Algebra II (Diskrete Mathematik) - Zusamenfassung

Patrick Pletscher

21. Oktober 2003

1 Mengen

1.1 Konzept

$A = \{a\} \Rightarrow a \in A$

$A \subset B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$

$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$:
$x \in A \Rightarrow x \in B$ und $x \in B \Rightarrow x \in A$

$\emptyset \subseteq A : \forall A$

$\emptyset$ ist eindeutig: $\emptyset \subseteq\supseteq \emptyset'$

1.2 Grundregeln der Mengenlehre

1. Idempotent
   $A \cap A = A,\ A \cup A = A$
2. Kommutativ
   $A \cap B = B \cap A,\ A \cup B = B \cup A$
3. Assoziativ
   $A \cap (B \cap C) = (A \cap B) \cap C$
   $A \cup (B \cup C) = (A \cup B) \cup C$
4. Absorption
   $A \cap (A \cup B) = A,\ A \cup (A \cap B) = A$
5. Distributiv
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ($\cap$ über $\cup$)
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ($\cup$ über $\cap$)
6. Komplementär
   $A \cap A' = \emptyset,\ A \cup A' = I$
7. Konsistenz
   $A \cap B = A \Leftrightarrow A \subseteq B \Leftrightarrow A \cup B = B$

1.3 Operationen auf Mengen

Allgemein

$\{x \in A | P(x)\}$

Potenzmenge

$P(A) = \{x \subseteq A\}$
immer 2^n Elemente
z.B.: $P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

Schnitt und Vereinigung

A': Komplement von A
$A \cap B$: A geschnitten B
$A \cup B$: A vereinigt B
$A \cap B = \emptyset$: A und B sind disjunkt
$B - A = \{x \in B | x \notin A\}$
$A \cup B - A \cap B = A \oplus B$: symm. Differenz

Das kartesische Produkt

Geordnete Paare
$(a, b) = (c, d) \Rightarrow a = c \wedge b = d$
Def. $(a, b) = \{\{a\}, \{a, b\}\}$

Produktmenge
$A \times B = \{(a, b) | a \in A, b \in B\}$

1.4 Relationen

Definition

$\rho \subseteq A \times B\ (a, b) \in \rho\ a\rho b$

Zusammensetzung:$\rho\sigma$
$a\ \rho\sigma\ b \Leftrightarrow \exists q \in B : a\rho q \wedge q\sigma b$

Umkehrung von $\rho : \breve{\rho}$
$\breve{\rho}\breve{\sigma} = \breve{\sigma}\breve{\rho}$

Äquivalenzrelation

Eine Äquivalenzrelation ρ_E auf eine Menge A ist eine Relation auf A so, dass für alle $a, b, c \in A$ gilt:

1. Reflexiv: $a\rho_E a$
2. Symmetrisch: $a\rho_E b \Leftrightarrow b\rho_E a$

3. Transitiv: $a\rho_E b$ und $b\rho_E c \Leftrightarrow a\rho_E c$

Wenn $a \in A$, definiert [a] die Äquivalenzklasse, die die Elemente a der Menge A enthält, die äquivalent zu a sind:
$[a] = \{b \in A | a\rho_E b\}$

A/E = Menge aller Äquivalenzklassen = $\{[a]|a \in A\}$
z.Bsp. Modulo: $Z/E_m = \{[0], [1], \ldots, [m-1]\}$

Partielle Ordnungnen

Eine partielle Ordnung $\leq$ auf einer Menge P ist eine Relation auf P so, dass für alle $x, y, z \in P$ gilt:

1. Reflexiv: $x \leq x$
2. Anti-Symmetrisch: $x \leq y \wedge y \leq x \Leftrightarrow x = y$
3. Transitiv: $x \leq y \wedge y \leq z \Leftrightarrow x \leq z$

Eine Menge P zusammen mit einer partiellen Ordnung $\leq$ auf P wird partiell geordnete Menge genannt, oder kurz Poset und wird als $[P; \leq]$ geschrieben.

Spezielle Elemente in Posets
$[P; \leq]$ ist ein Poset und X ist eine Untermenge von P. Dann

1. $y \in X$ ist das minimale (maximale) Element von X, falls $x < y$ $(x > y)$ für kein $x \in X$
2. $y \in X$ ist das kleinste (grösste) Element von X, falls $y \leq x$ $(y \geq x)$ für alle $x \in X$
3. $y \in P$ ist eine untere (obere) Schranke für X, falls $y \leq x$ $(y \geq x)$ für alle $x \in X$
4. $y \in P$ ist die grösste untere Schranke (kleinste obere Schranke) von x, falls y das grösste (kleinste) Element von der Menge aller unteren (oberen) Schranken von X.

Verbände (Lattices)

x und y Elemente eines Posets $[P; \leq]$. Wir bezeichnen deren grösste untere Schranke als $x \wedge y$ ("x meet y") und deren kleinste obere Schranke mit $x \vee y$ ("x join y").
Definition: Ein Verband ist ein Poset in welchem jedes Paar von Elementen ein Meet und ein Join hat.

Grundregeln der Verbände

1. Idempotent
   $x \wedge x = x$, $x \vee x = x$
2. Kommutativ
   $x \wedge y = y \wedge x$, $x \vee y = y \vee x$
3. Assoziativ
   $x \wedge (y \wedge z) = (x \wedge y) \wedge z$
   $x \vee (y \vee z) = (x \vee y) \vee z$
4. Absorption
   $x \wedge (x \vee y) = x$, $x \vee (x \wedge y) = x$
5. Konsistenz
   $x \leq y \Leftrightarrow x \wedge y = x \Leftrightarrow x \vee y = y$

1.5 Funktionen

[..]

1.6 Russell-Paradoxon

$R = \{x | x \notin x\}$, die Menge von allen Mengen, die nicht zu sich selbst gehören.

Dies führt zu einem Widerspruch: $R \in R$, wenn und nur wenn $R \notin R$

Meistens gehören die Mengen nicht zu sich selber, aber es gibt auch Ausnahmen, z.B. die Menge die mehr als fünf Elemente enthält, ist auch wieder eine Menge, die mehr als fünf Elemente enthält.

1.7 Zermelo's Axiome

Axiom 1

Zwei Mengen sind gleich, wenn sie die gleichen Elemente enthalten:
$\forall xy(\forall z(u \in x \leftrightarrow z \in y) \rightarrow x = y)$

Satz 1

Wir haben x=y, falls und nur falls $x \subset y$ und $y \subset x$:
$\forall xy(x \subset y \wedge y \subset x) \leftrightarrow x = y$

Axiom 2

Wenn x eine Menge und p ein Prädikat ist, dann existiert eine Menge y deren Elemente genau diese Elemente z von x sind, für welche p(z) gilt:
$\forall x \exists y \forall z(z \in y \leftrightarrow (z \in x \wedge p(z)))$

Satz 2

Keine Menge enthält alle Objekte:
$\forall x \exists y(y \notin x)$

Axiom 2.1

Es existiert eine Menge, $\exists x(x = x)$
So können wir auch die Menge $\emptyset := \{y \in x | y \neq y\}$

Axiom 3

Für zwei Mengen x und y existiert eine Menge, die x und y enthält.
$\forall xy \exists z(x \in z \wedge y \in z)$

Lemma

$\{x\} = \{y\}$ gilt nur dann, wenn x=y

Axiom 4

Für jede Menge X gibt es eine Menge, die alle Elemente enthält, enthalten zumindest in einem Element von X.
$\forall X \exists Y \forall xy((x \in X \wedge y \in x) \rightarrow y \in Y)$

Axiom 5

Für jede Menge x existiert eine Menge z, die als ihre Elemente alle Untermengen von x enthält.
$\mathcal{P}(x) := \{y \in z | y \subset x\}$

2 Natürliche Zahlen, Induktion und Zählbarkeit

2.1 Nachfolgerfunktion für Mengen

Definition Der Nachfolger einer Menge x ist definiert als
$s(x) := x \cup \{x\}$
Beispiel: $s(\{a, b\}) = \{a, b, \{a, b\}\}$

2.2 Definition der natürlichen Zahlen

$\mathbf{0} := \emptyset$
$\mathbf{1} := s(\mathbf{0}) = \{\mathbf{0}\} = \{\emptyset\}$
$\mathbf{2} := s(\mathbf{1}) = \{\mathbf{0}, \mathbf{1}\} = \{\emptyset, \{\emptyset\}\}$

Definition Eine Menge x wird als Nachfolgemenge bezeichnet wenn $\emptyset \in x$ und $s(y) \in x$ wenn immer $y \in x$:
$\emptyset \in x \wedge \forall y(y \in x \rightarrow s(y) \in x)$

Axiom
Es existiert eine Nachfolgemenge

Satz
Es existiert eine Nachfolgemenge ω welche minimal ist im Sinne, dass $\omega \subset x$ für alle Nachfolgemengen x.
$\exists \omega \forall x(\emptyset \in x \wedge \forall y(y \in x \rightarrow s(y) \in x) \rightarrow \omega \subset x)$

Definition ω ist die Menge der Natürlichen Zahlen

2.3 Mathematische Induktion

Korollar Wenn ein Prädikat p (auf eine Menge) stimmt für alle Elemente einer Nachfolgemenge:

1. Induktionsverankerung: p($\mathbf{0}$) gilt und
2. Induktionsschritt: p(s(x)) gilt für irgendeine Menge x für welche p(x) gilt.

