größte Primzahl, die eine dieser Zahlen teilt. Dann ist jede Zahl in A_m Produkt von Potenzen von Primzahlen $\leq q$ und jeder Exponent ist $\leq m$. Betrachte nun die Summen

  $$\sum_{i=0}^{m} \frac{1}{p^i}$$

  für $p \leq q$, p Primzahl. Es gilt:

  $$\sum_{i=0}^{m} \frac{1}{p^i} < \frac{1}{1-\frac{1}{p}} = \frac{p}{p-1}$$

  Bildet man das Produkt

  $$\prod_{p \leq q, p \text{ prim}} \sum_{i=0}^{m} \frac{1}{p^i}$$

  so besitzt dieses die folgenden Eigenschaften:

  1. Das Produkt ist kleiner als
  $$\prod_{p \leq q, p \text{ prim}} \frac{p}{p-1}$$
  2. Das ausmultiplizierte Produkt ist eine Summe von Kehrwerten der Form
  $$\frac{1}{p_1^{i_1} \cdot p_2^{i_2} \cdots}$$
  mit $p_j \leq q$ Primzahlen, $i_j \leq m$. Dabei kommt jeder Term der Form $\frac{1}{n}$, $n \in A_m$ vor. Das Produkt ist also größer gleich $\sum_{n \in A_m} \frac{1}{n}$.

  Man hat also:

  $$\prod_{p \leq q, p \text{ prim}} \frac{p}{p-1} \geq \prod_{p \leq q, p \text{ prim}} \sum_{i=0}^{m} \frac{1}{p^i} \geq \sum_{n=1}^{2^m} \frac{1}{n} \geq \frac{m}{2} + 1$$

  Für $m \to \infty$ wird die rechte Seite beliebig groß. Die linke Seite kann also nicht beschränkt sein, es kann deshalb keine größte Primzahl q geben.

- Satz: $\sum_{p \in \mathbb{P}} \frac{1}{p}$ divergiert. ($\mathbb{P}$ bezeichnet die Menge aller Primzahlen.) Daraus folgt erneut, dass es unendlich viele Primzahlen gibt. (Die Umkehrung ist keine Konsequenz)

- *Primzahlzwillinge* sind Paare von Primzahlen der Form (p,p+2) wie z.B. (3,5),(11,13),(59,61). Brun hat gezeigt, dass die Summe der Kehrwerte von Primzahlen in Zwillingen konvergiert. Es ist aber unbekannt, ob es unendlich viele Primzahlzwillinge gibt.

- $\mathbb{P}$ hat beliebig große Lücken: Es sei p_k die k-te Primzahl und $n := \prod_{p\in\mathbb{P}, p\leq p_k} p$ das Produkt der ersten k Primzahlen. Die Zahlen $n+2, \ldots, n+p_{k+1}-1$ sind sämtliche nicht prim.
- $\mathbb{P}$ hat keine allzugroßen Lücken (Bertrands Vermutung, bewiesen von Tschebysheff): Zwischen n und 2n liegt stets eine Primzahl, falls $n > 0$. Genauer: Zu jeder natürlichen Zahl $n > 0$ existiert eine Primzahl p mit $n < p \leq 2n$.

  „Beweis“ für $n < 4000$:

  $$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 2001$$

- Unbewiesen ist die folgende Vermutung von Legendre: Zu jeder natürlichen Zahl $n > 0$ existiert eine Primzahl p mit $n^2 < p \leq (n+1)^2$.
- Eine *arithmetische Progression* ist eine Folge der Form $a, a+d, \ldots, a+h\cdot d, \ldots$ mit $a, d \in \mathbb{N}$, $d > 0$. Bricht die Folge nach h ab, so spricht man von einer endlichen arithmetischen Progression der Länge h. Wenn $ggT(a,d) \neq 1$ ist, kann höchstens a prim sein.
- Mit

  $$\Pi(x) := |\{p \in \mathbb{P} \,|\, p \leq x\}|$$

  wird die Anzahl der Primzahlen $\leq x$ notiert. Der *Primzahlsatz* sagt:

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

  Intuitiv: Von den ersten n natürlichen Zahlen ist jede ln n-te eine Primzahl. Besser:

  $$\Pi(x) \sim Li(x) := \int_2^x \frac{dt}{\ln t}$$

  (Integrallogarithmus)
- Dirichletscher Primzahlsatz: Sind a und d teilerfremde natürliche Zahlen, $d > 0$, dann enthält die unendliche arithmetische Progression $a, a+d, \ldots, a+h\cdot d, \ldots$ unendlich viele Primzahlen.

