Kapitel 2
Diskrete Mathematik

Inhaltsverzeichnis

Kombinatorik

Grundaufgaben

Unterschied Variation und Kombination

- Variation: Die Reihenfolge ist eindeutig ($1234 \neq 4321$)
- Kombination: Die Reihenfolge ist egal ($1234 = 4321$)

Variationen mit Wiederholung

Ich habe k Elemente, von denen jedes Element n Zustände annehmen kann. Wie viele verschiedene Möglichkeiten gibt es, diese k-Elemente darzustellen?

Beispiel:

Wie viele "Wörter" können zustande kommen, wenn 5 Buchstaben (nacheinander) aus einem Alphabet vom Umfang 26 gewählt werden?

$$n = 26\ und\ k = 5 \Rightarrow Lösung = n^k = 26^5 = 11881376$$

Variationen ohne Wiederholung

Ich habe n Elemente, und möchte k verschiedene Elemente in einer bestimmten Reihenfolge auswählen. Wie viele Möglichkeiten habe ich?

Beispiel:

Auf wie viele Arten kann aus einem 20-köpfigen Verein ein Vorsitzender, ein Schriftführer und ein Kassierer ausgewählt werden (Achtung! Eine Person kann nicht zwei Aufgaben haben)?

$$n = 20\ und\ k = 3 \Rightarrow Lösung = \frac{n!}{(n-k)!} = \frac{20!}{(20-3)!} = 6840$$

Permutationen einer Menge

Ich habe n Elemente und möchte diese Elemente in einer bestimmten Reihenfolge anordnen. Wie viele Möglichkeiten habe ich?

Beispiel:

Es soll eine Sitzordnung für eine Klasse mit 10 Schülern erstellt werden. Wie viele Möglichkeiten gibt es?

$$n = 20 \Rightarrow Lösung = n! = 10! = 3628800$$

Permutationen einer Multimenge

Ich habe n Elemente. Unter diesen Elementen befinden sich gleiche Elemente, die nicht unterschieden werden können. Wie viele Möglichkeiten habe ich, aus diesen n Elementen verschiedene Reihenfolgen zu bilden?

Beispiel:

Wie viele verschiedene Wörter kann ich mit den Buchstaben „AABCCCDDE“ bilden, wenn immer alle Buchstaben verwendet werden sollen?

$$n = 9\ und\ 5\ Gruppen\ (2A, B, 3C, 2D, E) \Rightarrow Lösung = \frac{9!}{2! * 1! * 3! * 2! * 1!} = 15120$$

Kombination ohne Wiederholung

Ich habe n Elemente und muss k Mal ein Element auswählen, welches ich anschließend in meine Tasche gebe. Wie viele Möglichkeiten gibt es, meine Tasche zu füllen, wenn ich erst am Ende hineinblicke (die Reihenfolge also egal ist)?

Beispiel:

Aus einer Fußballmannschaft mit 20 Spielern muss der Trainer 11 Spieler für das nächste Match aussuchen. Wie viele Möglichkeiten gibt es?

$$n = 20\ und\ k = 11 \Rightarrow Lösung = \binom{n}{k} = \binom{20}{11} = \frac{20!}{11!\,(9)!} = 167960$$

Kombination mit Wiederholung

Ich habe n Elemente und muss k Mal ein Element auswählen, welches ich anschließend wieder zurücklege. Wie viele Möglichkeiten habe ich, k-Elemente zu wählen, wenn die Reihenfolge egal ist.

