Du wirst in DS mündlich geprüft? Dann sind die Übungsaufgaben weniger relevant, aber das Skript dafür umso mehr. Du solltest alle Definitionen, Sätze und Beweise aus der Vorlesung kennen und wiedergeben können. Diese Folien sollen dir beim Lernen helfen.

Wie funktionieren sie?

- 1. Folien einseitig auf Karteikarten drucken.
- 2. Fragen mithilfe des Skripts auf der Hinterseite beantworten.
- 3. Auswendig lernen!

Die Überschriftsfarben beziehen sich auf die jeweiligen Kapiteln: Grundlagen, Kombinatorik, Graphentheorie und Algebraische Strukturen.

Wichtig: Besprich zuerst mit dem Professor, welche Themen für die Prüfung relevant sind und welche nicht!

Was ist eine Menge?

 $Was\ ist\ ein\ Venn\text{-}Diagramm?$



Wie viele Bereiche kann ein Venn-Diagramm maximal haben?

Beschreiben Sie folgende Mengen:

 $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, [n], \mathbb{Z}_n, \emptyset$.

Welche zwei Schreibweisen gibt es für Mengen?

Was ist die Kardinalität |M| einer Menge M?

Was ist die Potenzmenge $\mathcal{P}(M)$ einer Menge M?

Was gilt für $|\mathcal{P}(M)|$?

Was ist die Vereinigungsmenge zweier Mengen *A* und *B*?

Was ist die Schnittmenge zweier Mengen A und B?

Was ist die Differenzmenge zweier Mengen A und B?

Was ist die Komplementmenge einer Menge A?

Was ist die Symmetrische Differenz zweier Mengen A und B?

Was ist die disjunkte Vereinigung zweier Mengen A und B?

Was ist eine Partition einer Menge M?

Was besagt die Idempotenz von Mengen?

Was besagt die Kommutativität von Mengen?

Was besagt die Assoziativität von Mengen?

Was besagt die Distributivität von Mengen?

Was ist ein Tupel?

Was ist das kartesische Produkt $M_1 \times ... \times M_n$ von n Mengen $M_1, ..., M_n$?

Was gilt für $|M_1 \times \ldots \times M_n|$?

Was ist ein Wort über einem Alphabet A?

Was ist die Konkatenation zweier Wörter $w_1 = a_1 \dots a_k$ und $w_2 = b_1 \dots b_m$?

Was ist die Konkatenation von Wörtermengen A_1, \ldots, A_n ?

Was ist eine binäre Relation und wann ist eine binäre Relation homogen?

Wann ist eine Relation $R \subseteq A \times A$ reflexiv?

Wann ist eine Relation $R \subseteq A \times A$ symmetrisch?

Wann ist eine Relation $R \subseteq A \times A$ asymmetrisch?

Wann ist eine Relation $R \subseteq A \times A$ antisymmetrisch?

Wann ist eine Relation $R \subseteq A \times A$ transitiv?

Wann ist eine Relation $R \subseteq A \times A$ total?

Welche Eigenschaften besitzt die Relation $<\subseteq \mathbb{N} \times \mathbb{N}$?

Welche Eigenschaften besitzt die Relation $\leq \subseteq \mathbb{N} \times \mathbb{N}$?

Welche Eigenschaften besitzt die Relation $\neq \subseteq \mathbb{N} \times \mathbb{N}$?

Welche Eigenschaften besitzt die Relation $=\subseteq \mathbb{N} \times \mathbb{N}$?

Welche Eigenschaften besitzt die Relation $\equiv_3 \subseteq \mathbb{N} \times \mathbb{N}$?

Was ist eine Äquivalenzrelation?

Welche Beziehung gibt es zwischen einer Äquivalenzrelation und einer Partition?

Was ist eine partielle Ordnung?

Was ist ein Hasse-Diagramm und was kann man damit darstellen?

Was ist das Bild und Urbild einer Relation?

Was ist die Inverse einer Relation?

Was ist das Relationenprodukt zweier Relationen?

Was ist die Komposition von Relationen?

Was ist die reflexive Hülle einer Relation?

Was ist die transitive Hülle einer Relation?



Was ist die reflexive transitive Hülle einer Relation?

Was ist eine Funktion?

Was ist die Komposition von Funktionen?