  Anders ausgedrückt: Sind a und $d > 0$ teilerfremd, dann gibt es unendlich viele Primzahlen kongruent zu $a \mod d$.
- Arithmetische Progressionen, die aus Primzahlen bestehen, und die Dichte von $\mathbb{P}$: Wenn $a, a+d, \ldots, a+h\cdot d$ aus Primzahlen besteht, dann muss d durch jede Primzahl $< h$ teilbar sein. Also: Solche arithmetischen Progressionen müssen endlich sein. Beispiel:

  $$5, 11, 17, 23, 29$$

  Frage: Enthält $\mathbb{P}$ beliebig lange endliche Progressionen?

  $$56211383760397 + i \cdot 44546738095860$$

  ist prim für $i = 0, \ldots, 22$ (Frind, Jabling, Underwood; 2004)
- Vermutung von Erdös: Jede Teilmenge $A \subseteq \mathbb{N}$ für die $\sum_{a\in A} \frac{1}{a}$ divergiert, enthält endliche arithmetische Progressionen beliebiger Länge. Für $A = \mathbb{P}$ ist die Voraussetzung erfüllt.
- Satz von Szemeredi: Jede Teilmenge $A \subseteq \mathbb{N}$ positiver oberer Dichte, d.h.

  $$\lim_{n\to\infty} \sup \frac{|A \cap \{1, \ldots, n\}|}{n} > 0$$

  enthält beliebig lange endliche arithmetische Progressionen. ($\mathbb{P}$ erfüllt die Bedingung nicht.)
- Green+Tao (2005): $\mathbb{P}$ enthält beliebig lange endliche arithmetische Progressionen.

  Beweisidee: Green + Tao konstruieren eine Menge $T \subseteq \mathbb{N}$ mit den folgenden Eigenschaften:

  1. Der Satz von Szemeredi kann auf T übertragen werden.
  2. $\mathbb{P}$ hat relativ zu T eine positive obere Dichte.

11.2 Gruppen

- Eine *Gruppe* ist eine Algebra $(G, \circ, ^{-1}, e)$ vom Typ $(2, 1, 0)$, die für alle $x, y, z \in G$ folgende Gleichungen erfüllt:

$$\begin{aligned} x \circ e &= x = e \circ x \\ x \circ x^{-1} &= e = x^{-1} \circ c \\ x \circ (y \circ z) &= (x \circ y) \circ z \end{aligned}$$

- Eine *n-stellige Operation* auf einer Menge A ist eine Abbildung $f : A^n \to A$ ($n \in \mathbb{N}$), $n = 0$ ist zugelassen. Die nullstelligen Operationen auf A sind Abbildungen von $A^0 = \{\emptyset\}$ nach A ($A^n := A^{\{0,\ldots,n-1\}}$ = Menge aller Abbildungen von $\{0, \ldots, n-1\}$ nach A) Die nullstelligen Operationen auf A entsprechen deshalb eineindeutig den Elementen von A. Man nennt sie auch Konstanten.

- Eine (allgemeine) *Algebra* vom Typ $(u_i | i \in I)$ besteht aus einer *Trägermenge* A und einer Folge $(f_i)_{i \in I}$ von Operationen auf A, wobeo für jedes $i \in I$ die natürliche Zahl n_i die Stelligkeit der Operation n_i ist.

- Alternative Schreibweise für Gruppe:

$$\Sigma := \{(\circ, 2), (^{-1}, 1), (e, 0)\}$$

  nennt man *Signatur* der Algebra, auch *Rangalphabet*.