Beispiel:

50 Sportlerinnen nehmen an 7 Bewerben teil (bei denen es jeweils genau eine Siegerin gibt). Auf wie viele Arten können die Preise verteilt werden?

$$n = 50\ und\ k = 7 \Rightarrow Lösung = \binom{n+k-1}{k} = \binom{50+7-1}{7} = \frac{56!}{7!\,(49)!} = 231917400$$

Beispiel 2:

Eine 3 köpfige Jury, von denen jeder unabhängig eine Stimme vergeben darf, wählt ihren Favoriten aus den letzten zwei Sängern. Wie viele Möglichkeiten gibt es, die Stimmen auf die Kandidaten zu verteilen?

$$n = 2\ und\ k = 3 \Rightarrow Lösung = \binom{2+3-1}{3} = \frac{4!}{3!\,(1!)} = 4$$

Erklärung der Stimmenvergabe: Kandidat 1 : Kandidat 2 = (3:0, 2:1, 1:2, 0:3)

Zusammenfassung

	mit Wiederholung	ohne Wiederholung
Variationen (Reihenfolge!)	$\overline{V}_n^k = \lvert A\rvert^k = n^k$	$V_n^k = \frac{n!}{(n-k)!}$
Kombination (ohne Reihenfolge!)	$\overline{C}_n^k = \frac{(n+k-1)!}{k!\,(n-1)!} = \binom{n+k-1}{k}$	$\boldsymbol{C_n^k = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}}$
	Menge	Multimenge
Permutation	$P_n = n! = V_n^n$	$P_n^{k,1,k2,\ldots} = \frac{n!}{Anzahl\ einzelner\ Mengen}$

Der binomische Lehrsatz

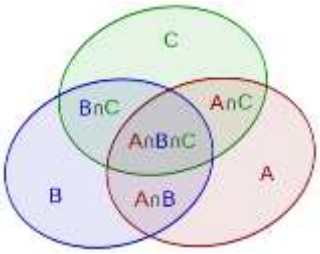
Eigenschaften

$$\binom{n}{0} = \binom{n}{n} = 1$$
$$\binom{n}{k} = \binom{n}{n-k}$$
$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$
$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Binomischer Lehrsatz

$$\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = (x+y)^n$$

Inklusions-Exklusions-Prinzip



Beim Inklusions-Exklusions-Prinzip will man zwei Mengen addieren, die jedoch gemeinsame Elemente haben können.

Somit ergibt sich für zwei Elemente: $|A \cup B| = |A| + |B| - |A \cap C|$
Also zuerst werden alle Elemente von A und B addiert und anschließend die doppelt gezählten Elemente subtrahiert (= Durchschnitt der Mengen).

Für zwei Mengen ist das noch einfach, jedoch möchte man auch die Summe von **n Mengen** wissen.

Unser Ziel ist es also die Vereinigung aller Mengen:

$$X = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n \qquad A_i \; sind \; die \; Mengen \; (können \; gleiche \; Elemente \; besitzen)$$

Weil gleiche Elemente vorkommen, können wir folgende Ungleichung definieren:

$$|X| \leq \sum_{1 \leq i \leq n} |A_i|$$

Nach dem Addieren der Mengen (= **Inklusion**) müssen wir also die gleichen Elemente abziehen (= **Exklusion**).

$$|X| \geq \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

Da wir jetzt aber wieder zu viele Elemente abgezogen haben, ändert sich die Ungleichung. Man müsste also zu viel abgezogene Elemente wieder dazuzählen. Damit tastet man sich langsam an das Ergebnis heran. Nach der Verallgemeinerung erhalten wir:

$$|X| = \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| \; ungerade}} |A_i| - \sum_{\substack{\emptyset \neq I \subseteq \{1,\ldots,n\} \\ |I| \; gerade}} |A_i|$$
$$= \sum_{I \subseteq \{1,\ldots,n+1\}} (-1)^{|I|-1} \left| \bigcap_{j \in J} A_j \right|$$

Beispiel:

Wie viele Wörter der Länge 4 kann ich aus den Buchstaben $\{a, b, c, d, e\}$ bilden, die mindestens ein $\{a, b, c\}$ enthalten?

