Lineare Algebra

Arbeitsgruppe Algebra

Skript

Erstellt von

Ghislain Fourier

Verity Mackscheidt
Maximilian Plenge

Inhaltsverzeichnis

Kapitel 0

Einleitung

Dieses Skript ist die gemeinsame Grundlage der Arbeitsgruppe Algebra für die Vorlesungen

- Grundlagen der Algebra
- Lineare Algebra 1
- Lineare Algebra 2.

Das Skript erhebt keinen Anspruch auf Vollständigkeit; manche Beweise werden von den in den Vorlesungen präsentierten Beweisen abweichen, was vor allem und insbesondere auch für die Beispiele gilt. Das zugrunde liegende Gerüst, die Inhalte und Reihenfolge werden aber unabhängig von den Dozierenden jeweils identisch sein.

Freuen Sie sich auf ein Jahr **Lineare Algebra**! Sie werden nach zwei Semestern souverän mit Begriffen umgehen, die Ihnen heute noch nichts sagen, so etwa jene der Gruppen, Ringe oder Bilinearformen. Aussagen wie das Rang-Theorem oder der Trägheitssatz von Sylvester werden mit Leben gefüllt sein und die Welt der Vektorräume und linearen Abbildungen wird Ihnen mehr als vertraut sein.
Der Weg dahin ist weit und schwer, vor allem aber ist er mit Arbeit verbunden. Das Mathematikstudium steht in dem Ruf, einer der schwierigeren Studiengänge zu sein, wobei die ersten beiden Semester mit den Vorlesungen zur Analysis und Linearen Algebra die wohl schwierigste Phase ausmachen. Dies liegt weniger an den Inhalten (die Algebraische Geometrie ist sicherlich komplizierter), sondern daran, dass Sie zum ersten Mal diese Sprache und Denkweise erleben.
Geben Sie sich selber Zeit, sich dort hineinzudenken und geben Sie nicht nach wenigen Wochen auf, dann werden Sie schließlich mit einer ganz neuen Welt belohnt. Die ersten Wochen werden frustrierend sein und Durchhaltevermögen erfordern. Der **beste Rat** für diese Wochen und auch für das restliche Studium ist dieser:

Suchen Sie sich Lerngruppen! Mathematik ist nichts für EinzelkämpferInnen.

Das vorliegende Skript ist nur eines von sehr vielen. Es mag Quellen geben, die die Inhalte für Sie persönlich zugänglicher gestalten. Im Literaturverzeichnis finden Sie einige Bücher zur Linearen Algebra, wobei diese Liste natürlich weit davon entfernt ist vollständig zu sein. Der Klassiker ist sicherlich [2], aber [1, 3, 4, 5, 6, 7], können gleichermaßen empfohlen werden. Herr Prof. Bödigheimer hat eine subjektive Einordnung einer möglichen Literaturliste für die Lineare Algebra erstellt.

Das Team der Algebra wünscht Ihnen viel Spaß und viel Erfolg mit der Linearen Algebra!

Kapitel 1

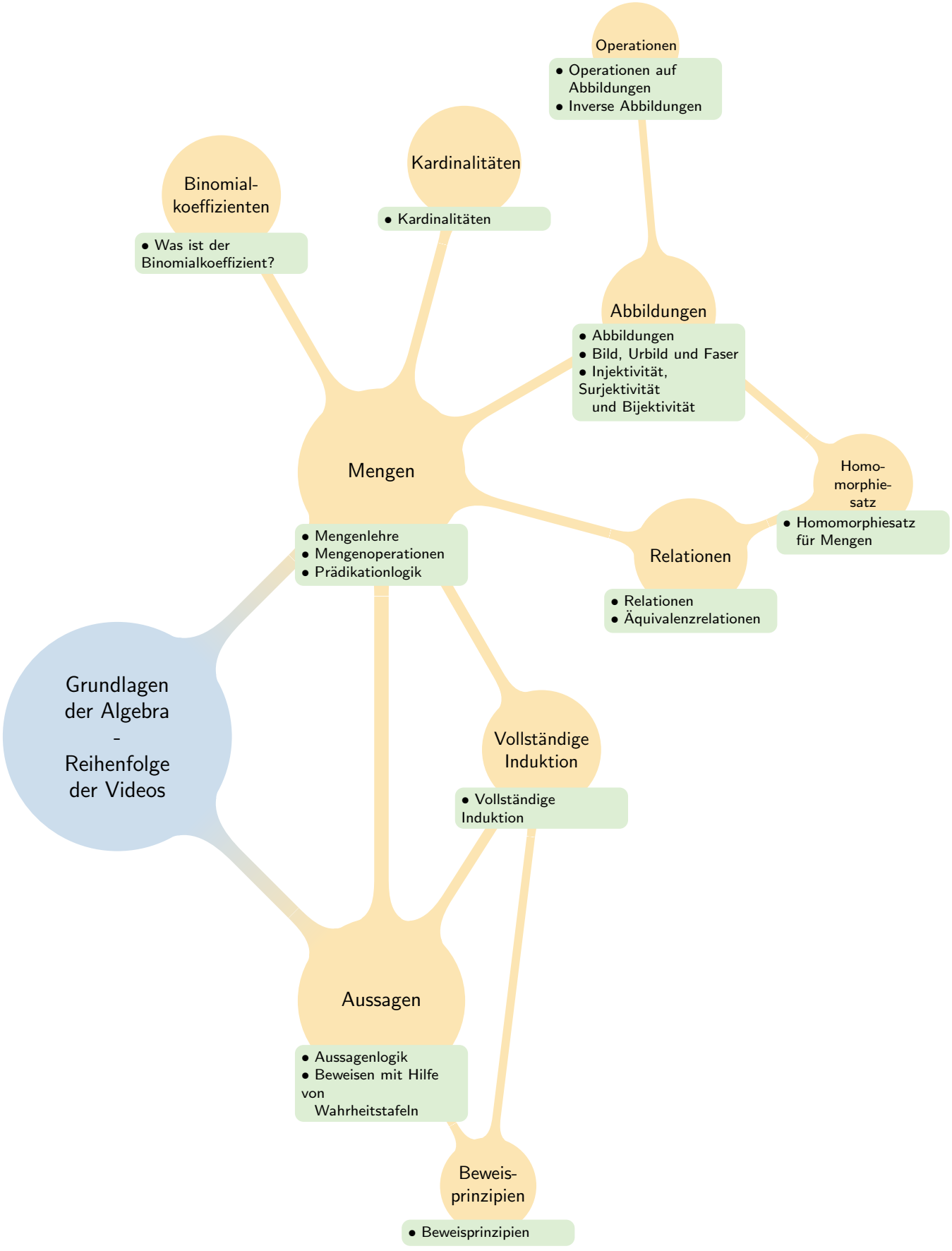
Grundlagen der Algebra

1.1 Mind map

Wir geben Ihnen hier eine Übersicht über die Inhalte der *Grundlagen der Algebra*-Vorlesung. Auf der folgenden Seite finden Sie eine Mind map, die grafisch die Zusammenhänge zwischen den einzelnen Themen darstellt. Insbesondere sieht man, wie sich der Inhalt Woche für Woche aufbaut, von den grundlegenden Definitionen der Mengenlehre und Aussagenlogik hinzu dem Homomorphiesatz für Mengen. In dem blauen Feld sehen Sie, zu welchen Themen wir Ihnen im Moodle-Lernraum erklärende Videos zur Verfügung stellen werden.

Inhalte:

- Aussagen (Vorlesung 1, Abschnitt 1.3)
  - Aussagenlogik: Definition 'logische Aussage', Beispiele, Verknüpfungen, Rechenregeln
  - Beweisen mit Hilfe von Wahrheitstafel: Beispiel - De Morgan Gesetze, Umgangssprache übersetzen
- Mengen (Vorlesung 2, Abschnitt 1.4)
  - Mengenlehre: Definition 'Menge', Beispiele, Leere Menge, Teilmenge, Potenzmenge
  - Mengenoperationen: Komplement, Schnitt, Vereinigung, Differenz, kartesisches Produkt, Rechenregeln
  - Prädikatenlogik: Existenz- und Allquantor, Beispiele, Negation, Anwendung Schnitt und Vereinigung unendlich vieler Mengen
  - Kardinalitäten: Definition 'Kardinalität', Zusammenhang mit verschiedenen Operationen
- Beweisprinzipien (Vorlesung 3, Abschnitt 1.5):
  - Direkter Beweis, Kontraposition, Widerspruch, Ringschluss
  - Vollständige Induktion (Vorlesung 3, Abschnitt 1.5): Prinzip, Beispiele, Varianten
- Abbildungen (Vorlesung 4, Abschnitt 1.6)
  - Abbildungen: Definition, Beispiele
  - Bild, Urbild und Faser: Definitionen und Beispiele, Urbildabbildung
  - Injektivität, Surjektivität und Bijektivität: Definitionen und Beispiele, Zusammenhang mit Fasern
  - Einschränkung, Komposition, Eigenschaften der Komposition
  - Umkehrabbildung, links- und rechtsinverse Abbildung, Zusammenhang zu Injektivität, Surjektivität und Bijektivität
- Relationen (Vorlesung 5, Abschnitt 1.7):
  - Definition Relation, Eigenschaften, Beispiele, Definition Äquivalenzrelation und Ordnung
  - Äquivalenzrelationen: Beispiele, Äquivalenzklassen, Transversale, Zusammenhang mit Partitionen
- Homomorphiesatz für Mengen (Vorlesung 6, Abschnitt 1.8) : Aussage, Beispiele, Anwendungen
- Binomialkoeffizient (Vorlesung 6, Abschnitt 1.9): Definition, Beispiele, Rechenregeln


Grundlagen der Algebra - Reihenfolge der Videos
Mengen
• Mengenlehre
• Mengenoperationen
• Prädikationlogik
Binomial-koeffizienten
• Was ist der Binomialkoeffizient?
Kardinalitäten
• Kardinalitäten
Operationen
• Operationen auf Abbildungen
• Inverse Abbildungen
Abbildungen
• Abbildungen
• Bild, Urbild und Faser
• Injektivität, Surjektivität und Bijektivität
Homo-morphie-satz
• Homomorphiesatz für Mengen
Relationen
• Relationen
• Äquivalenzrelationen
Vollständige Induktion
• Vollständige Induktion
Aussagen
• Aussagenlogik
• Beweisen mit Hilfe von Wahrheitstafeln
Beweis-prinzipien
• Beweisprinzipien

1.2 Notationen

Wir werden im Folgenden mit $\mathbb{N}$ die **natürlichen Zahlen** bezeichnen, das ist die Menge

$$\{1, 2, 3, \ldots\}.$$

Wir sind dabei nicht präzise, denn was sollen diese ... sein? Was soll eine Menge sein? usw. Eine formale Definition wäre auch möglich, beispielsweise als die *freie Halbgruppe erzeugt von einem Element*, aber wir wollen hier für den Einstieg auf unsere Intuition vertrauen. Die 0 ist für uns keine natürliche Zahl, daher notieren wir die Menge

$$\{0, 1, 2, 3, \ldots\}$$

mit $\mathbb{N}_0$.
Aus den natürlichen Zahlen können wir dann auch die **ganzen Zahlen** $\mathbb{Z}$ ableiten, das ist die Menge

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3 \ldots\}$$

Formal würden wir das wieder als *freie Gruppe erzeugt von einem Element* definieren können. Zur Definition einer Gruppe kommen wir in wenigen Wochen.

1.3 Aussagenlogik

Wir übernehmen aus Wikipedia:

> *Allgemein ist die klassische Logik durch zwei Eigenschaften charakterisiert:*
>
> - Jede Aussage hat einen von genau zwei Wahrheitswerten, meist „falsch“ oder „wahr“ (kurz „f“ oder „w“).
> - Der Wahrheitswert jeder zusammengesetzten Aussage ist eindeutig durch die Wahrheitswerte ihrer Teilaussagen bestimmt.

Diese zwei Eigenschaften werden wir im Folgenden näher untersuchen, wir fangen mit der ersten an. Eine (mathematische) Aussage muss also zwingend einen Wahrheitswert haben, der unabhängig von unserer Anschauung, unserer Meinung etc. ist.

Beispiel 1.3.1

Einige Aussagen und ihre Wahrheitswerte:

1. $2 + 4 = 6$ w
2. $2 + 4 = 1$ f

Manchmal kennen wir den Wahrheitswert einer Aussage nicht: Riemannsche Vermutung oder auch die Vermutung, dass jede natürliche Zahl größer als 2 die Summe zweier Primzahlen ist (Goldbachsche Vermutung). Obwohl wir den Wahrheitswert nicht wissen, wissen wir aber, dass diese Aussage entweder wahr oder falsch ist. Weil wir dazu nach heutigem Stand nicht mehr sagen können, nennen wir das eine *Vermutung*.

Beispiel 1.3.2

Nicht jede *umgangssprachliche* Aussage ist eine mathematische Aussage, die Folgenden sind keine mathematischen Aussagen sondern Meinungsäußerungen.

1. Das Wetter ist schön.
2. Die Vorlesung ist super.

Wir kommen in Grenzbereiche wenn wir Aussagen wie *Die Decke ist blau* oder $a^2+b^2 = c^2$ betrachten, hier fehlen uns schlicht Informationen, über welche Decke wird eine Aussage getroffen, was sind a, b, c? Insbesondere letzteres ist sicherlich nicht immer falsch und nicht immer richtig, es kommt auf die Definition von a, b, c an.

Beispiel 1.3.3

Wichtig ist, dass wir Aussagen betrachten, die Folgenden sind nicht mal Aussagen im umgangssprachlichen Sinne

1. Rot.
2. Ist die Tür auf oder zu?
3. $4 + 7$.

Es sei A eine mathematische Aussage, dann hat diese einen eindeutigen Wahrheitswert wahr oder falsch. Wir nutzen diese Eindeutigkeit und die binäre Logik um eine neue Aussage zu konstruieren:

Definition 1.3.4

Es sei A eine Aussage, dann ist die **Negation** von A, geschrieben $\neg A$, die Aussage deren Wahrheitswerte sich aus der folgenden Wahrheitstafel ergeben:

A	$\neg A$
w	f
f	w

Beispiel 1.3.5

Hierbei sprechen wir von der Verneinung als dem mathematischen Gegenteil. "Das Glas ist leer" wird in der Verneinung zu "Das Glas ist nicht leer" und nicht zu "Das Glas ist voll"!

Wir kommen zur zweiten Eigenschaft von Aussagen. Wir können aus gegebenen Aussagen neue Aussagen zusammensetzen und wichtig hierbei ist, dass der Wahrheitswert dieser neuen Aussagen schon durch die Wahrheitswerte der gegebenen Aussagen festgelegt ist.
Es seien A und B zwei Aussagen, wir wollen überlegen welche Aussagen wir daraus zusammensetzen können. A und B haben je zwei mögliche Wahrheitswerte, das bedeutet

wir haben insgesamt 4 Fälle:

A	B
w	w
w	f
f	w
f	f

Eine aus A und B zusammengesetzte Aussage C muss für jeden dieser Fälle einen Wahrheitswert haben:

A	B	C
w	w	ϵ_1
w	f	ϵ_2
f	w	ϵ_3
f	f	ϵ_4

Wir haben also für jedes ϵ_i die beiden Möglichkeiten „f“ oder „w“. Das liefert uns 16 Aussagen, die wir aus A und B zusammensetzen können.
Wir gucken uns hierzu ein paar Beispiele an:

Definition + Beispiele 1.3.6

Wir gucken uns hierzu ein paar Beispiele an, wir müssen dafür nur die Wahrheitswerte für jeden Fall spezifizieren, also für jedes ϵ_i sagen, ob es „f“ oder „w“ ist:

1.

A	B	C
w	w	w
w	f	f
f	w	f
f	f	f

Die Aussage C ist also genau dann wahr, wenn A UND B wahr sind. Wir nennen C auch die **Konjunktion** von A und B, und schreiben dafür kurz $A \wedge B$.

2.

A	B	C
w	w	w
w	f	w
f	w	w
f	f	f

Die Aussage C ist also genau dann wahr, wenn A wahr ist oder B wahr ist oder beide wahr sind. Wir nennen C auch die **Disjunktion** von A und B, und schreiben dafür kurz $A \vee B$. **Achtung**: Hierbei ist nicht das umgangssprachliche *entweder oder* gemeint. Beispiel: *Jede natürliche Zahl ist ungerade oder größer als* 2. Die Aussage ist richtig und für ungerade Zahlen welche größer als 1 sind, sind beide Teilaussagen richtig. Ein *entweder oder* wäre hier also falsch.

3.

A	B	C
w	w	w
w	f	f
f	w	w
f	f	w

Die Aussage C ist also genau dann wahr, wenn A falsch ist oder wenn beide Aussagen wahr. Wir nennen C auch die **Implikation**: $A \Rightarrow B$ und sagen dazu A impliziert B oder *aus* A *folgt* B. Diese Aussage ist eine der nützlichsten und stärksten in der Mathematik, wir folgern aus einer gegebenen Aussage A eine neue Aussage B.
Umgangssprachlich würden wir hierbei sagen, dass wir aus einer falschen Aussage alles folgern können.

4.

A	B	C
w	w	w
w	f	f
f	w	f
f	f	w

Die Aussage C ist also genau dann richtig, wenn die Aussagen A und B immer die gleichen Wahrheitswerte haben. Wir nennen C auch die **Äquivalenz**: A *ist äquivalent zu* B und schreiben dafür $A \Leftrightarrow B$. In der Schreibweise sind zwei Implikationen enthalten, $A \Rightarrow B$ und $B \Rightarrow A$, das ist konsistent mit der Aussagenlogik, denn wenn diese beiden Aussagen wahr sind, dann ist auch $A \Leftrightarrow B$ wahr und umgekehrt.

Wir haben hier nur vier der möglichen 16 Beispiele notiert, diese 4 werden uns immer wieder begegnen.

Beispiel 1.3.7

1. A = "Ich habe die Übungsaufgaben rechtzeitig abgegeben", $\neg A$ = "Ich habe die Übungsaufgaben nicht rechtzeitig abgegeben". Achtung, die Umgangssprachliche Verneinung ist nicht immer auch die logische Verneinung, z.B. ist die Verneinung von A = "a ist kleiner als b" eben nicht die Aussage B = "a ist größer als b" sondern die Aussage $\neg A$ ="a ist größer oder gleich b".

2. Es seien zwei Aussagen gegeben, A =" Sie müssen einen Führerschein besitzen " und B = " Sie müssen über 25 Jahre alt sein". Die Konjunktion ist dann die Aussage $A \wedge B$ = " Sie müssen einen Führerschein besitzen und über 25 Jahre alt sein".
Nur eine der beiden Bedingungen zu erfüllen reicht nicht, um den Mietwagen im Urlaub zu bekommen.

3. Die Disjunktion ist nicht das umgangssprachliche *entweder oder*, die Aussage A = "Eintritt erst ab 18 Jahren" oder B =

"Eintritt in Begleitung der Eltern" würden in der Disjunktion bedeuten, dass mindestens eine der beiden Bedingungen erfüllt sein müssen, aber wenn Sie 18 sind UND in Begleitung Ihrer Eltern erscheinen, dann dürfen Sie auch eintreten. Das Umgangssprachliche *oder* begegnet uns bei Aussagen wie "*Gutschein für eine Freifahrt oder Rückerstattung der Kosten*", hier ist das ausschließende oder gemeint.

4. Wir betrachten die beiden Aussagen $A =$ "In der Mensa ist Veggie-Day", $B =$ "In der Mensa ist Ihr Professor". Ihr Professor kündigt an, wenn Veggie-Day ist, dann ist er in der Mensa. Was können wir dann für die Implikation $A \Rightarrow B$ sagen? Wenn Veggie-Day ist und Ihr Professor ist ehrlich, dann ist er in der Mensa und $A \Rightarrow B$ ist richtig. Wenn er stattdessen gerade irgendwo ein Schnitzel isst, dann ist $A \Rightarrow B$ falsch. Interessanter wird es für den Fall, wenn A falsch ist, also kein Veggie-Day ist. Ihr Professor hat sich nur für den Fall festgelegt des Veggie-Days festgelegt, an allen anderen Tagen kann er machen was er möchte, ohne dass er eine Falschaussage gemacht hat, die Implikation $A \Rightarrow B$ ist also in diesen Fällen immer richtig.

5. Die Aussagen $A =$ "Die Mannschaft X wird deutscher Meister im Herrenfussball" und $B =$ "Die Mannschaft X ist der FC Bayern München" sind (leider) äquivalent.

Es gibt einige sehr nützliche Äquivalenzen zwischen Aussagen, als Beispiel hier:

Proposition 1.3.8

Es seien A und B Aussagen, dann ist

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A) \Leftrightarrow ((\neg A) \vee B)$$

Beweis. Wir beweisen das durch eine Wahrheitstafel:

A	$\neg A$	B	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	$(\neg A) \vee B$
w	f	w	f	w	w	w
w	f	f	w	f	f	f
f	w	w	f	w	w	w
f	w	f	w	w	w	w

□

Bemerkung 1.3.9

Proposition 1.3.8 liefert uns schon einen Hinweis darauf, dass man jede der 16 Möglichkeiten, insbesondere also die Implikation und Äquivalenz durch Kombinationen von $\neg, \wedge, \vee$ ausdrücken kann. Versuchen Sie sich selber einmal daran.

Wir können diese Äquivalenz nutzen, um $A \Rightarrow B$ zu beweisen.

Beispiel 1.3.10

Sei A die Aussage "*Es regnet*", B die Aussage "*Die Erde wird nass*". Dann gilt $A \Rightarrow B$. Genauso können wir aber auch schließen (**Kontraposition**), wenn die Erde nicht nass ist, also regnet es nicht.

In den Übungsaufgaben werden Sie noch viele weitere Aussagen beweisen.

1.4 Mengen

Hier ist eine ursprüngliche, aber problematische Definition:

Definition 1.4.1

Eine **Menge** ist eine Zusammenfassung von bestimmten und wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

Beispiel 1.4.2

1. Die Studierenden an der RWTH Aachen University.
2. Die Studierenden an der RWTH Aachen University, die sich nicht in Aachen befinden.
3. Die Studierenden an der RWTH Aachen University, die sich nicht in Aachen befinden, aber schon mal in Aachen waren.
4. Was ist mit der Menge, die alle Mengen enthält, die sich nicht selbst enthalten? Dies sorgt für ein Problem in unserer Definition. Wir wollen das Problem hier aber ignorieren und auf eine Vorlesung über *Logik* verweisen.

Definition 1.4.3

Es sei M eine Menge. Die Objekte von M nennen wir **Elemente**. Für ein Element x der Menge M schreiben wir $x \in M$. Falls x kein Element von M ist, dann schreiben wir $x \notin M$.

Bemerkung 1.4.4: E

seien M und N Mengen, Dann gilt

$$M = N \Leftrightarrow \text{Jedes Element von } M \text{ ist ein Element von } N \text{ und umgekehrt.}$$

Wie können wir Mengen beschreiben?

1. Man kann Mengen durch Aufzählung beschreiben: $\{a, b, c\} = \{b, c, a\} = \{a, b, b, a, c\}$. Wichtig hierbei: Jedes Element ist nur einmal in einer Menge.
2. Man kann Elemente in einer Menge beschreiben: Die Menge der ganzen Zahlen ($\mathbb{Z}$), die Menge der rationalen Zahlen ($\mathbb{Q}$), usw.
3. Man kann Elemente in einer Menge durch Eigenschaften beschreiben: M besteht aus den Elemente, die eine bestimmte Eigenschaften erfüllen. Zum Beispiel $M = \{x \in \mathbb{Z} \mid x \text{ ist gerade } \}$, die Menge der geraden Zahlen.

Um mit Mengen arbeiten zu können, führen wir einige Begriffe ein:

Definition 1.4.5

Es seien M und N Mengen.

1. Die **leere Menge** , geschrieben $\emptyset$, ist die Menge, die keine Elemente enthält.
2. N ist eine **Teilmenge** von M, geschrieben $N \subseteq M$, falls für alle $x \in N$ auch $x \in M$ gilt.
3. Der **Durchschnitt** von N und M, geschrieben $N \cap M$, ist die Menge aller Elemente, die sowohl in N als auch in M liegen. Also:
$$N \cap M = \{x \mid x \in N \text{ und } x \in M\}.$$
4. Die **Vereinigung** von N und M, geschrieben $N \cup M$, ist die Menge aller Elemente, die in N oder M liegen. Also:
$$N \cup M = \{x \mid x \in N \text{ oder } x \in M\}.$$
5. Die **Differenzmenge** von N und M, geschrieben $N \setminus M$, ist die Menge aller Elemente, die in N liegen, aber nicht in M. Also:
$$N \setminus M = \{x \mid x \in N \text{ und } x \notin M\}.$$
Achtung: Die Reihenfolge der Mengen ist hierbei wichtig!
6. Das **Kartesische Produkt** von N und M, geschrieben $N \times M$, ist die Menge aller geordneten Paare (n, m), wobei n ein Element aus N und m ein Element aus M ist. Also:
$$N \times M = \{(n, m) \mid n \in N, m \in M\}.$$
7. Es sei $A \subseteq M$ eine Teilmenge, dann ist das **Komplement von A in M** definiert als $\overline{A} := \{x \in M \mid x \notin A\}$.
8. Die **Potenzmenge** einer Menge N, geschrieben $\mathrm{Pot}(N)$, ist die Menge aller Teilmengen von N, also:
$$\mathrm{Pot}(N) = \{U \mid U \subseteq N\}.$$

Beispiel 1.4.6

Es seien $M = \{0, 1, 2\}$ und $N = \{2, 3, 4\}$, dann ist

- $\{0, 2\} \subseteq M$ eine Teilmenge.
- $M \cap N = \{2\}$.
- $M \cup N = \{0, 1, 2, 3, 4\}$.
- $M \setminus N = \{0, 1\}$.

- $M \times N = \{(0,2),(0,3),(0,4),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4)\}$.
- Falls $A = \{0,2\} \subset M$, dann ist $\overline{A} = \{1\}$.
- $\mathrm{Pot}(M) = \{\emptyset,\{0\},\{1\},\{2\},\{0,1\},\{0,2\},\{1,2\},\{0,1,2\}\}$.

Proposition 1.4.7

Es seien $A, B \subseteq M$ Teilmengen, dann gelten

1. $\overline{\overline{A}} = A$.
2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
3. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Beweis. Wir erinnern uns für $A \subseteq M$ gilt:

$$\overline{A} = M \setminus A = \{x \in M \mid x \notin A\}$$

1. Es ist
$$\overline{\overline{A}} = M \setminus \overline{A} = M \setminus \{M \setminus A\},$$
anders ausgedrückt
$$\overline{\overline{A}} = \{x \in M \mid x \notin M \setminus A\} = \{x \in M \mid x \in A\} = A.$$

2.
$$\begin{aligned} \overline{A \cap B} &= \{x \in M \mid x \notin A \cap B\} \\ &= \{x \in M \mid x \notin A \vee x \notin B\} \\ &= \{x \in M \mid x \notin A\} \cup \{x \in M \mid x \notin B\} \\ &= \overline{A} \cup \overline{B} \end{aligned}$$
Wir haben hier genutzt, dass $x \notin A \cap B$ genau dann gilt, wenn $x \notin A$ oder $x \notin B$. Wir können uns das durch eine Wahrheitstafel klarmachen

$x \notin A$	$x \notin B$	$x \notin A \cap B$	$x \notin A \vee x \notin B$
w	w	w	w
w	f	w	w
f	w	w	w
f	f	f	f

3. Analog erhalten wir
$$\begin{aligned} \overline{A \cup B} &= \{x \in M \mid x \notin A \cup B\} \\ &= \{x \in M \mid x \notin A \wedge x \notin B\} \\ &= \{x \in M \mid x \notin A\} \cap \{x \in M \mid x \notin B\} \\ &= \overline{A} \cap \overline{B} \end{aligned}$$

□

Es gibt noch viele weitere "Rechenregeln" für den Schnitt, die Vereinigung oder das Komplement, beispielsweise die de Morganschen Gesetze. Einiges werden Sie in Übungsaufgaben sehen.

Definition 1.4.8

Eine Menge M heißt **endlich**, wenn M nur endlich viele Elemente besitzt, dann schreiben wir

$$|M| = \text{Anzahl der Elemente von } M.$$

Diese Größe nennen wir die **Kardinalität** der Menge M. Falls M nicht endlich ist, so schreiben wir $|M| = \infty$.

Beispiel 1.4.9

1. $|\{a, b, c\}| = 3$.
2. $|\{a, a, b, c, c\}| = 3$.
3. $|\mathbb{Z}| = \infty$.
4. $|\emptyset| = 0$.

Proposition 1.4.10

Es sei M eine endliche Menge, dann gilt

$$|\mathrm{Pot}(M)| = 2^{|M|}.$$

Ausdrücke um Mengen zu beschreiben erfordern eine neue Notation:

Definition 1.4.11

Es sei M eine Menge und $A(x)$ für jedes $x \in M$ eine Aussage.

1. "$\forall\, x \in M : A(x)$" bedeutet " *für alle x aus M gilt die Aussage $A(x)$*".
2. "$\exists\, x \in M : A(x)$" bedeutet " *es existiert ein x in M, für welches $A(x)$ gilt*".

Beispiel 1.4.12

1. $\forall x \in \mathbb{Z} : 2x$ ist gerade .
2. $\forall x \in \mathbb{Z} : \exists\, y \in \mathbb{Z}$ mit $y > x$.

1.5 Beweisprinzipien

In der Mathematik beweisen wir Aussagen; ein mögliches Beweisprinzip haben wir schon gesehen (Kontraposition). Wir listen hier noch einige weitere Prinzipien und erläutern die anhand von Beispielen:

1. **Direkter Beweis**. Diesen verwendet man vor allem für Aussagen der Form $A \Rightarrow B$. Hier nehmen wir an, dass A wahr ist und folgern daraus die Aussage B.
2. **Indirekter Beweis**. Eine Variante ist die Kontraposition: statt $A \Rightarrow B$ zeigt man $\neg B \Rightarrow \neg A$. Eine weitere Variante ist der Widerspruchsbeweis. Wir wollen

dabei eine Aussage A zeigen und folgern aus der Annahme $\neg A$ einen Widerspruch. Das heißt, wir folgern $\neg A \Rightarrow B$ für eine Aussage B, von der wir wissen, dass $\neg B$ wahr ist.

3. **Vollständige Induktion**: Das scheint auf den ersten Blick eine komplizierte Technik zu sein, sie ist aber sehr stark. Meistens geht es um Aussagen der Form $\forall\, x \in \mathbb{N} : A(x)$. Wir zeigen dann die Aussage $A(1)$ und für ein beliebiges, aber festes $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$.

Ein Beispiel für einen direkten Beweis:

Proposition 1.5.1

Es sei $n \in \mathbb{N}$ und

$$A(n) : n \text{ ist ungerade}$$

und

$$B(n) : n^2 \text{ ist ungerade .}$$

Dann gilt: $A(n) \Rightarrow B(n)$.

Beweis. Es sei n ungerade, dann existiert ein $k \in \mathbb{N}$ mit $n = 2k + 1$. Damit ist $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, also ebenfalls ungerade. □

Ein Beispiel für einen Beweis durch Kontraposition:

Proposition 1.5.2

Es sei $n \in \mathbb{N}$ und

$$A(n) : n^2 \text{ ist gerade}$$

und

$$B(n) : n \text{ ist gerade .}$$

Dann gilt: $A(n) \Rightarrow B(n)$.

Beweis. Wir zeigen $\neg B(n) \Rightarrow \neg A(n)$. Aber das ist genau die Aussage von Proposition 1.5.1 und damit haben wir die zu zeigende Aussage durch Kontraposition bewiesen. □

Ein Beispiel für einen Widerspruchsbeweis:

Proposition 1.5.3

Es gilt die Aussage $A = \sqrt{2} \notin \mathbb{Q}$.

Beweis. Angenommen $\neg A$ wäre richtig, also $\sqrt{2} \in \mathbb{Q}$. Dann existieren $p, q \in \mathbb{Z} \setminus \{0\}$ mit

$$\sqrt{2} = \frac{p}{q}$$

und wir können annehmen, dass nicht p UND q durch 2 teilbar sind (ansonsten kürzen wir). Dann gilt aber

$$(\sqrt{2})^2 = 2 = (\frac{p}{q})^2 = \frac{p^2}{q^2}.$$

Damit ist $q^2 * 2 = p^2$, also 2 ein Teiler von p^2, also ein Teiler von p. Dann ist aber $2^2 = 4$ ein Teiler von p^2. Und damit 4 ein Teiler von $q^2 * 2$, also 2 ein Teiler von q^2. Mit der gleichen Überlegung wie vorher ist dann 2 ein Teiler von q. Das ist aber ein Widerspruch, denn nach Voraussetzung teilt 2 nicht p UND q. □

Wir wollen noch ein Beispiel für einen Beweis durch vollständige Induktion geben. Dafür möchten wir das Prinzip verstehen. Dafür überlegen wir uns folgende Eigenschaft der natürlichen Zahlen:

$$\text{Sei } A \subset \mathbb{N} \text{ mit } 1 \in A \text{ und } \forall\, n \in A : n+1 \in A. \text{ Dann ist } A = \mathbb{N}.$$

Das liefert uns das gewünschte Induktionsprinzip:

Induktionsanfang:	Zeige $A(1)$ ist wahr.
Induktionsschritt:	Annahme: $A(n)$ ist wahr. Zeige: $A(n+1)$ ist wahr.

Dann gilt nach der obigen Überlegung die Aussage für alle $n \in A$, also für alle $n \in \mathbb{N}$.

Proposition 1.5.4

Für alle $n \in \mathbb{N}$ gilt die Aussage

$$A(n) : \sum_{i=1}^{n} i = \frac{1}{2} n(n+1).$$

Beweis. Wir beweisen das per Induktion:

1. Induktionsanfang: Wir beweisen die Aussage für $n = 1$:

$$\sum_{i=1}^{1} i = 1 = \frac{1}{2} 1 * 2.$$

2. Induktionsvoraussetzung: Angenommen für ein beliebiges, aber festes n gelte

$$\sum_{i=1}^{n} i = \frac{1}{2} n(n+1)$$

3. Induktionsschritt:

$$\sum_{i=1}^{n+1} i = (n+1) + \sum_{i=1}^{n} i =_{IV} n+1+\frac{1}{2} n(n+1) = \frac{1}{2}(2(n+1)+n(n+1)) = \frac{1}{2}((n+1)(n+2)).$$

□

Wir erwarten von Ihnen, dass jeder Ihrer Induktionsbeweise diese Struktur hat:

- IA: Induktionsanfang
- IV: Voraussetzung, die Aussage gelte für einen beliebigen, aber festen Index.
- IS: Schritt.

Ein weiteres Beispiel:

Proposition 1.5.5

Es sei $1 \neq q \in \mathbb{R}$. Dann gilt für alle $n \in \mathbb{N}$ die Aussage

$$A(n) : \sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{q - 1}.$$

Beweis. Wir beweisen das per Induktion:

1. IA: Wir beweisen die Aussage für $n = 1$:

$$\sum_{i=0}^{1} q^i = q^0 + q^1 = 1 + q = \frac{(q+1)(q-1)}{(q-1)} = \frac{q^2 - 1}{q - 1}.$$

2. IV: Angenommen für ein beliebiges, aber festes n gelte

$$\sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{q - 1}.$$

3. IS:

$$\begin{array}{lcl} \sum_{i=0}^{n+1} q^i & = & q^{n+1} + \sum_{i=0}^{n} q^i \\ \text{nach IV} & = & q^{n+1} + \frac{q^{n+1}-1}{q-1} \\ & = & \frac{(q^{n+1})(q-1)+q^{n+1}-1}{(q-1)} \\ & = & \frac{q^{n+2}-q^{n+1}+q^{n+1}-1}{(q-1)} \\ & = & \frac{q^{n+2}-1}{q-1}. \end{array}$$

□

1.6 Abbildungen

Definition 1.6.1

Es seien M, N Mengen. Eine **Abbildung** ist eine *Vorschrift* (bspw. eine Formel) die jedem $m \in M$ genau ein $n \in N$ zuordnet, als Notation:

$$f : M \longrightarrow N \ , \ m \mapsto f(m) = n.$$

Wir nennen hierbei M den **Definitionsbereich** und N den **Wertebereich** der Abbildung.

Beispiel 1.6.2

Die Abbildungsvorschrift kann durch verschiedene Formen beschrieben werden, also Funktionsgleichung ($f(x) = x^2$) oder als Zuordnungsvorschrift ($x \mapsto x^2$), als Wertetabelle (für endliche Mengen M), als Relation (wie wir in Abschnitt 1.7 sehen werden), oder durch Herleitung aus anderen Abbildungen (Komposition, Inverse etc.)

1. $f : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$, $x \mapsto x^2$ ist eine Abbildung, der Wertebereich ist hier $\mathbb{R}_{\geq 0}$,

der Definitionsbereich $\mathbb{R}$.

2. $M = \{a, b, c\}$ (Definitionsbereich), $N = \{0, 1, 2\}$ (Wertebereich):

f	a	b	c
$f(x)$	1	2	2

   . Wir sehen, dass nicht alle Elemente aus der Wertemenge aus als Funktionswert auftauchen müssen.

3. 2 Pfeildiagramme malen.

4. Es sei M eine beliebige Menge, dann ist $\mathrm{id} : M \longrightarrow M$, $x \mapsto x$ immer eine Abbildung. Hier sind Definitions- und Wertebereich gleich. Diese Abbildung nennen wir auch die **Identität**

Definition 1.6.3

Zwei Abbildungen $f : M \longrightarrow N$ und $g : P \longrightarrow R$ heißen **gleich**, falls $M = P$, $N = R$ und $f(m) = g(m)$ für jedes $m \in M$.

Definition 1.6.4

Es sei $f : M \longrightarrow N$ eine Abbildung.

1. Die Menge $\mathrm{Im}\, f := \{y \in N \mid \exists x \in M : f(x) = y\}$ nennen wir das **Bild der Abbildung**.

2. Es sei $P \subseteq N$, dann nennen wir die Menge $f^{-1}(P) := \{x \in M \mid f(x) \in P\}$ das **Urbild von P unter f**.

3. Zu einem $y \in N$ nennen wir das Urbild $f^{-1}(y) \subset M$ auch die **Faser** von y unter f.

Beispiel 1.6.5

1. $f : \mathbb{R} \longrightarrow R$, $x \mapsto x^2$. Dann ist $\mathrm{Im}\, f = \mathbb{R}_{\geq 0}$ und $f^{-1}(y) = \{x \in \mathbb{R} \mid x^2 = y\}$, also beispielsweise die Fasern $f^{-1}(0) = \{0\}$, $f^{-1}(2) = \{\pm\sqrt{2}\}$ und das Urbild $f^{-1}(\mathbb{R}_{<0}) = \emptyset$. Wir sehen, dass das Urbild auch die leere Menge sein kann

2. Es sei $N = \{a, b\}$ und $M = \{1, 2, 3\}$ mit $f(a) = 1$, $f(b) = 1$, dann ist $f^{-1}(1) = \{a, b\}$ und $f^{-1}(\{1, 2\}) = \{a, b\}$. Es gilt immer $f^{-1}(M) = N$.

3. Es sei $f : M \longrightarrow N$ eine Abbildung, dann ist das Urbild für eine Teilmenge $P \subset N$ eine Teilmenge von M, insbesondere kann das Urbild auch eine leere Menge sein. Die **Faserabbildung** ist definiert als

$$f^{-1} : N \longrightarrow \mathrm{Pot}(M)\ ,\ y \mapsto f^{-1}(y).$$

   Nach der Vorüberlegung ist klar, dass der Wertebereich nicht M ist sondern die Potenzmenge von M.

Definition 1.6.6

Es sei $f : M \longrightarrow N$ eine Abbildung und $P \subseteq M$ eine Teilmenge. Dann ist die **Einschränkung von f auf P** definiert als

$$f_{|P} : P \longrightarrow N; \; ; p \mapsto f(p).$$

Beispiel 1.6.7

1. Wir betrachten $f : \mathbb{R} \longrightarrow \mathbb{R}$ mit $f(x) = x^2$, dann erhalten wir $f_{|\mathbb{R}_{\geq 0}}$ als Einschränkung. In diesem Fall besteht die Faser zu jedem Element aus höchstens einem Element.

Bemerkung 1.6.8: W

r können auch $f : M \longrightarrow N$ **auf das Bild einschränken**, damit meinen wir die *induzierte* Abbildung

$$f : M \longrightarrow \operatorname{Im} f; , \; m \mapsto f(m).$$

Wir haben hier den Wertebereich auf die Werte eingeschränkt, die im Bild der Abbildung auch tatsächlich auftauchen. Dadurch ist die Faser von jedem Element nicht leer.

Beispiel 1.6.9

Wir greifen nochmal das obige Beispiel auf und betrachten $f : \mathbb{R} \longrightarrow \mathbb{R}$ mit $f(x) = x^2$. Dann gilt für $f_{|\mathbb{R}_{\leq 0}} \longrightarrow \mathbb{R}_{\geq 0}$ sogar, dass jede Faser aus genau einem Element besteht.

Proposition 1.6.10

Es sei $f : M \longrightarrow N$ eine Abbildung, $M_1, M_2 \subseteq M$, $N_1, N_2 \subseteq N$ Teilmengen. Dann gelten:

1. $f(M_1 \cup M_2) = f(M_1) \cup f(M_2)$.
2. $f(M_1 \cap M_2) \subseteq f(M_1) \cap f(M_2)$.
3. $f^{-1}(N_1 \cup N_2) = f^{-1}(N_1) \cup f^{-1}(N_2)$.
4. $f^{-1}(N_1 \cap N_2) = f^{-1}(N_1) \cap f^{-1}(N_2)$.
5. $f(f^{-1}(N_1)) = N_1 \cap f(M) \subseteq N_1$.
6. $M_1 \subseteq f^{-1}(f(M_1))$.
7. $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$.

Beweis. Das wird teilweise in den Übungen bewiesen. □

Definition 1.6.11

Es sei $f : M \longrightarrow N$ eine Abbildung.

1. f heißt **injektiv**, falls für alle $x_1, x_2 \in M$ gilt: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
2. f heißt **surjektiv**, falls gilt: $\forall\, y \in N\ \exists x \in M$ mit $f(x) = y$.
3. f heißt **bijektiv**, falls f injektiv und surjektiv ist.

Beispiel 1.6.12

1. $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^2$ ist weder surjektiv noch injektiv.
2. $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^3$ ist bijektiv.
3. Die Zuordnung: RWTH-Studierende $\rightarrow$ sechsstellige Zahl ist injektiv (Matrikelnummer). Grundsätzlich sollte jeder Unique Identifier eine injektive Zuordnung sein.
4. FC-Fans $\rightarrow$ Dauerkarten ist eine surjektive Abbildung.
5. Es sei $f : M \longrightarrow N$ eine Abbildung, dann ist die Einschränkung auf das Bild $f : M \longrightarrow \operatorname{Im} f$ immer eine surjektive Abbildung. deutlich schwieriger ist es aus einer Abbildung eine injektive Abbildung zu konstruieren, dazu kommen wir später.

Definition 1.6.13

Es seien N, M Mengen, die Menge der Abbildungen von M nach N bezeichnen wir mit N^M, also

$$N^M = \{f : M \longrightarrow N\}$$

Beispiel 1.6.14

1. Es sei $M = \{a\}$ und $N = \{1, 2, 3\}$, wir sehen schnell, dass die Zuordnungen $a \mapsto 1, a \mapsto 2, a \mapsto 3$ alle möglichen Abbildungen beschreiben, also

$$\{1, 2, 3\}^{\{a\}} = \{a \mapsto 1, a \mapsto 2, a \mapsto 3\}$$

2. Es sei M beliebig und N habe nur ein Element $\{a\}$, dann gibt es genau eine Abbildung $m \mapsto a$ für jedes $m \in M$.
3. Es sei N beliebig und M habe nur ein Element $\{m\}$, dann ist bilden die Zuordnung $m \mapsto a$ für beliebiges $a \in A$ alle möglichen Abbildungen, die Anzahl ist also durch die Anzahl der Elemente in N gegeben.