- Erfüllt eine Gruppe zusätzlich die Gleichung

$$\forall x, y \in G : x \circ y = y \circ x$$

  dann nennt man sie *abelsch* bzw. *kommutativ*. Kommutative Gruppen findet man vielfältig beim Rechnen, nicht abelsche Gruppen entstehen leicht, wenn mit Symmetrien gearbeitet wird.

- Eine bis heute nicht vollständig abgeschlossene Großaktion der mathematischen Forschung der letzten Hundert Jahre betraf die Klassifikation der endlichen Gruppen, also die Frage: Welche endlichen Gruppen gibt es? (Bis auf Isomorphie)

- Beispiele:

  1. kommutative dreielementige Gruppe ($\mathbb{Z}_3$):

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

  2. Isomorphieklassen von n-elementigen Gruppen:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	1	1	1	2	1	2	1	5	2	2	1	5	1	2
abelsch	1	1	1	2	1	1	1	3	2	1	1	2	1	1

n	15	16	17	18	19	20	23	24	25	30	31	32
	1	14	1	5	1	5	1	15	2	4	1	51
abelsch	1	5	1	2	1	2	1	3	2	1	1	7

- Vollständig und gut verstanden ist die Klassikation der endlich (erzeugten) abelschen Gruppen. Die Zutaten sind die folgenden:

  1. Die zyklischen Gruppen $\mathbb{Z}_n$, $n \geq 0$, und $\mathbb{Z}$ sind abelsch. $\mathbb{Z}_n$ hat die Trägermenge $\{0, \ldots, n-1\}$ und als fundamentale zweistellige Operation die Addition modulo n.
  2. Jedes direkte Produkt (kommutativer) Gruppen ist eine kommutative Gruppe.
  3. Jede endliche kommutative Gruppe ist isomorph zu einem direkten Produkt zyklischer Gruppen von Primzahlpotenzordnung.
  4. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{m \cdot n} \Leftrightarrow \mathrm{ggT}(m, n) = 1$

- Beispiele:

  1. Welche abelsche Gruppen mit 8 Elementen gibt es? Als Faktoren kommen nur $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_8$ (außer $\mathbb{Z}_1$) in Frage: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$
  2. Welche abelschen Gruppen mit 15 Elementen gibt es? Als Faktoren kommen $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_{15}$ in Frage: $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$
  3. Die abelschen Gruppen mit 24 Elementen: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_8$ kommen als Faktoren in Frage. Möglichkeiten: $\mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$, $\mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_4)$, $\mathbb{Z}_3 \times \mathbb{Z}_8$

  Beispiele nicht-abelscher Gruppen:

  1. Die Symmetrien des regelmäßigen n-Ecks ($n > 2$) bilden eine (2n)-elementige Gruppe, die als D_n bezeichnet wird und die *Diedergruppe* der Ordnung 2n genannt wird.
  2. Die Symmetrien der n-elementigen Menge ($n > 2$) bilden eine ($n!$)-elementige Gruppe, die als *symmetrische Gruppe* S_n auf n Elementen bezeichnet wird. Darin enthalten ist die *alternierende Gruppe* A_n der geraden Permutationen, sie hat $\frac{n!}{2}$ Elemente.
  3. Weitere Beispiele kommen aus der linearen Algebra über endliche Körper.

- Eine ähnlich klare Klassifikation der endlichen nicht-abelschen Gruppen gibt es nicht. Man hat aber eine Klassifikation der endlichen einfachen gruppen. Unter den nicht-abelschen einfachen Gruppen gibt es 5 unendliche Serien sowie 26 sporadische Gruppen.

11.3 $\mathbb{Z}_p$ - Endliche Körper I

- Betrachte $\mathbb{Z}_{11}, a := 2$. Dann Potenzen von a:

  $$\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$$

  $\mathbb{Z}_{11}^*$ ist eine *zyklische Gruppe*, also eine von einem Element erzeugte Gruooe. Ein solches erzeugendes Element der multiplikativen Gruppe ist ein *primitives Element*.

- Die multiplikative Gruppe von $\mathbb{Z}_{11}$ ist also isomorph zur additiven Gruppe $\mathbb{Z}_{10}$ - Ähnliche Situation: $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +), x \mapsto \ln x$.

