Zusammenfassung Lineare Algebra
Prof. Wegner

Michael Gregorius

14. März 2001

Inhaltsverzeichnis

1 Exkurs in Logik

- **Was ist eine Aussage?**
  Eine Aussage ist ein Satz, für den es sich lohnt, zu fragen, ob er wahr oder falsch ist.
- **Wie sind die Operationen $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$ definiert?**
  Siehe Matheskript bzw. Buch.
- **Was ist eine Aussageform?**
  Eine Aussageform ist eine aus den *Junktoren* $\wedge, \vee, \Rightarrow, \Leftrightarrow$, sowie $\neg$ aufgebaute komplexere Aussage.
- **Was ist eine Tautologie? Was ist eine Kontradiktion? Gibt es „etwas dazwischen“?**
  Eine Tautologie ist eine Aussage, die bei jeder Belegung der Aussagevariablen wahr ist. Eine Kontradiktion wird bei keiner Belegung wahr. Eine Aussage, die für mindestens eine Belegung wahr wird nennt man *erfüllbar*.
- **Gebe Beispiele für Tautologien! Wie werden diese bewiesen?**
  Sehr einfache Tautologien sind zum Beispiel $A \vee \neg A$ oder $\neg(A \wedge \neg A)$. Tautologien kann man mit Hilfe einer Wahrheitstabelle beweisen, indem man zeigt, daß sie für jede Belegung wahr werden.

  Weitere wichtige Tautologien sind zum Beispiel *Idempotenz, Kommutativität, Assoziativität, das Distributivgesetz, das Absorptionsgesetz,* etc.
- **Wann heißen zwei Aussageformen äquivalent? Was kann man mit äquivalenten Aussageformen machen?**
  Zwei Aussageformen heißen äquivalent, wenn sie bei gleicher Belegung der Variablen entweder beide wahr sind oder beide nicht wahr. Seien A und B Aussageformen. Dann gilt also $A \Leftrightarrow B$. Äquivalente Aussagen können untereinander ausgetauscht werden.
- **Was ist eine Aussagefunktion?**
- **Was ist ein Axiomensystem?**
- **Was ist das Induktionsaxiom?**
- **Zeige die verallgemeinerte Dreiecksungleichung per Induktion!**

2 Mengen

- **Was ist eine Menge und wie wird sie aufgeschrieben?**

Eine Menge ist die Zusammenfassung einiger Objekte zu einer neuen Gesamtheit. Man schreibt eine Menge entweder durch explizites Aufzählen ihrer Elemente oder aber durch Angabe eines Prädikats. Zum Beispiel kann man die Menge der geraden Zahlen von 1 bis 10 schreiben als:

$$M = \{2,4,6,8,10\} = \{2,4,\ldots,10\}$$

Oder aber:

$$M = \{x | x \in \mathbb{N} \wedge 1 \leq x \leq 10\}$$

- **Was ist eine (echte) Teilmenge?**

Eine Menge A ist eine Teilmenge einer Menge B ($A \subseteq B$), wenn jedes Element in A auch in B enthalten ist. A ist eine echte Teilmenge von B ($A \subset B$), wenn A eine Teilmenge von B ist und B mindestens ein Element enthält, welches nicht in A enthalten ist.

$$A \subseteq B \Leftrightarrow x \in A \Rightarrow x \in B$$
$$A \subset B \Leftrightarrow x \in A \Rightarrow x \in B \wedge \exists y \in B : y \notin A$$

- **Wie ist die Potenzmenge definiert?**

Die Potenzmenge einer Menge M ist die Menge, die alle Teilmengen von M enthält:

$$P(M) = \{A | A \subseteq M\}$$

Enthält die Menge M n Elemente, so enthält die Potenzmenge 2^n Elemente.

- **Wie sind die Vereinigung, der Durchschnitt, die Differenz und das Komplement definiert? Wie die Vereinigung und der Schnitt beliebig vieler Mengen?**

  - $A \cup B = \{x | x \in A \vee x \in B\}$
  - $A \cap B = \{x | x \in A \wedge x \in B\}$
  - $A \backslash B = \{x | x \in A \wedge x \notin B\}$
  - $A^c = M \backslash A$

- **Zeige die Entsprechung $\cap$ und $\wedge$, sowie die anderen Entsprechungen! Was folgt aus diesen Entsprechungen?**

Die Entsprechnung $\cap$ und $\wedge$ ergibt sich, da $\wedge$ zur Definition von $\cap$ benutzt wird. Die anderen Entsprechungen sind: $\cup \leftrightarrow \vee, (.)^c \leftrightarrow \neg$, sowie $\subseteq \leftrightarrow \Rightarrow$. Aus diesen Entsprechungen folgt, daß für Mengen ähnliche Gesetze wie für Aussagen gelten. (siehe Boolesche Algebra)

- **Was ist eine Boolesche Algebra?**

Eine Menge B heißt Boolesche Algebra, wenn folgendes gilt: Die Menge enthält zwei ausgezeichnete Elemente $\emptyset$ und M. Desweiteren gibt es eine Operation $(.)^c : B \to B$, sowie zwei Operationen $\cup : B \times B \to B$, sowie $\cap : B \times B \to B$. Zuletzt gelten noch die Gesetze der *Idempotenz, Assoziativität, Kommutativität, Distributivität, das Absorptionsgesetz*, sowie $A \cap A^c = \emptyset$ ($A \cup A^c = M$), $A \cap \emptyset = \emptyset$ ($A \cup M = A$) und $A \cup \emptyset = A$ ($A \cap M = A$).

- **Gebe ein Beispiel für eine Boolesche Algebra!**

Die Potenzmenge $P(M)$ einer endlichen Menge M ist ein Beispiel für eine Boolesche Algebra.

- **Was besagt das Dualitätsprinzip?**

Das Dualitätsprinzip besagt, daß eine wahre Formel für eine Boolesche Algebra wahr bleibt, wenn man durchgehend $\cup$ und $\cap$, sowie $\emptyset$ und M vertauscht.

- **Wie lautet der Satz von de Morgan?**

$$(A \cap B)^c = A^c \cup B^c \text{ bzw. } (A \cup B)^c = A^c \cap B^c$$

- **Wie ist das kartesische Produnkt endlich vieler Mengen definiert?**

Das kartesische Produkt endlich vieler Mengen $M_1, M_2, ..., M_n$ ist definiert als:

$$M_1 \times M_2 \times \cdots \times M_n = \{(x_1, x_2, \ldots, x_n) | x_1 \in M_1 \wedge x_2 \in M_2 \wedge \cdots \wedge x_n \in M_n\}$$

Es gilt desweiteren:

$$M_1 \times \cdots \times M_n = \emptyset \Leftrightarrow \exists i \in \mathbb{N} : 1 \leq i \leq n : M_i = \emptyset$$

3 Relationen und Abbildungen

- **Was ist eine (binäre,n-äre) Relation zwischen zwei Mengen bzw. in einer Menge? Was ist der Vorbereich bzw. der Nachbereich?**

Eine binäre Relation zwischen zwei Mengen M_1 und M_2 ist definiert als eine Teilmenge des kartesischen Produktes $M_1 \times M_2$. Gilt $M_1 = M_2 = M$ so spricht man von einer Relation *in M*. Eine *n*-äre Relation ist dementsprechend definiert als Teilmenge des *n*-fachen kartesischen Produktes $M_1 \times M_2 \times \cdots \times M_n$. Man schreibt statt $(x,y) \in R$ auch oft xRy, bzw. für $(x,y) \notin R$ auch $x \not Ry$.
Der Vorbereich ist definiert als:

$$V(R) = \{x | x \in M_1 \wedge \exists y \in M_2 : xRy\}$$

Der Nachbereich ist definiert als:

$$N(R) = \{y | y \in M_2 \wedge \exists x \in M_1 : xRy\}$$

- **Gebe Beispiele für Relationen!**

Zwischen beliebigen Mengen M_1 unde M_2 gibt es in jedem Fall immer die leere Relation $\emptyset$ (keine zwei Elemente stehen in Relation) und die Allrelation $M_1 \times M_2$ (alle Elemente stehen in Relation).

Oder $\in$ definiert eine Relation zwischen einer Menge M und ihrer Potenzmenge $P(M)$. Beispiel:

$$M = \{1,2,3\}, P(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Es gilt also z.B. $2R\{2,3\}$. Für den Vorbereich gilt $V(R) = \{1,2,3\}$. Der Nachbereich ist in diesem Fall $N(R) = P(M) \backslash \emptyset$, da kein Element in der Menge $\emptyset$ enthalten ist. Desweiteren gilt $R(2) = \{\{2\}, \{1,2\}, \{2,3\}, \{1,2,3\}\}$.

- **Wie lassen sich Relationen darstellen?**

Relationen lassen sich z.B. grafisch darstellen oder aber durch eine Matrix.

- **Was ist eine Abbildung?**

Eine Abbildung ist eine Relation, bei der für jedes $x \in M_1$ gilt, daß $R(x)$ einelementig ist. Also $|R(x)| = 1$. Dabei heißt M_1 *Definitionsbereich* und M_2 *Bildbereich*.

Eine Abbildung ordnet also jedem $x \in M_1$ eindeutig ein Element $y \in M_2$ zu. Im folgenden wollen wir daher unter $R(x)$ stets das Element y selbst verstehen, wenn $R(x) = y$ gilt. Die Zuordnung eines y zu jedem x drücken wir durch $x \mapsto y$ aus. Die ganze Abbildung schreiben wir als $f : M_1 \longrightarrow M_2$.

- **Wann sind Abbildungen bzw. Relationen gleich?**

Die Gleichheit zweier Relationen ist gegeben durch die Gleichheit zweier Mengen. Ebenso ist die Gleichheit zweier Kompositionen gegeben. Also sind zwei Abbildungen $f : M \longrightarrow N$ und $g : M' \longrightarrow N$ in jedem Fall *verschieden*, wenn $M \neq M'$ oder $N \neq N'$ gilt. Man kann die Gleichheit zweier Abbildungen $f, g : M \longrightarrow N$ jedoch noch anders charakterisieren: $f = g \Leftrightarrow \forall x \in M : f(x) = g(x)$.

- **Wie sind Komplement, Durchschnitt, Vereinigung und Differenz bei (binären) Relationen definiert? Warum muß man bei diesen Operationen bei Abbildungen aufpassen?**
Diese Operationen sind über die Mengendefinitionen definiert, da Relationen ja nur Teilmengen eines kartesischen Produktes sind. Wendet man diese Operationen jedoch auf Abbildungen ab, so erhält man im allgemeinen keine Abbildungen.

- **Wie ist die Komposition $\circ$ von Relationen definiert?**
Die Komposition zweier Relationen R und S ist wie folgt definiert:

$$S \circ R = \{(x_1, x_3) | x_1 \in M_1 \wedge x_3 \in M_3 \wedge \exists x_2 \in M_2 : x_1 R x_2 \wedge x_2 R x_3\}$$

Wenn man sich diese Komposition auszeichnet, steht die Relation R zwar „links“ von S, jedoch ist diese Schreibweise praktischer, da dann gilt:

$$(S \circ R)(x) = S(R(x)) \text{ bzw. für Teilmengen } A \subseteq M_1 : (S \circ R)(A) = S(R(A))$$

Also wird erst die Abbildung R vorgenommen und auf das Ergebnis wird die Abbildung S vorgenommen. Der Nachbereich von R ist also der Vorbereich von S. Daher kann die Komposition zweier Relationen auch die leere Relation $\emptyset$ sein, wenn die Relationen R und S selbst nicht leer sind. Nämlich dann, wenn $N(R) \cap V(S) = \emptyset$.

- **Was erhält man bei der Komposition von Abbildungen?**
Bei der Komposition zweier Abbildungen erhält man wieder eine Abbildung, da jedem Element der Vorbereiche jeweils nur ein Element der Nachbereich zugeordnet wird.

- **Zeige die Assoziativität der Komposition von Relationen!**
- **Was ist die identische Relation und wie ist sie definiert?**
Die identische Relation I_M ist über Gleichheit von Elementen definiert:

$$x I_M y \Leftrightarrow x = y$$

- **Wie ist die inverse Relation R^{-1} definiert?**
Die inversere Relation ist definiert als:

$$R^{-1} = \{(y, x) | x \in M_1 \wedge y \in M_2 \wedge xRy\}$$

In der grafischen Darstellung ergibt sich die inverse Relation also durch umdrehen aller Pfeile.

- **Welche Rechenregeln gibt es für inverse Relationen?**
- **Wann heißt eine Abbildung injektiv/surjektiv/bijektiv?**
Eine Abbildung $f : M \to N$ heißt

injektiv , wenn $\forall x, y \in M : x \neq y \Rightarrow f(x) \neq f(y)$.

surjektiv , wenn gilt: $f(M) = N$.

bijektiv , wenn f injektiv *und* surjektiv ist.

- **Was ergibt die Komposition zweier injektiver/surjektiver/bijektiver Abbildungen?**

Die Komposition zweier injektiver/surjektiver/bijektiver Abbildungen ergibt wieder eine injektive/surjektive/bijektive Abbildung.

- **Wie lassen sich Injektivität und Surjektivität durch Kompositionseigenschaften charakterisieren?**
- **Wie läßt sich die Bijektivität einer Abbildung noch charakterisieren?**
- **Was hat es mit der abzählbaren bzw. überabzählbaren Unendlichkeit auf sich?**

Eine nicht endliche Menge M heißt abzählbar unendlich, wenn es eine bijektive Abbildung $f : \mathbb{N} \to M$ gibt. Existiert eine solche Abbildung nicht, so heißt die Menge M überabzählbar unendlich. So gilt zum Beispiel $|\mathbb{N}| = |\mathbb{Q}|$. $\mathbb{R}$ dagegen ist schon im Intervall $[0,1]$ überabzählbar unendlich.

- **Was ist eine Familie?**
- **Was ist eine Äquivalenzrelation?**

Sei $M \neq \emptyset$ und R eine Relation in M. Dann heißt R

reflexiv , wenn $\forall x \in M : xRx$ gilt.

symmetrisch , wenn $\forall x,y \in M : xRy \Rightarrow yRx$ gilt.

transitiv , wenn $\forall x,y,z \in M : xRy \wedge yRz \Rightarrow xRz$ gilt.

Äquivalenzrelation , wenn R reflexiv, symmetrisch und transitiv ist.

- **Wie ist die Kongruenz modulo m definiert? Zeige, daß es sich um eine Äquivalenzrelation handelt!**

Die Kongruenz modulo m für festes m ist wie folgt definiert:

$$xRy \Leftrightarrow x \equiv y \mod m \Leftrightarrow \exists k \in \mathbb{Z} : x - y = k \cdot m$$

Um zu zeigen, daß es sich um eine Äquivalenzrelation handelt, muß natürlich Reflexivität, Symmetrie und Transitivität nachgewiesen werden:

Reflexivität: Interessant ist nur der Fall $m \neq 0$. Sei also $m \neq 0$. Dann muß gelten $x - x = k \cdot m$. Wie man leicht sieht, erfüllt $k = 0$ diese Gleichung immer.

Symmetrie: Es existiere ein $k \in \mathbb{Z}$, so daß $x - y = k \cdot m$ gilt. $x - y = k \cdot m$ ist das gleiche wie $-y + x = k \cdot m$. Dies multiplizieren wir auf beiden Seiten mit -1 und es ergibt sich. $y - x = (-k) \cdot m$. Für jedes $k \in \mathbb{Z}$ gilt natürlich auch $-k \in \mathbb{Z}$.

Transitivität: Es gebe k_1, k_2 mit $x - y = k_1 \cdot m$ und $y - z = k_2 \cdot m$. Dann schreiben wir $x - z$ als $x - y + y - z = k_1 \cdot m + k_2 \cdot m = (k_1 + k_2) \cdot m$. Für $k_1, k_2 \in \mathbb{Z}$ gilt natürlich auch $k_1 + k_2 \in \mathbb{Z}$.

- **Was sind Äquivalenzklassen?**
- **Was ist eine Partition?**
- **Wie kann man eine Äquivalenzrelation mit Hilfe einer Abbildung $f : M \to N$ induzieren?**

4 Halbgruppen und Gruppen

- **Was ist eine algebraische Struktur?**
Allgemein ist eine algebraische Struktur eine nichtleere Menge M mit einer Menge von Operationen. Noch allgemeiner sind algebraische Strukturen Mengen mit Relationen, da sich Operationen auch als Relationen darstellen lassen.

Man kann zum Beispiel die Addition in $\mathbb{N}$ als eine Relation $(\mathbb{N}\times\mathbb{N})\times\mathbb{N}$ auffassen, so daß z.B. gilt: $(3,5)R8$.

- **Was ist eine Verknüpfung auf M?**
Eine Verknüpfung $*$ in M ist eine Abbildung $*: M\times M \longrightarrow M$, d.h. zwei Elementen in M wird ein Element in M zugeordnet.

- **Wann ist eine Verknüpfung assoziativ/kommutativ?**
Eine Verknüpfung $*$ in M heißt

assoziativ , wenn gilt: $\forall x,y,z \in M : (x*y)*z = x*(y*z)$.

kommutativ , wenn gilt: $\forall x,y \in M : x*y = y*x$.

Bei einer assoziativen Verknüpfung kann man Klammern also weglassen, bzw. beliebig setzen und bei einer kommutativen Verknüpfung ist die Reihenfolge der an der Verknüpfung beteiligten Elemente egal.

- **Was ist ein (links-, rechts-) neutrales Element bzw. eine (links-, rechts-) Null?**
Sei $M \neq \emptyset$ mit einer Verknüpfung $*$ gegeben. Dann heißt ein Element $e \in M$

linksneutral , wenn $\forall x \in M : e*x = x$.

rechtsneutral , wenn $\forall x \in M : x*e = x$.

neutral , wenn e links- und rechtsneutral ist.

Ein Element $n \in M$ heißt

Linksnull , wenn $\forall x \in M : n*x = n$.

Rechtsnull , wenn $\forall x \in M : x*n = n$.

Null , wenn n eine Links- und Rechtsnull ist.

- **Zeige, daß es höchstens ein neutrales Element bzw. eine Null gibt!**
Angenommen, es existiert ein linksneutrales Element e und ein rechtsneutrales Element f. Dann folgt $e*f = f$ aus der Linksneutralität von e und $e*f = e$ aus der Rechtsneutralität von f. Daraus folgt dann insgesamt $e = f$. Entsprechendes beweist man für die Null.

- **Was ist eine Halbgruppe (ein Monoid, eine Gruppe)?**
Gegeben sei eine nichtleere Menge $M \neq \emptyset$ mit einer Komposition $*$. Dann heißt $(M,*)$

Halbgruppe , wenn gilt: $*$ ist assoziativ.

Monoid , wenn $(M,*)$ eine Halbgruppe ist und zudem noch ein neutrales Element e existiert.

Gruppe , wenn $(M,*)$ ein Monoid ist und es zu jedem Element $x \in M$ ein eindeutiges Element x^{-1} gibt, so daß gilt: $x * x^{-1} = e = x^{-1} * x$.

Ist die Verknüpfung $*$ kommutativ, so spricht man von einer kommutativen Halbgruppe (Monoid, Gruppe). Eine kommutative Gruppe wird auch *abelsche Gruppe* genannt.

- **Zeige die Eindeutigkeit des inversen Elements in einer Gruppe!**

Angenommen zu einem Element $x \in M$ existieren zwei neutrale Elemente x' und $\overline{x}$. Aus der Definition des inversen Elementes folgt dann $xx' = e = \overline{x}x$. Dann kann man jedoch folgende Gleichungskette aufstellen:

$$x' = ex' = (\overline{x}x)x' = \overline{x}(xx') = \overline{x}e = \overline{x}$$

- **Wie nennt man eine kommutative Gruppe?**

Eine kommutative Gruppe wird auch *abelsche Gruppe* genannt.

- **Gebe Beispiele für Halbgruppen/Monoide/Gruppen!**

Halbgruppen	$(\mathbb{N},+),(\mathbb{N},*)$ mit $x*y=x$
Monoide	$(\mathbb{N}_0,+),(\mathbb{N},\cdot),(\mathbb{Z},\cdot),(P(M),\cap),(P(M),\cup)$ $(RelX,\circ),(AbbX,\circ)$
Gruppen	$(\mathbb{Z},+),(\mathbb{R},+),(\mathbb{R}\backslash\{0\},\cdot),(PerX,\circ)$

- **Warum bilden die Mengen $RelX, AbbX$ mit der Komposition als Verknüpfung ein Monoid, obwohl es zu jeder Relation/Abbildung auch immer eine Umkehrrelation/-abbildung gibt?**
- **Wenn $(M,\cdot)$ ein Monoid ist, kann für eine Teilmenge $M^* \subseteq M$ gelten, daß $(M^*,\cdot)$ eine Gruppe ist. Zeige dies!**

Wenn wir mit M^* die Menge aller invertierbaren Elemente in M bezeichnen, so ist $(M^*,\cdot)$ eine Gruppe. Zumindest enthält M^* das neutrale Element aus M, da ein neutrales Element immer zu sich selbst invers ist. Haben zwei Elemente in M ein Inverses, so ist auch das Produkt der beiden in M^*. Denn es gilt: $x \in M^* \Rightarrow x^{-1} \in M^*$. Dann besitzt jedoch auch das Produkt ein inverses Element, denn es gilt:

$$xyy^{-1}x^{-1} = e \in M^*$$

Also ist $y^{-1}x^{-1}$ das inverse Element zu xy und damit in M^* enthalten.