Proposition 1.6.15

Es seien N, M Mengen, dann ist

$$|N^M| = |N|^{|M|}$$

Beweis. Es seien N und M endlich Mengen.Die Elemente aus N haben $|M|$ mögliche Bilder, das liefert also $|N|^{|M|}$ mögliche Abbildungen und es ist leicht zu sehen, dass diese Abbildungen paarweise verschieden sind.
Für unendliche Mengen folgt die Aussage sofort. Übung. □

Wir kommen zu dem versprochenen Beweis von Proposition 1.4.10:

Beweis. Wir konstruieren eine Bijektion

$$\Psi : \mathrm{Pot}(M) \longrightarrow \{0,1\}^M \ , \ N \mapsto \chi_N$$

wobei $\chi_N : M \longrightarrow \{0,1\}, x \mapsto \begin{cases} 0 & x \notin N \\ 1 & x \in N \end{cases}$.
Es ist leicht zu sehen, dass Ψ eine Abbildung ist. Angenommen $\Psi(N_1) = \Psi(N_2)$, dann gilt für alle $m \in M$

$$\chi_{N_1}(m) = \chi_{N_2}(m)$$

aber dann ist $m \in N_1 \Leftrightarrow m \in N_2$, also $N_1 = N_2$. Die Abbildung ist also injektiv.
Sei $\phi \in \{0,1\}^M$, dann definieren wir

$$N = \{x \in M \mid \phi(x) = 1\} \subset M$$

Dann gilt $\chi_N(m) = \phi(m)$ für alle $m \in M$, also $\phi = \chi_N$. Damit ist Ψ surjektiv und damit bijektiv. □

Definition 1.6.16

Es seien $f : M \longrightarrow N$ und $g : N \longrightarrow P$ Abbildungen, dann ist die **Komposition der Abbildungen** $g \circ f$ definiert als

$$(g \circ f) : M \longrightarrow P \ , \ m \mapsto g(f(m)).$$

Beispiel 1.6.17

1. $M = \{a, b, c\}$, $N = \{0, 1, 2\}$, $P = \{w, x, y, z\}$ (Wertebereich):

f	a	b	c
$f(x)$	1	2	2

,

g	0	1	2
$g(x)$	z	y	y

.

   Dann ist die Komposition

$g \circ f$	a	b	c
$f(x)$	y	y	y

.

   Wir sehen sofort, dass die Komposition $f \circ g$ nicht definiert ist.

2. $f : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$, $f(x) = x^2$, $g : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}$, $g(x) = \sqrt{x}$. Dann ist $f \circ g = \mathrm{id}_{\mathbb{R}_{\geq 0}}$, da $(\sqrt{x})^2 = x$ für alle $x \geq 0$. Überlegen Sie sich, ob $g \circ f$ ebenfalls die Identität auf $\mathbb{R}$ ist.

Bemerkung 1.6.18: T

tsächlich muss g nur auf dem Bild von f in N (und nicht auf ganz N) definiert sein, damit wir die Komposition definieren können.

Proposition 1.6.19

Es seien Es seien $f : M \longrightarrow N, g : N \longrightarrow P$ und $h : P \longrightarrow R$ Abbildungen, dann gilt

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Die Komposition von Abbildungen ist also assoziativ.

Beweis. Es sei $m \in M$, dann ist

$$(h \circ (g \circ f))(m) = h((g \circ f)(m) = h(g \circ f(m)) = h(g(f(m)))$$

und

$$((h \circ g) \circ f)(m) = (h \circ g)f(m) = h(g(f(m))).$$

□

Definition 1.6.20

Es seien $f : M \longrightarrow N$ und $g : N \longrightarrow M$ zwei Abbildungen. Falls

$$g \circ f = \mathrm{id}_M$$

dann heißt g ein **Linksinverses zu** f und f ein **Rechtsinverses zu** g. Eine Abbildung heißt **invertierbar**, falls sie ein Rechts- und ein Linksinverses besitzt

Beispiel 1.6.21

1. Wir betrachten die Abbildung: $d : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ mit $d(n) = n - 1$ für $n \geq 1$ und $d(0) = 0$. Dann ist $\iota : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ mit $\iota(n) = n + 1$ ein Rechtsinverses zu d (da $d \circ \iota(n) = n$ aber kein Linksinverses, da $\iota \circ d(0) = 1$. Also auch in dem Fall $N = M$ ist, muss ein **Linksinverses kein Rechtsinverses** sein.

2. Wir betrachten $f : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$ mit $f(x) = x^2$. Dann liefert $g_1 : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}$ mit $g_1(x) = \sqrt{x}$ ein Rechtsinverses zu f, aber $g_2 : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}$ mit $g_2(x) = -\sqrt{x}$ ist ein weiteres Rechtsinverses zu f. Wir sehen also ein Rechtsinverses (bzw. Linksinverses) muss **nicht eindeutig** sein.

3. Ein Rechtsinverses nennen wir auch einen **Schnitt** zu f.

Proposition 1.6.22

Es sei $f : M \longrightarrow N$ eine Abbildung, dann gilt:

1. f ist injektiv, genau dann wenn f ein Linksinverses besitzt.

2. f ist surjektiv, genau dann wenn f ein Rechtsinverses besitzt.

3. f ist bijektiv, genau dann wenn f invertierbar ist.

Beweis. Es sei $f : M \longrightarrow N$.

1. Es sei M nicht leer und $m \in M$ ein beliebiges Element. Es sei f injektiv, dann ist für jedes $y \in N$: $|f^{-1}(y)| \leq 1$. Dann definieren wir die Abbildung $g : N \longrightarrow M$ durch
$$y \mapsto \begin{cases} m & \text{falls } f^{-1}(y) = \emptyset \\ f^{-1}(y) & \text{sonst} \end{cases}$$
Dann gilt $g \circ f(x) = g(f(x)) = f^{-1}(f(x)) = x$, da per Konstruktion $f^{-1}(f(x))$ nicht die leere Menge ist. Damit ist g ein Linksinverses zu f. Umgekehrt sei g ein Linksinverses zu f und $x_1, x_2 \in M$ mit $f(x_1) = f(x_2)$. Dann gilt, da g ein Linksinverses ist: $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, also $x_1 = x_2$ und f ist somit injektiv.

2. Es sei f surjektiv, wir konstruieren einen Schnitt zu f. Sei dafür $y \in N$, dann ist per Annahme $f^{-1}(y) \neq \emptyset$. Wir wählen in $f^{-1}(y)$ ein festes Element aus, das bezeichnen wir mit x_y. Dann definiert die Zuordnung $y \mapsto x_y$ eine Abbildung $g : N \longrightarrow M$. Die Abbildung ist wohldefiniert, da Urbilder von verschiedenen Elemente disjunkt sind. Es gilt darüber hinaus $f(g(y)) = f(x_y) = y$, da x_y im Urbild von y liegt. Damit ist g ein Schnitt zu f. Sei umgekehrt g ein Rechtsinverses (oder ein Schnitt) zu f und $y \in N$. Dann ist $y = f(g(y))$ und damit $y \in \operatorname{Im} f$, also f ist surjektiv.

3. Es sei f bijektiv, also injektiv und surjektiv. Damit ist aber für jedes $y \in N$, $|f^{-1}(y)| =$, also liefert die Zuordnung $y \mapsto f^{-1}(y)$ eine Abbildung $g : N \longrightarrow M$ und es gilt $f \circ g = \mathrm{id}_N$ und $g \circ f = \mathrm{id}_M$. Umgekehrt sei f invertierbar und g die inverse Abbildung, dann ist g ein Links- und ein Rechtsinverses, damit ist f injektiv und surjektiv, also bijektiv.

□

1.7 Relationen

Relationen verallgemeinern den Abbildungsbegriff; sie sind einfach Teilmengen des kartesischen Produkts zweier Mengen (bei Abbildungen: Definitions- und Wertebereich). Wir wollen diese etwas eingeschränkter betrachten und nur Relationen auf einer Menge M betrachten, d.h. Teilmengen des kartesischen Produkts $M \times M$.

Definition 1.7.1

Es sei M eine Menge.

1. Eine **Relation** R auf M ist eine Teilmenge von $M \times M$. Wir sagen dann für $(m, n) \in R$: *m steht in Relation zu n*, und schreiben dafür auch $m \sim_R n$ oder auch kurz $m \sim n$.

2. Eine Relation R heißt **reflexiv**, falls $(m, m) \in R$ für alle $m \in M$ gilt.

3. Eine Relation R heißt **symmetrisch**, falls $(n, m) \in R \Leftrightarrow (m, n) \in R$ für alle $m, n \in M$. R heißt **antisymmetrisch**, falls $(n, m), (m, n) \in R \Rightarrow n =$

m für alle $m, n \in M$.

4. Eine Relation R heißt **transitiv**, falls für alle $m, n, p \in M$ gilt:

$$(m, n), (n, p) \in R \Rightarrow (m, p) \in R.$$

5. Eine Relation R heißt **Äquivalenzrelation** falls R reflexiv, symmetrisch und transitiv ist.

6. Eine Relation R heißt **Halbordnung** falls R reflexiv, antisymmetrisch und transitiv ist.

Beispiel 1.7.2

1. Es sei $M = \mathbb{Z}$ und $R = \{(a, b) \in M \times M \mid a < b\}$. Das ist die **kleiner Relation**. R ist nicht reflexiv, da x nicht kleiner als x ist, nicht symmetrisch da $a < b$ nicht $b < a$ folgt, aber transitiv, da $a < b$, $b < c$ auch $a < c$ folgt.

2. Es sei M eine Menge und $R = \{(a, a) \in M \times M\}$, also $a \sim b \Leftrightarrow a = b$. Diese Gleichheitsrelation ist immer eine Äquivalenzrelation. I.A. sind Relation, die durch Gleichheit beschrieben werden, Äquivalenzrelationen, da *Gleichheit* reflexiv, symmetrisch und transitiv ist.

3. Es sei $M = \mathbb{R}^{\mathbb{R}}$, die Menge der Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$ und R sei definiert durch

$$f \sim g \Leftrightarrow \exists\, a \neq b \in \mathbb{R} \text{ mit } f(a) = g(a) \text{ und } f(b) = g(b).$$

   Diese Relation ist offensichtlich reflexiv und symmetrisch, aber nicht transitiv (denken Sie sich ein Gegenbeispiel aus).

4. Es sei M eine Menge, dann definieren wir $R = \{(U_1, U_2) \in \mathrm{Pot}(M)^2 \mid U_1 \subseteq U_2\}$. Wir sehen hier sofort reflexiv, transitiv und antisymmetrisch, denn $U_1 \subseteq U_2$ und $U_2 \subseteq U_1$ impliziert $U_1 = U_2$.

5. Es sei M die Menge aller Griffe in der Boulderhalle. Wir definieren eine Relation R durch $x \sim y \Leftrightarrow x$ ist von y erreichbar . Das ist offensichtlich reflexiv, es ist auch transitiv (bei entsprechender Kondition) aber nicht umbedingt symmetrisch.

6. Es sei M die Menge aller Menschen, welche Eigenschaften hat die Liebe als Relation zwischen zwei Menschen?

Definition 1.7.3

Es sei R eine Äquivalenzrelation auf M.

1. Es sei $m \in M$, dann ist die **Äquivalenzklasse** von m die Menge

$$[m] = \{x \in M \mid xRm\} = \{x \in M \mid mRx\}.$$

2. Ein **Repräsentant** oder **Vertreter** einer Äquivalenzklasse $[m]$ ist ein Element dieser Äquivalenzklasse (also jedes $n \in [m]$ ist ein Repräsentant von

$[m]$).

3. Die Menge aller Äquivalenzklassen der Relation auf M nennen wir den **Quotientenraum** und schreiben dafür M/R.

4. Ein **Repräsentantensystem** oder **Vertretersystem** der Äquivalenzrelation ist eine Teilmenge N von M mit $m \not\sim n$ für $m \neq n \in N$ und für alle $x \in M$ existiert ein $m \in N$ mit $x \sim m$. Anders ausgedrückt:

$$\forall\, x \in M \ : \ \exists!\, m \in N : x \in [m].$$

Bemerkung 1.7.4: D

e Notation $[m]$ für eine Äquivalenzklasse sorgt oft für Missverständnisse. Das m der Notation ist nur ein Repräsentant dieser Klasse. Für jedes $n \in [m]$ gilt $[n] = [m]$.

Beispiel 1.7.5

1. Wir verweisen gerne auf das wunderbare Beispiel aus den Videos: Die Menge sind die Einwohner Aachens, die in Relation zueinander stehen, wenn sie in einem gemeinsamen Haushalt stehen. Dann wäre jedes Mitglied im Haushalt ein Repräsentant und die Menge der Äquivalenzklassen ist die Menge der Haushalte.

2. Es sei $M = \mathbb{Z}$ und zwei Zahlen a, b stehen in Relation zueinander, wenn sie geteilt durch 2 den gleichen Rest ergeben. Das ist offensichtlich reflexiv und symmetrisch, und wir können uns schnell auch die Transitivität überlegen. Es gibt genau zwei Äquivalenzklassen, zu einen die Menge der Zahlen mit Rest 0 und die Menge der Zahlen mit Rest 1, also die Menge der geraden Zahlen und die Menge der ungeraden Zahlen. Ein Vertretersystem wäre dann beispielsweise $\{0, 1\}$ aber auch $\{0, 17\}$ oder $\{-4, 3\}$.

Proposition 1.7.6

Es sei R eine Äquivalenzrelation auf einer Menge M, dann ist die Abbildung

$$v_R : M \longrightarrow M/R\ ,\ m \mapsto [m]$$

surjektiv.

Beweis. Es sei $[m]$ eine Äquivalenzklasse, dann ist $[m]$ eine nichtleere Teilmenge von M, also sei $a \in [m]$. Dann gilt

$$v_R(a) = [a] = [m].$$

Denn es gilt für jeden Repräsentanten a einer Äquivalenzklasse $[m]$, dass $[a] = [m]$. □

Definition 1.7.7

Eine **Partition** einer Menge M ist eine Teilmenge $P \subseteq \mathrm{Pot}(M)$ so, dass gilt

1. $\emptyset \notin P$, also für alle $N \in P$ gilt $N \neq \emptyset$.
2. $\mathrm{M} = \bigcup_{N \in P} N$
3. Für $N_1 \neq N_2 \in P$ gilt $N_1 \cap N_2 = \emptyset$.

Beispiel 1.7.8

Wir betrachten die Menge $M = \{1, 2, 3\}$ und listen alle möglichen Partitionen

1. $\{1\} \cup \{2\} \cup \{3\}$.
2. $\{1, 2\} \cup \{3\}$.
3. $\{1, 3\} \cup \{2\}$.
4. $\{2, 3\} \cup \{1\}$.
5. $\{1, 2, 3\}$

Man beachte, dass die Teilmengen nicht leer sein dürfen und wir somit alle Möglichkeiten aufgelistet haben.

Proposition 1.7.9

Es sei M eine Menge.

1. Eine Äquivalenzrelation auf M liefert eine Partition von M.
2. Jede Partition von M definiert eine Äquivalenzrelation auf M.
3. Die beiden Konstruktionen sind invers zueinander.

Beweis. 1. Es sei R eine Äquivalenzrelation und es sei I eine Indizierung der Äquivalenzklassen, für $i \in I$ sei M_i die Äquivalenzklasse. Behauptung: $P = \{M_i \mid i \in I\}$ ist eine Partition von M.

- $M = \bigcup_{i \in I} M_i$, denn sei $m \in M$, dann ist $m \in [m]$, also in einer Äquivalenzklasse und somit existiert ein $i \in I$ mit $m \in M_i$. Die andere Inklusion ist klar, da $M_i \subset M$ für alle $i \in I$.
- Per Definition ist $M_i \neq \emptyset$ für alle $i \in I$.
- Wir beachten, dass für jedes $i \in$ gilt:

$$M_i = \{y \in M \mid x \sim y\} \text{ für jedes } x \in M_i.$$

Sei also $x \in M_i \cap M_j$, dann ist

$$M_i = \{y \in M \mid x \sim y\} = M_j.$$

Äquivalenzklassen sind entweder gleich oder disjunkt.

Damit erhalten wir eine Partition von der Menge M.

2. Es sei P eine Partition von M, $P = \{M_i \mid i \in I\}$ für eine Indexmenge I. Dann ist jedes $x \in M$ in genau einem M_i. Wir definieren eine Relation $R = \{(a, b) \in M \times M \mid \exists\, i \in I \text{ mit } a \in M_i, b \in M_i\}$.

   - R ist reflexiv, da für alle $a \in M$ gilt: $\exists\, i \in I \mid a \in I$, also $(a, a) \in R$.
   - R ist symmetrisch, denn falls $(x, y) \in R$, so existiert ein eindeutiges $i \in I$ mit $x, y \in M_i$, aber dann ist auch $(y, x) \in R$.
   - R ist transitiv, denn falls $(x, y), (y, z) \in R$ so existieren $i, j \in I$ mit $x, y \in M_i$ und $y, z \in M_j$. Da aber P eine Partition ist, ist y in genau einem M_s. Daraus folgt $M_i = M_j$, also $(x, z) \in R$.

3. Es sei R eine Äquivalenzrelation, P die induzierte Partition mit den Teilmengen $M_i, i \in I$ und S die von P induzierte Äquivalenzrelation. Es seien $x, y \in M$. Dann existiert per Definition der Partition genau dann ein $i \in I$ mit $x, y \in M_i$, falls $(x, y) \in R$. Dann gilt aber per Definition von S

$$(x, y) \in R \Leftrightarrow \exists\, i \in I \text{ mit } x, y \in M_i \Leftrightarrow (x, y) \in S$$

   Analog gilt das für eine Partition P, die induzierte Relation R und die davon induzierte Partition.

□

1.8 Homomorphiesatz

Zu einer gegebenen Abbildung $f : M \longrightarrow N$ definieren wir eine Äquivalenzrelation auf M und nutzen diese, um eine bijektive Abbildung zu konstruieren.

Definition 1.8.1

Es sei $f : M \longrightarrow N$, dann definiert

$$m \sim_f n :\Leftrightarrow f(m) = f(n)$$

die **Bildgleichheitsrelation**.

Beispiel 1.8.2

1. Sei M die Menge der EinwohnerInnen Aachens und N die Menge der Adressen in Aachen. Die Abbildung f ordnet jedem/jeder EinwohnerIn seine/ihre Meldeadresse zu. Die Abbildung ist weder injektiv (Personen könnten im selben Haus wohnen) noch surjektiv, da es leerstehende Häuser gibt. Durch die Bildgleichheitsrelation sind zwei Einwohnende in Relation, falls sie die selbe Meldeadresse haben.

2. Es sei $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^4$. Dann ist $y_1 \sim y_2 \Leftrightarrow y_1^4 = y_2^4$, also zwei reelle Zahlen stehen in Relation, wenn Sie vierte Wurzeln aus der selben reellen Zahl sind.

3. Es sei $n \in \mathbb{N}$ und $f : \mathbb{N} \longrightarrow \{0, 1, \ldots, n-1\}$ gegeben durch

$$a \mapsto \text{ Rest von } a \text{ geteilt durch } n.$$

f ist dabei surjektiv, aber nicht injektiv. Dann sind zwei natürliche Zahlen genau dann in Relation, wenn sie sich um ein ganzzahliges Vielfaches von n unterscheiden.

Proposition 1.8.3

Für $f : M \longrightarrow N$ definiert $\sim_f$ eine Äquivalenzrelation auf M.

Beweis. Wir zeigen die drei notwendigen Eigenschaften. Die Reflexivität von $\sim_f$ ist klar, die Symmetrie ebenfalls. Es bleibt die Transitivität zu zeigen, es seien also $m, n, p \in M$ gegeben mit $m \sim_f n$ und $n \sim_f p$, also $f(m) = f(n)$ und $f(n) = f(p)$. Dann folgt $f(m) = f(p)$, also $m \sim_f p$. □

Bemerkung 1.8.4

Relationen, welche durch eine Form von *Gleichheit* definieren werden, sind in vielen Fällen Äquivalenzrelationen.

Bemerkung 1.8.5: D

e Äquivalenzklassen der Bildgleichheitsrelation sind genau die nicht-leeren Fasern der Abbildung.

Das Ziel dieses Abschnitts ist der Homomorphiesatz für Mengen und wir bauen diesen Satz Schritt für Schritt auf:

Satz 1.8.6

Es sei $f : M \longrightarrow N$ eine Abbildung, dann definiert

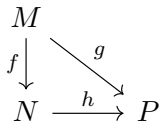
$$\overline{f} : M/\sim_f \longrightarrow N \ , \ [m] \mapsto f(m)$$

eine injektive Abbildung auf dem Quotientenraum.

Achtung: Wir wählen einen Repräsentanten, um eine Abbildung auf einer Äquivalenzklasse zu definieren. Damit das aber **wohldefiniert** ist, muss die Abbildung unabhängig von der Wahl des Repräsentanten sein. Egal welchen Repräsentanten wir für eine feste Äquivalenzklasse wählen, die Abbildung muss immer den gleichen Wert haben.

Beweis. Wir zeigen zuerst, dass $\overline{f}$ wohldefiniert ist. Es seien $[m] = [n]$, also m, n Repräsentanten derselben Äquivalenzklasse, dann haben wir zwei mögliche Werte von $\overline{f}$ auf $[m]$. Wir könnten $\overline{f}([m]) = f(m)$ wählen oder $\overline{f}([m]) = f(n)$. Wir müssen also zeigen, dass $f(m) = f(n)$ ist falls $m \sim_f n$. Aber das ist genau die Definition der Bildgleichheitsrelation (Definition 1.8.1).
Es bleibt zu zeigen, dass $\overline{f}$ injektiv ist. Es seien also $[m], [n] \in M/\sim_f$ mit $\overline{f}([m]) = \overline{f}([n])$ und damit, nach Wahl von Repräsentanten: $f(m) = f(n)$. Damit ist aber $m \sim_f n$ aufgrund der Bildgleichheitsrelation und damit $[m] = [n]$ und die Abbildung injektiv. □

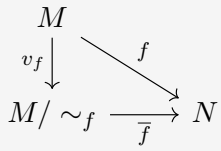
Zu den Eigenschaften dieser Abbildung führen wir ein *kommutatives Diagramm*. Diese können noch allgemeiner aussehen als unser Beispiel hier. Es seien $f : M \longrightarrow N, g : M \longrightarrow P, h : N \longrightarrow P$ Abbildungen zwischen Mengen M, N, P. Dann nennen wir folgendes Diagramm *kommutativ*, falls $g = h \circ f$ gilt.



Das heißt für alle $m \in M$ gilt: $g(m) = h \circ f(m) = h(f(m))$.

Satz 1.8.7: E

sei $f : M \longrightarrow N$ eine Abbildung, dann erhalten wir ein kommutatives Diagramm:



Hier bei ist $\overline{f}$ injektiv und v_f surjektiv.

Diesen Satz nennen wir den **Homomorphiesatz für Mengen**.

Beweis. Wir müssen nachrechnen, dass für jedes $m \in M$ gilt:

$$f(m) = \overline{f} \circ v_f(m)$$

gilt. Wir rechnen die rechte Seite aus

$$\overline{f} \circ v_f(m) = \overline{f}([m]) = f(m)$$

wobei wir hier m als Repräsentant von $[m]$ wählen können (die Abbildung ist nach Satz 1.8.6 unabhängig von der Wahl des Repräsentanten). □

Beispiel 1.8.8

Wir nehmen uns wieder ein Beispiel aus dem Leben. Sei M die Menge der EinwohnerInnen Aachens und N die Menge der Adressen in Aachen. Die Abbildung f ordnet jedem/jeder EinwohnerIn seine/ihre Meldeadresse zu. Die Abbildung ist weder injektiv (Personen könnten im selben Haus wohnen) noch surjektiv, da es leerstehende Häuser gibt. Durch die Bildgleichheitsrelation sind zwei Einwohnende in Relation falls sie die selbe Meldeadresse haben. Durch den Homomorphiesatz sammeln wir erst alle Personen, die die selbe Meldeadresse haben und ordnen diese dann dieser Adresse zu. Die Abbildung wird surjektiv, da wir in der induzierten Abbildungen nur noch die Meldeadressen betrachten, die auch bewohnt sind.

1.9 Binomialkoeffizienten

Definition 1.9.1

Es sei $0! := 1$ und induktiv $n! := (n-1)!n$ für alle $n \in \mathbb{N}$. Die natürliche Zahl $n!$ heißt **Fakultät**.

Beispiel 1.9.2

1. $1! = 1$.
2. $2! = 2$.
3. $3! = 6$.
4. $8! = 40320$.
5. $12! = 479001600$.

Bemerkung 1.9.3: D

e leere Summe ist als 0 definiert, das leere Produkt als 1. Konsequenterweise ist dann $0! = 1$.

Definition 1.9.4

Es sei M eine Menge. Die Menge der Bijektionen von M nach M notieren wir mit S_M und nennen diese Menge S_M, die **symmetrische Gruppe** von M. Für die Menge $M = \{1, 2, \ldots, n\}$ schreiben wir auch kurz S_n.

Beispiel 1.9.5

1. $n = 1$, dann ist S_2 die Menge der Bijektion von $\{1\}$ und damit besteht S_1 nur aus der Identität.
2. $n = 2$, dann ist die Identität auf der Menge $\{1, 2\}$ in S_2 und zusätzlich noch die Vertauschung $\sigma(1) = 2, \sigma(2) = 1$. Weitere Möglichkeiten gibt es nicht, Zuordnungen wie $\sigma(1) = \sigma(2)$ liefern keine Bijektion.
3. $n = 3$, dann ist die Identität auf der Menge $\{1, 2, 3\}$ in S_3 und zusätzlich noch die Elemente
   (a) $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$.
   (b) $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$.
   (c) $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 1$.
   (d) $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$.
   (e) $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2$.

   Wir sehen weiter unten, dass die S_3 genau 6 Elemente hat.

Proposition 1.9.6

Es sei $n \in \mathbb{N}$, dann hat die symmetrische Gruppe S_n genau $n!$ Elemente.

Beweis. Das ist ein Abzählargument, wir zählen die möglichen Bijektionen. Es sei φ eine solche Bijektion, dann ist $\varphi(1) \in \{1, \ldots, n\}$, wir haben also n-Möglichkeiten. $\varphi(2) \in \{1, \ldots, n\} \setminus \varphi(1)$, das sind $n-1$-Möglichkeiten und allgemein

$$\varphi(k) \in \{1, \ldots, n\} \setminus \{\varphi(1), \ldots, \varphi(k-1)\}$$

das sind $n-(k-1)$-Möglichkeiten (wir beachten, dass φ injektiv ist, also $|\{\varphi(1), \ldots, \varphi(k-1)\}| = k-1$). Insgesamt erhalten wir so $n*(n-1)*\cdots*2*1$-Möglichkeiten, also $n!$. □

Definition 1.9.7

Für $k, n \in \mathbb{N}_0$ ist der **Binomialkoeffizient** definiert als

$$\binom{n}{k} := \begin{cases} 0 & k > n \\ \frac{n!}{(n-k)!k!} & k \leq n \end{cases}$$

Beispiel 1.9.8

1. $\binom{4}{2} = \frac{4!}{2!2!} = 6$.
2. $\binom{49}{6} = 13.983.816$. Beachten Sie, dass Sie diese Anzahl für 6 aus 49 noch mit der Anzahl der möglichen Zusatzzahlen multiplizieren müssen.
3. $\binom{n}{0} = \frac{n!}{0!n!} = 1$.

Definition 1.9.9

Es sei M eine Menge, wir zerlegen die Potenzmenge von N in kleinere Teilmengen. Für jedes $k \leq |M|$ sei

$$\mathrm{Pot}_k(M) = \{U \subseteq M \mid |U| = k\}$$

die Menge der k-elementigen Teilmengen von M.

Beispiel 1.9.10

Es sei $M = \{1, 2, 3, 4\}$

1. Dann ist $\mathrm{Pot}_0(M) = \{\emptyset\}$.
2. Dann ist $\mathrm{Pot}_1(M) = \{\{1\}, \{2\}, \{3\}, \{4\}\}$.
3. Dann ist Dann ist $\mathrm{Pot}_4(M) = \{1, 2, 3, 4\}$.

Proposition 1.9.11

Es M eine Menge, $n = |M|$ und $k \leq n$. Dann gilt

$$|\mathrm{Pot}_k(M)| = \binom{n}{k},$$

insbesondere ist also $\binom{n}{k} \in \mathbb{N}_0$ für alle $k, n \in \mathbb{N}_0$.

Beweis. Es sei n fest und wir beweisen das per Induktion nach k

1. Induktionsanfang: Für $k = 0$ ist die Aussage richtig, denn
$$|\mathrm{Pot}_0(M)| = 1 = \binom{n}{0},$$
2. Induktionsvoraussetzung: Angenommen es gelte
$$|\mathrm{Pot}_k(M)| = \binom{n}{k},$$
für ein festes aber beliebiges $0 \leq k < n$.
3. Induktionsschritt: Wir zeigen
$$|\mathrm{Pot}_{k+1}(M)| = \binom{n}{k+1},$$
Es sei U eine der k-elementigen Teilmengen von M und sei x eines der übrigen $(n-k)$-Elemente. Für die Wahl von U und x haben wir somit
$$(n-k)\binom{n}{k} = \frac{n!(n-k)}{k!(n-k)!} = \frac{n!}{k!(n-(k+1))!}$$
Möglichkeiten. Eine gegebene $k+1$-elementige V Teilmenge kann aber auf $k+1$ unterschiedliche Arten konstruiert werden, für jedes $y \in V$ haben wir $V = V \setminus \{y\} \cup \{y\}$. Also müssen wir die Anzahl unserer Möglichkeiten noch durch $k+1$ teilen und erhalten
$$|\mathrm{Pot}_{k+1}(M)| = \frac{1}{k+1}\frac{n!}{k!(n-(k+1))!} = \frac{n!}{(k+1)!(n-(k+1))!} = \binom{n}{k+1}.$$

□

Wir können noch einige nützliche Identitäten zu Binomialkoeffizienten beweisen:

Proposition 1.9.12

Es seien $k \leq n \in \mathbb{N}_0$, dann gelten

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

Beweis. 1. Wir beweisen dass durch Umformung:
$$\binom{n}{n-k} = \frac{n!}{(n-k)!n!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$
Ein alternativer Beweis wäre: Für eine n-elementige Teilmenge M ist die Abbildung $\mathrm{Pot}_k(M) \longrightarrow \mathrm{Pot}_{n-k}(M)\ ,\ N \mapsto \overline{N} \subseteq M$ eine Bijektion.

2. Wir beweisen das wieder durch explizites Nachrechnen:

$$k\binom{n}{k} = \frac{n!}{(n-k)!(k-1)!} = n\frac{(n-1)!}{(n-1-(k-1))!(k-1)!} = n\binom{n-1}{k-1}.$$

3. Den Beweis überlassen wir gerne Ihnen zur Übung.

4. Wir haben in Proposition 1.9.11 gesehen, dass für eine Menge M mit $|M| = n$ gilt

$$|\mathrm{Pot}_k(M)| = \binom{n}{k}.$$

Dann ist aber

$$\sum_{k=0}^{n}\binom{n}{k} = \sum_{k=0}^{n}|\mathrm{Pot}_k(M)| = |\bigcup_{k=0}^{n}\mathrm{Pot}_k(M)| = |\mathrm{Pot}(M)|.$$

Das vorletzte Gleichheitszeichen folgt aus der Tatsache, dass

$$\mathrm{Pot}_\ell(M) \cap \mathrm{Pot}_k(M) = \emptyset \text{ falls } \ell \neq k.$$

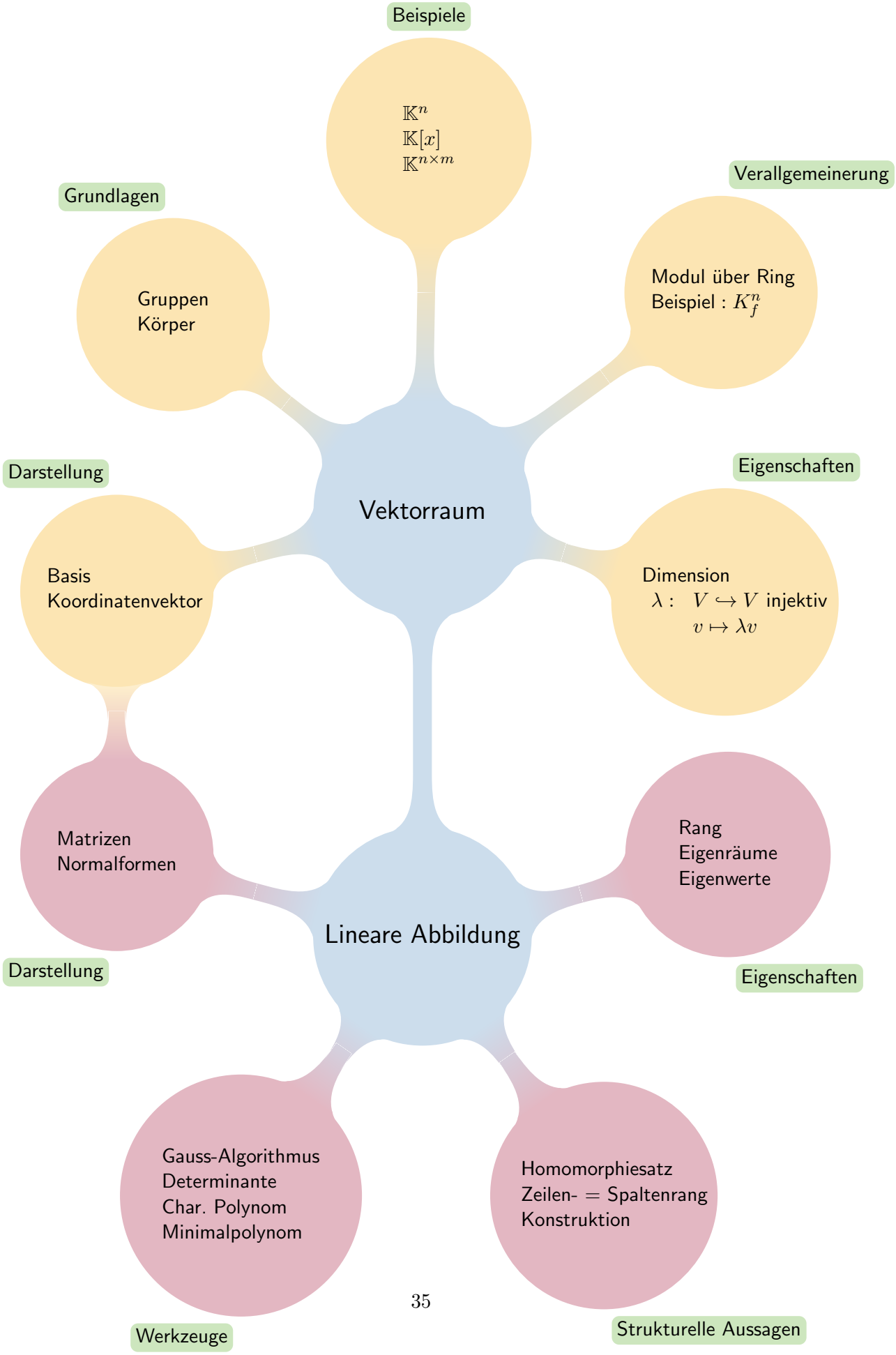
Jetzt folgt die Behauptung aus Proposition 1.4.10.

□

Kapitel 2

Kapitel der Linearen Algebra I

Wir geben Ihnen hier eine Mind Map über die Inhalte der *Linearen Algebra*, die grafisch die wichtigsten Punkte der einzelnen Themen und deren Zusammenhänge darstellt. Wir werden hier im Folgenden noch die erstellten Videos den Punkten in der Mind Map zuordnen.


Beispiele
$\mathbb{K}^n$
$\mathbb{K}[x]$
$\mathbb{K}^{n\times m}$
Grundlagen
Gruppen
Körper
Verallgemeinerung
Modul über Ring
Beispiel : K_f^n
Darstellung
Basis
Koordinatenvektor
Vektorraum
Eigenschaften
Dimension
$\lambda: \quad V \hookrightarrow V$ injektiv
$v \mapsto \lambda v$
Matrizen
Normalformen
Darstellung
Lineare Abbildung
Rang
Eigenräume
Eigenwerte
Eigenschaften
Gauss-Algorithmus
Determinante
Char. Polynom
Minimalpolynom
Werkzeuge
Homomorphiesatz
Zeilen- = Spaltenrang
Konstruktion
Strukturelle Aussagen

2.1 Lineare Gleichungssysteme und der Gauss-Algorithmus

Wir motivieren den Inhalt der folgenden Vorlesung anhand von linearen Gleichungssystemen und dem Gauss-Algorithmus; beides sollte aus der Schule bekannt sein. Vorher wollen wir nur ganz kurz über die Zahlen reden, die wir im folgenden verwenden werden. Viel detaillierter werden wir Gruppen, Ringe und Körper im anschließenden Kapitel besprechen.

Videos zu diesem Abschnitt

1. Lineare Gleichungssystem
2. Matrizen und Matrixmultiplikation
3. Gauss-Algorithmus

Definition 2.1.1

Es sei $\mathbb{R}$ der **Körper der reellen Zahlen** mit $+, *$ als Addition und Multiplikation.

Bemerkung 2.1.2

Wir können uns $\mathbb{R}$ als die *übliche* Zahlengerade vorstellen mit der bekannten Addition und Multiplikation. Dieser Körper stammt aus der Analysis und wird noch detaillierter und vor allem formal korrekt eingeführt. Wir halten uns damit nicht auf, sondern wollen auf unser bisheriges Verständnis der reellen Zahlen aus der Schule (auf-)bauen.

Bemerkung 2.1.3

Es gelten folgenden Rechenregeln in $\mathbb{R}$:

1. $a + b = b + a$, $a * b = b * a$ für alle $a, b \in \mathbb{R}$.
2. $0 + a = a$, $1 * a = a$ für alle $a \in \mathbb{R}$.
3. Für alle $a \in \mathbb{R}$ gilt: $a + (-a) = 0$.
4. Für alle $0 \neq a \in \mathbb{R}$ existiert $b \in \mathbb{R}$ mit $a * b = 1$.
5. $a * (b + c) = a * b + a * c$, $a * (b * c) = (a * b) * c$, $a + (b + c) = (a + b) + c$ für alle $a, b, c \in \mathbb{R}$

Letztere sind die Assoziativ- und Distributivgesetze für die reellen Zahlen.

Definition 2.1.4

Für jede natürliche Zahl n sei der **n-dimensionale reelle Raum** $\mathbb{R}^n$ die Menge der n-Tupel reeller Zahlen

$$(x_1, \ldots, x_n).$$

Die Elemente des Raumes nennen wir Vektoren und die Einträge eines Vektors die Komponenten.

Bemerkung 2.1.5

Wir beachten hierbei, dass $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ genau dann, wenn $x_1 = y_1, \ldots, x_n = y_n$.

2.1.1 LGS und Matrizen

Definition 2.1.6

Es seien $m, n \in \mathbb{N}, a_{ij}, b_i \in \mathbb{R}$. Dann nennt man

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n & = & b_m \end{array}$$

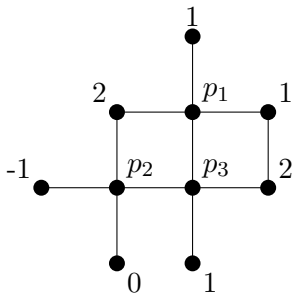
ein **lineares Gleichungssystem (LGS)**, wobei die Menge aller $(x_1, \ldots, x_n) \in \mathbb{R}^n$ gesucht ist, die alle Gleichungen erfüllen.

Beispiel 2.1.7

$$\begin{array}{ccccccccc} x_1 & + & 2x_2 & + & 0x_3 & - & x_4 & = & -1 \\ 2x_1 & - & x_2 & + & 3x_3 & + & 2x_4 & = & 0 \\ -x_1 & - & 2x_2 & - & x_3 & + & x_4 & = & 1 \end{array}$$

Beispiel 2.1.8

[Temperatur von Gitterpunkten] Man stelle sich folgendes Gitter vor, dessen Gitterpunkte jeweils eine Temperatur haben:



Die Temperaturen p_1 bis p_3 sind unbekannt. Jedoch weiß man, dass deren Wert der Mittelwert der verbundenen Gitterpunkte sein muss. Damit gilt:

$$\begin{aligned} p_1 &= \frac{1}{4} \cdot (p_3 + 1 + 1 + 2) \\ p_2 &= \frac{1}{4} \cdot (0 + p_3 + 2 - 1) \\ p_3 &= \frac{1}{4} \cdot (1 + 2 + p_1 + p_2) \end{aligned}$$

bzw.

$$\begin{aligned} p_1 - \frac{1}{4} \cdot p_3 &= 1 \\ p_2 - \frac{1}{4} \cdot p_3 &= \frac{1}{4} \\ -\frac{1}{4} \cdot p_1 - \frac{1}{4} \cdot p_2 + p_3 &= \frac{3}{4}. \end{aligned}$$

Im Folgenden möchten wir eine alternative Schreibweise einführen, mit deren Hilfe für ein lineares Gleichungssystem kompakter aufschreiben können. Dazu definieren wir:

Definition 2.1.9

Für $n, m \in \mathbb{N}$ und $a_{ij} \in \mathbb{R}$ nennt man

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

eine $m \times n$-**Matrix**, die Zahlen a_{ij} heißen **Einträge** oder **Elemente** der Matrix. Wir schreiben auch oft kurz $A = (a_{i,j})$ für diese Matrix. Die Menge aller $m \times n$-Matrizen mit reellen Einträgen schreiben wir als $\mathbb{R}^{m \times n}$. Für $m = 1$ (bzw. n=1) kürzen wir dies oft ab zu $\mathbb{R}^n$ (bzw. $\mathbb{R}^m$).

Beispiel 2.1.10

Wir betrachten einige Beispiele von Matrizen:

1. $$A = \begin{pmatrix} 3 & -2 & 1 \\ -1 & 0 & 2 \end{pmatrix}$$

   ist eine 2×3-Matrix.

2. $A = \begin{pmatrix} 1 & -2 & 0 & 4 \end{pmatrix}$ ist eine 1×4-Matrix.

3. $$A = \begin{pmatrix} -3 \\ 2 \\ -1 \end{pmatrix}$$

   ist eine 3×1-Matrix.

Wir wollen Matrizen nutzen, um Gleichungssysteme kompakter zu schreiben. Dafür formulieren wir ganz allgemein eine Multiplikation für Matrizen (die werden wir noch oft verwenden in der Linearen Algebra) und finden ein LGS als Spezialfall wieder.

Definition 2.1.11

Es seien $n, m, p \in \mathbb{N}$ und $A = (a_{i,j}) \in \mathbb{R}^{m \times n}, B = (b_{i,j}) \in \mathbb{R}^{n \times p}$ zwei reelle Matrizen, dann definieren wir als das Produkt von A und B die reelle $m \times p$-

Matrix $C = (c_{i,j})$ mit

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}.$$

Umgangssprachlich formuliert: wir multiplizieren die i-te Zeile von A mit der j-ten Spalte von B und schreiben das Ergebnis an die Stelle i, j. Das Zeilen-Spalten Produkt ist hierbei eintragsweise und anschließend aufsummiert.

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & \vdots & & \vdots \\ a_{i,1} & a_{i,2} & \dots & a_{i,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} b_{1,1} & \dots & b_{1,j} & \dots & b_{1,p} \\ \vdots & & \vdots & & \vdots \\ & \dots & b_{i,j} & \dots & \\ \vdots & & \vdots & & \vdots \\ b_{n,1} & \dots & b_{n,j} & \dots & b_{n,p} \end{pmatrix} = \begin{pmatrix} c_{1,1} & \dots & c_{1,j} & \dots & c_{1,p} \\ \vdots & & \vdots & & \vdots \\ & \dots & c_{i,j} & \dots & \\ \vdots & & \vdots & & \vdots \\ c_{m,1} & \dots & c_{m,j} & \dots & c_{m,p} \end{pmatrix}$$

Bemerkung 2.1.12

Man beachte dringend das Format der beteiligten Matrizen: Die Anzahl der Spalten von A muss gleich der Anzahl der Zeilen von B sein, ansonsten ist die Länge der Zeilen von A nicht gleich der Länge der Spalten von B und das Produkt ist nicht definiert.