- Man kann also für $\mathbb{Z}_{11}$ eine Art Logarithmus einführen. Man definiert zum primitiven Element $a = 2$:

  $$\log_a(z) = y :\Leftrightarrow a^y = z$$

  Man findet für $\mathbb{Z}_{11}$ und $a = 2$:

z	0	1	2	3	4	5	6	7	8	9	10
$\log_a z$	$-\infty$	0	1	8	2	4	9	7	3	6	5

  und hat für alle $x, y \in \mathbb{Z}_{11}$:

  $$x \cdot y = a^{\log_a x + \log_a y}$$

  (Zech-Logarithmus).

- Für $\mathbb{Z}_{13}$ ist $a = 2$ ebenfalls ein primitives Element, für $\mathbb{Z}_{17}$ jedoch nicht. $a = 3$ ist primitives Element von $\mathbb{Z}_{17}$. Für $p = 23$ findet man, dass $a = 5$ ein primitives Element ist. Allgemein gilt:
- Satz (vom primitiven Element): Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.
- Es gibt kein bekanntes schnelles Verfahren $\log_2 z$ in $\mathbb{Z}_p$ auszurechnen, das für beliebige Primzahlen p funktioniert (Binary log problem). Man kann das ausnutzen, um öffentlich Geheimnisse zu kommunizieren.
- Szenario: Zwei Teilnehmer möchten geheim kommunizieren. Sie verwenden dazu ein Verschlüsselungsverfahren mit einem geheimen Schlüssel, der für beide der gleiche ist.

  Vorgehensweise: Sie einigen sich (öffentlich) auf eine große Primzahl p ($> 10^{500}$). Teilnehmer A wählt eine Zahl $a \in \mathbb{Z}_p$ und sendet $2^a \mod p$, Teilnehmer B wählt $b \in \mathbb{Z}_p$ und sendet $2^b \mod p$. Der gemeinsame Schlüssel ist $2^{a \cdot b}$.
- Das *quadratische Reziprozitätsgesetz* von C.F. Gauß behandelt die Frage, welche Zahlen Quadratzahlen modulo p sind (p prim, $p \neq 2$).

  Beobachtung: Die Quadrate in $\mathbb{Z}_p$ bilden bzgl. der Multiplikation eine Untergruppe von Index 2. Der Index einer Untergruppe U der Gruppe G ist

  $$\mathrm{ind}(U) := \frac{|U|}{|G|}$$

  Mit anderen Worten: Genau die Hälfte der von Null verschiedenen Elemente in $\mathbb{Z}_p$ sind Quadrate ($p > 2$) und Produkte und multiplikativ Inverse von Quadraten sind selbst Quadrate:

  $$(a \cdot b)^2 = a^2 \cdot b^2 \qquad \frac{1}{a^2} = \left(\frac{1}{a}\right)^2$$

  Um zu zeigen, dass genau die Hälfte der Elemente von $\mathbb{Z}_p^*$ Quadrate sind, betrachtet man die Abbildung

  $$x \mapsto x^{\frac{p-1}{2}}$$

  und zeigt, dass die Quadrate genau die Urbilder des Elements 1 sind.

  $$a^2 \mapsto \left(a^2\right)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \mod p$$

- Das *Legendre-Symbol* ist für eine Primzahl $p \neq 2$ wie folgt definiert: Für $x \in \mathbb{Z}_p^*$ sei

  $$\left(\frac{x}{p}\right) := x^{\frac{p-1}{2}} \mod p \qquad \in \{\pm 1\}$$

  Man hat für $x \neq 0$:

  $$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ ist Quadrat} \\ -1 & x \text{ ist kein Quadrat} \end{cases}$$

  Man erweitert die Definition durch

  $$\left(\frac{z}{p}\right) := \frac{z \mod p}{p} \qquad (z \in \mathbb{Z})$$

  Offenbar gilt:

  $$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{a \cdot b}{p}\right)$$

  $$\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{1}{p}\right) = 1 \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

