# Diskrete Mathematik für Informatik 1 | DMI 1

Zusammenfassung

## Aussagenlogik

Eine Aussage ist ein feststellender Satz, dem eindeutig einer der beiden Wahrheitswerte wahr oder falsch zugeordnet werden kann.»

Auch wenn der Wahrheitswert unbekannt ist, können Behauptungen Aussagen sein, wenn sie im Prinzip beweis- oder widerlegbar sind. Auch Behauptungen über die Zukunft können Aussagen sein. Für Aussagen werden oft Symbole (z.B. A, B, C, …) verwendet.  
Wenn die Behauptung in eine «Wenn <Behauptung>, dann …» Form gebracht werden kann, handelt es sich um eine Aussage.

### **Junktoren**

|  |  |
| --- | --- |
| **¬** Negation nicht **∧** Konjunktion und **∨** Disjunktion oder | **⇒** Implikation wenn … dann …**¬** **⇔** Äquivalenz … genau dann, wenn … |

* + 1. **Negation / Verneinung / ¬**

Die Negation einer Aussage ist genau dann wahr, wenn die Aussage falsch ist.

* Heute regnet es ⇒ Heute regnet es nicht
* x > 1000 ⇒ x ≤ 1000
* A: x < 7 ⇒ ¬A: ¬(x<7) oder ¬A: x≥7

|  |  |  |
| --- | --- | --- |
| A | ¬A | ¬(¬A) |
| w | f | w |
| f | w | f |

* + 1. Konjunktion / und / ∧

Die Konjunktion zweier Aussagen ist genau dann wahr, wenn beide Aussagen wahr sind.

* A: Heute regnet es. B: Die Lufttemperatur ist unter null. ⇒ A ∧ B: Heute regnet es und die Lufttemperatur ist unter null.
* A: x < 3, B: y > 5 ⇒ A ∧ B: x < 3 und y > 5

|  |  |  |
| --- | --- | --- |
| A | B | A ∧ B |
| w | w | w |
| w | f | f |
| f | w | f |
| f | f | f |

Achtung: Mit der Konjunktion wird kein kausaler oder zeitlicher Zusammenhang berücksichtigt.   
**In der Aussagenlogik gilt A ∧ B ⇔ B ∧ A**

* + 1. **Disjunktion / (einschliessliches) ODER / ∨**

Die Disjunktion zweier Aussagen ist genau dann wahr, wenn mindestens eine der beiden Aussagen wahr ist.

* A: Heute regnet es. B: Die Lufttemperatur ist unter null. 🡪 A ∨ B: Heute regnet oder und die Lufttemperatur ist unter null.
* A: x < 3, B: y > 5 🡪 A ∨ B: x < 3 oder y > 5 oder beides

|  |  |  |
| --- | --- | --- |
| A | B | A ∨ B |
| w | w | w |
| w | f | w |
| f | w | w |
| f | f | f |

Eine Kontradiktion ist eine logische Aussage, die nie wahr ist. Alle Zeilen der Wahrheitstafel ergeben falsch. Eine Tautologie ist eine logische Aussage, die immer wahr ist. Alle Zeilen der Wahrheitstafel ergeben wahr.

* + 1. **Implikation / wenn x, dann y /** ⇒

Wenn die Aussage A wahr ist, dann gilt auch die Aussage B. Aus A folgt B.   
A ist hinreichend für B. B ist notwendig für A. A ist Voraussetzung / Annahme, B ist die Folgerung.

|  |  |  |
| --- | --- | --- |
| A | B | A ⇒ B |
| w | w | w |
| w | f | f |
| f | w | w |
| f | f | w |

Abtrennungsregel: Wenn A wahr ist, und A ⇒ B wahr ist, dann ist auch B wahr. (A ∧ (A ⇒ B)) ⇒ B

* + 1. **Äquivalenz / y genau dann, wenn x /** ⇔

Aussage A gilt genau dann, wenn B gilt. Es gilt A ⇒ B und B ⇒ A

|  |  |  |
| --- | --- | --- |
| A | B | A ⇔ B |
| w | w | w |
| w | f | f |
| f | w | f |
| f | f | w |

Hinweis: ein senkrechter Strich *x | y* bedeutet *x ist ein Teiler von y*

* + 1. Bindungsstärke

Die Bindungsstärke legt fest, welche Junktoren in aussagenlogischen Formeln zuerst ausgeführt werden. Das Nicht hat die grösste Bindungsstärke, gefolgt von den beiden Junktoren Und und Oder. Die kleinste Bindungsstärke besitzen die Implikationen und die Äquivalenz.

### Aussagenlogische Formeln

A und B seien Aussagen. Die verknüpften Aussagen ¬A, A ∧ B, A ∨ B, A ⇒ B und A ⇔ B sind aussagenlogische Formeln. Die verknüpften Aussagen sind auch aussagenlogische Formeln, wenn A oder B bereits selbst aussagenlogische Formeln sind. Eine aussagenlogische Formel ist selbst wieder eine Aussage. Die logische Konstante W bedeutet «wahr» und F bedeutet «falsch».

Satz 1: A, B, und C seien aussagenlogische Formeln. Dann gilt

1. Kommutativität: A ∧ B ⇔ B ∧ A, A ∨ B ⇔ B ∨ A  
Wenn A und B zutreffen, gilt auch B und A. Wenn A oder B zutreffen, gilt auch B oder A (umgekehrt)

2. Assoziativität: A ∧ (B ∧ C) ⇔ (A ∧ B) ∧ C, A ∨ (B ∨ C) ⇔ (A ∨ B) ∨ C

Wenn A und (B und C) zutreffen, können die Klammern beliebig verschoben oder weggelassen werden (gleich bei oder)

3. Distributivität: A ∧ (B ∨ C) ⇔ (A ∧ B) ∨ (A ∧ C), A ∨ (B ∧ C) ⇔ (A ∨ B) ∧ (A ∨ C)  
A und (B oder C) ist das gleiche wie (A und B) oder (A und C), A oder (B und C) ist das gleiche wie (A oder B) und (A oder C)

4. Absorption: A ∨ (A ∧ B) ⇔ A, A ∧ (A ∨ B) ⇔ A  
A oder (A und B) ist das Gleiche wie A. A und (A oder B) ist das Gleiche wie A

5. Idempotenz: A V A = A, A ∧ A = A  
A und A = A, A oder A = A

6. Doppelte Negation: ¬(¬A) ⇔ ¬¬A ⇔ A

Nicht nicht A ist gleich A

7. Konstanten: W = wahr, F = falsch. A ∨ W ⇔ W, A ∧ W ⇔ A, A ∨ ¬A ⇔ W  
A oder wahr = wahr, A und wahr = A, A oder nicht A = wahr

Implikation ersetzen: A ⇒ B kann man durch ¬A ∨ B ersetzen

Äquivalenz ersetzen: A ⇔ B kann man durch (A ∧ B) ∨ (¬A ∧ ¬B) ersetzen

Satz 2: A, B und C seien aussagenlogische Formeln. Dann bedeutet A ⇒ B ⇒ C, dass beide Implikationen, sowohl A ⇒ B als auch B ⇒ C gelten. Formal kann man also schreiben: (A ⇒ B ⇒ C) ⇔ (A ⇒ B) ∧ (B ⇒ C)