- **Zeige die Kürzungsregel bzw. die eindeutige Lösbarkeit von Gleichungen für Gruppen!**

Die Kürzelsregel besagt, daß in jeder Gruppe $(M,\cdot)$ folgendes gilt:

$$\forall a,x,y \in M : (ax = ay \Rightarrow x = y) \wedge (xa = ya \Rightarrow x = y)$$

Dies beweist man wie folgt, wobei $ax = ay$ gelte:

$$x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y$$

Die eindeutige Lösbarkeit von Gleichungen besagt:

$$\forall a,b \in M : (\exists_1 x \in M : ax = b) \wedge (\exists_1 y \in M : ya = b)$$

Das heißt jedes Element der Gruppe läßt sich eindeutig durch zwei andere Elemente darstellen. Hierbei sind die Lösungen offensichtlich $x = a^{-1}b$ und $y = ba^{-1}$.

Betrachtet man die Verknüpfungtafel einer Gruppe, so fällt auf, daß in jeder Zeile und Spalte jedes Element der Gruppe immer nur einmal als Ergebnis einer Verknüfung auftaucht. Dies ist eine Konsequenz der Kürzungsregel.

- **Wie sind die Potenzgesetze definiert?**

Hier unterscheidet man zwischen multiplikativer und additiver Schreibweise. Ist $(M,\cdot)$ eine Halbgruppe in multiplikativer Schreibweise, so setzen wir:

$$\forall a \in M : a^n := \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{-mal}} \text{ für } n \in \mathbb{N}$$

Handelt es sich um ein Monoid mit neutralem Element e, so gilt weiter:

$$\forall a \in M : a^0 := e$$

Existiert auch noch ein inverses Element zu a, so gilt:

$$a^{-n} := \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{n\text{-mal}} \text{ für } n \in \mathbb{N}$$

Desweiteren gelten die Potenzgesetze:

$$\forall a \in M : (a^n)^m = a^{nm} \text{ und } a^m a^n = a^{m+n} \text{ mit } n,m \in \mathbb{N} \text{ bzw. } \mathbb{Z}$$

Handelt es sich um eine Halbgruppe in additiver Schreibweise, so setzen wir:

$$\forall a \in M : na := \underbrace{a + a + \cdots + a}_{n\text{-mal}}$$

Bei einem Monoid gilt auch hier:

$$\forall a \in M : 0a = e$$

Und wenn das inverse Element zu a existiert:

$$(-n)a := \underbrace{(-a) + (-a) + \cdots + (-a)}_{n\text{-mal}}$$

Auch hier gibt es Potenzgesetze:

$$\forall a \in M : n(ma) = (nm)a \text{ und } ma + na = (m+n)a$$

- **Was ist eine Unterstruktur?**

Ist eine Menge mit Verknüpfung und ausgezeichneten Elementen gegeben, so kann es sein, daß eine Teilmenge dieser Menge selbst schon eine Struktur (mit denselben Verknüfungen und ausgezeichneten Elementen) bildet. Zum Beispiel Unterhalbgruppen/-monoide/-gruppen.

- **Was ist ein(e) Unterhalbgruppe/Untermonoid/Untergruppe?**

Sei $\emptyset \neq U \subseteq M$ und $(M,\circ)$ eine Halbgruppe. Dann ist $(U,\circ)$ eine Unterhalbgruppe von $(M,\circ)$, wenn $(U,\circ)$ selbst eine Halbgruppe ist.

Ist $(M,\circ)$ ein Monoid, so heißt $(U,\circ)$ Untermonoid, wenn $(U,\circ)$ selbst ein Monoid mit *demselben* neutralen Element e ist. Es ist wichtig, daß es sich um dasselbe neutrale Element handelt. Denn es kann vorkommen, daß $(U,\circ)$ zwar selbst ein Monoid ist, jedoch ein anderes neutrales Element als $(M,\circ)$ hat. In diesem Falle ist $(U,\circ)$ nur eine Unterhalbgruppe.

$(U,\circ)$ ist schließlich eine Untergruppe von $(M,\circ)$, wenn $(U,\circ)$ eine Gruppe ist und ein Untermonoid von $(M,\circ)$.

- **Gebe Beispiele für Unterhalbgruppen/Untermonoide/Untergruppen!**

$(\mathbb{N},+)$ ist ein Halbgruppe und $(n\mathbb{N},+)$ mit $n \in \mathbb{N}$ ist eine Unterhalbgruppe hiervon.

Sei $M \neq \emptyset$ und $A \subseteq M$. Wie wir schon gesehen haben sind $(P(M),\cap)$ und $(P(A),\cap)$ Monoide. Desweiteren ist $P(A) \subseteq P(M)$. Im Falle $A \neq M$ ist $(P(A),\cap)$ jedoch *kein* Untermonoid von $(P(M),\cap)$, da sich in den beiden Strukturen die neutralen Elemente unterscheiden. In $(P(A),\cap)$ ist dies nämlich A und in $(P(M),\cap)$ ist es M.

$(PerM,\circ)$ ist eine Untergruppe des Monoids $(AbbM,\circ)$ welches selbst ein Untermonoid des Monoids $(RelX,\circ)$ ist.

- **Was muß man zeigen, um zu beweisen, daß $(U,\cdot)$ Untergruppe des Monoids $(M,\cdot)$ ist?**

Man muß zeigen:

$$U \neq \emptyset \wedge \forall x,y \in U : (xy \in U \wedge x^{-1} \in U)$$

- **Was ist das Erzeugnis und wie ist es definiert?**

Das Erzeugnis ist die *kleinste Unterstruktur*, die eine gegebene Teilmenge einer Struktur enthält. Um die Definition zu geben, muß man sich erst davon überzeugen, daß der Schnitt von (gleichartigen) Unterstrukturen wieder eine Unterstruktur ist:

1. Ist F eine Familie von Unterhalbgruppen/Untermonoiden/Untergruppen von M, so ist auch $\bigcap_{U \in F} U$ eine Unterhalbgruppe/Untermonoid/Untergruppe, sofern dieser Schnitt nicht leer ist. Dies ist bei Untermonoiden bzw. Untergruppen immer der Fall, da der Schnitt hier mindestens das neutrale Element enthält.

2. Ist $\emptyset \neq A \subseteq M$ und F_A die Gesamtheit aller Unterhalbgruppen bzw. Untermonoide bzw. Untergruppen, die A enthalten, so ist $\bigcap_{U \in F_A} U$ die von A erzeugte Untergruppe $\langle A \rangle_H$ bzw. das von A erzeugte Untermonoid $\langle A \rangle_M$ bzw. die von A erzeugte Untergruppe $\langle A \rangle_G$.

- **Wie gibt man für einelementige Mengen das Erzeugnis an? Beweise dies!**

Sei $(M,\cdot)$ eine Halbgruppe und $a \in M$. Dann ist $\langle a \rangle_H = \{a^n | n \in \mathbb{N}\}$ und, falls a^{-1} existiert, $\langle a \rangle_G = \{a^n | n \in \mathbb{Z}\}$. Eine von einem Element erzeugte Halbgruppe bzw. Gruppen wird *zyklisch* genannt.

Sei $B = \{a^n | n \in \mathbb{N}\}$ im Halbgruppenfall. $\langle a \rangle_H$ ist der Durchschnitt aller Unterhalbgruppen, die a enthalten. Also enthalten diese Unterhalbgruppen auch alle Potenzen

von a. Daher gilt $B \subseteq \langle a \rangle_H$. Jedoch ist B auch eine der am Durchschnitt beteiligten Halbgruppen und damit folgt $B \supseteq \langle a \rangle_H$.

- **Was ist die Ordnung einer Gruppe $(G,\cdot)$? Was ist die Ordnung eines einzelnen Elementes aus einer Gruppe?**

Ist $(G,\cdot)$ eine endliche Gruppe, so ist $|G|$ die Ordnung von G. Die Ordnung für ein einzelnes Element $a \in G$ ist die kleinste Zahl $n \in \mathbb{N}$ für die gilt: $a^n = e$.

Ist n die Ordnung von $a \in G$, so gilt $\langle a \rangle_G = \{a, a^2, ..., a^{n-1}, a^n\} = \langle a \rangle_H$. Insbesondere gilt $aa^{n-1} = a^n = e$. Also ist $a^{-1} = a^{n-1}$. Desweiteren ist die Ordnung von a in diesem Fall die Ordnung von $\langle a \rangle$.

- **Was ist die symmetrische Gruppe S_n?**

Die symmetrische Gruppe S_n ist $(Per\{1,2,...,n\},\circ)$. Die Elemente dieser Gruppe sind also alle bijektiven Abbildungen $\{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$ und die Verknüpfung ist die Komposition. id_M ist das neutrale Element und zu jeder Abbildung existiert eine eindeutige Umkehrabbildung.

- **Welche Ordnung hat die S_n? Beweise dies!**

Es gilt $|S_n| = n!$. Dies wird mit Hilfe der vollständigen Induktion nach n bewiesen.

Induktionsanfang: Im Falle $n = 1$ gilt $|M| = |N| = 1$ und es gibt nur eine bijektive Abbildung.

Induktionsannahme: Wir gehen davon aus, daß es für $|M| = |N| = n$ insgesamt $n!$ bijektive Abbildungen $f : M \longrightarrow N$ gibt.

Induktionsschluß: Es gelte jetzt $|M| = |N| = n+1$. Wir wählen uns jetzt ein $a \in M$ fest. Da die Abbildung bijektiv ist gibt es also jeweils genau ein $b \in N$, so daß $f(a) = b$. Zur Auswahl dieses b haben wir $n+1$ Möglichkeiten. Danach bleiben uns nach Induktionsannahme noch $n!$ Möglichkeiten die restlichen Elemente aus M abzubilden. Dies macht insgesamt $(n+1)n! = (n+1)!$.

- **Was ist die Zyklenschreibweise?**

Betrachten wir die Permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 7 & 4 & 3 & 2 & 5 & 6 \end{pmatrix}$, so sehen wir, daß sie die Menge $\{1,\ldots,n\}$ in Zyklen $(z_1 z_2 \ldots z_k)$ zerlegt, so daß $f(z_i) = z_{i+1}$ für $i = 1,\ldots,k-1$ und $f(z_k) = z_1$ gilt. Obige Permutation läßt sich also wie folgt schreiben: $(1862)(375)(4)$. Wenn zudem noch klar ist, in welcher S_n man sich befindet, so kann man die Fixpunkte der Permutation einfach weglassen.

Wie berechnet man jetzt die Komposition mit der Zyklenschreibweise. Ein Beispiel:

$$(12) \circ (13) = (132)$$

Auch hier lesen wir von rechts nach links. Die 1 bildet auf die 3 ab und die 3 ist in (12) ein Fixpunkt. Also ergibt sich schonmal $(13\ldots)$. Die 2 ist ein Fixpunkt und bildet dann auf die 1 ab, also schreiben wir $(13\ldots2)$. Jetzt müssen wir nur noch verifizieren, daß die 3 auf die 2 abbildet, was sie auch macht.

- **Was ist eine Transposition?**

Transpositionen sind Permutationen, die genau zwei Elemente vertauschen und die anderen fix lassen. Die Transpositionen der S_3 sind zum Beispiel: $(12), (13)$ und (23).

Es ist anzumerken, daß sich jede Permutation auch als Komposition von Transpositionen darstellen läßt, was für die Signumsabbildung praktisch ist, da es sich um eine strukturerhaltende Abbildung handelt und Transpositionen stets das Signum -1 haben. Doch dazu später mehr.

- **Ist die S_n eine kommutative Gruppe?**

Nein. Zum Beispiel gilt in der S_3:

$$(12) \circ (13) = (132) \neq (123) = (13) \circ (12)$$

- **Wie ist die Signumsabbildung σ definiert?**

Die Signumsabbildung ist für $f \in S_n$ wie folgt definiert:

$$\sigma(f) = \prod_{1 \leq i < j \leq n} \frac{f(i) - f(j)}{i - j} \in \{-1, 1\}$$

Das Ergebnis der Signumsabbildung ist also immer -1 oder 1. Wie kommt das? Betrachten wir die Formel genauer, so sehen wir, daß in den Zählern jede Zahl genau so oft vorkommt, wie in den Nennern. Dies liegt offensichtlich daran, daß wir es ja mit bijektiven Abbildungen zu tun haben. Also kommt es nur noch auf die Vorzeichen an, da sich die Zähler und Nenner zu 1 kürzen lassen.

- **Was ist ein Halbgruppen-/Monoid-/Gruppenhomomorphismus?**

Im folgenden seien M und N jeweils nichtleer.

Halbgruppenhomomorphismus: Sei $(M, \circ)$ eine Halbgruppe und $(N, *)$ eine Menge mit Verknüpfung. Dann heißt eine Abbildung $f : M \longrightarrow N$ Halbgruppenhomomorphismus, wenn gilt:

$$\forall x, y \in M : f(x \circ y) = f(x) * f(y)$$

Monoidhomomorphismus: Seien $(M, \circ)$ und $(N, *)$ Monoide mit den neutralen Elementen e_M und e_N. Dann heißt eine Abbildung $f : M \longrightarrow N$ Monoidhomomorphismus, wenn gilt:

$$f \text{ ist Halbgruppenhomomorphismus und } f(e_M) = e_N$$

Gruppenhomomorphismus: Sind $(M, \circ)$ und $(N, *)$ Gruppen, so heißt eine Abbildung $f : M \longrightarrow N$ Gruppenhomomorphismus, wenn gilt:

$$f \text{ ist ein Monoidhomomorphismus und } \forall x \in M : f(x^{-1}) = (f(x))^{-1}$$

Wie wir gleich sehen werden, reicht für einen Gruppenhomomorphismus schon, daß f ein Halbgruppenhomomorphismus ist. Der Rest ergibt sich aus den Gruppeneigenschaften.

Wenn eine Abbildung also ein Homomorphismus ist, bedeutet dies, daß sie mit allem verträglich ist, was die Struktur der beiden Mengen ausmacht.

- **Gebe Beispiele für Homomorphismen an!**

Die Abbildungsvorschrift $x \mapsto 2x$ definiert einen Halbgruppenhomomorphismus $(\mathbb{N},+) \longrightarrow (\mathbb{N},+)$ bzw. einen Gruppenhomomorphismus $(\mathbb{Z},+) \longrightarrow (\mathbb{Z},+)$. Beweis:

$$f(x+y) = 2(x+y) = 2x+2y = f(x)+f(y)$$

Die Signumsabbildung definiert einen Gruppenhomomorphismus:

$$(S_n,\circ) \longrightarrow (\{-1,1\},\cdot)$$

Da es sich um zwei Gruppen handelt ist nur noch $\sigma(x \circ y) = f(x) \cdot f(y)$ zu verifizieren:

$$\begin{aligned}
\sigma(f \circ g) &= \prod_{1 \le i < j \le n} \frac{(f \circ g)(i) - (f \circ g)(j)}{i-j} \\
&= \prod_{1 \le i < j \le n} \frac{f(g(i)) - f(g(j))}{i-j} \\
&= \prod_{1 \le i < j \le n} \frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \cdot \prod_{1 \le i < j \le n} \frac{g(i) - g(j)}{i-j} \\
&= \sigma(f) \cdot \sigma(g)
\end{aligned}$$

Die Brüche wurden also um $\frac{g(i)-g(j)}{g(i)-g(j)}$ erweitert und entsprechend aufgeteilt.

- **Was hat es mit der Strukturübertragung auf sich? Beweise dies!**

Seien M und N nichtleer mit $(M,\circ)$ ist eine Struktur und $(N,*)$ ist eine Menge mit Verknüpfung. Weiter sei $f : M \longrightarrow N$ eine strukturverträgliche Abbildung. Dann kann man die Struktur von M mit Hilfe der Abbildung f auf N übertragen. Ist M also zum Beispiel ein Monoid und $f : M \longrightarrow N$ eine strukturverträgliche Abbildung, so ist auch $(f(M),*)$ ein Monoid.

Beweis: Wir benutzen im folgenden eigentlich nur $f(x \circ y) = f(x) * f(y)$. Es gilt: $\forall y \in f(M) : \exists x \in M : f(x) = y$. Zu jedem Element aus dem Bildbereich gibt es also ein Element im Definitionsbereich, welches darauf abbildet. Jetzt zeigen wir erst, daß wenn M ein neutrales Element e_M hat, dieses auf das neutrale Element in $f(M)$ abbildet:

$$y * f(e_M) = f(x) * f(e_M) = f(x \circ e_M) = f(x) = y = f(e_M \circ x) = f(e_M) * y$$

Daraus folgt, daß $f(e_M)$ das neutrale Element in $f(M)$ sein muß, also $f(e_M) = e_N$.

Nun betrachten wir, was passiert, wenn wir die Bilder von zueinander inversen Elementen verknüpfen:

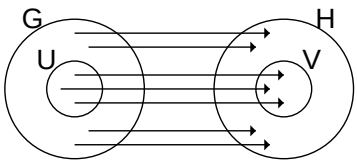
$$f(x) * f(x^{-1}) = f(x \circ x^{-1}) = f(e_M) = e_N$$

Also ist $f(x^{-1})$ das inverse Element zu $f(x)$. Sprich: $f(x^{-1}) = (f(x))^{-1}$.

- **Zeige folgenden Satz:**

Seien G,H Gruppen und $f : G \longrightarrow H$ ein Homomorphismus.

1. Ist U eine Untergruppe von G, so ist auch $f(U)$ eine Untergruppe von H.
2. Ist V eine Untergruppe von H, so ist auch $f^{-1}(V)$ eine Untergruppe von G.



Satz 1 wurde praktisch schon oben gezeigt, es reicht, die Elemente auf die Untergruppe einzuschränken.

Wir brauchen also nur noch Satz 2 zu zeigen: Zumindest ist schonmal $e_G \in f^{-1}(V)$, wegen $f(e_G) = e_H$.

- **Was sind Linksnebenklassen/Rechtsnebenklassen?**

Wie haben nun schon verschiedene Gruppen und Untergruppen kennengelernt. Man kann sich nun fragen, ob Gruppe und Untergruppe in irgend einem Verhältnis stehen. Um dies näher zu ergrüden definieren wir Links- bzw. Rechsnebenklassen:

Sei $(G,\cdot)$ eine Gruppe und $(U,\cdot)$ eine Untergruppe von G und $a \in G$. Dann bezeichnen wir mit

$$L_U(a) = aU = \{au | u \in U\} \text{ bzw. } R_U(a) = Ua = \{ua | u \in U\}$$

die Links- bzw. Rechtsnebenklassen von a. Wir nennen zwei Elemente nun äquivalent bezüglich einer Nebenklasse, wenn sie in derselben Nebenklasse liegen. Wenn also gilt:

$$x \in Uy \text{ bzw. } x \in yU$$

Dies kann man auch noch anders ausdrücken:

$$xR_Uy \Leftrightarrow xy^{-1} \in U \text{ bzw. } xL_Uy \Leftrightarrow y^{-1} \in U$$

Man kann nun zeigen, daß dies Äquivalenzrelationen sind, sie also reflexiv, symmetrisch und transitiv sind. Wir zeigen dies nun für die Rechtsnebenklassen:

reflexiv: Es gilt stets $e = xx^{-1} = \in U$. Also xR_Ux.

symmetrisch: Zu zeigen ist: $xR_Uy \Rightarrow yR_Ux$. Es gilt also $xy^{-1} \in U$. Dann gibt es jedoch ein inverses Element zu xy^{-1} in U. Dies ist logischerweise yx^{-1}. Es gilt also $yx^{-1} \in U$, also yR_Ux.

transitiv: Zu zeigen ist: $xR_Uy \wedge yR_Uz \Rightarrow xR_Uz$. Wir setzen also $xy^{-1} \in U$ und $yz^{-1} \in U$ vorraus. Da U eine Untergruppe ist, gilt auch: $xy^{-1}yz^{-1} = xz^{-1} \in U$. Also xR_Uz.