Lemma Keine natürliche Zahl ist eine Teilmenge von einem ihrer Elemente
$x \in n \rightarrow n \not\subset x$

Korollar $n \notin n$ für alle natürlichen Zahlen n.

Lemma Jedes Element der natürlichen Zahlen ist eine Teilmenge von ihr.
$x \in n \rightarrow x \subset n$

2.4 Peano's Axiomatisierung der natürlichen Zahlen

Satz $s(n) \neq \mathbf{0}$ für alle $n \in \omega$

Satz Wenn $s(m) = s(n)$, dann m=n

Peano's Axiome

1. $0 \in N$
2. $n \in N \rightarrow \widetilde{s}(n) \in N$
3. $A \subset N \wedge 0 \in A \wedge (n \in A \rightarrow \widetilde{s}(n) \in A) \Rightarrow A = N$
4. $\widetilde{s}(n) \neq 0$ für alle $n \in N$
5. $\widetilde{s}(n) = \widetilde{s}(m)$ impliziert n = m für irgendein $m, n \in N$

2.5 Arithmetik der natürlichen Zahlen

Rekursionssatz

X eine Menge und a ein Element von x und f eine Funktion von x nach x. Dann existiert eine Funktion $g : \omega \rightarrow x$ so, dass:

1. $g(0) = \mathbf{a}$ und
2. $g(s(n)) = f(g(n))$ für alle $n \in \omega$

Addition

Definition Für jedes $m \in \omega$, ist die Funktion $\sigma_m : \omega \rightarrow \omega$ definiert als:

1. $\sigma_m(\mathbf{0}) = m$
2. $\sigma_m(s(n)) = s(\sigma_m(n))$ für alle $n \in \omega$

Die Nummer $\sigma_m(n)$ ist die Summe von m und n, auch geschrieben als m+n.

Satz Die Addition auf den natürlichen Zahlen ist assoziativ. Für alle $k, m, n \in \omega$ gilt:
$(k + m) + n = k + (m + n)$

Satz Die Addition auf den natürlichen Zahlen ist kommutativ. Für alle $m, n \in \omega$ gilt:
$m + n = n + m$

Multiplikation

Definition Für jedes $m \in \omega$, ist die Funktion $p_m : \omega \to \omega$ definiert als:

1. $p_m(\mathbf{0}) = \mathbf{0}$
2. $p_m(s(n)) = p_m(n) + m$ für alle $n \in \omega$

Die Nummer $p_m(n)$ ist nach Definition das Produkt von m und n, auch geschrieben als $m \cdot n$
Die Regeln können auch so geschrieben werden:
- $m \cdot \mathbf{0} = \mathbf{0}$
- $m \cdot s(n) = m \cdot n + m$

Ordnungsrelation auf den natürlichen Zahlen

Definition $m < n$ wenn $m \in n$, und $m \leq n$ wenn $m < n$ oder $m = n$

Satz Für irgendwelche Zahlen k,m und n:

1. Wenn $m < n$ dann $m + k < n + k$
2. Wenn $m < n$ und $k \neq 0$ dann $m \cdot k < n \cdot k$
3. Wenn x eine nichtleere Menge von natürlichen Zahlen, dann existiert ein $m \in x$ so dass $m \leq n$ für alle $n \in x$

Von den natürlichen Zahlen zu den Zahlen

$\xi := \{(a, b) \in \omega \times \omega | a = \mathbf{0} \vee \mathbf{b} = \mathbf{0}\}$

$(m, \mathbf{0}) + (n, \mathbf{0}) = (m + n, \mathbf{0})$
$(\mathbf{0}, m) + (\mathbf{0}, n) = (\mathbf{0}, m + n)$

$$(m, \mathbf{0}) + (\mathbf{0}, n) = \begin{cases} (\mathbf{0}, n - m) & m < n \\ (m - n, \mathbf{0}) & n \leq m \end{cases}$$

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

2.6 Gleichheit von Mengen, Zählbarkeit und Unzählbarkeit von Mengen

Definition Zwei Mengen A und B werden als *gleich mächtig* bezeichnet ($A \sim B$), wenn es eine Bijektion $A \to B$ gibt. Eine Menge B dominiert eine Menge A ($A \preceq B$), wenn $A \sim C$ eine Teilmenge $C \subseteq B$ oder anders gesagt wenn eine injektive Funktion $A \to B$ existiert. Eine Menge A wird als zählbar bezeichnet wenn $A \preceq \mathbb{N}$ und sonst unzählbar.

Satz Eine Teilmenge einer zählbaren Menge ist auch zählbar.

Satz Die Menge $B = \{(m, n) | m, n \in \mathbb{N}\}$ von geordneten Paaren von natürlichen Zahlen ist zählbar.

Satz Für irgendein $n \in \mathbb{N}$ und irgendeine zählbare Menge S ist die Menge der n-Tupel über S zählbar.

Satz Die Vereinigung von einer zählbaren Menge und einer zählbaren Menge ist zählbar.

Korollar Die rationalen Zahlen $\mathbb{Q}$ sind zählbar

Satz Die Menge $\mathbb{R}$ der reellen Zahlen ist unzählbar. So auch die Menge $\{0, 1\}^\infty$ von unendlichen Binärfolgen.

Satz Jede Menge ist strikt dominiert von ihrer Potenzmenge. $A \preceq \mathcal{P}(A)$ aber $A \not\sim \mathcal{P}(A)$

3 Kombinatorik und Zählen

3.1 Grundlegene Zähl-Prinzipien

Additions-, Mulitiplikations- und Bijektionsgrundsatz

Additionsgrundsatz:
$\forall i, j \leq i < j \leq n : A_i \cap A_j = \emptyset \Rightarrow | A_1 \cup \cdots \cup A_n | = \sum_{i=1}^{n} | A_i |$

Multiplikationsgrundsatz:
$| A_1 \times \cdots \times A_n | = \Pi_{i=1}^{n} | A_i |$

Inklusion-Exklusion

Wenn die Mengen $A_1, \ldots, A_n$ nicht disjunkt sind, gilt:
$| A \cup B | = | A | + | B | - | A \cap B |$
Genereller:
$| A \cup B \cup C | = | A | + | B | + | C | - | A \cap B | - | B \cap C | + | A \cap B \cap C |$
Noch allgemeiner:
$| A_1 \cup \cdots \cup A_n | = \sum_{i=1}^{n} | A_i | - \sum_{1 \leq i_1 < i_2 \leq n} | A_{i1} \cap A_{i2} | + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} | A_{i1} \cap A_{i2} \cap A_{i3} | - \cdots + (-1)^{n-1} | A_1 \cap \cdots \cap A_n |$
Bonferroni Ungleichung:
$| A_1 \cup \cdots \cup A_n | \geq \sum_{i=1}^{n} | A_i | - \sum_{1 \leq i_1 < i_2 \leq n} | A_{i1} \cap A_{i2} |$

Auswahlprobleme

Wir betrachten eine Menge von n Elementen, von denen k selektiert werden.

	Geordnet	Ungeordnet
mit Wiederh.	n^k	$\binom{n+k-1}{k}$
ohne Wiederh.	$\Pi_{i=0}^{k-1}(n-i)$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Double Counting Prinzip

Es spielt keine Rolle, ob man über die Kolonnen oder Zeilen summiert. $\mid S \mid = \sum_{a \in A} r(a) = \sum_{b \in B} c(b)$

Pigeonhole Prinzip

Wenn n Objekte in $k < n$ Schachteln platziert werden, so enthält mindestens eine Schachtel ein oder mehr Objekte.

Binomial Koeffizienten

$\binom{n}{k} = \binom{n}{n-k}$

Theorem
x, y komplexe Zahlen. Für Zahlen $n \geq 0$ gilt:
$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

Pascal's Identität
$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ wenn $n > 0$

Theorem
$m, n \geq 0$ ganze Zahlen und $m + n > 0$ und k irgendeine ganze Zahl:
$\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$

Theorem
$n \geq 0$ und ganze Zahl, $0 < k \leq n$:
$(\frac{n}{k})^k \leq \binom{n}{k} < (\frac{en}{k})^k$

3.2 Reihen und Folgen

$(a_n)_{n \geq 0}$ wird benutzt um die Folge $(a_0, a_1, a_2, a_3, \ldots)$ zu beschreiben.