Satz 3 (de Morgan): Für beliebige Aussagen A und B gilt:

a) ¬(A ∧ B) ⇔ ¬A ∨ ¬B Nicht (A und B) ist das gleiche wie nicht A oder nicht B

b) ¬(A ∨ B) ⇔ ¬ A ∧ ¬B Nicht (A oder B) ist das gleiche wie nicht A und nicht B

### Normalformen

Dienen der Übersichtlichkeit – standardisierte Form

* + 1. Negationsnormalform

Eine aussagenlogische Formel steht in Negationsnormalform, wenn die Negation (¬) nur direkt vor Aussagen oder vor Konstanten steht.  
Beispiel: ¬(A ∨ B) ist keine Negationsnormalform, ¬A ∧ ¬B hingegen schon

* + 1. Verallgemeinerte Konjunktion

Eine verallgemeinerte Konjunktion ist…

* Eine einzelne Aussage oder seine Negation (also A oder ¬A) oder
* Einer der logischen Konstante T=wahr oder F=falsch oder
* Eine Konjunktion A ∧ B, falls A und B selbst verallgemeinerte Konjunktionen sind

Eine Verbindung von Aussagen, Negationen und logischen Konstanten mit «und».   
Liegt immer in **Negationsnormalform** vor.

* + 1. Disjunktive Normalform

Eine Aussage liegt in disjunktiver Normalform vor, wenn sie eine **verallgemeinerte Konjunktion** ist, oder wenn sie eine Disjunktion von verallgemeinerten Konjunktionen ist.

Eine Verbindung von **verallgemeinerten Konjunktionen** mit «oder».

* + 1. Verallgemeinerte Disjunktion

Eine verallgemeinerte Disjunktion ist…

* Eine einzelne Aussage oder seine Negation (also A oder ¬A) oder
* Einer der logischen Konstante T=wahr oder F=falsch oder
* Eine Disjunktion A ∨ B, falls A und B selbst verallgemeinerte Disjunktionen sind
  + 1. Konjunktive Normalform

Eine Aussage liegt in konjunktiver Normalform vor, wenn sie eine **verallgemeinerte Disjunktion** ist, oder wenn sie eine Konjunktion von verallgemeinerten Disjunktionen ist.

Beispiel: Aussage A: (X ∧ ¬Y) ∨ (¬X ∧ (Y ∨ ¬ Z))

|  |  |  |  |
| --- | --- | --- | --- |
| X | Y | Z | A |
| w | w | w | **f** |
| w | w | f | **f** |
| w | f | w | **w** |
| w | f | f | **w** |
| f | w | w | **w** |
| f | w | f | **w** |
| f | f | w | **f** |
| f | f | f | **w** |

Um A in **disjunktiver Normalform** zu schreiben, werden die Zeilen der Tabelle ausgewertet, in denen A richtig ist. Um A in **konjunktiver Normalform** zu schreiben, werden die Zeilen der Tabelle ausgewertet, in denen A falsch ist.

Das heisst, die **konjunktive Normalform** wäre wie folgt:  
A ⇔ ¬ ((X ∧ Y ∧ Z) ∨ (X ∧ Y ∧ ¬Z) ∨ (¬X ∧ ¬Y ∧ Z))

Daraus lässt sich mit der Regel von de Morgan eine **Negationsnormalform** erstellen:

A ⇔ (¬X ∨ ¬Y ∨ ¬Z) ∧ (¬X ∨ ¬Y ∨ Z) ∧ (X ∨ Y ∨ ¬Z))

### Ein Bild, das Text, Kreuzworträtsel enthält. Automatisch generierte BeschreibungKarnaugh-Veitch-Diagramme

Aus der Wahrheitstafel wird eine **disjunktive** oder **konjunktive Normalform** abgeleitet und in das Diagramm eingetragen. Wir verwenden die Minterm-Methode.

* + 1. Vorgehen:

1. Diagramm mit 2n Zellen erzeugen. Bei n=3:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **B** | **B** | **¬B** | **¬B** |
| **A** |  |  |  |  |
| **¬A** |  |  |  |  |
|  | **C** | **¬C** | **C** | **¬C** |

Die Beschriftungen müssen so gewählt sein, dass 2 benachbarte Zellen sich genau in einer Aussage unterscheiden.

1. Werte aus der Wahrheitstabelle eintragen. Hier werden Beispielwerte verwendet

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **B** | **B** | **¬B** | **¬B** |
| **A** | w | f | f | w |
| **¬A** | w | f | w | w |
|  | **C** | **¬C** | **C** | **¬C** |

1. Alle benachbarten w-Felder zu Blöcken in 2er-Potenz (2,4,8 etc.) zusammenfassen und vereinfachen.   
   Über den Rand hinaus gilt auch als benachbart. Alle w-Zellen müssen überdeckt werden, ohne dass eine f-Zelle überdeckt wird. Zellen dürfen mehrfach überdeckt werden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **B** | **B** | **¬B** | **¬B** |
| **A** | w | f | f | w |
| **¬A** | w | f | w | w |
|  | **C** | **¬C** | **C** | **¬C** |

Im Beispiel gibt es folgende Nachbarn:  
2 Felder unten rechts (¬A ∧ ¬B ∧ C) ∨ (¬A ∧ ¬B ∧ ¬C) ⇔ ¬A ∧ ¬B  
4 Felder ganz links und ganz rechts (A ∨ ¬A) ∧ (B ∨ ¬B) ∧ C ⇔ C   
Zusammengefasst: (¬A ∧ ¬B) ∨ C

## Prädikatenlogik

Aussagen können auch von Variablen abhängen. Aussagen mit Variablen können *wahr* oder *falsch* sein, je nachdem, welche Variable eingesetzt wird. Es geht also um Aussagen, die «manchmal wahr» sind.

Beispiele:   
A(n): 5 | n, 5 ist ein Teiler von n

B(n): 1 + 2 + 3 + 4 + … + n

R(X): der Weg X führt nach Rom.

### Aussageformen

Aussagen, deren Wahrheitswert von einer oder mehreren Variablen abhängt, heissen Aussageformen.

* Wenn in eine Aussageform der Wert einer Variablen eingesetzt wird, dann erhalten wir eine Aussage, die eindeutig entweder wahr oder falsch ist.
* Aussageformen sind unbestimmt, weil nicht bestimmt ist, welcher Wert für eine Variable eingesetzt wird.
* Was in eine Aussageform eingesetzt wird, muss für die Aussageform geeignet sein, muss also ein zulässiges Subjekt sein. A(m): m ist Primzahl. m=7 ist wahr, m=8 ist falsch, m=7.8 ist nicht zulässig

### Prädikat

Aussagen und Aussageformen bestehen aus zwei Teilen: Dem Subjekt und dem Prädikat.

Subjekt: «konkretes Ding» oder Stellvertreter für «konkretes Ding»

Prädiktat: «Eigenschaft», die ein Ding haben kann.

* Einstelliges Prädikat: «ist eine Primzahl» ist die Eigenschaft der natürlichen Zahlen.   
  P(n) ist ein Prädikat für ℕ.
* Zweistelliges Prädikat: «ist Teiler von» ist eine Eigenschaft, die ein Paar von natürlichen Zahlen besitzen kann. T(n,m) ist ein Prädikat für zwei natürliche Zahlen (zweistelliges Prädikat
* Dreistelliges Prädikat: T(k,n,m): k teilt das Produkt von n und m

Anmerkung:   
Prädikate und Aussageformen werden in Mengenbeschreibungen verwendet, um die Menge zu charakterisieren:

### Quantoren

Bei Aussagen, die Variablen enthalten, sind 2 Fälle besonders wichtig:

* Gilt die Aussageform für alle zugelassenen Werte der Variablen?
* Gilt die Aussageform für einen der zugelassenen Werte der Variablen?