Wann ist eine Funktion injektiv?

Wann ist eine Funktion surjektiv?

Wann ist eine Funktion bijektiv?



Wann haben zwei Mengen A und B die gleiche Kardinalität?

Wann ist eine Menge *B* mindestens so mächtig wie eine Menge *A*?



Wann ist eine Menge abzählbar und wann überabzählbar?

Wieso ist die Menge $\ensuremath{\mathbb{Z}}$ abzählbar?

Sei A eine Menge. Wieso ist A^* abzählbar?



Wie sind die Formationsregeln für aussagenlogische Formeln?

Was ist der Syntaxbaum zu folgender Formel F?

$$F = (\neg(p \land q) \to (q \lor \neg q))$$

Geben Sie die Semantik (als Tabelle) folgender Operatoren an:

$$\neg, \land, \lor, \rightarrow, \leftrightarrow, \otimes$$
.

Was ist die Semantik (als Wahrheitstabelle) folgender Formel F?

$$F = (((p \lor \neg q) \to r) \leftrightarrow r))$$

Wann ist eine aussagenlogische Formel erfüllbar?

Wann ist eine aussagenlogische Formel allgemeingültig bzw. eine Tautologie?

Wann ist eine aussagenlogische Formel unerfüllbar bzw. ein Widerspruch?



Wann sind zwei aussagenlogische Formeln F und G äquivalent?



Was besagt die Identität aussagenlogischer Formeln?



Was besagt die Dominanz aussagenlogischer Formeln?



Was besagt die Idempotenz aussagenlogischer Formeln?



Was besagt die Doppelte Negation aussagenlogischer Formeln?

Was besagt die Triviale Tautologie/Kontradiktion aussagenlogischer Formeln?



Was besagt die Kommutativität aussagenlogischer Formeln?



Was besagt die Assoziativität aussagenlogischer Formeln?



Was besagt die Distributivität aussagenlogischer Formeln?

Was besagt die Regeln von De Morgan für aussagenlogische Formeln?

Welche Äquivalenzregeln gibt es für das Exklusive-Oder?

Welche Äquivalenzregeln gibt es für die Implikation?

Welche Äquivalenzregeln gibt es für das Bikonditional?



Was sind die Vor- und Nachteile von Wahrheitstafeln?



Was sind die Vor- und Nachteile der Äquivalenzregeln?

Wie viele verschiedene Semantiken gibt es für Formeln mit n Variablen?



Wann ist eine Menge von logischen Operatoren vollständig?

Die Menge $\{\land,\lor,\lnot\}$ von Operatoren ist vollständig. Wieso ist die Menge $\{\land,\lnot\}$ auch vollständig?

Die Menge $\{\land,\lor,\lnot\}$ von Operatoren ist vollständig. Wieso ist die Menge $\{\lor,\lnot\}$ auch vollständig?

Die Menge $\{\land,\lor,\lnot\}$ von Operatoren ist vollständig. Wieso ist der NAND-Operator $\{\bar{\land}\}$ auch vollständig?

Die Menge $\{\land,\lor,\lnot\}$ von Operatoren ist vollständig. Wieso ist der NOR-Operator $\{\,\bar{\lor}\,\}$ auch vollständig?

Was ist ein Literal?

Was ist eine Klausel?

Wann ist eine Formel in Konjunktiver Normalform?

Wann ist eine Formel in Disjunktiver Normalform?

Für das DPLL-Verfahren ist folgender Fakt wichtig:

F ist genau dann erfüllbar, wenn $F[p \setminus \text{true}]$ oder $F[p \setminus \text{false}]$ erfüllbar sind.

Wieso gilt das?

Wie funktioniert der DPLL-Algorithmus? (Algorithmus 1)

Wie kann man mithilfe von One-Literal-Klauseln den DPLL-Algorithmus beschleunigen?



Wieso terminiert der DPLL-Algorithmus für jede Eingabeformel?

Wieso ist DPLL-Algorithmus korrekt?

Wie stellt man KNF-Formeln als Mengen dar?

Was stellen die leere Formel $\{\}$ und die Formel mit der leeren Klausel $\{\{\}\}$ dar?

Was ist der Resolvent R von zwei Klauseln K_1 und K_2 ? Geben Sie ein Beispiel für K_1 , K_2 und R an.