Erzeugende Funktionen

$G(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k + \ldots = \sum_{k=0}^{\infty} a_k x^k$

Produkt
$G_1(x)G_2(x) = \sum_{k=0}^{\infty} (\sum_{i=0}^{k} a_i b_{k-i}) x^k$

Wichtige erzeugende Funktionen

Folge	Erz. Funktion	Geschl. Form
$(1, a, \binom{a}{2}, \binom{a}{3}, \binom{a}{4}, \ldots)$	$\sum_{k=0}^{\infty} \binom{a}{k} x^k$	$(1+x)^a$
$(1, 1, 1, 1, \ldots)$	$\sum_{k=0}^{\infty} x^k$	$\frac{1}{1-x}$
$(1, 2, 3, 4, \ldots)$	$\sum_{k=0}^{\infty} (k+1) x^k$	$\frac{1}{(1-x)^2}$
$(1, a, \binom{a+1}{2}, \binom{a+2}{3}, \ldots)$	$\sum_{k=0}^{\infty} \binom{a+k-1}{k} x^k$	$\frac{1}{(1-x)^a}$
$(1, a, a^2, a^3, \ldots)$	$\sum_{k=0}^{\infty} a^k x^k$	$\frac{1}{1-ax}$
$(1, \binom{b}{1}a, \binom{b+1}{2}a^2, \binom{b+2}{3}a^3, \ldots)$	$\sum_{k=0}^{\infty} \binom{b+k-1}{k} a^k x^k$	$\frac{1}{(1-ax)^b}$
$(1, 1, \frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \ldots)$	$\sum_{k=0}^{\infty} \frac{1}{k!} x^k$	e^x

Lineare Rekursion

Eine linear rekursive Folge $(a_n)_{n \geq 0}$ mit Rekursionslänge L ist definiert bei den ersten L Elementen $a_0, \ldots, a_{L-1}$ der Folge und bei einer Rekursionsgleichung:
$a_n = \sum_{i=1}^{L} c_i a_{n-i}$
wobei $c_1, \ldots, c_L$ fixe Koeffizienten sind. Wir definieren das Polynom $c(x) := 1 - c_1 x - c_2 x^2 - \ldots - c_L x^L$ als das Rekursionspolynom der Reihe.

Ansatz für inhomogene Rekursionsgleichung: $a(x)c(x) = p(x) + b(x)$
Wobei $a(x)$ die Fkt. ist, die man sucht, $c(x)$ das Rekursionspoly. und $b(x)$ die Störfaktoren in der Rek.gl., $p(x)$ sind Terme die möglicherweise noch fehlen.

4 Graphen Theorie

4.1 Grundlagen

Definitionen von Graphen

Ein Graph $G = (V, E)$ besteht aus einer endlichen Menge V von Eckpunkten und einer Menge $E \subseteq \{\{u, v\} \subseteq V | u \neq v\}$ von Kanten.

Die *Nachbarn* eines Eckpunktes v ist die Menge $\Gamma(v) := \{u \in V | \{u, v\} \in E\}$.

Der *Grad* $deg(v)$ eines Eckpunktes ist: $deg(v) :=\mid \Gamma(v) \mid$. Ein Graph ist k-regulär, wenn $deg(v) = k$, $\forall v \in V$.

$\sum_{v \in V} deg(v) = 2 \mid E \mid$ und die Anzahl Eckpunkte mit ungeraden Grad ist gerade.

Subgraph
Ein Graph $G = (V, E)$ ist ein Subgraph von einem Graph $H = (V', E')$, bezeichnet als $G \sqsubseteq H$, wenn $V \subseteq V'$ und $E \subseteq E'$.

Vereinigung
Die Vereinigung von zwei Graphen $G = (V, E)$ und

$H = (V', E')$ ist der Graph $G \cup H := (V \cup V', E \cup E')$

Komplement
Das Komplement $\bar{G}$ eines Graphes $G = (V, E)$ ist der Graph $\bar{G} = (V, \bar{E})$, wobei $\bar{E}$ aus allen Kanten besteht, die nicht in E sind.

Bipartit
Ein Graph $G = (V, E)$ wird als bipartit bezeichnet, wenn V in zwei disjunkte Mengen V_1 und V_2 von Knoten getrennt werden, $V = V_1 \cup V_2$, so dass keine Kante zwei Knoten im gleichen Subgraph verbindet.

Isomorphismus

Zwei Graphen $G = (V, E)$ und $H = (V', E')$ sind isomorph, geschrieben $G \cong H$, wenn eine Bijektion $\pi : V \to V'$ so dass, das umbennen der Knoten von G nach π in H resultiert, oder umgekehrt.

Spezielle Graphen

Ein *kompletter Graph* von n Knoten, geschrieben K_n ist ein Graph in dem jedes Paar von Knoten verbunden ist. Das Komplementär von K_n ist der leere Graph.

Ein *(m,n)-Gittergraph* ist ein ein Graph Mm, n von mn Knoten mit $V = \{(i, j) | 1 \leq i \leq m, 1 \leq j \leq n\}$ und wo (i, j) und (i', j') nur verbunden sind, wenn $i = i'$ und $\mid j - j' \mid = 1$ oder $j = j'$ und $\mid i - i' \mid = 1$.

Ein *Pfad* P_n (Pfad der Länge n) besteht aus n+1 Knoten.

Ein *Zyklus* C_n besteht aus n Knoten die zyklisch verbunden sind.

Ein *komplett bipartiter Graph* $K_{m,n}$ ist ein Graph mit m+n Knoten, der aus zwei Teilmengen B und W der Grösse m bzw. n besteht und der jeden Knoten von B mit jedem Knoten von W verbindet, die aber nicht untereinander verbunden sind.

Adjazenzmatrix

Die *Adjazenzmatrix* $A_G = [a_{ij}]$ eines nicht orientierten Graphen $G = (V, E)$ mit $V = \{v_1, \ldots, v_n\}$ ist die binäre $n \times n$ Matrix wobei $(a_{i,j}) = 1$ falls $\{v_i, v_j\} \in E$, sonst 0.

4.2 Pfade und Kreise

Ein *Weg* von u nach v der Länge n in einem (orientierten) Graph ist eine Reihe $(u, v_1, \ldots, v_{n-1}, v)$ von Knoten so dass aufeinanderfolgende Knoten verbunden sind. Wenn die Knoten verschieden sind, wird es als *Pfad* bezeichnet und wenn alle Kanten im Pfad verschieden sind, wird es als *Tour* bezeichnet. Wenn der Start- und Endpunkt der gleiche ist wird der Pfad als *Kreis* und eine Tour als Schleife bezeichnet.

Hamiltonscher Kreis

Ein Kreis in einem Graph wird als hamiltonsch bezeichnet wenn er alle Knoten besucht.

Theorem
Ein Graph $G = (V, E)$ für welche für alle nicht verbundenen Paare (u,v) von Knoten gilt, dass $deg(u) + deg(v) \geq \mid V \mid$ ist hamiltonsch. Im einzelnen falls $deg(v) \geq \mid V \mid /2$ für alle $v \in V$.

Graucodes

Es ändert sich nur ein Bit.

Ein Hyperkubus Q_d ist hamiltonsch für $d \geq 2$.

Ein hamiltonscher Kreis in einem Hyperkubus wird als Graucode bezeichnet.

Euler Kreise

Ein Eulerkreis (Eulerpfad) in einem Graph ist ein Kreis (Pfad) der alle Kanten des Graphes beeinhaltet.

Theorem
Ein nichtorientierter Graph ist eulerisch, falls jeder Knoten einen geraden Grad hat. Ein orientierter Graph ist eulerisch falls für jeden Knoten gilt, dass die In-Grade gleich den Out-Graden sind.

4.3 Bäume

Ein Baum ist ein verbundener Graph ohne Zyklus. Ein Wald ist ein Graph ohne Zyklen, die Vereinigung von verschiedenen Bäumen mit disjunkten Knotenmengen. Ein Blatt ist ein Knoten mit Grad 1.

Lemma
Ein Baum mit $m \geq 2$ Knoten hat mindestens 2 Blätter.

Theorem
Für einen Graphen G mit m Knoten, sind die folgenden Aussagen äquivalent:

1. G ist ein Baum
2. G hat m-1 Kanten und keine Zyklen
3. G hat m-1 Kanten und ist verbunden

Ein *Spannbaum* eines verbundenen Graphen G ist ein Subgraph von G welcher ein Baum ist und alle Knoten von G enthält.

4.4 Planare Graphen

Definition

Ein Graph ist planar, falls er in der Ebene so gezeichnet werden kann, dass sich keine Kanten kreuzen.

Die Graphen K_4 und $K_{2,3}$ sind planar. K_5 und $K_{3,3}$ sind es nicht. Der Hyperkubus Q_d ist nur planar, falls $d \leq 3$.