Beispiel: Die Summe S(n) aller natürlichen Zahlen von 1 bis n ist . Das gilt für alle natürlichen Zahlen. Das bedeutet:

* Allquantor: «für alle n aus den natürlichen Zahlen gilt…»
* Existenzquantor: «es gibt eine natürliche Zahl n, für die gilt...»

Der Existenzquantor mach in diesem Beispiel wenig Sinn, da der Allquantor auch verwendet werden kann. Beispiel für eine sinnvolle Verwendung des Existenzquantors: «Es gibt ein Schiff, das uns über den Fluss bringen kann»

### Beweisen

Ein Beweis zeigt die Gültigkeit einer Behauptung unter gewissen Voraussetzungen und Annahmen:

* Direkter Beweis:
* Indirekter Beweis:
* Widerspruchsbeweis:
* Vollständige Induktion:
* Vollständige Fallunterscheidung: Wenn und es gilt, dass  
   ist, dann gilt auch
* Schubfachprinzip: Wenn n + 1 Gegenstände (Objekte) auf n Schubladen (Kategorien) verteilt werden, dann befinden sich in mindestens einem Schubfach 2 Gegenstände.
* Diagonalverfahren (Georg Cantor): Anzahl rationaler Zahlen ist genau so gross wie die Anzahl natürlicher Zahlen.

## Vollständige Induktion

Wie kann man natürliche Zahlen mathematisch exakt festlegen?

### Peano-Axiome:

* Null ist eine natürliche Zahl.
* Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n0, der auch eine natürliche Zahl ist.
* Null ist nicht Nachfolger einer natürlichen Zahl.
* Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.
* Die Menge der natürlichen Zahlen ist die kleinste Menge, die die Zahl Null und mit jeder natürlichen Zahl auch ihren Nachfolger enthält.

### Das Schema der vollständigen Induktion

1. Verankerung: Es wird geprüft, ob A(n) für den ersten Wert richtig ist. Ob also die Aussage A(n0) gilt. Z.B. für n0 = 0 oder für n0 = 1
2. Induktionsschritt: n -> n + 1  
   Es wird gezeigt: wenn A(n) gilt, dann gilt auch A(n+1). Als Formel:   
   **a. Induktionsannahme:** A(n) sei richtig für n  
   **b. Induktionsbehauptung:** A(n+1)  
   **c. Induktionsbeweis:** es wird die Aussage A(n) verwendet, um die Richtigkeit der Behauptung A(n+1) zu zeigen.

### Beispiel anhand der Summenformel

1. Induktionsanfang (Verankerung), hier für n0 = 1

**Linke Seite:**

**Rechte Seite:**

**Die Summenformel gilt für n0 = 1.**

1. Induktionsschritt n -> n+1

**a. Induktionsannahme:**

**b. Induktionsbehauptung:**

**c. Induktionsbeweis:**Wir nehmen die linke Seite der Induktionsbehauptung und teilen diese Summe in zwei Teile, sodass für den einen Teil die Induktionsannahme eingesetzt werden kann:

Dann setzen wir die Induktionsannahme ein:

Multiplizieren und klammern ½ aus:

Und schreiben die Klammer als Produkt:

Damit haben wir die Induktionsbehauptung gezeigt und die Gültigkeit der Summenformel für alle natürlichen Zahlen bewiesen.

## Mengen

|  |  |  |  |
| --- | --- | --- | --- |
| P(M) | Potenzmenge | Alle möglichen Resultate als Mengen + leere Menge |  |
| |M| | Mächtigkeit | Anzahl Resultate | (In der Menge M sind 3 Elemente a, b & c) |
|  | Enthalten in | kann Elemente & Mengen vergleichen |  |
|  | Teilmenge von | kann nur Mengen vergleichen. Jede Menge ist eine Teilmenge von sich selbst. Echte Teilmenge: wenn nicht identisch |  |
| {} | Leere Menge | Menge, die keine Elemente beinhaltet. Ist Teilmenge jeder anderen Menge. |  |

### Schreibweisen Mengen

* Aufzählende Form: Die Elemente einer Menge werden zwischen geschweiften Klammern aufgezählt {1, 2, 3} oder {2, 4, 6, 8, …}
* Beschreibende Form: Durch {X ∈ G | E(x)} wird die Menge bezeichnet, die aus allen Elementen x einer Grundmenge G besteht, die die Eigenschaft E besitzen. Z.B. alle reellen Zahlen, die die Gleichung x^2 = 1 lösen, bilden die Lösungsmenge

### Vereinigung

Ein Bild, das Uhr enthält.

Automatisch generierte BeschreibungWenn A und B Mengen sind, dann bezeichnen wir: 1. Die Vereinigung von A und B ist die Menge mit allen Objekten, die Element von A oder Element von B sind.

### Durchschnitt / Schnittmenge

Der Durchschnitt von A und B ist die Menge mit allen Objekten, die sowohl Element von A als auch Element von B sind.

Rechenregeln für Durchschnitt und Vereinigung:

Satz 9: Für Mengen A, B und C gelten die folgenden Gesetze:

Ein Bild, das Tisch enthält.

Automatisch generierte BeschreibungEin Bild, das Tisch enthält.

Automatisch generierte Beschreibung

### Komplement und Differenz

Sei A eine Teilmenge einer Obermenge M. Dann heisst die Menge das Komplement von A bezüglich der Obermenge M.

Für die Mengen A und B in der Obermenge M gelten die folgenden Aussagen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Die Differenz von zwei Mengen A und B besteht aus allen Elementen von A, die nicht in B sind, und wird definiert durch

Das Komplement besitzt die grösste Bindungsstärke, gefolgt von den anderen Mengen-Operatoren Vereinigung, Durchschnitt und Mengendifferenz. Es gilt:

* + 1. Beispiele

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

## Relationen und Abbildungen

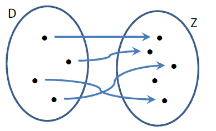
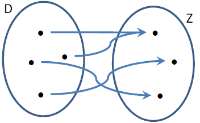
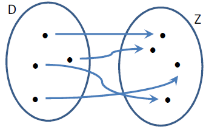
Eine Relation zwischen den nicht-leeren Mengen A und B ist eine Teilmenge des kartesischen Produktes AxB.

Eine Abbildung ist eine Formel, der sämtliche Werte im Definitionsbereich einem Zielbereich zugeordnet werden (analog Funktion in Analysis) und kein Input mehrere Outputs ergibt. Ist f eine Abbildung mit Definitionsmenge D und Zielmenge Z, so schreibt man f : D -> Z. Die Elemente von D heissen Argumente oder Stellen, die Elemente von Z heissen Werte.

Der Graph einer Funktion f ist die Menge aller Punkte, deren Koordinaten (x,y) die Funktionsgleichung von f erfüllen. G kann man als eine Menge von Paaren (x, f(x)) auffassen.