Beispiel 2.1.13

Wir betrachten einige Beispiele für Matrizenmultiplikation

1. $$\begin{pmatrix} 1 & 2 \\ 0 & -1 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 & 1 & 4 \\ 1 & 1 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ -1 & -1 & 0 & 2 \\ 1 & -2 & 3 & 10 \end{pmatrix}.$$

   Hier gilt für die rot markierten Elemente

   $$3 \cdot 1 + 1 \cdot 0 = 3.$$

2. $$\begin{pmatrix} 2 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 6 \end{pmatrix}.$$

3. $$\begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \end{pmatrix} = \begin{pmatrix} 6 & -3 \\ 4 & -2 \end{pmatrix}.$$

4. $$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Kommen wir zurück zu den motivierenden Gleichungssystemen, die können wir jetzt

auch anders formulieren:

$$\text{Für } A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \text{ und } x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

liefert die Matrizenmultiplikation

$$A \cdot x = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{pmatrix}.$$

Dann liest sich das Gleichungssystem als

$$A \cdot x = b,$$

wobei

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

Definition 2.1.14

Für ein lineare Gleichungssystem $A \cdot x = b$ nennt man

$$(A, b) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right)$$

die **erweiterte Koeffizientenmatrix**, und b den **Lösungsvektor**.

Beispiel 2.1.15

Wir übernehmen das obige Beispiel 2.1.7 und erhalten

$$(A, b) = \left(\begin{array}{cccc|c} 1 & 2 & 0 & -1 & -1 \\ 2 & -1 & 3 & 2 & 0 \\ -1 & -2 & -1 & 1 & 1 \end{array}\right)$$

Bemerkung 2.1.16

Tatsächlich können wir aus der erweiterten Koeffizientenmatrix das lineare Gleichungssystem zurückgewinnen, wir haben also kompakte Schreibweise für so ein LGS gefunden und wollen mit dieser weiterarbeiten. Man sollte immer im Hinterkopf behalten, was diese Schreibweise eigentlich bedeutet, so vermeidet man im Folgenden Interpretationsfehler.

Definition 2.1.17

Es sei $Ax = b$ ein lineares Gleichungssystem. Falls $b = 0$ ist, so nennen wir das lineare Gleichungssystem **homogen** ansonsten heißt das Gleichungssystem **inhomogen**.

2.1.2 Lösungsmengen und der Gauss-Algorithmus

Wie in dem Beispiel erläutert, interessieren wir uns vor allem für die Lösungen eines LGS. Seien also $A \in \mathbb{R}^{m\times n}$ und $b \in \mathbb{R}^m$ gegeben, dann bezeichnen wir mit

$$L(A, b) = \{x \in \mathbb{R}^n \mid A \cdot x = b\}$$

die Lösungen des Gleichungssystems. Im restlichen Abschnitt wollen wir den Gauss-Algorithmus beschreiben, der uns ein Verfahren liefert, wie wir mit endlich vielen Schritten alle Lösungen des Gleichungssystems erhalten oder der mit dem Nachweis endet, dass es keine Lösungen gibt.
Wir starten mit einem LGS, bei welchem wir die Lösungen mit geringem Aufwand ablesen können.

Definition 2.1.18

Eine Matrix $A = (a_{i,j}) \in \mathbb{R}^{m\times n}$ ist in **Zeilenstufenform**, kurz ZSF, falls es ein $r \geq 0$ gibt und Zahlen $s_1 < \ldots < s_r$ gibt so, dass

1. $a_{i,j} = 0$ für alle $i > r$.
2. $a_{i,j} = 0$ für alle $j < s_i$.
3. $a_{i,s_i} \neq 0$.

Die Elemente $a_{1,s_1}, \ldots, a_{r,s_r}$ heißen **Pivots**, per Definition sind diese von Null verschieden.

Beispiel 2.1.19

Verschiedene Matrizen in Zeilenstufenform und ein anderes Beispiel

1. $$(A, x) = \left(\begin{array}{ccccc} 1 & 2 & 0 & -1 & -1 \\ 0 & -1 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right)$$
   ist in Zeilenstufenform, die rot markierten Elemente sind die Pivots.
2. $$(A, x) = \left(\begin{array}{ccccc} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$
   ist in Zeilenstufenform, die rot markierten Elemente sind die Pivots.
3. $$(A, x) = \left(\begin{array}{ccccc} 0 & 2 & 0 & -1 & -1 \\ 2 & -1 & 3 & 2 & 0 \\ 3 & 0 & 0 & 1 & 1 \end{array}\right)$$

ist nicht in Zeilenstufenform.

Definition 2.1.20

Es sei $A = (a_{i,j}) \in \mathbb{R}^{m \times n}$ in Zeilenstufenform mit den Stufen in den Spalten $s_1 < \ldots < s_r$. Wir sagen, dass A in **reduzierter Zeilenstufenform** ist, wenn

1. $\forall\, 1 \leq i \leq r : a_{k,s_i} = 0 \;\; \forall\, 1 \leq k < i$,
2. $\forall\, 1 \leq i \leq r : a_{i,s_i} = 1$.

Beispiel 2.1.21

In den obigen Beispielen ist die zweite Matrix in reduzierter ZSF, die erste dagegen nicht.

Bemerkung 2.1.22

Wenn wir mit einem LGS starten, dann ergibt sich die Reihenfolge der Spalten aus einer Numerierung der Variablen. Wir können diese frei wählen, also immer erreichen, dass die r Pivots in den ersten r Spalten stehen. Das ändert nichts grundsätzliches an dem Gleichungssystem, aber wir könnten dadurch statt $s_1 < \ldots < s_r$ einfach $1, \ldots, r$ wählen.

Proposition 2.1.23

Es sei $A \cdot x = b$ gegeben und die erweiterte Koeffizientenmatrix (A, b) habe Zeilenstufenform (mit den Stufen bei $s_1 < \ldots < s_r$), dann gilt

1. Falls $s_r = n + 1$, dann ist die Lösungsmenge $L(A, b)$ leer.
2. In allen anderen Fällen wird die Lösungsmenge durch $\mathbb{R}^{n-r}$ parametrisiert.

In dem Beweis geben wir eine Konstruktion der Parametrisierung an; die Variablen $x_{s_1}, \ldots, x_{s_r}$ nennen wir **gebundene Variablen**, die übrigen $n - r$-Variablen nennen wir **freie Variablen**.

Beweis. Sei $A \cdot x = b$ gegeben und $A(A, b)$ habe Zeilenstufenform mit den Stufen bei $s_1 < \ldots < s_r$.

1. Angenommen $s_r = n + 1$, dann lautet die r-te Zeile der Matrix

$$0 \quad 0 \quad \cdots \quad 0 \quad 0 \;\big|\; b_r$$

wobei $b_r \neq 0$. Übersetzt in das LGS ist das die Gleichung

$$0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = b_r \neq 0$$

Diese Gleichung hat keine Lösungen und damit hat das Gleichungssystem keine Lösungen und es ist $L(A, b) = \emptyset$.

2. Wie vorher beschrieben können wir annehmen, dann $s_i = i$ ist und die freien Variablen gerade $x_{r+1}, \ldots, x_n$ sind. Da $s_r < n+1$ folgt, dass $b_{r+1} = \ldots = b_m = 0$. Wir wählen $\lambda_1, \ldots, \lambda_{n-r} \in \mathbb{R}$ als *Parameter* und setzen

$$x_{r+i} = \lambda_i \; \forall \; i = 1, \ldots, n-r.$$

Wir betrachten die r-te Zeile von (A, b) und erhalten also Gleichung

$$a_{r,r}x_r + a_{r,r+1}\lambda_1 + \ldots + a_{r,n}\lambda_{n-r} = b_r$$

und damit, da $a_{r,r} \neq 0$

$$x_r = \frac{1}{a_{r,r}}(b_r - a_{r,r+1}\lambda_2 - \ldots - a_{r,n}\lambda_{n-r})$$

Damit haben wir x_r eindeutig festgelegt, die obige Schreibweise ist abhängig von den Parametern $\lambda_1, \ldots, \lambda_{n-r}$. Wir setzen das fort um $x_{r-1}, \ldots, x_1$ zu bestimmen. In jedem Schritt erhalten wir eine Darstellung von $x_i = \phi_i(\underline{\lambda})$, die nur von den Einträgen in (A, b) sowie den Parametern abhängig ist. Wir erhalten eine Abbildung $\Phi : \mathbb{R}^{n-r} \longrightarrow L(A, b) \subseteq \mathbb{R}^n$ mit

$$(\lambda_1, \ldots, \lambda_{n-r}) \mapsto (\phi_1(\underline{\lambda}), \ldots, \phi_r(\underline{\lambda}), \lambda_1, \ldots, \lambda_{n-r}).$$

Nach Konstruktion ist Φ eine surjektive Abbildung auf $L(A, b)$ und injektiv da sich aus den letzten $n - r$ Einträgen das Urbild eindeutig rekonstruieren lässt.

□

Beispiel 2.1.24

Zwei Beispiele:

1. Wir betrachten das Gleichungssystem der erweiterten Koeffizientenmatrix

$$\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 0 & 0 & 0 & 2 & -6 & -2 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{array}\right)$$

Dann sind x_1, x_3, x_4 die gebundenen Variablen und x_2, x_5 die freien Variablen. Da in diesem Fall die letzte Stufe erst in der letzten Spalte steht, ist die Lösungsmenge des Gleichungssystem leer.

2. Wir betrachten das Gleichungssystem der erweiterten Koeffizientenmatrix

$$\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 1 & 2 & -1 & 2 & 1 \\ 0 & 0 & 1 & 2 & -6 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Dann sind x_1, x_2, x_3 die gebundenen Variablen und x_4, x_5 die freien Variablen. Die Lösungsmenge ist dann durch den $\mathbb{R}^2$ parametrisiert, die Details der Parametrisierung dürfen Sie gerne nachrechnen.

Für ein LGS in Zeilenstufenform können wir also die Lösungen ausrechnen; es bleibt also zu zeigen, dass wir jedes LGS in Zeilenstufenform bringen können und dabei die Kontrolle über die Lösungen behalten. Dafür wollen wir folgende Manipulationen nutzen:

Proposition 2.1.25

Es sei $A \cdot x = b$ gegeben und (A, b) die erweiterte Koeffizientenmatrix. Es sei $(\overline{A}, \overline{b})$ eine Matrix, die durch mehrere der folgenden **elementaren Zeilenoperationen** aus (A, b) entstanden ist:

1. Vertauschen zweier Zeilen.
2. Addition des λ-fachen der i-ten Zeile zur j-ten Zeile. Hierbei ist $\lambda \in \mathbb{R}$ und falls $i = j$, so ist $\lambda \neq -1$.

Dann ist $L(\overline{A}, \overline{b}) = L(A, b)$.

Bemerkung 2.1.26

Die Addition eines Vielfachen der i-ten Zeile auf sich selbst können wir auch als Multiplikation der i-ten Zeile mit einer Konstanten $\lambda \neq 0$ auffassen.

Beweis. Da jede Gleichung des LGS erfüllt sein muss, macht es keinen Unterschied wenn man zwei Zeilen (übersetzt also Gleichungen) vertauscht. Wir betrachten die zweite Operation, die betrifft nur die Zeilen i und j, also genügt es diese zu betrachten

$$\begin{array}{rcl} a_{i,1}x_1 + \ \ldots \ + a_{i,n}x_n & = & b_i \\ a_{j,1}x_1 + \ \ldots \ + a_{j,n}x_n & = & b_j \end{array}$$

und die durch Addition des λ-fachen der i-ten Zeile zur j-ten Zeile transformierten Gleichungen

$$\begin{array}{rcl} a_{i,1}x_1 + \ \ldots \ + a_{i,n}x_n & = & b_i \\ (a_{j,1} + \lambda a_{i,1})x_1 + \ \ldots \ + (a_{j,n} + + \lambda a_{i,n})x_n & = & b_j + \lambda b_i \end{array}$$

Wir sehen, dass wenn $(x_1, \ldots, x_n)$ den ersten Gleichungssatz erfüllt, dann natürlich auch die erste Gleichung des zweiten Satzes. Andererseits ist die zweite Gleichung des zweites Satzes nur die Addition des λ-fachen der ersten Gleichung auf die zweite. Also erfüllt $(x_1, \ldots, x_n)$ auch den zweiten Gleichungssatz. Jetzt erleichtern wir uns die Arbeit und stellen fest, dass wir die Transformation rückgängig machen können durch Addition des $-\lambda$-fachen der i-ten Zeile zur j-ten Zeile. □

Für das Lösen eines allgemeinen linearen Gleichungssystem fehlt uns noch ein letzter Schritt:

Proposition 2.1.27

Es sei $A \in \mathbb{R}^{m \times n}$, dann lässt sich A durch endlich viele elementare Zeilenoperationen auf (reduzierte) Zeilenstufenform bringen.

In dem Beweis geben wir einen Algorithmus an, der die Zeilenstufenform nach endlich vielen Schritten erreicht. Wir empfehlen die Nutzung dieses Algorithmus', um eventuelle (unendliche) Wiederholungen zu vermeiden.

Beweis. Wir beweisen die Aussage per Induktion. Der Induktionsanfang ist $n = m = 1$ und hier ist die Aussage klar. Jetzt seien n, m beliebig und die Aussage richtig für alle $k \times \ell$-Matrizen mit $k < m$ und $\ell < n$.
Sei $A \in \mathbb{R}^{m \times n}$. Falls $A = 0$ ist, so ist A in ZSF. Andernfalls gibt es einen Eintrag $\neq 0$, also eine Spalte in A, die verschieden von 0 ist. Wir wählen unter den nicht-trivialem Spalten, diejenige mit dem kleinsten Index j_1 aus. Es sei $a_{i,j_1} \neq 0$, dann tauschen wir die 1-te und i-te Zeile, und können annehmen, dass $a_{1,j_1} \neq 0$. Jetzt multiplizieren wir die erste Zeile mit $\frac{1}{a_{1,j_1}}$ und können annehmen, dass $a_{1,j_1} = 1$.
Es sei nun $1 < k \leq m$, dann erhalten wir durch das Addieren des $(-a_{k,j_k})$-fachen der 1-ten Zeile auf die k-te Zeile, dass alle bis auf den ersten Eintrag in der j_1-Spalte gleich 0 sind. Somit haben wir eine Matrix erhalten, die folgende Form hat

$$\left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & & & 0 & & & \\ & \ddots & & & & \tilde{A} & \\ & & 0 & 0 & & & \end{array}\right)$$

wobei $\tilde{A}$ eine $m - 1 \times n - j_1$-Matrix ist. Wir können damit, per Induktion, $\tilde{A}$ durch elementare Zeilenoperationen auf ZSF bringen. Wir beachten dabei, dass die 1-te Zeile von $\tilde{A}$ die 2-te Zeile von A ist, wir also die erste Zeile von A dabei nicht weiter nutzen werden. Darüber hinaus besteht A in den Zeilen 2 bis m und den Spalten 1 bis j_1 aus der Nullmatrix. Das bedeutet, dass wir notwendigen Umformungen für die Matrix $\tilde{A}$ auf die Matrix A ausdehnen können, ohne das wir die grundlegende Struktur ändern, wir erhalten also für $\tilde{A}$ eine Matrix B in ZSF und insgesamt

$$\left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & & & 0 & & & \\ & \ddots & & & & B & \\ & & 0 & 0 & & & \end{array}\right)$$

Insgesamt haben wir damit A in ZSF gebracht. Uns fehlt noch der Beweis, dass wir auch immer eine Mit Hilfe reduzierte Zeilenstufenform erreichen können. Diesen Teil überlassen wir Ihnen als Übungsaufgabe. □

Definition 2.1.28

Der **Gaussalgorithmus** zum Lösen eines LGS $A \cdot x = b$ besteht aus den Schritten

1. Berechnung einer Zeilenstufenform der erweiterten Koeffizientenmatrix..
2. Bestimmung der Lösungsmenge durch Parametrisierung oder durch Feststellung, dass diese leer ist.

Beispiel 2.1.29

$$
\begin{aligned}
(A|b) \quad &= \left(\begin{array}{ccccc|c} 0 & 0 & 2 & -1 & 2 & 1 \\ 1 & -2 & 3 & 4 & 2 & 2 \\ 2 & -4 & 8 & 9 & 0 & 3 \\ -1 & 2 & -5 & -6 & 5 & 0 \end{array}\right) && 1.\text{Zeile} \leftrightarrow 2.\text{Zeile} \\
&\longrightarrow \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 2 & -4 & 8 & 9 & 0 & 3 \\ -1 & 2 & -5 & -6 & 5 & 0 \end{array}\right) && -2 \times \text{ 1.Zeile addiert auf 3.Zeile} \\
&\longrightarrow \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 0 & 0 & 2 & 1 & -4 & -1 \\ -1 & 2 & -5 & -6 & 5 & 2 \end{array}\right) && \begin{array}{c} 1.\text{Zeile addiert auf 4.Zeile} \\ \text{-2.Zeile addiert auf 3.Zeile} \end{array} \\
&\longrightarrow \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 0 & 0 & 0 & 2 & -6 & -2 \\ 0 & 0 & -2 & -2 & 7 & 3 \end{array}\right) && -1 \times \text{ 2.Zeile addiert auf 3.Zeile} \\
&\longrightarrow \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 0 & 0 & 0 & 2 & -6 & -2 \\ 0 & 0 & 0 & -3 & 9 & 3 \end{array}\right) && 2.\text{Zeile addiert auf 4.Zeile} \\
&\longrightarrow \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 4 & 2 & 2 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 0 & 0 & 0 & 2 & -6 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) && \tfrac{3}{2} \times \text{ 3.Zeile addiert auf 4.Zeile}
\end{aligned}
$$

An dieser Stelle haben wir die Zeilenstufenform erreicht und stellen fest, dass die letzte Stufe schon in der 4.Spalte ist, also hat das Gleichungssystem $Ax = b$ mindestens eine Lösung. Dann liest sich das modifizierte Gleichungssystem

$$
\begin{array}{rcrcrcrcr}
x_1 & - & 2x_2 & + & 3x_3 & + & 4x_4 & + & 2x_5 & = & 2 \\
 & & & & 2x_3 & - & x_4 & + & 2x_5 & = & 1 \\
 & & & & & & 2x_4 & - & 6x_5 & = & -2
\end{array}
$$

Wir lesen ab, dass die Variablen x_1, x_3, x_4 gebunden ist und wählen Parameter λ_1, λ_2 für die freien Variablen $x_2 = \lambda_1, x_5 = \lambda_2$. Damit erhalten wir

$$
\begin{array}{rcrcrcrcrcr}
x_1 & + & 3x_3 & + & 4x_4 & = & 2 & + & 2\lambda_1 & - & 2\lambda_2 \\
 & & 2x_3 & - & x_4 & = & 1 & & & - & 2\lambda_2 \\
 & & & & 2x_4 & = & -2 & & & + & 6\lambda_2
\end{array}
$$

Das Gleichungssystem können wir jetzt von unten nach oben durch Rückwärtssubstitution lösen und erhalten

$$
\begin{aligned}
x_4 &= -1 + 3\lambda_2 \\
x_3 &= \tfrac{1}{2}\lambda_2 \\
x_1 &= 6 + 2\lambda_1 - \tfrac{31}{2}\lambda_2
\end{aligned}
$$

2.2 Der euklidische Algorithmus und rationale Zahlen

Neben dem Gauss-Algorithmus ist der euklidische Algorithmus ein fundamentaler Baustein im ersten Studienjahr, er liefert beispielsweise die Lösungen zu simultanen Kongruenzen.

Videos zu diesem Abschnitt

1. Lemma von Bézout und erweiterter Euklidscher AlgorithmusTextseite
2. Der Restklassenring modulo n

2.2.1 Der euklidische Algorithmus

Definition 2.2.1

Der **Ring der ganzen Zahlen** besteht aus der Menge

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$$

mit der üblichen Addition und Multiplikation.

Bemerkung 2.2.2

Es gelten, wie bei den reellen Zahlen, die Assoziativ- und Distributivgesetze, sowie die Rechenregeln:

1. $a + b = b + a$, $a \cdot b = b \cdot a$ für alle $a, b \in \mathbb{Z}$.
2. $0 + a = a$, $1 \cdot a = a$ für alle $a \in \mathbb{Z}$.
3. Für alle $a \in \mathbb{Z}$ gilt: $a + (-a) = 0$.

Es gibt allerdings eine Einschränkung, denn nur für ± 1 gibt es ein inverses Element bezüglich der Multiplikation.

Definition 2.2.3

Es seien $a, b \in \mathbb{Z}$ gegeben. Wir sagen a **teilt** b (oder a ist ein Teiler von b) falls es $c \in \mathbb{Z}$ gibt mit $a \cdot c = b$.

Beispiel 2.2.4

1. 2 teilt 6, denn $2 \cdot 3 = 6$.
2. 5 teilt -20, denn $-20 = (-4) \cdot 5$.
3. 1 teilt jede ganze Zahl.
4. Primzahlen p werden nur von ± 1 und $\pm p$ geteilt.

Proposition 2.2.5

Einige Eigenschaften von Teilbarkeit, es seien im Folgenden $x, y, z, a, b, \lambda, \mu \in \mathbb{Z}$, dann gilt:

1. $x|y$ und $y|z$ dann gilt $x|z$.
2. $0|x \Rightarrow x = 0$.
3. $x|0$ für alle x.
4. $\pm 1|x$ für alle x.
5. $x| \pm 1 \Rightarrow x = \pm 1$.
6. $x|y$ und $y|x \Longrightarrow x = \pm y$.

Beweis. Sie dürfen sich dazu selber Gedanken machen, nutzen Sie dabei aus

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0.$$

□

Satz 2.2.6

Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Dann existieren eindeutig bestimmte $q \in \mathbb{Z}$ und $0 \leq r < |b|$ mit

$$a = q \cdot b + r.$$

Definition 2.2.7

Der **Rest von** a **geteilt durch** b ist dann r, wir schreiben dafür $r = a$ **mod** b.

Beweis. Wir zeigen erst die **Existenz**:
Hier genügt es den Beweis für $b > 0$ zu führen, denn falls $b < 0$, so ist $-b > 0$. Falls dann $a = \tilde{q}(-b) + r$ mit $0 \leq r < |a = | - a|$ folgt $a = qb + r$ mit $q = -\tilde{q}$.
Es sei $M = \{x \in \mathbb{Z} \mid x = y \cdot b \text{ für ein } y \in \mathbb{Z} \text{ und } x \leq a\}$, es sei x das maximale Element in M. Wir schreiben dann

$$r = a - x.$$

Es gilt $0 \leq r < b$, denn falls $r < 0$, so wäre $x > a$ und falls $r \geq b$, so wäre $x + 1 \in M$, also x nicht maximal. Damit können wir schreiben

$$a = x + r = q \cdot b + r.$$

Der zweite Teil des Beweis behandelt die **Eindeutigkeit**:
Angenommen es gäbe eine weitere Schreibweise

$$a = p \cdot b + c,$$

ohne Einschränkung sei dabei $c \geq r$. Dann gilt

$$(q - p) \cdot b = c - r \geq 0.$$

Aber gleichzeitig $b > c - r = (q - b) \cdot b$. Also folgt $(q - p) \cdot b = 0$, also $q = p$ (da $b \neq 0$), also also $c = r$. □

Definition 2.2.8

Es seien $a, b \in \mathbb{Z}$ gegeben. Eine Zahl c heißt **größter gemeinsamer Teiler** von a und b, falls folgende zwei Bedingungen erfüllt sind:

1. c ist ein Teiler von a und ein Teiler von b.
2. Für jeden weiteren Teiler d von a und b gilt, dass d auch c teilt.

Wir schreiben dafür $ggT(a, b)$. Zwei ganze Zahlen a und b heißen **teilerfremd** falls $ggT(a, b) = \pm 1$.

Beispiel 2.2.9

Verschiedene ggT.

1. $ggT(1234, 5678) = \pm 2$.
2. $ggT(-a, b) = ggT(a, b)$.

Bemerkung 2.2.10

Der größte gemeinsame Teiler von a, b ist nur eindeutig bis auf das Vorzeichen. Wir können diesen mit Hilfe des euklidischen Algorithmus bestimmen.

Algorithmus 2.2.11

Euklidischer Algorithmus
INPUT: $a \geq b \geq 1 \in \mathbb{Z}$
OUTPUT: $ggT(a, b)$
PROCEDURE: Euklid(a,b)

1. if $b = 0$, RETURN a.
2. if $b \neq 0$, RETURN Euklid(b, a mod b).

Wir beweisen das der Algorithmus funktioniert und den ggT von a und b liefert:

Beweis. Es gilt für alle $a, b \geq 0$ in $\mathbb{Z}$, dass $0 \leq a \bmod b$. Damit wird der erste Parameter in der Procedure mit jedem Schritt echt kleiner, aber da es nur endlich viele ganze Zahlen gibt, die ≥ 0 und $< b$ sind, terminiert der Algorithmus.
Die Iteration im Algorithmus liefert eine Folge von Zahlen r_i und q_i definiert durch die Gleichung aus Satz 2.2.6:

$$r_{i-2} = q_{i-1} r_{i-1} + r_i$$

wobei $r_0 = a, r_1 = b$ gesetzt sind. Es sei dabei n minimal, so dass $r_{n+1} = 0$ ist, also $r_n = d$ ist der Output des Algorithmus. Es folgt sofort, dass $d | r_n$ aber auch $d | r_{n-1}$ wie aus der letzten Gleichung

$$r_{n-1} = q_n r_n + 0$$

folgt. Das ist der Induktionsanfang, wir nehmen also an, dass d ein Teiler von r_j und r_{j+1} ist, dann folgt aus

$$r_{j-1} = q_j r_j + r_{j+1}$$

sofort, dass d auch r_{j-1} teilt. Wir nutzen hier die Transitivität der Teilbarkeit (1. Aussage von Proposition 2.2.5). Wir schließen daraus, dass d ein Teiler von a und b ist. Es sei c ein weiterer Teiler von a und b, dann folgt aus der Gleichung

$$r_0 = q_1 r_1 + r_2 \Leftrightarrow r_2 = r_0 - q_1 r_1,$$

dass c auch ein Teiler von r_2 ist. Iterativ setzen wir das fort und erhalten, dass c ein Teiler von $r_n = d$ ist. Damit ist d ein $ggT(a, b)$. □

2.2.2 Restklassenringe ganzer Zahlen

Es sei n eine ganze Zahl, dann definieren wir auf der Menge $\mathbb{Z}$ eine Äquivalenzrelation durch

$$a \equiv b \Leftrightarrow a \mod n = b \mod n.$$

Die Menge der Äquivalenzklassen bezeichnen wir mit $\mathbb{Z}/n\mathbb{Z}$ ($\mathbb{Z}$ modulo $n\mathbb{Z}$).

Proposition 2.2.12

Für eine ganze Zahl $n \neq 0$ hat die Äquivalenzrelation genau $|n|$ Äquivalenzklassen.

Beweis. Es seien $a, b \in \mathbb{Z}$, dann ist per Definition

$$a \sim b \Leftrightarrow a \mod n = b \mod n$$

das bedeutet, dass der Rest von a geteilt durch n der gleiche ist wie der Rest von b geteilt durch n. Wir sortieren Elemente nach den möglichen Resten und Satz 2.2.6 sagt, dass es maximal n verschiedene Reste gibt. Die Zahlen $\{0, \ldots, n-1\}$ liefern genau $|n|$ verschiedene Äquivalenzklassen, daraus folgt die Behauptung. □

Bemerkung 2.2.13

Mit einer Wahl von Repräsentanten können wir diese Äquivalenzklassen mit $[0], [1], \ldots, [n-1]$ bezeichnen. ACHTUNG: Dabei haben wir eine Wahl getroffen, genauso könnten wir auch $[n], [n+1], \ldots, [2n-1]$ oder $[0], [-1], \ldots, [-n+1]$ als Repräsentanten wählen. Mit Hilfe von Satz 2.2.6 können wir zu jedem a den Repräsentanten aus $0, \ldots, n-1$ bestimmen.

Beispiel 2.2.14

Es sei $n = 8$, dann gilt

$$[2] = \{2 + 8a \mid a \in \mathbb{Z}\}.$$

Es gibt unendlich viele mögliche Repräsentanten, nämlich die ganzen Elemente $2 + 8a$ mit $a \in \mathbb{Z}$, beispielsweise $2, 10, 18, 26, , -6, -14, \ldots$.

Wir definieren auf der Menge $\mathbb{Z}/n\mathbb{Z}$ eine Addition durch

$$[a] + [b] := [a + b]$$

und eine Multiplikation durch

$$[a] \cdot [b] := [a \cdot b].$$

Lemma 2.2.15

Die beiden Operationen sind wohldefinierte Abbildungen.

Beweis. Wir müssen zeigen, dass die Summe und das Produkt unabhängig von den gewählten Repräsentanten ist. Es seien $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ mit $a_1 \equiv a_2, b_1 \equiv b_2$, dann existieren $x, y \in \mathbb{Z}$ mit

$$a_1 = a_2 + xn, b_1 = b_2 + yn.$$

1. Es ist $a_1 + b_1 = a_2 + xn + b_2 + yn = a_2 + b_2 + (x + y)n$, also gilt

   $$a_1 + b_1 \bmod n = a_2 + b_2 \bmod n,$$

   und damit

   $$[a_1 + b_1] = [a_2 + b_2].$$

2. Es ist

   $$a_1 \cdot b_1 = (a_2 + xn)(b_2 + yn) = a_2 \cdot b_2 + (a_2 \cdot y + b_2 \cdot x + x \cdot y \cdot n)n.$$

   Also gilt

   $$a_1 \cdot b_1 \bmod n = a_2 \cdot b_2 \bmod n,$$

   und damit

   $$[a_1 \cdot b_1] = [a_2 \cdot b_2].$$

□

Bemerkung 2.2.16

Es ist [0] ein neutrales Element bezüglich der Addition und [1] ein neutrales Element bezüglich der Multiplikation.

Beispiel 2.2.17

Wenn Sie um 11 Uhr gefragt werden, ob Sie sich in 3 Stunden treffen möchten, dann überlegen Sie, ob Sie um 2 Uhr Zeit haben. Sie rechnen also modulo 12, Sie kennen also die obigen Rechnungen seitdem Sie Uhrzeiten kennen. Die Addition auf $\mathbb{Z}/n\mathbb{Z}$ für $n = 12$ entspricht als unserer **Uhrenarithmetik**.

Definition 2.2.18

Wir bezeichnen mit $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ den Restklassenring von $\mathbb{Z}$.

2.2.3 Die rationalen Zahlen

Auf der Menge $(\mathbb{Z}, \mathbb{Z} \setminus \{0\})$ definieren wir eine Äquivalenzrelation

$$(a, b) \equiv (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Die Menge der Äquivalenzklassen bezeichnen wir mit $\mathbb{Q}$ und schreiben für einen Repräsentanten $\frac{a}{b}$ statt (a, b).

Definition 2.2.19

Die Menge $\mathbb{Q}$ zusammen mit der Addition

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

und der Multiplikation

$$\frac{a}{b} \cdot \frac{c}{d} == \frac{ac}{bd}$$

nennen wir den **Körper der rationalen Zahlen**.

Bemerkung 2.2.20

Das neutrale Element der Addition ist die Klasse $0 = \frac{0}{1}$ und das neutrale Element der Multiplikation die Klasse $1 = \frac{1}{1}$. Es gilt für $0 \neq a, b \in \mathbb{Z}$

$$\frac{a}{b} \cdot \frac{b}{a} = 1$$

Proposition 2.2.21

Die Addition und die Multiplikation sind wohldefiniert.

Beweis. Wir müssen nachrechnen, dass die Addition und Multiplikation unabängig von der Wahl der Repräsentanten ist. Es reicht hierbei offensichtlich die Unabhängigkeit im ersten Argument zu zeigen, es seien also Es seien $(a_1, b_1) \equiv (a_2, b_2)$ und (c_1, d_1) gegeben.

1. Es ist per Definition

   $$\frac{a_1}{b_1} + \frac{c}{d} = \frac{a_1 d + b_1 c}{b_1 d} \text{ und } \frac{a_2}{b_2} + \frac{c}{d} = \frac{a_2 d + b_2 c}{b_2 d}$$

   Wir müssen zeigen, dass die beiden rechten Seiten äquivalent sind, also zeigen, dass

   $$\frac{a_1 d + b_1 c}{b_1 d} \equiv \frac{a_2 d + b_2 c}{b_2 d},$$

   also $a_1 b_2 = b_1 a_2$. Das ist per Definition der Relation äquivalent zu

   $$(a_1 d + b_1 c)(b_2 d) = (a_2 d + b_2 c)(b_1 d) \Leftrightarrow a_1 b_2 \cdot d^2 + b_1 b_2 cd = a_2 b_1 \cdot d^2 + b_1 b_2 cd$$

   Wir nutzen aus, dass $(a_1, b_1) \equiv (a_2, b_2)$, also $a_1 b_2 = b_1 a_2$ und erhalten die obige Gleichheit.

2. Es ist per Definition

   $$\frac{a_1}{b_1} \cdot \frac{c}{d} = \frac{a_1 c}{b_1 d} \text{ und } \frac{a_2}{b_2} \cdot \frac{c}{d} = \frac{a_2 c}{b_2 d}$$

   Wieder müssen wir zeigen, dass die beiden rechten Seiten äquivalent sind, also

   $$a_1 c b_2 d = b_1 d a_2 c \Leftrightarrow a_1 b_2 \cdot cd = a_2 b_1 \cdot cd.$$

   Die rechte Aussage folgt hier wiederum aus $(a_1, b_1) \equiv (a_2, b_2)$.

□

2.3 Gruppen, Ringe, Körper

Wir beginnen mit einigen fundamentalen Definitionen der Algebra. Dabei gilt unsere Aufmerksamkeit insbesondere einigen grundlegenden Strukturen: den Gruppen, Ringen und Körpern. Unter einer algebraischen Struktur verstehen wir eine Menge im Zusammenhang mit einer oder mehreren Operationen. Je nach Struktur kann dies eine Addition, eine Multiplikation, eine Verknüpfung oder etwas ganz anderes sein.

Videos zu diesem Abschnitt

1. Gruppen
2. Ringe
3. Polynomring
4. Ideale

2.3.1 Gruppen

Die grundlegendste algebraische Struktur ist die einer Gruppe:

Definition 2.3.1

Eine **Gruppe** ist eine nichtleere Menge G, versehen mit einer inneren Verknüpfung $\circ : G \times G \longrightarrow G$, $(a, b) \mapsto a \circ b$, die folgenden Axiomen genügt:

G1 $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ (**Assoziativität**)

G2 Es existiert ein $e \in G$ so, dass für alle $a \in G : a \circ e = e \circ a = a$. (**neutrales Element**)

G3 für alle $a \in G : \exists\, a^{-1} \in G$ mit $a^{-1} \circ a = a \circ a^{-1} = e$ (**inverses Element**)

Die Gruppe G heißt **kommutativ** (oder **abelsch**), falls

G4 für alle $a, b \in G : a \circ b = b \circ a$.

Wenn man von einer Gruppe G mit einer Verknüpfung $\circ$ spricht, dann schreibt man auch $(G, \circ)$. Ob man dies macht, hängt davon ab, ob einen die Verknüpfung interessiert bzw. ob diese bereits bekannt ist oder aus dem Zusammenhang folgt.

Sprechen wir von einer abelschen Gruppe, dann bezeichnen wir die Verknüpfung meistens mit einem + und das neutrale Element mit 0. Die Verknüpfung muss jedoch nicht die gewohnte Addition zwischen Zahlen sein.

Beispiel 2.3.2

Einige Beispiele für Gruppen:

1. $(\mathbb{Z}, +)$ ist eine abelsche Gruppe:

   G1: für alle $a, b, c \in \mathbb{Z} :\ (a + b) + c = a + (b + c)$
   G2: $e = 0$: für alle $a \in \mathbb{Z} :\ 0 + a = a + 0 = a$
   G3: für alle $a \in \mathbb{Z} :\ a^{-1} := -a$, womit $-a + a = 0 = a + (-a)$
   G4: für alle $a, b \in \mathbb{Z} :\ a + b = b + a$

   .

2. $(\mathbb{Q}^*, \cdot) = (\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe:

   G1: für alle $\frac{a}{b}, \frac{c}{d}, \frac{g}{f} \in \mathbb{Q}^*$: $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{g}{f}) = \frac{a \cdot (c \cdot g)}{b \cdot (d \cdot f)} = \frac{(a \cdot c) \cdot g}{(b \cdot d) \cdot f} = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{g}{f}$

   G2: $e = 1$: für alle $\frac{p}{q} \in \mathbb{Q}^*$: $\frac{p}{q} \cdot 1 = 1 \cdot \frac{p}{q} = \frac{p}{q}$

   G3: für alle $\frac{p}{q} \in \mathbb{Q}^*$: $\left(\frac{p}{q}\right)^{-1} := \frac{q}{p}$, womit $\frac{p}{q} \cdot \frac{q}{p} = \frac{pq}{pq} = 1 = \frac{q}{p} \cdot \frac{p}{q}$

   G4: für alle $\frac{a}{b}, \frac{p}{q} \in \mathbb{Q}^*$: $\frac{a}{b} \cdot \frac{p}{q} = \frac{p}{q} \cdot \frac{a}{b}$

   Bei G3 wird klar, warum die Null aus $\mathbb{Q}$ entfernt wurde. Denn die Null besitzt kein Inverses, sodass das Produkt 1 wäre.

3. Es seien $(G, \circ_G)$ und $(H, \circ_H)$ Gruppen, dann hat ist $G \times H$ (das kartesische Produkt) wieder ein Gruppe mit der Verknüpfung

   $$(a, b) \circ (c, d) := (a \circ_G c, b \circ_H d).$$

   $G \times H$ ist sicherlich abgeschlossen unter der Verknüpfung und wenn $a, a, a_3 \in G, b_1, b_2, b_3 \in H$ dann ist

   $$(a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3)) = (a_1 \circ_G (a_2 \circ_G a_3), b_1 \circ_H (b_2 \circ_H b_3))$$

   da aber G und H Gruppen sind, sind deren Verknüpfungen assoziativ, also erhalten wir

   $$((a_1 \circ_G a_2) \circ_G a_3), (b_1 \circ_H b_2) \circ_H b_3) = ((a_1, b_1) \circ (a_2, b_2)) \circ (a_3, b_3).$$

   Das neutrale Element ist $e = (e_G, e_H)$ und damit ist

   $$(a, b) \circ (a^{-1}, b^{-1}) = (e_G, e_H) = (a^{-1}, b^{-1}) \circ (a, b).$$

   Wir haben also gesehen, dass $G \times H$ wieder eine Gruppe ist und diese ist genau dann abelsch, wenn G und H abelsch sind.

4. $(S_n, \circ)$
   Sei $n \in \mathbb{N}$. Wir wiederholen an dieser Stelle Definition 1.9.4, und führen den Begriff weiter aus: Man definiert S_n als

   $$S_n := \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} | \sigma \text{ bijektiv}\}$$

   und nennt diese die symmetrische Gruppe. Die symmetrische Gruppe ist also die Gruppe aller Bijektionen von $\{1, ..., n\}$ nach $\{1, ..., n\}$. Wir haben schon gesehen, dass $|S_n| = n!$ gilt.

   Wir entwickeln nun zwei kompakte Schreibweisen, um diese Bijektionen darzustellen. Nehmen wir $n = 4$ an. Wir betrachten als Beispiel die Bijektion σ_1, die die Elemente 1 und 2 vertauscht. Dann können wir diese wie folgt als Matrix darstellen (**Matrixschreibweise**):

   $$\sigma_1 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

In der oberen Zeile stehen die Argumente und in der unteren Zeile jeweils die Bilder unter der entsprechenden Bijektion. σ_1 ist in dieser Schreibweise nicht als Matrix aufzufassen, sondern als Element der S_4. Hier folgen noch zwei weitere Beispiele:

$$\sigma_2 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},$$

$$\sigma_3 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Kommen wir nun zur zweiten Schreibweise (**Zykelschreibweise**). Diese ist zwar noch kompakter, erfordert aber auch eine höhere Interpretationsleistung. Man notiert, welche Elemente durch sukzessives Anwenden der Bijektion erreicht werden. Konkret beginnt man mit 1, als nächstes notiert man das Bild der 1, dann das Bild des Bildes usw. Da wir auf einer endlichen Menge operieren (und eine Bijektion haben), wird dort erneut eine 1 auftauchen. Damit ist der erste Zykel dargestellt. Jetzt wählen wir ein Element, welches bisher noch nicht erreicht wurde (beispielsweise das kleinste der übrigen Elemente), und setzen die Konstruktion fort. Unsere obigen Beispiele liefern dann

$$\begin{aligned} \sigma_1 &= (12)(3)(4) \\ \sigma_2 &= (1)(2)(3)(4) \\ \sigma_3 &= (14)(23) \end{aligned}$$

Zykel mit nur einem Element werden dabei üblicherweise nicht notiert:

$$\begin{aligned} \sigma_1 &= (12) \\ \sigma_2 &= \mathrm{id} \\ \sigma_3 &= (14)(23) \end{aligned}$$

Wir können so auch Verknüpfungen bilden, wobei wir hierbei beachten müssen, dass wir die Verknüpfung von Abbildungen betrachten, was bedeutet, dass wir von rechts nach links lesen:

$$\sigma_3 \circ \sigma_1 = (14)(23) \circ (12) = (1324).$$

Man muss sich bewusst sein, dass aus dieser Schreibweise nicht offensichtlich hervorgeht, aus welcher Symmetrischen Gruppe wir kommen. Es könnte die S_4 sein, aber auch beispielsweise die S_6. Sollte es also relevant sein, so sollte man hierbei erwähnen, in welcher S_n diese Elemente gerade betrachtet werden.

Da die Verknüpfung von Bijektionen wieder eine Bijektion ergibt, können die Gruppenaxiome einfach nachgerechnet werden:

G1: für alle $\sigma_1, \sigma_2, \sigma_3 : (\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3)$, da die Verknüpfung von Abbildungen assoziativ ist.

G2: $e = \mathrm{id} = \begin{pmatrix} 1 \cdots n \\ 1 \cdots n \end{pmatrix} = (1) \cdots (n)$

G3: Sei $\sigma \in S_n$: $\sigma \circ \sigma^{-1} = \mathrm{id}$, wobei σ^{-1} die Umkehrabbildung ist, die existiert, weil σ eine Bijektion ist.

G4: Die S_n ist nicht abelsch, was wir an diesem Beispiel erkennen können: $(12) \circ (23) = (123) \neq (132) = (23) \circ (12)$.
Die S_n ist also eine Gruppe, aber im Allgemeinen nicht kommutativ.

Proposition 2.3.3

Eine Gruppe hat die folgenden Eigenschaften:

1. Das neutrale Element e einer Gruppe ist eindeutig bestimmt.
2. Das inverse Element zu $a \in G$ ist eindeutig bestimmt.
3. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ für alle $a, b \in G$.
4. Für $a, b \in G$ hat die Gleichung $a \cdot x = b$ eine eindeutige Lösung in G. Die Gleichung $y \cdot a = b$ hat eine eindeutige Lösung in G. Es gilt $x = a^{-1} \cdot b$ und $y = b \cdot a^{-1}$.

Beweis. Sei G eine Gruppe.