$W = Menge\ aller\ Wörter\ mit\ \{a, b, c, d, e\}$
$W_a = Menge\ aller\ Wörter\ ohne\ a$
$W_b = Menge\ alle\ Wörter\ ohne\ b$
$W_c = Menge\ alle\ Wörter\ ohne\ c$
$|W_a' \cap W_b' \cap W_c'| = |W| - |W_a| - |W_b| - |W_c| + |W_a \cap W_b| + |W_a \cap W_c| + |W_b \cap W_c| - |W_a \cap W_b \cap W_c|$
$= 5^4 - 4^4 - 4^4 - 4^4 + 3^4 + 3^4 + 3^4 - 2^4 = 4^4 - 3 * 4^4 + 3 * 3^4 - 2^4 = 84$

Graphentheorie

Grundlagen und Begriffsbildungen

Es muss zwischen einem gerichteten und einem ungerichteten Graphen unterschieden werden. Die Kanten eines gerichteten Graphen besitzen Richtungspfeile.

Variablen

$$V = Knotenmenge$$
$$\alpha_0 = |V| = Anzahl\ der\ Knoten$$
$$E = Kanten$$
$$\alpha_1 = |E| = Anzahl\ der\ Kanten$$

Schlicht/Einfach

Es existieren keine Schlingen oder Mehrfachkanten.

Teilgraph G‘

Ein Graph G‘ heißt Teilgraph von G, wenn alle Knoten und Kanten von G‘ auch in G vorhanden sind.

Stark zusammenhängend

Ein gerichteter Graph heißt stark zusammenhängend, wenn ich von jedem Knoten alle anderen Knoten erreiche, ohne dass ich gegen eine Pfeilrichtung gehe.

Handschlaglemma

In einem schlichten ungerichteten Graphen G gilt

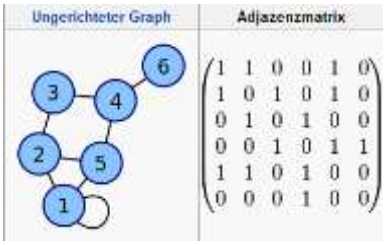
$$\sum_{v \in V(G)} d(v) = 2|E(G)| \qquad d(v) \dots Kantennachbarn$$

In einem gerichteten Graphen G gilt hingegen

$$\sum_{v \in V(G)} d^+(v) = \sum_{v \in V(G)} d^-(v) = |E(G)| \qquad d^+(v) \dots Weggrad / d^-(v) \dots Hingrad$$

Adjazenzmatrix

Die Adjazenzmatrix fasst die Kanten eines Graphen in einer Matrix zusammen. Dabei werden die Spalten und Reihen abwärts bzw. nach rechts den Knoten zugewiesen. Somit gehört Knoten 1 die erste Spalte und die erste Zeile. Ist ein Knoten mit einem anderen Knoten verbunden, trägt man in dem entsprechenden Feld eine 1 ein, andernfalls eine 0.



Bipartit

Knotenmenge V(G) wird in zwei disjunkte, nichtleere Teilmengen V1 und V2 zerlegt.

Planar

Die Kanten dürfen sich nicht schneiden.

Euler’sche Polyederformel

$\alpha_0 + \alpha_1 - \alpha_2 = 2$ Knoten + Kanten – Flächen = 2

Bäume und Wälder

Wald

Ein schlichter ungerichteter Graph, der keine Kreise enthält, heißt Wald.

Baum

Ein Wald, der auch zusammenhängend ist, heißt Baum. Es darf jedoch nur einen Weg von Knoten a zu Knoten b geben.

Es gilt: $\alpha_0 = \alpha_1 + 1$ (Knotenanzahl = Kantenanzahl + 1)

Euler'sche und Hamilton'sche Linien

Euler'sche Linie

Eine Kantenfolge heißt Euler'sche Linie, wenn sie **jeden Knoten** und **jede Kante** enthält. Es darf dabei aber nur jede Kante **einmal** enthalten werden.

In einem ungerichteten Graphen ist dann eine Euler'sche Linie vorhanden, wenn alle Knotengrade gerade ist.

In einem gerichteten Graphen ist dann eine Euler'sche Linie vorhanden, wenn für alle Knoten Hin- und Weggrad gleich sind.