Definitionsmenge = **Urbild**, Zielmenge = **Bildmenge**

### Injektiv, Surjektiv, Bijektiv

* Injektiv: Die Abbildung *f : D -> Z , a -> f(a)* heisst injektiv, wenn für je zwei verschiedene Elemente a1, a2 von A auch die Bilder verschieden sind. Alle Inputs müssen eindeutige Outputs ergeben.
* Surjektiv: Die Abbildung *f: D -> Z, a -> f(a)* heisst surjektiv, wenn jedes Element der Bildmenge als Bild vorkommt.
* Bijektiv: Die Abbildung *f: D -> Z, a -> f(a)* heisst bijektiv, wenn f sowohl injektiv als auch surjektiv ist.

## Modulo-Rechnen

Für heisst die Relation die modulo Relation. Man sagt «a ist gleich r modulo q».

Wenn ist, dann ist a gleich r plus ein Vielfaches von b.

Beispiele:

Zwei wichtige Regeln beim Modulo-Rechnen mit Potenzen sind das Auseinandernehmen von Potenzen und das «Reinziehen»

|  |  |
| --- | --- |
| Potenzen auseinandernehmen | «Reinziehen» |
|  | Der Term in der Klammer kann zuerst berechnet werden: |

Seien . Dann ist

Beispiel:

Kleiner Fermat

Sei eine Primzahl und mit ggT(x,p) = 1.

Dann ist:

**Beispiel:**

**Beispiel:**

Damit lassen sich sehr hohe Potenzen berechnen.

Beispiel: Weil p = 5 eine Primzahl ist, ist . Dann schreiben wir   
.

**Oder kürzer:**

Satz von Euler

Sei und mit ggT(**z**,**n**) = 1. Dann ist

Eulersche -Funktion

Sei und . Dann berechnet sich die Eulersche -Funktion als

Anzahl Zahlen mit und ggT(n,m) = 1 => Anzahl der teilerfremden Zahlen zwischen 0 und n

Anzahl Elemente mit multiplikativem Inversen

**Formen zur Berechung:**

1. Sei eine Primzahl: Dann ist

2. Sei eine Primzahl und : Dann ist

3. Seien und ggT(m,n) = 1: Dann ist

Beispiel 1:

Beispiel 2:

Beispiel 3:

Multiplikatives Inverses

Seien und . Dann gilt:   
Es gibt eine Zahl mit

Beispiel: Multiplikatives Inverse von **7** in

X kann auf 2 Arten berechnet werden. Entweder durch Durchprobieren oder durch den erweiterten euklidischen Algorithmus.

**Durchprobieren:**

nicht durch 11 teilbar

nicht durch 11 teilbar

…

durch 11 teilbar, **x** **= 8**

**Erweiterter euklidischer Algorithmus:** Siehe unten, danach das letzte Resultat von t (in diesem Fall -3) durch Modulo der Zahl in der Originalrechnung nehmen.= multiplikatives Inverses von 7 in

## Euklidischer Algorighmus (Modulo)

Gibt ggT (grösster gemeinsamer Teiler) & kgV (kleinstes gemeinsames Vielfaches) aus.

Wenn der ggT von zwei Zahlen 1 ist, sind die beiden Zahlen teilerfremd (sie haben keinen gemeinsamen Teiler). Bei geraden Zahlen sind alle kleineren geraden Zahlen **nicht** teilerfremd. Bei Primzahlen sind alle Zahlen kleiner als die Primzahl teilerfremd. Die Zahl 1 ist bei jeder Zahl teilerfremd.

Teilerfremde Zahlen der Zahlen 1-10

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 | 1 | 1,2 | 1,3 | 1,2,3,4 | 1,5 | 1,2,3,4,5,6 | 1,3,5,7 | 1,2,4,5,7,8 | 1,3,7,9 |

### Primfaktorzerlegung

12 = **2** \* ~~2~~ \* ~~3~~, 18 = ~~2~~ \* ~~3~~ \* **3** => 2 \* 3 = 6 => ggT. (12 \* 18) / 6 = 36 => kgV

Bei grossen Zahlen sehr rechenaufwendig. Deshalb bestimmen wir den ggT mit dem Euklidischen Algorithmus, und das kgV aus (a\*b) / ggT(a,b)

Euklidischer Algorithmus (ggT finden)

Seien

Initialisierung: Setze und (wie oft passt y in x)und (d.h. bestimme q und r so, dass ist.

Wiederhole, bis r = 0 ist.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ablauf | x | y |  |  |
| Initialisierung | 122 | 72 | 1 | 122 – 72 = 50 |
| 1. Wiederholung | 72 | 50 | 1 | 72 – 50 = 22 |
| 2. Wiederholung | 50 | 22 | 2 | 50 – 44 = 6 |
| 3. Wiederholung | 22 | 6 | 3 | 22 – 18 = 4 |
| 4. Wiederholung | 6 | 4 | 1 | 6 – 4 = 2 |
| 5. Wiederholung | 4 | 2 = ggT | 2 | 0 |

Erweiterter Euklidischer Algorithmus (ggT finden und als Linearkombination darstellen)

Seien

Initialisierung: Setze , (wie oft passt y in x), (d.h. bestimme q und r so, dass ist), und ***(u, s, v, t) = (1,0,0,1)***

Wiederhole, bis r = 0 ist.

**x = y** aus der vorangegangenen Zeile

**y = r** aus der vorangegangenen Zeile

**q = x div y**, **r = x mod y** = x-y\*q

**u = s** aus der vorangegangenen Zeile

**s = u – q \* s** mit u, q & s aus der vorangegangenen Zeile

**v = t** aus der voangegangenen Zeile

**t = v – q \* t** mit v, q & t aus der vorangegangenen Zeile

Ergebnis: In der letzten Zeile gilt y = ggT, s \* a + t \* b. Wenn ggT = 1 ist, dann folgt: t\*b = 1 mod a

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ablauf | x | y |  |  | ***u*** | ***s*** | ***v*** | ***t*** |
| Initialisierung | 99 | 79 | 1 | 99 – 79 = 20 | 1 | 0 | 0 | 1 |
| 1. Wiederholung | 79 | 20 | 3 | 79 – 60 = 19 | 0 | 1 – **1** \* 0 = **1** | 1 | 0 – **1** \* 1 = **-1** |
| 2. Wiederholung | 20 | 19 | 1 | 20 – 19 = 1 | 1 | 0 – **3** \* 1 = **-3** | -1 | 1 – **3** \* -1 = **4** |
| 3. Wiederholung | 19 | 1 | 19 | 19 – 19 = **0** | -3 | 1 – 1\*-3 = **4** | 4 | -1 – 1\*4 = **-5** |

Bedeutet:

## RSA-Verschlüsselung

Die RSA-Verschlüsselung ist ein Public-Key-Verfahren. Funktionsprinzip: Sie vergeben einen öffentlichen Schlüssel, mit dem jeder Botschaften an Sie so verschlüsseln kann, dass nur Sie sie entschlüsseln können.

### Public & Private Key erhalten

1. Zwei Primzahlen (**p**,**q**) multiplizieren zum Produkt **n**:

2. Die Eulersche -Funktion von n berechnen.ergibt dasselbe Resultat und da beide Zahlen Primzahlen sind, kann einfach gerechnet werden.

3. Eine beliebige Zahl a zwischen 1 und auswählen, die mit teilerfrend ist:   
z.B. **a** = **3**, Test: ggt(20,3)=1

4. Das multiplikative Inverse von in berechnenKleinstmögliche Zahl => durch **20** teilbar, also

5. Nun haben wir den Public Key (b & n) und den Private Key(a) zur Verschlüsselung:

### Text verschlüsseln

Ein Bild, das Text, Wasser, schließen, hell enthält.