Da R_U eine Äquivalenzrelation ist, partitioniert sie die Menge, auf der sie definiert ist. Also wird G partitioniert. Jetzt wollen wir noch eine Aussage bezüglich der Mächtigkeit der Links- bzw. Rechtsnebenklassen machen. Es zeigt sich nämlich, daß gilt:

$$|aU| = |Ua| = |U|$$

Durch die durch $u \mapsto ua$ definierte Abbildung $U \longrightarrow Ua$ ist nämlich bijektiv. Dies folgt aus der Kürzungsregel. Angenommen zwei verschiedene Elemente $x, y \in U$ würden auf dasselbe Element abbilden, also $xa = ya$. Dann folgt nach der Kürzungsregel in Gruppen: $x = y$. Die Elemente wären also gleich.

Aus der Erkenntnis, daß die Menge G in gleich große Klassen partitioniert wird, folgt nun der *Satz von Lagrange*:

$$|G| = |U| \cdot |G : U|$$

In einer endlichen Gruppe ist also die Ordnung der Untergruppe ein Teiler der Gruppenordnung. Jedoch gilt *nicht*, daß es zu jedem Teiler m von $|G|$ eine Untergruppe gibt!

- **Was ist ein Normalteiler?**

Ist G eine Gruppe und U eine Untergruppe von G, so heißt U *Normalteiler*, wenn gilt:

$$\forall a \in G : aU = Ua$$

Ein Schnellerkennungsprogramm für Normalteiler sieht wie folgt aus:

$$\forall a \in G : aUa^{-1} \subseteq U$$

- **Was ist die Faktorgruppe?**

Hat man eine Gruppe $(G, \cdot)$ und U ist ein Normalteiler, so kann man die sogenannte *Faktorgruppe* ${}^{G}/_{U}$ bilden:

$${}^{G}/_{U} = \{aU | a \in G\}$$

Mit der wie folgt definierten Verknüpfung bildet ${}^{G}/_{U}$ tatsächlich eine Gruppe:

$$xU \cdot yU = (xy)U$$

Man kann sich leicht überzeugen, daß diese Verknüpfung assoziativ ist. Neutrales Element ist U bzw. $e_G U$. Inverses Element zu xU ist $x^{-1}U$. Desweiteren ist die Verknüpfung unter Ausnutzung der Normalteilereigenschaft wohldefiniert:

$$xUyU = x(Uy)U = x(yU)U = xy(UU) = (xy)U$$

Damit ist das Rechnen in der Faktorgruppe auf das Rechnen mit Rerpräsentanten zurückgeführt. Um zu wissen welches Ergebnis $xUyU$ liefert, braucht man also nur xy ausrechnen und weiß dann, welche Klasse das Ergebnis ist. Man kann sich demnach aus jeder Klasse einen Repräsentanten auswählen und dann mit diesen rechnen wie mit den ganzen Klassen.

- **Was besagt der erste Isomorphiesatz?**

Sind $(G, \cdot)$ und $(H, +)$ Gruppen und $f : G \longrightarrow H$ ein Homomorphismus, so gilt:

$${}^{G}/_{\ker f} \equiv f(G)$$

Das Bild des Homomorphismus ist also isomorph zur Faktorgruppen des Kerns der Abbildung. Auf jeden Fall ist $K := \ker f$ ein Normalteiler. Wir definieren nun eine

Abbildung $g : {}^{G}/_{K} \longrightarrow f(G)$ durch die Abbildungsvorschrift $xK \mapsto f(x)$. Wir zeigen, daß diese Abbildung ein bijektiver Homomorphismus ist, damit folgt die Behauptung. Zuerst zeigen wir die Injektivität:

$$xK = yK \Rightarrow x^{-1}y \in K \Rightarrow e_H = f(x^{-1}y) = f(x)^{-1}f(y) \Rightarrow f(x) = f(y)$$

Diese Schlusskette ich auch umkehrbar, woraus die Injektivität folgt:

$$f(x) = f(y) \Rightarrow f(x^{-1}y) = e_H \Rightarrow x^{-1}y \in K \Rightarrow xK = yK$$

Die Surjektivität ist eh klar, also bleibt nur noch zu zeigen, daß g ein Homomorphismus ist:

$$g(xKyK) = g(xyK) = f(xy) = f(x)f(y) = g(xK)g(yK)$$

- **Was folgt aus dem ersten Isomorphiesatz?**
Aus dem ersten Isomorphiesatz folgt z.B., daß $({}^{\mathbb{Z}}/_{n\mathbb{Z}}, +)$ für alle $n \in \mathbb{N}$ die bis auf Isomorphie einzige zyklische Gruppe der Ordnung n ist.
Beweis: Sei $G =< a >$ zyklisch von der Ordnung n, d.h. $a^n = e$. Dann definieren wir eine Abbildung $f : (\mathbb{Z}, +) \longrightarrow (G, \cdot)$ durch $k \mapsto a^k$. Der Kern dieser Abbildung ist, wie man leicht einsieht $n\mathbb{Z}$. Die Abbildung ist ein surjektiver Homomorphismus, denn es gilt:

$$f(x+y) = a^{x+y} = a^x a^y = f(x)f(y)$$

Damit gilt also:

$$({}^{\mathbb{Z}}/_{n\mathbb{Z}}, +) \equiv (G, \cdot)$$

5 Ringe und Körper

- **Was ist ein Ring?**
Ein Ring $(R,+,\cdot)$ ist eine nichtleere Menge R mit zwei Operationen $+$ (Addition) und $\cdot$ (Multiplikation) für die gilt:

R1 $(R,+)$ ist eine abelsche Gruppe.

R2 $(R,\cdot)$ ist eine Halbgruppe.

R3 Es gelten die Distributivgesetze: $\forall x,y,z \in R : \begin{cases} x(y+z) = xy+xz \\ (x+y)z = xz+yz \end{cases}$

Das neutrale Element bezüglich der Addition wird *Nullelement* genannt. Ist $(R,\cdot)$ ein Monoid, so nennt man das neutrale Element der Multiplikation *Einselement*.

- **Wann heißt ein Ring kommutativ?**
Wenn die Multiplikation kommutativ ist.

- **Was ist ein Körper?**
Ein Ring R heißt Körper, wenn gilt:

R4 $(R\backslash\{0\},\cdot)$ ist eine abelsche Gruppe.

- **Warum betrachtet man bei Körpern bezüglich der Multiplikation die Menge ohne die Null.**
Weil für jedes Element $x \in R$ gilt:

$$0x = 0 \neq 1$$

Dabei ist 1 das neutrale Element der Multiplikation. Somit besitzt die 0 kein inverses Element.

- **Gebe Beispiele für Ringe und Körper!**
Mit der gewöhnlichen Addition und Multiplikation ist $\mathbb{Z}$ ein Ring und $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.

- **Zeige, daß sich das Nullelement auch bezüglich der Multiplikation wie eine Null verhält!**
Dies zeigt man über folgende Gleichungkette:

$$0+0x = 0x = (0+0)x = 0x+0x$$

Mit der Kürzungsregel folgt dann $0x = 0$. Analog zeigt man $x0 = 0$.

- **Warum ist ein Körper immer nullteilerfrei?**
Weil $(R\backslash\{0\},\cdot)$ eine abelsche Gruppe ist und daher für zwei beliebige $x,y \in R$ gilt: $xy \in R\backslash\{0\}$. Es gibt also keine von Null verschiedenen Elemente die auf die Null abbilden.

- **Was ist ein Unterring? „Erkennungsprogramm“?**

Ist $(R,+,\cdot)$ ein Ring und es gilt $S \subseteq R$, so heißt S Unterring von R, wenn S selbst ein Ring ist. Es gilt:

$$S \text{ ist ein Unterring } \Leftrightarrow \forall x,y \in S : \begin{cases} x-y \in S \\ xy \in S \end{cases}$$

- **Was ist ein Ringhomomorphismus?**

Es seien R,S Ringe und $f : R \longrightarrow S$ eine Abbildung. Dann gilt:

$$f \text{ ist ein Ringhomomorphismus } \Leftrightarrow \forall x,y \in R : \begin{cases} f(x+y) = f(x)+f(y) \\ f(x\cdot y) = f(x)\cdot f(y) \end{cases}$$

- **Zeige, daß $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ nur dann ein endlicher Körper ist, wenn n eine Primzahl ist!**

Da $(\mathbb{Z}/n\mathbb{Z},+)$ eine abelsche Gruppe ist, müssen wir uns nur noch fragen, wann $(\mathbb{Z}/n\mathbb{Z},\cdot)$ eine abelsche Gruppe ist. Damit $(\mathbb{Z}/n\mathbb{Z},\cdot)$ eine Gruppe ist, muß gelten, daß Gleichungen eindeutig lösbar sind. So hat die Gleichung $\overline{a}+\overline{x}=\overline{b}$ in $(\mathbb{Z}/n\mathbb{Z},+)$ immer eine eindeutige Lösung, nämlich $\overline{x}=\overline{b}-\overline{a}$. Es gibt jedoch Beispiele für die eine solche Gleichnug keine Lösung hat. So zum Beispiel die Gleichung $\overline{2}\cdot\overline{x}=\overline{3}$ in $(\mathbb{Z}/6\mathbb{Z},\cdot)$.

Wir müssen uns also die Frage stellen, wann denn die Gleichung $\overline{a}\cdot\overline{x}=\overline{b}$ eine Lösung hat. Zuerst stellen wir fest, daß folgende Äquivalenz gilt:

$$\exists \overline{x} \in \mathbb{Z}/n\mathbb{Z} : \overline{a}\cdot\overline{x}=\overline{b} \Leftrightarrow \exists x,y \in \mathbb{Z} : ax+ny=b$$

Dies gilt (für $a,n \in \mathbb{Z}$ gegeben) wegen:

$$\begin{aligned} \overline{a}\cdot\overline{x}=\overline{b} &\Leftrightarrow (a+n\mathbb{Z})(x+n\mathbb{Z}) = b+n\mathbb{Z} \\ &\Leftrightarrow ax+an\mathbb{Z}+xn\mathbb{Z}+n\mathbb{Z}n\mathbb{Z} = b+n\mathbb{Z} \\ &\Leftrightarrow ax+n\mathbb{Z}+n\mathbb{Z}+n\mathbb{Z} = b+n\mathbb{Z} \\ &\Leftrightarrow ax+n\mathbb{Z} = b \\ &\Leftrightarrow \exists x,y \in \mathbb{Z} : ax+ny=b \end{aligned}$$

Jetzt müssen wir uns also die Frage stellen, welche $b \in \mathbb{Z}$ sich in der Form $b=ax+ny$ mit $x,y,a,n \in \mathbb{Z}$ darstellen lassen. Wir werden sehen, daß dies die Vielfachen des ggT von a und n sind. Nach dem Lemma von Bezout gilt nämlich, daß wenn d der ggT von a und n ist, sich d darstellen läßt als

$$\text{ggT}(a,n) = d = ax+ny$$

Also lassen sich auch die Vielfachen des ggT in dieser Form darstellen, wegen:

$$m\cdot d = m(ax+ny) = a\underbrace{mx}_{\in\mathbb{Z}} + n\underbrace{my}_{\in\mathbb{Z}}$$

Demnach besitzt doch $ax+ny=b$ eine Lösung, wenn der ggT von a und n ein Teiler von b ist, also $\text{ggT}(a,n)|b$ oder anders gesagt, wenn b ein Vielfaches des ggT von a und n ist. Die Gleichung besitzt also immer eine eindeutige Lösung für $\text{ggT}(a,n)=1$. Und dies ist immer der Fall wenn n eine Primzahl ist.

- **Was ist der ggT zweier Zahlen?**

Der ggT zweier Zahlen $a,n \in \mathbb{Z}$ ist die Zahl $d \in \mathbb{N}$, für die gilt:

$$d|a \wedge d|n \wedge (s|a \wedge s|n) \Rightarrow s|d$$

- **Wie berechnet man den ggT?**

Zur Berechnung des ggTs kann man den euklidischen Algorithmus benutzen. Dieser funktioniert wie folgt: Seien $a,n \in \mathbb{Z}$ und $a \neq 0$. Wir setzen $r_0 = a$ und $r_1 = |n|$ stellen folgende Kette auf:

$$\begin{aligned} r_0 &= q_0 r_1 + r_2 \\ r_1 &= q_1 r_2 + r_3 \\ &\dots \\ r_{m-1} &= q_{m-1} r_m + r_{m+1} \\ r_m &= q_m r_{m+1} \end{aligned}$$

Dabei gilt stets für $r_k = q_k r_{k+1} + r_{k+2}$, daß $0 \leq r_{k+2} < r_{k+1}$. Dies machen wir so lange bis $r_{m+2} = 0$ gilt, denn dann ist r_{m+1} der gesuchte ggT.

Der Algorithmus terminiert auch tatsächlich, da ja stets $r_1 > r_2 > \dots > 0$ gilt. Desweiteren ist r_{m+1} auch tatsächlich der ggT. Durchläuft man die Kette von unten nach oben, so sieht man, daß r_{m+1} ein Teiler von $r_m, r_{m-1}, \dots, r_1, r_0$ ist. So läßt sich r_m als ein Vielfaches von r_{m+1} beschreiben. Setzt man dies in die Formel für r_{m-1} ein, sieht man, daß sich auch r_{m-1} als ein Vielfaches von r_{m+1} beschreiben läßt, usw. Nun durchlaufen wir die Kette von oben nach unten. Angenommen s ist ein weiterer gemeinsamer Teiler von $r_0 = a$ und $r_1 = |n|$. Dann gilt $r_0 = s \cdot x_0$ und $r_1 = s \cdot x_1$. Setzt man dies ein, ergibt sich:

$$\begin{aligned} s \cdot x_0 &= q_0 \cdot s \cdot x_1 + r_2 \\ r_2 &= s \cdot x_0 - q_0 \cdot s \cdot x_1 \\ r_2 &= s(x_0 - q_0 x_1) \end{aligned}$$

Also ist s dann auch ein Teiler von r_2. Da s nun Teiler von r_1 und r_2 ist, ergibt sich, daß es auch ein Teiler von r_3 sein muß. Dies setzt sich bis r_{m+1} fort, so daß ein beliebiger Teiler von a und n, dann auch ein Teiler von r_{m+1} ist. Damit ist r_{m+1} der gesuchte ggT.

- **Was besagt das Lemma von Bezout? Beweis?**

Das Lemma von Bezout besagt, daß wenn d der ggT von $a,n \in \mathbb{Z}$ ist, zwei ganze Zahlen $x,y \in \mathbb{Z}$ existieren mit:

$$\text{ggT}(a,n) = d = ax + ny$$

Der ggT läßt sich also als Linearkombination von a und n schreiben. Der Beweis erfolgt über den euklidischen Algorithmus zur ggT-Berechnung.

- **Zeige folgenden Satz!**

$$\mathbb{Z}/_{n\mathbb{Z}} \text{ ist ein Körper } \Leftrightarrow n \text{ ist eine Primzahl}$$

Zu zeigen sind beide Richtungen:

„⇒“: Angenommen, n wäre keine Primzahl. Dann gäbe es eine Primfaktorzerlegung und n wäre darstellbar als Produkt zweier Zahlen $pq = n$. Daraus würde folgen, daß ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ Nullteiler enthält, nämlich p und q und es würde gelten:

$$(p+n\mathbb{Z})(q+n\mathbb{Z}) = pq+n\mathbb{Z} = n+n\mathbb{Z} = 0+n\mathbb{Z}$$

Dann wäre ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ jedoch kein Körper.

„⇐“: Wenn n eine Primzahl ist, gilt für jedes $a \in \{1,\ldots,n-1\}$:

$$\mathrm{ggT}(a,n) = 1$$

Also gibt es $x,y \in \mathbb{Z}$ mit:

$$ax+ny = 1$$

Dies kann man jedoch umstellen zu:

$$1-ax = ny$$

Dies ist die altbekannte Kongruenz modulo n. 1 und ax sind also in einer Äquivalenzklasse, d.h.

$$[ax] = [1] \Leftrightarrow [a][x] = [1]$$

Also gibt es zu jedem $[a]$ in ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ ein $[x]$, welches verknüpft mit $[a]$ auf das neutrale Element der Multiplikation abbildet. Jedes Element besitzt also ein inverses, also ist $({}^{\mathbb{Z}}/_{n\mathbb{Z}}\backslash\{[0]\},\cdot)$ eine (kommutative) Gruppe und damit $({}^{\mathbb{Z}}/_{n\mathbb{Z}},+,\cdot)$ ein Körper.

6 Vektorräume

- **Was ist ein Vektorraum?**
Ein Vektorraum ist eine nicht leere Menge V mit zwei Operationen

  1. $+ : V \times V \longrightarrow V$ (Addition)
  2. $\cdot : K \times V \longrightarrow V$ (äußere Multiplikation)

wobei K ein Körper ist und folgende Gesetze gelten:

V1 $(V,+)$ ist eine abelsche Gruppe.

V2 Es gilt: $\forall x,y \in V \wedge \forall r,s \in K :$ $\begin{cases} (r+s)\vec{x} = r\vec{x}+s\vec{x} \\ r(\vec{x}+\vec{y}) = r\vec{x}+r\vec{y} \\ r(s\vec{x}) = (rs)\vec{x} \\ 1\vec{x} = \vec{x} \end{cases}$

- **Zeige, daß folgendes gilt:**

  1. $r\vec{x} = \vec{0} \Leftrightarrow (r = 0 \vee \vec{x} = \vec{0})$
  2. $(-1)\vec{x} = -\vec{x}$

Beweis:

1. „$\Leftarrow$“: Zuerst zeigen wir, daß Behauptung für $r = 0$ gilt:

$$\vec{0} + 0\vec{x} = 0\vec{x} = (0+0)\vec{x} = 0\vec{x} + 0\vec{x}$$

   Hieraus ergibt sich mit der Kürzungregel für Gruppen: $0\vec{x} = \vec{0}$. Analog argumentiert man für $\vec{x} = \vec{0}$:

$$\vec{0} + 0\vec{x} = 0\vec{x} = (0+0)\vec{x} = 0\vec{x} + 0\vec{x}$$

   „$\Rightarrow$“: Hier muß $r \neq 0$ sein, sonst gilt nach dem ersten Beweisteil $0\vec{x} = \vec{0}$. Sei also $r \neq 0$ und es gelte $r\vec{x} = \vec{0}$. Dann gilt folgende Kette:

$$\vec{x} = (r^{-1}r)\vec{x} = r^{-1}(r\vec{x}) = r\vec{0} = \vec{0}$$

2. Auch dieser Beweis geht mit einer kurzen Gleichungkette:

$$\vec{x} + (-1)\vec{x} = 1\vec{x} + (-1)\vec{x} = (1 + (-1))\vec{x} = 0\vec{x} = \vec{0}$$

   Also ist $(-1)\vec{x}$ das inverse Element zu $\vec{x}$ und damit $-\vec{x}$.

- **Gebe Beispiele für Vektorräume!**
Einer der wichtigsten Vektorräume ist der K^n mit der komponentenweise definierten Addition und Multiplikation:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

Und die Multiplikation:

$$r\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ ra_2 \\ \vdots \\ ra_n \end{pmatrix}$$

- **Was ist ein Unterraum?**
Sei V ein K-Vektorraum. Dann heißt eine Teilmenge $U \subseteq V$ mit $U \neq \emptyset$ ein Unterraum von V, wenn U selbst ein K-Vektorraum ist. Triviale Unterräume sind V selbst, sowie $\{\vec{0}\}$. Ist $\vec{v} \in V$, so ist auch $K\vec{v} = \{r\vec{v} | r \in K\}$ ein Unterraum von V.

- **Welches „Erkennungsprogramm" gibt es für Unterräume?**
Ist V ein Vektorraum, so gilt:

$$U \text{ ist ein Unterraum von } V \Leftrightarrow \forall x,y \in U, \forall r \in K : \begin{cases} x+y \in U \\ rx \in U \end{cases}$$

- **Was ist eine Linearkombination?**
Eine endliche Summe der Form

$$\sum_{k=1}^{n} r_k \vec{v}_k$$

heißt eine Linearkombination der Vektoren $\vec{v}_1, \ldots, \vec{v}_n$.