Hamilton'sche Linie

Eine Kantenfolge eines Graphen heißt Hamilton'sche Linie, wenn sie jeden Knoten verbindet, ohne eine Kante zweimal zu beinhalten.

Netzwerke und Algorithmen

Definition

Jeder Kante wird ein Wert zugeordnet, der als Gewicht oder Kosten interpretiert werden kann.

Spannender Baum

Ein spannender Baum eines Graphen enthält alle Knoten und einige bis alle der Kanten. Es dürfen keine Kreise entstehen!

Der minimale spannende Baum kann ganz einfach mit dem Kruskal-Algorithmus herausgefunden werden.

Gerüst/Spannender Wald

Es werden alle Knoten und einige bis alle Kanten eines Graphen verwendet. Es dürfen keine Kreise entstehen.

Algebraische Strukturen

Die algebraischen Strukturen definieren allgemeine strukturelle Übereinstimmungen zwischen Mengen und deren Verknüpfungen.

Nehmen wir folgendes Beispiel an

$\mathbb{N}$ $+$
$\mathbb{Z}$ $*$

Wir erkennen, dass beide Strukturen Gemeinsamkeiten vorweisen. Das wäre unteranderem

- Assoziativ $((a + b) + c = a + (b + c))$
- Abgeschlossenheit (Zwei Elemente aus $\mathbb{N}$ addiert gibt wieder ein Element in $\mathbb{N}$)
- Kommutativ $(a + b = b + a; a * b = b * a)$

Das Gegenteil wäre $(\mathbb{N}\ -)$, denn 2 – 3 liegt nicht mehr in der Menge. Zusätzlich ist die Operation weder assoziativ noch kommutativ.
Zusammengefasst kann man den Begriff „Algebraische Strukturen“ so definieren: Die abstrakte Sicht auf die Zahlenmengen, verknüpft mit deren Operationen und das Definieren von Gemeinsamkeiten bzw. Ähnlichkeiten.

Eigenschaften von algebraischen Strukturen

Für algebraische Strukturen, können folgende Gesetzmäßigkeiten gelten:

- Assoziativgesetz $(a\ o\ b)\ o\ c = a\ o\ (b\ o\ c)$
- Existenz eines neutralen Elements $e\ o\ a = a\ o\ e = a$
  Es darf jedoch **nur ein** neutrales Element geben
- Existenz inverser Elemente $a\ o\ a^{-1} = a^{-1}\ o\ a = e$
  $\forall a \in A$ muss ein individuelles Inverses vorhanden sein, d.h. dass kein Element mehrere Inverse besitzt und kein Element das Inverse von zwei Elementen sein kann.
- Kommutativgesetz $a\ o\ b = b\ o\ a$

Binäre Operationen

Eine binäre Operation ist eine Abbildung $A\ x\ A \rightarrow A$, sie ordnet je zwei Elemente a, b aus der Menge A ein Element $a\ o\ b$ zu.

Schreibweise

Eine binäre Operation wird als Klammerausdruck in der Form $(\boldsymbol{A}, \boldsymbol{o})$ dargestellt. Dabei steht o für eine beliebige Operation.

Gruppen

Die Gruppe ist die populärste algebraische Struktur.

Definition

Eine algebraische Struktur (G, o) heißt Gruppe genau dann, wenn die folgenden Axiome erfüllt sind:

- **Abgeschlossenheit**: Die Menge G ist bezüglich der Operation abgeschlossen
  $$\forall a, b \in G \ \exists c \in G: \ a \ o \ b = c$$
- **Assoziativität**: $\forall a, b, c \in G: \ a \ o \ (b \ o \ c) = (a \ o \ b) o c$
- **Neutrales Element**: In G gibt es ein Neutralelement (= es belässt jedes Element so wie es ist).
  $$\exists n \in G \ \forall a \in G: \ a \ o \ n = a = n \ o \ a$$
  Achtung! Es gibt nur **ein einziges** neutrales Element in einer Gruppe
- **Inverses Element**: In G gibt es für jedes Element ein Inverses
  $$\forall a \in G \ \exists \bar{a} \in G: \ a \ o \ \bar{a} = n = \bar{a} \ o \ a$$
  Achtung! Es gibt zu **jedem Element** in einer Gruppe sein eigenes, individuelles Inverses