Automatisch generierte Beschreibung1. Buchstabentabelle generieren, zum Beispiel

2. Text in Zahlen aus Tabelle umwandeln: T = 20, E = 5, S = 19, T = 20

3. Zahlen mit **b** potenzieren und Modulo **n** rechnen:

4. Nun kann die Nachricht «26, 14, 13, 26» gesendet werden.

### Text entschlüsseln

1. Dieselbe Buchstabentabelle wie beim Verschlüsseln verwenden.

2. Die empfangene Nachricht mit potenzieren und Modulo **n** rechnen:

3. Zahlen in Buchstaben umwandeln: 20 = **T**, 5 = **E**, 19 = **S**, 20 = **T**

## Lineare Algebra

Allgemein ist eine linare Gleichung in einer Variablen x von der Form , wobei reelle Konstanten sind. Eine lineare Gleichung in Variablen hat die Gestalt , wobei und reelle Konstanten sind.

### Lineares Gleichungssystem mit zwei Unbekannten

Die beiden Gleichungen unten bilden ein lineares Gleichungssystem mit zwei Unbekannten.

Bei einem Gleichungssystem wie unten, lässt sich erkennen, dass das System unendlich viele Lösungen hat:

Für die freie Variable kann man einen beliebigen Parameter wählen. Die unendlich vielen Lösungen haben somit die parametrisierte Form

## Matrizen (Lineare Algebra)

Ein lineare Gleichungssystem kann auch als Matrizen ausgedrückt werden.

Zum Beispiel das Geichunggsystem oben (Hinterste Spalte ist die Lösung):

Anzahl Zeilen = m, hier 2; Anzahl Spalten = n, hier 3 (mit Lösung).

Besteht eine Matrix aus einer einzigen Spalte, so heisst sie Spaltenmatrix, besteht sie aus einer einzigen Zeile, ist sie eine Zeilenmatrix. Eine (1,1)-Matrix ist sowohl Zeilen- als auch Spaltenmatrix und wird auch als Skalar bezeichnet.

Vertauscht man Zeilen und Spalten einer Matrix, so erhölt man die transponierte Matrix.

Spaltenmatrizen   
werden mit Kleinbuchstaben angeschrieben. Sie können auch mit Vektoren identifiziert werden.

Einheitsmatrix

Quadratische Diagonalmatrix, deren Diagonalelemente alle gleich 1 sind

Obere und untere Dreiecksmatrix

Eine obere Dreiecksmatrix hat unterhalb der Diagonale nur Nullen. Eine untere Dreiecksmatrix hat oberhalb der Diagonale nur Nullen.

### Rechnen mit Matrizen

Zwei Matrizen sind gleich, wenn sie dieselbe Ordnung haben und die einander entsprechenden Elemente übereinstimmen.

und sind gleich, wenn und .

Addition und Subtraktion (Linearkombination)

Sind und zwei Matrizen gleicher Ordnung, so ist ihre Summe diejenige Matrix, die durch Addition der einander entsprechenden Elemente entsteht. Subtraktion funktioniert analog.

und

Multiplikation (Produkt)

Das Matrizenprodukt berechnet sich durch Zeile von A \* Spalte von B.

und

|  |  |
| --- | --- |
|  |  |
|  |  |

Achtung: Das Matrizenprodukt ist nur für Matrizen A und B mit der Eigenschaft «Spalten von A gleich Zeilen von B» definiert.

Inverse

Die inverse Matrix ist die Matrix, die multipliziert mit der ursprünglichen Matrix die Einheitsmatrix ergibt. Besitzt eine quadratische Matrix eine Inverse, so ist diese eindeutig bestimmt. Das lineare quadratische Gleichungssystem hat genau dann eine eindeutige Lösung , wenn A invertierbar (regulär) ist.

Bei 2x2 Matrix

Bei 3x3 Matrix

1. Die Einheitsmatrix neben die ursprüngliche Matrix schreiben. Ab jetzt wird diese erweiterte Matrix als Gesamtpaket betrachtet.

2. Matrix umformen, dass links die Einheitsmatrix ist (mit dem Gauss-Jordan-Algorithmus)

3. Invertierte Matrix ablesen.

### Elementare Umformungen und Zeilenstufenformen

Unter einer elementaren Gleichungsumformung versteht man eine der drei grundlegenden Operationen:

* Gleichungen vertauschen
* Gleichung mit einer Konstante multiplizieren
* Addition eines Vielfachen einer Gleichung zu einer anderen Gleichung

Elementare Gleichungsumformungen ändern nicht die Lösungsmenge eines linearen Gleichungssystems.

Zeilenstufenform

Durch elementare Zeilenumformungen kann man nun jede Matrix auf Zeilenstufenform bringen. Eine Matrix hat Zeilenstufenform, wenn folgende Eigenschaften erfüllt sind:

* Alle Zeilen, die nur Nullen enthalten, stehen in den untersten Zeilen der Matrix.
* Wenn eine Zeile nicht nur aus Nullen besteht, so ist die erste von Null verschiedene Zahl eine Eins (führende Eins).
* In zwei aufeinanderfolgenden Zeilen, die nicht nur aus Nullen bestehen, steht die führende Eins der unteren Zeile rechts von der führenden Eins der oberen Zeile.

Die Zeilenstufenform kann dann wieder als Gleichung geschrieben werden. Dabei entspricht jede Spalte einer Variable (hier ).

Die führenden Einsen werden so zu führenden Variablen, die übrigen (hier ) werden zu freien Variablen. Nun kann man die freien Variablen auf die rechte Seite subtrahieren, um die Gleichungen nach den führenden Variablen aufzulösen.

Reduzierte Zeilenstufenform

Besitzt eine Matrix Zeilenstufenform und gilt noch zusätzlich, dass eine Spalte, die eine führende Eins enthält, keine weiteren von Null verschiedenen Einträge enthält, dann hat sie reduzierte (normierte) Zeilenstufenform.

-> Siehe Gauss-Jordan-Algorithmus

## Gauss-(Jordan-)Algorithmus (Lineare Algebra)

Damit lässt sich ein lineares Gleichungssystem in (reduzierte) Zeilenstufenform bringen.

Gauss -Verfahren (Zeilenstufenform)

1. Wir bestimmen die am weitesten links stehende Spalte, die von Null verschiedene Werte enthält.

2. Die oberste Zahl in der ersten Spalte darf keine Null sein. Sonst mit anderen Zeile vertauschen.

3. Ist das erste Elemente der in Schritt 1 gefundenen Spalte, dann dividieren wir die erste Zeile durch , um die führende Eins zu erzeugen. (falls zB. )

4. Wir addieren passende Vielfache der ersten Zeile zu den übrigen Zeilen, um unterhalb der führenden Eins Nullen zu erzeugen.

ergibt:

5. Wir wenden die ersten vier Schritte auf den Teil der Matrix an, den wir durch Streichen der ersten Zeile erhalten, und wiederholen dieses Verfahren, bis die erweiterte Koeffizientenmatrix Zeilenstufenform hat.

6. Wir lösen das System in Zeilenstufenform durch Rückwärtssubstitution.

Gauss -Jordan-Verfahren (reduzierte Zeilenstufenform)

1. Schritte 1-5 vom Gauss-Jordan-Verfahren durchführen.

2. Mit der letzten nicht verschwindenden Zeile beginnend, addiere man geeignete Vielfache jeder Zeile zu den darüber liegenden Zeilen, um über den führenden Einsen Nullen zu erzeugen.