- **Wie sieht das Erzeugnis bei Vektorräumen aus?**
Wie bei anderen algebraischen Strukturen kann man auch bei Vektorräumen ein Erzeugnis definieren. Allerdings ist es bei Vektorräumen einfacher, das Erzeugnis für Mengen mit mehr als einem Element anzugeben. Die *lineare Hülle* einer Teilmenge A eines Vektorraumes V ist definiert als:

$$\operatorname{lin} A := \bigcap_{U \in F_A} U.$$

Dabei ist F_A die Familie aller Unterräume, die A enthalten. Dabei setzen wir desweiteren $\operatorname{lin} \emptyset = \{\vec{0}\}$. Für eine einelementige Menge ist das Erzeugnis $\operatorname{lin}\{\vec{a}\} = K\vec{a}$. Wie schon gesagt, kann man das Erzeugnis größerer Mengen hier auch leicht angeben. Sei $A \subseteq V$ und V ein K-Vektorraum:

$$\operatorname{lin} A := \left\{ \sum_{k=0}^{n} r_k \vec{v}_k | n \in \mathbb{N} \wedge r_1, \ldots, r_n \in K \wedge \vec{v}_1, \ldots, \vec{v}_n \in A \right\}$$

Das Erzeugnis von A ist also die Menge aller Linearkombinationen der Vektoren aus A.
Beweis: Es gilt auf jeden Fall $W \subseteq \operatorname{lin} A$, da die lineare Hülle alle Vielfachen von $\vec{x} \in A$ enthalten muß. Denn sonst wäre $\operatorname{lin} A$ ja kein Vektorraum. Aus demselben Grund muß $\operatorname{lin} A$ auch alle Summen enthalten. Und mit beidem kombiniert alle Linearkombinationen.

Es gilt jedoch auch $\operatorname{lin} A \subseteq W$. Zuerst einmal ist W wie wir schon gesehen haben ein Untervektorraum von V. Es gilt jedoch auch $A \subseteq W$, da jeder Vektor $\vec{x} \in A$ in W enthalten ist, nämlich als $1\vec{x}$. Also ist W am Schnitt beteiligt und damit gilt $\operatorname{lin} A \subseteq W$. Beides zusammen ergibt die Gleichheit.

- **Was ist ein Vektorraumhomomorphismus bzw. eine lineare Abbildung?**

Es seien V, W beides K-Vektorräume. Eine Abbildung $f : V \longrightarrow W$ heißt genau dann *Vektorraumhomomorphismus* oder *lineare Abbildung*, wenn gilt:

$$\forall x, y \in V, \forall r \in K : \begin{cases} f(\vec{x}+\vec{y}) = f(\vec{x}) + f(\vec{y}) \\ f(r\vec{x}) = r \cdot f(\vec{x}) \end{cases}$$

Ist die Abbildung bijektiv handelt es sich um einen *Vektorraumisomorphismus*. Gilt zudem $V = W$, spricht man von einem *Vektorraumautomorphismus*.

Eine lineare Abbildung ist stets verträglich mit Linearkombinationen, d.h. es gilt:

$$\forall n \in \mathbb{N}, \vec{x}_1, \ldots, \vec{x}_n \in V, \forall r_1, \ldots, r_k \in K : f\left(\sum_{k=1}^{n} r_k \vec{x}_k\right) = \sum_{k=0}^{n} r_k f(\vec{x}_k)$$

Dies beweist man per Induktion nach der Anzahl der Summanden.

- **Gebe Beispiele für lineare Abbildungen!**

Stets ist die Nullabbildung $\vec{x} \mapsto \vec{0}$ eine lineare Abbildung. Durch die Identität $\mathrm{id}_V : \vec{x} \mapsto \vec{x}$ und durch $\vec{x} \mapsto r\vec{x}$ mit $r \in K$ beliebig aber fest, werden Vektorraumautomorphismen definiert.

Ein Beispiel für eine etwas kompliziertere lineare Abbildung ist die Differentation $f \mapsto f'$ im Vektorraum aller auf ganz $\mathbb{R}$ differenzierbaren Funktionen.

- **Wann sind zwei Unterräume komplementär?**

Sei V ein K-Vektorraum. Zwei Unterräume U_1 und U_2 heißen komplementär, wenn V ihre direkte Summe ist, d.h.:

$$V = U_1 + U_2 \text{ und } U_1 \cap U_2 = \emptyset$$

- **Was besagt der erste Isomorphiesatz (für Vektorräume)?**

Sei $f : V \longrightarrow W$ eine lineare Abbildung zwischen zwei K-Vektorräumen. Dann gibt es einen Vektorraumisomorphismus ${}^{V}/_{\ker f} \cong f(V)$. Wir benutzen dieselbe Abbildung, wie beim Isomorphiesatz für Gruppen. Nämlich $\vec{x} + \ker f \mapsto f(\vec{x})$. Da V bezüglich der Addition eine Gruppe ist, stimmt die Aussage bis hierhin schonmal. Es ist also nur noch zu zeigen, daß diese Abbildung mit der äußeren Multiplikation verträglich ist. Dies ist jedoch der Fall, da f verträglich ist:

$$g(r(\vec{x} + \ker f)) = g(r\vec{x} + \ker f) = f(r\vec{x}) = rf(\vec{x}) = rg(\vec{x} + \ker f)$$

- **Wann heißt eine Familie von Vektoren linear abhängig bzw. unabhängig?**

Eine Familie $(\vec{a}_1, \ldots, \vec{a}_m)$ von Vektoren heißt linear abhängig, wenn sie nicht-trivial zum Nullvektor $\vec{0}$ linearkombiniert werden können:

$$\exists r_1, \ldots, r_m \in K : \sum_{k=1}^{m} r_k \vec{a}_k = \vec{0} \wedge \exists k \in \{1, \ldots, m\} : r_k \neq 0$$

Man kann dies auch umformulieren zu: $(\vec{a}_1, \ldots, \vec{a}_m)$ ist linear unabhängig $\Leftrightarrow$:

$$\forall r_1, \ldots, r_m \in K : \sum_{k=1}^{m} r_k \vec{a}_k = 0 \Rightarrow r_i = 0 \text{ mit } 1 \leq i \leq k$$

Aus dieser Definition ergeben sich schon einige Eigenschaften:

1. Eine Familie, in der ein Vektor tatsächlich mehr als einmal vorkommt, ist linear abhängig.
2. Eine Familie, in der der Nullvektor vorkommt, ist linear abhängig.
3. Eine Teilmenge einer linear unabhängigen Menge ist wieder linear unabhängig.
4. Eine Familie, die eine linear abhängige Teilfamilie enthält, ist ebenfalls linear abhängig.
5. In einer linear abhängigen Familie gibt es *mindestens* einen Vektor, der sich als Linearkombination der anderen Vektoren schreiben läßt.

- **Was ist eine Basis?**

Sei V ein (endlich erzeugter) K-Vektorraum und $V \neq \{\vec{0}\}$. B sei eine Menge von Vektoren aus V. Dann heißt B eine *Basis* von V, wenn eine der drei äquivalenten Aussagen erfüllt ist:

1. B ist ein *minimales Erzeugendensystem* für V, d.h. $\operatorname{lin} B = V$ und keine Teilmenge von B ist ebenfalls ein Erzeugendensystem.
2. B ist eine *maximale, linear unabhängige Teilmenge* von V, d.h. jede echte Obermenge von B ist linear abhängig.
3. Jeder Vektor aus V besitzt genau *eine Darstellung als Linearkombination* der Vektoren aus B.

- **Was besagt der Basisergänzungssatz?**

Sei V ein K-Vektorraum. Der Basisergänzungssatz besagt, daß man jede Menge linear, unabhängiger Vektoren aus V zu einer Basis B von V ergänzen kann, wenn man ein Erzeugendensystem E hat. Es gilt dann:

$$A \subseteq B \text{ und } B \backslash A \subseteq E$$

- **Was besagt das Austauschlemma von Steinitz?**

Es seien B_1 und B_2 zwei Basen des Vektorraumes V und desweiteren sei $\vec{a} \in B_1$. Es gibt dann ein $\vec{b} \in B_2$, so daß auch $(B_1 \backslash \{\vec{a}\}) \cup \{\vec{b}\}$ eine Basis von V ist.
Beweis: Wir benutzen den Basisergänzungssatz mit $A = B_1 \backslash \{\vec{a}\}$ und den Erzeugendensystem $E = B_2$. Dieser liefert eine Basis B mit $A \subseteq B$ und $B \backslash A \subseteq B_2$. Dabei besteht $B \backslash A$ aus genau einem Element $b \in B_2$.

- **Was folgt aus dem Austauschlemma von Steinitz?**

- **Was ist die Dimension eines Vektorraumes? Welche Formeln gelten?**
- **Wodurch ist eine lineare Abbildung eindeutig bestimmt?**
- **Zeige, daß jeder n-dimensionale Vektorraum isomorph zu K^n ist!**

7 Matrizen und lineare Gleichungssysteme

- **Was haben Matrizen mit linearen Abbildungen zu tun?**

Ein lineares Gleichungssystem hat folgende Form:

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n = b_1 \\ \vdots & + & \vdots & + & + & \vdots & = \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n = b_m \end{array}$$

Dabei können wir die $x_i, 1 \leq i \leq n$ und die $b_j, 1 \leq j \leq m$ zu folgenden Vektoren $\vec{x}$ und $\vec{b}$ zusammenfassen:

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ und } \vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

Dann definiert die Zuordnung

$$\vec{x} \mapsto \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}$$

eine lineare Abbildung $f : \mathbb{R}^n \longrightarrow \mathbb{R}^m$. Im obigen Beispiel soll diese Abbildung also $\vec{b}$ ergeben. Über Erkenntnisse bezüglich linearer Abbildungen können wir also Erkenntnisse bezüglich linearer Gleichungssysteme gewinnen.

Wir werden bald sehen, daß die obige Abbildung *die* allgemeine lineare Abbildung ist, denn sie entspricht ja $\vec{x} \mapsto A\vec{x}$.

Zuerst einmal ist festzuhalten, daß ja jeder n-dimensionale Vektorraum isomorph ist zu K^n. Die isomorphe Abbildung wird gegeben durch:

$$\vec{v} = \sum_{k=1}^{n} x_k v_k \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Es kommt bezüglich einer fest gewählten Basis also nur auf die Skalare an, da durch sie ein Vektor *eindeutig* bestimmt ist. Die Abbildung ist also auf jeden Fall injektiv. Sie ist auich surjektiv, da jede Belegung $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ja einen Vektor aus V darstellen muß, da V sonst kein Vektorraum wäre.

Die Basisvektoren $B_V = \{v_1, v_2, ..., v_n\}$ werden dabei auf die kanonischen Basisvektoren des K^n abgebildet, also auf $e_1, e_2, ..., e_n$. Wie wir schon gesehen haben wird eine lineare Abbildung $f : V \longrightarrow W$ eindeutig dadurch definiert, daß wir zu jedem Basisvektor aus V seinen Bildvektor in W angeben. Wenn in W auch eine Basis B_W gegeben ist, lassen sich die Bilder also eindeutig bezüglich dieser Basis darstellen, also $f(\vec{v}_k) = \sum_{i=1}^{m} a_{ik}\vec{w}_i, \forall k \in \{1, \ldots, n\}$. Wenn wir die Bilder aller n Basisvektoren aus V in

dieser Form angeben, wobei es ja auch (bezüglich fester Basis in W) wieder nur auf die Skalare a_{ik} ankommt, erhalten wir ein Schema mit $m \cdot n$ Elementen, eine $m \times n$-Matrix:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \text{ mit } a_{ik} \in K \text{ für } i \in \{1,...,m\}, k \in \{1,...,n\}$$

Die Elemente mit $i = k$ bilden die *Hauptdiagonale* der Matrix. Im Falle $m = n$ heißt die Matrix *quadratisch*. Die Gesamtheit aller $m \times n$-Matrizen über dem Körper K wird mit $M(m \times n, K)$ bezeichnet, die Gesamtheit aller quadratischen Matrizen $n \times n$-Matrizen mit $M_n(K)$.

Zwischen linearen Abbildungen $f : V \longrightarrow W$ und Matrizen besteht also eine bijektive Beziehung. Jeder linearen Abbildung $f : V \longrightarrow W$ wird also in eindeutiger Weise eine Matrix A zugeordnet, die wie oben gebildet wird. Ebenso entspricht jeder Matrix A genau eine lineare Abbildung $f_A : V \longrightarrow W$, wobei in den Spalten der Matrix A die Koordinatentupel der Bilder der Basisvektoren aus V stehen.
Das Bild eines beliebigen Vektors $\vec{v} = \sum_{k=1}^{n} x_k \vec{v}_k$ ist also:

$$f(\vec{v}) = f\left(\sum_{k=1}^{n} x_k \vec{v}_k\right) = \sum_{k=0}^{n} x_k f(\vec{v}_k) = \sum_{k=0}^{n} x_k \sum_{i=0}^{m} a_{ik} \vec{w}_i = \sum_{i=1}^{m} (\sum_{k=1}^{n} a_{ik} x_k) \vec{w}_i$$

Die Vektoren werden hier im übrigen mit ihren Koordinatentupeln identifiziert.
Zusammenfassung:
Bezüglich fest gewählter Basen $B_V = \{v_1, \dots, v_n\}$ und $B_W = \{w_1, \dots, w_m\}$ wird durch jede $m \times n$-Matrix $A = (a_{ik})$ eine lineare Abbildung $f_A : V \longrightarrow W$ definiert, wobei gilt:

$$f_A(\sum_{k=1}^{n} x_k \vec{v}_k) = \sum_{i=1}^{m} (\sum_{k=1}^{n} a_{ik} x_k) \vec{w}_i$$

Die Zuordnung $A \mapsto f_A$ liefert eine bijektive Abbildung aus der Menge aller $m \times n$-Matrizen in die Menge aller linearen Abbildungen $f : K^n \longrightarrow K^m$.

Mit der elementweise Addition und skalaren Multiplikation bildet $M(m \times n, K)$ einen zu $K^{m \cdot n}$ isomorphen Vektorraum. Kommen wir jedoch darauf zurück, daß durch Matrizen lineare Abbildungen gegeben sind. Wie wir schon in früheren Kapiteln gesehen haben, kann man (lineare) Abbildungen komponieren und das Ergebnis ist wieder eine (lineare) Abbildung. Interessanterweise kann man für Matrizen eine Multiplikation definieren, die der Komposition von Abbildungen entspricht. Beweis: siehe *Skript*.

Für $A \in M(k \times m, K)$ und $B \in M(m \times n, K)$ wird das Matrizenprodukt AB definiert durch:

$$AB = (c_{hi}) \text{ mit } c_{hi} = \sum_{j=1}^{m} a_{hj} b_{ji} \text{ für } h \in \{1, \dots, k\}, i \in \{1, \dots, n\}$$

Das Produkt ist also nur definiert, wenn die Anzahl der Spalten von A mit der Anzahl der Zeilen von B übereinstimmt. (Merken über lineare Gleichungssysteme)

Insbesondere ist das Matrizenprodukt nicht kommutativ. Insgesamt gilt also für das Matritzenprodukt:

$$f_A \circ f_B = f_{AB}$$

$M(m \times n, K)$ ist bezüglich der Addition eine abelsche Gruppe und bezüglich der Multiplikation gelten (sofern definiert):

Assoziativgesetz: $A(BC) = (AB)C$

Das Assoziativgesetz gilt allein schon, weil Matrizen lineare Abbildungen und damit Relationen sind. Relationen sind assoziativ:

$$f_{(AB)C} = f_{AB} \circ f_C = (f_A \circ f_B) \circ f_C = f_A \circ (f_B \circ f_C) = f_{A(BC)}$$

Distributivgesetze: $A(B+C) = AB+AC$
$(A+B)C = AC+BC$

Die Gültigkeit des Distributivgesetzes ergibt sich daraus, daß wir mit Elementen aus dem Körper K rechnen und dort gilt: Sind $A \in M(k \times m, K)$ und $B, C \in M(m \times n, K)$ dann gilt für das Ergebnis $A(B+C) \in M(k \times n)$ bzw. für das Element (h,i):

$$\sum_{j=1}^{m} a_{hj}(b_{ji} + c_{ji}) = \underbrace{\sum_{j=1}^{m} a_{hj} b_{ji}}_{(h,i) \text{ in } AB} + \underbrace{\sum_{j=1}^{m} a_{hj} c_{ji}}_{(h,i) \text{ in } AC}$$

Desweiteren gibt es in $M_n(K)$ ein neutrales Element E_n bezüglich der Multiplikation, die *Einheitsmatrix*. Sie ist definiert als:

$$E_n = (\delta_{ik}) \in M_n(K) \text{ mit } \delta_{ik} = \begin{cases} 1 \text{ für } i = k \\ 0 \text{ sonst} \end{cases}$$

Es gilt insbesondere für $M(m \times n, K)$:

$$AE_n = A \text{ und } E_m A = A$$

Im Falle der quadratischen Matrizen gelten also das Assoziativ- und Distributivgesetz der Multiplikation, sowie die Existenz eines neutralen Elementes im Sinne eines Monoids ($E_n A = A = AE_n$). Also ist $M_n(K)$ ein Ring mit Einselement.

- **Was haben Matrizen mit linearen Gleichungssystemen zu tun?**

Wie wir oben schon gesehen haben, lassen sich lineare Gleichungssysteme auch als Abbildungen $f : K^n \longrightarrow K^m$ auffassen. Betrachten wir noch einmal folgende Abbildung:

$$\vec{x} \mapsto \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}$$

Es fällt auf, daß sie dem oben definierten Matrizenprodukt $A\vec{x}$ entspricht, wenn wir den Vektor $\vec{x}$ als eine $n \times 1$-Matrix auffassen. Wir können ein lineares Gleichungssystem also auch in der Form $A\vec{x} = \vec{b}$ schreiben.

Man unterscheidet zwischen zwei Arten von linearen Gleichungssystemen. Ist $\vec{b} = \vec{0}$, so nennt man das Gleichungssystem *homogen*, sonst *inhomogen*. Ein inhomogenes Gleichungssystem ist also $A\vec{x} = \vec{b}$, ein homogenes $A\vec{x} = \vec{0}$.

Mit $L(A,\vec{b})$ bezeichnen wir die Lösungsmenge des inhomogenen Gleichungssystem und dementsprechend ist $L(A,\vec{0})$ die Lösungsmenge des homogenen. Es gilt also:

$$L(A,\vec{b}) = \{\vec{x}|A\vec{x} = \vec{b}\} \text{ bzw. } L(A,\vec{0} = \{\vec{x}|A\vec{x} = \vec{0}\})$$

Weil man lineare Gleichungssysteme auch als lineare Abbildung auffassen kann, gilt also $L(A,\vec{b}) = f_A^{-1}(\vec{b})$, d.h. die Lösungsmenge $L(A,\vec{b})$ ist der Urbildbereich von $\vec{b}$. Dieser kann leer sein, denn $\vec{b}$ muß ja nicht zum Bildraum von f_A gehören.

$L(A,\vec{0})$ ist jedoch nicht leer, da ja $L(A,\vec{0}) = f_A^{-1}(\vec{0}) = \ker f_A$ gilt. Da $\vec{0}$ immer ein Unterraum des K^m ist, ist also $\ker f_A$ ein Unterraum von K^n. Denn es gilt ja für lineare Abbildungen immer zumindest $f_A(\vec{0}) = \vec{0}$. Da $\ker f_A$ ein Unterraum ist, hat er also eine Dimension. Welche Dimension hat er?

- **Wie ist der Rang einer Abbildung bzw. Matrix definiert?**

Der Rang einer linearen Abbildung $f : V \longrightarrow W$ ist definiert als $\text{rg}\, f = \dim f(V)$. Der Rang einer Matrix $A \in M(m \times n, K)$ ist entsprechend definiert als $\text{rg}A = \text{rg}\, f_A$.

Man kann den Rang einer Matrix jedoch auch noch anders charakterisieren. Da die Spaltenvektoren der Matrix $A \in M(m \times n, K)$ die Bilder der kanonischen Basisvektoren von K^n sind und $f_A : K^n \longrightarrow K^m$, bilden sie ein Erzeugendensystem für die Bilder $f_A(K^n)$. Aus diesem Erzeugendensystem kann man sich eine Basis auswählen, deren Anzahl an Vektoren also gleich der Dimension des Bildraumes $f_A(K^n)$ ist. Daher ist der Rang einer Matrix die maximale Anzahl linear unabhängiger Vektoren von $A \in M(m \times n, K)$.

Wie groß ist jetzt die Dimension von $L(A,\vec{0})$? Es gilt für eine lineare Abbildung $f : V \longrightarrow W$:

$$\underbrace{\dim V}_{=n} = \dim \underbrace{\ker f}_{L(A,\vec{0})} + \underbrace{\dim f(V)}_{\text{rg}A}$$

Also gilt:

$$\dim L(A,\vec{0}) = n - \text{rg}A$$

Dies gilt wegen $\dim {}^V/_U = \dim V - \dim U$. ${}^V/_U = W$ ist der zu U komplementäre Unterraum, daher $\dim V = \dim {}^V/_U + \dim U$. Mit $f : V \longrightarrow W$ und $U = \ker f$ folgt also $\dim V = \dim {}^V/_{\ker f} + \dim \ker f$. Insgesamt also $\dim V = \dim f(V) + \dim \ker f$.