1. Angenommen es gibt zwei neutrale Elemente e_1, e_2. Dann folgt:
$$e_1 \overset{G2}{=} e_1 \circ e_2 \overset{G2}{=} e_2,$$
womit das neutrale Element eindeutig sein muss.
2. Angenommen a_1, a_2 sind Inverse zu $a \in G$. Dann gilt:
$$a_1 = a_1 \circ e \overset{G3}{=} a_1 \circ (a \circ a_2) \overset{G1}{=} (a_1 \circ a) \circ a_2 \overset{G3}{=} e \circ a_2 = a_2.$$
Das Inverse eines Elementes ist also eindeutig.
3. Beim Invertieren dreht sich die Reihenfolge um:
$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ ((a^{-1} \circ a) \circ b) = b^{-1} \circ (e \circ b) = b^{-1} \circ b = e.$$
Also muss $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. Wer Probleme hat sich dies zu merken oder dies nicht intuitiv findet, sollte sich folgendes Beispiel vor Augen führen: Wenn Sie sich morgens anziehen, um das Haus zu verlassen, dann ziehen Sie sich zuerst Ihre Kleidung an und danach Ihre Jacke. Kommen Sie jedoch nach Hause, dann ziehen Sie zuerst Ihre Jacke aus und dann Ihre restliche Kleidung.
4. Folgt sofort aus 2.

□

Wir haben jetzt Eigenschaften von Gruppen für sich betrachtet. Der nächste Schritt ist die Betrachtung der Beziehungen verschiedener Gruppen untereinander. Dies führt uns zum Begriff **strukturerhaltender Abbildungen**.

Definition 2.3.4

Es sei $\phi : G_1 \longrightarrow G_2$ eine Abbildung zwischen zwei Gruppen $(G_1, \cdot_{G_1})$ und $(G_2, \cdot_{G_2})$. Dann heißt ϕ **Gruppenhomomorphimus** falls für alle $g_1, g_2 \in G_1$:

$$\phi(g_1 \cdot_{G_1} g_2) = \phi(g_1) \cdot_{G_2} \phi(g_2).$$

Der **Kern** von ϕ ist die Menge

$$\mathrm{Ker}(\phi) := \{g \in G_1 \mid \phi(g) = e_{G_2}\}.$$

Ein bijektiver (resp. surjektiver bzw injektiver) Gruppenhomomorphismus heißt **Isomorphismus** (resp. **Epimorphismus** bzw. **Monomorphismus**).

Gruppenhomomorphismen sind strukturerhaltende Abbildungen, weil die Struktur des Verknüpfens erhalten wird. Es macht keinen Unterschied, ob vor dem Verknüpfen oder nach dem Verknüpfen abgebildet wird.

Beispiel 2.3.5

1. $e^x = \exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot) : x \mapsto \exp(x)$
   Es handelt sich dabei tatsächlich um einen Gruppenhomomorphismus, denn es gilt für alle $x, y \in \mathbb{R}$

   $$\exp(x + y) = \exp(x) \cdot \exp(y)$$

   sowie

   $$\exp(x) > 0$$

   und

   $$\exp(0) = 1$$

   Der Ausdruck $x+y$ findet noch in $(\mathbb{R}, +)$ statt und $\exp(x)\cdot\exp(y)$ in $(\mathbb{R}^*, \cdot)$, wobei die neutralen Elemente 0 und 1 sind.

   Die Abbildung ist injektiv, aber nicht surjektiv, da das Bild nur positive Zahlen enthält. Also ist $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ ein Monomorphismus.

   Würden wir aber $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*_+, \cdot)$ betrachten, dann wäre exp bijektiv und damit ein Isomorphismus.

2. $\mathrm{sgn} : (S_n, \circ) \to (\{1, -1\}, \cdot) : \sigma \mapsto \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$
   Man nennt diese Abbildung das Signum. Es wird Bestandteil einer Übungsaufgabe sein zu zeigen, dass das Signum ein Gruppenhomomorphismus ist. Zum Verständnis erarbeiten wir eine zweite Definition. Den geneigten Lesenden ist dann überlassen zu zeigen, dass die beiden Definitionen übereinstimmen.

   Wir beginnen mit dem Begriff der Fehlstellung. Man spricht davon, dass in einer Bijektion $\sigma \in S_n, n \in \mathbb{N}$, eine Fehlstellung vorliegt genau dann, wenn für zwei $i, j \in \{1, ..., n\}$ mit $i < j$ gilt, dass $\sigma(i) > \sigma(j)$, also wenn die betrachtete Bijektion das Ordnungsverhältnis zwischen den Argumenten in den Bildern umkehrt.

Damit definiert man nun das Signum zu für alle $n \in \mathbb{N}$ für alle $\sigma \in S_n$:

$$\operatorname{sgn}(\sigma) := (-1)^k \text{ mit } k = \#(\text{Fehlstellungen in } \sigma).$$

Für die Beispiele zur symmetrischen Gruppe weiter oben gilt $k_1 = 1$, $k_2 = 0$ und $k_3 = 6$, womit:

$$\begin{aligned}\operatorname{sgn}(\sigma_1) &= (-1)^1 = -1,\\ \operatorname{sgn}(\sigma_2) &= (-1)^0 = 1,\\ \operatorname{sgn}(\sigma_3) &= (-1)^6 = 1.\end{aligned}$$

Wie man an diesen Beispielen direkt sehen kann, ist das Signum für $n \geq 3$ nicht bijektiv, weil es nicht injektiv ist. Für $n \geq 2$ gibt es in S_n immer die Identität und mindestens eine Bijektion mit genau einer Fehlstellung (nur 1 und 2 vertauschen). Damit werden aber mit dem Signum 1 und -1 getroffen, d.h. für $n \geq 2$ ist das Signum surjektiv, also ein Epimorphismus.

Definition 2.3.6

Es seien G, H Gruppen, dann bezeichnen wir mit $\operatorname{Hom}(G, H)$ die Menge aller Gruppenhomomorphismen von G nach H. Für die Menge aller Gruppenhomomorphismen von G nach G werden wir die Notation $\operatorname{End}_{\mathbb{Z}}(G)$ verwenden.

Proposition 2.3.7

Es seien G eine Gruppe und H eine abelsche Gruppe, dann ist $\operatorname{Hom}(G, H)$ eine abelsche Gruppe mit der Verknüpfung

$$+ : \operatorname{Hom}(G, H) \times \operatorname{Hom}(G, H) \longrightarrow \operatorname{Hom}(G, H)$$

gegeben durch

$$(\phi, \psi) \mapsto (\phi + \psi) : G \longrightarrow H,\ g \mapsto (\phi + \psi)(g) := \phi(g) +_H \psi(g).$$

Hier ist $+_H$ die Verknüpfung in H. Das neutrale Element ist hier $\phi_0 \in \operatorname{Hom}(G, H)$ mit $\phi(g) = 0_H$ für alle $g \in G$.

Beweis. Wir rechnen zunächst nach, dass die Addition wohldefiniert ist, also $f_1 + f_2 \in \operatorname{Hom}(G, H)$ falls, $f_1, f_2 \in \operatorname{Hom}(G, H)$. Dafür seien $g_1, g_2 \in G$, dann gilt

$$(f_1+f_2)(g_1 \circ_G g_2) = f_1(g_1 \circ_G g_2) +_H f_2(g_1 \circ_G g_2) = (f_1(g_1) +_H f_1(g_2)) +_H (f_2(g_1) +_H f_2(g_2)).$$

Jetzt nutzen wir aus, dass H eine abelsche Gruppe ist und erhalten

$$\begin{aligned}(f_1(g_1) +_H f_1(g_2)) +_H (f_2(g_1) +_H f_2(g_2)) &= (f_1(g_1) +_H f_2(g_1)) +_H (f_1(g_2) +_H f_2(g_2))\\ &= (f_1 + f_2)(g_1) +_H (f_1 + f_2)(g_2)\end{aligned}$$

Nun müssen wir noch die Gruppenaxiome nachrechnen:

G1: Es ist für alle $g \in G$ und $f_1, f_2, f_3 \in \mathrm{Hom}(G,H)$:

$$\begin{aligned}(f_1 + (f_2 + f_3))(g) &= f_1(g) + (f_2 + f_3)(g) \\ &= f_1(g) + (f_2(g) + f_3(g)) \\ &= (f_1(g) + f_2(g)) + f_3(g) \\ &= ((f_1 + f_2) + f_3)(g)\end{aligned}$$

G2 : Es ist für alle $f \in \mathrm{Hom}(G,H)$, $g \in G$:

$$(\phi_0 + f)(g) = \phi_0(g) + f(g) = 0_H + f(g) = f(g) = (f + \phi_0)(g).$$

G3 : Es sei $f \in \mathrm{Hom}(G,H)$ und wir definieren $(-f)(g) := -(f(g))$, wobei hiermit das additiv inverse Element in H gemeint ist. Dann ist $-f \in \mathrm{Hom}(G,H)$, denn

$$(-f)(g_1 + g_2) = -(f(g_1) + f(g_2)) = -f(g_1) - f(g_2) = (-f)(g_1) + (-f)(g_2)$$

und

$$(f + (-f))(g) = f(g) - f(g) = 0_H = \phi_0(g) = ((-f) + f)(g).$$

G4 : Es seien $f_1, f_2 \in \mathrm{Hom}(G,H)$ und $g \in G$, dann ist

$$(f_1 + f_2)(g) = f_1(g) + f_2(g) = f_2(g) + f_1(g) = (f_2 + f_1)(g).$$

□

Bemerkung 2.3.8

Dazu einige Bemerkungen

1. Überlegen Sie sich, wieso wir auf G keine abelsche Struktur benötigen, aber umgekehrt, wenn H nicht abelsch ist, dann $\mathrm{Hom}(G,H)$ mit der obigen Operation i.A. keine Gruppe ist.
2. Für eine abelsche Gruppe G, ist dann $\mathrm{End}_{\mathbb{Z}}(G)$ eine abelsche Gruppe.
3. Das $\mathbb{Z}$ im Index von $\mathrm{End}_{\mathbb{Z}}(G)$ werden wir im Kapitel über Moduln erläutern, die Endomorphismen einer abelschen Gruppe sind genau die $\mathbb{Z}$-Modul-Endomorphismen.

Proposition 2.3.9

Sei $\phi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus, dann gelten

1. $\phi(e_1) = e_2$.
2. $\phi(a^{-1}) = (\phi(a))^{-1}$ für alle $a \in G_1$.
3. Falls ϕ bijektiv ist, so ist $\phi^{-1} : G_2 \longrightarrow G_1$ (die Umkehrabbildung) ebenfalls ein Gruppenhomomorphismus
4. Sei $\psi : G_2 \longrightarrow G_3$ ein weiterer Gruppenhomomorphimus, dann ist auch $\psi \circ \phi : G_1 \longrightarrow G_3$ ein Gruppenhomomorphimus.

Beweis (Proposition 2.3.9): Seien $\phi : G_1 \to G_2$, $\psi : G_2 \to G_3$ Gruppenhomomorphismen. Aus Gründen der Übersichtlichkeit lassen wir weg, welche der Gruppenstrukturen wir gerade nutzen, da dies aus dem Kontext folgt:

1. z.z.: $\phi(e_1) = e_2$
   Sei $a \in G_1$:
   $$\begin{aligned} e_2 &= (\phi(a))^{-1} \circ \phi(a) = (\phi(a))^{-1} \circ \phi(a \circ e_1) \\ &= (\phi(a))^{-1} \circ (\phi(a) \circ \phi(e_1)) \\ &= ((\phi(a))^{-1} \circ \phi(a)) \circ \phi(e_1) \\ &= e_2 \circ \phi(e_1) = \phi(e_1) \end{aligned}$$

2. z.z.: für alle $a \in G_1$: $(\phi(a))^{-1} = \phi(a^{-1})$
   Sei $a \in G_1$:
   $$e_2 = \phi(e_1) = \phi(a^{-1} \circ a) = \phi(a^{-1}) \circ \phi(a)$$
   Damit muss aber wegen der Eindeutigkeit des Inversen
   $\phi(a^{-1}) = (\phi(a))^{-1}$.

3. Es sei ϕ bijektiv, ϕ^{-1} die Umkehrabbildung und $x, y \in G_2$. Es ist, da ϕ ein Gruppenhomomorphismus ist:
   $$\phi(\phi^{-1}(x) \circ \phi^{-1}(y)) = \phi(\phi^{-1}(x)) \circ \phi(\phi^{-1}(y)) = x \circ y$$
   Da ϕ injektiv ist, folgt damit
   $$\phi^{-1}(x) \circ \phi^{-1}(y) = \phi^{-1}(x \circ y).$$

4. z.z.: $\psi \circ \phi$ ist Gruppenhomomorphismus
   Seien $a, b \in G_1$:
   $$\psi(\phi(a \circ b)) \overset{\phi \text{ GH.}}{=} \psi(\phi(a) \circ \phi(b)) \overset{\psi \text{ GH.}}{=} \psi(\phi(a)) \circ \psi(\phi(b))$$

□

Bemerkung 2.3.10

Insbesondere ist auch $\mathrm{End}_{\mathbb{Z}}(G)$ für jede abelsche Gruppe G wiederum eine abelsche Gruppe.

Definition 2.3.11

Eine Teilmenge H von G heißt **Untergruppe** von G, wenn folgende Axiome erfüllt sind:

U1 $a, b \in H \Longrightarrow a \cdot b \in H$ (abgeschlossen unter $\cdot$).

U2 $e \in H$.

U3 $a \in H \Longrightarrow a^{-1} \in H$ (abgeschlossen unter Inversen).

Wir nutzen als Notation für eine Untergruppe auch $(H, \cdot) \subset (G, \cdot)$.

Beispiel 2.3.12

1. $(m\mathbb{Z}, +) \subset (\mathbb{Z}, +)$
   Dabei ist $m\mathbb{Z} := \{a \in \mathbb{Z} | a = l \cdot m \text{ für ein } l \in \mathbb{Z}\}$. Für $m = 3$ also: $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Man zeigt nun, dass $(m\mathbb{Z}, +)$ tatsächlich eine Untergruppe ist.

   U1: $a_1 = l_1 \cdot m$, $a_2 = l_2 \cdot m$. Dann ist

   $$a_1 + a_2 = l_1 \cdot m + l_2 \cdot m = (l_1 + l_2) \cdot m \in m\mathbb{Z}$$

   U2: $0 \in m\mathbb{Z}$, da $0 = 0 \cdot m$.

   U3: Sei $a = l \cdot m \in m\mathbb{Z}$. Dann folgt:

   $$-a = -(l \cdot m) = (-l) \cdot m \in m\mathbb{Z}$$

2. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$
   Also $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$. Es ist klar, dass die Untergruppenaxiome erfüllt sind.

3. $(S_n, \circ) \subset (S_{n+1}, \circ)$
   Man kann S_n in S_{n+1} einbetten, indem man eine beliebige Bijektion aus S_n so erweitert, dass $n + 1$ auf $n + 1$ abgebildet wird. Da S_n selber eine Gruppe ist, ist S_n insbesondere eine Untergruppe von S_{n+1}.

   $$\sigma \mapsto \sigma \circ (n + 1)$$

Proposition 2.3.13

Es sei $\phi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus.

1. $\mathrm{Ker}(\phi)$ ist eine Untergruppe von G_1.
2. $\mathrm{Im}(\phi)$ ist eine Untergruppe von G_2.
3. ϕ ist injektiv $\Leftrightarrow \mathrm{Ker}(\phi) = \{e_1\}$.

Beweis (Proposition 2.3.13). Sei $\phi : G_1 \to G_2$ ein Gruppenhomomorphismus.

1. U1: Seien $a, b \in \mathrm{Ker}\,\phi$ d.h. $\phi(a) = e_2 = \phi(b)$. Damit gilt:

   $$\phi(a \circ b) = \phi(a) \circ \phi(b) = e_2 \circ e_2 = e_2,$$

   also $a \circ b \in \mathrm{Ker}\,\phi$.

   U2: Es gilt nach Proposition 2.3.9: $\phi(e_1) = e_2$, womit $e_1 \in \mathrm{Ker}\,\phi$.

   U3: Sei $a \in \mathrm{Ker}\,\phi$.

   $$\phi(a^{-1}) = (\phi(a))^{-1} = (e_2)^{-1} = e_2.$$

   Damit $a^{-1} \in \mathrm{Ker}\,\phi$.

   Also ist $\mathrm{Ker}\,\phi$ eine Untergruppe von G_1.

2. Zur Erinnerung: $\mathrm{Im}\,\phi = \{x \in G_2 | \exists\, a \in G_1 : \phi(a) = x\}$

U1: Seien $x, y \in \operatorname{Im}\phi$. Dann gibt es $a_1, a_2 \in G_1$ mit $\phi(a_1) = x$ und $\phi(a_2) = y$. Dann gilt:

$$x \circ y = \phi(a_1) \circ \phi(a_2) = \phi(a_1 \circ a_2).$$

Da $a_1 \circ a_2 \in G_1$, ist $x \circ y \in \operatorname{Im}\phi$.

U2: Es gilt nach Proposition 2.3.9: $\phi(e_1) = e_2$, womit $e_2 \in \operatorname{Im}\phi$.

U3: Sei $x \in \operatorname{Im}\phi$. Dann gibt es $a \in G_1$ mit $\phi(a) = x$.

$$x^{-1} = (\phi(a))^{-1} = \phi(a^{-1})$$

Da $a^{-1} \in G_1$, ist $x^{-1} \in \operatorname{Im}\phi$.

3.
- "$\Rightarrow$" Sei ϕ injektiv. Dann:

$$\text{für alle } a \in \operatorname{Ker}\phi : \phi(a) = e_2 = \phi(e_1) \overset{\phi \text{ inj.}}{\Rightarrow} a = e_1.$$

Damit muss $\operatorname{Ker}\phi = \{e_1\}$.

- "$\Leftarrow$" Sei $\operatorname{Ker}\phi = \{e_1\}$.
Angenommen es gibt $a, b \in G_1$ mit $\phi(a) = \phi(b)$. Dann

$$e_2 = \phi(a) \circ (\phi(a))^{-1} = \phi(a) \circ (\phi(b))^{-1} = \phi(a \circ b^{-1}).$$

Also $a \circ b^{-1} \in \operatorname{Ker}\phi$. Damit gilt aber

$$e_1 = a \circ b^{-1} \Leftrightarrow a = e_1 \circ b = b.$$

Da a und b beliebig waren, ist ϕ injektiv.

□

Insbesondere die dritte Aussage macht uns klar, wie rigide ein Gruppenhomomorphismus ist. Anstatt die Injektivität für alle Urbilder zu untersuchen, reicht es uns, dass Urbild des neutralen Elementes zu untersuchen. Tatsächlich sehen wir später, dass wir mit Hilfe des Kerns und einem Element des Urbilds, schon immer das ganze Urbild kennen. Das erinnert uns daran, dass die Lösungen eines inhomogenen Gleichungssystems aus einer speziellen Lösungen und den ganzen Lösungen des zugehörigen homogenen Gleichungssystems zusammengesetzt sind.

Wir nutzen Untergruppen zur Definition von Äquivalenzrelationen auf einer Gruppe.

Definition 2.3.14

Es sei G eine Gruppe, H eine Untergruppe von G. Für $g_1, g_2 \in G$ definieren wir

$$g_1 \equiv g_2 (\operatorname{mod} H) :\Leftrightarrow g_1 (g_2)^{-1} \in H.$$

Wir sagen, dass g_1 **kongruent zu** g_2 ist **modulo** H.

Beispiel 2.3.15

1. $G = (\mathbb{Q}, +), H = (\mathbb{Z}, +)$

$$\begin{aligned} g_1 \equiv g_2 \mod H &\Leftrightarrow g_1 \circ (g_2)^{-1} \in H \\ &\Leftrightarrow g_1 + (g_2)^{-1} \in \mathbb{Z} \\ &\Leftrightarrow g_1 - g_2 \in \mathbb{Z} \end{aligned}$$

   In diesem Beispiel sind also zwei rationale Zahlen genau dann kongruent, wenn sie sich um eine ganze Zahl unterscheiden. So wären zum Beispiel $\frac{1}{4}$ und $\frac{5}{4}$ kongruent $\mod \mathbb{Z}$ zueinander.

2. $(\mathbb{Q}, +) \subset (\mathbb{R}, +)$
   Dieses Beispiel funktioniert analog zum ersten Beispiel.

3. $H = (m\mathbb{Z}, +) \subset (\mathbb{Z}, +) = G$

$$g_1 \equiv g_2 \mod H \Leftrightarrow g_1 - g_2 \in m\mathbb{Z}.$$

   Kongruenz bezüglich H bedeutet in diesem Fall also, dass die Differenz zweier Elemente durch m teilbar ist. Das bedeutet also, dass zwei Elemente genau dann kongruent zueinander sind, wenn diese den gleichen Rest bezüglich Division durch m haben. Deshalb nennt man in diesem Fall die Kongruenzklassen auch Restklassen.

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &= \{[a] | a \in \mathbb{Z}\} \\ [a] &= \{x \in \mathbb{Z} : x \equiv a \mod m\mathbb{Z}\} \\ &= \{x \in \mathbb{Z} : m | (x - a)\} \end{aligned}$$

4. $H = 3\mathbb{Z}, G = \mathbb{Z}$

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &= \{[0], [1], [2]\} \\ [0] &= \{0, \pm 3, \pm 6, \pm 9, \ldots\} \\ [1] &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, ...\} \\ [2] &= \{\ldots, -4, 1, 2, 5, 8, \ldots\} \\ [3] &= [0] \end{aligned}$$

Proposition 2.3.16

Die Kongruenz modulo H ist eine Äquivalenzrelation. Wir schreiben G/H für die Menge der Äquivalenzklassen.

Beweis. Seien G Gruppe, H Untergruppe
und $g_1, g_2, g_3 \in G$.

Reflexivität: $g_1 \circ (g_1)^{-1} = e \in H \Rightarrow g_1 \equiv g_1 \mod H$

Symmetrie:

$$\begin{aligned} g_1 \equiv g_2 \mod H &\Rightarrow g_1 \circ (g_2)^{-1} \in H \\ &\overset{H \text{ UG.}}{\Rightarrow} g_2 \circ (g_1)^{-1} = (g_1 \circ (g_2)^{-1})^{-1} \in H \Rightarrow g_2 \equiv g_1 \mod H \end{aligned}$$

Transitivität:

$$\begin{aligned} &(g_1 \equiv g_2 \mod H) \wedge (g_2 \equiv g_3 \mod H) \\ &\Rightarrow (g_1 \circ (g_2)^{-1} \in H) \wedge (g_2 \circ (g_3)^{-1} \in H) \\ &\overset{H \text{ UG.}}{\Rightarrow} g_1 \circ (g_3)^{-1} = (g_1 \circ (g_2)^{-1}) \circ (g_2 \circ (g_3)^{-1}) \in H \\ &\Rightarrow g_1 \equiv g_3 \mod H \end{aligned}$$

□

Proposition 2.3.17

Sei G eine abelsche Gruppe. Dann ist G/H eine abelsche Gruppe mit der Verknüpfung

$$+ : G/H \times G/H \longrightarrow G/H, ([g_1], [g_2]) \mapsto [g_1] + [g_2] := [g_1 + g_2].$$

Beweis. Sei G eine abelsche Gruppe und H eine Untergruppe.

G0: Wir müssen prüfen, ob die definierte Addition überhaupt wohldefiniert ist, d.h. unabhängig von der Wahl der Vertreter. Seien dafür $[g_1], [g_2] \in G/H$ und $a \in [g_1]$,$b \in [g_2]$. Zu zeigen ist also, dass

$$[a + b] = [g_1 + g_2]$$

Da $a \in [g_1]$ und $b \in [g_2]$,

$$\begin{aligned} a \equiv g_1 \mod H &\Leftrightarrow a - g_1 \in H \Rightarrow \exists c_1 \in H : a - g_1 = c_1 \\ b \equiv g_2 \mod H &\Leftrightarrow b - g_2 \in H \Rightarrow \exists c_2 \in H : b - g_2 = c_2 \end{aligned}$$

Damit gilt,

$$\begin{aligned} (a + b) - (g_1 + g_2) = a + b - g_2 - g_1 &\overset{G \text{ abelsch}}{=} (a - g_1) + (b - g_2) \\ &= c_1 + c_2 \in H \\ &\Rightarrow a + b \equiv g_1 + g_2 \mod H \\ &\Rightarrow [a + b] = [g_1 + g_2] \end{aligned}$$

G1:

$$\begin{aligned} \text{für alle } [g_1], [g_2], [g_3] \in G/H : ([g_1] + [g_2]) + [g_3] &= [g_1 + g_2] + [g_3] \\ &= [(g_1 + g_2) + g_3] = [g_1 + (g_2 + g_3)] \\ &= [g_1] + [g_2 + g_3] = [g_1] + ([g_2] + [g_3]) \end{aligned}$$

G2: für alle $[g] \in G/H : [g] + [e] = [g + e] = [e + g] = [e] + [g] = [e + g] = [g]$

G3: für alle $[g] \in G/H : [g] + [-g] = [g + (-g)] = [e] = [-g + g] = [-g] + [g]$

G4: für alle $[g_1], [g_2] \in G/H : [g_1] + [g_2] = [g_1 + g_2] = [g_2] + [g_1]$

□

Lemma 2.3.18

Es sei G eine abelsche Gruppe, $H \subseteq G$ eine Untergruppe. Die Abbildung

$$\pi : G \longrightarrow G/H, g \mapsto [g]$$

ist ein surjektiver Gruppenhomomorphimus mit $\mathrm{Ker}(\pi) = H$.

Beweis. Sei G abelsche Gruppe und H Untergruppe.

- Gruppenhomomorphismus:

$$\begin{aligned} \text{für alle } g_1, g_2 \in G/H : \pi(g_1 + g_2) &= [g_1 + g_2] = [g_1] + [g_2] \\ &= \pi(g_1) + \pi(g_2) \end{aligned}$$

- Epimorphismus: Sei $[g] \in G/H$ und $a \in [g]$. Dann $\pi(a) = [a] = [g]$, womit π surjektiv ist.

- $\mathrm{Ker}\,\pi = H$:

$$\begin{aligned} a \in \mathrm{Ker}\,\pi \Leftrightarrow [a] = \pi(a) = e_{G/H} = [e_G] \Leftrightarrow a \equiv e_G \mod H \\ \Leftrightarrow a = a + e = a + (-e) \in H \end{aligned}$$

□

Beispiel 2.3.19

Wir betrachten die Untergruppe $m\mathbb{Z} \subseteq \mathbb{Z}$, dann erhalten wir den Gruppenhomomorphismus $\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]$.

Korollar 2.3.20

$\mathbb{Z}/m\mathbb{Z}$ ist eine abelsche Gruppe für jedes $m \in \mathbb{Z}^*$ und besteht aus m paarweise verschiedenen Restklassen.

Beweis (Korollar 2.3.20). Es wurde bereits gezeigt, dass für alle $m \in \mathbb{Z}$ die Menge $m\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ ist. Da $\mathbb{Z}$ abelsch ist, gilt nach Proposition 2.3.17, dass $\mathbb{Z}/m\mathbb{Z}$ abelsch ist. Wir haben außerdem in Proposition 2.2.12 gesehen, dass es genau m Äquivalenzklassen gibt. □

2.3.2 Bonus: Normalteiler

Wir möchten nun die Frage klären, wann auch nicht abelsche Gruppen modulo einer Untergruppe wieder eine Gruppe bilden. Dafür führen wir den Begriff des Normalteilers ein.

Wann ist G/H eigentlich wieder eine Gruppe mit $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$?

Definition 2.3.21

Eine Untergruppe $N \subseteq G$ heißt **Normalteiler** von G, falls für alle $g \in G$ gilt:

$$\{g \cdot n \mid n \in N\} =: gN = Ng := \{n \cdot g \mid n \in N\}.$$

Beispiel 2.3.22

Wir lernen eine weitere Untergruppe der S_n für $n \geq 2$ kennen. Es handelt sich dabei um die sogenannte alternierende Gruppe

$$A_n := \{\sigma \in S_n | \operatorname{sgn}(\sigma) = 1\}$$

Es sei den geneigten Lesenden überlassen, die Untergruppenaxiome nachzuweisen. Wir rechnen nun nach, dass es sich bei A_n um einen Normalteiler von S_n handelt. Es ist also zu zeigen, dass

$$\text{für alle } \sigma \in S_n : \sigma A_n = A_n \sigma$$

Sei dazu $\sigma \in S_n$:

- "$\subset$" Sei $\tau \in A_n$. Damit $\sigma \circ \tau$ in $A_n\sigma$ liegt, müssen wir ein $\tau' \in A_n$ finden, sodass
$$\sigma \circ \tau = \tau' \circ \sigma$$
Es liegt nahe,
$$\tau' = \sigma \circ \tau \circ \sigma^{-1}$$
anzusetzen. Es bleibt dabei noch zu zeigen, dass $\tau' \in A_n$. Dafür nutzen wir aus, dass das Signum ein Gruppenhomomorphismus ist:
$$\begin{aligned}
\operatorname{sgn}(\tau') &= \operatorname{sgn}(\sigma \circ \tau \circ \sigma^{-1}) \\
&= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma^{-1}) \\
&= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma^{-1}) \cdot \operatorname{sgn}(\tau) \\
&= \operatorname{sgn}(\sigma \circ \sigma^{-1}) \cdot 1 \\
&= \operatorname{sgn}(\mathrm{id}) \\
&= 1
\end{aligned}$$
Also ist $\tau' \in A_n$, womit $\sigma \circ \tau \in A_n\sigma$.
- "$\supset$" Erfolgt analog.

Satz 2.3.23

Sei N ein Normalteiler von G, dann ist G/N mit obiger Verknüpfung eine Gruppe.

Beweis (Satz 2.3.2): Sei G eine Gruppe und $N \subset G$ ein Normalteiler in G.

G0: Man prüft wieder Vertreterunabhängigkeit der Verknüpfung. Seien dafür $[g], [h] \in G/N$, $a \in [g]$ und $b \in [h]$. Es gilt
$$\begin{aligned}
a \circ g^{-1} &\in N \\
b \circ h^{-1} &\in N \\
(a \circ b) \circ (g \circ h)^{-1} &= a \circ (b \circ h^{-1}) \circ g^{-1} \\
&= a \circ g^{-1} \circ g \circ (b \circ h^{-1}) \circ g^{-1}
\end{aligned}$$

Man untersucht nun $g \circ (b \circ h^{-1}) \circ g^{-1}$: Per Definition ist $b \circ h^{-1} \in N$. Damit ist $(b \circ h^{-1}) \circ g^{-1} \in Ng^{-1}$. Da N ein Normalteiler ist, ist $Ng^{-1} = g^{-1}N$, womit $g \circ (b \circ h^{-1}) \circ g^{-1} \in N$. Damit ist

$$\begin{aligned}&(a \circ b) \circ (g \circ h)^{-1} \in N\\ \Rightarrow\ &a \circ b \equiv g \circ h \mod N\end{aligned}$$

G1-G3: Die Nachweise können analog zu dem Beweis von Proposition 2.3.17 geführt werden.

Also ist G/N eine Gruppe. □

Satz 2.3.24

Sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus, dann gilt:

1. $\operatorname{Ker}\varphi$ ist ein Normalteiler von G.
2. φ induziert einen Isomorphismus von Gruppen $\overline{\varphi} : G/\operatorname{Ker}\varphi \longrightarrow \operatorname{Im}(\varphi), [g] \mapsto \varphi(g)$.

Beweis (Satz 2.3.2): Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.

1. Sei $g \in G$. Es ist zu zeigen, dass $g \operatorname{Ker}\varphi = (\operatorname{Ker}\varphi)g$.
   - "$\subset$" Sei $x \in \operatorname{Ker}\varphi$. Man setzt $x' := g \circ x \circ g^{-1}$ an für $g \circ x = x' \circ g$. Man prüft $x' \in \operatorname{Ker}\varphi$:
   $$\begin{aligned}\varphi(x') &= \varphi(g \circ x \circ g^{-1})\\ &= \varphi(g) \circ \varphi(x) \circ \varphi(g^{-1})\\ &= \varphi(g) \circ e_H \circ \varphi(g^{-1})\\ &= \varphi(g \circ g^{-1})\\ &= \varphi(e_G)\\ &= e_H\end{aligned}$$
   - "$\supset$" Analog.

   Es ist also $g \operatorname{Ker}\varphi = (\operatorname{Ker}\varphi)g$, womit $\operatorname{Ker}\varphi$ ein Normalteiler ist.

2. - Wohldefiniertheit: Da $\operatorname{Ker}\varphi$ ein Normalteiler ist, ist $G/\operatorname{Ker}\varphi$ eine Gruppe. $\operatorname{Im}\varphi$ ist nach Proposition 2.3.13 auch eine Gruppe. Bleibt also nur noch die Vertreterunabhängigkeit von $\overline{\varphi}$ zu zeigen. Seien dafür $[g] \in G/\operatorname{Ker}\varphi$ und $a \in [g]$. Dann
   $$\begin{aligned}&a \equiv g \mod \operatorname{Ker}\varphi\\ \Leftrightarrow &a \circ g^{-1} \in \operatorname{Ker}\varphi,\end{aligned}$$
   womit
   $$\begin{aligned}\overline{\varphi}([a]) &= \varphi(a) = \varphi(a \circ g^{-1} \circ g)\\ &= \varphi(a \circ g^{-1}) \circ \varphi(g) = e_H \circ \varphi(g)\\ &= \varphi(g) = \overline{\varphi}([g]).\end{aligned}$$
   Also ist $\overline{\varphi}$ vertreterunabhängig.

- Injektivität: Sei $[g] \in \operatorname{Ker} \overline{\varphi}$. Dann

$$e_H = \overline{\varphi}([g]) = \varphi(g),$$

  womit $g \in \operatorname{Ker} \varphi$. Damit

$$g \equiv e_G \mod \operatorname{Ker} \varphi \Rightarrow [g] = [e_G] = e_{G/\operatorname{Ker} \varphi}.$$

  Also ist $\overline{\varphi}$ injektiv.
- Surjektivität: Es gilt

$$\begin{aligned} \operatorname{Im} \varphi &= \{h \in H | \exists g \in G : \ \varphi(g) = h\} \\ &= \{h \in H | \exists [g] \in G/\operatorname{Ker} \varphi : \ \overline{\varphi}([g]) = \varphi(g) = h\} \\ &= \operatorname{Im} \overline{\varphi}. \end{aligned}$$

Insgesamt ist $\overline{\varphi}$ ein Isomorphismus.

□

Der Isomorphiesatz wird sich für uns noch an vielen Stellen sehr nützlich erweisen. Wir merken uns hier, dass die Normalteiler einer Gruppe G genau die möglichen Kerne von Gruppenhomomorphismen $G \longrightarrow H$ sind.

2.3.3 Ringe

Definition 2.3.25

Ein **Ring** (genauer ein **Ring mit Eins**) ist eine Menge R mit zwei inneren Verknüpfungen $+, \cdot$ so, dass $(R, +)$ eine abelsche Gruppe ist und $\cdot$ eine assoziative Verknüpfung für R mit einem neutralen Element (**Einselement**, das bezeichnen wir mit 1) ist. Es sollen für alle $a, b, c \in R$ gelten:

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$.

D2 $(b + c) \cdot a = b \cdot a + c \cdot a$.

Das neutrale Element bezüglich der Addition $+$ bezeichnen wir mit 0 und das Inverse von a mit $-a$. Wir schreiben $a - b$ für $a + (-b)$.

Beispiel 2.3.26

Einige Beispiele

1. $(\mathbb{Z}, +, \cdot)$

   (a) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.
   (b) Die Multiplikation ganzer Zahlen ist assoziativ.
   (c) Das Einselement ist in diesem Fall die bereits bekannte 1. Denn es gilt $a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Z}$.

(d) Es gilt für alle $a, b, c \in \mathbb{Z}$:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

2. $(Z/mZ, +, \cdot)$

   (a) $(Z/mZ, +)$ ist eine abelsche Gruppe

   (b) Man definiert die multiplikative Verknüpfung zu

   $$\cdot_{Z/mZ} : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$
   $$([a], [b]) \mapsto [a \cdot b]$$

   Wie immer muss bei Definition über Repräsentanten die Wohldefiniertheit gezeigt werden. In diesem Fall haben wir das schon in Lemma 2.2.2 gezeigt.

   (c) $1_{(Z/mZ,+,\cdot)} = [1]$

   (d) Man führt Assoziativität und die Distributivgesetze auf die Repräsentanten zurück.

3. $(\{0\}, +, \cdot)$ mit $0 \in \mathbb{Z}$.

   (a) $(\{0\}, +)$ ist eine Gruppe.

   (b) Die Addition und Multiplikation sind hier die gleichen Abbildungen, und die Distributivgesetze lassen sich sofort verifizieren.

4. Es seien $(R, +, \cdot)$ und $(S, +, \cdot)$ zwei Ringe mit Eins, dann ist $R \times S$ (das kartesische Produkt) wieder ein Ring mit Eins, wobei Verknüpfungen gegeben sind durch

   $$(a_1, b_1) + (a_2, b_2)(a_1 + a_2, b_1 + b_2),\ (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

   Die Eigenschaften der abelschen Gruppe haben wir schon in Beispiel 2.3.1 gesehen, die assoziative Verknüpfung folgt ganz analog, $D1$ und $D2$ lassen sich ebenso einfach verifizieren. Das Einselement ist gegeben durch $(1_R, 1_S)$.

Beispiel 2.3.27

Sei $n \geq 1$, dann bilden die $n \times n$-Matrizen über $(\mathbb{Q}, +, \cdot)$ einen Ring, wobei die Multiplikation in Definition 2.1.11 beschrieben wurde und die Addition durch

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix} := \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \dots & a_{nn} + b_{nn} \end{pmatrix}$$

gegeben ist. Das neutrale Element der Addition ist die **Nullmatrix**

$$O = O_n = (a_{i,j}) \text{ mit } a_{i,j} = 0 \ \forall\, i, j$$

und das neutrale Element der Multiplikation ist die **Einheitsmatrix** oder **Einsmatrix**:

$$E_n = (a_{i,j}) \text{ mit } a_{i,j} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

Manchmal schreiben wir dafür auch 1_n.

Definition 2.3.28

Ein Ring R heißt **kommutativ**, falls für alle $a, b \in R$ gilt: $a \cdot b = b \cdot a$.

Beispiel 2.3.29

Die obigen Beispiele $\mathbb{Z}$ und $\mathbb{Z}/mZ$, sowie $\mathbb{Q}$ und $\mathbb{R}$ sind alles kommutative Ringe. Der Ring $\mathbb{Q}^{n\times n}$ ist für $n \geq 2$ nicht kommutativ. Ein weiteres Beispiel für nichtkommutative Ringe sind die $\mathrm{End}_Z(G)$ für eine abelsche Gruppe G sowie die Quaternionen.

Beispiel 2.3.30

Es sei G eine abelsche Gruppe, dann haben wir schon in Proposition 2.3.7 gesehen, dass $\mathrm{End}_{\mathbb{Z}}(G)$ eine abelsche Gruppe ist. Wir definieren noch eine Multiplikation auf $\mathrm{End}_{\mathbb{Z}}(G)$:

$$\mathrm{End}_{\mathbb{Z}}(G) \times \mathrm{End}_{\mathbb{Z}}(G) \longrightarrow \mathrm{End}_{\mathbb{Z}}(G),\ (f_1, f_2) \mapsto (f_1 \circ f_2),$$

der üblichen Verknüpfung von Abbildungen. Diese ist immer assoziativ und die Eins ist in diesem Fall die Identität auf G. Wir müssen also nur die beiden Distributivgesetze nachrechnen, aber das überlassen wir den Lesenden. Ebenfalls überlassen wir den Lesenden nachzuweisen, dass $\mathrm{End}_{\mathbb{Z}}(G)$ im Allgemeinen nicht kommutativ ist.

Beispiel 2.3.31

[Quaternionen] Man betrachtet die Menge

$$\{\pm 1, \pm i, \pm j, \pm k\}$$

mit den Relationen

$$i^2 = j^2 = k^2 = i \cdot j \cdot k = -1$$

Tatsächlich ist das eine Gruppe mit 8 Elemente, aber diese Gruppe ist nicht abelsch denn

$$k \cdot k = k^2 = i \cdot j \cdot k \cdot \Rightarrow k = i \cdot j$$
$$k \cdot j \cdot i = i \cdot j \cdot j \cdot i = 1 = -k^2 \Rightarrow j \cdot i = -k$$

Wir erweitern diese Menge (wie wir später sehen, wählen wir die obigen Elemente als Erzeuger eines reellen Vektorraums) mit reellen Skalaren zu den sogenannten **Quaternionen** erweitern.

$$\mathbb{H} = \mathbb{R} \cdot i + \mathbb{R} \cdot j + \mathbb{R} \cdot k + \mathbb{R}$$

Man zeigt, dass es sich bei $\mathbb{H}$ um einen Ring mit 1 handelt.

1. Die Addition definiert man für alle $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{R}$ als

$$\begin{aligned}&(a_1 \cdot i + a_2 \cdot j + a_3 \cdot k + a_4) + (b_1 \cdot i + b_2 \cdot j + b_3 \cdot k + b_4)\\ &= (a_1 + b_1) \cdot i + (a_2 + b_2) \cdot j + (a_3 + b_3) \cdot k + (a_4 + b_4)\end{aligned}$$

2. Die Gruppeneigenschaften von $(\mathbb{H}, +)$ ergeben sich dabei durch Rückführung auf die einzelnen Komponenten.

3. Die Multiplikation definiert man für alle $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{R}$ als

$$\begin{aligned}&(a_1 \cdot i + a_2 \cdot j + a_3 \cdot k + a_4) \cdot (b_1 \cdot i + b_2 \cdot j + b_3 \cdot k + b_4)\\ =&(a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) \cdot 1\\ &+ (a_1b_2 + a_2b_1 - a_3b_4 - a_4b_3) \cdot i\\ &+ (a_3b_1 + a_1b_3 - a_2b_4 + a_4b_2) \cdot j\\ &+ (a_4b_1 + a_1b_4 + a_2b_3 - a_3b_2) \cdot k\end{aligned}$$

4. Es sei den geneigten Lesenden überlassen, die Assoziativität zu zeigen.

5. Wäre die Multiplikation kommutativ, dann müsste mit obiger Wahl der Skalare gelten

$$\begin{aligned}(a_3b_1 + a_1b_3 - a_2b_4 + a_4b_2) &= (b_3a_1 + b_1a_3 - b_2a_4 + b_4a_2)\\ \Rightarrow -a_2b_4 + a_4b_2 &= -b_2a_4 + b_4a_2\\ \Rightarrow 2 \cdot a_4b_2 &= 2 \cdot b_4a_2\\ \Rightarrow b_2a_4 &= b_4a_2.\end{aligned}$$

   Für beliebige a und b gilt aber natürlich $b_2a_4 \neq b_4a_2$, also ist die Multiplikation nicht kommutativ.

Es ist wichtig anzumerken, dass in Ringen im Allgemeinen für Elemente eines Rings keine multiplikativen Inversen existieren. Das einfachste Beispiel hierzu sind die ganzen Zahlen, hier hat 2 kein multiplikativ Inverses.

Definition 2.3.32

Ein **Körper** ist ein kommutativer Ring K so, dass $K \setminus \{0\}$ mit der Multiplikation als Verknüpfung eine Gruppe ist. Insbesondere ist $0 \neq 1$.

Beispiel 2.3.33

Einige Beispiele zu Körpern

1. $(\mathbb{R}, +, \cdot)$
2. $(\mathbb{Q}, +, \cdot)$
3. $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$

- $(\{[0],[1]\},+,\cdot)$ ist ein kommutativer Ring (nach dem Vorherigen)
- $(\{[1]\},\cdot)$ ist eine Gruppe (die triviale Gruppe)

Das ist der kleinste Körper und wir bezeichnen diesen mit $\mathbb{F}_2$.

Bemerkung 2.3.34

Für einen Ring R gelten die Rechenregeln für alle $a, b, c \in R$:

1. $a \cdot 0 = 0 \cdot a = 0$.
2. Das Einselement ist eindeutig. Wenn $1 = 0$, dann ist $R = \{0\}$.
3. $-a = (-1) \cdot a$.
4. $a \cdot (b - c) = a \cdot b - a \cdot c$ und $(b - c) \cdot a = b \cdot a - c \cdot a$.