Nun kann die Lösung direkt abgelesen werden

Pivotsuche

Man kann bei den Matrizen auch die Zeilen vertauschen, wenn sich dadurch das Verfahren einfacher anwenden lässt, das muss man sich jedoch merken und am Schluss wieder zurücktauschen.

### Zu Gauss-Algorithmus und Determinante

* Das Tauschen von benachbarten Zeilen führt in der Determinante zu Vorzeichenwechseln.
* Multiplikation einer Zeile mit führt zu .
* Addition eines Vielfachen einer Zeile zu einer anderen ändert die Determinante nicht.

## Vektoren

### Begriffe

* Ortsvektor: Vektor vom Ursprung zu einem Punkt
* Normalenvektor: Vektor, der im 90°-Winkel zu einem anderen Vektor steht.
* Parameterform: Möglichkeit, um eine Gerade oder eine Ebene darzustellen. Dabei wird ein Stütz- und ein Richtungsvektor benötigt.
* Stützvektor: Vorder Vektor in der Parameterform, fast immer Ortsvektor. Definiert den «Startpunkt» des Vektors.
* Richtungsvektor: Hinterer Vektor in der Parameterform. Definiert die Länge und Richtung des Vektors und kann mithilfe des Parameters t beliebig skaliert werden.

Rechenregeln für geometrische Vektoren

**1. Kommutativität:**

**2. Assoziativität:**

**3. Nullvektor:** Für jeden Vektor gilt

**4. Existenz negativer Vektoren:** Zu jedem Vektor gibt es einen Gegenvektor mit .

### Skalares Vielfaches

Für einen Vektor und eine reelle Zahl bezeichnet man mit dem skalaren Vielfachen den Vektor, dessen Pfeile:

* Parallel zu den Pfeilen von sind
* -mal so lang wie die Pfeile von sind
* Gleich gerichtet zu den Pfeilen von sind, falls , entgegengesetzt gerichtet zu den Pfeilen von , falls ist.

Die Verknüpfung eines Skalars mit einem Vektor nenne man skalare Multiplikation. Dafür gelten folgende Regeln:

Rechenregeln für skalare Multiplikation

Für alle reellen Zahlen und für alle geometrischen Vektoren gelten die folgenden Eigenschaften:

**1. Distributivität:**

**2. Distributivität:**

**3. Assoziativität:**

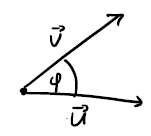
**4.**

**5.**

**6.**

**7.**

### Skalarprodukt

Mit dem Skalarprodukt lassen sich zwei Vektoren miteinander multiplizieren, die gleich gross sind. Als Ergebnis erhält man eine reelle Zahl, die Skalar genannt wird.

Damit lässt sich auch der Winkel zwischen Vektoren berechnen:

Eigenschaften

* ist positiv, wenn (spitzer Winkel)
* ist 0, wenn (rechter Winkel, orthogonal)
* ist negativ, wenn (stumpfer Winkel)
* , wenn oder

### Orthogonale Vektoren

Stehen zwei Vektoren senkrecht aufeinander, so nennt man das auch orthogonal. Wenn wir noch vereinbaren, dass der Nullvektor senkrecht zu jedem Vektor ist, erhalten wir:

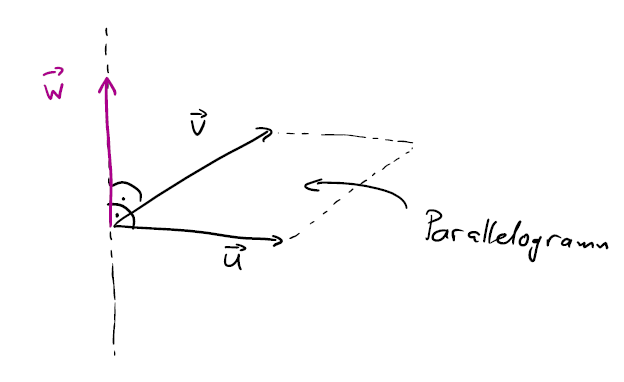
Zwei Vektoren und sind genau dann orthogonal, wenn ist.

### Koordinaten- und Komponentenform

Ein Bild, das Antenne enthält.

Automatisch generierte BeschreibungIst , so sind und die Koordinaten des Vektors und seine Koordinatenform (links im Bild). Eine andere Darstellungsform erhalten wir mit den natürlichen Einheitsvektoren und . Das Skalarprodukt des Einheitsvektors mit dem Vektor ergbit die erste Koordinate von :   
Der Vektor ist der orthogonale Projektionsvektor von auf . Den Vektor kann man daher folgendermassen schreiben (***Komponentenform***, rechts im Bild):

### Kreuzprodukt

Existiert nur im Raum . Unter dem Kreuzprodukt zweier räumlicher Vektoren und versteht man den eindeutig bestimmten Vektor mit folgenden drei Eigenschaften

* ist sowohl zu als auch zu orthogonal (steht senkrecht auf beide)
* Die Länge des Vektors ist gleich dem Produkt aus den Längen der Vektoren und und dem Sinus des von ihnen eingeschlossenen Winkels:
* Die Vektoren und bilden in dieser Reihenfolge ein Rechtssystem.

**Weiter gilt:**

* Die Länge des Kreuzproduktes entspricht dem Flächeninhalt des von den Vektoren und aufgespannten Parallelogramms (Vektorprodukt).
* Wenn das Kreuzprodukt Null ergibt, so sind die Vektoren parallel.

Kreuzprodukt berechnen

Rechenregeln des Kreuzproduktes

Sind und beliebige Vektoren im Raum und eine reelle Zahl, so gilt:

1. Anti-Kommutativität:

2. Distributivität:

3. Distributivität:

**4. Assoziativität:**

**5.**

## Lineare Abblidungen

Eine Abbildung heisst linear, wenn sie mit den Vektorraum-Verknüpfungen und in und verträglich ist, das heisst, wenn es gleichgültig ist, ob ich zwei Vektoren in erst addiere und dann die Summe nach abbilde oder ob ich sie erst abbilde und dann ihre Bilder addiere; entsprechend für die skalare Multiplikation.

Eine Abbildung von nach ist linear, wenn sie die Form hat, wobei ein reeller Parameter ist.

Der Graph einer linearen Funktion von nach ist eine Gerade und geht durch den Koordinatenursprung, dabei ist die Steigung der Geraden. ist nur dann eine lineare Abbildung, wenn der Graph von eine Gerade ist und durch den Koordinatenursprung geht.

Jede reelle lineare Funktion hat die folgenden Eigenschaften:

Für alle gilt:

1.

2.

3.

Beispiel:

Eine Abbildung ist nur linear, wenn diese Bedingungen zutreffen.

Matrizen und lineare Abbildungen

1. Eine Lineare Abbildung wird eindeutig durch eine Matrix dargestellt.

2. Eine Matrix erzeugt eine lineare Abbildung .

*Das heisst, Lineare Abbildungen und Matrizen sind «dasselbe» (Lineare Abbildung ist eine Funktion und eine Matrize ein rechteckiges Zahlensystem)*

Zu beachten: Die Addition findet im Vektorraum statt, während die Addition im Vektorraum stattfindet.