Wenn das Kommutativgesetzt gilt, dann heißt die Gruppe kommutativ bzw. abelsch.

$$\forall a, b \in G: \ a \ o \ b = b \ o \ a$$

Halbgruppe

Erfüllt eine algebraische Struktur nur die Abgeschlossenheit sowie die Assoziativität ist sie eine Halbgruppe.

Beispiele

- $(\mathbb{N}; +)$, Halbgruppe, da es keine inverse Element gibt
- $(\mathbb{N}; *)$, Halbgruppe, da es keine inverse Elemente gibt
- $(\mathbb{Z}; +)$, Gruppe, da alle Axiome erfüllt sind
- $(\mathbb{Z}; *)$, Ist eine Halbgruppe, da es kein inverses Element für 0 gibt.
- $(\mathbb{Z}; :)$, Ist weder eine Halbgruppe noch eine Gruppe (nicht abgeschlossen, nicht assoziativ, …)
- $(\mathbb{Q}; *)$, Ist eine Halbgruppe, da es kein inverses Element für 0 gibt. (Info: $(\mathbb{Q}\backslash\{0\}; *) = Gruppe$)
- $(\mathbb{Q}; :)$, Ist weder eine Halbgruppe noch eine Gruppe (nicht assoziativ)

Restklassen

Beispiel: $(\mathbb{Z}_4; \oplus)$ Additions-Verknüpfungstafel der Restklassen modulo 4

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\mathbf{\overline{0}}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\mathbf{\overline{2}}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\mathbf{\overline{0}}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\mathbf{\overline{2}}$

- Ist die Restklassenaddition in $\mathbb{Z}_4$ abgeschlossen?
  Ja, weil nur die Elemente als Ergebnisse vorkommen, die bereits vorhanden sind.
- Ist die Restklassenaddition in $\mathbb{Z}_4$ assoziativ? – Ja (es ist also mindestens eine Halbgruppe)
- Gibt es ein neutrales Element bzw. woran kann ich es erkennen?
  Ja, die Restklasse $\overline{0}$. Immer wenn ich sie dazu addiere erhalte ich das Ausgangselement.
- Gibt es inverse Elemente? – Ja, weil in jeder Zeile und in jeder Spalte mindestens einmal $\overline{0}$ steht.
- Ist unsere Restklassenaddition kommutativ? Ja, man kann die Tafel spiegeln.

Zusammengefasst lässt sich sagen, dass die Struktur $(\mathbb{Z}_m; \oplus)$ eine abelsche Gruppe ist.

Untergruppe

Will man eine Untergruppe konstruieren, wählt man eine Teilmenge einer Gruppe, welche wiederum eine Gruppe ist, sie also alle Bedingungen einer Gruppe erfüllt (Abgeschlossenheit, Assoziativität, Neutrales Element, Inverse). Das neutrale Element von G **muss** in jeder Untergruppe vorhanden sein, da es nur eines geben darf.

Man schreibt für eine Untergruppe von G: $U \leq G$

Will man überprüfen, ob eine Menge eine Untergruppe ist, braucht man nur folgendes Kriterium zu überprüfen:

$$a, b \in U \rightarrow a \; o \; b^{-1} \in U$$

Links- und Rechtsnebenklasse

Bei der Links- bzw. Rechtsnebenklasse wählt man $a \in G$ und $U \leq G$. Anschließend verknüpft man das Element a mit jedem Element der Untergruppe U und erzeugt so eine neue Untergruppe.

$$Linksnebenklasse: a \; o \; U = \{a \; o \; u \mid u \in U\}$$
$$Rechtsnebenklasse: U \; o \; a = \{u \; o \; a \mid u \in U\}$$

Eine Nebenklasse ist also eine um das Element a „verschobene“ Untergruppe. Man spricht „U in G“.