Jetzt zeigen wir, daß wenn $L(A,\vec{b})$ eine Lösung hat, diese eng verwandt ist mit der Lösung von $L(A,\vec{0})$. Zuerst überlegen wir uns jedoch, wann $L(A,\vec{b})$ *überhaupt* eine Lösung hat. Wie schon gesagt bilden die maximal, linear unabhängigen Spaltenvektoren von A eine Basis für den Bildraum $f_A(K^n)$. Wenn sich diese Spaltenvektoren zu $\vec{b}$ linear kombinieren lassen, liegt $\vec{b}$ also im Bildbereich der Abbildung. Dies bedeutet: Wenn wir den Spaltenvektor $\vec{b}$ an die Spaltenvektoren von A anfügen und dadurch die *erweiterete Matrix* $(A,\vec{b})$ entsteht, darf der Rang dieser Matrix nicht größer werden. Denn sonst wäre $\vec{b}$ linear unabhängig von den Spaltenvektoren von A und ließe sich nicht als Linearkombination darstellen. Es gilt also:

$$L(A,\vec{b}) \neq \emptyset \Leftrightarrow \text{rg}(A,\vec{b}) = \text{rg}A$$

Wie schon gesagt, ist die Lösung $L(A,\vec{b})$ end verwandt mit $L(A,\vec{0})$. Dazu müssen wir einführen, was ein affiner Unterraum ist. Ein *affiner Unterraum* A von V ist das *Translat* $\vec{a}+U = \{\vec{a}+\vec{u} | \vec{u} \in U\}$ eines (linearen) Unterraumes U von V. Dabei heißt U die Richtung von A und es gilt $\dim U = \dim A$ (wird nur verschoben).

Ist $A\vec{x} = \vec{b}$ lösbar, dann ist $L(A,\vec{b})$ ein affiner Unterraum von K^n der Dimension $n - \text{rg}A$, denn es gilt:

$$L(A,\vec{b}) = \vec{v} + L(A,\vec{0}) \text{ mit } \vec{v} \in L(A,\vec{b})$$

$L(A,\vec{b})$ ist also ein Translat von $L(A,\vec{0})$ und hat dieselbe Dimension, wie das homogene Gleichungssystem.
Beweis: Wir behaupten $L(A,\vec{b}) = \vec{v} + L(A,\vec{0})$ mit $\vec{v} \in L(A,\vec{b})$. Wir zeigen:

1. $L(A,\vec{b}) \subseteq \vec{v} + L(A,\vec{0})$
2. $L(A,\vec{b}) \supseteq \vec{v} + L(A,\vec{0})$

Als Vorraussetzung sei also $A\vec{x} = \vec{b}$ lösbar und $\vec{v} \in L(A,\vec{b})$ beliebig gewählt:

1. „$\subseteq$“: Für alle $\vec{x} \in L(A,\vec{b})$ gilt:

   $$A(\vec{x}-\vec{v}) = A\vec{x} - A\vec{v} = \vec{b} - \vec{b} = \vec{0}$$

   Das heißt, daß der Vektor $(\vec{x}-\vec{v})$ eine Lösung des homogenen Gleicgungssystem ist. Jeder Vektor $x \in L(A,\vec{b})$ läßt sich jedoch darstellen als:

   $$\vec{x} = \vec{v} + (\vec{x}-\vec{v}) \in \vec{v} + L(A,\vec{0})$$

2. „$\supseteq$“: Für alle $\vec{x} \in L(A,\vec{0})$ gilt:

   $$A(\vec{v}+\vec{x}) = A\vec{v} + A\vec{x} = \vec{b} + \vec{0}$$

   Also $\vec{v} + \vec{b} \in L(A,\vec{b})$.

- **Wann ist ein lineares Gleichungssystem eindeutig lösbar? Wann universell?**
  Es sei $A \in M(m \times n, K)$ und $\vec{b} \in K^m$. Desweiteren sei $A\vec{x} = \vec{b}$ ein lineares Gleichungssystem mit $\text{rg}\, A = \text{rg}\,(A,\vec{b})$. Es gilt dann:

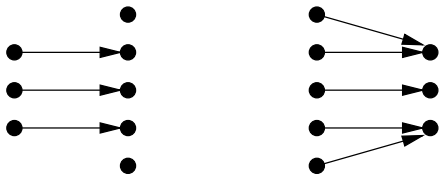
  1. $\text{rg}\, A = n \Leftrightarrow f_A$ ist injektiv $\Leftrightarrow A\vec{x} = \vec{b}$ ist eindeutig lösbar.

     Dies bedeutet, daß zu jedem Vektor $\vec{x} \in L(A,\vec{b})$ genau ein Vektor in K^n existiert, der auf $\vec{x}$ abbildet.

  2. $\text{rg}\, A = m \Leftrightarrow f_A$ ist surjektiv $\Leftrightarrow A\vec{x} = \vec{b}$ ist universell lösbar.

     Dies bedeutet, daß zu jedem Vektor $\vec{x} \in K^m$ mindestens ein Vektor existiert, der auf diesen Vektor abbildet.

Es ist dabei zu beachten, daß (1) nur im Falle $n \leq m$ eintreten kann und (2) nur im Falle $n \geq m$. Dies läßt sich über die grafische Veranschaulichung der Injektivität und Surjektivität gut einprägen. Bei der Injektivität sollte der Bildbereich mindestens so groß sein wie der Urbildbereich, während bei der Surjektivität der Urbildbereich mindestens so groß sein muß wie der Bildbereich:



- **Wann heißt eine Matrix regulär?**

Ein Matrix $A \in M_n(K)$ heißt *regulär*, wenn sie invertierbar ist, d.h. eine Matrix A^{-1} existiert mit

$$AA^{-1} = E_n = A^{-1}A$$

Genau bei den regulären Matrizen kann es vorkommen, daß ein Gleichungssystem eindeutig *und* universell lösbar ist. Es gilt nämlich:

$$A \in M_n(K) \text{ ist regulär } \Leftrightarrow f_A \text{ ist bijektiv } \Leftrightarrow \operatorname{rg} A = n$$

Die regulären Matrizen bilden bezüglich der Matrizenmultiplikation die *General Linear Group*, kurz $\mathrm{Gl}(n,K)$.

- **Was sind elementare Zeilenumformungen? Wie erreicht man sie?**

Unter elementaren Zeilenumformungen verstehen wir:

1. Vertauschung zweier Zeilen.
2. Multiplikation einer Zeile mit $\lambda \neq 0 \in K$.
3. Addition einer mit $\lambda \in K$ multiplizierten Zeile zu einer anderen.

Unter einer Zeilenumformung schlechthin verstehen wir die Hintereinanderschaltung endlich vieler solcher Umformungen. Entsteht eine Matrix $\tilde{A}$ durch eine Zeilenumformung aus A, so gibt eine Matrix $T \in \mathrm{Gl}(n,K)$, die diese Zeilenumformung bewirkt.
Beweis: Es genügt die Regularität der elementaren Zeilenumformungen zu beweisen. Die Transformationsmatrix $T \in \mathrm{Gl}(n,K)$ entsteht, dann durch Multiplikation endlich vieler solcher elementaren Transformationsmatrizen. Wie diese Transformationsmatrizen aussehen und ihre Inversen (die die Regulrität belegen) findet sich im Wegener-Skript.

- **Wie funktioniert der Gauß-Algorithmus?**

- **Wie berechnet man eine inverse Matrix mit dem Gauß-Algorithmus?**

Wendet man den Gauß-Algorithmus auf das System (A,E_n) an, so erhält man:

1. $r < n \Rightarrow A$ ist nicht invertierbar oder
2. $r = n$ und (E_n,A^{-1}).

Beweis: Im ersten Falle kann die normierte Zeilenstufenform nicht hergestellt werden und damit ist der Rang kleiner als n und die Matrix nicht invertierbar.

Im zweiten Falle kann die normierte Zeilenstufenform hergestellt werden. Erreicht wird die mit einer Transformationsmatrix T. Gleichzeitig multipliziert man jedoch diese Transformationsmatrix mit E_n und da E_n die Einheitsmatrix ist, gilt: $TE_n = T$. Da sich aus A durch Multiplikation mit T die Einheitsmatrix ergibt, muß also T, die inverse zu A sein, also: $T = A^{-1}$.

8 Determinanten

- **Wofür braucht man Determinanten?**
Determinanten klassifizieren quadratische Matrizen $A \in M_n(K)$. Determinanten sind also eine Abbildung $\det : M_n(K) \longrightarrow K$. Dabei gilt für regulären Matrizen $\det R \neq 0$, während für singuläre Matrizen $\det S = 0$ gilt. Desweiteren sind Determinanten verträglich mit der Matrizenmultiplikation, d.h. die Determinantenabbildung definiert einen Gruppenhomomorphismus $\mathrm{Gl}(n,K) \longrightarrow K^*$.

- **Wie ist die Determinante definiert?**
Die Determinante einer Matrix $A \in M_n(K)$ ist definiert als:

$$\sum_{\pi \in S_n} \sigma(\pi) \cdot a_{1\pi(1)} \cdot \ldots \cdot a_{n\pi(n)}$$

Es wird also eine Summe gebildet, so daß aus jeder Zeile und jeder Spalte genau *ein* Element ausgewählt wird. Dabei werden alle möglichen Kombinationen (oder besser Permutationen) berücksichtigt. Zusätzlich wird das Signum der entsprechenden Permutation berechnet. Für kleine Matrizen gibt es Merkregeln, wie die Determinante berechnet wird. Für Matrizen $A \in M_n(K), n \geq 4$ gibt es solche Regeln nicht. Wie wir jedoch noch sehen werden, gibt es für solche Matrizen noch andere Verfahren, um die Determinante zu berechnen.

- **Welche Merkregeln gibt es für Matrizen $A \in M_n(K), n \leq 3$?**

n=1 Für Matrizen aus $A \in M_1(K)$ gilt $\det A = a_{11}$.

n=2 Für Matrizen $A \in M_2(K)$ gibt es ebenfalls eine einfache Merkregel:

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \underbrace{a_{11}a_{22}}_{\mathrm{id}} - \underbrace{a_{12}a_{21}}_{(12)}$$

Die Merkregel ist hier: Hauptdiagonale minus Nebendiagonale.

n=3 Für 3×3-Matrizen gibt es die *Merkregel von Sarrus*:

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{cases} a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} \end{cases}$$

Wenn man also die ersten zwei Spalten der Matrix rechts an die Matrix anfügt, so ergibt sich die Determinante aus der Summe den drei von links oben nach rechts unten verlaufenden Diagonalen minus der Summe der von links unten nach rechts oben laufenden Diagonalen.

- **Welche Eigenschaften hat die Determinante?**

1. $\det E_n = 1$
2. $\det A = 0$, wenn A mindestens eine Nullzeile enthält.
3. $\det A = 0$, wenn A zwei gleiche Zeilen enthält.

4. $\det B = \lambda \det A$, wenn B dadurch entsteht, daß man eine Zeile in A mit λ multipliziert.

5. Die Determinante ist linear in den Zeilen, d.h. wenn wir die i-te Zeile als Vektor $\vec{a}_i = (a_{i1}, \ldots, a_{in})$ auffassen und gilt $\vec{a}_r = \lambda \vec{b}_r + \mu \vec{c}_r$ für ein $r \in \{1, \ldots, n\}, \lambda, \mu \in K$, dann gilt:

$$\det \begin{pmatrix} \square \\ \lambda \vec{b}_r + \mu \vec{c}_r \\ \square \end{pmatrix} = \lambda \det \begin{pmatrix} \square \\ \vec{b}_r \\ \square \end{pmatrix} + \mu \det \begin{pmatrix} \square \\ \vec{c}_r \\ \square \end{pmatrix}$$

6. Entsteht B aus A durch Vertauschung zweier Zeilen, so gilt:

$$\det B = -\det A$$

7. Entsteht B aus A durch Addition einer mit λ multiplizierten Zeile so gilt:

$$\det B = \det A$$

Beweise:

1. Der zu id gehörende Summand ist der einzige, der keine Null enthält.

2. Jeder Summand enthält mindestens eine Null aus der entsprechenden Zeile.

3. Mit (6) gilt, daß man die beiden Zeilen vertauschen kann, ohne daß sich die Determinante ändert. Bei Vertauschung zweier Zeilen ändert sich jedoch das Vorzeichen, also kann nur $\det A = 0$ gelten.

4. Jeder Summand der Determinante enthält genau *ein* mit dem Faktor λ multipliziertes Element der Zeile. Also kann man λ vor die Summe ziehen.

5. Wegen (4) muß man nur den Fall $\lambda = \mu = 1$ zeigen. Die Formel gilt, da man die Summen distributiv aufteilen kann.

6. Wir zeigen:

$$\begin{aligned} 0 \quad = \quad & \det \begin{pmatrix} \square \\ b_r + c_r \\ \square \\ b_r + c_r \\ \square \end{pmatrix} = \det \begin{pmatrix} \square \\ b_r + c_r \\ \square \\ b_r \\ \square \end{pmatrix} + \det \begin{pmatrix} \square \\ b_r + c_r \\ \square \\ c_r \\ \square \end{pmatrix} \\ & \det \begin{pmatrix} \square \\ c_r \\ \square \\ b_r \\ \square \end{pmatrix} + \det \begin{pmatrix} \square \\ b_r \\ \square \\ c_r \\ \square \end{pmatrix} \end{aligned}$$

Also gilt insgesamt:

$$\det\begin{pmatrix}\square\\ c_r\\ \square\\ b_r\\ \square\end{pmatrix} = 0 - \det\begin{pmatrix}\square\\ b_r\\ \square\\ c_r\\ \square\end{pmatrix} = -\det\begin{pmatrix}\square\\ b_r\\ \square\\ c_r\\ \square\end{pmatrix}$$

7. Hier gilt:

$$\det\begin{pmatrix}\square\\ a_r\\ \square\\ a_s+\lambda a_r\\ \square\end{pmatrix} = \det\begin{pmatrix}\square\\ a_r\\ \square\\ a_s\\ \square\end{pmatrix} + \lambda\det\begin{pmatrix}\square\\ a_r\\ \square\\ a_r\\ \square\end{pmatrix} = \det\begin{pmatrix}\square\\ a_r\\ \square\\ a_s\\ \square\end{pmatrix} + \lambda\cdot 0$$

- **Wie kann man die Determinante mit Hilfe des Gauss-Verfahrens berechnen?**
Indem man aus der Matrix mit Hilfe der elementaren Zeilenumformungen eine obere bzw. untere Dreiecksmatrix macht. Eine Matrix $A = (a_{ik})$ heißt obere Dreiecksmatrix wenn gilt $a_{ik} = 0$ für $i > k$.
Für obere bzw. untere Dreiecksmatrizen gilt:

$$\det A = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}$$

Beweis: Dies sieht man, wenn man sich eine obere Dreiecksmatrix anschaut. Die zu id gehörende Summe ist die einzige, die keine Null enthält, da man aus jeder Zeile und Spalte jeweils ein Element auswählen muß. Angenommen wir wählen für die erste Zeile nicht a_{11}, dann haben wir nur noch Spalten mit Nullen zur Verfügung. Also müssen wir schonmal a_{11} wählen. Analog können wir für alle anderen Spalten argumentieren.

Wir müssen eine Matrix A also nur durch endlich viele Umformungen zu einer oberen Dreiecksmatrix umformen. Zeilenvertauschungen (Z1) ändern das Vorzeichen, während das hinzu addieren einer mit λ multiplizierten Zeile (Z3) die Determinante nicht ändert. Die zweite Art der Zeilenumformung (Z2), wobei eine Zeile mit λ multipliziert wird, um ein Element auf 1 zu normieren, wird hier nicht benötigt.

Entsteht die obere Dreiecksmatrix B also durch k Schritte (Z1) und beliebig viele Schritte (Z3), so gilt für die Determinante:

$$\det A = (-1)^k \det B = (-1)^k b_{11} \cdot \ldots \cdot b_{nn}$$

Im Falle einer singulären Matrix ist mindestens einer der Zeilen eine Nullzeile und daher gilt:

$$\det A = 0 \Leftrightarrow \text{Die Zeilen von } A \text{ sind linear abhängig} \Leftrightarrow \operatorname{rg} A < n$$

- **Zeige, daß für jede Matrix A gilt:** $\det A = \det A^T$**.**

Sei $A^T = (b_{ik})$. Dann gilt $b_{ik} = a_{ki}$. Die Determinante von A^T ist dann:

$$\det A^T = \sum_{\pi \in S_n} \sigma(\pi) b_{1\pi(1)} \cdot \ldots \cdot b_{n\pi(n)} = \sum_{\pi \in S_n} \sigma(\pi) a_{\pi(1)1} \cdot \ldots \cdot a_{\pi(n)n}$$

In letzterem Ausdruck kann man die $\pi(1), \ldots, \pi(n)$ vertauschen und zeigen, daß das Signum des „Originalausdrucks“ mit dem Signum der Vertauschung übereinstimmt. Also gilt $\det A = \det A^T$.

- **Zeige, daß die Determinantenbildung mit der Matrizenmultiplikation verträglich ist!**

Wir zeigen also, daß für beliebige $A, B \in M_n(K)$ gilt: $\det AB = \det A \cdot \det B$. Es gibt zwei Fälle zu unterscheiden:

1. A ist singulär. Dann ist auch AB singulär. Damit gilt dann jedoch $\operatorname{rg} A < n$, also $\det A = 0$ und somit auch $\det AB = 0$. Insgesamt gilt also:

   $$\det AB = 0 = 0 \cdot \det B = \det A \cdot \det B$$

2. A ist regulär und gehört somit zur *General Linear Group* $\mathrm{Gl}(n, K)$. Also gibt es Transformationsmatrizen, mit denen man A zur Einheitsmatrix umformen kann, d.h. es gilt:

   $$T_r \ldots T_1 A = E_n$$

   Dies ist jedoch gleichbedeutend damit, daß A durch Multiplikation der Inversen jedes $T_k, k \in \{1, \ldots, r\}$ gebildet werden kann. Es gilt also $A = T_1^{-1} \ldots T_r^{-1}$. Wenn man A mit B multipliziert, ist dies also gleichwertig mit der Multiplikation $T_1^{-1} \ldots T_r^{-1} B$. Dabei sind die T_k^{-1} auch wieder Umformungsmatrizen der Arten (Z1)-(Z3). Man muß die Verträglichkeit mit der Multiplikation also nur für die drei Transformationsmatrizen zeigen. Tatsächlich gilt für eine Umformung des Typs

   (Z1) $\det S = -1$ und entsprechend $\det SB = -\det B$

   (Z2) $\det S = \lambda$ und entsprechend $\det SB = \lambda \det B$

   (Z3) $\det S = 1$ und entsprechend $\det SB = \det B$

Hierraus kann man jetzt folgern, daß die Determinantenbildung einen Gruppenhomomorphismus $\mathrm{Gl}(n, K) \longrightarrow K^*$ bildet. Desweiteren gilt für alle regulären Matrizen:

$$\det A \cdot \det A^{-1} = \det AA^{-1} = \det E_n = 1 \Rightarrow \det A^{-1} = \frac{1}{\det A}$$

- **Wie funktioniert die Laplaceentwicklung?**

Im folgenden sei A_{ik} die Matrix, die entsteht, wenn man in A die i-te Zeile und k-te Spalte streicht. Dann gilt:

$$\det A = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det A_{ik}$$

Man nennt dies die Laplaceentwicklung von $\det A$ nach der i-ten Zeile und entsprechend gilt für die Laplaceentwicklung nach der k-ten Spalte:

$$\det A = \sum_{i=1}^{n} (-1)^{i+k} a_{ik} \det A_{ik}$$

- **Wie berechnet man die Inverse einer Matrix mit Laplace?**
  Es sei $A \in \mathrm{Gl}(n,K)$. Dann gilt:

$$A^{-1} = \frac{1}{\det A} \left((-1)^{i+k} \det A_{ik} \right)^T$$

Zum Beispiel für:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

- **Was besagt die Cramersche Regel?**
  Wenn man ein Gleichungssystem mit n Gleichungen und n Unbekannten hat und die Koeffizientenmatrix regulär ist ergibt sich die k-te Komponentes des Lösungsvektors $\vec{x} \in L(A,\vec{b})$ durch:

$$x_k = \frac{\det A_k(\vec{b})}{\det A}$$

Dabei ergibt sich die Matrix $A_k(\vec{b})$ dadurch, daß man in der Matrix A die k-te Spalte durch den Vektor $\vec{b}$ ersetzt.