- Satz (Reziprozitätsgesetz): Sind p und l Primzahlen, so gilt

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

- Beispiel: Ist 215 eine Quadratzahl in $\mathbb{Z}_{313}$?

$$\begin{aligned}
\left(\frac{215}{313}\right) &= \left(\frac{5 \cdot 43}{313}\right) = \left(\frac{5}{313}\right) \cdot \left(\frac{43}{313}\right) \\
&= \left(\frac{313}{5}\right) \cdot (-1)^{2 \cdot 156} \cdot \left(\frac{313}{43}\right) \cdot (-1)^{21 \cdot 156} \\
&= \left(\frac{313}{5}\right) \cdot \left(\frac{313}{43}\right) = \left(\frac{3}{5}\right) \cdot \left(\frac{12}{43}\right) \\
&= \left(\frac{3}{5}\right) \cdot \left(\frac{3}{43}\right) \cdot \left(\frac{2}{43}\right)^2 = \ldots = 1
\end{aligned}$$

11.4 Endliche Körper II

- Wir konstruieren einen Körper mit 8 Elementen. Weil $2^3 = 8$ ist, gehen wir vom zweielementigen Körper $\mathbb{Z}_2$ aus. Man sucht ein irreduzibles Polynom $p \in \mathbb{Z}_2[x]$ vom Grad 3. Ein Beispiel dafür ist

$$p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$$

  Hätte dieses Polynom eine Zerlegung in ein Produkt von Polynomen kleineren Grades, dann hätte es auch eine Nullstelle in $\mathbb{Z}_2$.

- Wir rechnen nun in $\mathbb{Z}_2/_{x^3+x+1}$. Die Elemente dieses Faktorrings (genauer: ein Repräsentantensystem der Klassen) sind

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

  Die Addition ist die gewöhnliche in $\mathbb{Z}_2[x]$. Zum Multiplizieren benutzt man die Polynommultiplikation von $\mathbb{Z} - 2$, rechnet aber modulo $x^3 + x + 1$. Beispiel:

$$(x^2+1) \cdot (x+1) = x^3 + x^2 + x + 1 \equiv x^2 \mod x^3 + x + 1$$

- Tafel:

Element	Repräsentant	Koeffiziententupel	Logarithmus
0	0	(0,0,0)	$-\infty$
x	x	(0,1,0)	1
x^2	x^2	(0,0,1)	2
x^3	$x+1$	(1,1,0)	3
x^4	x^2+x	(0,1,1)	4
x^5	x^2+x+1	(1,1,1)	5
x^6	x^2+1	(1,0,1)	6
x^7	1	(1,0,0)	0

  Hieraus können die Operationen wie folgt abgelesen werden:

  1. Addition: komponentenweise
  2. Multiplikation: Addieren der zugehörigen Logarithmen
  3. Finden des Inversen: Logarithmus der Zahl + Logarithmus des Inversen = 0 mod 7

Anzahl der Untervektorräume der Dimension d:

d	0	1	2	3
♯ UVR	1	7	7	1

- $PG(2,2)$ ist die projektive Ebene über dem zweielementigen Körper (s. Geometrie, M. Hamann).
- Die Addition des achtelementigen Körpers entspricht der im Vektorraum $\mathbb{Z}_2^3$, also der komponentenweisen Addition gemäß binärer 3-Tupel. Multiplikation mit einem festen Element a ist wegen
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
eine lineare Abbildung und für $a \neq 0$ sogar bijektiv, also ein Isomorphismus. Wählt man für a ein primitives Element, dann ist diese Abbildung auf den von Null verschiedenen Elementen eine zyklische Permutation.

Klassifikation der endlichen Körper

- Satz: Die Anzahl der Elemente eines endlichen Körpers ist eine Primzahlpotenz. Zu jeder Primzahlpotenz $q = p^n$ (p prim, $n \in \mathbb{N}$) gibt es bis auf Isomorphie genau einen Körper mit q Elementen (dieser wird mit GF(q) bezeichnet).
- Schon bewiesen: Der Körper muss endlich dimensionaler Vektorraum über seinem Primkörper sein. Zu jeder Primzahl p und jeder natürlichen Zahl $n > 0$ existiert ein in $\mathbb{Z}_p[x]$ irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ und $GF(p^n) \cong \mathbb{Z}_p[x]/f$.