Index bzw. Ordnung

Will man diese Nebenklassen zählen, bezeichnet man die Anzahl der Links- bzw. Rechtsnebenklassen von U in G als Index, dagegen wird die Anzahl der Gruppenelemente als Ordnung von G bezeichnet.

$$Index: |G : U| \quad \text{Von G nach U}$$
$$Ordnung: |G| \quad \text{Ordnung von G}$$

Nach dem „Satz von Lagrange“ gilt:

$$|U| \; ist \; stets \; Teiler \; von \; |G|$$
$$|G : U| = \frac{|G|}{|U|}$$

Normalteiler

Eine Untergruppe heißt Normalteiler, wenn stets LNK = RNK gilt, also $a \; o \; N = N \; o \; a$. Das ist dann der Fall, wenn

$$\begin{matrix} \text{G abelsch}, U \leq G \\ U \leq G, |G : U| = 2 \end{matrix} \Rightarrow \; U \trianglelefteq G$$

Beispiel: Man zeige, dass die von $\overline{3}$ erzeugte Untergruppe von $(\mathbb{Z}_9, +)$ ein Normalteiler von $(\mathbb{Z}_9, +)$ ist.

Die Restklasse $\overline{3}$ erzeugt folgende Untergruppen: U, U + 1, U + 2

Wenn wir beweisen wollen, dass U tatsächlich ein Normalteiler ist, müssen wir nur unsere erste Definition des Normalteilers ansehen. Da wir wissen, dass $(\mathbb{Z}_9, +)$ kommutativ ist, wissen wir auch, dass jede Untergruppe ein Normalteiler ist.

Faktorgruppe

Für eine Faktorgruppe nehmen wir einen Normalteiler $N \trianglelefteq G$ und die Menge der Nebenklassen von G nach N (G/N).

Dabei bedeutet das nur die Verknüpfung $G/N \coloneqq \{gN : g \in G\}$.

Zusätzlich wird noch eine innere Verknüpfung benötigt:
Für $G/N \; x \; G/N \to G/N$ gilt: $(gN) \; o \; (hN) \coloneqq (gh)N$

Beispiel: Man zeige, dass die von $\overline{3}$ erzeugte Untergruppe von $(\mathbb{Z}_9, +)$ ein Normalteiler von $(\mathbb{Z}_9, +)$ ist und bestimmte die Gruppentafel der Faktorgruppe $\mathbb{Z}_9/U$.

Den ersten Teil haben wir bereits bewiesen. Die Gruppentafel der Faktorgruppe $\mathbb{Z}_9/U$ besteht aus den drei Normalteilern. Mit dem Kommutativgesetz kann man sich die Arbeit erleichtern.

$$(1+U)+(2+U) = (1+2)+U = U$$

$+$	U	$1+U$	$2+U$
U	U	$1+U$	$2+U$
$1+U$	$1+U$	$2+U$	U
$2+U$	$2+U$	U	$1+U$

Homomorphismus

Ein Homomorphismus findet immer zwischen zwei Gruppen (G, o) und $(H, \star)$ statt. Es bedeutet die strukturelle Gleichheit zweier Gruppen:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Isomorph zu

o	x	y
x	x	y
y	y	x

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$$e \star a = Normateiler\ der\ Gruppe$$

Es muss folgende Bedingung gelten:

$$\varphi(a \; o \; b) = \varphi(a) \star \varphi(b)$$

Ist φ bijektiv, wird es auch **Isomorphismus** genannt. Im Homomorphismus gelten bestimmte Voraussetzungen:

$$\varphi(e_G) = e_H$$
$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

Beispiel:

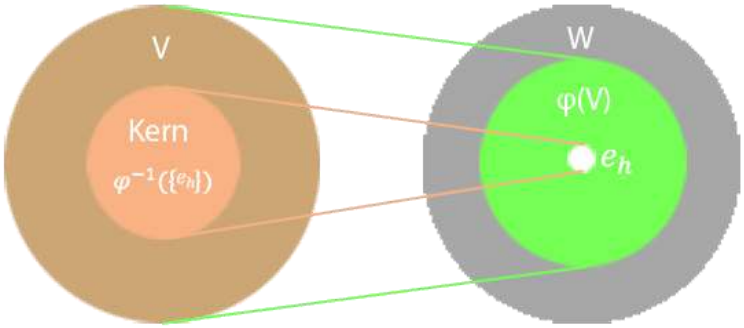
$$\varphi(\mathbb{Z}, +) \to < a > = (a * \mathbb{Z}, +)$$
$$n \to n * a$$
$$n, m \in \mathbb{Z}: \varphi(n+m) = (n+m) * a$$
$$\varphi(n) + \varphi(m) = n * a + m * a$$
$$= Homomorphismus\ von\ \mathbb{Z}\ in\ eine\ Untergruppe.$$

Beispiel:

$$(G, o), a \in G$$
$$\varphi: (\mathbb{Z}, +) \to (G, o)$$
$$n \to a^2$$
$$\varphi(n+m) = a^{n+m} = a^n \; o \; a^m = \varphi(n) \; o \; \varphi(m)$$
$$"Homomorphie\ bedeutet\ Vertauschbarkeit!"$$

Kern

Als Kern von φ wird das Urbild $\varphi^{-1}(\{e_h\})$ des neutralen Elements e_H bezeichnet.



Ringe und Körper

Bisher haben wir immer nur zweistellige Strukturen (z.B. $(\mathbb{Z},*)$) betrachtet. Will man jedoch das Distributivgesetz untersuchen, müssen wir eine algebraische Struktur konstruieren, die mehrere Operationen unterstützt.

Definition Ring

Folgende drei Eigenschaften müssen in Bezug auf $(R,+,*)$ erfüllt sein, damit man von einem Ring spricht:

- $(R,+)$ ist eine abelsche Gruppe (=kommutativ)
- $(R,*)$ ist eine Halbgruppe, also mindestens Assoziativ
- Es gilt das Distributivgesetz:

$$a*(b+c)=ab+ac$$
$$(a+b)*c=ac+bc$$

Definition Integritätsring

Ein kommutativer Ring mit Einselement ohne Nullteiler heißt Integritätsring.

Einselement: Das neutrale Element von $(R,*)$ wird Einselement genannt, da man als Symbol meistens das Multiplikationszeichen verwendet, und in der Multiplikation die 1 das neutrale Element ist.

Nullteiler: $a\neq 0, b\neq 0 \Rightarrow a*b=0\ oder\ b*a=0$

Körper

Ein kommutativer Ring mit Einselement $1\neq 0$, in dem jedes Element $a\neq 0$ eine Einheit ist, also ein multiplikatives Inverses besitzt, heißt ein Körper.

Verbände und Boolesche Algebren

Verband

$(M,\ \wedge,\ \vee)$ ist ein Verband, wenn folgende Eigenschaften erfüllt sind:

- $(M,\ \wedge)$ ist eine kommutative Halbgruppe
- $(M,\ \vee)$ ist eine kommutative Halbgruppe
- Es gelten die **Verschmelzungsgesetze**
  - $a=a\wedge(a\vee b)$
  - $a=a\vee(a\wedge b)$

Distributiver Verband

Es gelten die Distributivgesetzte:

$$a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$$
$$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)$$

Boole'sche Algebra

Ein distributiver Verband $(M,\wedge,\vee)$ heißt Boole'sche Algebra, wenn er die folgenden Eigenschaften besitzt:

- Es gibt ein neutrales Element zu $(M,\wedge)$
- Es gibt ein neutrales Element zu $(M,\vee)$
- Zu jedem $a\in M$ gibt es ein Komplement $a'\in M$