Für Gruppen haben wir strukturerhaltender Abbildungen betrachtet, ähnliches wollen wir hier auch machen. Der wichtige Unterschied ist, dass BEIDE Strukturen eines Ringes erhalten bleiben sollen:

Definition 2.3.35

Es seien R und S zwei Ringe mit Eins und $\varphi : R \longrightarrow S$ eine Abbildung. Dann heißt φ ein **Ringhomomorphismus**, falls für alle $a, b, c \in R$ gilt

$$\varphi(a \cdot b + c) = \varphi(a) \cdot \varphi(b) + \varphi(c) \text{ und } \varphi(1_R) = 1_S.$$

Beispiel 2.3.36

Ringhomomorphismen:

1. $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto [a]$. Wir nutzen hier ohne weitere Erwähnung aus, dass die Addition und Multiplikation in $\mathbb{Z}/m\mathbb{Z}$ wohldefiniert, also unabhängig von der Wahl der Repräsentanten ist:
   - $\forall\, a, b, c \in \mathbb{Z}$:
   $$\pi(a \cdot b + c) = [a \cdot b + c] = [a] \cdot [b] + [c] = \pi(a) \cdot \pi(b) + \pi(c)$$
   - $\pi(1) = [1]$, was nach vorherigen Überlegungen das Einselement in $\mathbb{Z}/m\mathbb{Z}$ ist.
2. Wir überlegen uns allgemein welche Bedingungen für $a, b \in \mathbb{Z}$ gelten müssen, damit
   $$\varphi : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z} : [x]_{\mathbb{Z}/a\mathbb{Z}} \mapsto [x]_{\mathbb{Z}/b\mathbb{Z}}$$
   ein wohldefinierter Ringhomomorphismus ist. Man zeigt, dass dies der Fall ist, wenn b ein Teiler von a ist: Sei $c \in [x] \in \mathbb{Z}/a\mathbb{Z}$. Dann gibt es $l \in \mathbb{Z}$, sodass $c = x + l \cdot a$. Gilt nun $b|a$, so folgt, dass $\exists\, k \in \mathbb{Z} : a = k \cdot b$. Also gilt
   $$[c]_{\mathbb{Z}/b\mathbb{Z}} = [x + l \cdot a]_{\mathbb{Z}/b\mathbb{Z}} = [x + l \cdot k \cdot b]_{\mathbb{Z}/b\mathbb{Z}} = [x]_{\mathbb{Z}/b\mathbb{Z}},$$

womit φ wohldefiniert ist.
Ist andererseits b kein Teiler von a, dann finden wir k und r mit ist $a = k \cdot b + r$ und $0 < r < b$. Dann ist

$$\pi([0]) = \pi([a]) = \pi([k \cdot b + r]) = [k \cdot b + r] = [r] \neq [0].$$

Also ist π kein Gruppenhomomorphismus für die Addition, also auch kein Ringhomomorphismus.
Die Ringhomomorphismus-Eigenschaften für den ersten Fall führen wir wie gehabt auch ein Nachrechnen auf Repräsentanten zurück, das ist aber jetzt für uns schon Standard.

3. $\varphi : \mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ ist nach Obigem ein wohldefinierter Homomorphismus.

2.3.4 Polynomring

Wir gehen nun zu einem weiteren grundlegenden Objekt über, mit dem Sie bereits oft Bekanntschaft gemacht haben sollten, dem Polynomring.

Definition 2.3.37

Ein **Polynom** ist eine Folge $(a_i)_{i\in\mathbb{N}_0}$ von Elementen aus einem Körper K, sodass nur endlich viele $a_i \neq 0$. Wir definieren $x := (\delta_{i,1})_{i\in\mathbb{N}_0}$. Die Menge aller Polynome mit Koeffizienten in K bezeichnen wir als $K[x]$.

Bemerkung 2.3.38

Es sei K ein Körper:

1. Wir können Polynome über K mit endlichen Folgen (nur endlich viele Folgeglieder sind ungleich Null) in K identifizieren. Beliebige Folgen würden wir mit Potenzreihen identifizieren.

2. Zwei Polynome $(a_i)_{i\in\mathbb{N}_0}$ und $(b_i)_{i\in\mathbb{N}_0}$ sind per Definition gleich, wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$.

Beispiel 2.3.39

Wir gucken uns nochmal einige Beispiele für Polynome an:

1. Wir betrachten nochmal genauer die Folge, die auch schon in der Definition auftaucht: $\delta_{i,1}$ (Kronecker-Delta), also die Folge

$$(\delta_{i,1})_{i\in\mathbb{N}_0} = (\delta_{0,1}, \delta_{1,1}, \delta_{2,1}, \delta_{3,1}, \ldots) = (0, 1, 0, 0, \ldots)$$

Im Schulunterricht hätte man dieses Polynom einfach mit x identifiziert und so wollen wir diese Folge auch im weiteren nennen.

2. $0 = (0, \ldots)$ (die Null)

3. $1 = (1, 0, 0, \ldots)$ (die Eins, diese Bezeichnung wird mit der nächsten Definition klar)

4. $(-1, 3, 5, 3, -3, 0, 1, 2, 3, 0, \ldots)$
5. $(1, 1, 1, ...)$ ist kein Polynom, da es keinen Index gibt, ab dem alle Einträge der Folge null sind.
6. für alle $\lambda \in K : (\lambda, 0, \ldots)$.

Definition 2.3.40

Es sei K ein Körper und $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0} \in K[x]$. Dann definieren wir zwei Operationen

1. Die **Addition**

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} := (a_i + b_i)_{i\in\mathbb{N}_0} \in K[x]$$

2. Die **Multiplikation** mit der Folge $(c_i)_{i\in\mathbb{N}_0}$

$$c_i := \sum_{k+\ell=i} a_k b_\ell = a_i b_0 + a_{i-1} b_1 + \ldots a_1 b_{i-1} + a_0 b_i.$$

durch

$$(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} := (c_i)_{i\in\mathbb{N}_0} \in K[x].$$

Die Multiplikation ist hier ein **Faltungsprodukt**, ähnliche Konstruktionen werden Sie in der Algebra immer mal wieder sehen.

Bemerkung 2.3.41

Ein $\lambda \in K$ identifizieren wir mit $(\lambda\delta_{i,0})_{i\in\mathbb{N}_0}$. Dann gilt

$$\lambda \cdot (a_i)_{i\in\mathbb{N}_0} = (\lambda a_i)_{i\in\mathbb{N}_0} \in K[x]$$

(die **skalare Muliplikation**).

Beispiel 2.3.42

[Rechnen mit Polynomen] Seien $p = (1, 2, 1, 0, 0, \ldots) = 1 + 2x + x^2 \in \mathbb{R}[x]$ und $q = (3, 1, 0, 0, 0, \ldots) \in \mathbb{R}[x]$.

1. Addition

$$\begin{aligned} p + q &= (1 + 3, 2 + 1, 1 + 0, 0 + 0, \ldots) \\ &= (4, 3, 1, 0, \ldots) \end{aligned}$$

2. Multiplikation

$$\begin{aligned} p \cdot q = (&1 \cdot 3, 2 \cdot 3 + 1 \cdot 1, 1 \cdot 0 + 2 \cdot 1 + 0 \cdot 3, 1 \cdot 0 + 2 \cdot 0 + 1 \cdot 1 + 0 \cdot 3, \\ &1 \cdot 0 + 2 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 3, 0, \ldots) \\ &= (3, 7, 2, 1, 0, \ldots) \end{aligned}$$

Das Rechnen und Beweisen mit solch einer Folgendarstellung ist unhandlich. Deshalb führen wir eine Kurzschreibweise ein, in der unsere Definition $x := (\delta_{i,1})_{i\in\mathbb{N}_0}$ zur Geltung kommt. Dazu überlegen wir uns für $j \geq 1$:

$$\begin{aligned}(x)^j = ((\delta_{i,1})_{i\in\mathbb{N}_0})^j \\ = (\delta_{i,j})_{i\in\mathbb{N}_0}\end{aligned}$$

So können wir jetzt jedes Polynom $p = (a_j)_{j\in\mathbb{N}_0} \in K[x]$ schreiben als

$$p = \sum_{j\in\mathbb{N}_0} a_j x^j.$$

Wir fassen diese Schreibweise allerdings nicht als Abbildung aus, sondern als formalen Ausdruck für die Folge p. Die Schreibweise x^j ist kompatibel mit der j-fachen Multiplikation von x mit sich selbst. Die Notation ist also sinnvoll und formal gesehen nur eine andere Darstellungsweise der Folgen. Jedoch ist diese Darstellungsweise sehr praktisch, weil wir hier mit x rechnen können *wie* mit einer Variablen, ohne dass wir es tatsächlich tun.

Warum nehmen wir überhaupt so eine komplizierte Definition von Polynomen vor? Wo liegt der Unterschied zu der bisher bekannten Definition von Polynomen? In der Schulmathematik bezeichnet man meistens Ausdrücke wie x^4+3x^2-7 als ein Polynom, wobei diese als Abbildungen aufgefasst werden. In unserem Beispiel wäre das

$$\begin{aligned}\mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^4 + 3x^2 - 7.\end{aligned}$$

Wir haben hier den Körper $\mathbb{R}$ gewählt, denn in der Schule werden Polynome in der Regel hierüber betrachtet. Wir können aber nach unserer Definition einen beliebigen Körper wählen und dann stellen wir fest, dass wir ein Polynom nicht mehr unbedingt durch die zugehörige Abbildung eindeutig beschreiben können:

Beispiel 2.3.43

Wir wählen $K = \mathbb{F}_2$ und betrachten die Polynome $(0,\ldots)$ und $(0,1,1,0,\ldots)$. Diese sind offensichtlich unterschiedlich als Polynome, aber als Abbildungen aufgefasst ein und dieselbe. Für das erste Polynom als Abbildung aufgefasst gilt:

$$\begin{aligned}\overline{0} &\mapsto \overline{0} \\ \overline{1} &\mapsto \overline{0}\end{aligned}$$

für das Zweite:

$$\begin{aligned}\overline{0} &\mapsto \overline{1}\cdot\overline{0} + \overline{1}\cdot\overline{0}^2 = \overline{0} \\ \overline{1} &\mapsto \overline{1}\cdot\overline{1} + \overline{1}\cdot\overline{1}^2 = \overline{1}+\overline{1} = \overline{0}\end{aligned}$$

Wir sehen also, dass wir zwischen Polynomen und Polynomfunktionen unterscheiden müssen.

Definition 2.3.44

Sei $p = \sum_{i \in \mathbb{N}_0} a_i x^i \in K[x]$. Dann bezeichnet man

$$\begin{aligned} K &\to K \\ t &\mapsto \sum_{i \in \mathbb{N}_0} a_i t^i \end{aligned}$$

als die **Polynomfunktion** von p.

Wir identifizieren nun die algebraische Struktur hinter $K[x]$. Tatsächlich entsprechen unsere Addition und Multiplikation der *üblichen* Operationen auf Polynomen:

Proposition 2.3.45

Mit den Operationen $+$ und $\cdot$ wird $K[x]$ zu einem kommutativen Ring (mit Eins).

Beweis. Sei K ein Körper.

1. $(K[x], +)$ abelsche Gruppe:

   G0: Wie man oben bereits gesehen hat, gilt für alle $(a_i)_{i \in \mathbb{N}_0}, (b_i)_{i \in \mathbb{N}_0} \in K[x]$: $(a_i)_{i \in \mathbb{N}_0} + (b_i)_{i \in \mathbb{N}_0} = (a_i + b_i)_{i \in \mathbb{N}_0} \in K[x]$

   Man führt die Gruppeneigenschaften auf die Einträge der Folgen zurück, welche im Körper K liegen.

   G1: Seien $(a_i)_{i \in \mathbb{N}_0}, (b_i)_{i \in \mathbb{N}_0}, (c_i)_{i \in \mathbb{N}_0} \in K[x]$.

$$\begin{aligned} ((a_i)_i + (b_i)_i) + (c_i)_i &= \left(\left(\sum_{i \in \mathbb{N}_0} a_i x^i \right) + \left(\sum_{i \in \mathbb{N}_0} b_i x^i \right) \right) + (c_i)_i \\ &= \left(\sum_{i \in \mathbb{N}_0} (a_i + b_i) x^i \right) + \left(\sum_{i \in \mathbb{N}_0} c_i x^i \right) \\ &= \sum_{i \in \mathbb{N}_0} ((a_i + b_i) + c_i) x^i \\ &= \sum_{i \in \mathbb{N}_0} (a_i + (b_i + c_i)) x^i \\ &= \left(\sum_{i \in \mathbb{N}_0} a_i x^i \right) + \left(\sum_{i \in \mathbb{N}_0} (b_i + c_i) x^i \right) \\ &= (a_i)_i + \left(\left(\sum_{i \in \mathbb{N}_0} b_i x^i \right) + \left(\sum_{i \in \mathbb{N}_0} c_i x^i \right) \right) \\ &= (a_i)_i + ((b_i)_i + (c_i)_i) \end{aligned}$$

   G2: $0 := (0, 0, 0, \ldots)$

G3: Sei $(a_i)_{i\in\mathbb{N}_0} \in K[x]$. Man definiert das Inverse $-(a_i)_{i\in\mathbb{N}_0} := (-a_i)_{i\in\mathbb{N}_0}$. Es gilt:

$$\left(\sum_{i\in\mathbb{N}_0} a_i x^i\right) + \left(\sum_{i\in\mathbb{N}_0} -a_i x^i\right) = \left(\sum_{i\in\mathbb{N}_0} 0 \cdot x^i\right) = 0$$

G4: Seien $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0}, (c_i)_{i\in\mathbb{N}_0} \in K[x]$:

$$\begin{aligned}\left(\sum_{i\in\mathbb{N}_0} a_i x^i\right) + \left(\sum_{i\in\mathbb{N}_0} b_i x^i\right) &= \left(\sum_{i\in\mathbb{N}_0} (a_i + b_i) \cdot x^i\right) \\ &= \left(\sum_{i\in\mathbb{N}_0} (b_i + a_i) \cdot x^i\right) \\ &= \left(\sum_{i\in\mathbb{N}_0} b_i x^i\right) + \left(\sum_{i\in\mathbb{N}_0} a_i x^i\right)\end{aligned}$$

2. Eins:
   Man definiert als die Eins $(1, 0, \ldots)$. Dass es sich tatsächlich um die Eins handelt ist einfach zu zeigen.

3. Distributivgesetz:
   Seien $p = (a_i)_{i\in\mathbb{N}_0}, q = (b_i)_{i\in\mathbb{N}_0}, r = (c_i)_{i\in\mathbb{N}_0} \in K[x]$:

$$\begin{aligned}p \cdot (q + r) &= \left(\sum_{i\in\mathbb{N}_0} a_i x^i\right)\left(\left(\sum_{i\in\mathbb{N}_0} b_i x^i\right) + \left(\sum_{i\in\mathbb{N}_0} c_i x^i\right)\right) \\ &= \left(\sum_{i\in\mathbb{N}_0} a_i x^i\right)\left(\sum_{i\in\mathbb{N}_0} (b_i + c_i) x^i\right) \\ &= \sum_{i\in\mathbb{N}_0}\left(\sum_{k=0}^{i} a_{i-k} \cdot (b_k + c_k)\right) x^i \\ &\overset{K \text{ Körper}}{=} \sum_{i\in\mathbb{N}_0}\left(\sum_{k=0}^{i} (a_{i-k} b_k + a_{i-k} c_k)\right) x^i \\ &= \sum_{i\in\mathbb{N}_0}\left(\left(\sum_{k=0}^{i} a_{i-k} b_k\right) + \left(\sum_{k=0}^{i} a_{i-k} c_k\right)\right) x^i \\ &= \sum_{i\in\mathbb{N}_0}\left(\sum_{k=0}^{i} a_{i-k} b_k\right) x^i + \sum_{i\in\mathbb{N}_0}\left(\sum_{k=0}^{i} a_{i-k} c_k\right) x^i \\ &= \left(\sum_{i\in\mathbb{N}_0} a_i x^i\right)\left(\sum_{i\in\mathbb{N}_0} b_i x^i\right) + \left(\sum_{i\in\mathbb{N}_0} a_i x^i\right)\left(\sum_{i\in\mathbb{N}_0} c_i x^i\right) \\ &= p \cdot q + p \cdot r\end{aligned}$$

4. Assoziativgesetz:
   Wegen des Distributivgesetzes reicht es, die Assoziativität für Monome zu zeigen,

wobei wir unter einem Monom ein Polynom mit genau einem Eintrag ungleich Null verstehen. Weiterhin kann man o.B.d.A. diesen Eintrag gleich Eins setzen.

Seien also $j, l, k \in \mathbb{N}_0$:

$$\begin{aligned}
x^j \cdot (x^k \cdot x^l) &= (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot ((\delta_{i,k})_{i\in\mathbb{N}_0} \cdot (\delta_{i,l})_{i\in\mathbb{N}_0}) \\
&= (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot \left(\sum_{n=0}^{i} \delta_{n,k} \cdot \delta_{i-n,l}\right)_{i\in\mathbb{N}_0} \\
&= (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot \left(\sum_{n=0}^{i} \delta_{n,k} \cdot \delta_{-n,l-i}\right)_{i\in\mathbb{N}_0} \\
&= (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot \left(\sum_{n=0}^{i} \delta_{n,k} \cdot \delta_{n,i-l}\right)_{i\in\mathbb{N}_0} \\
&= (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot (\delta_{k,k} \cdot \delta_{k,i-l})_{i\in\mathbb{N}_0} \\
&= (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot (\delta_{i,k+l})_{i\in\mathbb{N}_0} \\
&\overset{\text{s.o.}}{=} (\delta_{i,j+k+l})_{i\in\mathbb{N}_0} \\
&\overset{\text{s.o.}}{=} (\delta_{i,j+k})_{i\in\mathbb{N}_0} \cdot (\delta_{i,l})_{i\in\mathbb{N}_0} \\
&\overset{\text{s.o.}}{=} (x^j \cdot x^k) \cdot x^l
\end{aligned}$$

5. Kommutativgesetzt:
   Auch hier reicht der Nachweis für Monome. Seien $j, k \in \mathbb{N}_0$:

$$\begin{aligned}
x^j \cdot x^k = (\delta_{i,j})_{i\in\mathbb{N}_0} \cdot (\delta_{i,k})_{i\in\mathbb{N}_0} &\overset{\text{s.o.}}{=} (\delta_{i,j+k}) = (\delta_{i,k+j})_{i\in\mathbb{N}_0} \\
= (\delta_{i,k})_{i\in\mathbb{N}_0} \cdot (\delta_{i,j})_{i\in\mathbb{N}_0} &= x^k \cdot x^j
\end{aligned}$$

Also ist $(K[x], +, \cdot)$ ein Ring. Man nennt diesen deshalb auch den Polynom*ring*. □

Definition 2.3.46

Es sei $p = \sum_{i\in\mathbb{N}_0} a_i x^i \in K[x]$ und m maximal mit $a_m \neq 0$. Dann heißt a_m der **Leitkoeffizient** von p. In diesem Fall definieren wir den **Grad** von p als $\deg p = m$. Konvention: $\deg (0)_{i\in\mathbb{N}_0} = -\infty$.

Beispiel 2.3.47

1. $\deg(2x^2 + 4) = 2$ mit Leitkoeffizient 2
2. $\deg(x^3 + 2x^2 + 1) = 3$ mit Leitkoeffizient 1
3. $\deg(1x^0) = 0$
4. $\deg(0) = -\infty$

Satz 2.3.48

Es sei $\alpha \in K$ gegeben, dann ist die Abbildung

$$\pi_\alpha : K[x] \longrightarrow K; p \mapsto p(\alpha) := \sum_{i \in \mathbb{N}_0} a_i \alpha^i$$

ein Ringhomomorphimus, der **Einsetzungshomomorphismus**.

Beispiel 2.3.49

[Einsetzungshomomorphismus.] Seien $K = \mathbb{Q}, \alpha = 2 \in \mathbb{Q}$:
Wir betrachten nun

$$\begin{aligned} &\pi_2 : \mathbb{Q}[x] \to \mathbb{Q} \\ &\sum_{i \in \mathbb{N}_0} a_i x^i \mapsto \left(\sum_{i \in \mathbb{N}_0} a_i x^i \right)(2) = \sum_{i \in \mathbb{N}_0} a_i 2^i \end{aligned}$$

Für die Polynome

$$\begin{aligned} p_1 &:= x^2 - 2 \\ p_2 &:= x^3 - 2x^2 + x + 4 \end{aligned}$$

gilt

$$\begin{aligned} \pi_2(p_1) &= 2^2 - 2 = 4 - 2 = 2 \\ \pi_2(p_2) &= 2^3 - 2 \cdot 2^2 + 2 + 4 = 8 - 8 + 6 = 6 \end{aligned}$$

Beweis (Satz 2.3.4): Sei K Körper und $\alpha \in K$ fixiert.

- Addition: Seien $p, q \in K[x]$ mit $p = \sum_{i=0}^{\infty} a_i x^i$ und $q = \sum_{i=0}^{\infty} b_i x^i$.

$$\begin{aligned} \pi_\alpha(p+q) &= \pi_\alpha \left(\sum_{i=0}^{\infty} (a_i + b_i) x^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) \alpha^i \\ &= \sum_{i=0}^{\infty} a_i \alpha^i + \sum_{i=0}^{\infty} b_i \alpha^i = \pi_\alpha(p) + \pi_\alpha(q) \end{aligned}$$

- Multiplikation: Es reicht die Verträglichkeit von π mit der Multiplikation für Monome zu zeigen. Die allgemeine Aussage folgt mit dem Distributivgesetz und der Additivität. Seien also $p = x^l, q = x^k$:

$$\pi_\alpha(x^l \cdot x^k) = \pi_\alpha(x^{l+k}) = \alpha^{l+k} = \alpha^l \cdot \alpha^k = \pi_\alpha(x^l) \cdot \pi_\alpha(x^k)$$

Damit ist π_α ein Ringhomomorphismus. □

Definition 2.3.50

Es sei $\alpha \in K$ gegeben. Dann heißt α eine **Nullstelle** von $p \in K[x]$, falls $\pi_\alpha(p) = p(\alpha) = 0$.

Beispiel 2.3.51

Beispiele für Nullstellen:

1. $x^2 - 1 \in \mathbb{Q}[x]$
   1 und -1 sind Nullstellen, denn
   $$\pi_1(x^2 - 1) = 1^2 - 1 = 0$$
   $$\pi_{-1}(x^2 - 1) = (-1)^2 - 1 = 0$$
2. $x^2 + 1 \in \mathbb{Q}[x]$
   hat keine Nullstellen in $\mathbb{Q}$, da
   $$\forall \alpha \in \mathbb{Q} : \alpha^2 + 1 \geq 0^2 + 1 > 0$$
3. $x^2 + x \in \mathbb{F}_2[x]$
   Wir haben bereits gesehen, dass für dieses Polynom alle Elemente in $\mathbb{F}_2$ Nullstellen sind.

Proposition 2.3.52

Für Polynome $p, q \in K[x]$ gilt:

1. $\deg(p + q) \leq \max\{\deg p, \deg q\}$. Falls $\deg p \neq \deg q$, dann gilt Gleichheit.
2. $\deg(p \cdot q) = \deg p + \deg q$.

Beweis (Proposition 2.3.52): Sei K Körper und seien $p = \sum_{i=0}^{n} a_i x^i, q = \sum_{i=0}^{l} b_i x^i \in K[x]$ mit $a_n \neq 0$ und $b_l \neq 0$. Damit
$$\deg(p) = n$$
$$\deg(q) = l$$

1. Man betrachtet die Summe
   $$p + q = \sum_{i=0}^{\max\{n,l\}} (a_i + b_i) \cdot x^i$$
   und stellt fest, dass damit
   $$\deg(p + q) \leq \max\{n, l\} = \max\{\deg(p), \deg(q)\}$$
   gilt. Angenommen, es gilt $n \neq l$, dann gilt o.B.d.A. $n > l$, womit $\max\{n, l\} = n$ und
   $$a_n + b_n = a_n \neq 0.$$
   Als Konsequenz ergibt sich
   $$\deg(p + q) = n = \max\{n, l\} = \max\{\deg(p), \deg(q)\}$$

2. Man betrachtet das Produkt

$$p \cdot q = \sum_{i=0}^{n+l} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) \cdot x^i$$

und dann den $n+l$-ten Koeffizienten,

$$\sum_{j=0}^{n+l} a_j b_{n+l-j},$$

wobei für alle $j > n : a_j = 0$ wegen $\deg(p) = n$. Weiterhin gilt für alle $j < n$:

$$n + l - j = l + n - j > l + n - n = l,$$

womit für alle $j < n : b_{n+l-j} = 0$. Damit reduziert sich der $n+l$-te Koeffizient zu

$$a_n \cdot b_{n+l-n} = a_n \cdot b_l.$$

Angenommen dieser wäre Null. Da K ein Körper ist, existiert a_n^{-1}:

$$0 = a_n^{-1} \cdot 0 = a_n^{-1} \cdot a_n \cdot b_l = 1 \cdot b_l = b_l,$$

was aber im Widerspruch zu $b_l \neq 0$ steht. Daraus folgt $a_n \cdot b_l \neq 0$ und

$$\deg(p \cdot q) = \deg(p) + \deg(q)$$

□

Korollar 2.3.53

Der Ring $K[x]$ ist **nullteilerfrei**:

$$p \cdot q = 0 \implies p = 0 \vee q = 0.$$

Zudem gilt die Kürzungsregel:

$$p \cdot q = p \cdot r \wedge p \neq 0 \implies q = r$$

Beweis (Korollar 2.3.53): Sei K Körper und seien $p, q, r \in K[x]$.

1. Angenommen, $p \cdot q = 0$. Dann gilt nach Proposition 2.3.52

$$\deg(p) + \deg(q) = \deg(p \cdot q) = -\infty,$$

womit

$$\deg(p) = -\infty \ \vee \ \deg(q) = -\infty,$$

woraus

$$p = 0 \ \vee \ q = 0$$

folgt. Durch Kontraposition erhält man die Nullteilerfreiheit.

2. Es gelte $p \cdot q = p \cdot r \wedge p \neq 0$. Man folgert

$$\begin{aligned} & p \cdot q = p \cdot r \\ \Rightarrow & p \cdot (q - r) = 0 \\ \overset{p \neq 0}{\Rightarrow} & q - r = 0 \\ \Rightarrow & q = r \end{aligned}$$

□

Theorem 2.3.54

Für $p, q \in K[x]$ mit $q \neq 0$ gibt es eindeutige $a, b \in K[x]$ mit

$$p = a \cdot q + b \ \wedge \ \deg b < \deg q.$$

Beispiel 2.3.55

Seien $p = x^5 - x^3 + x^2 - x - 1 \in \mathbb{R}[x]$ und $q = x^3 + x + 1 \in \mathbb{R}[x]$. Dann gilt

$$p = (x^2 - 1) \cdot q + (x + 1)$$

In diesem Fall wären $a = (x^2 - 1)$ und $r = x + 1$. Die geneigten Lesenden können die Division überprüfen.

Beweis (Theorem 2.3.54): Seien K Körper, $p, q \in K[x]$ und $q \neq 0$. Man definiert

$$A := \{n \in \mathbb{N}_0 \cup \{-\infty\} \mid \exists a \in K[x] : n = \deg(p - a \cdot q)\}$$

Die Menge A ist nicht leer, da $1 \in K[x]$. Wegen der Wohlordnung der natürlichen Zahlen hat die Menge A ein eindeutig bestimmtes Minimum. Damit existiert ein $a \in K[x]$, für das $\deg(p - a \cdot q)$ minimal wird.

Angenommen, es wäre $\deg(p - a \cdot q) \geq \deg(q)$. Da $q \in K[x]$ und $q \neq 0$, gibt es $b_i \in K$ mit

$$q = \sum_{i=0}^{n} b_i x^i$$

und $b_n \neq 0$. Ähnlich gibt es für $(p - a \cdot q) \in K[x]$ Koeffizienten $c_i \in K$ mit

$$p - a \cdot q = \sum_{i=0}^{l} c_i x^i,$$

wobei nach Annahme $c_l \neq 0$ und $l \geq n$. Man setzt

$$a' = a + \frac{c_l}{b_n} x^{l-n}$$

und stellt fest, dass

$$\begin{aligned} p - a' \cdot q &= p - (a + \frac{c_l}{b_n} x^{l-n}) \cdot q \\ &= p - aq - \frac{c_l}{b_n} x^{l-n} \cdot q \\ &= p - aq - \sum_{i=0}^{n} \frac{c_l \cdot b_i}{b_n} x^{i+l-n} \\ &= \sum_{i=0}^{l} c_i x^i - c_l x^l - \sum_{i=0}^{n-1} \frac{c_l \cdot b_i}{b_n} x^{i+l-n} \\ &= \underbrace{\sum_{i=0}^{l-1} c_i x^i}_{\deg < l} - \underbrace{\sum_{i=0}^{n-1} \frac{c_l \cdot b_i}{b_n} x^{i+l-n}}_{\deg < n \leq l} \end{aligned}$$

Damit wäre aber $\deg(p - a' \cdot q) < \deg(p - a \cdot q)$, was ein Widerspruch zur Minimalität von a ist. Durch den Widerspruch folgt $\deg(p - a \cdot q) < \deg(q)$. Setzt man $b = p - a \cdot q$, erhält man die Existenzaussage.

Es bleibt die Eindeutigkeit zu zeigen. Angenommen, es gäbe ein zweites Paar $a', b' \in K[x]$, das die Divisionseigenschaft erfüllt. Aus

$$a \cdot q + b = q = a' \cdot q + b'$$

folgt

$$(a - a') \cdot q = b' - b.$$

Nach Proposition 2.3.52 gilt

$$\begin{aligned} \max\{\deg(b'), \deg(b)\} = \max\{\deg(b'), \deg(-b)\} &\geq \deg(b' - b) \\ &= \deg((a - a') \cdot q) = \deg(a - a') + \deg(q). \end{aligned}$$

Nach Voraussetzung gilt aber $\deg(b) < \deg(q) \wedge \deg(b') < \deg(q)$ und damit

$$\max\{\deg(b'), \deg(b)\} < \deg(q).$$

Damit die große Ungleichung noch wahr sein kann, muss $\deg(a - a') = -\infty$. Dann ist aber $a - a' = 0$, womit $a = a'$ und damit $b = b'$. Man erhält also Eindeutigkeit. □

Korollar 2.3.56

Es sei $\alpha \in K$ eine Nullstelle von $0 \neq p \in K[x]$. Dann $\exists! \, q \in K[x]$ mit $\deg(q) = \deg(p) - 1$ und

$$p = (x - \alpha) \cdot q.$$

Daher hat jedes Polynom von Grad m maximal m paarweise verschiedene Nullstellen.

Beweis (Korollar 2.3.56): Es sei $\alpha \in K$ eine Nullstelle von $0 \neq p \in K[x]$. Nach Theorem 2.3.54 gibt es $q, b \in K[x]$, sodass

$$p = q \cdot (x - \alpha) + b$$

und $\deg(b) < \deg(x - \alpha) = 1$. Damit ist $b \in K$. Man erhält

$$0 = p(\alpha) = q \cdot (\alpha - \alpha) + b = 0 + b = b,$$

womit

$$p = (x - \alpha) \cdot q.$$

Durch das sukzessive Abspalten von Nullstellen verringert sich der Grad jeweils um 1. Das kann aber nur endlich oft erfolgen und der Quotient muss irgendwann den Grad 0 haben, also ein konstantes Polynom sein. Damit folgt der zweite Teil der Aussage. □

2.3.5 Von Polynomringen zu allgemeineren Ringen

In diesem Kapitel wollen wir die bereits bekannte Struktur des Rings wieder aufgreifen und vertiefen, indem wir die innere Strukturierung mit Hilfe einiger neuer Begriffe untersuchen. Der wichtigste dieser Begriffe wird das Ideal sein. Zum Abschluss gehen wir noch ein wenig auf Algebren ein.

An dieser Stelle sollte man bemerken, dass es auch sinnvoll sein kann, Ringe ohne Einselement zu betrachten. Es treten zum Beispiel in der Analysis einige Funktionenringe auf, die kein Einselement besitzen. Wir werden aber im Folgenden nur Ringe mit Einselement betrachten.

Definition 2.3.57

Einen kommutativen Ring mit 1 nennen wir einen **Kring**.

Die Bezeichnung Kring ist **nicht** allgemein üblich. Wir benutzen diese innerhalb der Vorlesung und Sie dürfen diese auch in Klausur und Hausaufgaben benutzen. Sollten Sie den Begriff außerhalb dieses Kontexts benutzen wollen, sollten Sie daran denken diesen zu definieren. Das Wort geht auf den Mathematiker Wolfgang Soergel zurück.[1]

Beispiel 2.3.58

Beispiele für Kringe:

- $K[x]$ ist ein Kring.
- $K[x_i | i \in I]$ für eine Indexmenge I. Diese Polynomringe in mehreren Veränderlichen spielen eine wichtige Rolle in der Computeralgebra. Sie kommen insbesondere innerhalb der algebraischen Geometrie zur Anwendung.

Definition 2.3.59

Es sei $R \neq 0$ ein Ring. Dann heißt R **nullteilerfrei**, wenn für alle $a, b \in R$ gilt:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0.$$

Ist R darüber hinaus ein Kring, so nennen wir R einen **Integritätsbereich**.

[1] Soergel, W. (2020, Februar 10). Lineare Algebra I, Abgerufen 27. August 2020, von https://home.mathematik.uni-freiburg.de/soergel/Skripten/XXLA1.pdf

Beispiel 2.3.60

Beispiele zu Integritätsbereichen und nullteilerfreien Ringen

- Für einen Körper K ist $K[x]$ nullteilerfrei, denn für zwei Polynome $p, q \in K[x]$ gilt, dass
$$\deg(p \cdot q) = \deg(p) + \deg(q).$$
Gilt also $pq = 0$, dann
$$-\infty = \deg(p) + \deg(q),$$
womit wegen $\deg(p), \deg(q) \in \mathbb{N} \cap \{-\infty\}$
$$\deg(p) = -\infty \vee \deg(q) = -\infty,$$
also
$$p = 0 \vee q = 0.$$
- $K^{n\times n}$ – also die $n \times n$-Matrizen mit Einträgen in K – hat Nullteiler (für $n > 1$). Man betrachtet die Elementarmatrizen $E_{i,j}, E_{k,l}$ für $1 \leq i, j, k, l \leq n$, welche überall null sind bis auf eine Eins an der Stelle (i, j) bzw. (k, l). Für $j \neq k$ gilt
$$E_{i,j} \cdot E_{k,l} = 0.$$
- $\mathbb{Z}$ ist nullteilerfrei. Angenommen, man hat $a, b \in \mathbb{Z} \setminus \{0\}$ mit $ab = 0$, dann
$$0 = |ab| = |a| \cdot |b| \geq 1 \cdot 1 > 0,$$
was ein Widerspruch ist.
- Körper sind nullteilerfrei und kommutativ, also Integritätsbereiche.
- $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Integritätsbereich wenn m eine Primzahl oder Null ist.
- Da $\mathbb{Z}$ und $K[x]$ jeweils kommutativ sind und nach dem obigen nullteilerfrei, handelt es sich um Integritätsbereiche.

Proposition 2.3.61

Es sei R ein endlicher Integritätsbereich, dann ist R ein Körper.

Beweis. Wir müssen nur zeigen, dass jedes $x \in R\setminus\{0\}$ ein multiplikativ Inverses besitzt. Dazu betrachten wir die Abbildung $\ell_x : R \longrightarrow R$, $r \mapsto x \cdot r$. Wir zeigen, dass ℓ_x injektiv ist, dann folgt (da R endlich ist), dass ℓ_x surjektiv ist, damit existiert aber ein $b \in R$ mit $\ell_x(b) = 1$, also $x \cdot b = 1$, also wäre b ein inverses zu x.
Es seien also $r_1, r_2 \in R$ mit

$$\begin{aligned} \ell_x(r_1) = \ell_x(r_2) &\Leftrightarrow xr_1 = xr_2 \\ &\Leftrightarrow x \cdot (r_1 - r_2) = 0 \\ \text{da } R \text{ nullteilerfrei ist} &\Leftrightarrow r_1 - r_2 = 0 \\ &\Leftrightarrow r_1 = r_2. \end{aligned}$$

□

Wir betrachten nun kurz eine spezielle Sorte von Integritätsbereichen.

Definition 2.3.62

Sei R ein Integritätsbereich. R heißt ein **euklidischer Ring**, falls eine Funktion $\sigma : R \setminus \{0\} \longrightarrow \mathbb{N}$ existiert mit: Für alle $a, b \in R$, $a \neq 0$ existieren $q, r \in R$ mit

$$b = qa + r \text{ so, dass wenn } r \neq 0 \Rightarrow \sigma(r) < \sigma(a).$$

Beispiel 2.3.63

Man betrachtet die ganzen Zahlen $\mathbb{Z}$ mit

$$\sigma : \mathbb{Z} \setminus \{0\} \to \mathbb{N} : a \mapsto |a|.$$

Die Aussage reduziert sich darauf, dass die Division mit Rest, also der euklidische Divisionsalgorithmus, funktioniert.

Proposition 2.3.64

Es sei K ein Körper, dann ist $K[x]$ ein euklidischer Ring.

Beweis. Mit der Wahl von $\sigma = \deg$ reduziert sich der Beweis auf die Polynomdivision. □

2.4 Ideale und Restklassenringe

Wie kann man aus Ringen neue Ringe konstruieren? Wir haben bei Gruppen den Begriff Normalteiler kennengelernt und die Faktorgruppe gesehen. Wir lernen hier die analoge Konstruktion kennen.

2.4.1 Ideale

Definition 2.4.1

Es sei R ein Ring und $I \subseteq R$ eine Untergruppe (bzgl. $+$). Dann heißt I

- ein **Linksideal** von R, falls für alle $r \in R$ und $a \in I$: $ra \in I$.
- ein **Rechtsideal** von R, falls für alle $r \in R$ und $a \in I$: $ar \in I$.
- ein **(beidseitiges) Ideal** von R, falls für alle $r \in R$ und $a \in I$: $ra \in I$ und $ar \in I$.

Beispiel 2.4.2

[Ideale]

1. Man betrachtet erneut das Beispiel der ganzen Zahlen $\mathbb{Z}$. Man fixiert ein

$a \in \mathbb{Z}$ und zeigt, dass die Menge

$$I := a\mathbb{Z} = \{ax | x \in \mathbb{Z}\}$$

ein Ideal in $\mathbb{Z}$ ist. Aus den vorigen Kapiteln ist bekannt, dass es sich dabei um eine Untergruppe von $\mathbb{Z}$ handelt.

Seien nun $b \in I$ und $r \in \mathbb{Z}$. Es gibt per Definition $x \in \mathbb{Z}$, sodass $b = ax$, womit

$$r \cdot b = r \cdot (ax) = a \cdot (rx) \in a\mathbb{Z} = I.$$

2. Sei K ein Körper und $K[x]$ der Polynomring. Man fixiert ein $a \in K$ und definiert

$$I_a = \{g \in K[x] \mid \exists p \in K[x] : g = (x - a) \cdot p\}.$$

Man argumentiert analog zum ersten Beispiel, um die Idealeigenschaft nachzuweisen.

3. Es sei $R = \mathbb{Q}^{2\times 2}$ und $I = \mathbb{Q}E_{1,1} + \mathbb{Q}E_{2,1}$. Alle Matrizen aus I sind also von der Form

$$\begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix}.$$

Es sei $B \in K^{2\times 2}$:

$$\begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix} = \begin{pmatrix} b_{1,1}a_1 + b_{1,2}a_2 & 0 \\ b_{2,1}a_1 + b_{2,2}a_2 & 0 \end{pmatrix} \in I$$

und

$$\begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix} \cdot \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} a_1b_{1,1} & a_1b_{1,2} \\ a_2b_{2,1} & a_2b_{2,2} \end{pmatrix},$$

was im Allgemeinen nicht in I ist. Also ist I ein Linksideal, aber kein Rechtsideal.

4. R wie oben, aber $I = \mathbb{Q}E_{1,1} + \mathbb{Q}E_{1,2}$. Damit sind die Matrizen von der Form

$$\begin{pmatrix} a_1 & a_2 \\ 0 & 0 \end{pmatrix}.$$

Analog sieht man, dass es sich um ein Rechtsideal handelt, aber nicht um ein Linksideal.

5. In einem Kring sind alle Ideale beidseitig.

6. Ideale sind im Grunde Unterringe ohne Einselement mit der zusätzlichen Eigenschaft, dass sie den umgebenden Ring 'einfangen'. $R \cdot I \subset I$ für Linksideale und $I \cdot R \subset I$ für Rechtsideale.

2.4.2 Bonus: Hauptidealringe

Definition 2.4.3

Es sei R ein kommutativer Ring mit Eins und $I \subset R$ ein Ideal. Dann heißt I **Hauptideal**, falls ein $a \in R$ existiert mit

$$I = (a) = R \cdot a = a \cdot R.$$

Beispiel 2.4.4

Einige Beispiele dazu

1. Wir werden später sehen, dass in $\mathbb{Z}$ und $K[x]$, jedes Ideal ein Hauptideal ist.
2. Es sei $R = K[x, y]$, dann ist $I = \{q \in K[x, y] \mid q = xy \cdot p \text{ für ein } p \in K[x, y]\}$ kein Hauptideal.

Wir nutzen diese Definition um Teilbarkeit in Integritätsbereichen zu definieren

Definition 2.4.5

Es sei R ein Integritätsbereich und $a, b \in R$. Dann sagen wir a teilt b falls $b \in (a)$, wir schreiben dann wie bisher $a|b$.

Bemerkung 2.4.6

Diese Definition von Teilbarkeit stimmt mit der bisherigen für $\mathbb{Z}$ überein.

Definition 2.4.7

Es sei R ein Integritätsbereich und $a, b \in R$. Ein größter gemeinsamer Teiler von a und b, $\text{ggT}(a, b)$ ist ein Element $d \in R$ mit $d|a$, $d|b$ und falls $\exists\, c \in R$ mit $c|a, c|b$, dann gilt $c|d$.

Hier stimmt die Definition wieder mit unserer intuitiven Definition in $\mathbb{Z}$ überein. Wir können diese Definition auch wieder in Hauptideal übersetzen: d ist ein ggT von a und b, falls $a, b \in (d)$ und wenn $a, b \in (c)$, so ist $c \in (d)$.

Definition 2.4.8

Es sei R ein euklidischer Ring, $f, g \in R$ heißen **teilerfremd** , falls $\forall\, d \in R$ mit $f = dr_1, g = dr_2$, gilt, dass d invertierbar in R ist.

Beispiel 2.4.9

Einige Beispiele dazu:

1. Für $R = \mathbb{Z}$ stimmt das wiederum mit unserer Intuition überein.
2. $f = (x-1)(x-2)^2$ und $g = (x-1)(x-3)$ in $\mathbb{R}[x]$ sind nicht teilerfremd, da $d = (x-1)$ nicht invertierbar ist.

Definition 2.4.10

Es sei R ein kommutativer Ring mit Eins der nullteilerfrei ist, dann heißt R **Hauptidealring** falls jedes Ideal von R ein Hauptideal ist.

Satz 2.4.11

Es sei R ein euklidischer Ring, dann ist R ein Hauptidealring.

Beweis (Satz 2.4.2): Sei R ein euklidischer Ring und $I \subset R$ ein Ideal. Da R euklidisch ist, gibt es eine Bewertungsfunktion

$$\sigma : R \setminus \{0\} \to \mathbb{N}.$$

I ist nicht leer, also muss muss es bezüglich σ ein minimales $f \in I \setminus \{0\}$ geben. Per Definition muss $Rf \subseteq I$, also

$$(f) \subseteq I.$$

Angenommen, es gibt $s \in I \setminus (f)$, dann gibt es, weil R ein euklidischer Ring ist, $q, r \in R$ mit

$$s = q \cdot f + r,$$

wobei $r = 0$ oder $\sigma(r) < \sigma(f)$. Da $f \in I$ und I ein Ideal ist, gilt $qf \in I$, womit $s, qf \in I$, sodass $r \in I$. f ist jedoch das minimale Element in $I \setminus \{0\}$ bezüglich σ. Es bleibt also nur die Möglichkeit $r = 0$ übrig. Dann ist jedoch $s \in (f)$, was im Widerspruch zur Wahl von s steht.