Wie funktioniert das Resolutionsverfahren?

Für das Resolutionsverfahren ist folgender Fakt wichtig:

Wenn R Resolvent zweier Klauselnvon F ist, dann gilt $F \equiv F \cup \{R\}$.

Wieso gilt das?



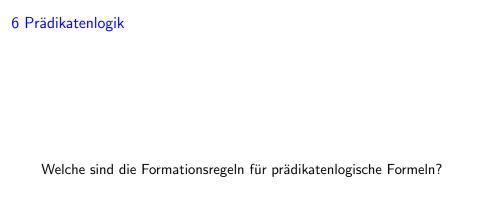
Wieso terminiert das Resolutionsverfahren für jede Eingabeformel?

Wenn dir Formel erfüllbar ist, dann antwortet das Resolutionsverfahren "erfüllbar". Begründen Sie das.

Was bedeutet $A \vdash F$?

Was bedeutet $A \models F$?

Welche Beziehung gibt es zwischen $A \vdash F$ und $A \models F$ in der Aussagenlogik?



6 Prädikatenlogik

Was ist eine Struktur?

Was besagt die Regeln von De Morgan für prädikatenlogische Formeln?



Was besagt die Kommutativität prädikatenlogischer Formeln?



Was besagt die Distributivität prädikatenlogischer Formeln?

Welche wichtige Äquivalenzregel gibt es für prädikatenlogische Formeln außer den Regeln von De Morgan, der Kommutativität und der Distributivität?

Was besagt die Allquantoreinführung?

 $Was\ be sagt\ die\ All quantorbe seitigung?$

Was besagt die Existenzquantoreinführung?

Was besagt die Existenzquantobeseitigung?

Welche Beziehung gibt es zwischen $A \vdash F$ und $A \models F$ in der Prädikatenlogik?

Wie funktioniert ein direkter Beweis?

Wie funktioniert ein indirekter Beweis?

Wie funktioniert ein Widerspruchsbeweis?



Wie funktioniert ein Beweis mit vollständiger Induktion?

Beweisen Sie mit vollständiger Induktion:

Der DPLL-Algorithmus terminiert für jede Eingabeformel F.

Beweisen Sie mit vollständiger Induktion:

Wenn *F* erfüllbar ist, dann antwortet der DPLL-Algorithmus "erfüllbar".

Beweisen Sie mit vollständiger Induktion:

Wenn F unerfüllbar ist, dann antwortet das Resolutionsverfahren "unerfüllbar".

Was bedeutet $f \in \mathcal{O}(g)$?

Was bedeutet $f \in o(g)$?

Was bedeutet $f \in \Omega(g)$?

Was bedeutet $f \in \omega(g)$?

Was bedeutet $f \in \Theta(g)$?

Was bedeutet $f \in \mathcal{O}(g)$?



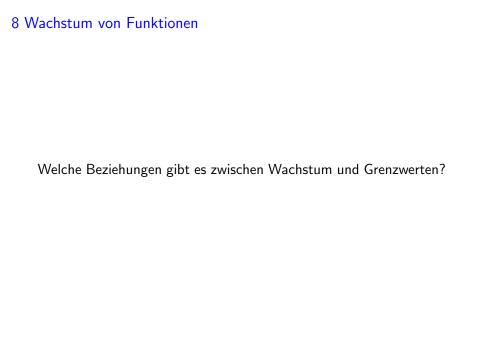
Wieso spielen Konstante Faktoren keine wichtige Rolle?

Wieso betrachten wir das Verhalten von Funktionen für große Eingabewerte?



Beweisen Sie, dass jedes Polynom von Grad n in $\mathcal{O}(x^n)$ liegt.

Welche Beziehung gibt es zwischen $\mathcal{O}(g)$, o(g), $\Omega(g)$, $\omega(g)$ und $\Theta(g)$?



Wie viele Möglichkeiten gibt es, *k* Elemente aus einer *n*-elementigen Menge mit Zurücklegen und mit Betrachtung der Reihenfolge zu ziehen?

Wieso gibt es genau n^k Möglichkeiten, k Elemente aus einer n-elementigen Menge mit Zurücklegen und mit Betrachtung der Reihenfolge zu ziehen?