9 Basistransformation und Eigenwerte

- **Wie ändert sich eine Matrix, wenn man die Basis in einem der Räume ändert?**

Wie wir schon gesehen haben ist jeder n-dimensionale Vektorraum isomorph zum K^n. Dementsprechend gibt es bezüglich einer festen Basis für jeden Vektor einen Koordinatenvektor in K^n. Dieser Koordinatenvektor repräsentiert den Vektor jedoch nur bezüglich einer festen Basis. Ändert man die Basis, so ändert sich auch die Koordinatendarstellung. Angenommen wir haben zwei verschiedene Basen in einem n-dimensionalen Vektorraum V:

$$B_V = \{\vec{v}_1, \ldots, \vec{v}_n\} \text{ bzw. } B_{\tilde{V}} = \{\tilde{v}_1, \ldots, \tilde{v}_n\}$$

Für einen Vektor $v \in V$ gibt es bezüglich dieser beiden Basen verschiedene Darstellungen. Es gilt:

$$v = \sum_{k=1}^{n} x_k \vec{v}_k = \sum_{k=1}^{n} \tilde{x}_k \tilde{v}_k$$

Und dem entsprechend gibt es verschiedene Koordinatenvektoren:

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ und } \tilde{x} = \begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix}$$

Um zu wissen, welche Koordinatendarstellung ein Vektor v bezüglich der neuen Basis $\tilde{B}_V$ hat müssen wir die neuen Basisvektoren bezüglich der alten Basisvektoren darstellen. Es gilt:

$$\tilde{v}_k = \sum_{i=1}^{n} c_{ik} \vec{v}_i$$

Die Elemente c_{ik} kann man wieder in einer Matrix zusammenfassen. Diese Matrix ist dann eine $n \times n$-Matrix und ist auch regulär, da sie die Koordinatendarstellung einer Basis ist. Es gilt also für einen Vektor:

$$\vec{v} = \sum_{k=1}^{n} \tilde{x}_k \tilde{v}_k = \sum_{k=1}^{n} \tilde{x}_k \sum_{i=0}^{n} c_{ik} \vec{v}_i = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} c_{ik} \tilde{x}_k \right) \vec{v}_i$$

Um die Koordinaten bezüglich der alten Basis zu erhalten, muß ich also den neuen Koordinatenvektor mit der Matrix $C \in M_n(K)$ multiplizieren:

$$x = C\tilde{x}$$

Da die Matrix C regulär ist, kann ich diese Operation auch umkehren, denn die durch C definierte Abbildung ist ja bijektiv:

$$\tilde{x} = C^{-1}x$$

Wenn wir also von einem n-dimensionalen Vektorraum V abbilden in einen m-dimensionalen Vektorraum W und wir in W auch die Basis geändert haben ergibt sich also:

$$\tilde{y} = D^{-1}AC\tilde{x}$$

Dabei ist D die Matrix, die die Koordinatenumrechnung in W durchführt. Ändert man die Basen in beiden Räumen permanent, so führt man natürlich nur einmal eine Matrizenmultiplikation durch und erhält dann die neue Abbildungs-Matrix B:

$$B = D^{-1}AC$$

- **Was sind Eigenwerte bzw. Eigenvektoren?**

Sei V ein n-dimensionaler Vektorraum. Ein Vektor $\vec{v} \neq \vec{0} \in V$ heißt Eigenvektor zum Eigenwert $\lambda \in K$ bezüglich einer linearen Abbildung $f : V \longrightarrow V$ bzw. Matrix $A \in M_n(K)$, wenn gilt $f(\vec{v}) = \lambda\vec{v}$ bzw. $A\vec{v} = \lambda\vec{v}$. Die zu einem Eigenwert gehörenden Vektoren bilden einen Unterraum, den sogenannten Eigenraum $Eig(f,\lambda)$ bzw. $Eig(A,\lambda)$.
Beweis: Es ist zu zeigen, daß für $\vec{v},\vec{w} \in Eig(f,\lambda)$ und $r \in K$ auch $\vec{v}-\vec{w}$ und $r\vec{v}$ wieder zu $Eig(f,\lambda)$ gehören:

$$f(\vec{v}-\vec{w}) = f(\vec{v}) - f(\vec{w}) = \lambda\vec{v} - \lambda\vec{w} = \lambda(\vec{v}-\vec{w})$$
$$f(r\vec{v}) = rf(\vec{v}) = r\lambda\vec{v} = \lambda r\vec{v}$$

- **Wie berechnet man die Eigenwerte und Eigenvektoren?**

Wie wir schon gesehen haben muß für $A \in M_n(K)$ gelten: $A\vec{x} = \lambda\vec{x}$. Diese Gleichung kann man jedoch noch umformen. Wir ändern nichts an $\vec{x}$, wenn wir den Vektor mit der Einheitsmatrix E_n multiplizieren:

$$A\vec{x} = \lambda\vec{x}$$
$$A\vec{x} = \lambda E_n\vec{x}$$
$$A\vec{x} - \lambda E_n\vec{x} = \vec{0}$$
$$(A - \lambda E_n)\vec{x} = \vec{0}$$

Dies ist ein homogenes Gleichungssystem. Allerdings interessieren uns nur die nichttrivialen Lösungen dieses Gleichungssystem, da für den Nullvektor $\vec{0}$ immer gilt $A\vec{0} = \vec{0} = \lambda\vec{0}$.

Wann hat ein homogenes Gleichungssystem eine nichttriviale Lösung? Wenn die Dimension des Lösungsraumes $L(A,\vec{0})$ Null ist, gibt es nur die Lösung $\vec{x} = \vec{0}$. Dies ist gleichbedeutend damit, daß $\mathrm{rg}A = n$ ist, denn es gilt ja:

$$\dim L(A,\vec{0}) = n - \mathrm{rg}A$$

Ist $\mathrm{rg}A < n$ besitzt der Lösungsraum $L(A,\vec{0})$ also eine von Null verschiene Dimension und es existieren auch nichttriviale Lösungen. $\mathrm{rg}A < n$ bedeutet jedoch wiederum $\det A = 0$ und damit haben wir ein Kriterium. Es muß also gelten $\det(A - \lambda E_n) = 0$ und somit:

$$\det \begin{pmatrix} a_{11}-t & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-t & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn}-t \end{pmatrix} = 0$$

Man nennt $\chi_A(t) = \det(A - \lambda E_n)$ auch das *charakteristische Polynom* von A. Die Nullstellen dieses Polynoms sind also die Eigenwerte der Abbildung. Setzt man einen

Eigenwert in die Matrix ein und löst das homogene Gleichungssystem, so erhält man den Eigenraum.

- **Wann ist eine Matrix diagonalisierbar?**
  Eine Matrix $A \in M_n(K)$ ist diagonalisierbar, wenn der Raum V eine Basis aus Eigenvektoren von A besitzt. Also ist A diagonalisierbar, wenn

  1. Das charakteristische Polynom zerfällt in n verschiedene Linearfaktoren. Dann gibt es n verschiedene linear unabhängige Eigenvektoren.

  2. Das charakteristische Polynom zerfällt nicht in n verschiedene Linearfaktoren, doch es gilt, daß die algebraische Vielfachheit jeder Nullstelle gleich der Dimension des Eigenraum zum zugehörigen Eigenwert ist.

10 Abzählende Kombinatorik

- **Welche zwei grundlegenden Formel werden in der Kombinatorik (auch etwas abgewandelt) häufig benutzt?**

Seien $M_1, \ldots, M_N$ Teilmengen einer beliebigen Grundmenge M.

1. $|\bigcup_{k=1}^{n} M_k| = \sum_{k=1}^{n} |M_k|$, wenn die $M_i, 1 \leq i \leq n$ disjunkt sind.

2. $|\times_{k=1}^{n} M_k| = \prod_{k=1}^{n} |M_k| = |M_1||M_2| \ldots |M_n|$

- **Zeige $|P(M)| = 2^{|M|}$!**

Wir nehmen im folgenden an, daß $|M| = n$ gilt und somit $|P(M)| = 2^n$. Dies beweisen wir nun mit vollständiger Induktion nach n.

Induktionsanfang: Für $n = 0$ gilt $P(M) = \{\emptyset\}$ und somit $|P(M) = 1 = 2^0$.

Induktionsannahme: Es gilt für $|M| = n - 1$, daß $|P(M)| = 2^{n-1}$ ist.

Induktionsschritt: Wir haben nun eine Menge M mit n Elementen. Aus dieser Menge wählen wir nun ein ausgezeichnetes Element $a \in M$ aus. Betrachten wir nun die Potenzmenge $P(M)$, so fällt auf, daß einige Mengen das Element enthalten, andere nicht. Genau hier setzen wir an. Wir unterteilen die Potenzmenge in zwei Mengen:

$$G_1 = \{A | A \subseteq M \wedge a \notin A\} \text{ sowie } G_2 = \{A | A \subseteq M \wedge a \in A\}$$

G_1 ist nichts anderes als $P(M \backslash \{A\})$ und damit gilt $|G_1| = 2^{n-1}$. Betrachten wir die Menge G_2, so fällt auf, daß wir diese Menge durch die Zuordnung $A \mapsto A \backslash \{a\}$ bijektiv auf G_1 abbilden können. Also gilt auch $|G_2| = 2^{n-1}$. Insgesamt macht dies $2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n$.

- **Zeige, daß die Anzahl der k-Teilmengen einer n-Menge $\binom{n}{k}$ ist!**

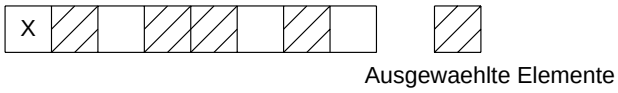
$a(n,k)$ sei die gesuchte Anzahl. Dann gelten folgende Bedingungen:

1. $a(0,k) = 0, k > 0$, denn es gibt keine Möglichkeit $k > 0$ Elemente aus nicht vorhandenen Elementen auszusuchen.

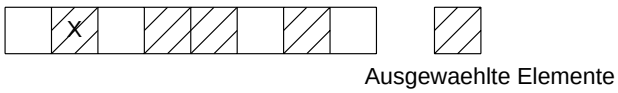
2. $a(n,0)$ für alle n. Denn man hat immer genau eine Möglichkeit 0 Elemente aus n auszuwählen, nämlich die, einfach keines zu wählen.

Für die anderen Fälle $n, k \geq 1$ gehen wir ähnlich vor, wie im vorhergehenden Beweis. Wir nehmen $|M| = n + 1$ an und möchten wissen, wie viele $k+1$-Auswahlen es gibt. Wieder wählen wir ein ausgezeichnetes Element $x \in M$ aus. Wir unterscheiden auch hier zwei Fälle:

1. x kommt in der k-Auswahl nicht vor. Die Anzahl dieser Auswahlen entspricht $a(n, k+1)$, denn man muß aus den restlichen n Elementen immer noch $k+1$ auswählen.



2. x kommt in der k-Auswahl vor. Dann müssen wir aus den restlichen n Elemente noch k Elemente auswählen. Also gibt es $a(n,k)$ solcher Auswahlen.



Insgesamt ergibt dies also die Formel $a(n+1,k+1) = a(n,k+1) + a(n,k)$. Betrachtet man nun nocheinmal die Binomialkoeffizienten, so fallen folgende Entsprechungen auf:

1. $a(0,k) = 0 = \binom{0}{k}, k > 1$.
2. $a(n,0) = 1 = \binom{n}{0}, \forall n$.
3. $a(n+1,k+1) = a(n,k+1) + a(n,k) \leftrightarrow \binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$.

Beide Zahlenfolgen genügen also denselben Anfangsbedingungen und derselben Rekursion. Also sind sie gleich.

- **In welcher Form treten die Binomialkoeffizienten im binomischen Satz auf? Welche einfachen Identitäten gibt es aufgrund dessen?**

Es gilt:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Dementsprechend gibt es für $a = b = 1$ folgende Identität:

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

Desweiteren für $a = -1$ und $b = 1$:

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

- **Was ist das Pascalsche Dreieck?**

Das Pascalsche Dreieck verdeutlicht die Rekursionsformel für Binomialkoeffizienten:

$n \backslash k$	0	1	2	3	4
0	1	0	0	0	0
1	1	1	0	0	0
2	1	2	1	0	0
3	1	3	3	1	0
4	1	4	6	4	1

Es gilt ja $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, was sich auch aus der Tabelle ergibt. Wollen wir z.B. $\binom{4}{2}$ berechnen, so schauen wir in der Tabelle $\binom{3}{2} = 3$ und $\binom{3}{1} = 3$ nach. Also ist $\binom{4}{2} = 3+3 = 6$. Mit dieser Formel kann man also sukzessive größere Binomialkoeffizienten berechnen.

Bei der Berechnung von Binomialkoeffizienten mit Rechnern ist diese Art der Berechnung interessanter, da hier nicht zwischenzeitlich sehr große Werte entstehen, im Gegensatz zur Berechnung mit der Formel $\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!}$.

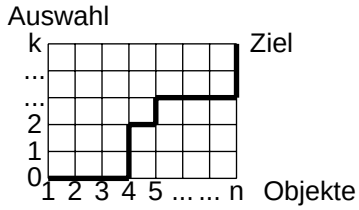
- **Wieviele Möglichkeiten gibt es, aus einer n-Menge eine k-Menge auszuwählen?**
  Hier kann man noch unterscheiden, ob man Wiederholungen zuläßt und ob es auf die Ordnung ankommt oder nicht. Damit ergibt sich folgende Tabelle:

	ungeordnet	geordnet
ohne Wiederholungen	$\binom{n}{k}$	$k! \cdot \binom{n}{k}$
mit Wiederholungen	$\binom{n+k-1}{k}$	n^k

1. $\binom{n}{k}$ entspricht der Anzahl der Möglichkeiten eine k-Menge aus einer n Menge auszuwählen. Desweiteren ist $\binom{n}{k}$ die Anzahl aller möglichen injektiven, monoton wachsenden Abbildungen von einer Menge mit k Elementen in eine Menge mit n Elementen.

2. $k! \cdot \binom{n}{k}$ ist die Anzahl der Möglichkeiten eine k-Menge aus einer n-Menge auszuwählen, wenn es dabei auch noch auf die Reihenfolge der Elemente ankommt. $k! \cdot \binom{n}{k}$ ist auch die Anzahl aller injektiven Abbildungen aus einer k-Menge in eine n-Menge.

3. Um dies zu beweisen, kann man ein Gitterweg-Argument bringen:



   Wir möchten k Elemente aus insgesamt n auswählen. Dabei kommt es auf die Reihenfolge nicht an. Daher können wir uns die n Elemente in einer Reihe aufgestellt vorstellen, wie etwa in der Grafik entlang der x-Achse. Wann immer wir ein Element auswählen, gehen wir einen Schritt nach oben in die k-Richtung. Die Anzahl aller Auswahlen, die wir treffen können, ist die Anzahl der kürzesten Wege von $(1,0)$ bis zum Ziel (n,k). Die kürzesten Wege, das sind die bei denen man sich nur nach rechts oder nach oben bewegt haben die Länge $n+k-1$, da man sich $n-1$ Schritte nach rechts bewegen muß (weil man schon bei 1 startet) und k Schritte nach oben. Wir Bewegungen nach rechts durch eine 0 codieren und Bewegungen nach oben durch eine 1. Dann haben wir eine $n+k-1$ Bit lange 0-1-Sequenz, die genau k Einsen enthalten muß. Wieviele solcher Sequenzen gibt es? Genau $\binom{n+k-1}{k}$.

$\binom{n+k-1}{k}$ ist auch die Anzahl aller monoton wachsenden Abbildungen, was man sich auch sehr gut an der obigen Grafik klar machen kann.

4. Wir haben k-mal jeweils die Auswahl aus allen n Elementen. Also:

$$\underbrace{n \cdot \ldots \cdot n}_{k\text{–mal}} = n^k$$

n^k ist auch die Anzahl aller Abbildungen aus einer k-Menge in eine n-Menge.

- **Was ist der Multinomialkoeffizient und was ist seine kombinatorische Bedeutung?**

Für $n = n_1 + \cdots + n_k$ mit $n_1, \ldots, n_k \in \mathbb{N}_0, k \in \mathbb{N}$ heißt

$$\begin{pmatrix} n \\ n_1, \ldots, n_k \end{pmatrix} = \frac{n!}{n_1! \cdot \ldots \cdot n_k!}$$

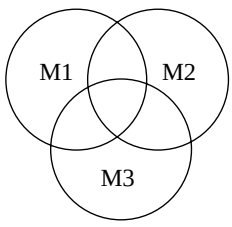
Multinomialkoeffizient. Die kombinatorische Bedeutung des Multinomialkoeffizient liegt in folgender Anzahlbestimmung:

Angenommen wir haben n Objekte von k Sorten. Desweiteren gibt es n_k Objekte der k-ten Sorte. Dann ist der Multinomialkoeffizient die Anzahl der möglichen Anordnungen dieser Objekte. $(n_1, \ldots, n_k)$ nennt man in diesem Zusammenhang die *Spezifikation* der Objekte.

- **Was ist die Formel vom Ein- und Ausschließen?**

Die Formel $|\bigcup_{k=1}^{n} M_k| = \sum_{k=1}^{n} |M_k|$ gilt ja nur, wenn die Mengen $M_1, \ldots, M_k$ disjunkt sind. Was macht man jedoch, wenn man die Vereinigung von nicht disjunkten Mengen bestimmen möchte?

Angenommen wir möchten die Anzahl aller Zahlen $n \leq 100$ bestimmen, die durch $2, 3$ und 5 teilbar sind. Wenn M_k die Menge aller durch k teilbaren Zahlen angibt, so gilt: $|M_k| = \lfloor \frac{100}{k} \rfloor$. Es gilt also $|M_2| = 50, |M_3| = 33$ und $|M_5| = 20$. Wenn wir diese Werte einfach aufaddieren, erhalten wir einen falschen Wert, was man schon an $50 + 33 + 20 = 103 > 100$ sieht. Dies verwundert auch nicht, denn wir haben einige Elemente zu oft gezählt. Es gibt ja Zahlen, die z.B. durch 2 und 3 teilbar sind. Dies sind alle Vielfachen von 6. Wenn wir diese zu oft gezählten Elemente jetzt einfach abziehen, erhalten wir wieder ein falsches Ergebnis, denn es gibt ja auch Zahlen, die durch $2, 3$ und 5 teilbar sind. Dies sind die Vielfachen von 30. Zum Beispiel wurde 30 dreimal gezählt, jedoch dann auch dreimal wieder abgezogen. Also müssen wir alle Vielfachen von 30 noch einmal hinzuaddieren. Am besten sieht man dies in folgendem Diagramm:



Es gilt also:

$$\begin{aligned} |M_2 \cup M_3 \cup M_5| &= |M_2| + |M_3| + |M_5| \\ &\quad - |M_2 \cap M_3| - |M_2 \cap M_5| - |M_3 \cap M_5| \\ &\quad + |M_2 \cap M_3 \cap M_5| \end{aligned}$$

Die allgemeine Formel für das Ein- und Ausschließen lautet:

$$|M_1 \cup \cdots \cup M_n| = \sum_{k=1}^{n} (-1)^{k+1} \cdot \sum_{1 \le i_1 < \cdots < i_k \le n} |M_{i_1} \cap \cdots \cap M_{i_k}|$$

Diese Formel kann man auch noch verallgemeinern. Anstatt die Elemente zu zählen, kann man auch eine Gewichtung einbringen. Diese Gewichtung ist dann eine Abbildung $w : M \longrightarrow K$, wobei K eine additive Gruppe (z.B. ein Körper) ist. Die Formel lautet dann:

$$w(M_1 \cup \cdots \cup M_n) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le n} w(M_1 \cap \cdots \cap M_{i_k})$$

- **Was sind die Stirlingschen Zahlen zweiter Art?**

Die Stirlingschen Zahlen zweiter Art $S(n,k), 1 \le k \le n$ geben an, wieviele Möglichkeiten es gibt, eine Menge mit n Elemente in eine Partition mit genau k (nichtleeren) Klassen zu unterteilen. Eine solche Partition wird auch k-Partition genannt. Da eine Äquivalenzrelation in einer Menge M diese Menge partitioniert und eine Partition eine Äquivalenzrelation induziert, ist $S(n,k)$ auch die Anzahl aller Äquivalenzrelationen mit k Äquivalenzklassen in einer Menge mit n Elementen.
Die Rekursionsformel für die Stirlingschen Zahlen zweiter Art lautet:

$$S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k) \text{ für } n,k \in \mathbb{N}$$

Desweiteren gilt $S(0,0) = 1$ und $S(n,k) = 0$ für $k = 0, n \neq 0$, sowie für $n < k$. Der Beweis hierfür läuft ähnlich, wie die obigen Beweise: Es sei $|M| = n \ge 2$. Wieder wählen wir ein ausgezeichnetes Element $a \in M$ aus und unterscheiden zwei Fälle:

1. $\{a\}$ ist selbst eine Klasse. Dann bilden die übrigen Klassen eine $(k-1)$-Partition von $M \setminus \{a\}$. Also $S(n-1,k-1)$.