**Sei eine lineare Funktion. Dann:**

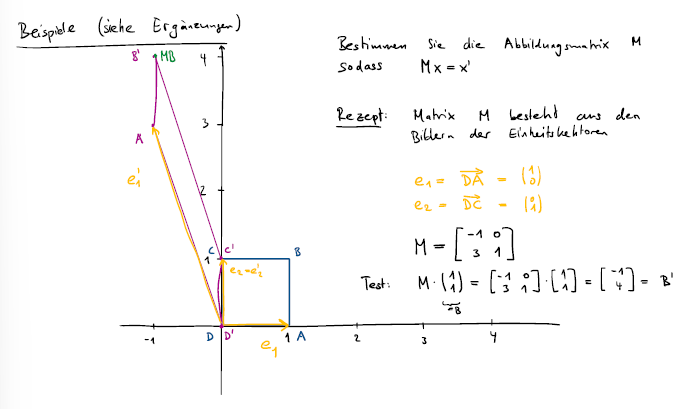
Die Matrix besteht aus den Bildern der kanonischen Einheitsvektoren.

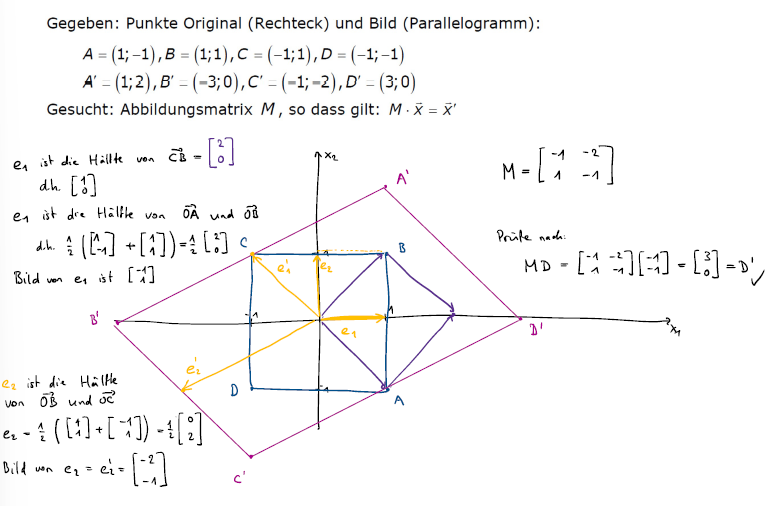
### Nullabbildung

Es ist die -Nullmatrix und der Nullvektor im . Dann gilt für jeden Vektor

,

also bildet die Multiplikation mit der Nullmatrix jeden Vektor des in den Nullvektor des ab. heisst Nullabbildung von nach





## Geraden und Ebenen

Eine Gerade hat keinen Start- oder Endpunkt (sonst wäre es eine Strecke).

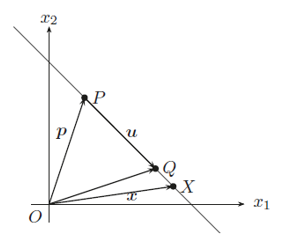
### Darstellungen von Geraden

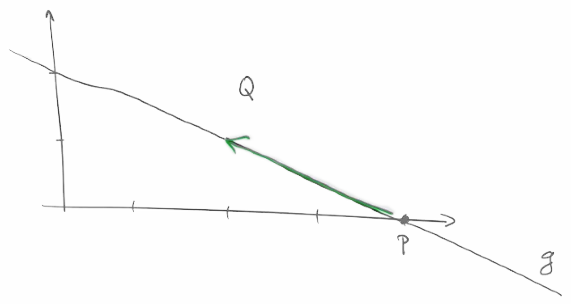
Sind eine Gerade und zwei Punkte und auf dieser gegeben, so gilt: Für einen beliebigen Punkt der Geraden ist der Ortsvektor. Da und auf derselben Geraden liegen, sind und Vielfache voneinander.

Parameterform

Jede Gerade in der Ebene oder im Raum lässt sich durch eine Gleichung der Form

Beschreiben. Hierbei ist ein **Stützvektor**, ein **Richtungsvektor** und ein reeller Parameter.





**Beispiel:**

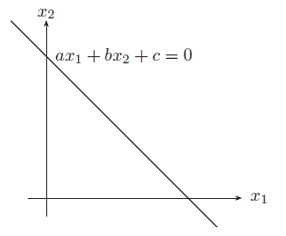
*Achtung: bei t() sind die Zahlen nicht gleich Q, sondern der Abstand von P zu Q.*

Koordinatenform

Jede Gerade in der -Ebene lässt sich durch eine Koordinatengleichung

oder

Beschreiben, bei der mindestens einer der beiden Koeffizienten und ungleich Null ist.

**Beispiel von oben in Koordinatenform**

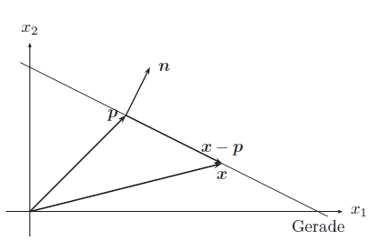
In Komponentengleichung umwandeln:

Ersetze mit 2. Gleichung, die nach aufgelöst wurde

Danach noch umstellen:

--> ist eine parameterfreie Darstellung und nicht eindeutig.

*Es lässt sich auch hier der Normalenvektor ablesen:*

Normalenform

Jede Gerade in der Ebene lässt sich durch eine Normalengleichung

oder

Beschreiben. Hierbei ist ein Stützvektor und ein Normalenvektor.

Normalenvektor steht senkrecht zur Geraden.

**Beispiel von oben in Normalenform:**

*ist von der Parameterform, gedreht und zweite Komponente negiert.*

***Skalarprodukt***

vereinfachte Normalengleichung

--> ist eine parameterfreie Darstellung und nicht eindeutig.

Hessesche Normalform

Ist ein Spezialfall der Normalenform für Geraden oder Ebenen.

Weil bei der Hesse Normalform ein **normierter Vektor** verwendet wird,

kann man einen Abstand besonders gut berechnen.