Wie viele Möglichkeiten gibt es, *k* Elemente aus einer *n*-elementigen Menge ohne Zurücklegen und mit Betrachtung der Reihenfolge zu ziehen?

Wieso gibt es genau n^k Möglichkeiten, k Elemente aus einer n-elementigen Menge ohne Zurücklegen und mit Betrachtung der Reihenfolge zu ziehen?

Wie viele Möglichkeiten gibt es, *k* Elemente aus einer *n*-elementigen Menge ohne Zurücklegen und ohne Betrachtung der Reihenfolge zu ziehen?

Wieso gibt es genau $\binom{n}{k}$ Möglichkeiten, k Elemente aus einer n-elementigen Menge ohne Zurücklegen und ohne Betrachtung der Reihenfolge zu ziehen?

Wie viele Möglichkeiten gibt es, *k* Elemente aus einer *n*-elementigen Menge mit Zurücklegen und ohne Betrachtung der Reihenfolge zu ziehen?

Wieso gibt es genau $\binom{n+k-1}{n-1}$ Möglichkeiten, k Elemente aus einer n-elementigen Menge mit Zurücklegen und ohne Betrachtung der Reihenfolge zu ziehen?

10 Kombinatorische Beweisprinzipien

Was besagt die Produktregel?

Was besagt die Summenregel?

Was besagt die Gleichheitsregel?

Was besagt das Prinzip des doppelten Abzählens?

Wie viele Teiler haben die natürliche Zahlen zwischen 1 und 8 im Durchschnitt?



Was besagt das Prinzip für Inklusion und Exklusion? (Siebformel)

Wie viele natürliche Zahlen zwischen 1 und 1000 sind durch 7 oder 11 teilbar?

Was besagt das Schubfachprinzip?

Zeigen Sie mithilfe des Schubfachprinzips:

In jeder Menge P von Personen, $|P| \ge 2$, gibt es mindestens 2 Personen, die die gleiche Anzahl von Personen aus P kennen.



Was besagt das verallgemeinerte Schubfachprinzip?



Beweisen Sie das verallgemeinerte Schubfachprinzip.

Zeigen Sie mithilfe des verallgemeinerten Schubfachprinzips:

In jeder Menge von 6 Personen gibt es 3, die sich alle untereinander kennen oder 3, die sich alle nicht kennen (wobei die Relation "kennen" symmetrisch sei).

Was gibt die Ramsey-Zahl R(m, n) an?

Was kann man mit Binomialkoeffizienten zählen?

Was besagt die Binomische Formel und wieso gilt sie?

Was besagt die Pascalsche Identität und wieso gilt sie?



Was besagt die Vandermonde Identität und wieso gilt sie?

Was kann man mit $S_{n,k}$ zählen?

Begründen Sie folgende Gleichung:

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$$
.

Was kann man mit $s_{n,k}$ zählen?

Begründen Sie folgende Gleichung:

$$s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$$
.

Was kann man mit $P_{n,k}$ zählen?

Begründen Sie folgende Gleichung:

$$P_{n,k} = \sum_{i=0}^{k} P_{n-k,i} .$$

Begründen Sie:

Es gibt genau m^n Möglichkeiten n unterscheidbare Bälle auf m unterscheidbare Urnen beliebig zu verteilen.

Begründen Sie für $n \le m$:

Es gibt genau $m^{\underline{n}}$ Möglichkeiten n unterscheidbare Bälle auf m unterscheidbare Urnen injektiv zu verteilen.

Begründen Sie für $n \ge m$:

Es gibt genau $m! \cdot S_{n,m}$ Möglichkeiten n unterscheidbare Bälle auf m unterscheidbare Urnen surjektiv zu verteilen.

Begründen Sie für n = m:

Es gibt genau n! Möglichkeiten n unterscheidbare Bälle auf m unterscheidbare Urnen bijektiv zu verteilen.

Begründen Sie:

Es gibt genau $\binom{m+n-1}{n}$ Möglichkeiten n gleiche Bälle auf m unterscheidbare Urnen beliebig zu verteilen.

Begründen Sie für $n \le m$:

Es gibt genau $\binom{m}{n}$ Möglichkeiten n gleiche Bälle auf m unterscheidbare Urnen injektiv zu verteilen.