2. a ist in einer Klasse A mit $|A| \ge 2$. Wenn man a nun entfernt, also $A = A \setminus \{x\}$, dann hat man immer noch eine k-Partition einer $n-1$-elementigen Menge. Davon gibt es $S(n-1,k)$ Stück. Für jede solche Partition gibt es k Möglichkeiten, das Element a einer Klasse hinzuzufügen, da es ja k Klassen gibt. Dann hat man wieder eine Partition aus der Menge der Partitionen $S(n,k)$. Also gibt es insgesamt $k \cdot S(n-1,k)$ Partitionen in denen $a \in A$ mit $|A| \ge 2$ gilt.

Auch hier kann man wieder eine Tabelle angeben, aus der man sukzessive die $S(n,k)$ berechnen kann:

6	0	1	31	90	65	15	1
5	0	1	15	25	10	1	0
4	0	1	7	6	1	0	0
3	0	1	3	1	0	0	0
2	0	1	1	0	0	0	0
1	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0
$^n/_k$	0	1	2	3	4	5	6

- **Was sind die arithmetischen Partitionszahlen?**

Die arithmetischen Partitionszahlen $P(n,k)$ geben an, wie viele Möglichkeiten es gibt, eine natürliche Zahl $n \in \mathbb{N}$ in k natürliche Summanden zu zerlegen. Dabei kommt es auf die Reihenfolge der Summanden nicht an. Es gilt die Rekursionsformel

$$P(n,k) = P(n-1,k-1) + P(n-k,k)$$

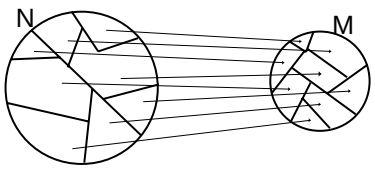
mit $P(n,k) = 0$ für $k > n$ und $P(n,k) = 1$ für $k = n$. Beweis:

1. Die 1 kommt in der Summe vor. Dann müssen die restlichen $k-1$ Summanden zusammen $n-1$ ergeben. Dafür gibt es $P(n-1,k-1)$ Möglichkeiten.

2. Keiner der Summanden ist 1. Dann sind also alle größer als 1 und wir ändern nicht viel an den Möglichkeiten, die es gibt, wenn wir von jedem der Summanden 1 abziehen. Dann ist die Anzahl dieser Möglichkeiten gleich $P(n-k,k)$.

- **Was ist die Anzahl aller surjektiven Abbildungen einer n-Menge in eine k-Menge?**

Die Anzahl aller surjektiven Abbildungen $f : M \longrightarrow N$ einer n-Menge in eine k-Menge beträgt $k! \cdot S(n,k)$. Da die Abbildung surjektiv sein soll, gilt $\forall y \in N : f^{-1}(y) \neq \emptyset$, d.h. auf jedes Element in N bildet mindestens ein Element aus M ab. Da $f^{-1}(N) = M$ ist, bildet also jedes Element aus M auf genau ein $y \in N$ ab. Es können auch mehrere Elemente aus M auf ein Element aus N abbilden. Also induziert eine surjektive Abbildung eine k-Partition der Urbildmenge. Wieviele k-Partitionen einer n-Menge gibt es? Genau $S(n,k)$. Betrachtet man nun eine solche Partition, so gibt es $k!$ verschiedene Möglichkeiten, wie diese auf N abbilden können. Insgesamt gibt es also $k! \cdot S(n,k)$ verschiedene surjektive Abbildungen.



- **Bestimme die Anzahl aller surjektiven Abbildungen mit Hilfe der Formel vom Ein- und Ausschließen!**

Wir möchten die Anzahl aller surjektiven Abbildungen einer n-Menge in eine k-Menge bestimmen. Zuerst einmal gilt:

$$\#\text{surj. Abb.} = \#\text{alle Abb.} - \#\text{nicht surj. Abb.}$$

Die Anzahl aller Abbildungen einer n-Menge in eine k-Menge ist k^n, denn ich habe n mal die Auswahl aus allen k Elementen. Wir definieren nun:

$$M_j := \{f : \{1,\ldots,n\} \longrightarrow \{1,\ldots,k\} \mid j \notin f(\{1,\ldots,n\}), 1 \leq j \leq k\}$$

Die Menge M_j ist also die Menge aller Abbildungen, bei denen kein Element auf j abbildet. Damit gilt also:

$$f \text{ nicht surjektiv } \Leftrightarrow f \in \bigcup_{j=1}^{k} M_j$$

Was ist nun $\left|\bigcup_{j=1}^{k} M_j\right|$? Nach der Formel vom Ein- und Ausschließen ist dies:

$$|M_1 \cup \cdots \cup M_k| = \sum_{s=1}^{k} (-1)^{s+1} \cdot \sum_{1 \leq i_1 \leq \cdots \leq i_s \leq k} |M_{i_1} \cap \cdots \cap M_{i_s}|$$

Nun betrachten wir $M_{i_1} \cap \cdots \cap M_{i_s}$ näher. Es gilt doch:

$$M_{i_1} \cap \cdots \cap M_{i_s} = \{f : \{1,\ldots,n\} \longrightarrow \{1,\ldots,k\} \setminus \{i_1,\ldots,i_s\}\}$$

Dies ist die Anzahl aller Abbildungen einer n-Menge in eine ganz bestimmte $(k-s)$-Menge. Davon gibt es $(k-s)^n$. Desweiteren gibt es $\binom{k}{s}$ Arten aus einer k-Menge eine $(k-s)$-Menge zu machen. Also gibt es insgesamt

$$\binom{k}{s}(k-s)^n$$

solcher Abbildungen. Dies ergibt insgesamt:

$$\#\text{surj. Abb.} = k^n - \sum_{s=1}^{k} (-1)^{s+1} \cdot \binom{k}{s}(k-s)^n$$

- **Was sind die Fibonacci-Zahlen?**

Die Fibonacci-Zahl $F(n)$ mit $n \geq 2$ gibt an, wie viele Null-Eins-Sequenzen der Länge $n-2$ es gibt, in denen keine zwei Einsen nebeneinander stehen. Die Fibonacci-Zahlen sind wie folgt rekursiv definiert:

$$F(0) = 0, F(1) = 1 \text{ und } F(n) = F(n-1) + F(n-2)$$

Der Beweis erfolgt über vollständige Induktion nach n:

Induktionsanfang: Für $n = 2$ gibt es genau eine Möglichkeit eine Sequenz der Länge 0 zu bilden. Man bildet einfach keine. Also $1 = F(2)$.

Induktionsannahme: Es gibt $F(n)$ solcher Sequenzen der Länge $n-2$.

Induktionsschritt: Wir betrachten eine Sequenz der Länge $n-1$ und unterscheiden zwei Fälle:

1. Die Sequenz hat eine 0 am Ende. Dann dürfen davor alle Sequenzen der Länge $n-2$ stehen, da die Bedingung nicht verletzt ist. Davon gibt es nach Induktionsannahme $F(n)$.

$$\overbrace{(\underbrace{a_1,\ldots,a_{n-2}}_{n-2},0)}^{n-1}$$

2. Die Sequenz hat eine 1 am Ende. Dann *muß* vor dieser 1 eine 0 stehen, da sonst die Bedingung verletzt ist. Vor dieser 0 dürfen dann wieder alle Sequenzen der Länge $n-3$ stehen. Davon gibt es $F(n-1)$.

$$\overbrace{(\underbrace{a_1,\ldots,a_{n-3}}_{n-3},0,1)}^{n-1}$$

Also gibt es $F(n-1)+F(n)=F(n+1)$ Sequenzen der Länge $n-1$.

11 Ordnungsstrukturen

• **Welche Relationseigenschaften außer Reflexivität, Symmetrie und Transitivität sind für Ordnungsrelationen noch wichtig?**
Sei $M \neq \emptyset$ und R eine Relation in M. Dann heißt R

irreflexiv: $\forall x \in M : (x,x) \notin R \Leftrightarrow I_M \cap R = \emptyset$

asymmetrisch: $\forall x,y \in M : xRy \Rightarrow (y,x) \notin R \Leftrightarrow R \cap R^{-1} = \emptyset$

antisymmetrisch: $\forall x,y \in M : xRy \wedge x \neq y \Rightarrow (y,x) \notin R \Leftrightarrow R \cap R^{-1} \subseteq I_M$

Es ist wichtig anzumerken, daß irreflexiv nicht „nicht reflexiv“ bedeutet, da es Relationen gibt , die nicht reflexiv jedoch auch nicht irreflexiv sind, da ja bei beiden Definitionen die Eigenschaft für *alle* Elemente aus M gefordert wird.

• **Zeige, daß eine Relation asymmetrisch ist, wenn sie irreflexiv und antisymetrisch ist!**
Wenn eine Relation irreflexiv ist, heißt dies, daß kein Element in Relation zu sich selbst steht, also $\forall x \in M : (x,x) \notin R$. Da die Relation irreflexiv ist, wird bei der Antisymmetrie die Forderung $xRy \wedge x \neq y$ immer wahr. Also folgt aus xRy sofort $(y,x) \notin R$.

• **Was ist eine Halbordnung?**
Eine Relation heißt Halbordnung oder *Poset* (**P**artially **O**rdered **Set**), wenn sie reflexiv, antisymmetrisch und transitiv ist. Zwei Elemente $x,y \in M$ heißen *vergleichbar*, wenn entweder xRy oder yRx gilt. Ein Beispiel für eine Halbordnung ist $(P(M), \subseteq)$. In dieser Halbordnung sind nicht alle Elemente vergleichbar.

• **Was ist eine Ordnung?**
Eine Halbordnung heißt Ordnung bzw. totale Ordnung, wenn je zwei Elemente vergleichbar sind.

• **Was ist eine strikte Halbordnung?**
Eine Relation R heißt strikte Halbordnung, wenn R irreflexiv und transitiv ist. Zum Beispiel ist $(P(M), \subset)$ eine strikte Halbordnung.

• **Wie kann man zwischen Halbordungen und strikten Halbordnungen wechseln?**
Ist R eine strikte Halbordnung auf M, so ist $R \cup I_M$ eine Halbordnung auf M. Genauso gilt, daß wenn R eine Halbordnung auf M ist $R \backslash I_M$ eine strikte Halbordnung ist.

• **Was ist die transitive/reflexive Hülle einer Relation?**
Die transitive bzw, reflexive Hülle ist quasi das Erzeugnis einer Relation. Hat man eine Menge M und ist F_R die Gesamtheit aller transitiven Relationen auf M, die die Relation R enthalten, so ist $R_{tr} = \bigcap_{S \in F_R} S$ die transitive Hülle von R. Entsprechendes gilt für die reflexive Hülle, die man im übrigen durch $R_{re} = R \cup I_R$ erhält.

• **Was ist ein Hassediagramm?**
Wie wir gesehen haben, kann man eine Hüllenbildung für Halbordnungen durchführen. Zeichnet man die Relationen auf, die eine Halbordnung ausmachen, so wird diese sehr schnell unübersichtlich. Man kann jedoch nach der kleinsten Teilrelation S fragen, so daß man durch Hüllenbildung die ursprüngliche Relation R zurückgewinnt.

Dazu definieren wir: Ein Element a heißt *unterer Nachbar* eines Elementes b, welches dann der *obere Nachbar* von a ist, wenn gilt:

$$a \overset{<}{_N} b \Leftrightarrow a < b \wedge \{x | a < x < b\} = \emptyset$$

a ist also kleiner als b und es gibt kein Element welches „zwischen a und b steht". Das *Hassediagramm* einer Halbordnung erhält man, indem man diese Nachbarschaftsbeziehung graphisch darstellt. Jedes Element wird durch einen Punkt dargestellt. Und zwei Punkte a und b werden verbunden, wenn $a \overset{<}{_N} b$ gilt.

Ist N_R die aus dieser Abmagerung entstehende Nachbarschaftsrelation, so gilt $R = (N_R)_{tr}$, wenn R eine strikte Halbordnung ist und $R = (N_R)_{tr,re}$, wenn R eine Halbordnung ist. N_R ist also der Informationskern der Relation R.
Beispiel: Angenommen es gilt: $(a,b),(a,c),(b,c) \in R$, also $(a < b) \wedge (a < c) \wedge (b < c)$. Dann würde es doch ausreichen, unter Berücksichtigung der Transitivität die Information $(a,b),(b,c) \in R$ anzugeben, also $(a < b) \wedge (b < c)$, denn daraus könnte man folgern, daß auch $a < c$ gilt.

Im Hassediagramm sieht man auch sehr schnell, wann zwei Elemente vergleichbar sind. Nämlich wenn es einen Weg von einem Element zum anderen gibt. Allerdings darf man sich dafür nur nach oben bewegen.

- **Was besagt das Dualitätsprinzip der Ordnungstheorie?**
Werden in einem für jede Halbordnung gültigen Satz durchweg $\leq$ und $\geq$, sowie $<$ und $>$ vertauscht, so erhält man wieder einen für jede Halbordnung gültigen Satz. Dies resultiert daraus, daß man das Hassediagramm der Relation R^{-1} dadurch erhält, daß man das Hassediagramm für R auf den Kopf stellt.

- **Was ist ein maximales/größtes bzw. minimales/kleinstes Element?**
Sei $(M,\leq)$ eine halbgeordnete Menge und $a \in M$. Dann heißt a

maximales Element , wenn gilt: $\{x | x \in M \wedge x > a\} = \emptyset$.

größtes Element , wenn gilt: $\{x | x \in M \wedge x \leq a\} = M$.

minimales Element , wenn gilt: $\{x | x \in M \wedge x < a\} = \emptyset$.

kleinstes Element , wenn gilt: $\{x | x \in M \wedge x \geq a\} = M$.

- **Was sind Atome?**
Besitzt $(M,\leq)$ ein kleinstes Element, so heißen die oberen Nachbarn davon *Atome*.

- **Zeige, daß jede Halbordnung höchstens ein größtes bzw. kleinstes Element enthält!**
Angenommen $(M,\leq)$ besitzt zwei größte Elemente a und b. Dann gilt $a \leq b$ und $b \leq a$, woraus $a = b$ folgt. Entsprechendes gilt natürlich für minimale Elemente.

- **Zeige, daß jede endliche Halbordnung maximale/minimale Elemente enthält und wenn es nur eines gibt, dieses das größte bzw. kleinste Element ist!**
Ein einfacher Suchalgorithmus liefert uns ein maximales Element: Wir starten mit einem beliebigen Element $a \in M$. Der Reihe nach überprüfen wir nun, ob wir ein Element b finden mit $a < b$. Finden wir ein solches, so ersetzen wir a durch b und fahren mit den restlichen Elementen fort. Da die Halbordnung endlich ist, bricht dieses

Verfahren irgendwann mit einem maximalen Element ab. Im Hassediagramm sieht der Algorithmus so aus, daß man sich langsam aber sicher nach oben hangelt, bis man nicht mehr weiter kommt.

Ist a das einzige maximale Element, so ist es auch das größte. Denn sonst könnte man $M \backslash \{x | x \in M \wedge x \leq a\}$ betrachten. Ist diese Menge nicht leer, so hätte der Algorithmus ein weiteres maximales Element gefunden und zwar eines aus dieser Menge.

- **Was ist die Adjunktion eines kleinsten/größten Elementes?**

Sei $(M, \leq)$ eine Halbordnung und $a \notin M$. Dann kann man $\leq$ durch

$$a \leq a \wedge a \leq x, \forall x \in M$$

auf $M \cup \{a\}$ fortsetzen und $(M \cup \{a\}, \leq)$ ist eine Halbordnung.

Hat M schon vorher ein minimales Element z besessen, so verliert dies natürlich seine Eigenschaft, da ja nun $a \leq z$ gilt, bzw. da $a \neq z : a < z$. Im Hassediagramm sieht diese Adjunktion so aus, daß man a nach ganz unten zeichnet und mit allen vorher minimalen Elementen verbindet.

- **Was ist eine Teilhalbordnung?**

Ist $(M, \leq)$ eine Halbordnung und $N \subseteq M$, so ist $(N, \leq)$ eine Teilhalbordnung von $(M, \leq)$. Man betrachtet also nur noch $(x, y) \in R_M$ mit $x, y \in N$. Es dürfte klar sein, daß dies dann wieder eine Halbordnung ist.

- **Was ist ein Intervall?**

Sei $(M, \leq)$ eine Halbordnung. Ein Intervall ist eine durch zwei Elemente $a, b \in M$ definierte Teilmenge der Form $[a, b] := \{x | x \in M \wedge a \leq x \leq b\}$. Das heißt in einem Intervall liegen alle Elemente, die mit *a und b* vergleichbar sind.

- **Was ist eine Kette? Wann heißt eine Kette maximal? Was ist die Länge einer Kette?**

Eine Kette K ist eine Teilmenge von M in der jeweils zwei Elemente miteinander vergleichbar sind, d.h. im Hassediagramm kann man alle diese Elemente über einen Weg erreichen, wenn man sich nur nach oben bewegt.

Eine Kette K heißt *maximal*, wenn benachbarte Elemente in der Kette K auch schon in M benachbart sind. Die *Länge* $l(K)$ einer Kette K ist die Anzahl ihrer Elemente minus 1.

- **Was ist die Dimension eines Elementes?**

Besitzt $(M, \leq)$ ein kleinstes Element 0, so ist die Dimension eines Elementes x definiert als $d(x) = \sup\{l(K) | K \text{ ist eine Kette von 0 nach } x\}$. Die Dimension eines Elementes ist also die Länge der längsten Kette vom kleinsten Element 0 zu diesem Element.

- **Wann heißt eine Abbildung ordnungstreu (isoton)?**

Sind $(M, \leq)$ und $(N, \leq)$ halbgeordnete Mengen, so heißt eine Abbildung $f : M \longrightarrow N$ *ordnungstreu* oder *isoton*, wenn gilt:

$$\forall x, y \in M : x \leq y \rightarrow f(x) \leq f(y)$$

Eine Abbildung ist natürlich ein *Ordnungsisomorphismus*, wenn sie bijektiv ist und f als auch f^{-1} ordnungstreu sind.

Beispiele:

1. Die Identität id_M liefert für jede Halbordnung einen Ordnungsisomorphismus in sich.

2. Die Identität $\mathrm{id}_{\mathbb{N}}$ liefert eine ordnungstreue Abbildung $(\mathbb{N},/) \longrightarrow (\mathbb{N},\leq)$. Jede Zahl, die ein Teiler einer anderen Zahl ist, muß also kleiner oder gleich dieser Zahl sein. Jedoch ist dies kein Ordnungsisomorphismus, da nicht jede Zahl, die kleiner als eine andere ist, ein Teiler dieser Zahl sein muß.

• **Zeige, daß man jede Halbordnung ordnungstreu in eine total geodnete Menge einbetten kann!**
Wir suchen also für $(M,\leq)$ mit $|M| = n$ eine ordnungstreue, injektive Abbildung $(M,\leq) \longrightarrow (\{1,\ldots,n\},\leq)$. Wir machen also eigentlich nicht vergleichbare Elemente vergleichbar, ohne jedoch die anderen Nachbarschaftsbeziehungen zu verletzen. Dies leistet der folgende einfache Algorithmus:

Wir suchen in $(M,\leq)$ ein minimales Element a und setzen $f(a) = 1$. Allgemein suchen wir in jedem Schritt ein minimales Element b in der Teilhalbordnung $(M\backslash N)$ und setzen $f(x) = |N| + 1$.

• **Was ist ein Verband?**
Eine Halbordnung ist eine relativ schwache Struktur. Betrachtet man zum Beispiel $(P(M),\subseteq)$, so fällt auf, daß diese Struktur zusätzliche Merkmale hat. So gibt es zum Beispiel zu je zwei Elementen stets ein kleinstes gemeinsames Oberelement (die Vereinigung) und ein größtes gemeinsames Unterelement (den Schnitt). Dementsprechend definieren wir:

Eine Halbordnung $(M,\leq)$ heißt *Verband*, wenn es zu je zwei Elementen a und b ein kleinstes gemeinsames Oberelement gibt, welches *Supremum* genannt wird und mit $a \sqcup b$ bezeichnet wird, sowie ein größtes gemeinsames Unterelement, das *Infimum* $a \sqcap b$.