Euler's Formeln und Bedingungen für Planarität

Ein planarer Graph unterteilt die Ebene in disjunkte *Regionen*, eine davon ist unendlich. Der Grad einer Region ist die Anzahl Kanten von denen sie begrenzt wird.

Theorem
Jeder verbundene Graph $G = (V, E)$ unterteilt die Ebene in $r :=\mid E \mid - \mid V \mid +2$ Regionen.

Lemma
Für jeden verbundenen Graphen $G = (V, E)$, ist die Summe der Grade der Regionen gleich $2 \mid E \mid$.

Theorem
Jeder verbundene planare Graph $G = (V, E)$ mit $\mid V \mid \geq 3$ erfüllt: $\mid E \mid \leq 3 \mid V \mid -6$. Wenn G bipartit ist, dann gilt: $\mid E \mid \leq 2 \mid V \mid -4$.

Korollar
K_n ist nur planar, wenn $n \leq 4$

Korollar
$K_{3,3}$ ist nicht planar.

Kuratowski's Theorem

Ein Graph H ist eine Untereinheit eines Graphen G, falls H aus G erhalten werden kann, wenn man neue Knoten auf Kanten von G einfügt.

Lemma
Wenn ein Graph eine Untereinheit eines nicht-planaren Graphen enthält, dann ist er nicht-planar.

Theorem (Kurotowski)
Ein Graph ist nur planar falls er keine Untereinheit von K_5 oder $K_{3,3}$ enthält.

Reguläre Polyeder

Ein Polyeder ist regülar wenn für irgendwelche $m, n \geq 3$ jeder Knoten genau m Flächen (und es folgt m Kanten) und jede Fläche ist ein reguläres n-gon.

Theorem
Es gibt genau fünf regelmässige Polyeder, wobei (m,n) (3,3), (3,4), (4,3), (3,5) oder (5,3) ist.

4.5 Graphenfärbung

Definition
Einen Graphen $G = (V, E)$ zu färben (*Knotenfärbung*) heisst die Knotenmenge V in k Mengen zu unterteilen, so dass keine zwei Knoten der gleichen Farbe verbunden sind. Eine solche Färbung wird als k-Färbung bezeichnet. Die chromatische Nummer $\chi(G)$ von G ist die Färbung mit minimalem k.

Lemma
Wenn $G \preceq H$, dann gilt $\chi(G) \leq \chi(H)$.

Theorem
$\chi(G) \leq 4$ für jeden planaren Graphen G.

Definition
Einem Graphen G die *Kanten zu färben* bedeutet, dass sich keine gleichfarbigen Kanten in einem Knoten treffen dürfen. Die minimale Anzahl Farben wird durch $\chi'(G)$ bezeichnet.

Theorem

1. Wenn d der maximale Index eines Graphen ist, so ist $\chi'(G) = d$ oder $\chi'(G) = d+1$. Für bipartite Graphen gilt $\chi'(G) = d$.
2. $\chi'(K_n) = n$ wenn n ungerade ist $\chi'(K_n) = n-1$ wenn n gerade ist.

5 Zahlentheorie

5.1 Die ganzen Zahlen: Axiome und Grundlagen

Die Menge der ganzen Zahlen $\mathbb{Z}$ ist eine Menge mit zwei Operationen, Addition $(+)$ und Multiplikation $(\cdot)$ und einer Ordnungsrelation $(\leq)$.

Addition und Multiplikation

Axiome Die folgenden Gleichungen halten für alle $a, b, c \in \mathbb{Z}$.

I1. Kommutativität von + und ·

1. $a + b = b + a$
2. $ab = ba$

I2. Assoziativität von + und ·

1. $(a + b) + c = a + (b + c)$
2. $(ab)c = a(bc)$

I3. Existenz eines Neutralelements für + und ·

1. Es existiert $0 \in \mathbb{Z}$ so dass $a + 0 = a$ für alle a

2. Es existiert $1 \in \mathbb{Z}$ so dass $a \cdot 1 = a$ für alle a

I4. Distributivität von $\cdot$ über $+$

1. $a(b+c) = ab + ac$

I5. Existenz von Negativen
Für jedes $a \in \mathbb{Z}$ existiert $-a \in \mathbb{Z}$, so dass $a + (-a) = 0$

I6. Keine Nicht-Null Nullteiler
$ab = 0 \Rightarrow a = 0 \vee b = 0$

5.2 Diskussion der Axiome

Axiom I7: Es gibt eine Zahl die nicht Null ist. $\exists a : a \neq 0$

Lemma: $1 \neq 0$

5.3 Einfache Fakten

Das folgende Theorem gilt für irgendeinen Integritätsbereich, 1., 2. und 3. gelten für jeden kommutativen Ring, da wir nur Axiome **I1** bis **I5** benutzen.

Theorem Die folgenden Aussagen gelten für irgendwelche ganzen Zahlen a,b,c:

1. Aufhebungsgesetz für $+$: $a + b = a + c \Rightarrow b = c$
2. Eigenschaften von 0
   a) 0 ist eindeutig
   b) $-0 = 0$
   c) $0a = a0 = 0$
3. Eigenschaften von Negativen
   a) -a ist eindeutig für ein gegebenes a
   b) $(-a)b = -ab$
   c) $(-a)(-b) = ab$
4. 1 ist eindeutig, wenn ab=a für alle a, dann ist b=1
5. Aufhebungsgesetz für $\cdot$: $a \neq 0 \wedge ab = ac \Rightarrow b = c$

Die Ordnungsrelation

Axiom Es gibt eine Ordnungsrelation $\leq$ auf $\mathbb{Z}$ so dass für alle $a, b, c \in \mathbb{Z}$ gilt:

I8 $a \leq b \Rightarrow a + c \leq b + c$

I9 $a \leq b \wedge 0 \leq c \Rightarrow ac \leq bc$

I10 Die nicht-negativen Zahlen, $\mathbb{N} = \{n \in \mathbb{Z} | 0 \leq n\}$, sind strikt geordnet durch $\leq$. Jeder nicht-leere Untermenge S von $\mathbb{Z}$ hat mindest ein kleinstes Element $z \in S$.

Theorem Die folgenden Aussagen gelten für alle ganzen Zahlen $a, b, c \in \mathbb{Z}$:

1. $0 \leq a \Rightarrow -a \leq 0$
2. $a \leq b \wedge c \leq 0 \Rightarrow bc \leq ac$
3. $0 \leq a^2$
4. $0 \leq 1$ (da $0 < 1$)
5. Es gibt keine ganze Zahl zwischen 0 und 1. $\nexists a : 0 < a < 1$
6. Die ganzen Zahlen $1, 1+1, 1+1+1, \ldots$ sind alle disjunkt, darum gibt es unendlich viele Integers.

$| a | \cdot | b | = | ab |$ und $| a + b | \leq | a | + | b |$

Axiom I11 Alle Zahlen sind mit 0 vergleichbar:$\forall a : a \leq 0 \vee 0 \leq a$

5.4 Teiler und Division

Teiler

Für Integers a und b mit $a \neq 0$ sagen wir dass a b teilt, geschrieben $a|b$, wenn eine Zahl c existiert, so dass $b = ac$.

Lemma Wenn $a|b$, dann ist der Integer c mit $b = ac$ eindeutig und wird geschrieben als $c = \frac{b}{a}$

Theorem a,b and c sind Integers:

1. Wenn $a|b$ und $b|c$ dann $a|c$
2. Wenn $a|b$, dann $a|bc$ für alle Integers c
3. Wenn $a|b$ und $a|c$, dann $a|(b+c)$
4. Wenn $a|b$ und $c|(b/a)$, dann $c|b$ und $a|(b/c)$
5. Die einzigen Teiler von 1 sind 1 und -1
6. Wenn $a|b$ und $b|a$, dann a=b oder a=-b

Division mit Rest

Theorem (Euklid)
Für alle Integer a und $d \neq 0$ existiert eindeutige Integers a und r die erfüllen:
$a = dq + r$ und $0 \leq r \leq | d |$
Dabei wird a als Dividend, d als Divisor, q als Quotient und r als Rest bezeichnet. Der Rest r wird oft geschrieben als $R_d(a)$ oder $amodd$.

Grösste gemeinsame Teiler

Definition Für gegebene Integers a und b, das Ideal generiert von a und b, geschrieben (a, b) ist die Menge
$(a, b) := \{ua + vb | u, v \in \mathbb{Z}\}$
Ähnlich gilt für eine einzige Ganzzahl:
$(a) := \{ua | u \in \mathbb{Z}\}$ Es gilt z.Bsp.: $(4, 6) = (2)$, $(3, 7) =$

(1)

Lemma Für $a, b \in \mathbb{Z}$ (nicht beide 0), existiert $d \in \mathbb{Z}$, so dass $(a, b) = (d)$

Definition Für Integers a und b (nicht beide 0), ein Integer d wird als grösster gemeinsamer Teiler d von a und b bezeichnet, falls jeder gemeinsame Teiler von a und b d teilt, also $d|a$, $d|b$ und $c|a \wedge c|b \Rightarrow c|d$.