Begründen Sie für $n \ge m$:

Es gibt genau $\binom{n-1}{m-1}$ Möglichkeiten n gleiche Bälle auf m unterscheidbare Urnen surjektiv zu verteilen.

Begründen Sie:

Es gibt genau $\sum_{k=1}^{m} S_{n,k}$ Möglichkeiten n unterscheidbare Bälle auf m gleiche Urnen beliebig zu verteilen.

Begründen Sie für $n \ge m$:

Es gibt genau $S_{n,m}$ Möglichkeiten n unterscheidbare Bälle auf m gleiche Urnen surjektiv zu verteilen.

Begründen Sie:

Es gibt genau $\sum_{k=1}^{m} P_{n,k}$ Möglichkeiten n gleiche Bälle auf m gleiche Urnen beliebig zu verteilen.

Begründen Sie für $n \ge m$:

Es gibt genau $P_{n,m}$ Möglichkeiten n gleiche Bälle auf m gleiche Urnen surjektiv zu verteilen.

13 Grundlagen Graphen

Was ist ein Graph?

13 Grundlagen Graphen

Wieso sind bei Graphen keine Mehrfachkanten oder Schlingen erlaubt?

13 Grundlagen Graphen

Was ist ein gerichteter Graph?



Was ist ein Hypergraph?

Was ist ein vollständiger Graph?



Wie viele Kanten besitzt der vollständige Graph K_n ?

Was ist ein Kreis C_n ?

Was ist ein Gittergraph $M_{n,m}$?



Was ist ein Hyperwürfel Q_n ?



Was ist ein bipartiter Graph und wann ist ein bipartiter Graph vollständig?



Was ist die Nachbarschaft und der Grad eines Knotens?



Was ist die Gradfolge eines Graphen?

Wann ist ein Graph k-regulär?



Was sind Wege, Pfade, Touren und Kreise?



Was ist ein Teilgraph und wann ist ein Teilgraph induziert?



Was ist eine Zusammenhangskomponente?

Wann ist ein Graph zusammenhängend?

Begründen Sie das Handshake-Theorem:

$$\sum_{v\in V} \deg(v) = 2|E| \ .$$

Wieso muss die Summe $\sum_{v \in V} \deg(v)$ aller Knotengrade immer gerade sein?

Mit welchem Satz kann man immer überprüfen, ob ein Graph mit einer gegebenen Gradfolge existiert?

Was ist ein Baum?

Was ist ein Wald?



Wieso besitzt jeder Baum mit $|V| \geq 2$ mindestens zwei Blätter?

Was ist ein Spannbaum?

Beweisen Sie mit vollständiger Induktion:

Jeder zusammenhängender Graph enthält mindestens einen Spannbaum.

Folgende Aussagen sind für einen beliebigen Graph G = (V, E) äquivalent:

- (1) G ist ein Baum.
- (2) Je zwei Knoten in G sind durch genau einen Pfad verbunden.
- (3) G ist zusammenhängend und |V| = |E| + 1.

Zeigen Sie: $(1) \Leftrightarrow (2)$.

Folgende Aussagen sind für einen beliebigen Graph G = (V, E) äquivalent:

- (1) G ist ein Baum.
- (2) Je zwei Knoten in G sind durch genau einen Pfad verbunden.
- (3) G ist zusammenhängend und |V| = |E| + 1.

Zeigen Sie durch Induktion über |V|: (1) \Rightarrow (3).

Folgende Aussagen sind für einen beliebigen Graph G = (V, E) äquivalent:

- (1) G ist ein Baum.
- (2) Je zwei Knoten in G sind durch genau einen Pfad verbunden.
- (3) G ist zusammenhängend und |V| = |E| + 1.

Zeigen Sie: $(3) \Rightarrow (1)$.

Sei G = (V, E) ein Baum mit Gradfolge (d_1, \ldots, d_n) . Zeigen Sie:

$$\sum_{i=1}^n d_i = 2n-2.$$



Wie viele verschiedene Bäume mit Knotenmenge [n] gibt es?

14 Bäume
Wie bestimmt man den Prüfer-Code zu einem gegebenen Baum?

14 Bäume			

Wie bestimmt man den Baum zu einem gegebenen Prüfer-Code?

Was ist ein Wurzelbaum?

Sei G ein Wurzelbaum und v ein beliebiger Knoten in G. Wann ist ein Knoten u ein Vorgänger von v?