$a \sqcup b$ ist also das kleinste Element der Teilhalbordnung $\{x | x \in M \wedge x \geq a \wedge x \geq b\}$. Entsprechend ist $a \sqcap b$ das größte Element der Teilhalbordnung $\{x | x \in M \wedge x \leq a \wedge x \leq b\}$.
Beispiele:

1. Jede total geordnete Menge ist ein Verband, wenn man $a \sqcup b$ als das größere der beiden Elemente und $a \sqcap b$ als das kleinere der beiden Elemente setzt. So ist $(\mathbb{R},\leq)$ zum Beispiel ein Verband mit $a \sqcup b = \max\{a,b\}$ und $a \sqcap b = \min\{a,b\}$.

2. Wie schon oben gesehen, ist $(P(M),\subseteq)$ ein Verband mit $A \sqcup B = A \cup B$, sowie $A \sqcap B = A \cap B$. Beliebige Teilmengen der Potenzmenge bilden jedoch im allgemeinen keine Verbände.

3. $(\mathbb{N},/)$ ist ein Verband mit $a \sqcup b = \mathrm{kgV}(a,b)$ und $a \sqcap b = \mathrm{ggT}(a,b)$. Auch hier gilt, daß $(\{1,\ldots,n\},/)$ kein Verband ist, da zwar $a \sqcap b$ existiert, nicht jedoch immer $a \sqcup b$.

• **Welche Rechengesetze gelten in einem Verband? Woran erinnern sie?**
Es gelten die folgenden Rechenregeln für Verbände:

1. Es bestehen die Äquivalenzen

$$x \leq y \Leftrightarrow x = x \sqcap y \Leftrightarrow y = x \sqcup y.$$

2. Für Infimum $\sqcap$ und Supremum $\sqcup$ bestehen die folgenden Rechenregeln:

Idempotenzgesetze: $(L1)$ $\begin{cases} x \sqcap x = x \\ x \sqcup x = x \end{cases}$

Kommutativgesetze: $(L2)$ $\begin{cases} x \sqcap y = y \sqcap x \\ x \sqcup y = y \sqcup x \end{cases}$

Assoziativgesetze: $(L3)$ $\begin{cases} x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z \\ x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z \end{cases}$

Absorptionsgesetze: $(L4)$ $\begin{cases} x \sqcap (x \sqcup y) = x \\ x \sqcup (x \sqcap y) = x \end{cases}$

3. Ist $(M, \leq)$ ein *endlicher* Verband, so gibt es ein kleinstes Element 0 und ein größtes Element 1.

Dabei haben wir die Rechenregeln aus 2 schon bei den *booleschen Algebren* gesehen.

- **Was ist die Monotonieregel für Verbände?**

Beim Rechnen in $\mathbb{R}$ gilt die Regel $a < b \Rightarrow a + c < b + c$. Ähnliche Regeln gelten auch für Verbände bezüglich $\sqcap$ und $\sqcup$:

Sei $(V, \leq)$ ein Verband. Dann gilt für alle $a, b, c, d \in V$:

1. $a \leq b \Rightarrow (a \sqcap c \leq b \sqcap c) \wedge (a \sqcup c \leq b \sqcup c)$.
2. $a \leq b \wedge c \leq d \Rightarrow (a \sqcap c \leq b \sqcap d) \wedge (a \sqcup c \leq b \sqcup d)$.

- **Wann heißt ein Verband distributiv?**

Ein Verband $(V, \leq)$ heißt *distributiv*, wenn gilt:

$$\forall x, y, z \in V : \begin{cases} x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z) \\ x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z) \end{cases}$$

- **Wann heißt ein Verband komplementär?**

Ein Verband $(V, \leq)$ heißt *komplementär*, wenn es zu jedem $x \in V$ *mindestens* ein $y \in V$ gibt, so daß gilt:

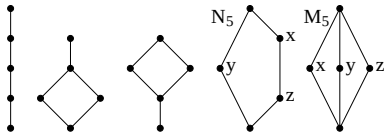
$$x \sqcap y = 0 \wedge x \sqcup y = 1$$

- **Wann heißt ein Verband modular?**

Ein Verband $(V, \leq)$ heißt *modular*, wenn gilt:

$$\forall x, y, z \in V \wedge x \leq z : x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap z$$

- **Gebe alle Verbände mit fünf Elementen an! Welche Eigenschaften haben sie?**



1. distributiv und modular, nicht komplementär (wäre ja sonst auch boolesch)
2. distributiv und modular, nicht komplementär
3. distributiv und modular, nicht komplementär
4. N_5 : nicht distributiv, nicht modular (da nicht immer $x \leq z$), komplementär
   Die fehlende Distributivität wird bezeugt durch:
   $$x = x \sqcap (y \sqcup z) \neq (x \sqcap y) \sqcup (x \sqcap z) = z$$
5. M_5 : nicht distributiv, modular, komplementär
   Gegenbeispiel für Distributivität:
   $$x = x \sqcap (y \sqcup z) \neq (x \sqcap y) \sqcup (x \sqcap z) = 0$$

- **Was ist ein boolescher Verband?**
Ein Verband $(V, \leq)$ heißt *boolesch*, wenn V zugleich distibutiv *und* komplementär ist.

- **Was besagt der Satz von Stone?**
Der *Satz von Stone* besagt, daß jeder boolesche Verband $(V, \leq)$ isomorph ist zu einem Potenzmengenverband $(P(A), \subseteq)$, wobei A die Menge der Atome von V ist. Es gilt: $|A| = n, n \in \mathbb{N}_0 \Rightarrow P(A) = 2^n$. Also gilt $|V| = 2^n, n \in \mathbb{N}_0$, wobei n die Anzahl der Atome ist.

12 Graphentheorie

- **Was ist ein Graph/gerichteter Graph?**

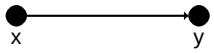
Ungerichteter Graph: Ein ungerichteter Graph ist ein Paar $G = (V,E)$ bestehend aus einer Menge V von Knoten und einer Menge $E \subseteq V \times V$ von ungeordneten Paaren (verschiedener oder gleicher) Elemente aus V, genannt Kanten. Schreibweise:

$$u = \{x,y\} \text{ für } u \in E$$

Gerichteter Graph: Auch *Digraph* (**Di**rected **Graph**). Ein Digraph ist ein Paar $G = (V,E)$ bestehend aus einer nicht-leeren Menge V von Knoten und einer Menge $E \subseteq V \times V$ gerichteter Kanten. Schreibweise:

$$u = (x,y) \text{ für } u \in E$$

Es handelt sich also um eine nicht leere Menge V mit einer Relation in V. Darstellung:

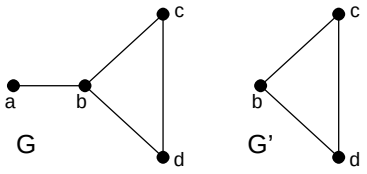


für $u = (x,y) \in E, x \neq y$

- **Was ist ein Abschnittsgraph?**

Ein Graph $G' = (V',E')$ heißt *Untergraph* von $G = (V,E)$, falls $V' \subseteq V$ und $E' \subseteq E$ gilt.

Ein Untergraph heißt *Abschnittsgraph* von $G = (V,E)$, wenn E' genau aus allen Kanten von G besteht, die beide Kanten in V' haben. Dieser ist durch V' in G eindeutig bestimmt und heißt der von V' aufgespannte Abschnittsgraph.
Beispiel: Zu G ist G' der von $\{b,c,d\}$ aufgespannte Abschnittsgraph.



- **Wie lautet der Isomorphiesatz für Graphen?**

Zwei Graphen $G = (V,E)$ und $G' = (V',E')$ heißen isomorph, wenn es eine bijektive Abbildung $f : V \longrightarrow V'$ gibt, so daß gilt:

$$\forall x,y \in V : \{x,y\} \in E \Leftrightarrow \{f(x), f(y)\} \in E'$$

f heißt dann *Graphisomorphismus*.

- **Erläutere die Begriffe Kantenfolge, Linie, Weg und Kreis für Graphen!**

Sei $G = (V,E)$ ein Graph. Eine (ungerichtete) *Kantenfolge* mit Startknoten x_0 und Zielknoten x_n ist eine Sequenz von Kanten der Form:

$$u_1 = \{x_0,x_1\}, u_2 = \{x_1,x_2\}, u_3 = \{x_2,x_3\}, \ldots, u_n = \{x_{n-1},x_n\}$$

Eine *Linie* ist eine Kantenfolge aus lauter *verschiedenen* Kanten.

Ein *Weg* ist eine Linie $u_1 = \{x_0, x_1\}, u_2 = \{x_1, x_2\}, \ldots, u_n = \{x_{n-1}, x_n\}$ mit $x_i \neq x_j$ für $i \neq j (0 \leq i, j \leq n)$, abgesehen von $x_0 = x_n$, was möglicherweise auftreten kann.

Im Falle von $x_0 = x_n$ heißt die Kantenfolge/die Linie/der Weg *geschlossen*. Ein *Kreis* ist ein geschlossener Weg.

- **Was ist eine Zusammenhangskomponente? Wann heißt ein Graph zusammenhängend?**

Sei $G = (V, E)$ ein Graph. Die von den Äquivalenzklassen von V bezüglich Z aufgespannten Abschnittsgraphen heißen *Zusammenhangskomponenten* von G. Ist ganz G eine Zusammenhangskomponente, so heißt G *zusammenhängend*. (wobei Äquivalenzrelation $Z : aZb :\Leftrightarrow$ es existiert ein Weg von a nach b)
Es gilt: Ist $G = (V, E)$ zusammenhängend, so ist $|E| \geq |V| - 1$
Beweis: Induktion nach $n = |V|$:

- **Wann heißt ein Graph planar?**

Ein Graph $G = (V, E)$ heißt planar (plättbar), wenn er isomorph zu einem Graphen in der Ebene $\mathbb{R}^2$ ist, bei dem sich die Kanten nur in den Ecken schneiden (kreuzungsfreie Kanten).

- **Wie lautet die Eulersche Formel? Beweise diese!**

Sei G ein zusammenhängender, planarer Graph im $\mathbb{R}^2$ und seien n, m und f entsprechend die Anzahl der Ecken, Kanten und Flächen von G. Dann gilt:

$$n - m + f = 2 \text{ bzw. } n + f = m + 2$$

Beweis: Induktion nach m:

Induktionsanfang: $m = 0 \Rightarrow n = 1$ (G zusammenhängend) und $f = 1$ (unendliche Fläche), also gilt:

$$n + f = 1 + 1 = 2 = 0 + 2 = m + 2$$

Induktionsannahme: Sei $m \geq 1$ und $n + f = m + 2$ gelte für alle G mit $m - 1$ Kanten.

Induktionsschluß: Hier müssen wir zwei Fälle unterscheiden:

1. Ist G ein Baum, so enthält er keine geschlossenen Flächen und es gilt $f = 1$. Desweiteren gilt in Bäumen $|E| = |V| - 1$, also $m = n - 1$. Insgesamt also:

$$n - m + f = n - (n-1) + 1 = n - n + 1 + 1 = 2$$

2. G ist kein Baum. Sei e die Kante eines geschlossenen Weges. Dann ist $G' = (V, E \setminus \{e\})$ ein zusammenhängender Graph mit n Ecken, $m - 1$ Kanten und $f - 1$ Flächen. Laut Induktionsvorraussetzung gilt die Formel für $m - 1$, also:

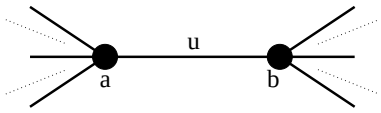
$$n - (m-1) + (f-1) = 2 \Rightarrow n - m + f = 2$$

- **Zeige, daß in Bäumen $|E| = |V| - 1$ gilt!**

Auch dies wird mit Induktion nach $n = |V|$ bewiesen:

1. $n = 1$. Der Graph besteht aus einem Knoten und hat dementsprechend keine Kanten. Also gilt $0 = 1 - 1$.

2. $n \geq 2$ und $u = \{a, b\}$ Kante:



$G' = (V, E \setminus \{u\})$ hat zwei Zusammenhangskomponenten $G'_1 = (V_1, E_1)$ und $G'_2 = (V_2, E_2)$, wobei $a \in V_1$ und $b \in V_2$. G'_1, G'_2 sind Bäume. Es folgt: $|E_i| = |V_i| - 1$ für $i = 1, 2$. Also:

$$|E| = |E_1| + |E_2| + \underbrace{1}_{u} = |V_1| + |V_2| - 2 + 1 = |V| - 1$$

- **Sind $K_5, K_{3,3}$ planar? Beweise deine Antwort!**

Um diese Frage zu beantworten, untersuchen wir erst, in welchem Verhältnis die Knoten zu den Kanten stehen bei planaren Graphen. Sei G zusammenhängend und planar mit n Ecken und $m \geq 3$ Kanten, dann gelten folgende Verhältnisse:

1. $m \leq 3n - 6$

2. Wenn jeder Kreis in G mindestens vier Kanten enthält gilt sogar:

$$m \leq 2n - 4$$

Beweis:

1. Sei ein ebenes Diagramm eines planaren Graphen mit n Ecken, $m \geq 3$ Kanten $e_1, e_2, \ldots, e_m$ und f Flächen $F_1, \ldots, F_f$ gegeben. Wir stellen nun eine $m \times f$-Matrix $A = (a_{ij})$ auf, für die gilt:

$$a_{ij} = \begin{cases} 1 \text{ falls die Kante } e_i \text{ die Fläche } F_j \text{ begrenzt} \\ 0 \text{ sonst} \end{cases}$$

Wieviele Einsen stehen in dieser Matrix? Jede Kante begrenzt höchstens zwei Flächen, kann jedoch auch nur ein Fläche begrenzen. Also stehen in jeder Zeile höchstens zwei Einsen. Also ist die Gesamtzahl der Einsen *höchstens* $2m$. Jede Fläche braucht jedoch mindestens drei Kanten. Also stehen *mindestens* $3f$ Einsen in der Matrix. Insgesamt ergibt dies:

$$3f \leq 2m$$

Mit Hilfe der Polyederformel können wir die Anzahl der Flächen auch durch die Anzahl der Ecken und Kanten angeben. Es gilt ja:

$$n - m + f = 2 \Rightarrow f = m - n + 2$$

Die setzen wir in die oben gewonnene Ungleichung ein:

$$\begin{aligned} & 3(m - n + 2) \leq 2m \\ \Leftrightarrow \quad & 3m - 3n + 6 \leq 2m \\ \Leftrightarrow \quad & m \leq 3n - 6 \end{aligned}$$

2. Hier gilt, daß jede Fläche von mindestens vier Kanten begrenzt ist, also: $4f \leq 2m$. Einsetzen:

$$\begin{aligned} & 4(m-n+2) \leq 2m \\ \Leftrightarrow \quad & 4m-4n+8 \leq 2m \\ \Leftrightarrow \quad & 2m \leq 4n-8 \\ \Leftrightarrow \quad & m \leq 2n-4 \end{aligned}$$

Mit diesen beiden Ungleichungen können wir jetzt auch zeigen, daß K_5 und $K_{3,3}$ nicht planar sind. Für K_5 gilt $m = 10$ und $n = 5$. Dies setzen wir ein:

$$m = 10 \leq 3n-6 = 15-6 = 9 \text{ Widerspruch!}$$

Für $K_{3,3}$ gilt $m = 9$ und $n = 6$. Mit 2 folgt:

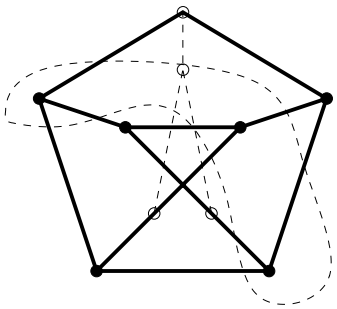
$$m = 9 \leq 2n-4 = 12-4 = 8 \text{ Widerspruch!}$$

- **Wie lautet der Satz von Kuratowski?**

Ein Graph ist planar, genau dann wenn er keinen zu K_5 oder $K_{3,3}$ homöomorphen Untergraphen enthält.

Zwei Graphen heißen homöomorph, wenn sie beide aus ein und demselben Graph herleitbar sind, durch das Einfügen neuer Ecken vom Grad 2.

So kann man zum Beispiel mit dem Satz von Kuratowski zeigen, daß der Petersen-Graph nicht planar ist, da er einen zu $K_{3,3}$ homöomorphen Untergraphen enthält:



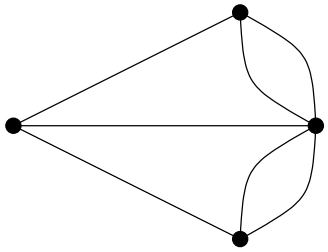
Wenn man die nicht ausgefüllten Ecken herausnimmt, entsteht der $K_{3,3}$ dessen eine Knotenpartition durch die gestrichelte Linie verdeutlicht wird.

- **Was ist eine Eulersche Linie bzw. ein Eulerscher Zyklus?**

Eine Eulersche Linie (Zyklus) in einem Graphen $G = (V,E)$ ist eine Linie (Zyklus), die jede Kante des Graphen *genau einmal* enthält.

- **Wie lautet das Königsberger Brückenproblem und warum ist es nicht lösbar?**

Das Königsberger Brückenproblem gilt als die Wurzel der Graphenthoerie. Das Problem besteht darin, herauszufinden, ob es einen Rundgang durch Königsberg gibt, so daß man jede der sieben Brücken über die Pregel überquert. Graphisch läßt sich dies wie folgt veranschaulichen:



Dabei werden die Brücken durch die Kanten symbolisiert und die Ufer durch die Knoten. Es stellt sich nun also die Frage, ob es in diesem Graphen einen eulerschen Zyklus gibt. Schon Euler konnte zeigen, daß das Königsberger Brückenproblem keine Lösung besitzt. Es gilt nämlich:

Ein Graph G besitzt genau dann einen eulerschen Zyklus, wenn G zusammenhängend ist und keine Ecken ungeraden Grades besitzt.

Beweis: Zu zeigen sind natürlich beide Richtungen:

„$\Rightarrow$“: G besitzt nach Vorraussetzung einen eulerschen Zyklus. Wir zeigen nun, daß daraus folgt, daß G nur Ecken geraden Grades besitzt. Der Zyklus sei:

$$(v_0, v_1), (v_1, v_2), \ldots, (v_n, v_0)$$

Da der Graph einen eulerschen Zyklus enthält, ist er zusammenhängend. Desweiteren besitzt jede Ecke mindestens eine eingehende und eine ausgehende Kante und verursacht damit, jedesmal wenn sie auftaucht in Zyklus die Kosten 2.

„$\Leftarrow$“: Diese Richtung kann bewiesen werden, indem man einen Algorithmus angibt, der einen Eulerschen Zyklus erzeugt. Wir verwenden hier *Tuckers Algorithmus*. Nach Vorraussetzung ist der Graph G zusammenhängend und jeder Knoten hat geraden Grad. Der Algorithmus arbeitet in zwei Phasen:

Zerlegungsphase: In der Zerlegungsphase suchen wir Knoten $x \in V$ mit $\rho(x) \geq 2k, k \geq 2, k \in \mathbb{N}$. Haben wir einen solchen Knoten gefunden, so zerlegen wir ihn in k Knoten mit Grad 2. Über eine Äquivalenzrelation merken wir uns jedoch, daß diese Knoten zu einem Knoten gehören. Dabei zerfällt der Graph in lauter Zyklen und jeder Knoten hat Grad 2. Nun gehen wir über zur Aufbauphase:

Aufbauphase: In der Aufbauphase nehmen wir uns einen beliebigen Zyklus und schauen, ob er alle Kanten des Graphen enthält. Ist dies nicht der Fall, dann gibt es auf dem Zyklus einen Knoten, der zusammen mit einem anderen Knoten in einer Äquivalenzklasse liegt. Diesen fügen wir nun an den betreffenden Knoten an und das Spiel geht von vorne los. Der Algorithmus terminiert auf jeden Fall, da die Knotenmenge eines Graphen und damit auch die Kantenmenge endlich ist.

- **Was ist ein hamiltonscher Weg/Kreis? Wann heißt ein Graph hamiltonsch?**

Ein hamiltonscher Weg bzw. Kreis ist ein Weg bzw. Kreis, der alle Knoten enthält. Ein Graph heißt hamiltonsch, wenn er einen hamiltonschen Kreis enthält.

Für dieses Problem ist kein effizienter Algorithmus bekannt, was eigentlich verwundert, da dieses Problem dem eulerschen Zyklus sehr ähnlich sieht. Jedoch gibt es den Satz von Ore, der besagt: Ein Graph ist genau dann hamiltonsch, wenn für alle Paare nicht benachbarter Knoten $x, y \in V$ gilt:

$$\rho(x) + \rho(y) \geq n = |V| > 2$$