Lemma $a, b \in \mathbb{Z}$. Wenn $(a, b) = (d)$ dann ist d der grösste gemeinsame Teiler von a und b, anders geschrieben $gcd(a, b) = ua + vb$ für $u, v \in \mathbb{Z}$.

Definition Wenn $gcd(a, b) = 1$ dann sind a und b relativ prim oder coprim.

Euklid's erweiterter GCD Algorithmus

Euklid GCD Algorithmus
$\sigma_1 := a$; $\sigma_2 := b$;
$u_1 := 1$; $u_2 := 0$;
$v_1 := 0$; $v_2 := 1$;
while $\sigma_2 > 0$ **do begin**
$q :=$ σ_1 **div** σ_2;
$r := \sigma_1 - q\sigma_2$;
$\sigma_1 := \sigma_2$; $\sigma_2 := r$;
$t := u_2$; $u_2 := u_1 - qu_2$; $u_1 := t$;
$t := v_2$; $v_2 := v_1 - qv_2$; $v_1 := t$;
end;
$d := \sigma_1$; $u = u_1$; $v := v_1$

Theorem Dieser Algorithmus berechnet für gegebene nichtnegative a und b mit $a \geq b$ (nicht beide 0), die Integers $d = gcd(a, b)$, wie auch u und v, die $ua + vb = gcd(a, b)$ erfüllen.

5.5 Faktorisierung in Primzahlen

Das Fundamentale Theorem der Arithmetik

Definition Eine positive Ganzzahl p ¿ 1 wird als prim bezeichnet, falls alle positiven Divisoren von p 1 und p sind. Alle Integer grösser 1 welche nicht prim sind werden als composite bezeichnet. 1 ist weder prim noch composite.

Theorem Wenn p eine Primzahl ist, welche das Produkt $x_1 x_2 \cdots x_n$ von Integers $x_1, \ldots, x_n$ teilt, dann teilt p eine davon, $p|x_i$ für $i \in \{1, \ldots, n\}$

Theorem Jede positive Ganzzahl kann eindeutig (bis auf die Ordnung der Faktoren) als das Produkt von Primzahlen geschrieben werden.

Irrationalität von Wurzeln

Theorem $\sqrt{2}$ ist irrational.

Kleinste gemeinsame Vielfache

Definition Das kleinste gemeinsame Vielfache l von zwei positiven Integers a und b, geschrieben $l = lcm(a, b)$ oder $[a, b]$, ist das gemeinsame Vielfache von a und b welches jedes gemeinsame von a und b teilt, $a|l$, $b|l$ und $a|l' \wedge b|l' \Rightarrow l|l'$.

$a = \prod_i p_i^{e_i}$ und $b = \prod_i p_i^{f_i}$
$(a, b) = gcd(a, b) = \prod_i p_i^{min(e_i, f_i)}$
$[a, b] = lcm(a, b) = \prod_i p_i^{max(e_i, f_i)}$

$gcd(a, b) \cdot lcm(a, b) = ab$
$(a, b, c)[ab, ac, bc] = abc$
$(a, [b, c]) = [(a, b), (a, c)]$ und $[a, (b, c)] = ([a, b], [a, c])$
$([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)]$

5.6 Grundlegendes über Primzahlen

Dichte von Primzahlen

Theorem Es gibt unendlich viele Primzahlen.

Theorem Lücken zwischen Primzahlen können willkürlich gross sein, für jedes $k \in \mathbb{N}$ existiert ein $n \in \mathbb{N}$, so dass die Menge $\{n, n+1, \ldots, n+k-1\}$ keine Primzahl beinhaltet.
Definition Die Primzahlzählfunktion $\pi : \mathbb{R} \to \mathbb{N}$ wird wiefolgt definiert: Für jede reelle Zahl x ist $\pi(x)$ gleich der Anzahl Primzahlen, die kleiner oder gleich x sind.

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

Bemerkungen zum Primzahltesten

Theorem Jede composite Integer n hat einen primen Divisor $\leq \sqrt{n}$

5.7 Kongruenzen und modulare Arithmetik

modulare Kongruenz

Definition Für $a, b, m \in \mathbb{Z}$ mit $m \geq 1$, sagen wir dass a kongruent zu b modulo m ist, wenn m a-b dividiert. Wir schreiben $a \equiv_m b \Leftrightarrow m|(a - b)$

Lemma Für $m \geq 1$, $\equiv_m$ ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Lemma Wenn $a \equiv_m b$ und $c \equiv_m d$, dann $a + c \equiv_m b + d$ und $ac \equiv_m bd$.

Korollar $f(x_1, \ldots, x_k)$ ist ein Polynomal mit k Variablen und Integer Koeffizienten, und $m \geq 1$. Wenn $a_i \equiv_m b_i$ für $1 \leq i \leq k$, dann $f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$.

Modulare Arithmetik

Es gibt m Äquivalenzklassen von der Äquivalenzrelation $\equiv_m$, nämlich $[0], [1], \ldots, [m-1]$. Jede Äquivalenzklasse $[a]$ hat einen Represäntant $R_m(a) \in [a]$ in der Menge $Z_m := \{0, \ldots, m-1\}$.

Lemma $a, b, m \in \mathbb{Z}$ mit $m \geq 1$.

1. $a \equiv_m R_m(a)$
2. $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$

Lemma $a, b, m \in \mathbb{Z}$ mit $m \geq 1$

1. $R_m(a+b) = R_m(R_m(a) + R_m(b))$
2. $R_m(ab) = R_m(R_m(a) \cdot R_m(b))$

Die Kongruenz $ax \equiv_m b$ und multiplikative Inverse

Lemma Wenn $gcd(a, m) = 1$, dann gibt es eine eindeutige Lösung x zu der Kongruenzgleichung $ax \equiv_m 1$.

Definition Die eindeutige Lösung x der Kongruenzgleichung $ax \equiv_m 1$ wird als multiplikatives Inverserses von a modulo m bezeichnet. Es wird auch die Notation $x \equiv_m a^{-1}$ oder $x \equiv_m 1/a$ benutzt.

Lemma Die Kongruenzgleichung $ax \equiv_m b$ hat $d = gcd(a, m)$ Lösungen in $\mathbb{Z}_m$ wenn $d|b$ und Null Lösungen, wenn $d \not| b$.

Der chinesische Restwertsatz

Theorem $m_1, m_2, \ldots, m_r$ paarweise relative Primzahlen und $M = \prod_{i=1}^{r} m_i$. Für jede Liste $a_1, \ldots, a_r$ mit $0 \leq a_i < m_i$ für $1 \leq i \leq r$, das System von Kongruenzgleichungen

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &\cdots \\ x &\equiv_{m_r} a_r \end{aligned}$$

für x hat eine eindeutige Lösung x für welche gilt $0 \leq x < M$.
$M_i = M/m_i$ $M_i N_i \equiv_{m_i} 1$
$\Rightarrow x = R_M(\sum_{i=1}^{r} a_i M_i N_i)$

5.8 Einige Anwendungen

Diffie-Hellman Protokoll

Alice	**insecure channel**	**Bob**
wähle x_A zufällig aus $\{0, \ldots, p-2\}$		wähle x_B zufällig aus $\{0, \ldots, p-2\}$
$y_A := R_p(g^{x_A})$		$y_B := R_p(g^{x_B})$
	$\rightarrow y_A$	
	$y_B \leftarrow$	
$k_{AB} := R_p(y_B^{x_A})$		$k_{BA} := R_p(y_A^{x_B})$

$$k_{AB} \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p g^{x_A x_B} \equiv_p k_{BA}$$

6 Algebra

6.1 Einführung

Algebraische Systeme

Definition Eine *Operation* auf eine Menge S ist eine Funktion $S^n \rightarrow S$, wobei $n \geq 0$ als arity der Operation bezeichnet wird..

Definition Eine Algebra ist ein Paar $\langle S; \Omega \rangle$, wobei S eine Menge und Ω eine Liste von Operationen auf S ist.

Definition Der Typ einer Algebra $\langle S; \Omega \rangle$ ist die Liste von Arities von den Operationen.

Beispiele:

1. $\langle \mathbb{Z}; +, \cdot, -, 0, 1 \rangle$
2. $\langle \mathbb{Z}_m; \oplus \rangle$ Integers modulo m mit Addition modulo m als einziger binären Operation. Wir können auch $\langle \mathbb{Z}_m; \oplus, 0 \rangle$ schreiben, der Typ davon wäre $(2, 0)$.