Insgesamt ergibt sich durch Beweis mit Widerspruch, dass

$$I = (f).$$

Da I beliebig war, ist R ein Hauptidealring. □

Definition 2.4.12

Es seien $f, g \in R$, dann nennen wir einen Erzeuger des Ideals $(f) \cap (g)$ ein **kleinstes gemeinsames Vielfaches**, wir schreiben dafür $\mathrm{kgV}(f, g)$.

Wiederum entspricht das unserer Intuition in $\mathbb{Z}$ und in dem obigen Beispiel, $f = (x-1)(x-2)^2$ und $g = (x-1)(x-3)$ in $\mathbb{R}[x]$, ist ein kgV $(x-1)(x-2)^2(x-3)$.

Proposition 2.4.13

Es sei R ein Hauptidealring und $f, g \in R \setminus \{0\}$ teilerfremd, dann ist fg ein kgV von f und g.

Beweis. Wir schreiben kurz $m = \mathrm{kgV}(f, g)$. Es ist $fg \in (f)$ und $fg \in (g)$, also $fg \in (f) \cap (g)$. Damit gibt es ein $v \in R$ mit $fg = vm$. Wegen $m \in (f) \cap (g)$ gibt es aber auch $p, q \in R$, sodass

$$m = p \cdot f$$
$$m = q \cdot g,$$

womit

$$fg = v \cdot m = v \cdot p \cdot f \Rightarrow f \cdot (g - vp) = 0$$
$$fg = v \cdot m = v \cdot q \cdot g \Rightarrow g \cdot (f - vq) = 0.$$

Hauptidealringe sind nullteilerfrei und $f \neq 0 \neq g$, also

$$g = vp$$
$$f = vq.$$

Weil f, g teilerfremd sind, existiert $v^{-1} \in R$, sodass

$$fg = vm \Rightarrow v^{-1}fg = m \Rightarrow m \in (fg).$$

Insgesamt gilt damit

$$(fg) = (m) = (f) \cap (g),$$

□

2.4.3 Restklassenringe

Es sei R ein Ring und I ein Ideal. Wie bei abelschen Gruppen und Untergruppen definieren wir eine Äquivalenzrelation auf R durch $a \equiv b \Leftrightarrow a - b \in I$. Wir überlassen es den Lesenden nachzuweisen, dass das eine Äquivalenzrelation ist. Die Menge der Äquivalenzklassen bezeichnen wir mit R/I.

Proposition 2.4.14

Es sei R ein Ring und I ein Ideal, dann ist R/I mit den induzierten Verknüpfungen

$$[a] + [b] = [a + b] \text{ und } [a] * [b] = [a * b]$$

wieder ein Ring. Wir nennen diesen Ring den **Restklassenring**

Proposition 2.4.15

Es sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, dann ist $\ker \varphi$ ein Ideal in R. Umgekehrt sei $I \subseteq R$ ein Ideal, dann ist die kanonische Abbildung $\pi : R \longrightarrow R/I, r \mapsto \overline{r}$ ein Ringhomomorphismus.

Beweis (Proposition 2.4.15): Sei R ein Ring.

1. Sei $\varphi : R \to S$ ein Ringhomomorphismus. Man zeigt, dass $I = \operatorname{Ker} \varphi$ ein Ideal ist. Es ist bereits bekannt, dass $\operatorname{Ker} \varphi$ eine Untergruppe ist.

   Es bleibt also übrig, $RIR \subset I$ zu zeigen. Seien dazu $a \in I = \operatorname{Ker} \varphi$ und $l, r \in R$. Nun erhält man

   $$\varphi(l \cdot a \cdot r) = \varphi(l) \cdot \varphi(a) \cdot \varphi(r) = \varphi(l) \cdot 0 \cdot \varphi(r) = 0,$$

   womit es sich tatsächlich um ein beidseitiges Ideal handelt.

2. Sei I ein Ideal R. Aus dem Abschnitt zu Gruppen ist bereits bekannt, dass

$$\pi : R \to R/I : r \mapsto r + I$$

ein Gruppenhomomorphismus ist.

Es gilt für alle $a, b \in R$, dass

$$\begin{aligned}\pi(a) \cdot \pi(b) &= (a + I)(b + I) = a \cdot b + a \cdot I + b \cdot I + I \cdot I \\ &= a \cdot b + I + I + I \\ &= ab + I = \pi(ab),\end{aligned}$$

wegen $aI, bI, I^2 \subset I$. Per Definition gilt $\pi(1_R) = 1_{R/I}$. Insgesamt wird π zu einem Ringhomomorphismus.

□

Bemerkung 2.4.16

Das Bild eines Ringhomomorphismus ist nicht unbedingt ein Ideal.

Satz 2.4.17

Es sei R ein euklidischer Ring, $f, g \in R$ teilerfremd. Dann ist

$$R/(fg) \cong R/(f) \times R/(g),$$

wobei der Isomorphismus ψ gegeben ist durch $r + (fg) \mapsto (r + (f), r + (g))$.

Beweis (Satz 2.4.3): Seien R ein euklidischer Ring und $f, g \in R$ teilerfremd. Man zeigt, dass

$$\psi : R/(fg) \to R/(f) \times R/(g) : (x + (fg)) \mapsto (x + (f), x + (g))$$

ein Isomorphismus ist. Die Ringhomomorphieeigenschaften sind einfach nachzuprüfen und werden deshalb als Übung offen gelassen. Stattdessen wird hier nur die Vertreterunabhängigkeit verifiziert:

Seien $s, r \in R$ mit

$$s = r \mod fg \quad \Rightarrow s - r \in (fg).$$

Damit muss es $p \in R$ geben, sodass mit R als Kring

$$s - r = p \cdot fg = \underbrace{pf \cdot g}_{\in(g)} = \underbrace{pg \cdot f}_{\in(f)},$$

womit

$$s + (f) = r + (f) \quad \wedge \quad s + (g) = r + (g).$$

Insgesamt wird ψ damit vertreterunabhängig.
Wir zeigen, dass ψ ein Isomorphismus ist. Falls f oder g gleich Null sind, so folgt das leicht:
O.B.d.A. $f = 0$. Damit gilt insbesondere

$$\begin{aligned}g &= 1 \cdot g \\ f &= 0 \cdot g.\end{aligned}$$

Da f, g teilerfremd sind, muss g invertierbar sein, womit $(g) = R$. Es ergibt sich

$$\begin{aligned} R/(f) \times R/(g) = R/\{0\} \times R/R &\cong R \times \{0\} \\ &\cong R \cong R/(0) = R/(fg). \end{aligned}$$

Wir können also annehmen, dass $f \neq 0 \neq g$.

Da ψ ein Ringhomomorphismus ist, zeigen wir die Injektivität durch

$$\operatorname{Ker} \psi = \{0 + (fg)\}.$$

Sei dafür $x + (fg) \in \operatorname{Ker} \psi$.

$$(x + (f), x + (g)) = \psi(x + (fg)) = 0 = (0 + (f), 0 + (g))$$

ergibt

$$x \in (f) \wedge x \in (g) \Rightarrow x \in (f) \cap (g).$$

Die geneigten Lesenden zeigen, dass der Schnitt zweier Ideale wieder ein Ideal ist. Mit Satz 2.4.2 folgt, da R euklidisch ist, dass R insbesondere ein Hauptidealring ist. Da $f, g \neq 0$ teilerfremd sind, gilt nach Proposition 2.4.13, dass

$$(fg) = (f) \cap (g).$$

Damit folgt, dass also auch $x \in (fg)$, womit

$$x + (fg) = 0 + (fg).$$

Da $x + (fg) \in \operatorname{Ker} \psi$ beliebig war, ist ψ injektiv.

Surjektivität zeigt man ähnlich zu der Konstruktion des euklidischen Algorithmus. Sei $y = (a + (f), b + (g)) \in R/(f) \oplus R/(g)$. R ist ein Hauptidealring, also gibt es $r \in R$, sodass

$$(f, g) = r,$$

was bedeutet, dass es $p, q \in R$ gibt, sodass

$$\begin{aligned} f &= pr \\ g &= qr. \end{aligned}$$

Weil f, g teilerfremd sind, muss r multiplikativ invertierbar sein, also $(r) = R$, womit

$$(f, g) = R.$$

Damit wiederum gibt es insbesondere $p, q \in R$, sodass

$$1 = pf + qg.$$

Als Konsequenz ergibt sich

$$1 = pf \mod g \quad \wedge \quad 1 = qg \mod f,$$

was insbesondere für

$$x := b \cdot pf + a \cdot qg$$

die Relationen

$$\begin{aligned} x = b \cdot 0 + a \cdot 1 = a \mod f \\ x = b \cdot 1 + a \cdot 0 = b \mod f \end{aligned}$$

erzeugt. Also $\psi(x + (fg)) = y$. Da $x + (fg)$ beliebig war, ist ψ surjektiv und insgesamt ein Isomorphismus. □

Beispiel 2.4.18

1. 3 und 5 sind teilerfremd in $\mathbb{Z}$.
2. 8 und 9 sind teilerfremd in $\mathbb{Z}$.
3. 6 und 8 sind nicht teilerfremd in $\mathbb{Z}$, da beide den gemeinsamen Teiler 2 haben.
4. 9 und 12 sind nicht teilerfremd in $\mathbb{Z}$, da beide den gemeinsamen Teiler 3 haben.
5. x^2+1 und x sind teilerfremd in $\mathbb{Q}[x]$.

   x^2+1 hat in $\mathbb{Q}$ keine Nullstellen, womit keine Linearfaktoren herausgeteilt werden können. Das Polynom wird also nur durch sich selbst und alle $a \in \mathbb{R} \setminus \{0\}$ geteilt.

   x wird ebenfalls nur durch sich und reelle Zahlen geteilt.

   Gemeinsame Teiler sind also die reellen Zahlen ungleich null, welche invertierbar in $\mathbb{R}[x]$ sind.
6. x^2-1 und $x+1$ sind nicht teilerfremd in $\mathbb{Q}[x]$ wegen $x^2-1=(x+1)(x-1)$.

Bemerkung 2.4.19

Der chinesische Restsatz ist auf den ersten Blick eher abstrakt und eine wichtige enthaltene Aussage versteckt sich: eine hinreichende Bedingung zur Lösung von Gleichungssystemen der Form

$$\begin{aligned} x &= a_1 \mod f_1 \\ x &= a_2 \mod f_2 \\ &\vdots \\ x &= a_n \mod f_n, \end{aligned}$$

wobei $a_1, \ldots, a_n, f_1, \ldots, f_n \in R$ gegeben sind, R ein euklidischer Ring ist und x gesucht wird. Das Problem ist äquivalent dazu, ein $x \in R$ mit

$$\begin{aligned} (x+(f_1), \ldots, x+(f_n)) &= (a_1+(f_1), \ldots, a_n+(f_n)) \\ &=: y \in R/(f_1) \times \ldots \times R/(f_n) \end{aligned}$$

zu finden.
Für die f_i teilerfremd ist nach dem Restsatz[a]

$$R/(f_1) \times \ldots \times R/(f_n) \cong R/(f_1 \cdot \ldots \cdot f_n)$$

und es gibt $x \in R$, sodass

$$y = \psi(x+(f_1 \cdot \ldots \cdot f_n)) = (x+(f_1), \ldots, x+(f_n)).$$

Es gibt also eine Lösung. Man nennt so ein System auch eine simultane Kongruenz. Man bemerkt, dass alle Lösungen kongruent sind bezüglich $f_1 \cdot \ldots \cdot f_n$.

Mit Hilfe des Lemmas von Bézout können wir sogar einen Lösungsalgorithmus für $R = \mathbb{Z}$ entwickeln. Man definiert $F = f_1 \cdot \ldots \cdot f_n$ und für alle $1 \leq j \leq n$:

$$F_j := F/f_j.$$

Für alle $1 \leq j \leq n$ gibt es nach dem Lemma von Bézout $p_j, q_j \in \mathbb{Z}$, sodass

$$p_j \cdot F_j + q_j \cdot f_j = \mathrm{ggT}(F_j, f_j) = 1,$$

womit

$$1 - p_j \cdot F_j = q_j \cdot f_j \in (f_j) \quad \Leftrightarrow \quad 1 = p_j \cdot F_j \mod f_j.$$

Da die F_j per Konstruktion durch alle f_i mit $i \neq j$ teilbar sind, gilt für alle $1 \leq i, j \leq n$:

$$p_j \cdot F_j = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \mod f_i \quad \Leftrightarrow \quad p_j \cdot F_j = \delta_{i,j} \mod f_i.$$

Damit muss

$$x = \sum_{j=1}^{n} a_j p_j F_j$$

eine Lösung sein, da für alle $1 \leq i \leq n$

$$x = \sum_{j=1}^{n} a_j \delta_{i,j} = a_i \mod f_i.$$

Die geneigten Lesenden können sich überlegen, weshalb alle Lösungen durch

$$x + k \cdot F$$

mit $k \in \mathbb{Z}$ gegeben sind.

[a] Man erhält durch Induktion den chinesischen Restsatz für teilerfremde $f_1, \ldots, f_n$.

Beispiel 2.4.20

Man sucht eine ganze Zahl $x \in \mathbb{Z}$, sodass

$$\begin{aligned} x &= 1 \mod 3 \\ x &= 1 \mod 4 \\ x &= 0 \mod 5. \end{aligned}$$

Es sind $f_1 = 3$, $f_2 = 4$ und $f_3 = 5$, und somit

$$F = 3 \cdot 4 \cdot 5 = 60$$

und

$$\begin{aligned} F_1 &= 4 \cdot 5 = 20 \\ F_2 &= 3 \cdot 5 = 15 \\ F_3 &= 3 \cdot 4 = 12. \end{aligned}$$

Man findet

$$\begin{aligned} 1 &= p_1 \cdot F_1 + q_1 \cdot f_1 \\ &= p_1 \cdot 20 + q_1 \cdot 3 \\ &= -1 \cdot 20 + 7 \cdot 3, \end{aligned}$$

$$\begin{aligned} 1 &= p_2 \cdot F_2 + q_2 \cdot f_2 \\ &= p_2 \cdot 15 + q_2 \cdot 4 \\ &= -1 \cdot 15 + 4 \cdot 4 \end{aligned}$$

und

$$\begin{aligned} 1 &= p_3 \cdot F_3 + q_3 \cdot f_3 \\ &= p_3 \cdot 12 + q_3 \cdot 5 \\ &= -2 \cdot 12 + 5 \cdot 5. \end{aligned}$$

Also

$$\begin{aligned} p_1 = -1 \Rightarrow \quad & p_1 F_1 = -20 \\ p_2 = -1 \Rightarrow \quad & p_2 F_2 = -15 \\ p_3 = -2 \Rightarrow \quad & p_3 F_3 = -24, \end{aligned}$$

womit

$$x = 1 \cdot (-20) + 1 \cdot (-15) + 0 \cdot (-24) = -35$$

eine Lösung ist. Die Gesamtheit aller Lösungen ist durch

$$-35 + k \cdot F = -35 + k \cdot 60$$

gegeben mit $k \in \mathbb{Z}$.

2.4.4 Bonus: Einheiten

Definition 2.4.21

Es sei R ein Ring, die Menge der **Einheiten** $R^\times$ in R ist die Menge der multiplikativ invertierbaren Elemente.

Wir vermeiden i.A. die Bezeichnung *die Menge der invertierbaren Elemente*, da wir zwei Verknüpfungen auf dem Ring haben und diese Bezeichnung nicht eindeutig wäre.

Beispiel 2.4.22

1. $\mathbb{Z}^\times = \{-1, 1\}$
2. Für einen Körper K sind per Definition die Einheiten $K^\times = K \setminus \{0\}$.
3. $(K[x])^\times = K^\times$.

4. Sei $n \in \mathbb{Z}$. Man betrachtet $\mathbb{Z}/n\mathbb{Z}$. Die geneigten Lesenden zeigen (Übung), dass
$$(\mathbb{Z}/n\mathbb{Z})^\times = \{m + n\mathbb{Z} | m, n \text{ teilerfremd}\}.$$
(Hinweis: Satz von Bézout.)

Bemerkung 2.4.23

Es sei R ein Integritätsbereich, $a \in R$ und $b \in R^\times$. Dann ist b ein Teiler von a, denn $a = b^{-1} \cdot (ba) = (b^{-1}b) \cdot a$. Anders gesehen: Das Ideal, welches von B erzeugt wird ist ganz R, denn $b^{-1}b \in (b)$, also ist $1 \in (b)$, also ist $R \cdot 1 = R \subseteq (b)$. Damit ist natürlich $(a) \subseteq (b)$ und damit gilt per Definition 2.4.2 $b|a$.

Proposition 2.4.24

Es sei R ein Ring, dann ist $(R^\times, \cdot)$ eine Gruppe (nicht unbedingt abelsch).

Beweis. Die Assoziativität der Verknüpfung gilt schon für R. Wir müssen, neben den Gruppenaxiomen, vor allem auch die Abgeschlossenheit unter der Multiplikation zeigen. Es seien also $a, b \in R^\times$, dann existieren a^{-1}, b^{-1} mit

$$a \cdot a^{-1} = a^{-1} \cdot a = 1 \text{ und } b \cdot b^{-1} = b^{-1} \cdot b = 1.$$

Dann gilt
$$(ab) \cdot (b^{-1}a^{-1}) = (b^{-1}a^{-1}) \cdot (ab) = 1.$$
Also ist $ab \in R^\times$. Weiter ist $1 \in R^\times$ und wenn $a \in R^\times$, dann ist offensichtlich $a^{-1} \in R^\times$. □

Wir nennen $R^\times$ auch die **Einheitengruppe** von R. Insbesondere ist also $\{m + n\mathbb{Z} | m, n \text{ teilerfremd}\} \subset \mathbb{Z}/n\mathbb{Z}$ eine Gruppe bezüglich der Multiplikation. Ein sehr wichtiges Beispiel, welches uns im Laufe des ersten Jahres immer wieder begleitet, ist die Einheitengruppe des Matrizenrings. Wir formulieren diese schon, im Vorgriff auf den nächsten Abschnitt, für beliebige Körper:

Definition 2.4.25

Es sei $n \in \mathbb{N}$ und $\mathbb{K}$ ein Körper, dann bezeichnen wir die Einheitengruppe von $\mathbb{K}^{n \times n}$ mit $\mathrm{GL}_n(\mathbb{K})$ (die **Allgemeine Lineare Gruppe** oder **G**eneral **L**inear Group).

Von einem algebraischen Standpunkt aus würden wir jetzt noch die Begriffe **irreduzibel** (eine Nicht-Einheit, die sich nicht als Produkt von zwei Nicht-Einheiten schreiben lässt) und **prim** (eine Nicht-Einheit, die wenn sie ein Produkt teilt, mindestens einen der Faktoren teilt) für Elemente eines Krings einführen, aber das geht über alles hinaus, was wir im ersten Jahr benötigen. Deswegen verweisen wir hier auf die Vorlesung *Computeralgebra*.

2.5 LGS - revisited

Wir gucken uns nochmal das erste Kapitel an und überlegen, durch was wir $\mathbb{R}$ ersetzen könnten.

Videos zu diesem Abschnitt

1. Elementare Umformungsmatrizen

2.5.1 Beispiele weiterer Körper

Beispiel 2.5.1

[$\mathbb{Z}/5\mathbb{Z}$ als Körper] Wir wissen bereits, dass $\mathbb{Z}/5\mathbb{Z}$ ein kommutativer Ring mit 1 ist. Also müssen wir nur noch zeigen, dass $\mathbb{Z}/5\mathbb{Z}$ ohne die Null eine kommutative Gruppe bezüglich der Multiplikation bildet.
Wir führen die Notation $\overline{a}$ für einen Vertreter der Äquivalenzklasse $[a]$ ein. Damit betrachten wir nun die multiplikative Verknüpfungstabelle von $\mathbb{Z}/5\mathbb{Z} \setminus \{\overline{0}\}$:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\boxed{\overline{1}}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\boxed{\overline{1}}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\boxed{\overline{1}}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\boxed{\overline{1}}$

Wir sehen sofort die Abgeschlossenheit bezüglich Multiplikation (Nullteilerfreiheit) und die Existenz der Inversen, welche hier durch Kästen markiert wurden. Da $\mathbb{Z}/5\mathbb{Z}$ ein kommutativer Ring mit 1, folgt die Assoziativität und das neutrale Element. Insgesamt muss $\mathbb{Z}/5\mathbb{Z}$ also ein Körper sein.

Proposition 2.5.2

$\mathbb{Z}/m\,\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis. Sei $m \in \mathbb{Z}$.

- "$\Rightarrow$" Man geht durch Kontraposition vor. Sei m also keine Primzahl. Dann gibt es $a, b > 1$, sodass $m = a \cdot b$ und a, b keine Vielfachen von m sind. In $\mathbb{Z}/m\mathbb{Z}$ gilt

$$[0] = [m] = [a \cdot b] = \underbrace{[a]}_{\neq [0]} \cdot \underbrace{[b]}_{\neq [0]}$$

  Damit kann $[a]$ aber kein Inverses haben. Angenommen, es gäbe eines, dann müsste

$$[0] = [a]^{-1} \cdot [0] = [a]^{-1} \cdot ([a] \cdot [b]) = ([a]^{-1} \cdot [a]) \cdot [b] = [b]$$

  gelten. Also kann $\mathbb{Z}/m\mathbb{Z}$ kein Körper sein.

- "$\Leftarrow$" Sei m eine Primzahl. Da bereits gezeigt wurde, dass $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring mit 1 ist, muss nur noch gezeigt werden, dass in $\mathbb{Z}/m\mathbb{Z} \setminus \{[0]\}$ die Inversen bezüglich Multiplikation existieren.

Sei also $0 < a < m$. Gesucht ist $[a]^{-1}$, sodass $[a]^{-1} \cdot [a] = [1]$. Dafür betrachtet man den Gruppenhomomorphismus (bzgl. der Addition):

$$\begin{aligned} \varphi_a : \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ [b] &\mapsto [a \cdot b] \end{aligned}$$

Es sei den geneigten Lesenden überlassen, zu zeigen, dass es sich tatsächlich um einen Gruppenhomomorphismus bezüglich der Addition handelt.

Sei $[b] \in \operatorname{Ker} \varphi_a$. Man schlussfolgert, dass

$$0 = \varphi_a([b]) = [a \cdot b] \Rightarrow m \mid a \cdot b \overset{m \text{ prim und } m \nmid a}{\Rightarrow} m \mid b \Rightarrow [b] = [0].$$

Da b beliebig war, ist $\operatorname{Ker} \varphi_a = \{[0]\}$, womit φ_a injektiv ist. Es sind der Definitionsbereich und der Wertebereich dieselbe Menge. Also ist φ_a auch surjektiv und damit bijektiv. Das heißt aber, dass es zu $[1] \in \mathbb{Z}/m\mathbb{Z}$ genau ein $[b] \in \mathbb{Z}/m\mathbb{Z}$ gibt mit

$$[1] = \varphi_a([b]) = [a \cdot b] = [a] \cdot [b]$$

Da a beliebig war, ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper.

□

Man nennt den Körper aus dem obigen Beweis auch den $\mathbb{F}_m$, den Körper mit m-Elementen, wobei man statt m meistens p schreibt, um zu verdeutlichen, dass es sich um eine Primzahl handelt.

Bemerkung 2.5.3

Wir haben hier unsere Konstruktion von Restklassenringen genutzt und nachgewiesen, dass für den Fall $R = \mathbb{Z}$, der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper ist, wenn m eine Primzahl ist. Wenn wir einen beliebigen kommutativen Ring R nehmen, dann können wir uns genauso fragen, für welche Ideale I der Ring R/I ein Körper ist. Anders als im endlichen Fall von $\mathbb{Z}/m\mathbb{Z}$ reicht es hier nicht aus, dass R/I nullteilerfrei ist, denn z.B. der Polynomring $\mathbb{R}[x]$ ist nullteilerfrei aber kein Körper. Für den Ring $\mathbb{R}[x]$ werden wir diese Frage erst in der Vorlesung *Computeralgebra* beantworten. Im folgenden betrachten wir, auf eine andere Art und Weise, den Restklassenring $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ und Sie dürfen sich überlegen, wieso die beiden Konstruktionen übereinstimmen.

Definition 2.5.4

Auf der Menge $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ definieren wir eine Addition durch

$$(a, b) + (c, d) = (a + c, b + d)$$

und eine Multiplikation durch

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

Lemma 2.5.5

Mit diesen Verknüpfungen wird $\mathbb{C}$ zu einem Körper (den **komplexen Zahlen**), das Einselement ist hierbei $(1, 0)$.

Beweis. Wir sehen schnell ein, dass $(\mathbb{C}, +)$ eine abelsche Gruppe ist, diese ist isomorph zur Gruppe $(\mathbb{R}^2, +)$ und das neutrale Element ist $(0, 0)$. Es bleiben noch einige Punkte

1. $(\mathbb{C} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe: Es seien dazu $(a, b), (c, d), (e, f) \in \mathbb{C} \setminus \{0\}$. Dann ist

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

   und

   $$(a,b)\cdot((c,d)\cdot(e,f)) = (a,b)\cdot(ce-df, cf+de) = (a(ce-df)-b(cf+de), a(cf+de)+b(ce-df)).$$

   Also ist die Verknüpfung assoziativ und es gilt

   $$(1,0)\cdot(a,b) = (1\cdot a - 0\cdot b, 1\cdot b, 0\cdot a) = (a,b)\cdot(1,0)$$

   sowie für $(a, b) \neq (0, 0)$ (Achtung, das bedeutet nur, dass mindestens eine Koordinate ungleich Null ist)

   $$(a,b)\cdot(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = (\frac{a^2-(b)(-b)}{a^2+b^2}, \frac{a(-b)+ba}{a^2+b^2} = (1,0).$$

   Damit ist haben wir die Gruppeneigenschaften nachgewiesen und es gilt darüber hinaus

   $$(a,b)\cdot(c,d) = (ac-bd, ad+bc) = (ca-db, da+cb) = (c,d)\cdot(a,b),$$

   also ist die Gruppe kommutativ.

2. Es bleibt zu zeigen, dass die Distributivgesetze gelten, das folgt aber aufgrund der Kommutativität der Multiplikation schon aus

   $$(a,b)\cdot((c,d)+(e,f)) = (a(c+e)-b(d+f), a(d+f)+b(c+e)) = (ac-db, ad+bc)+(ae-bf, af+be).$$

□

Bemerkung 2.5.6

Wir schreiben für $(0, 1)$ im Folgenden i und können damit

$$(a, b) = a + ib$$

schreiben.

2.5.2 LGS und Gauss für beliebige Körper

Wir gehen zurück zu linearen Gleichungssystemen und wollen diese über beliebigen Körpern formulieren. Tatsächlich können wir in den Definitionen 2.1.6, 2.1.9, 2.1.11 die reellen Zahlen durch einen beliebigen Körper $\mathbb{K}$ ersetzen.

Beispiel 2.5.7

Es sei $\mathbb{K} = \mathbb{F}_5$, dann ist

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 & 0 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 2 & 1 \end{pmatrix}$$

Da wir den Begriff eines Rings eingeführt haben, wollen wir hier nachrechnen, dass die Menge der $n \times n$-Matrizen über einem Körper $\mathbb{K}$ eine Ringstruktur besitzt mit der obigen Multiplikation und der komponentenweise Addition.

Lemma 2.5.8

Es sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$, dann ist $(\mathbb{K}^{n\times n}, +\cdot)$ ein Ring mit Eins, wobei die Null die Nullmatrix ist und die Eins die Einheitsmatrix.

Beweis. Der Beweis ist völlig analog zum Fall $K = \mathbb{R}, \mathbb{Q}$. □

Bemerkung 2.5.9

Für beliebigen Körper gilt, dass $(\mathbb{K}^{n\times n}, +, \cdot)$ genau dann nicht kommutativ ist, wenn $n \geq 2$. In jedem Körper $\mathbb{K}$ gibt es $1 \neq 0$ und wir betrachten

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Für beliebiges $n \geq 2$ betten wir diese 2×2-Matrizen oben links ein.

Wie zuvor (Definition 2.1.14) übersetzen wir ein lineares Gleichungssystem $A \cdot x = b$ mit $A \in \mathbb{K}^{m\times n}, x \in K^n, b \in K^m$ in eine erweiterte Koeffizientenmatrix $(A \mid b)$. Wir definieren wie zuvor (Definition 2.1.18) die reduzierte Zeilenstufenform, aus der wir sofort ablesen können, ob ein LGS mindestens eine Lösung hat oder nicht (Proposition 2.1.23).

Bemerkung 2.5.10

Falls $|\mathbb{K}| < \infty$, so hat jedes LGS entweder keine Lösung oder nur endlich viele Lösungen, denn $|\mathbb{K}^n| < \infty$.

Wir müssen uns für den Gauss-Algorithmus jetzt nur überlegen ob wir weiterhin elementare Zeilenoperationen haben. Tatsächlich nutzen wir in Proposition 2.1.25 nur aus, dass $\mathbb{R}$ ein Körper ist, also gilt diese Proposition auch über $\mathbb{K}$. Selbiges gilt für Proposition 2.1.27 und damit haben wir den Gauss-Algorithmus über beliebigen Körpern.

Bemerkung 2.5.11

Tatsächlich können wir LGS und Matrizen genauso für kommutative Ringe betrachten (beispielsweise $\mathbb{Z}$ oder $\mathbb{K}[x]$). Was passiert mit dem Gauss-Algorithmus in diesen Fällen? Kann jede Matrix auf eine reduzierte Zeilenstufenform gebracht werden? Die Antwort darauf ist Nein, wir müssen andere Bedingungen an die reduzierte Form stellen, wir kommen in Lineare Algebra 2 darauf zurück.

Bemerkung 2.5.12

Überlegen Sie sich, was für nicht-kommutative Ringe passiert.

Zusammenfassend haben wir damit bisher die folgende Liste von Körpern kennengelernt:

1. $\mathbb{R}$, die reellen Zahlen.
2. $\mathbb{Q}$, die rationalen Zahlen.
3. $\mathbb{C}$, die komplexen Zahlen.
4. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, für eine Primzahl p.

Es gibt noch viele, viele weitere Körper, die Vorlesung *Computeralgebra* wird sich mehr mit der Körpertheorie beschäftigen.

2.5.3 Matrizen und Gauss

Wir wollen hier unser gewonnenes Wissen über Matrizenmultiplikation nutzen, um elementare Zeilenumformungen und den Gauss-Algorithmus nochmal anders zu betrachten. Dazu betrachten wir folgendes Beispiel

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 6 & 9 \end{pmatrix}$$

Die Linksmultiplikation mit

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$$

bedeutet also, dass wir die zweite Zeile in

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

mit 3 multiplizieren. Ähnliches können wir für die anderen elementaren Zeilenoperationen auch machen. Um die Schreibweise etwas zu vereinfachen, führen wir die folgende Notation für Matrizen ein, die an genau einer Stelle eine 1 haben und ansonsten alle Einträge gleich Null:

$$E_{i,j} \in \mathbb{K}^{n\times n} \text{ mit } (E_{i,j})_{k,\ell} := \begin{cases} 1 & \text{falls } i = k, j = \ell \\ 0 & \text{sonst} \end{cases}.$$

Definition 2.5.13

elem-matrize Es sei $\lambda \neq 0 \in \mathbb{K}$ und $1 \leq i, j \leq n$, dann definieren folgende **Elementarmatrizen**

1. Für $i \neq j$: $E^{i,j} := \mathbb{E}_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$.
2. $E^{\lambda,i} := \mathbb{E}_n + (\lambda - 1)E_{i,i}$.
3. Für $i \neq j$: $E^{\lambda,i,j} := \mathbb{E}_n + \lambda E_{i,j}$

Proposition 2.5.14

Es sei $A \in \mathbb{K}^{n,p}$, dann gilt

1. Die Linksmultiplikation von A mit $E^{i,j}$ vertauscht die Zeilen i und j von A.
2. Die Linksmultiplikation von A mit $E^{\lambda,i}$ multipliziert die i. Zeile von A mit λ.
3. Die Linksmultiplikation von A mit $E^{\lambda,i,j}$ addiert das λ-fache der j. Zeile von A auf die i.-Zeile.

Beweis. Übungsaufgabe. □

Proposition 2.5.15

Es seien $0 \neq \lambda \in \mathbb{K}$ und $1 \leq i, j \leq n$ gegeben, dann gilt:

1. $E^{i,j} \cdot E^{i,j} = \mathbb{E}_n$.
2. $E^{\lambda,j} \cdot E^{\frac{1}{\lambda},j} = \mathbb{E}_n$.
3. $E^{\lambda,i,j} \cdot E^{-\lambda,i,j} = \mathbb{E}_n$.

Die Elementarmatrizen sind also in der Einheitengruppe von $\mathbb{K}^{n\times n}$, mehr noch das (multiplikativ) Inverse einer Elementarmatrix ist wieder eine Elementarmatrix.

Beweis. Wir können das explizit Nachrechnen oder überlegen uns, dass die einzige $n \times n$-Matrix X für die gilt

$$X \cdot A = A \text{ für alle } A \in \mathbb{K}^{n\times p} \forall\, p$$

ist $X = \mathbb{E}_n$. Dann folgt aus der vorherigen Proposition 2.5.14 die Aussage. □

Wir haben also die Operationen im Gaussalgorithmus in Linksmultiplikationen mit Elementarmatrizen umformuliert. Zu einer gegebenen Matrix $A \in \mathbb{K}^{m\times n}$ finden wir eine Folge von Elementarmatrizen $C_1, \ldots, C_s$ so, dass

$$C_s \cdots C_1 \cdot A$$

reduzierte Zeilenstufenform hat. Da die Einheiten eine Gruppe bilden, ist das Produkt der Elementarmatrizen wieder eine Einheit B in $\mathbb{K}^{m\times m}$. Zusammengefasst gibt es also für $A \in \mathbb{K}^{m\times n}$ ein $B \in (\mathbb{K}^{m\times m})^\times$ so, dass $B \cdot A$ reduzierte Zeilenstufenform hat.
Sei nun A eine Einheit, also $A \in \mathrm{GL}_m(\mathbb{K}) \subseteq \mathbb{K}^{m\times m}$, mit der vorherigen Überlegung gibt es also ein $B \in \mathrm{GL}_m(\mathbb{K})$, so dass $B \cdot A$ in reduzierter Zeilenstufenform ist. Wir erinnern uns, dass die reduzierte Zeilenstufenform einer Matrix eindeutig ist.

Proposition 2.5.16

Es sei $A \in \mathrm{GL}_m(\mathbb{K})$, dann ist die reduzierte Zeilenstufenform von A genau die Einheitsmatrix $\mathbb{E}_m$.

Beweis. Angenommen $B \cdot A$ ist in reduzierter Zeilenstufenform. Wir zeigen, dass $B \cdot A$ keine Nullzeile hat:
Angenommen $B \cdot A$ hat eine Nullzeile, o.E. seien die Einträge in der m.-Zeile alle gleich Null. Dann gilt für jede Matrix $D \in \mathbb{K}^{m \times m}$, dass die m.-Zeile in $(B \cdot A) \cdot D$ alle Einträge gleich Null hat. Allerdings ist, da $A, B \in \mathrm{GL}_m(\mathbb{K})$:

$$(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = \mathbb{E}_m.$$

Das ist ein Widerspruch, also hat $B \cdot A$ keine Nullzeile, das bedeutet, dass in der reduzierten Zeilenstufenform genau m Stufen stehen, aber die einzige $m \times m$-Matrix in reduzierter Zeilenstufenform, welche m Stufen besitzt ist $\mathbb{E}_m$. □

Diese Proposition können wir jetzt noch weiter nutzen:

Proposition 2.5.17

Es sei $A \in \mathrm{GL}_m(\mathbb{K})$, dann gibt es Elementarmatrizen $C_1, \ldots, C_s$ mit

$$A = C_1 \cdots C_s.$$

Jede Einheit in $\mathbb{K}^{m \times m}$ ist somit das Produkt von Elementarmatrizen.

Beweis. Wir wissen aus Proposition 2.1.27, Proposition 2.5.16 und Proposition2.5.14, dass es Elementarmatrizen $D_1, \ldots, D_s \in \mathrm{GL}_m(\mathbb{K})$ gibt, so dass

$$(D_s \ldots D_1) \cdot A = \mathbb{E}_m.$$

Aber dann ist

$$A = D_1^{-1} \cdots D_s^{-1}.$$

Wir setzen $C_i := D_i^{-1}$ und wissen mit Proposition 2.5.15, dass die C_i wieder Elementarmatrizen sind. □

Wir haben also gesehen, dass die Einheitengruppe $\mathrm{GL}_m(\mathbb{K})$ **erzeugt** ist von den Elementarmatizen.

2.6 Vektorräume

Wir kommen nun zu einem der wichtigsten Begriffe der linearen Algebra überhaupt: dem Vektorraum. Der Begriff des Vektors wird hier, im Gegensatz zur Schulmathematik, abstrakt und allgemein eingeführt. Die aus der Schulmathematik bekannten Begriffe ergeben sich dann als Spezialfall.

2.6.1 Definition: Vektorraum

Definition 2.6.1

Sei K ein Körper. Ein **K-Vektorraum** $(V, +, \cdot)$ ist eine Menge V mit einer **Addition** $+ : V \times V \longrightarrow V$ und einer **skalaren Multiplikation** $\cdot : K \times V \longrightarrow V, (\lambda, v) \mapsto \lambda \cdot v$. Die folgenden Axiome genügen für alle $\lambda, \mu \in K, v, w \in V$:

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

V2 $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ und $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$.

V3 $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$.

V4 $1 \cdot v = v$.

Die Elemente in einem Vektorraum nennen wir **Vektoren.** Oft schreiben wir für den Vektorraum $(V, +, \cdot)$ auch einfach V, wenn die Operationen klar sind.

Beispiel 2.6.2

1. Sei $(K, +_K, \cdot_K)$ ein beliebiger Körper und $n \geq 1$. Dann ist $K^{m \times n}$ ein Vektorraum. Wir haben bereits gesehen, dass $K^{n \times n}$ eine abelsche Gruppe ist, wir definieren noch die Skalarmultiplikation komponentenweise

   $$k \times K^{n \times n} \longrightarrow K^{n \times n},\ (a_{i,j}) \mapsto (\lambda a_{i,j}).$$

   Die Axiome V1, V2, V3 ergeben sich dann sofort aus der Definition, da die Addition ebenfalls komponentenweise definiert ist.

2. Als Spezialfall des obigen betrachten wir hier $K^{n \times 1} =: K^n$ und formulieren schreiben nochmal explizit die skalare Multiplikation für einen Vektor

   $$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$$

   Sei dafür $\lambda \in K$:

   $$\lambda \cdot x := \begin{pmatrix} \lambda \cdot_K x_1 \\ \vdots \\ \lambda \cdot_K x_n. \end{pmatrix}$$

Wir definieren im K^n die **Einheitsvektoren**:

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots e_n := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

also hat der i-te Einheitsvektor den Eintrag 1 an Stelle i, und sonst 0.

3. Wir können noch weiter spezialisieren und finden $K^{1\times 1} = K$ als K-Vektorraum.

4. Die Lösungen eines homogenen LGS bilden einen Vektorraum: Sei $A \in K^{m\times n}$ die Koeffizientenmatrix des LGS, dann sind die Lösungen des homogenen Gleichungssystems

$$L(A, 0) = \{x \in K^n : Ax = 0\}.$$

Wir zeigen, dass $L(A, 0)$ einen Vektorraum bildet. Dafür erben wir die Addition und die Skalarmultiplikation aus dem K^n, also jeweils komponentenweise. Um die Wohldefiniertheit der Skalarmultiplikation zu erhalten, müssen wir zeigen, dass

$$\text{für alle } x \in L(A, 0) : \text{ für alle } \lambda \in K : \lambda \cdot x \in L(A, 0).$$

Dies erledigen wir durch für alle $x \in L(A, 0)$ für alle $\lambda \in K$:

$$A \cdot (\lambda \cdot x) = (A \cdot \lambda) \cdot x = \lambda \cdot (Ax) = \lambda \cdot 0 = 0$$

V1: Nun müssen wir noch zeigen, dass $L(A, 0)$ eine abelsche Gruppe ist. A definiert einen Gruppenhomomorphismus von $K^n \to K^n$ und $L(A, 0)$ ist der Kern, also eine Untergruppe, also insbesondere eine abelsche Gruppe.

V2-V4: Die Eigenschaften gelten schon im K^n, von dort haben wir die Addition und Skalarmultiplikation geerbt, also gelten diese auch für $L(A, 0)$.

5. $K[x]$ bildet einen Vektorraum:

V0: Die Skalarmultiplikation ist komponentenweise definiert, wenn wir Polynome als Folgen auffassen. Man sieht leicht, dass dann $\lambda \cdot p$ wieder eine endliche Nullfolge ist, also erneut ein Polynom.

V1: $(K[x], +)$ ist bekannterweise eine abelsche Gruppe.

V2-V4: Diese Eigenschaften ergeben sich durch Betrachtung der Koeffizienten und können von den geneigten Lesenden gezeigt werden.

6. Die Menge der Funktionen $\mathfrak{F}$ von $\mathbb{R}$ nach $\mathbb{R}$ mit der Addition $(f + g)(x) := f(x) + g(x)$.

V0: Die Skalarmultiplikation ist definiert als

$$(\lambda \cdot f)(x) := \lambda \cdot f(x),$$

wobei Letzteres die Multiplikation in $\mathbb{R}$ ist.

V1: Die geneigten Lesenden können die Gruppeneigenschaften von $\mathfrak{F}$ nachweisen.

V2-V4: Für diese Axiome nutzen wir die Körpereigenschaften von $\mathbb{R}$ und überlassen den Rest wieder den Lesenden.

7. Der Nullraum $\{0\}$.

8. Der Körper K als K-Vektorraum.

Wir leiten nun aus den definierenden Eigenschaften des Vektorraums einige Regeln ab:

Proposition 2.6.3

Für $\lambda \in K$ und v aus einem K-Vektorraum V gilt:

1. $\lambda \cdot 0_V = 0_V$.
2. $0_K \cdot v = 0_V$.
3. $(-\lambda) \cdot v = \lambda \cdot (-v) = -(\lambda \cdot v)$.
4. $\lambda \cdot v = 0_V \Rightarrow \lambda = 0_K$ oder $v = 0_V$.

Beweis. Sei K ein Körper und V ein K-Vektorraum.

1. für alle $\lambda \in K$:

$$\begin{aligned} \lambda \cdot 0_V + \lambda \cdot 0_V &\overset{\text{V2}}{=} \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V \\ \Rightarrow \lambda \cdot 0_V &= \lambda \cdot 0_V - (\lambda \cdot 0_V) = 0_V \end{aligned}$$

2. für alle $v \in V$:

$$0_K \cdot v + 0_K \cdot v \overset{\text{V2}}{=} (0_K + 0_K) \cdot v = 0_K \cdot v$$

   Analog folgt $0_K \cdot v = 0_V$.

3. Seien $\lambda \in K$ und $v \in V$ beliebig, aber fest. Man zeigt die zweite Gleichheit:

$$\lambda \cdot (-v) + \lambda \cdot v \overset{\text{V2}}{=} \lambda \cdot (-v + v) = \lambda \cdot 0_V = 0_V,$$

   womit $\lambda \cdot (-v) = -(\lambda \cdot v)$. Man zeigt nun die erste Gleichheit mit Hilfe der zweiten Gleichheit:

$$(-\lambda) \cdot v + \lambda \cdot v \overset{\text{V2}}{=} (-\lambda + \lambda) \cdot v = 0_K \cdot v = 0_V$$

   Damit muss $(-\lambda) \cdot v = -(\lambda \cdot v)$.