  In jedem Körper $\mathbb{K}$ der Charakteristik $p > 0$ ist die Abbildung φ, die durch
  $$\varphi(a) := a^p$$
  für $a \in \mathbb{K}$ ein Automorphismus (Fröbenius-). Es gilt also
  $$(a + b)^p = a^b + b^p \qquad (a \cdot b)^p = a^p \cdot b^p$$
  für alle $a, b \in \mathbb{K}$.

  Beweis:

  – p prim,
  $$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot a^i \cdot b^{p-i}$$
  Für $0 < i < p$ folgt $p | \binom{p}{i}$, also $\binom{p}{i} = 0 \mod p$. Damit
  $$(a + b)^p = a^p + b^p \mod p$$
- Ist $f \in \mathbb{K}[x]$ ein Polynom und hat $\mathbb{K}$ die Charakteristik $p > 0$, dann gilt $f(x)^p = f(x^p)$. Insbesondere gilt: Ist a Nullstelle von f, dann auch a^p.
- Die Elemente der Primkörper sind Fixpunkte unter dem Automorphismus φ. Der Primkörper ist nämlich isomorph zu $\mathbb{Z}_p$. In $\mathbb{Z}_p$ gilt nach dem Lemma von Fermat $x^p = x$ für jedes Element x.
- Es ist nicht einfach irreduzible Polynome vom Grad n in $\mathbb{Z}_p[x]$ für alle n und p anzugeben (Tafelwerke). Der allgemeine Beweis für die Existenz wird über den Begriff des Zerfällungskörpers geführt.

11.5 Polynomcodes

- Der (7,4)-Hamming-Code besteht aus dem Kern der Kontrollmatrix

$$\begin{aligned} H_3 &:= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}(3 \times 7, GF(2)) \\ C &:= \{v \in GF(2)^7 | H \cdot v = 0\} \end{aligned}$$

  mit $\dim C = 7-3 = 4$. C hat folglich 2^4 Elemente. Er hat die Minimaldistanz 3 und ist deshalb 1-Fehler-korrigierend. Der (7,4)-Hamming-Code (und allgemeiner jeder $(2^k - 1, 2^k - k - 1)$ Hamming-Code) ist 1-Fehler korrigierend perfekt, d.h. die Kugeln vom Radius 1 um die Codewörter bilden eine Partition des Raumes aller $(2^k - 1)$-Tupel. Man kann den (7,4)-Hamming-Code noch besser hinschreiben, indem man die Spalten der Kontrollmatrix geeignet vertauscht und zwar so:

$$\tilde{H}_3 := \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

  Man stellt für denCode

$$\tilde{C} = \{v \in GF(2)^7 | \tilde{H}_3 \cdot v = 0\}$$

  dass es sich um einen zyklischen Untervektorraum handelt. Das bedeutet folgendes: Ist $(c_0, \ldots, c_6)^T \in \tilde{C}$, dann auch $(c_1, \ldots, c_6, c_0)^T \in \tilde{C}$.

- Beispiel:

  1. Ist $c := (1,1,1,0,1,0,1)^T \in \tilde{C}$? Wir berechnen $\tilde{H}_3 \cdot c$ und erhalten $(1,0,1)^T$. c ist also kein Codewort, unterscheidet sich deshalb nur in einem Bit von einem Codewort, nämlich $(1,1,0,0,1,0,1)^T$, da $(1,0,1)^T$ 3. Spaltenvektor von $\tilde{H}_3$. Damit sich auch alle zyklischen Shifts Codewörter. Besonders nützlich ist diese Eigenschaft, wenn man die Tupel als Koeffizienten von Polynomen liest:

$$(1,0,1,1,1,0,0)^T \longleftrightarrow 1 + x^2 + x^3 + x^4 \in GF(2)[x]$$

- Ein zyklischer binärer Code der Länge k ist eine Menge $C \subset GF(2)[X]$ von Polynomen vom Grad $< k$ mit folgenden Eigenschaften:

  1. C ist ein Untervektorraum des Vektorraums $GF(2)[X]$.
  2. Ist $p \in C$, dann auch $x \cdot p \mod x^k + 1$ (zyklischer Shift von p).