6.2 Halbgruppen, Monoide, Gruppen

Neutralelemente

Definition Ein links [rechts] neutrales Element einer Algebra $\langle S; * \rangle$ ist ein Element $e \in S$, so dass $e * a = a$ $[a * e = a]$ für alle $a \in S$. Wenn $e * a = a * e = a$ für alle $a \in S$, dann wird e einfach als Neutralelement bezeichnet.

Lemma Wenn $\langle S; * \rangle$ ein links und ein rechts neutrales Element hat, so sind sie gleich. Da $\langle S; * \rangle$ höchstens ein Neutralelement haben kann.

Assozitivität, Halbgruppen und Monoide

Definition Eine *Halbgruppe* ist eine Algebra $\langle S; * \rangle$ welche das Assoziativitätsgesetz erfüllt: $a * (b * c) = (a * b) * c$ für alle $a, b, c \in S$. Beispiele von Halbgruppen sind: $\langle \mathbb{Z}; + \rangle, \langle \mathbb{Z}; \cdot \rangle, \langle \mathbb{Q}; + \rangle, \langle \mathbb{Q}; \cdot \rangle, \langle \mathbb{R}; + \rangle, \langle \mathbb{R}; \cdot \rangle, \langle \mathbb{Z}_m; \oplus \rangle, \langle \mathbb{Z}_m; \odot \rangle$.

Lemma Das Element $a_1 * a_2 * \ldots * a_n$ $(a_1, \ldots, a_n \in S)$ in einer Halbgruppe $\langle S; * \rangle$ ist eindeutig definiert und unabhängig von der Ordnung in welcher die Elemente kombiniert werden.

Definition Ein Monoid ist eine Algebra $\langle M; *, e \rangle$, so dass $\langle M; * \rangle$ eine Halbgruppe ist mit einem Neutralelement e.

Inverse und Gruppen

Definition Ein links [rechts] inverses Element eines Elementes a in einer Algebra $\langle S; *, e\rangle$ mit Neutralelement e ist ein Element $b \in S$, so dass $b * a = e$ $[a * b = e]$. Wenn $b * a = a * b = e$, dann wird b einfach als Inverses von a bezeichnet

Lemma in einem Monoid $\langle M; *, e\rangle$, wenn $a \in M$ eine links und rechts Inverse hat, so sind sie gleich. a hat höchstens eine Inverse.

Definition Eine *Gruppe* ist eine Algebra $\langle G; *, \hat{}, e$ (vom Typ $(2, 1, 0)$) so dass $\langle G; *, e\rangle$ ein Monoid ist und jedes Element a ein inverses Element $\hat{a}$ besitzt.

Gruppenaxiome: $\langle G; *\rangle$ ist eine Gruppe, wenn $*$ eine Operation auf G ist, so dass:

G1 $*$ ist assoziativ

G2 Es existiert ein Neutralelement e, so dass $a * e = e * a = a \forall a \in G$

G3 Jedes $a \in G$ ein Inverses Element $\hat{a}$ besitzt, $a * \hat{a} = \hat{a} * a = e$

Für eine gegebene Struktur R, die Addition und Multiplikation unterstützt, beschreibt $R[x]$ die Menge der Polynome mit Koeffizienten in R. $\langle \mathbb{Z}[x]; +\rangle$, $\langle \mathbb{Q}[x]; +\rangle$ und $\langle \mathbb{R}[x]; +\rangle$ sind abelsche Gruppen, wobei + die polynmielle Addition ist. $\langle \mathbb{Z}[x]; \cdot\rangle$, $\langle \mathbb{Q}[x]; \cdot\rangle$ und $\langle \mathbb{R}[x]; \cdot\rangle$ sind abelsche Monoide, das NE ist das Polynom 1.

Definition Eine Gruppe $\langle G; *\rangle$ (oder Monoid oder Halbgruppe) wird als kommutativ oder abelsch bezeichnet, falls $*$ kommutativ ist, $a * b = b * a \forall a, b \in G$.

Lemma Für eine Gruppe $\langle G; *, \hat{}, e\rangle$, gilt für alle $a, b, c \in G$:

1. $\widehat{(\hat{a})} = a$
2. $\widehat{a * b} = \hat{b} * \hat{a}$
3. Linksaufhebungsgesetz: $a * b = a * c \Rightarrow b = c$.
4. Rechtsaufhebungsgesetz: $b * a = c * a \Rightarrow b = c$.
5. Die Gleichung $a * x = b$ hat eine eindeutige Lösung für irgendein a und b. So auch die Gleichung $x * a = b$.

Direkte Produkte

Definition $\langle S_1; \Omega_1\rangle, \ldots, \langle S_n; \Omega_n\rangle$ sind n Algebren vom gleichen Typ. Ihr direktes Produkt ist die Algebra $\langle S; \Omega\rangle$ vom selben Typ, wobei $S = S_1 \times \ldots \times S_n$ und wobei jede Operation $\omega \in \Omega$ komponentenweise fur die i-te Komponente die dazugehörige Operation in $\langle S_i; \Omega_i\rangle$.

Definition Das direkte Produkt von n Gruppen $\langle G_1; *_1, \hat{}^{(1)}, e_1\rangle, \ldots, \langle G_n; *_n, \hat{}^{(n)}, e_n\rangle$
ist die Algebra
$\langle G_1 \times \cdots \times G_n; \star, \hat{}, (e_1, \ldots, e_n)\rangle$
wobei
$(a_1, \ldots, a_n) \star (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n)$
und $\widehat{(a_1, \ldots, a_n)} = (\hat{a_1}^{(1)}, \ldots, \hat{a_n}^{(n)})$.

Unteralgebren und Untergruppen

Definition Eine Untermenge T von S wird als abgeschlossen unter einer n-ären Operation ω auf S bezeichnet, falls $a_1, \ldots, a_n \in T \Rightarrow \omega(a_1, \ldots, a_n) \in T$.

Definition $\langle S; \Omega\rangle$ ist eine Ω-Algebra. Eine Untermenge T von S ist eine Ω-Unteralgebra von $\langle S; \Omega\rangle$, geschrieben $\langle T; \Omega\rangle \leq \langle S; \Omega\rangle$ oder einfach $T \leq S$, wenn T abgeschlossen ist unter allen $\omega \in \Omega$.

Definition Eine Subalgebra einer Gruppe (Halbgruppe, Monoid etc.) wird als Untergruppe (Unterhalbgruppe, Untermonoid etc.), wenn es selber eine Gruppe (Halbgruppe, Monoid etc.) ist.

Definition Gegeben eine Algebra $\langle S; \Omega\rangle$ und eine Untermenge $T \subseteq S$ von S, die Unteralgebra generiert bei T, geschrieben $\langle T\rangle$, ist der Abschluss von T unter allen Operationen in Ω. Wenn $T = \{t_1, \ldots, t_k\}$ schreiben wir auch $\langle t_1, \ldots, t_k\rangle$ statt $\{\langle t_1, \ldots, t_k\rangle\}$.

Lemma Für eine Gruppe $\langle G; *, \hat{}, e\rangle$ und eine Untermenge $H \subseteq G$ (mit $H \neq \emptyset$), $\langle H; *, \hat{}, e\rangle$ ist eine Untergruppe von $\langle G; *, \hat{}, e\rangle$ wenn $a * \hat{b} \in H \, \forall a, b \in H$.

Isomorphismus

Definition Zwei Algebren $\langle S; \Omega\rangle$ und $\langle S'; \Omega'\rangle$ vom selben Typ sind *isomorph*, geschrieben $\langle S; \Omega\rangle \cong \langle S'; \Omega'\rangle$ wenn eine Bijektion $\psi : S \to S'$ existiert, so dass für jede n-äre Operation $\omega \in \Omega$ und dazugehörende $\omega' \in \Omega'$ $\psi(\omega(a_1, \ldots, a_n)) = \omega'(\psi(a_1), \ldots, \psi(a_n))$.

Die Ordnung von Elementen

$n \in \mathbb{Z}$, a^n ist rekursiv definiert als:

- $a^0 = e$
- $a^n = a \cdot a^{n-1}$
- $a^n = (a^{-n})^{-1} = (a^{-1})^n$ für $n \leq -1$

$a^m \cdot a^n = a^{m+n}$ und $(a^m)^n = a^{mn}$.

Definition G eine Gruppe und a ein Element von G, die Ordnung von a, geschrieben $ord(a)$, ist das kleinste $m \geq 1$, so dass $a^m = e$, wenn ein solches m existiert, sonst $ord(a) = \infty$. Bei Definition: $ord(e) = 1$. Wenn $ord(a) = 2$ für ein a, dann $\hat{a} = a$.

Lemma In einer endlichen Gruppe G hat jedes Element eine endliche Ordnung.

Lemma Wenn G eine Gruppe ist und $a \in G$ endliche Ordnung hat, dann gilt für $m \in \mathbb{Z}$: $a^m = a^{R_{ord(a)}(m)}$ und ausserdem ist $\langle a \rangle = \{e, a, a^2, \ldots, a^{ord(a)-1}\}$ die kleinste Untergruppe von G, die a enthält und ist abelsch.