mit

**Eigenschaften:**

vom Ursprung weg

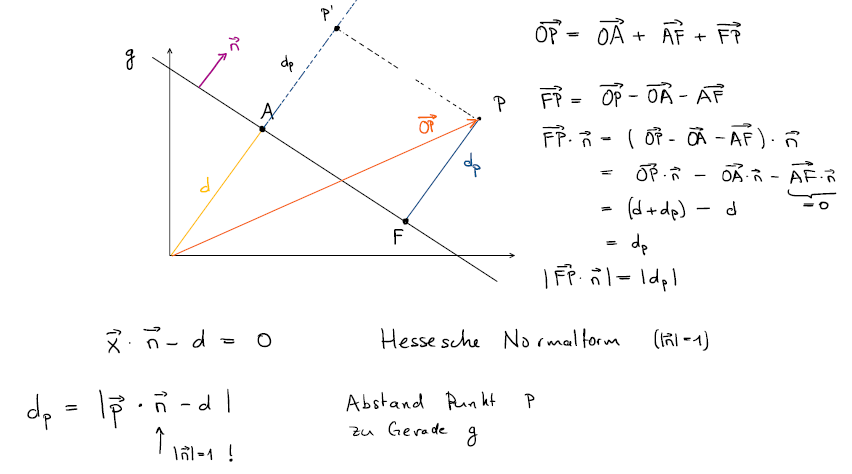
zum Ursprung hin

Gerade geht durch Ursprung

**Beispiel von oben in Hessescher Normalenform:**

-> Der Vektor muss um den Faktor gekürzt werden

### Abstand von Punkt zu Gerade

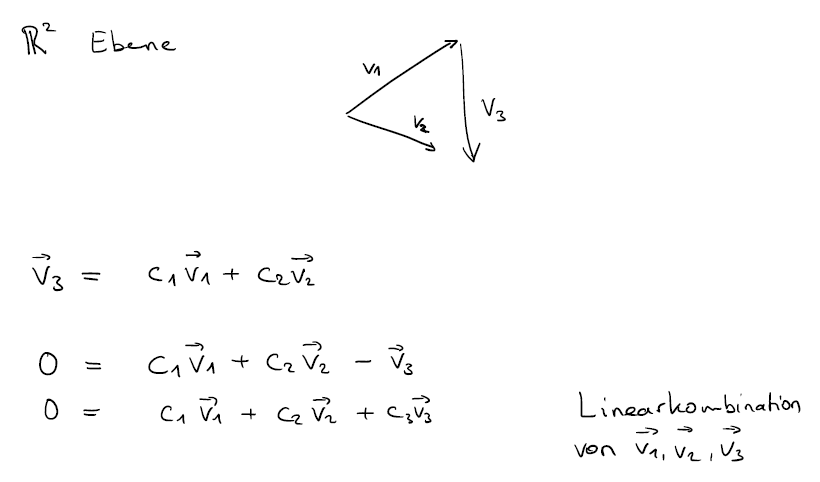


### In der Ebene

nicht parallel

* Parameterform:
* Koordinatengleichung:
* Normalengleichung:
* Hessesche Normalengleichung:

### Lineare Unabhängigkeit



Die Menge ist linear abhängig, wenn es eine Linearkombination

gibt, mit mindestens einem Koeffizienten

Die Menge ist linear unabhängig, wenn

nur für lösbar ist.

Bzw. genau dann, wenn das lineare Gleichungssystem

Eine eindeutige Lösung hat, nämlich

Beispiel

Kann als Linearkombination von dargestellt werden?

Wenn ja, dann ist linear abhängig.

Lässt sich mit dem Gauss-Algorithmus lösen

Beispiel

, mindestens 1 Koeffizient darf nicht 0 sein, damit linear abhängig

Wenn ein Vektor ein Vielfaches von einem anderen Vektor ist, geht das gut

**Beispiel für linear unabhängige Vektoren wären die kanonischen Einheitsvektoren.**

### Basis eines Vektorraums

Die Vektoren bilden genau dann eine Basis des Vektorraumes , wenn jeder Vektor aus als eindeutige Linearkombination der Vektoren dargestellt werden kann. Die Dimension eines Vektorraumes ist gleich der Anzahl der Vektoren einer Basis für . Hierfür schreiben wir .

Ein Vektorraum ist endlich dimenstional, wenn eine Basis für aus nur endlich vielen Vektoren besteht, sonst ist unendlich dimensional.

Die Menge ist eine Basis für genau dann, wenn jeder Vektor als eindeutige Linearkombination dargestellt werden kann. M ist linear unabhängig.

### Determinante

Die Determinante gibt an, wie viel grösser die Fläche einer Form sein wird, wenn sie mit dieser Matrix multipliziert wird (nur bei quadratischen Matrizen). Ist die Determinante negativ, wird die Form gespiegelt. Wenn entweder eine Zeile / Spalte null ist oder zwei Zeilen/Spalten übereinstimmen oder zwei Zeilen/Spalten linear abhängig sind, ist die Determinante 0.

2x2 Matrix

3x3 Matrix: Regel von Sarrus

Dreiecksmatrix

**Bei grösseren Matrizen: Auf kleinere zurückführen.**

Laplacescher Entwicklungssatz

Schritt 1: Jedem Element in der Matrix ein Plus oder Minus zuordnen, abwechslungsweise, beim Plus beginnend:

Schritt 2: Wir rechnen die Determinante von der ersten Zeile. Man nimmt den ersten Eintrag, und rechnet die Determinante von den Spalten und Zeilen, die nicht beinhalten.

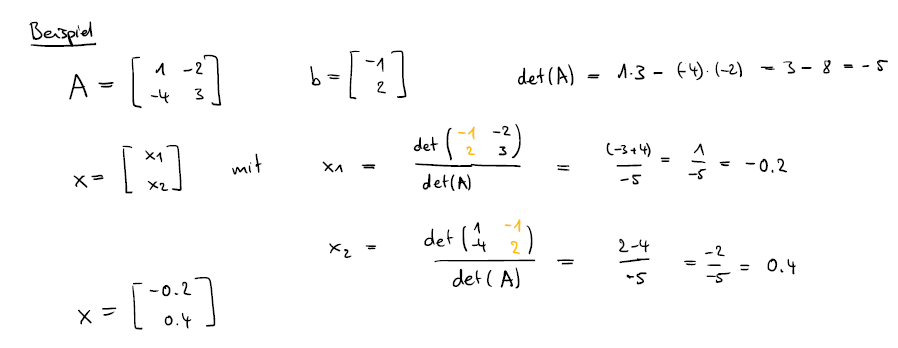
Das wiederholt man mit den anderen Einträgen der ersten Zeile:

ergibt:

Cramersche Regel

Ein Lineares Gleichungssystem ist gegeben, mit . Dann ist die Lösung eindeutig bestimmt () und kann berechnet werden mit:

Matrix mit Spalte ersetzt durch .



## Eigenwerte und Eigenvektoren

Definition

Wenn erfüllt ist, dann nennen wir Eigenwert und Eigenvektor.

ist ein Eigenpaar («sie gehen immer zusammen, existieren nicht separat»)

**Eigenvektor:** es reicht einen geeigneten Vektor zu wählen, weil gestreckte Eigenvektoren sind wieder Eigenvektoren:

-> Wähle Eigenvektor so, dass er einfache Komponenten hat, bzw

Beispiel

### Berechnung

Gegeben eine Matrix

Die Lösungen von sind Eigenwerte von .

Beispiel: Bestimme Eigenwerte von A:

Eigenwerte:

Satz

, mit verschiedenen Eigenwerte mit zugehörigen Eigenvektoren.

Dann gilt: sind linear unabhängig.

Spezialfall: Wenn es paarweise verschiedene Eigenwerte gibt (So viele Eigenwerte wie Dimensionen), dann gibt es linear unabhängige Eigenvektoren. Diese bilden eine Basis.

Bei einer Dreiecksmatrix sind die Diagonalelemente gleich den Eigenwerten.

### Diagonalisierung einer Matrix

Umwandlung einer Matrix in eine Diagonalmatrix.

Schritt 1: Finden der Eigenwerte (

-> Die Eigenwerte sind die Nullstellen, die Nullstellen sind dort, wo eine Klammer = 0 ist.

Eigenwerte: .

Schritt 2: Diagonalisierbarkeit prüfen:

* Die Matrix ist quadratisch
* Das charakteristische Polynom hat Nullstellen (in diesem Fall: 3x3 Matrix, 3 Nullstellen (), also erfüllt)
* Die algebraische und geometrische Vielfachheit der Eigenwerte sind gleich (Anzahl Eigenwerte und Eigenvektoren ist gleich)

Schritt 3: Diagonalmatrix aufschreiben