4. Es seien $\lambda \in K$ und $v \in V$ beliebig, aber fest mit der Eigenschaft $\lambda \cdot v = 0_V$. Angenommen $\lambda \neq 0$, dann existiert λ^{-1}. Mit V3 und V4 folgt dann:

$$v = \lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0_V = 0_V$$

   Wenn $\lambda \cdot v = 0_V$, kann also nur $\lambda = 0_K$ oder $v = 0_V$.

□

Es sei $(V_i)_{i\in I}$ eine Familie von K-Vektorräumen V_i. Dann wird das kartesische Produkt $\Pi_{i\in I}V_i$ zu einem Vektorraum durch

$$(v_i)_{i\in I} + (w_i)_{i\in I} := (v_i + w_i)_{i\in I}.$$

und

$$\lambda \cdot (v_i)_{i\in I} := (\lambda v_i)_{i\in I}.$$

Daraus erhalten wir zum Beispiel den K^n als n-faches kartesisches Produkt von K.

Wie bereits im Kapitel zu Gruppen und Ringen, interessieren uns vor allem die strukturerhaltenden Abbildungen zwischen algebraischen Objekten:

2.6.2 Lineare Abbildungen

Definition 2.6.4

Eine **lineare Abbildung** (oder **Vektorraumhomomorphimus**) $\varphi : V \longrightarrow W$ zwischen K-Vektorräumen V und W ist ein Gruppenhomomorphismus der abelschen Gruppen $(V, +)$ und $(W, +)$ so, dass $\varphi(\lambda v) = \lambda\varphi(v)$ für alle $v \in V, \lambda \in K$.

Beispiel 2.6.5

Sei K ein Körper.

1. Sei $A \in K^{n\times n}$ eine Matrix. Dann ist $f_A : K^n \to K^n : x \mapsto Ax$ eine lineare Abbildung.

2. Sei $\alpha \in K$ und $\pi_\alpha : K[x] \to K$ der zugehörige Einsetzungshomomorphismus. π_α ist eine lineare Abbildung, denn für alle $p, q \in K[x], \lambda \in K$:

   - $\pi_\alpha(p + q) = (p + q)(\alpha) = p(\alpha) + q(\alpha) = \pi_\alpha(p) + \pi_\alpha(q)$
   - $\pi_\alpha(\lambda \cdot p) = (\lambda \cdot p)(\alpha) = \lambda \cdot p(\alpha) = \lambda \cdot \pi_\alpha(p)$

3. Sei $\alpha \in \mathbb{R}$. Die Abbildung $r : \mathbb{R}^2 \to \mathbb{R}^2$, welche die Ebene um den Winkel α rotiert, ist eine lineare Abbildung. Für $x \in \mathbb{R}^2$ gilt:

   $$r(x) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \cdot x$$

   Also ist r eigentlich die Abbildung bezüglich einer Matrix, also linear.

4. Sei $s : \mathbb{R}^2 \to \mathbb{R}^2$ die Spiegelung an der y-Achse. Man stellt analog zu oben fest, dass die Abbildung durch eine Matrix beschrieben werden kann, und zwar mit

   $$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

   Also muss auch s linear sein.

5. $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ ist keine lineare Abbildung. Zum Beispiel gelten

$$f(1 + (-1)) = f(0) = 0 \neq 2 = 1^2 + (-1)^2 = f(1) + f(-1)$$
$$f(2 \cdot 2) = 4^2 = 16 \neq 8 = 2 \cdot 4 = 2 \cdot f(2).$$

6. Man betrachtet die Menge $\mathfrak{F}_{a,b} := \{f : [a, b] \to \mathbb{R} | \, f \text{ stetig } \}$ mit $a < b \in \mathbb{R}$. Stetige Funktionen sind immer integrierbar.[a] Deshalb ist die Abbildung

$$I : \mathfrak{F}_{a,b} \to \mathbb{R} : f \mapsto \int_a^b f(x)dx$$

wohldefiniert. Auf Grund der Eigenschaften des Integrals gelten für alle $f, g \in \mathfrak{F}_{a,b} : \lambda \in \mathbb{R}$:

$$\begin{aligned} I(f + g) &= \int_a^b f(x) + g(x)dx = \int_a^b f(x)dx + \int_a^b g(x)dx \\ &= I(f) + I(g) \end{aligned}$$

und

$$I(\lambda f) = \int_a^b \lambda f(x)dx = \lambda \int_a^b f(x)dx = \lambda \cdot I(f),$$

womit I eine lineare Abbildung ist.

7. $\mathfrak{F}^D := \{f : [a, b] \to \mathbb{R} | f \text{ differenzierbar}\}$. Man definiert die Abbildung $D : \mathfrak{F}^D \to \mathfrak{F} : f \mapsto f'$, welche wegen der Wahl von $\mathfrak{F}^D$ wohldefiniert ist. Nach der Analysis gelten für alle $f, g \in \mathfrak{F}^D :$ für alle $\lambda \in \mathbb{R}$:

$$D(f + g) = (f + g)' = f' + g' = Df + Dg$$

und

$$D(\lambda \cdot f) = (\lambda \cdot f)' = \lambda \cdot f' = \lambda \cdot D(f)$$

Also ist auch D eine lineare Abbildung.

[a] Hier greifen wir den Analysis etwas voraus. Also nehmen Sie die analytischen Aussagen als gegeben an und verschieben deren Überprüfung auf einen anderen Zeitpunkt.

Proposition 2.6.6

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung von K-Vektorräumen. Dann gilt:

1. $\varphi(0) = 0$
2. $\varphi(-v) = -\varphi(v)$.
3. Wenn $\psi : W \longrightarrow U$ eine weitere K-lineare Abbildung ist, dann ist $\psi \circ \varphi : V \longrightarrow U$ eine K-lineare Abbildung.

Beweis (Proposition 2.6.6): Seien K ein Körper, V,W,U K-Vektorräume und $\varphi : V \to$

W und $\psi : W \to U$ lineare Abbildungen. Aussage 1 und 2 folgen sofort, da φ ein Gruppenhomomorphismus ist. Weil ψ auch ein Gruppenhomomorphismus ist, muss $\psi \circ \varphi$ ein Gruppenhomomorphismus sein. Es bleibt also, die Verträglichkeit mit der skalaren Multiplikation zu zeigen: für alle $\lambda \in K$: für alle $v \in V$:

$$\psi \circ \varphi(\lambda v) = \psi(\varphi(\lambda v)) = \psi(\lambda \cdot \varphi(v)) = \lambda \cdot \psi(\varphi(v)),$$

wobei die letzten beiden Gleichheiten gelten, weil φ und ψ linear sind. Also ist $\psi \circ \varphi : V \to U$ eine K-lineare Abbildung. □

Definition 2.6.7

Eine K-lineare Abbildung $\varphi : V \longrightarrow W$ heißt **Isomorphimus**, wenn es eine K-lineare Abbildung $\psi : W \longrightarrow V$ gibt mit:

$$\psi \circ \varphi = \mathrm{id}_V \text{ und } \phi \circ \psi = \mathrm{id}_W .$$

Wenn es zwischen zwei Vektorräumen V und W einen Isomorphismus gibt, so nennen wir diese Vektorräume **isomorph**.

Beispiel 2.6.8

1. Für jeden Vektorraum V ist id_V ein Isomorphismus, da $\mathrm{id}_V \circ \mathrm{id}_V = \mathrm{id}_V$.
2. Seien $A, B \in K^{n\times n}$ so, dass $AB = \mathbb{E} = BA$. Dann ist f_A ein Isomorphismus mit f_B als Inverses.
3. Die Abbildung
$$p : \mathbb{R}^2 \to \mathbb{C} : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto x + iy$$
ist linear und besitzt das Inverse
$$p : \mathbb{R}^2 \to \mathbb{C} : x + iy \mapsto \begin{pmatrix} x \\ y, \end{pmatrix}$$
also ist $\mathbb{R}^2$ isomorph zu $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.

Proposition 2.6.9

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Dann sind äquivalent:

1. φ ist ein Isomorphismus.
2. φ ist bijektiv.

Beispiel 2.6.10

Polynome vom Grad $\leq n$ und der K^{n+1}: Man definiert $P_n := \{p \in K[x] :$

$\text{grad}(p) \leq n\}$. Die Abbildung

$$P_n \to K^{n+1}$$
$$a_0 + a_1 x^1 + \ldots + a_n x^n \mapsto (a_0, a_1, \ldots, a_n)$$

ist offensichtlich linear, aber auch bijektiv, da P_n genau die Folgen sind, die ab dem $n+2$-Folgeglied 0 sind, was aber sofort die Bijektion zum K^{n+1} liefert.

Beweis (Proposition 2.6.9): Sei $\varphi : V \longrightarrow W$ eine K-lineare Abbildung

(2) $\Rightarrow$ (1): Da φ bijektiv ist, gibt es eine Umkehrabbildung $\psi : W \to V$, die ein Gruppenhomomorphismus ist. Es bleibt also, die Verträglichkeit zur skalaren Multiplikation zu zeigen: für alle $w \in W$: für alle $\lambda \in K$:

$$\varphi(\psi(\lambda w)) = \lambda w$$
$$\varphi(\lambda\psi(w)) = \lambda \cdot \varphi(\psi(w)) = \lambda w$$

Da φ injektiv ist, folgt:

$$\lambda\psi(w) = \psi(\lambda w)$$

Damit ist ψ linear und folglich φ ein Isomorphismus.

(1) $\Rightarrow$ (2) : Per Definition muss φ bijektiv sein.

□

Definition 2.6.11

Eine Teilmenge U des K-Vektorraums V heißt Untervektorraum oder Unterraum von V genau dann, wenn folgende Axiome erfüllt sind:

U1 $u_1, u_2 \in U \Longrightarrow u_1 + u_2 \in U$

U2 $\lambda \in K, u \in U \quad \Longrightarrow \quad \lambda u \in U.$

U3 $0 \in U.$

U3 ist notwendig, um $U = \emptyset$ auszuschliessen.

Beispiel 2.6.12

1. Sei $U \subset V$ ein Unterraum. Dann ist U insbesondere eine Untergruppe, da sie wegen U1 abgeschlossen bezüglich der Addition ist. Wegen U3 ist das neutrale Element enthalten. Und wegen U2 gilt für alle $u \in U$:
$$-u = (-1) \cdot u \in U$$
2. Man betrachtet das LGS
$$\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 - x_2 + x_3 &= 0 \\ x_2 + x_3 &= 0 \end{aligned}$$
,

welches den Lösungsraum $\mathcal{L}_1$ besitzt. Betrachtet man nun nur die ersten beiden Gleichungen des LGS, dann erhält man einen größeren Lösungsraum $\mathcal{L}_2$. Es ist $\mathcal{L}_1 \subset \mathcal{L}_2$ und $\mathcal{L}_1$ erfüllt U1-U3, weil $\mathcal{L}_1$ ein Unterraum ist.

3. Seien K ein Körper und $m < n$ natürliche Zahlen. Man erinnere sich daran, dass P_n der Vektorraum der Polynome vom Grad kleiner gleich n ist. Dann ist P_m ein Untervektorraum von P_n.

4. Es bilden

$$\mathfrak{F}^D \subset \mathfrak{F}_{-\infty,\infty} \subset \mathfrak{F}$$

eine Kette von Untervektorräumen, wobei $\mathfrak{F}^D$ die differenzierbaren Abbildungen sind.

Proposition 2.6.13

Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Dann ist $\operatorname{Ker}\varphi$ ein Unterraum von V, $\operatorname{Im}\varphi$ ein Unterraum von W.

Beweis (Proposition 2.6.13): Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Aus der Gruppentheorie wissen wir, dass $\operatorname{Ker}\varphi$ und $\operatorname{Im}\varphi$ Untergruppen von V und W sein müssen. Damit sind bereits die Axiome U1 und U2 erfüllt.

Seien nun $v \in \operatorname{Ker}(\varphi), \lambda \in K$ beliebig, dann

$$\varphi(\lambda v) = \lambda\varphi(v) = \lambda \cdot 0_W = 0_W,$$

womit $\lambda v \in \operatorname{Ker}(\varphi)$ und U2 für den Kern erfüllt ist.

Seien nun $w \in \operatorname{Im}(\varphi), \lambda \in K$ beliebig, dann gibt es $v \in V$ mit $w = \varphi(v)$. Also gilt

$$\lambda w = \lambda\varphi(v) = \varphi(\lambda v) \in \operatorname{Im}(\varphi).$$

Damit gilt auch U2 für $\operatorname{Im}\varphi$, womit sowohl der Kern als auch das Bild von φ Unterräume sind. □

Proposition 2.6.14

Es seien U_1, U_2 Unterräume eines Vektorraums V, dann ist auch

$$U_1 + U_2 = \{u_1 + u_2 \in V \mid u_1 \in U_1, u_2 \in U_2\}$$

ein Unterraum von V.

Beweis (Proposition 2.6.14): Seien K ein Körper, V ein K-Vektorraum und U_1, U_2 Unterräume von V.

U0: $U_1 + U_2$ ist ein wohldefinierter Ausdruck, da für alle $u_1 \in U_1$: für alle $u_2 \in U_2$: $u_1, u_2 \in V \Rightarrow u_1 + u_2 \in V$.

U1: Es gilt für alle $u_1, \tilde{u}_1 \in U_1$: für alle $u_2, \tilde{u}_2 \in U_2$:

$$(u_1 + u_2) + (\tilde{u}_1 + \tilde{u}_2) \overset{(V,+) \text{ abelsch}}{=} \underbrace{\underbrace{(u_1 + \tilde{u}_1)}_{\in U_1} + \underbrace{(u_2 + \tilde{u}_2)}_{\in U_2}}_{\in U_1 + U_2}$$

U2: Außerdem gilt für alle $u_1 \in U_1, u_2 \in U_2$: für alle $\lambda \in K$:

$$\lambda \cdot (u_1 + u_2) = \underbrace{\lambda u_1}_{\in U_1} + \underbrace{\lambda u_2}_{\in U_2} \in U_1 + U_2$$

U3: Es gilt $0 \in U_1 + U_2$, da $0 \in U_1, U_2$ und $0 + 0 = 0$.

Also ist $U_1 + U_2$ ein Untervektorraum von V. □

Proposition 2.6.15

Es sei $(U_i)_{i \in I}$ eine Familie von Unterräumen eines Vektorraums V. Dann ist auch $\bigcap_{i \in I} U_i$ ein Unterraum von V.

Beweis (Proposition 2.6.15): Seien K ein Körper, V ein K-Vektorraum und $(U_i)_{i \in I}$ eine Familie von Unterräumen von V.

U1: Es seien $u, u' \in \bigcap_{i \in I} U_i$ beliebig, aber fest. Dann gilt für alle $i \in I : u, u' \in U_i$, womit auch $u + u' \in U_i$ gelten muss, da die U_i Unterräume sind. Damit ist aber $u + u' \in \bigcap_{i \in I} U_i$.

U2: Es gilt für alle $u \in \bigcap_{i \in I} U_i$: für alle $\lambda \in K$:

$$\text{für alle } i \in I : u \in U_i \Rightarrow \lambda u \in U_i,$$

womit $\lambda u \in \bigcap_{i \in I} U_i$.

U3: Da für alle $i \in I : 0 \in U_i$, ist $0 \in \bigcap_{i \in I} U_i$.

Damit ist $\bigcap_{i \in I} U_i$ ein Unterraum. □

Proposition 2.6.16

Es seien U_1, U_2 Unterräume eines Vektorraums V und $U := U_1 + U_2$. Dann sind die folgenden Bedingungen äquivalent

1. $U_1 \cap U_2 = \{0\}$
2. $\forall\, u \in U$ gilt: $\exists!\, (u_1, u_2) \in U_1 \times U_2$ mit $u = u_1 + u_2$.

Ist eine der beiden Bedingungen erfüllt, so heißt U die **direkte Summe** von U_1 und U_2, mit der Notation $U_1 \oplus U_2$.

Beweis (Proposition 2.6.16): Seien K ein Körper, V ein K-Vektorraum und U_1, U_2 Unterräume von V mit $U_1 + U_2 = V$.

(1) $\Rightarrow$ (2) Es ist $U_1 \cap U_2 = \{0\}$. Sei $v \in V$ beliebig, aber fest. Dann gibt es wegen $U_1 + U_2 = V$ Vektoren $u_1 \in U_1$ und $u_2 \in U_2$, sodass $v = u_1 + u_2$.

Angenommen, es gibt $\tilde{u}_1 \in U_1$ und $\tilde{u}_2 \in U_2$ mit $v = \tilde{u}_1 + \tilde{u}_2$. Dann gilt

$$u_1 - \tilde{u}_1 = \tilde{u}_2 - u_2,$$

wobei $u_1 - \tilde{u}_1 \in U_1$ und $u_1 - \tilde{u}_1 = \tilde{u}_2 - u_2 \in U_2$. Damit sind $u_1 - \tilde{u}_1 = \tilde{u}_2 - u_2 \in U_1 \cap U_2 = \{0\}$, womit

$$u_1 = \tilde{u}_1$$
$$u_2 = \tilde{u}_2.$$

Also ist die Darstellung von v durch u_1, u_2 eindeutig.

(2) $\Rightarrow$ (1) Es ist $0 \in U_1$ und $0 \in U_2$. Sei nun $v \in U_1 \cap U_2$ beliebig:

$$v = \underbrace{v}_{\in U_1} + \underbrace{0}_{\in U_2} = \underbrace{0}_{\in U_1} + \underbrace{v}_{\in U_2}$$

Da nach (2) die Darstellung eindeutig ist, gilt $v = 0$. Wegen v beliebig ist $U_1 \cap U_2 = \{0\}$.

□

Beispiel 2.6.17

Seien $n, m \in \mathbb{N}$

V	U_1	U_2	$U_1 + U_2$	$U_1 \cap U_2$
$\mathbb{R}^2$	$\{(x, 0)\}$ (x-Achse)	$\{(0, y)\}$ (y-Achse)	$\mathbb{R}^2$	$\{0, 0\}$
P_n	P_m	P_n	P_n	P_m

Die direkte Summe aus Proposition 2.6.16 bezeichnet man auch mit $\oplus$. So ist $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$.

Ähnlich wie bei der Behandlung von Gruppen, gehen wir nach der Betrachtung von Unterstrukturen dazu über, Quotienten- bzw. Faktorstrukturen zu betrachten.

Es sei $W \subset V$ ein Unterraum, also auch eine Untergruppe bzgl. $+$. Also können wir die Kongruenz modulo W betrachten:

$$v_1 \equiv v_2 (\mathrm{mod}\, W) :\Leftrightarrow v_1 - v_2 \in W.$$

Die Menge der Äquivalenzklassen heißt **Quotientenraum** und wird mit V/W bezeichnet.

Proposition 2.6.18

Seien V K-Vektorraum und $W \subset V$ ein Unterraum. V/W ist ein K-Vektorraum mit den Operationen

$$[v] + [w] := [v + w] \text{ und } \lambda[v] := [\lambda v].$$

Beweis (Proposition 2.6.18): Seien V K-Vektorraum und $W \subset V$ ein Unterraum.

V0: Die Skalarmultiplikation ist wohldefiniert, denn seien $[v] = [v'] \in V/W$ mit $v \neq v'$ und $\lambda \in K$, dann gilt $v - v' \in W$ per Definition, womit

$$\lambda v - \lambda v' = \lambda(v - v') \in W,$$

da V ein Vektorraum ist und W ein Unterraum. Das bedeutet:

$$[\lambda v] = [\lambda v']$$

V1: $(V/W, +)$ ist nach der behandelten Gruppentheorie eine abelsche Gruppe mit $[0]$ als neutralem Element und für alle $v \in V : -[v] = [-v]$.

V2: Seien $v, w \in V$ und $\lambda, \mu \in K$ beliebig, aber fest. Dann gelten

$$(\lambda + \mu)[v] = [(\lambda + \mu)v] = [\lambda v + \mu v] = [\lambda v] + [\mu v] = \lambda[v] + \mu[v]$$

und

$$\begin{aligned}\lambda([v] + [w]) = \lambda[v + w] = [\lambda(v + w)] = [\lambda v + \lambda w] \\ = [\lambda v] + [\lambda w] = \lambda[v] + \lambda[w].\end{aligned}$$

V3: Seien $v \in V$ und $\lambda, \mu \in K$ beliebig, aber fest. Dann gilt:

$$\lambda(\mu[v]) = \lambda[\mu v] = [\lambda(\mu v)] = [(\lambda\mu)v] = (\lambda\mu)[v]$$

V4: Die Eigenschaft folgt aus der Definition der Skalarmultiplikation und der Vektorraumeigenschaft von V (für alle $v \in V : 1 \cdot v = v$).

□

Proposition 2.6.19

Die kanonische Abbildung $\pi : V \longrightarrow V/W, v \mapsto [v]$ ist eine surjektive, lineare Abbildung mit $\mathrm{Ker}(\pi) = W$.

Beweis (Proposition 2.6.19): Seien V K-Vektorraum und $W \subset V$ ein Unterraum. Aus der Gruppentheorie ist bekannt, dass

$$\pi : V \to V/W : v \mapsto [v]$$

ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}(\pi) = W$ ist. Es bleibt, die Linearität bezüglich Skalarmultiplikation zu zeigen. Per Definition der Skalarmultiplikation gilt für alle $v \in V :$ für alle $\lambda \in K :$

$$\pi(\lambda v) = [\lambda v] = \lambda[v] = \lambda\pi(v)$$

Damit ist π linear. □

Beispiel 2.6.20

Kanonischer Isomorphismus:
Seien V K-Vektorraum und $U, W \subset V$ Unterräume und $U \cap W = \{0\}$. Dann gibt es eine Injektion

$$\iota : U \to U \oplus W : u \mapsto u + 0$$

und die kanonische Surjektion

$$\pi : U \oplus W \to (U \oplus W)/W : u + w \mapsto [u + w].$$

Man definiert $f := \pi \circ \iota$. Da sowohl ι als auch π linear sind, ist f linear. Es gilt

$$\mathrm{Ker}(f) = \{u \in U : [u] = [0] = W\} = U \cap W = \{0\},$$

womit f injektiv ist.
Sei nun $[u + w] \in (U \oplus W)/W$ beliebig, aber fest. Es gilt

$$(u + w) - u = w \in W,$$

womit $[u + w] = [u]$, wofür wiederum

$$[u] = \pi(u) = \pi(u + 0) = \pi(\iota(u)) = f(u)$$

gilt. Also ist f surjektiv und insgesamt bijektiv. Man nennt f den kanonischen Isomorphismus.

Wir beginnen nun mit einer Tätigkeit, die Ihnen im Laufe der Algebra immer häufiger begegnen wird: dem Zeichnen von sogenannten kommutativen Diagrammen. In einem derartigen Diagramm wird die Beziehung verschiedener algebraischer Objekte und deren Abbildungen zueinander dargestellt. Unser erstes Beispiel ist hierbei der Homomorphiesatz.

Theorem 2.6.21

Sei $\varphi : V_1 \longrightarrow V_2$ eine lineare Abbildung, $W_1 \subset V_1$ ein Unterraum. Es gibt genau dann eine lineare Abbildung

$$\overline{\varphi} : V_1/W_1 \longrightarrow V_2$$

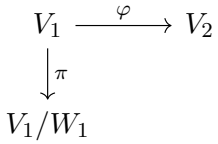
mit $\overline{\varphi}([v_1]) = \varphi(v_1)$ für alle $v_1 \in V_1$, wenn $W_1 \subseteq \mathrm{Ker}(\varphi)$. In diesem Fall ist $\overline{\varphi}$ eindeutig.

Satz 2.6.22

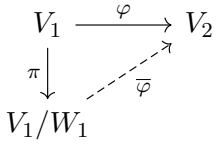
Sei $\varphi : V_1 \longrightarrow V_2$ eine lineare Abbildung. Dann ist $\overline{\varphi}$ ein Isomorphismus:

$$\overline{\varphi} : V_1/\mathrm{Ker}(\varphi) \xrightarrow{\sim} \varphi(V_1),\ [v_1] \mapsto \varphi(v_1).$$

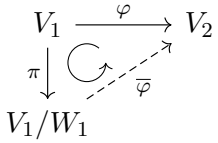
Man beginnt das Bild mit den gegebenen Abbildungen φ und der kanonischen Abbildung π



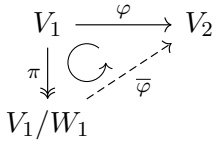
Der Homomorphiesatz sagt nun aus, dass es eine dritte Abbildung $\overline{\varphi}$ gibt, sodass das Diagramm



kommutiert. Mit kommutieren ist gemeint, dass es keinen Unterschied macht, ob man oben lang geht oder unten herum. Formal also $\varphi = \overline{\varphi} \circ \pi$. Um die Kommutativität im Diagramm selbst auszudrücken, zeichnet man häufig einen Kringel in die Mitte:

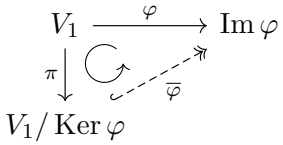


Man kann das Diagramm aber noch mehr erweitern. Zum Beispiel kann durch Modifikation der Pfeile angegeben werden, dass es sich bei π um eine surjektive Abbildung handelt:



Man tut dies jedoch nur, wenn man die Surjektivität betonen möchte. Zeichnet man zu viel ein, wird das Diagramm unübersichtlich und das Wesentliche geht verloren.

Das Diagramm zum Isomorphiesatz ist



.

Der Haken am Ende von Pfeil von $\overline{\varphi}$ drückt aus, dass es sich um eine injektive Abbildung handelt. Die doppelte Spitze symbolisiert die Surjektivität.

Man geht nun dazu über, die Sätze zu beweisen:

Beweis (Theorem 1.8.6): Sei $\varphi : V_1 \longrightarrow V_2$ eine lineare Abbildung, $W_1 \subset V_1$ ein Unterraum mit $W_1 \subseteq \mathrm{Ker}(\varphi)$. Man definiert

$$\begin{aligned} \overline{\varphi} : V_1/W_1 &\to V_2 \\ [v_1] &\mapsto \varphi(v_1). \end{aligned}$$

Da π surjektiv ist, legt die Bedingung, dass eine Abbildung das Diagramm zum Kommutieren bringen soll, bereits alle Bilder der Abbildung fest. Damit ist $\overline{\varphi}$ der einzige Kandidat, um das Diagramm zum Kommutieren zu bringen.

$$\begin{array}{ccc} V_1 & \xrightarrow{\varphi} & V_2 \\ {\scriptstyle\pi}\big\downarrow & & \\ V_1/W_1 & & \end{array}$$

Man zeigt nun, dass $\overline{\varphi}$ vertreterunabhängig ist: Seien also $v' \in [v] \in V_1/W_1$. Damit gilt $v - v' \in W_1$ und wegen $W_1 \subset \mathrm{Ker}\,\varphi$

$$0 = \varphi(v - v') = \varphi(v) - \varphi(v') \Leftrightarrow \varphi(v) = \varphi(v').$$

Es bleibt zu zeigen, dass $\overline{\varphi}$ linear ist. Seien $[v_1], [v_2] \in V_1/W_1$ und $\lambda \in K$ beliebig, aber fest:

$$\begin{aligned} \overline{\varphi}(\lambda[v_1] + [v_2]) = \overline{\varphi}([\lambda v_1 + v_2]) = \varphi(\lambda v_1 + v_2) &= \lambda\varphi(v_1) + \varphi(v_2) \\ &= \lambda\overline{\varphi}(v_1) + \overline{\varphi}(v_2) \end{aligned}$$

Also ist $\overline{\varphi}$ linear. □

Beweis (Satz 2.6.2): Sei $\varphi : V_1 \longrightarrow V_2$ eine lineare Abbildung. Man setzt ohne Beschränkung der Allgemeinheit $V_2 = \mathrm{Im}\,\varphi$. Also gilt nach 1.8.6, dass $\overline{\varphi}$ linear ist. Nach dem Isomorphiesatz für Gruppen folgt die Bijektivität. □

2.6.3 Räume von Abbildungen

Es seien V_1, V_2 jeweils K-Vektorräume und es sei

$$\mathrm{Hom}_K(V_1, V_2) := \{\varphi : V_1 \longrightarrow V_2 \mid \varphi \text{ ist eine lineare Abbildung}\}.$$

Proposition 2.6.23

$\mathrm{Hom}_K(V_1, V_2)$ wird zu einem K-Vektorraum mit

$$\phi + \psi : V_1 \longrightarrow V_2,\ v \mapsto \phi(v) + \psi(v) \text{ und } \lambda \cdot \phi : V_1 \longrightarrow V_2,\ v \mapsto \lambda\varphi(v).$$

Beweis. Es seien V_1, V_2 jeweils K-Vektorräume.

V1: Man zeigt, dass es sich bei $(\mathrm{Hom}_K(V_1, V_2), +)$ um eine abelsche Gruppe handelt:

G1: Die Assoziativität erhält man durch Rückführung auf die Bilder, welche schließlich in einem Vektorraum liegen.

G2: Als neutrales Element verwendet man die Nullabbildung:

$$0 : V_1 \to V_2 : v_1 \mapsto 0_{V_2}$$

Die Neutralität ergibt sich durch Rückführung auf die Bilder.

G3: Zu einer Abbildung $\phi \in \mathrm{Hom}_K(V_1, V_2)$ bildet man das Inverse, indem man

$$(-\phi) : V_1 \to V_2 : v_1 \mapsto -\phi(v_2)$$

definiert. Der Nachweis, dass es sich um ein Inverses handelt, geschieht ebenfalls auf Ebene der Bilder.

V2: Seien $\lambda \in K$ und $\phi, \psi \in \mathrm{Hom}_K(V_1, V_2)$ beliebig, aber fest: für alle $v \in V$

$$\begin{aligned}(\lambda \cdot (\phi + \psi))(v) &= \lambda \cdot ((\phi + \psi)(v)) = \lambda \cdot (\phi(v) + \psi(v)) \\ &= \lambda \cdot (\phi(v)) + \lambda(\cdot\psi(v)) = (\lambda \cdot \phi)(v) + (\lambda \cdot \psi)(v) \\ &= (\lambda \cdot \phi + \lambda \cdot \psi)(v)\end{aligned}$$

Das zweite Distributivgesetz folgt analog.

V3-V4: Erfolgt ebenfalls durch Rückführung auf die Bilder.

□

Zwei Spezialfälle wollen wir hier betrachten, zum einen

Definition 2.6.24

Es sei V ein Vektorraum, dann bezeichnen wir $\mathrm{Hom}_K(V, V)$ als $\mathrm{End}_K(V)$, den Raum der Endomorphismen von V.

Beispiel 2.6.25

Einige Beispiele dazu

1. Wir haben schon gesehen, dass $A \in \mathrm{End}_K(K^n)$ für jede Matrix $A \in K^{n \times n}$. Wir werden später sehen, dass wir in diesem Fall $\mathrm{End}_K(K^n)$ mit den $n \times n$-Matrizen identifizieren können.
2. Es sei $V = K[x]$ und für $p = \sum_{i=0}^{n} a_i x^i$ definieren wir die formale Ableitung $\frac{\partial}{\partial x} p = \sum_{i=1}^{n} i \cdot a_i x^{i-1}$. Das ist, wie vorher schon gesehen, eine lineare Abbildung und damit ist $\frac{\partial}{\partial x} \in \mathrm{End}_K(K[x])$.

Definition 2.6.26

Für den Spezialfall $V_2 = K$ nennen wir $\mathrm{Hom}_K(V_1, K)$ den **Dualraum** von V_1 und schreiben dafür V_1^*. Die Elemente aus V_1^* nennen wir **Linearformen**.

Beispiel 2.6.27

Sei $V_1 = \mathbb{R}^n$. Für $v \in \mathbb{R}^n$ gilt:

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

Man definiert

$$\varphi : \mathbb{R}^n \to \mathbb{R} : v \mapsto a_1 + \ldots + a_n.$$

Bei φ handelt es sich um eine Linearform, womit $\varphi \in (\mathbb{R}^n)^*$.

Proposition 2.6.28

Die Abbildung

$$\langle \cdot, \cdot \rangle : V^* \times V \longrightarrow K,\ (f, v) \mapsto f(v)$$

ist bilinear, also für alle $\lambda, \mu \in K, v_1, v_2 \in V, f_1, f_2 \in V^*$ gilt

$$\langle \mu f_1 + f_2, \lambda v_1 + v_2 \rangle = \lambda\mu\langle f_1, v_1\rangle + \lambda\langle f_2, v_1\rangle + \mu\langle f_1, v_2\rangle + \langle f_2, v_2\rangle.$$

Bilinearität bedeutet, dass eine Abbildung sowohl im 1. als auch im 2. Argument linear ist und dies unabhängig voneinander geschieht. Das bedeutet, die Abbildung als Ganzes gesehen ist nicht linear. Mit den Bezeichnungen von oben ist im Allgemeinen

$$\langle \mu f_1 + f_2, \lambda v_1 + v_2 \rangle \neq \langle \mu f_1, v_2\rangle + \langle f_2, \lambda v_1\rangle.$$

Beweis. Es gilt für alle $\lambda, \mu \in K, v_1, v_2 \in V, f_1, f_2 \in V^* = \mathrm{Hom}(V, K)$

$$\begin{aligned} \langle \mu f_1 + f_2, \lambda v_1 + v_2 \rangle &= (\mu f_1 + f_2)(\lambda v_1 + v_2) \\ &\overset{\mathrm{Hom}(V,K) \text{ VR.}}{=} \mu f_1(\lambda v_1 + v_2) + f_2(\lambda v_1 + v_2) \\ &\overset{f_1, f_2\ K\text{-lin.}}{=} \mu\lambda f_1(v_1) + \mu f_1(v_2) + \lambda f_2(v_1) + f_2(v_2) \\ &= \lambda\mu\langle f_1, v_1\rangle + \lambda\langle f_2, v_1\rangle + \mu\langle f_1, v_2\rangle + \langle f_2, v_2\rangle. \end{aligned}$$

□

Beispiel 2.6.29

Seien $V = \mathbb{R}^n$ und $A \in \mathbb{R}^{1\times n}$. Dann ist

$$\varphi_A : \mathbb{R}^n \to \mathbb{R} : v \mapsto Av$$

eine $\mathbb{R}$-lineare Abbildung. Daraus schließen wir, dass $\mathbb{R}^{1\times n} \subset (\mathbb{R}^n)^*$. Wie wir später sehen werden, gilt sogar Gleichheit.

2.6.4 Bonus: Moduln über Ringen I

In diesem Abschnitt möchten wir den Körper K durch einen Ring R ersetzen und überlegen, was denn dann ein "Vektorraum" über einem Ring ist und welche der Eigenschaften dann immer noch gelten:

Definition 2.6.30

modul Es sei R ein Ring (mit Eins) und M eine abelsche Gruppe. Dann heißt M ein **Linksmodul** über R oder ein R-Linksmodul, falls es eine Abbildung

$$R \times M \longrightarrow M,\ (r, m) \mapsto r.m$$

gibt mit den Eigenschaften:

1. $r_1.(r_2.m) = (r_1 \cdot r_2).m$ für alle $r_1, r_2 \in R$, $m \in M$.
2. $(r_1 + r_2).m = r_1.m + r_2.m$ für alle $r_1, r_2 \in R$, $m \in M$.
3. $r.(m_1 + m_2) = r.m_1 + r.m_2$ für alle $r \in R$, $m_1, m_2 \in M$.
4. $1.m = m$ für alle $m \in M$.

Bemerkung 2.6.31

Die Betonung bei *dem Modul* liegt auf dem "o", das *Modul* mit der Betonung auf dem "u" belegen Sie aktuell und es heißt *Lineare Algebra 1*

Bemerkung 2.6.32

Wir können Moduln auch für Ringe ohne Eins definieren, dann würde die letzte Bedingung wegfallen. Manchmal nennen wir Linksmoduln mit der letzten Bedingung auch **unitäre Linksmoduln**

Bemerkung 2.6.33

Ein **Rechtsmodul** ist dann eine abelsche Gruppe M mit einer Abbildung $M \times R \longrightarrow M$, $(m, r) \mapsto m.r$ mit den Eigenschaften:

1. $(m.r_1).r_2 = m.(r_1 \cdot r_2)$ für alle $r_1, r_2 \in R$, $m \in M$.
2. $m.(r_1 + r_2) = m.r_1 + m.r_2$ für alle $r_1, r_2 \in R$, $m \in M$.
3. $(m_1 + m_2).r = m_1.r + m_2.r$ für alle $r \in R$, $m_1, m_2 \in M$.
4. $m.1 = m$ für alle $m \in M$.

Beispiel 2.6.34

Einige Beispiele zu Moduln:

1. Jeder K-Vektorraum V über einem Körper K ist auch ein K-Modul.
2. Jede abelsche Gruppe G ist ein $\mathbb{Z}$-Modul wie in Proposition 2.6.36 bewiesen.
3. $\mathbb{K}^n$ ist ein $\mathbb{K}^{n\times n}$-Modul durch $(A, v) \mapsto A.v$.
4. Es sei M die triviale abelsche Gruppe, dann ist M für jeden Ring R ein Linksmodul.

Bemerkung 2.6.35

Für einen kommutative Ring unterscheiden wir nicht zwischen Links- und Rechtsmoduln, sondern sagen einfach nur Modul.

Proposition 2.6.36

Es sei G eine abelsche Gruppe, wird G zu einem $\mathbb{Z}$-Modul durch

$$\mathbb{Z} \times G \longrightarrow G,\ (a,g) \mapsto \begin{cases} a \cdot g := g + \ldots + g & \text{falls } a > 0 \\ a \cdot g := -g - \ldots - g & \text{falls } a < 0 \\ 0_G & \text{falls } a = 0 \end{cases}$$

Beweis. □

Proposition 2.6.37

Es seien R, S Ringe. M ein R-Modul, und $\varphi : S \longrightarrow R$ ein Ringhomomorphismus, dann wird M zu einem S-Modul durch

$$S \times M \longrightarrow M,\ (s,m) \mapsto \varphi(s).m$$

Beweis. □

Bemerkung 2.6.38

Es sei $A \in \mathbb{K}^{n\times n}$, dann ist die Abbildung

$$\pi_A : \mathbb{K}[x] \longrightarrow \mathbb{K}^{n\times n},\ p = \sum_{i=0}^{k} a_i x^i \mapsto p(A) = \sum_{i=0}^{k} a_i A^i$$

ein Ringhomomorphismus, der Einsetzungshomomorphismus. Andererseits ist $\mathbb{K}^n$ ein $\mathbb{K}^{n\times n}$-Modul. Mit Proposition 2.6.37, erhalten wir also für jedes $A \in \mathbb{K}^{n\times n}$ eine $\mathbb{K}[x]$-Modulstruktur auf K^n, wir bezeichnen diesen Modul mit $\mathbb{K}^n_A$.

2.6.5 Der Bidualraum und die duale Abbildung

Für ein festes $v \in V$ ist

$$\langle \_, v\rangle : V^* \longrightarrow K,\ f \mapsto \langle f, v\rangle$$

eine lineare Abbildung, also in $(V^*)^*$.

Proposition 2.6.39

Die Abbildung

$$\iota : V \longrightarrow (V^*)^* :\ v \mapsto \langle \_, v\rangle$$

ist linear.

Beweis (Proposition 2.6.39): Seien $v_1, v_2 \in V$ und $\lambda \in K$ beliebig, aber fest. Dann gilt für alle $f \in V^*$:

$$\begin{aligned}(\iota(\lambda v_1 + v_2))(f) &= \langle f, \lambda v_1 + v_2\rangle = \lambda\langle f, v_1\rangle + \langle f, v_2\rangle \\ &= \lambda(\iota(v_1))(f) + (\iota(v_2))(f) \\ &= (\lambda\iota(v_1) + \iota(v_2))(f)\end{aligned}$$

Damit gilt

$$\iota(\lambda v_1 + v_2) = \lambda\iota(v_1) + \iota(v_2),$$

was ι linear macht. □

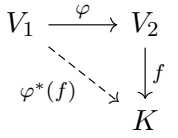
Proposition 2.6.40

Sei $\varphi : V_1 \longrightarrow V_2$ eine lineare Abbildung. Dann existiert genau eine Abbildung $\varphi^* : V_2^* \longrightarrow V_1^*$ so, dass für alle $v \in V_1, f \in V_2^*$ gilt

$$\langle f, \varphi(v)\rangle = \langle \varphi^*(f), v\rangle.$$

Diese Abbildung ist linear und gegeben durch $\varphi^*(f) = f \circ \varphi$ für alle $f \in V_2^*$.

Beweis. Sei $\varphi : V_1 \longrightarrow V_2$ eine lineare Abbildung. Es ist eine Abbildung φ^* gesucht, sodass für alle $v \in V_1$ und $f \in V_2^*$ das Diagramm kommutiert.



Um dies zu erreichen, scheint die Definition $\varphi^*(f) = f \circ \varphi$ genau passend. Damit gilt für alle $v \in V_1$ und $f \in V_2^*$

$$\langle f, \varphi(v)\rangle = f(\varphi(v)) = (f \circ \varphi)(v) = (\varphi^*(f))(v) = \langle \varphi^*(f), v\rangle.$$

Darüber hinaus gilt für alle $f_1, f_2 \in V_2^*, \lambda \in K$:

$$\begin{aligned}\varphi^*(\lambda f_1 + f_2) &= (\lambda f_1 + f_2) \circ \varphi \\ &= \lambda \cdot (f_1 \circ \varphi) + (f_2 \circ \varphi) \\ &= \lambda \cdot \varphi^*(f_1) + \varphi^*(f_2)\end{aligned}$$

□

Beispiel 2.6.41

Es sei $v \in V$. Dann wird v durch ι abgebildet auf die Abbildung

$$\iota(v) : V^* \to K : \ f \mapsto \langle f, v\rangle.$$

Man kann ι also auch schreiben als eine Abbildung von V nach $\mathrm{Hom}(V^*, K)$.

Man nennt $\mathrm{Hom}(V^*, K)$ den Bidualraum und bezeichnet diesen als $(V^*)^*$.

2.7 Dimensionstheorie

In diesem und dem folgenden Kapitel beschäftigen wir uns mit der Reduzierung von Komplexität. Es gilt dabei einen Weg zu finden, Vektorräume und lineare Abbildungen durch wenige Elemente beschreiben zu können. Der Begriff der Dimension wird sich auf natürliche Weise mit entwickeln, in der Art, dass sich dieser als die Anzahl der Elemente ergeben wird, die wir benötigen, um einen Vektorraum eindeutig zu beschreiben. Wir beginnen damit, das Konzept einer Basis zu entwickeln.

2.7.1 Linearkombinationen

Definition 2.7.1

Es sei V ein K-Vektorraum und $v_1, \ldots, v_n \in V$. Ein Vektor der Form

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n, \quad \lambda_i \in K$$

heißt **Linearkombination** von $v_1, \ldots, v_n$.

Beispiel 2.7.2

1. Es seien

$$v_1 = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}, \; v_2 = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \; v_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{R}^3.$$

   Wählt man $\lambda_1 = 1$,$\lambda_2 = 0$ und $\lambda_3 = -2$, dann ist

$$v = \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3 = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} - 2 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -3 \\ 0 \\ -2 \end{pmatrix}$$

   eine Linearkombination aus v_1, v_2 und v_3.

2. Es sei $V = \mathbb{Q}[x]$. Dann ist das Polynom

$$p = 5x^4 - 3x^2 + x - 2 \cdot (1) \in \mathbb{Q}[x]$$

   eine Linearkombination von x^4, x^2, x und 1. Man nennt die einzelnen Summanden auch Monome.

Definition 2.7.3

Sei $V = K^n$. Dann sei der Vektor e_i definiert als für alle $1 \leq j \leq n$:

$$(e_i)_j = \delta_{i,j}.$$

Wir nennen e_i den i-ten Einheitsvektor.