Definition Eine Gruppe $G = \langle g \rangle$ generiert bei einem Element $g \in G$ wird als zyklisch bezeichnet und g wird als Generator von G bezeichnet.

Lemma Eine zyklische Gruppe der Ordnung n ist isomorph zu $\langle \mathbb{Z}_n, \oplus \rangle$ (und folglich abelsch) und hat $\varphi(n)$ Generatoren.

Nebengruppen und Lagrange's Theorem

Definition G eine Gruppe, $H \leq G$ eine Untergruppe von G und $a \in G$. Die Menge $H * a := \{h * a | h \in H\}$ wird als rechte Nebengruppe und ähnlich wird $a * H := \{a * h | h \in H\}$ als linke Nebengruppe von H bezeichnet. Wenn G abelsch ist, dann $a * H = H * a$, welche als Nebengruppe bezeichnet wird.

Lemma G eine Gruppe, $H \leq G$ eine Untergruppe von G, dann gilt:

1. H ist selber eine rechte/linke Nebengruppe von H.
2. Irgendwelche zwei rechte/linke Nebengruppen sind entweder gleich oder disjunkt.
3. Wenn H endlich, dann haben alle Nebengruppen gleiche Kardinalität $|H|$.

Definition Für eine endliche Gruppe G, wird $|G|$ als die Ordnung der Gruppe bezeichnet.

Theorem G eine endliche Gruppe und $H \leq G$ eine Untergruppe von G. Dann teilt die Ordnung von H die Ordnung von G, $|H|$ teilt $|G|$.

Korollar G eine endliche Gruppe. Dann teilt $ord(a)$ $|G|$ $\forall a \in G$.

Korollar G eine endliche Gruppe. Dann $a^{|G|} = e$ $\forall a \in G$.

Korollar Jede Gruppe mit primer Ordnung ist zyklisch und jedes Element ausser e ist ein Generator.

Die Gruppe $\mathbb{Z}_m^*$

Definition $\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m | gcd(a, m) = 1\}$. Die Eulerfuktion $\varphi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ ist definiert als die Kardinalität von $\mathbb{Z}_m^*$: $\varphi(m) = |\mathbb{Z}_m^*|$.

Lemma Wir haben $\varphi(m) = m \cdot \prod_{p|m} (1 - \frac{1}{p})$. (p prim). Äquivalent, wenn $m = \prod_{i=1}^{r} p_i^{e_i}$, dann $\varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$

Lemma $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ ist eine Gruppe.

Lemma $\langle \mathbb{Z}_m - \{0\}; \odot, ^{-1}, 1 \rangle$ ist eine Gruppe wenn und nur wenn m prim ist.

Korollar (Fermat,Euler) Für alle $m \geq 2$ und alle a mit $gcd(a, m) = 1$, $a^{\varphi(m)} \equiv_m 1$. Im speziellen, für jede Primzahl p und jedes a, dass nicht durch p teilbar ist $a^{p-1} \equiv_p 1$.

Theorem Die Gruppe $\mathbb{Z}_m^*$ ist zyklisch wenn und nur wenn $m = 2, m = 4, m = p^e$ oder $m = 2p^e$, wobei p eine ungerade Primzahl ist und $e \geq 1$.

Theorem Jede abelsche Gruppe G ist isomorph zu einem direkten Produkt einer Liste von zyklischen Gruppen, wobei die Ordnung von jeder Gruppe die Ordnung der in der Liste nachfolgenden Gruppe teilt.

RSA Public-Key

Theorem G eine endliche Gruppe (mit Neutralelement 1) und $e \in \mathbb{Z}$ ein gegebener Exponent, der relativ zu $|G|$ prim ist ($gcd(e, |G|) = 1$). Die (eindeutige) e-te Wurzel von $y \in G$, namentlich $x \in G$ befriedigend $x^e = y$, kann ausgerechnet werden gemäss
$x = y^d$,
wobei d das multiplikative Inverse von e modulo $|G|$ ist,
$d \equiv_{|G|} e^{-1}$.

Alice	**insecure channel**	**Bob**
Generiere Primzahlen p und q $m = p \cdot q$, $f = (p-1)(q-1)$		
wähle e, $d \equiv_f e^{-1}$	$\rightarrow m, e$	Klartext $x \in \{1, \ldots, m-1\}$
$x = R_m(y^d)$	$y \leftarrow$	Verschlüsselt $y = R_m(x^e)$

6.3 Ringe und Körper

Definition einer Ringes

Definition Ein Ring $\langle R; +, -, 0, \cdot, 1 \rangle$ ist ein algebraisches System für welches gilt:

1. $\langle R; +, -, 0 \rangle$ ist eine abelsche Gruppe
2. $\langle R; \cdot, 1 \rangle$ ist ein Monoid
3. $a(b+c) = ab + ac$ und $(b+c)a = ba + ca$ für alle $a, b, c \in R$ (links und rechts distributiv)

Ein Ring wird als kommutativ bezeichnet, falls die Multiplikation kommutativ ist ($ab = ba$). Das

multiplikative Neutralelement 1 wird als Einheit von R bezeichnet.

Theorem Für jeden Ring $\langle R; +, -, 0, \cdot, 1\rangle$ gilt:

1. $0a = a0 = 0 \, \forall a \in R$
2. $(-a)b = -ab$
3. $(-a)(-b) = ab$
4. Wenn R mehr als ein Element hat, dann ist $1 \neq 0$

Integritätsbereich und Körper

Definition Ein Element $a \neq 0$ eines Ringes R wird als Nullteiler bezeichnet, wenn $ab = 0$ für ein $b \neq 0 \in R$.

Defintion Ein Element $u \neq 0$ von einem Ring wird als Einheit bezeichnet, wenn u invertierbar ist (uv=1 für $v \in R \, (v = u^{-1})$). Die Menge der Einheiten von R wird geschrieben als $U(R)$.

Lemma Für ein Ring R ist $U(R)$ eine multiplikative Gruppe.

Definition Ein Integritätsbereich ist ein nichttrivaler kommutativer Ring ohne Nullteiler: $ab = 0 \Rightarrow a = 0 \vee b = 0$.

Definition Ein Polynom $a(x)$ über einem Ring R in welchen das unbestimmte x ein formaler Ausdruck der Form $a(x) = \sum_{i=0}^{n} a_i x^i$ ist, für positive Integer n. Wir schreiben die Menge der Polynome (in X) über R als $R[x]$.

Lemma Wenn R ein Ring ist, dann ist $R[x]$ auch ein Ring. Die Einheiten von $R[x]$ sind die konstanten Polynome welche Einheiten von R sind.

Lemma Wenn D ein Integritätsbereich ist, so ist es auch $D[x]$.

Definition Ein *Körper* ist ein nichttrivaler, kommutativer Ring F in welchem jedes nicht-Null Element eine Einheit ist, in anderen Worten so, dass $\langle F - \{0\}; \cdot, ^{-1}, 1\rangle$ eine abelsche Gruppe ist.

Theorem $\mathbb{Z}_m$ ist ein Körper wenn und nur wenn m prim ist.

Lemma Ein Körper ist ein Integritätsbereich.

Quotientenkörper

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

Theorem Für ein Integritätsbereich D, $Q(D)$ mit Addition und Multiplikation wie oben ist ein Körper, wobei $0 = 0/1$, $1 = 1/1$, $-(a/b) = (-a)/b$ und $(a/b)^{-1} = b/a$ (wenn $a \neq 0$).

6.4 Polynome über einem Körper

$a(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$

Der Grad $deg(a(x))$ von $a(x)$ ist das kleinste i für welches $a_i \neq 0$. Das spezielle Polynom 0 hat Grad "minus unendlich".

Teilbarkeitseigenschaft in $F[x]$

Theorem F sei ein Körper. Für irgendein $a(x)$ und $b(x) \neq 0$ in $F[x]$ existiert ein eindeutiges $q(x)$ (der Quotient) und $r(x)$, so dass
$a(x) = b(x)q(x) \cdot + r(x)$ und $deg(r(x)) < deg(b(x))$

Der Körper mit p Elementen wird geschrieben als $GF(p)$

Teiler und Irreduzible Polynome

Definition F ein Körper. Für $a(x), b(x) \in F[x]$, $b(x)$ teilt $a(x)$, geschrieben $b(x)|a(x)$, wenn $a(x) = b(x) \cdot c(x)$ für ein $c(x) \in F[x]$.

Definition Ein Polynom $a(x) \in F[x]$ wird als *monic* bezeichnet, wenn der führende Koeffizient 1 ist.

Definition Ein Polynom $a(x) \in F[x]$ wird als *irreduzibel* bezeichnet, wenn es nur von konstanten Polynomen und konstanten Vielfachen von $a(x)$ geteilt wird.