Sei G ein Wurzelbaum und v ein beliebiger Knoten in G. Wann ist ein Knoten u der Vater bzw. die Mutter von v?

Sei G ein Wurzelbaum und v ein beliebiger Knoten in G. Wann ist ein Knoten u ein Nachfolger von v?

Sei G ein Wurzelbaum und v ein beliebiger Knoten in G. Wann ist ein Knoten u ein Kind von v?

Was die Höhe eines gewurzelten Baumes?

15 Euler-Touren und Hamilton-Kreise

Was ist eine Euler-Tour?

15 Euler-Touren und Hamilton-Kreise

Wie lautet der Satz von Euler für Euler-Touren?

15 Euler-Touren und Hamilton-Kreise

Beweisen Sie den Satz von EUler für Euler-Touren:

Ein zusammenhänger Graph besitzt genau dann eine Euler-Tour, wenn alle Knoten des Graphen geraden Grad haben. 15 Euler-Touren und Hamilton-Kreise

Was ist ein Hamilton-Kreis?

Was ist ein planarer Graph?

Was besagt die Eulersche Polyederformel?

Beweisen Sie die Eulersche Polyederformel für planare Graphen:

$$|R| = |E| - |V| + 2$$
.

Zeigen Sie:

Für jeden planaren Graphen G = (V, E) mit $|V| \ge 3$ gilt:

$$|E| \leq 3|V| - 6.$$



Zeigen Sie:

Jeder planare Graph hat einen Knoten mit Grad höchstens 5.

Zeigen Sie:

Der K_5 ist nicht planar.

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

Wie lautet der Satz von Kuratowski?

Was ist eine Knotenfärbung?



Was ist die chromatische Zahl $\chi(G)$ eines Graphen G?

Welche chromatische Zahl hat ein vollständiger Graph mit *n* Knoten?



Welche chromatische Zahl hat ein Kreis mit *n* Knoten?

Welche chromatische Zahl haben Bäume?

16	Planarität	und	Färbung	von	Graphen
----	------------	-----	---------	-----	---------

Welche chromatische Zahl haben bipartite Graphen?



Wie viele Farben braucht man, um planare färben?

Beschreiben Sie kurz das Heiratsproblem.

Was ist ein Matching?

Was ist ein perfektes Matching?

Wie lautet der Heiratssatz von Hall?

Skizzieren Sie den Beweis des Heiratssatzes.

17 Matchings			

Was folgt aus dem Heiratssatz für bipartite, k-reguläre Graphen?

Was ist eine Heirat?

Was ist eine stabile Heirat?



Beschreiben Sie den Gale-Shapley-Algorithmus für stabile Heiraten.



Wieso benötigt der Gale-Shapley-Algorithmus maximal n^2 Schritte?



Wieso berechnet der Gale-Shapley-Algorithmus eine stabile Heirat?

Was ist eine Algebra?

Geben Sie drei unterchiedliche Algebren mit jeweils nur einem Operator an, die keine Halbgruppen sind.

Sei A eine Algebra. Was ist ein links- bzw. rechtsneutrales Element?



Sei A eine Algebra. Was ist ein neutrales Element?

Sei A eine Algebra und a ein Element. Was ist ein links- bzw. rechtsinverses Element von a?

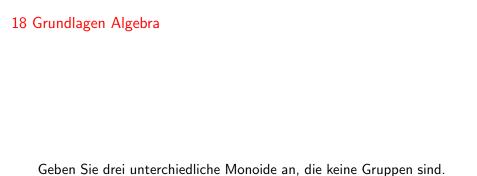
Sei A eine Algebra und a ein Element. Was ist ein inverses Element von a?

Was ist eine Halbgruppe?



Geben Sie drei unterchiedliche Halbgruppen an, die keine Monoide sind.

Was ist ein Monoid?



Was ist eine Gruppe?

Geben Sie drei unterchiedliche Gruppen an.

Was bedeutet $x \equiv_m y$?

Was ist $x \mod y$?

Was ist $x +_m y$ und $x \cdot_m y$?



Wann ist eine Gruppe, ein Monoid oder eine Halbgruppe abelsch?

Was ist (\mathbb{Z}_n) , $+_n$?

Sei $G = (S, \circ)$ eine Gruppe. Zeigen Sie:

G enthält genau ein neutrales Element.