- Sei $r := \sum_{i=0}^{k} r_i \cdot x^i \in GF(2)[X]$, $c \in C$. Wir berechnen $r \cdot c \mod x^k + 1$:

$$\begin{aligned} r \cdot c &= \left(\sum_{i=0}^{k} r_i \cdot x^i \right) \cdot c \\ &= \sum_{i=0}^{k} r_i \cdot c \cdot x^i \in C \mod x^k + 1 \end{aligned}$$

  Es folgt, dass C gegen Multiplikation mit beliebigen Polynomen aus $GF(2)[X]$ abgeschlossen ist, wenn man modilo $x^k + 1$ rechnet. (C ist ein Ideal.)

- Die algebraische Theorie ergibt nun folgendes: Jeder solche zyklische Polynomcode besitzt ein eindeutig bestimmes (normiertes) Polynom $\neq 0$ vom kleinsten Grad in C und alle Elemente von C sind $\mod x^k + 1$ Vielfache dieses Polynoms. Man nennt dieses Polynom das *Generatorpolynom* des Codes C. Es ist notwendigerweise ein Teiler des Polynoms $x^k + 1$ in $GF(2)[X]$. Für den (7,4)-Hamming-Code ist dies das Polymom

$$1 + x^2 + x^3 + x^4$$

- Um Polynomcodes der Länge n zu finden, muss man also die Teiler des Polynoms $x^n + 1$ in $GF(2)[X]$ durchsuchen. Wie findet man die?
- Die Teiler von $x^n + 1$ in GF(2)[X] bestimmt man (für ungerade n) wie folgt: Man sucht eine möglichst kleine Potenz q von 2 mit der Eigenschaft, dass n ein Teiler von $q - 1$ ist.

  Beispiel: $n = 11$:

  $$2, 4, 8, 5, 10, 9, 7, 3, 6, 1 \Rightarrow 2^{10} \mod 11 = 1 \Rightarrow 2^{10} - 1|11$$

  Rechne nun in $GF(2^{10}) = GF(1024)$. Die multiplikative Gruppe von GF(1024) ist zyklisch. Es gibt ein primitives Element $\alpha \in GF(1024)$, d.h. die Potenzen $\alpha, \ldots, \alpha^{1023}$ sind paarweise verschieden. Das Element

  $$\beta := \alpha^{\frac{1023}{11}} = \alpha^{93}$$

  erfüllt $\beta^{11} = \alpha^{1023} = 1$ und $\beta, \beta^2, \ldots, \beta^{11}$ sind paarweise verschieden. In GF(1024) hat das Polynom $x^k + 1$ also 11 verschiedene Nullstellen. β heißt *primitive elfte Einheitswurzel*. Wir können also in GF(2)[X] das Polynom $X^{11} + 1$ in Linearfaktoren zerlegen:

  $$(x + \beta) \cdot (x + \beta^2) \cdots (x + \beta^{11})$$

  Die Teiler von $X^{11} + 1$ in GF(2)[X] sind allesamt Produkte dieser Linearfaktoren.

  Wir wissen, dass die Abbildung $x \mapsto x^2$ ein Automorphismus von GF(1024) ist, der $\{0, 1\}$ festlässt. Deshalb gilt: Ist $\gamma \in GF(2^{10})$ eine Nullstelle eines Polynoms aus GF(2)[X], dann auch γ^2. Insbesondere gilt: Ist γ eine Nullstelle von $X^{11} + 1$, dann auch γ^2. Das gilt auch für jeden Teiler von $X^{11} + 1$, der Koeffizienten in GF(2) hat. Ist also $g(X)$ ein Teiler von $X^{11} + 1$ und ist β^i eine Nullstelle von g in GF(1024), dann ist auch β^{2i} eine Nullstelle von g. Diese Information genügt, um alle Teiler zu bestimmen.