Polynome als Funktionen

Ein Polynom $a(x) \in F[x]$ kann als Funktion $F \to F$ interpretiert werden, wenn wir die Auswertung von $a(x)$ in $\alpha \in F$ in gewohnter Weise definieren. Dies definiert eine Funktion $F \to F : \alpha \mapsto a(\alpha)$.

Definition $a(x) \in F[x]$. Ein Element $\alpha \in F$ für welches $a(\alpha) = 0$ wird als Wurzel von $a(x)$ bezeichnet.

Lemma $\alpha \in F$ ist eine Wurzel von $a(x)$ wenn und nur wenn $x - \alpha$ $a(x)$ teilt.

Definition Wenn α eine Wurzel von $a(x)$ ist, dann ist seine Vielfachheit die höchste Potenz von $x - \alpha$ die $a(x)$ teilt.

Korollar Ein Polynom $a(x)$ von Grad 3 über einem Körper F ist irreduzibel wenn und nur wenn es keine Wurzel hat.

Theorem Für ein Integritätsbereich D hat ein nichtnull Polynom $a(x) \in D[x]$ vom Grad d höchstens d Wurzeln, zählende Vielfache.

Polynom Interpolation

Lemma Ein Polynom $a(x) \in F[x]$ vom Grad d ist eindeutig bestimmt durch d+1 Werte von $a(x)$, i.e. durch $a(\alpha_1), \ldots, a(\alpha_{d+1})$ für disjunkte $\alpha_1, \ldots, \alpha_{d+1} \in F$.

Analogien zwischen $\mathbb{Z}$ und $F[x]$, Euklidischer Bereich

Definition Für $a, b \in D$, b teilt a in D, geschrieben $b|a$, wenn $a = bc$ für ein c. Ausserdem werden a,b als *associates* bezeichnet, geschrieben $a \sim b$, wenn $a = ub$ für eine Einheit $u \in D$. Eine Nicht-Einheit $p \in D - \{0\}$ ist prim wenn immer $p = ab$, dann ist entweder a oder b eine Einheit.

Lemma $a \sim b \Leftrightarrow a|b \wedge b|a$.

Definition Ein *Euklidischer Bereich* ist ein Integritätsbereich zusammen mit einer *Grad Funktion*: $D^* \to \mathbb{N}$, wobei gilt:

1. $d(ab) \geq d(a)$ für alle nicht-Null $a, b \in D$
2. Für jedes a und $b \neq 0$ in D existiert q und r, so dass $a = bq + r$ und $d(r) < d(b)$ oder $r = 0$.

Theorem In einem Euklidischen Bereich kann jedes Element eindeutig (bis auf associates) in Primzahlen faktorisiert werden.

Der Ring $F[x]_{m(x)}$

$a(x) \equiv_{m(x)} b(x) \Leftrightarrow m(x)|(a(x) - b(x))$

Lemma Kongruenz modulo $m(x)$ ist eine Äquivalenzrelation auf $F[x]$ und jede Äquivalenzklasse hat einen eindeutigen Repräsentent vom Grad kleiner als $deg(m(x))$.

Definition $m(x)$ ein Polynom vom Grad d über F. Dann
$F[x]_{m(x)} = \{a(x) \in F[x] \mid deg(a(x)) < d\}$
$F[x]^*_{m(x)} = \{a(x) \in F[x]_{m(x)} \mid gcd(a(x), m(x)) = 1\}$

Lemma $F[x]_{m(x)}$ ist ein Ring mit Addition und Multiplikation modulo m(x).

Theorem Der Ring $F[x]_{m(x)}$ ist ein Körper wenn und nur wenn $m(x)$ irreduzibel ist.

Definition Ein Körper $F[x]_{m(x)}$ wird als *ausgeweiteter Körper* von F bezeichnet und F wir als Unterkörper von $F[x]_{m(x)}$ bezeichnet.

Endliche Körper

Theorem Für jede Primzahl p und jedes $d \geq 1$ existiert ein irreduzibles Polynom vom Grad d in $GF(p)[x]$. Im Besonderen existiert ein endlicher Körper mit p^d Elementen.

Theorem Es existiert ein endlicher Körper mit q Elementen wenn und nur wenn q eine Potenz einer Primzahl ist. Ausserdem irgendwelche Körper gleicher Grösse q sind isomorph, i.e. jeder endliche Körper ist ein ausgeweiteter Körper von $GF(p)$ für eine Primzahl p.

Theorem Die multiplikative Gruppe von jedem endlichen Körper GF(q) ist zyklisch.

6.5 Anwendungen von endlichen Körpern

Secret Sharing

Definition Ein *(t,n)-secret sharing Schema* für einen endlichen Bereich $\mathcal{S}$ ist eine Methode um einen geheimen Wert $s \in \mathcal{S}$ so unter $P_1, \ldots, P_n$ Gruppen aufzuteilen, so dass irgendwelche t von den Gruppen den Schlüssel s rekonstruieren können, aber t-1 (oder weniger) keine Information darüber haben.

Theorem $n < q$ und jede Gruppe P_i zu einem eindeutigen Element α_i von $GF(q)$ zugehörig. Wenn $a_1, \ldots, a_{t-1}$ uniform und zufällig von GF(q) gewählt werden und jede Gruppe P_i erhält einen Teil $a(\alpha_i)$, wobei das Polynom $a(x) \in GF(x)$ definert ist durch
$a(x) := a_{t-1}x^{t-1} + \ldots + a_1 x + s$
dann ist das ein (t,n)-secret sharing Schema.

Fehlerkorrigierungs Codes

Definition Die *Verschlüsselungsfunktion* E eines Fehlerkorrigierungs-Codes für ein Alphabet $\mathcal{A}$ nimmt k Informationssymbole $a_0, \ldots, a_{k-1} \in \mathcal{A}$ von $\mathcal{A}$ und verschlüsselt diese in eine Liste $c_0, \ldots, c_{n-1}$ von $n > k$ Symbolen in $\mathcal{A}$ (das Codewort).
$E : \mathcal{A}^k \to \mathcal{A}^n : [a_0, \ldots, a_{k-1}] \mapsto E(a_0, \ldots, a_{k-1}) = [c_0, \ldots, c_{n-1}]$
Anstatt der Verschlüsselungsfunktion betrachtet man oft die Menge $\mathcal{C}$ von Codewörtern, welche als Fehlerkorrigierungs-Code bezeichnet wird:
$=\{E(a_0, \ldots, a_{k-1}) | a_0, \ldots, a_{k-1} \in \mathcal{A}\}$

Definition Ein *(n,k)-Fehlerkorrigierungs-Code* (oder (n,k)-Code) $\mathcal{C}$ über einem Alphabet $\mathcal{A}$ mit $|\mathcal{A}| = q$ ist eine Untermenge der Kardinalität q^k von $\mathcal{A}^n$.

Definition Die *minimale Distanz* eine Fehlerkorrigierungs-Codes $\mathcal{C}$ ist die minimale *Hamming Distanz* zwischen zwei Codewörtern, wobei die Hamming Distanz definiert ist als die Nummer von Positionen an welchen die zwei Codewörter verschieden sind.

Definition Eine *Dekodierfunktion* D nimmt eine beliebige Liste $[r_0, \ldots, r_{n-1}] \in \mathcal{A}^n$ von Symbolen

und dekodiert diese zu einem Informationsvektor $[a_0, \ldots, a_{k-1}]$. In anderen Worten
$D : \mathcal{A}^n \to \mathcal{A}^k : [r_0, \ldots, r_{n-1}] \mapsto [a_0, \ldots, a_{k-1}]$.

Definition Ein Code $\mathcal{C}$ kann t Fehler korrigieren wenn eine Dekodierfunktion D existiert, so dass wenn man $[r_0, \ldots, r_{n-1}]$ von einem beliebigen Codewort $[c_0, \ldots, c_{n-1}]$ erhält wenn man beliebige t Positionen ändert, dann
$E(D([r_0, \ldots, r_{n-1}])) = [c_0, \ldots, c_{n-1}]$

Theorem Ein Code $\mathcal{C}$ mit minimaler Distanz d kann t Fehler korrigieren, wenn und nur wenn $d \geq 2t + 1$.

Theorem $\mathcal{A} = GF(q)$ (i.e. $\mathcal{A}$ hat eine Körper Struktur) und $\alpha_0, \ldots, \alpha_{n-1}$ beliebige disjunkte Elemente von $GF(q)$. Die Encode Funktion: $E(a_0, \ldots, a_{k-1}) = [a(\alpha_0), \ldots, a(\alpha_{n-1})]$,
wobei $a(x)$ das Polynom
$a(x) := a_{k-1}x^{k-1} + \ldots + a_1 x + a_0$.
Dieser Code hat die minimale Distanz n-k+1.