Sei $G = (S, \circ)$ eine Gruppe. Zeigen Sie:

Jedes $a \in S$ hat genau ein inverses Element a^{-1} .

Sei $G = (S, \circ)$ eine Gruppe. Zeigen Sie für alle $a, b, c \in S$:

 $\text{wenn } a \circ c = b \circ c \text{ dann } a = b \ ,$

wenn $c \circ a = c \circ b$ dann a = b.

Sei $G = (S, \circ)$ eine Gruppe mit neutralem Element e.

Was ist die Ordnung ord(a) eines Elements $a \in S$?

Sei $G = (S, \circ)$ eine Gruppe.

Was ist eine Untergruppe von *G*?

Was ist eine rechte bzw. linke Nebenklasse?

Sei H eine Untegruppe von G. Was ist der Index ind $_G(H)$ von H in G?

Sei *H* eine Untergruppe von *G*. Zeigen Sie:

Die Menge der rechten bzw. linken Nebenklassen von H bildet eine Partition von G.

Sei H eine Untergruppe von G. Zeigen Sie den Satz von Lagrange:

- (1) Alle Nebenklassen von H in G haben gleich viele Elemente.
- (2) $|G| = \operatorname{ind}_G(H) \cdot |G|$
- (3) |H| teilt |G|

Sei $G = (S, \circ)$ eine Gruppe. Begründen Sie:

ord(a) teilt |S| für alle $a \in S$.

Was ist $(\mathbb{Z}_n^*, \cdot_n)$?

Wie ist der größte gemeinsame Teiler ggT(x, y) von zwei Zahlen $x, y \in \mathbb{N}$ definiert?

Beweisen Sie für alle $x, y \in \mathbb{N}$ mit $x \leq y$:

- (1) Wenn $y \mod x = 0 \operatorname{dann} \operatorname{ggT}(x, y) = x$
- (2) Wenn $y \mod x > 0$ dann $ggT(x, y) = ggT(y \mod x, y)$



Was kann man mit dem Euklidischen Algorithmus berechnen?

Beschreiben Sie den Euklidischen Algorithmus.

Zeigen Sie für beliebige $x, y \in \mathbb{N}$:

Es gibt $a, b \in \mathbb{Z}$ mit ggT(x, y) = ax + by.

Was kann man mit dem Erweitertem Euklidischen Algorithmus berechnen?

Beschreiben Sie den Erweitertem Euklidischen Algorithmus.

Wie berechnet man für $x \in \mathbb{Z}_n^*$ sein inverses Elemenet in $(\mathbb{Z}_n^*, \cdot_n)$?

Was ist $\varphi(n)$?

Wie berechnet man $\varphi(n)$?

Was ist eine zyklische Gruppe?

Wieso sind $(\mathbb{Z},+)$ und $(\mathbb{Z}_n,+_n)$ zyklische Gruppen?

 $Was\ ist\ ein\ Gruppen isomorphismus?$

Sei $G = (S, \circ)$ eine zyklische Gruppe. Zeigen Sie:

- (1) Falls $|S| = \infty$, dann ist G isomorph zu $(\mathbb{Z}, +)$.
- (2) Falls |S| = n, dann ist G isomorph zu $(\mathbb{Z}_n, +_n)$.

Was ist die Symmetrische Gruppe (S_n, \circ) ?

19 Gruppen

Wie bestimmt man die Ordnung einer Permutation in (S_n, \circ) ?

Was muss für den öffentlichen Schlüssel (n, c) gelten?

Was muss für den privaten Schlüssel d gelten?



Mit welcher Funktion f(m) wird eine Nachricht m verschlüsselt?

Mit welcher Funktion $f^{-1}(x)$ kann eine verschlüsselte Nachricht x wieder entschlüsselt werden?

Wieso funktioniert das RSA Kryptosystem für $m \in \mathbb{Z}_n^*$

Worauf beruht die Sicherheit des RSA Kryptosystems?

Was ist ein Ring?

Geben Sie drei Ringe an, die keine Körper sind.

Was ist ein Körper?

Geben Sie drei Körper an.

Was ist $(\mathbb{Z}_n, +_n, \cdot_n)$ für alle $n \geq 2$?

Für welche n ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein Körper?