Beispiel 2.7.4

1. Es sei

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \\ -1 \end{pmatrix} \in \mathbb{C}^3.$$

Man kann diesen als eine Linearkombination darstellen:

$$\begin{aligned} v &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= e_1 + 2 \cdot e_2 + 3 \cdot e_3 - 1 \cdot e_4 \end{aligned}$$

2. Es sei $V = \mathbb{R}^3$. Man betrachtet $e_1, e_2, e_3 \in \mathbb{R}^3$. Man untersucht, ob e_3 als Linearkombination von e_2 und e_1 dargestellt werden kann. Gibt es also $a_1, a_2 \in \mathbb{R}$, sodass

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = a_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + a_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

möglich ist? Man übersetzt dies in ein LGS mit der erweiterten Koeffizientenmatrix

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right).$$

Aus der letzten Zeile ließt man ab, dass es keine Lösung geben kann.

Bemerkung 2.7.5

Linearkombinationen sind immer ENDLICHE Summen.

Proposition 2.7.6

Für jedes $S \subseteq V$ existiert ein kleinster Unterraum W von V mit der Eigenschaft $S \subseteq W$. Wenn $S = \emptyset$, so ist dieser Unterraum $\{0\}$.

Beweis. Seien V ein K-Vektorraum und $S \subset V$ beliebig, aber fest. Man definiert

$$\mathcal{U} := \{U \subset V \mid S \subset U \wedge U \text{ Unterraum von } V\}.$$

Also ist $\mathcal{U}$ die Menge aller Unterräume von V, die S enthalten. $\mathcal{U}$ kann nicht leer sein, da V selbst ein Unterraum von V ist.

Das gesuchte W wird nun als

$$W := \bigcap_{U \in \mathcal{U}} U$$

festgelegt. Seit dem letzten Kapitel ist bekannt, dass W selbst wieder ein Unterraum sein muss. Außerdem ist klar, dass $S \subset W$ wegen für alle $U \in \mathcal{U} : S \subset U$.

Es bleibt zu zeigen, dass W die Minimalitätsbedingung erfüllt: Angenommen, es gäbe einen Unterraum $W' \subset V$ mit $S \subset W'$. Dann müsste $W' \in \mathcal{U}$ und somit

$$W' \supset \bigcap_{U \in \mathcal{U}} U = W$$

gelten. Also ist W der kleinste Unterraum mit $S \subset W$. □

Definition 2.7.7

Der kleinste Unterraum von V, der S enthält, heißt **lineare Hülle** von S. Wir bezeichnen ihn mit $\langle S \rangle$.

Proposition 2.7.8

Es sei $S \neq \emptyset$. Die lineare Hülle von S ist gleich der Menge der Linearkombinationen, die man aus endlich vielen Elementen aus S bilden kann (wir sprechen daher auch vom **Spann** von S).

Beweis (Proposition 2.7.8): Seien V ein K-Vektorraum und $\emptyset \neq S \subset V$ beliebig, aber fest. Alle Linearkombinationen, die aus S gebildet werden können, müssen in $\langle S \rangle$ enthalten sein, da $\langle S \rangle$ ein Unterraum ist. Man definiert

$$M := \{v \in V \mid v \text{ ist Linearkombination aus } S\}.$$

Nach Obigem ist $M \subset \langle S \rangle$. Man versucht nun, $\langle S \rangle \subset M$ nachzuweisen, indem man zeigt, dass M ein Unterraum von V ist. Da $\langle S \rangle$ der *kleinste* Unterraum ist, der S enthält, gilt in diesem Fall nämlich, dass $\langle S \rangle \subset M$.

U1: Seien $v, w \in M$. Dann sind beide Vektoren endliche Summen von Vektoren aus S. Die Summe von v und w muss immer noch endlich sein, also $v + w \in M$.

U2: Seien $v \in M$ und $\lambda \in K$ beliebig, aber fest. Dann gibt es eine Indexmenge $I \subset \mathbb{N}$, sodass man v als

$$v = \sum_{i \in I} a_i \cdot s_i$$

darstellen kann, wobei die $a_i \in K$ und die $s_i \in S$. Nun gilt

$$\lambda \cdot v = \lambda \cdot \left(\sum_{i \in I} a_i \cdot v_i \right) \overset{V \text{ VR.}}{=} \sum_{i \in I} \lambda \cdot (a_i \cdot v_i) \overset{V \text{ VR.}}{=} \sum_{i \in I} (\lambda \cdot a_i) \cdot v_i \in M.$$

U3: Da $S \neq \emptyset$, gibt es mindestens ein Element $s \in S$. Aufgrund der Vektorraumeigenschaften von V gilt

$$0 = 0 \cdot s \in M.$$

Also ist M ein Unterraum von V und damit gilt insgesamt $M = \langle S \rangle$. □

Der Begriff des Spanns von S rührt von der Vorstellung, dass die Linearkombinationen in S die lineare Hülle aufspannen, sofern man sich Vektoren als Pfeile im Raum vorstellt.

Proposition 2.7.9

Es seien V, W zwei K-Vektorräume und $\varphi : V \longrightarrow W, \psi : V \longrightarrow W$ zwei lineare Abbildungen. Angenommen,

$$\varphi(v) = \psi(v) \text{ für alle } v \in S \subseteq V,$$

dann ist auch

$$\varphi(v) = \psi(v) \text{ für alle } v \in \langle S \rangle.$$

Die Aussage aus Proposition 2.7.9 ist eine sehr wichtige Aussage, da sie es uns ermöglicht, das Verhalten einer gesamten Abbildung mittels Betrachtung einiger weniger Elemente zu studieren.

Beweis. Es seien V, W zwei K-Vektorräume und $\varphi : V \longrightarrow W, \psi : V \longrightarrow W$ zwei lineare Abbildungen mit der Eigenschaft, dass

$$\varphi(v) = \psi(v) \text{ für alle } v \in S \subseteq V$$

gilt. Sei nun $v \in \langle S \rangle$ beliebig, aber fest und

$$v = \sum_{i \in I} a_i s_i$$

eine Darstellung wie im Beweis zu Proposition 2.7.8. Dann gilt

$$\begin{aligned} \varphi(v) = \varphi\left(\sum_{i \in I} a_i s_i\right) &\overset{\varphi \text{ lin.}}{=} \sum_{i \in I} a_i \varphi(s_i) \overset{\text{Vorraussetzung}}{=} \sum_{i \in I} a_i \psi(s_i) \\ &\overset{\psi \text{ lin.}}{=} \psi\left(\sum_{i \in I} a_i s_i\right) = \psi(v), \end{aligned}$$

womit die Aussage gezeigt ist. □

Es wurde bereits angesprochen, dass ein Ziel dieses Kapitels die Beschreibung von Vektorräumen durch wenige Elemente ist, sodass sich der Rest als Linearkombinationen ergibt. Eine zentrale Frage dabei besteht darin, wie viele Elemente man weglassen kann und welche sich eben nicht durch die Linearkombination anderer ergeben. Diese Frage führt zu dem Begriff der linearen Unabhängigkeit.

Definition 2.7.10

Die Vektoren $v_1, \ldots, v_n \in V$ heißen **linear abhängig**, wenn es $\lambda_1, \ldots, \lambda_n \in K$ gibt, die nicht alle 0 sind, und für die gilt

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0.$$

Die Vektoren heißen **linear unabhängig**, wenn aus

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0, \quad \lambda_i \in K$$

immer folgt $\lambda_1 = \ldots = \lambda_n = 0$.
Allgemein definiert man eine Familie $(v_i)_{i \in I}$ mit $v_i \in V$ als

- linear abhängig, wenn es eine endliche Teilfamilie gibt, die linear abhängig ist.
- linear unabhängig, wenn jede endliche Teilfamilie linear unabhängig ist.

Beispiel 2.7.11

1. Seien
$$v_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix},\ v_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix} \in \mathbb{R}^2$$
Die beiden Vektoren sind linear abhängig, da
$$-2 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} + \begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

2. Man möchte jedoch ein zuverlässigeres Verfahren nutzen als im obigen Beispiel. Seien dafür v_1, v_2 wie oben. Man betrachtet also das Problem, $\lambda_1, \lambda_2 \in K$ zu finden, sodass
$$\lambda_1 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
gilt, bzw. zu bestimmen, ob es überhaupt solche λ_1, λ_2 gibt. Glücklicherweise kann man das Problem als das LGS
$$\begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
auffassen. Man erhält die Koeffizientenmatrix
$$\left(\begin{array}{cc|c} 2 & 4 & 0 \\ 1 & 2 & 0 \end{array}\right)$$
und Umformung ergibt
$$\left(\begin{array}{cc|c} 2 & 4 & 0 \\ 0 & 0 & 0 \end{array}\right).$$
Durch die Nullzeile erhält man eine freie Variable, sodass der Lösungsraum mehr als die 0 enthalten muss, womit v_1, v_2 linear-abhängig sind.

3. Es seien
$$v_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix},\ v_2 = \begin{pmatrix} 4 \\ 1 \end{pmatrix} \in \mathbb{R}^2.$$
Man betrachtet analog zu oben das Problem der Abhängigkeit als ein LGS:
$$\left(\begin{array}{cc|c} 2 & 4 & 0 \\ 1 & 1 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 2 & 4 & 0 \\ 0 & -1 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 2 & 0 \\ 0 & 1 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right)$$
Der Lösungsraum beinhaltet also nur die Null. Damit müssen die beiden Vektoren linear unabhängig sein.

4. Man betrachtet die kanonischen Vektoren $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$. Seien $\lambda_1, \ldots, \lambda_n \in K$ mit

$$\sum_{i=1}^{n} \lambda_i e_i = 0.$$

Per Definition der e_i gilt dann

$$I_n \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (I_n = \mathbb{E}_n).$$

Also sind die e_i linear unabhängig.

5. Seien $V = \mathbb{C}[x]$ und $x^{i_1}, \ldots, x^{i_s} \in \mathbb{C}[x]$ mit $i_l \neq i_k$ für $l \neq k$. Seien $a_{i_1}, \ldots, a_{i_s} \in K$ mit

$$0 = \sum_{k=1}^{s} a_{i_k} x^{i_k},$$

wobei mit 0 das Nullpolynom gemeint ist. Es gilt

$$\begin{aligned} -\infty = \operatorname{grad} 0 &= \operatorname{grad} \sum_{k=1}^{s} a_{i_k} x^{i_k} \\ &= \begin{cases} -\infty, & \text{für alle } 1 \leq k \leq s : a_{i_k} = 0 \\ \max\{i_1, \ldots, i_s\}, & \text{sonst} \end{cases} \end{aligned}$$

Da $i_1, \ldots, i_s \in \mathbb{N}_0$, muss $a_{i_1} = \ldots = a_{i_s} = 0$ gelten. Damit haben wir gezeigt, dass Monome unterschiedlicher Potenzen linear unabhängig sind.

Bemerkung 2.7.12

Es seien $v_1, \ldots, v_m \in \mathbb{K}^n$ gegeben. Wie kann man beantworten, ob diese linear unabhängig in $\mathbb{K}^n$ sind? Dafür muss man zeigen, dass es genau eine Lösung

$$x = \begin{pmatrix} x_1 \\ \ldots \\ x_m \end{pmatrix}$$

für das Gleichungssystem

$$0_{\mathbb{K}^n} = x_1 v_1 + \ldots + x_m v_m$$

gibt. Das können wir umformulieren und dafür sei $A \in \mathbb{K}^{n \times m}$. Die i.Spalte von A sei v_i, dann liest sich obige Gleichung

$$A \cdot x = 0$$

Das homogene Gleichungssystem soll also eine eindeutige Lösung haben

$$\mathcal{L}(A \mid 0) = \{0\}.$$

Dazu bringen wir A in Zeilenstufenform A', dann können wir ablesen: $(v_1 \dots, v_n)$ ist genau dann linear unabhängig wenn alle Stufen in A' die Länge 1 haben (also keine freien Variablen existieren).

Proposition 2.7.13

Es seien $v_1, \dots, v_n \in V$, mit $n \geq 2$. Dann sind folgende Aussagen äquivalent:

1. $v_1, \dots, v_n$ sind linear abhängig.
2. Es existiert $1 \leq i \leq n$, so dass v_i eine Linearkombination der restlichen Vektoren ist.

Beweis. Es seien V ein K-Vektorraum und $v_1, \dots, v_n \in V$, mit $n \geq 2$.

(1) $\Rightarrow$ (2) Die Vektoren $\{v_1, \dots, v_n\}$ sind linear abhängig. Das bedeutet, es gibt $\lambda_1, \dots, \lambda_n \in K$, sodass es ein $1 \leq j \leq n$ gibt mit $\lambda_j \neq 0$ und

$$\sum_{i=1}^{n} \lambda_i v_i = 0.$$

Ohne Beschränkung der Allgemeinheit ist $j = 1$. Dann gilt

$$-\lambda_1 v_1 = \sum_{i=2}^{n} \lambda_i v_i$$

und wegen $\lambda_1 \neq 0$

$$v_1 = -\sum_{i=2}^{n} \lambda_1^{-1} \lambda_i v_i,$$

womit man v_1 als Linearkombination der anderen Vektoren dargestellt hat.

(2) $\Rightarrow$ (1) Es gibt ein $1 \leq i \leq n$, sodass es $\lambda_1, \dots, \lambda_{i-1}, \lambda_{i+1}, \dots, \lambda_n \in K$ gibt mit

$$v_i = \sum_{j=1}^{i-1} \lambda_j v_j + \sum_{j=i+1}^{n} \lambda_j v_j.$$

Setzt man $\lambda_i = -1$, dann erhält man

$$0 = \sum_{j=1}^{n} \lambda_j v_j.$$

Also sind $\{v_1, \dots, v_n\}$ linear abhängig.

□

Definition 2.7.14

Es sei $U \subseteq V$ ein Unterraum eines K-Vektorraums V. Eine Familie $(v_i)_{i \in I}$ heißt **Erzeugendensystem** von U genau dann, wenn ihre lineare Hülle gleich U ist. Einen Unterraum, dessen Erzeugendensystem endlich ist, nennen wir **endlich erzeugt**.

Beispiel 2.7.15

1. Es sei $V = \mathbb{R}[x]$. Per Definition ist $\left(x^i\right)_{i \geq 0}$ ein Erzeugendensystem von V, denn für alle $p \in \mathbb{R}[x]$ gibt es a_i, sodass

$$p = \sum_{i=0}^{\deg(p)} a_i x^i.$$

2. Es sei $A \in \mathbb{R}^{m \times n}$. Man sucht ein Erzeugendensystem von $\mathrm{Im}(A)$.

$$\begin{aligned}
\mathrm{Im}(A) &= \{y \in \mathbb{R}^m \mid \exists\, x \in \mathbb{R}^n : Ax = y\} \\
&= \left\{ y \in \mathbb{R}^m \;\middle|\; \exists \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n : A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = y \right\} \\
&= \left\{ y \in \mathbb{R}^m \;\middle|\; \exists \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n : x_1 \cdot \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \end{pmatrix} + \cdots + x_n \cdot \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{n,n} \end{pmatrix} = y \right\}
\end{aligned}$$

   Das Bild von A ist also der Spann der Spalten von A.

3. Es seien $v_1, \ldots, v_4 \in \mathbb{R}^3$. Diese sind ein Erzeugendensystem ihres Spanns.

4. Sei

$$A = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

   Das Bild von A ist dann

$$\mathrm{Im}(A) = \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle.$$

   Die Bearbeitung der Matrix A durch den Gauß-Algorithmus liefert

$$A' = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

   wobei

$$\mathrm{Im}(A') = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle.$$

   Die beiden Bilder sind offensichtlich unterschiedlich. Man merke sich also, dass der Gaußalgorithmus das Bild einer Matrix verändert, aber nicht ihren Kern.

Bemerkung 2.7.16

Es seien $v_1, \ldots, v_m \in \mathbb{K}^n$ gegeben. Wie kann man beantworten, ob diese ein Erzeugendensystem für $\mathbb{K}^n$ sind? Dafür muss man zeigen, dass für jedes $w \in \mathbb{K}^n$ existieren $x_1, \ldots, x_m$ mit

$$w = x_1 v_1 + \ldots + x_m v_m.$$

Das können wir umformulieren und dafür sei $A \in \mathbb{K}^{n \times m}$. Die i.Spalte von A sei v_i, dann liest sich obige Gleichung

$$A \cdot x = w$$

wobei

$$x = \begin{pmatrix} x_1 \\ \ldots \\ x_m \end{pmatrix}.$$

Wir suchen also für jedes $w \in \mathbb{K}^n$ eine Lösung für das LGS. Dazu bringen wir A in Zeilenstufenform A'. Jetzt können wir ablesen:
$\{v_1 \ldots, v_n\}$ ist genau dann ein Erzeugendensystem von $\mathbb{K}^n$ falls A' keine Nullzeile enthält.

2.7.2 Basis eines Vektorraums

Wir bringen nun den Begriff des Erzeugendensystems und der linearen Unabhängigkeit im Begriff der Basis zusammen.

Definition 2.7.17

Es sei V ein K-Vektorraum. Eine **Basis** von V ist ein linear unabhängiges Erzeugendensystem $(b_i)_{i \in I}$ von V. (Konvention: Die leere Familie ist die Basis des Nullraums).

Beispiel 2.7.18

Sei K ein Körper. Dann handelt es sich bei $(e_1, \ldots, e_n)$ um eine Basis vom K^n. Es wurde bereits gezeigt, dass diese linear unabhängig sind. Sei also $a \in K$ ein beliebiger Vektor und für alle $1 \leq i \leq n : a_i$ die Komponenten. Dann gilt

$$a = \sum_{i=1}^{n} a_i \cdot e_i$$

und somit ist $(e_1, \ldots, e_n)$ ein Erzeugendensystem vom K^n.

Satz 2.7.19

Für eine Familie $(b_i)_{i \in I}$ von Vektoren $b_i \in V$ sind folgende Aussagen äquivalent:

1. $(b_i)_{i \in I}$ ist eine Basis von V.

2. $(b_i)_{i\in I}$ ist eine maximale linear unabhängige Familie. d.h.

$$\forall\, v \in V \setminus \{b_i \mid i \in I\} : \{v\} \cup \{b_i \mid i \in I\} \text{ ist linear abhängig .}$$

3. $(b_i)_{i\in I}$ ist linear unabhängig und $\exists$ Erzeugendensystem $(w_j)_{j\in J}$ von V so, dass

$$\forall\, j \in J \text{ mit } w_j \neq b_i \forall\, i \in I : \{w_j\} \cup \{b_i \mid i \in I\}$$

ist linear abhängig.

4. $(b_i)_{i\in I}$ ist ein minimales Erzeugendensystem, d.h.

$$\forall\, k \in I : (b_i)_{i\in I\setminus\{k\}} \text{ ist kein Erzeugendensystem.}$$

Beweis. Sei V ein K-Vektorraum und $(b_i)_{i\in I}$ eine Familie von Vektoren.

(1) $\Rightarrow$ (2) B ist eine Basis von V. Sei also $v \in V \setminus B$ beliebig, aber fest. Da B eine Basis ist, gibt es $a_i \in K$, sodass

$$v = \sum_{i\in I} a_i b_i \Rightarrow v - \sum_{i\in I} a_i b_i = 0,$$

womit $\{v\} \cup \{B\}$ linear abhängig ist.

(2) $\Rightarrow$ (3) V ist ein Erzeugendensystem von V. Wählt man nun ein beliebiges Element $v \in V$, sodass für alle $i \in I : v \neq b_i$, dann ist $v \in V \setminus B$ und nach (2) ist $\{v\} \cup \{b_i \mid i \in I\}$ linear abhängig. Damit ist (3) gezeigt.

(3) $\Rightarrow$ (4) Man beginnt mit der Eigenschaft des Erzeugendensystems. Aus (3) folgt, dass es ein Erzeugendensystem $(w_j)_{j\in J}$ gibt, sodass für alle $j \in J$ mit für alle $i \in I$: $w_j \neq b_i$ die Menge $\{w_j\} \cup \{b_i \mid i \in I\}$ linear abhängig ist. In diesem Fall gilt $w_j \in \langle (b_i)_{i\in I} \rangle$. Im Fall, dass es ein $i \in I$ gibt, sodass $w_j = b_i$, gilt $w_j \in (b_i)_{i\in I} \subset \langle (b_i)_{i\in I} \rangle$. Insgesamt gilt also

$$(w_j)_{j\in J} \subset \langle (b_i)_{i\in I} \rangle,$$

womit $(b_i)_{i\in I}$ ein Erzeugendensystem erzeugt, was $(b_i)_{i\in I}$ selbst zu einem Erzeugendensystem macht.

Angenommen, es gibt ein $i \in I$, sodass es $a_i \in K$ gibt, sodass

$$b_i = \sum_{\substack{j\in I \\ j\neq i}} a_j b_j.$$

Dann wäre $(b_i)_{i\in I}$ nicht mehr linear unabhängig. Da aber nach (3) $(b_i)_{i\in I}$ linear unabhängig ist, kann der obige Fall nicht eintreten, was $(b_i)_{i\in I}$ zu einem minimalen Erzeugendensystem macht.

(4) $\Rightarrow$ (1) Nach Voraussetzung ist $(b_i)_{i\in I}$ ein Erzeugendensystem. Man weist nun die lineare Unabhängigkeit nach: Nach Proposition 2.7.13 ist lineare Unabhängigkeit dazu äquivalent, dass man keinen Vektor als Linearkombination der Anderen darstellen kann. Da $(b_i)_{i\in I}$ ein *minimales* Erzeugendensystem ist, ist die letztere Aussage gegeben. Damit ist $(b_i)_{i\in I}$ eine Basis von V.

□

Satz 2.7.20

Seien $v_1, \ldots, v_n$ linear unabhängige Vektoren aus V und $w_1, \ldots, w_m$ ein Erzeugendensystem von V. Dann gibt es $1 \leq j_1 < \ldots < j_r \leq m$ so, dass

$$v_1, \ldots, v_n, w_{j_1}, \ldots, w_{j_r}$$

eine Basis von V ist.

Beweis. Seien $v_1, \ldots, v_n$ linear unabhängige Vektoren aus V und $w_1, \ldots, w_m$ ein Erzeugendensystem von V. Man betrachtet die Potenzmenge

$$\mathcal{P} \subset \mathcal{P}(\{w_1, \ldots, w_m\})$$

und nimmt davon die Teilmenge

$$M := \{U \in \mathcal{P} \mid \{v_1, \ldots, v_n\} \cup U \text{ linear unabhängig}\}.$$

Es gelten $\emptyset \in \mathcal{P}$ und $\{v_1, \ldots, v_n\} \cup \emptyset$ linear unabhängig, womit $\emptyset \in M$. Das bedeutet, dass die Menge M nicht leer ist. Man beginnt nun eine (partielle) Anordnung auf $\mathcal{P}$ zu definieren: für alle $U_1, U_2 \in \mathcal{P}$:

$$U_1 \leq U_2 :\Leftrightarrow U_1 \subseteq U_2$$

Da $\mathcal{P}$ endlich ist, ist M endlich, damit muss M aber Maxima besitzen. Für so ein Maximum $U \in M$ gilt, dass $\{v_1, \ldots, v_n\} \cup U$ linear unabhängig ist. Aufgrund der Maximalität von U gilt, dass für jedes weitere $w_i \notin U$ die Familie $\{v_1, \ldots, v_n\} \cup U \cup \{w_i\}$ linear abhängig wird. Damit erfüllt $\{v_1, \ldots, v_n\} \cup U$ die dritte Aussage aus Theorem 2.7.19 und ist somit eine Basis. □

Korollar 2.7.21

Wenn V ein Erzeugendensystem $w_1, \ldots, w_m$ hat, dann bildet ein geeigneter Teil $w_{j_1}, \ldots, w_{j_r}$ eine Basis von V.

Beweis (Korollar 2.7.21): Sei $w_1, \ldots, w_m$ ein Erzeugendensystem von V. Setzt man in Theorem 2.7.20 die Familie linear unabhängiger Vektoren zu $\{v_1, \ldots, v_n\} = \emptyset$, dann erhält man die Aussage. □

Satz 2.7.22

Sei $(v_i)_{i \in I}$ eine linear unabhängige Familie aus V und sei $(w_j)_{j \in J}$ ein Erzeugendensystem von V. Dann $\exists\, S \subseteq J$ so, dass $(v_i)_{i \in I}, (w_j)_{j \in S}$ eine Basis von V ist.

Der Beweis erfordert Zorn's Lemma, liegt damit außerhalb unserer derzeitigen Möglichkeiten und wird hier ausgelassen. Trotzdem liefert der Satz uns eine sehr nützliche Aussage, die wir nutzen wollen:

Korollar 2.7.23

Jeder Vektorraum hat eine Basis.

Beweis (Korollar 2.7.23): Sei V ein K-Vektorraum. V ist ein Erzeugendensystem von sich selbst und besitzt somit nach Theorem 2.7.22 eine Teilmenge $B \subset V$, sodass $B = \emptyset \cup B$ eine Basis ist. □

Korollar 2.7.24

Sei U ein Unterraum von V. Dann gibt es einen Unterraum W von V so, dass $V = U \oplus W$. Wir nennen W ein **Komplement** von U in V.

Beweis (Korollar 2.7.24): Sei U ein Unterraum von V. Dann gibt es eine Basis $B = \{v_i \mid i \in I\}$ von U. B ist insbesondere linear unabhängig, womit dieses nach Theorem 2.7.22 durch Elemente $\{w_j \mid j \in J\}$ aus V zu einer Basis von V erweitert werden kann. Man definiert

$$W := \langle w_j \mid j \in J \rangle.$$

Folglich gilt

$$V = \langle v_i, w_j \mid i \in I, j \in J \rangle = U + W.$$

Angenommen, es würde $a_i \in K$ und $b_j \in K$ geben, sodass

$$\sum_{i \in I} a_i v_i = \sum_{j \in J} b_j w_j,$$

dann

$$\sum_{i \in I} a_i v_i - \sum_{j \in J} b_j w_j = 0.$$

Da $(v_i, w_j \mid i \in I, j \in J)$ eine Basis von V ist und damit linear unabhängig, müssen alle $a_i = 0$ und alle $b_j = 0$. Das bedeutet, dass $U \cap W = \{0\}$, womit $V = U \oplus W$. □

Beispiel 2.7.25

Es sei $V = \mathbb{R}^2$, dann sind folgende Mengen Unterräume:

1. $\{(0,0)\}$
2. $\mathbb{R}^2$
3. $\left\{ \lambda \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \middle| \lambda \in \mathbb{R}^2 \right\}$ (x-Achse)
4. $\left\{ \lambda \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \middle| \lambda \in \mathbb{R}^2 \right\}$ (y-Achse)

Erstens ist das Komplement zu Zweitens und Drittens zu Viertens. Weitere Komplemente zu 3. sind alle Geraden durch den Ursprung, die nicht die x-Achse sind. Eine analoge Aussage gilt für die y-Achse.

Korollar 2.7.26

Sei $U \subseteq V$ ein Unterraum und $f \in U^*$. Dann existiert $g \in V^*$ mit $g_{|U} = f$.

Beweis (Korollar 2.7.26): Sei $U \subseteq V$ ein Unterraum und $f \in U^*$. Sei W ein Komplement von U in V. D.h. $V = U \oplus W$. Man definiert

$$\pi_U : V \to U : v = u + w \mapsto u.$$

Die Abbildung π_U ist wohldefiniert, da die Summe $v = u + w$ eindeutig ist wegen $V = U \oplus W$. Seien $v, v' \in V$ und $\lambda \in K$ beliebig:

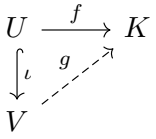
$$\begin{aligned}\pi_U(\lambda v + v') &= \pi_U(\lambda u + \lambda w + u' + w') = \pi_U(\underbrace{\lambda u + u'}_{\in U} + \underbrace{\lambda w + w'}_{\in W}) \\ &= \lambda u + u' = \lambda \pi_U(v) + \pi_U(v')\end{aligned}$$

Also ist π_U linear, was auch $g := f \circ \pi_U$ linear macht. Damit ist $g \in V^*$. Es gilt für alle $u \in U$:

$$g_{|U}(u) = f(\pi_U(u)) = f(u),$$

womit $g_{|U} = f$. □

Um sich die Bedeutung von Korollar 2.7.26 zu veranschaulichen, kann man wieder ein kommutatives Diagramm malen. Für einen Unterraum $U \subseteq V$ und eine Linearform $f \in U^*$ wird also ein $g \in V^*$ gesucht, sodass das Diagramm



kommutiert, wobei $\iota : U \to V : u \mapsto u$ die kanonische Injektion ist (**Lift einer Linearform**).

Korollar 2.7.27

Die kanonische Abbildung $\varphi : V \longrightarrow (V^*)^*$, $v \mapsto \langle \_, v \rangle$ ist eine injektive lineare Abbildung.

Beweis (Korollar 2.7.27): Sei V ein K-Vektorraum. Die Linearität von φ ist bereits bekannt. Man betrachtet also

$$\mathrm{Ker}(\varphi) = \{v \in V \mid \text{ für alle } f \in V^* : \langle f, v \rangle = f(v) = 0\}.$$

Sei $0 \neq v \in V$ beliebig, aber fest. Man definiert $U := \langle v \rangle = K \cdot v$ und

$$f : U \to K : \lambda v \to \lambda.$$

Es gilt für alle $x = \alpha v, y = \beta v \in U :$ für alle $\mu \in K$:

$$f(\mu x + y) = f(\mu\alpha v + \beta v) = f((\mu\alpha + \beta)v) = \mu\alpha + \beta = \mu f(x) + f(y),$$

also $f \in U^*$. Nach Korollar 2.7.26 gibt es $g \in V^*$, sodass $g_{|U} = f$. Damit gilt nun

$$g(v) = f(v) = 1 \neq 0,$$

womit $v \notin \mathrm{Ker}(\varphi)$. Da v beliebig war, ist $\mathrm{Ker}(\varphi) = \{0\}$ und somit φ injektiv. □

Satz 2.7.28

Für Vektoren $b_1, \ldots, b_n \in V$ sind folgende Aussagen äquivalent:

1. $b_1, \ldots, b_n$ ist eine Basis von V.
2. $\forall\, v \in V$ gilt: $\exists!\, \lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 b_1 + \ldots + \lambda_n b_n$.

Beweis. Seien V K-Vektorraum und $b_1, \ldots, b_n \in V$ Vektoren.

(1) ⇒ (2) Sei $v \in V$ beliebig, aber fest. Die Vektoren $b_1, \ldots, b_n$ bilden eine Basis. Da Basen Erzeugendensysteme sind, gibt es $\lambda_1, \ldots, \lambda_n \in K$, sodass

$$v = \sum_{i=1}^{n} \lambda_i b_i.$$

Angenommen, es gibt $\lambda_1', \ldots, \lambda_n' \in K$, sodass

$$v = \sum_{i=1}^{n} \lambda_i' b_i.$$

Dann gilt

$$0 = \sum_{i=1}^{n} \lambda_i b_i - \sum_{i=1}^{n} \lambda_i' b_i = \sum_{i=1}^{n} (\lambda_i - \lambda_i') b_i.$$

Da die b_i linear unabhängig sind, gilt für alle $1 \leq i \leq n$:

$$\lambda_i - \lambda_i' = 0 \Rightarrow \lambda_i = \lambda_i'.$$

Da v beliebig war, wird also jeder Vektor aus V eindeutig durch die Basis dargestellt.

(2) ⇒ (1) Die $b_1, \ldots, b_n$ sind ein Erzeugendensystem, weil es für alle $v \in V$ $\lambda_1, \ldots, \lambda_n \in K$ gibt, sodass

$$v = \sum_{i=1}^{n} \lambda_i b_i.$$

Für den Fall $v = 0$ gibt es nach Voraussetzung genau eine Möglichkeit $\lambda_1, \ldots, \lambda_n \in K$ zu wählen, sodass

$$0 = \sum_{i=1}^{n} \lambda_i b_i.$$

Da dies bereits für $\lambda_1 = \cdots = \lambda_n = 0$ der Fall ist, sind die $b_1, \ldots, b_n$ linear unabhängig.

□

Definition 2.7.29

Für die Basis $B = (b_1, \ldots, b_n)$ aus dem vorherigen Satz nennen wir die Zahlen $\lambda_1, \ldots, \lambda_n$ die **Koordinaten** von v bzgl. B. Weiter heißt $v_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in K^n$ der **Koordinatenvektor** von v bzgl. B. Der Koordinatenvektor hängt also nicht nur von v ab, sondern auch von der Wahl der Basis B und sogar der Reihenfolge der Basiselemente.

Beispiel 2.7.30

1. Sei $V = \mathbb{R}^3$. Dann sind e_1, e_2, e_3 eine Basis von $\mathbb{R}^3$.

$$v = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

   Der Koordinatenvektor ist also

$$v_B = \begin{pmatrix} 3 \\ 2 \\ 1. \end{pmatrix}$$

2. Nicht alle Koordinatenvektoren sind identisch zum Ausgangsvektor: Die Vektoren

$$b_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \; b_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

   bilden eine Basis des $\mathbb{R}^2$. Man erhält damit

$$\begin{aligned} v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} &\rightsquigarrow (v_1)_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ v_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 0 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} &\rightsquigarrow (v_2)_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ v_3 = \begin{pmatrix} 3 \\ 5 \end{pmatrix} = 4 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} &\rightsquigarrow (v_3)_B = \begin{pmatrix} 4 \\ -1 \end{pmatrix} \end{aligned}$$

   .

3. Man betrachtet P_2 für $K = \mathbb{R}$ und die Basis $(x^i)_{0 \leq i \leq 2}$. Dann hat das Polynom $p = 5x^2 - 7x + 4$ den Koordinatenvektor

$$p_{(x^i)_{0 \leq i \leq 2}} = \begin{pmatrix} 4 \\ -7 \\ 5 \end{pmatrix}.$$

Proposition 2.7.31

Es sei $B = (b_1, \ldots, b_n)$ eine Basis von V. Dann ist die Abbildung

$$\kappa_B : K^n \longrightarrow V \text{ mit } \quad (\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1 b_1 + \ldots + \lambda_n b_n$$

ein Isomorphismus, dessen Umkehrabbildung jedem $v \in V$ seinen Koordinatenvektor bzgl. B zuordnet.

Beweis. Es sei $B = (b_1, \ldots, b_n)$ eine Basis von einem K-Vektorraum V. Es sei den geneigten Lesenden überlassen, die Linearität von κ_B nachzurechnen.

Es ist

$$\operatorname{Ker} \kappa_B = \left\{ (\lambda_i)_i \middle| 0 = \sum_{i=1}^{n} \lambda_i b_i \right\} \overset{b_1,\ldots,b_n \text{ lin. unabhängig}}{=} \{(0, \ldots, 0)\},$$

womit κ_B injektiv ist.

Da B eine Basis ist, ist B ein Erzeugendensystem. Damit für alle $v \in V : \exists\, \lambda_1, \ldots, \lambda_n$:

$$v = \sum_{i=1}^{n} \lambda_i b_i = \kappa_B(\lambda_1, \ldots, \lambda_n)$$

Also ist κ_B auch surjektiv und damit bijektiv und insgesamt ein Isomorphismus. Wie oben bereits gezeigt wurde, ordnet κ_B^{-1} jedem Vektor seine Koordinaten bezüglich B zu. □

Bemerkung 2.7.32

Jeder endlich erzeugte Vektorraum ist also isomorph zu einem K^n.

Beispiel 2.7.33

1. Seien $b_1, \ldots, b_n \in \mathbb{R}^n$ eine Basis und $v \in \mathbb{R}^n$ ein beliebiger Vektor, dessen Koordinaten ermittelt werden sollen. Man kann das Problem als LGS ausdrücken:

$$\begin{pmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

2. Aus einem früheren Beispiel kennen wir

$$b_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ b_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

als eine Basis vom $\mathbb{R}^2$. Wir suchen nun den Koordinatenvektor zu

$$\begin{pmatrix} 3 \\ 5 \end{pmatrix}.$$

Es ergibt sich das LGS

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix},$$

was zu folgender Koeffizientenmatrix und Umformungskette führt:

$$\left(\begin{array}{cc|c} 1 & 1 & 3 \\ 1 & -1 & 5 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & -2 & 2 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & -1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & -1 \end{array}\right)$$

Am Ende erhalten wir den bereits bekannten Koordinatenvektor.

3. Die Vektoren

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} -2 \\ -1 \\ 1 \end{pmatrix},\ v_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

sind aus dem $\mathbb{R}^3$. Man kann obiges Verfahren nicht nur dafür nutzen, Koeffizientenvektoren zu einer Basis zu finden, sondern auch als einen Test, ob Vektoren $v_1, \ldots, v_3$ tatsächlich linear unabhängig sind. Dafür sucht man den Koeffizientenvektor des Null-Vektors. Gibt es mehr als eine Lösung, dann können die Vektoren nicht linear unabhängig sein.

$$\left(\begin{array}{ccc|c} | & | & | & 0 \\ v_1 & v_2 & v_3 & 0 \\ | & | & | & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right)$$
$$\rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Aus der letzten Zeile liest man ab, dass die Vektoren v_1, v_2, v_3 linear abhängig sind. Es zeigt sich hiermit, dass der Gauß-Algorithmus sehr nützlich ist, um lineare Unabhängigkeit nachzurechnen. Später werden wir sehen, dass dieser auch benutzt werden kann, um zu überprüfen, ob es sich bei einer Familie von Vektoren um ein Erzeugendensystem handelt.

Bemerkung 2.7.34

Wie bestimmt man, ob eine Menge von Vektoren

- linear unabhängig ist,
- ein Erzeugendensystem bildet,
- eine Basis ist?

Antwort: Gauß-Algorithmus!

Lemma 2.7.35

Sei $b_1, \ldots, b_n$ eine Basis von V und v eine Linearkombination

$$v = \lambda_1 b_1 + \ldots + \lambda_n b_n$$

mit $\lambda_1 \neq 0$. Dann ist auch $v, b_2, \ldots, b_n$ eine Basis von V.

Beweis. Man sieht sofort, dass

$$b_1 = \lambda_1^{-1} \cdot \left(v - \sum_{i=2}^{n} \lambda_i b_i \right),$$

also $b_1 \in \langle v, b_2, \ldots, b_n \rangle$, womit

$$V = \langle b_1, \ldots, b_n \rangle \subseteq \langle v, b_2, \ldots, b_n \rangle \subseteq V.$$

Das macht $\{v, b_2, \ldots, b_n\}$ zu einem Erzeugendensystem von V.

Falls

$$0 = \mu_1 v + \sum_{i=2}^{n} \mu_i b_i$$

für $\mu_1, \ldots, \mu_n \in K$ gilt, dann

$$0 = \mu_1 \sum_{i=1}^{n} \lambda_i b_i + \sum_{i=2}^{n} \mu_i b_i = \mu_1 \cdot \lambda_1 \cdot b_1 + \sum_{i=2}^{n} (\mu_1 \cdot \lambda_i + \mu_i) b_i.$$

Da die Vektoren $b_1, \ldots, b_n$ linear unabhängig sind, gelten

$$\begin{aligned} 0 &= \mu_1 \cdot \lambda_1 \\ 0 &= \mu_1 \cdot \lambda_i + \mu_i \quad \text{für alle } 2 \leq i \leq n. \end{aligned}$$

Wegen $\lambda_1 \neq 0$ muss $\mu_1 = 0$, womit für alle $2 \leq i \leq n : 0 = \mu_1 \cdot \lambda_i + \mu_i = \mu_i$. Insgesamt ist $\{v, b_2, \ldots, b_n\}$ also eine Basis von V. □

Beispiel 2.7.36

Man betrachtet im $\mathbb{R}^3$ die Vektoren

$$\underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}}_{\text{Basis } B}, \quad \underbrace{\begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}}_{=:v}$$

und folgert aus dem Austauschlemma, dass v mit jeweils zwei der anderen Vektoren eine Basis bildet.

Satz 2.7.37

Es sei $b_1, \ldots, b_n$ eine Basis und $(w_j)_{j \in J}$ ein Erzeugendensystem von V. Für $k \in \{0, \ldots, n\}$ gibt es eine k-elementige Teilmenge S von J so, dass $(w_j)_{j \in S}, b_{k+1}, \ldots, b_n$ eine Basis von V ist.

Beweis. Es seien $b_1, \ldots, b_n$ eine Basis und $(w_j)_{j \in J}$ ein Erzeugendensystem von V. Der Beweis erfolgt mit Hilfe des Austauschlemmas und dem Prinzip der vollständigen Induktion.

IA: Für $k = 0$ wählt man $S = \emptyset$ und erhält sofort die Aussage.

IV: Sei $k \in \{0, \dots, n-1\}$ mit der Eigenschaft, dass es ein $S \subset J$ gibt mit $\mid S \mid = k$, sodass $(w_s)_{s\in S}, b_{k+1}, \dots, b_n$ eine Basis von V ist.

IS: Angenommen für alle $j \in J \setminus S$ gäbe es $u_s, \lambda_i \in K$, sodass

$$w_j = \sum_{s\in S} u_s w_s + 0 \cdot b_{k+1} + \sum_{i=k+2}^{n} \lambda_i b_i.$$

Dann wäre für alle $j \in J$:

$$w_j \in \langle (w_s)_{s\in S}, b_{k+2}, \dots, b_n \rangle$$

Damit wäre $(w_s)_{s\in S}, b_{k+2}, \dots, b_n$ ein Erzeugendensystem, weil $(w_j)_{j\in J}$ ein Erzeugendensystem ist.

Nach der IV ist $(w_j)_{j\in S}, b_{k+1}, \dots, b_n$ eine Basis und damit insbesondere ein *minimales* Erzeugendensystem. So erhält man jedoch einen Widerspruch, da

$$(w_j)_{j\in S}, b_{k+2}, \dots, b_n \subsetneq (w_j)_{j\in S}, b_{k+1}, \dots, b_n$$

und die linke Seite auch ein Erzeugendensystem ist.

Aus dem Widerspruch folgt, dass es ein $j \in J \setminus S$ geben muss mit $u_s, \lambda_i \in K$ und $\mu \in K \setminus \{0\}$, sodass

$$w_j = \sum_{s\in S} u_s w_s + \mu \cdot b_{k+1} + \sum_{i=k+2}^{n} \lambda b_i.$$

Nach dem Austauschlemma muss auch $(w_s)_{s\in S'}, b_{k+2}, \dots, b_n$ mit $S' = S \cap \{j\}$ eine Basis sein.

Nach dem Prinzip der vollständigen Induktion folgt die Aussage. □

Theorem 2.7.38

In einem endlich erzeugten Vektorraum gibt es eine endliche Basis und alle Basen von V haben dieselbe Länge.

Beweis (Theorem 2.7.38). Sei V ein endlich erzeugter Vektorraum. Also hat V ein endliches Erzeugendensystem. Durch sukzessives Entfernen von Elementen erhält man ein minimales Erzeugendensystem und somit eine Basis B von V.

Die Basis B habe die Kardinalität n. Sei B' eine weitere Basis. O.B.d.A. ist $|B'| \geq n$. Nach Theorem 2.7.37 kann man die Elemente von B in B' hinein tauschen und erhält eine Basis $\tilde{B}$, für die gilt $|\tilde{B}| = |B'|$. Da B eine Basis ist (insbesondere eine *maximale* linear unabhängige Familie) und in $\tilde{B}$ enthalten ist, muss $\tilde{B} = B$ und damit $|B'| = n$. □

Wir können also nun endlich den Begriff der Dimension eines Vektorraums erlangen.

2.7.3 Dimension eines Vektorraums

Definition 2.7.39

Die Länge einer endlichen Basis von V nennen wir **Dimension** von V (kurz $\dim V$). Wenn V keine endliche Basis haben sollte, so heißt V unendlich-dimensional (kurz $\dim V = \infty$).

Beispiel 2.7.40

1. Der K^n hat Dimension n, da dieser die kanonische Basis $(e_1, \ldots, e_n)$ besitzt.
2. Sei K ein Körper und $K^{m\times n}$ ein zugehöriger Matrizenring. Man erhält als Basis $(E^{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n)$. Damit muss der Matrizenring die Dimension $m \cdot n$ haben.
3. Man betrachtet den $K[x]$. Dieser hat $(x^i \mid i \geq 0)$ als eine Basis und damit die Dimension ∞.

Proposition 2.7.41

Der Vektorraum $M_{m,n}(K)$ hat Dimension $m \cdot n$.

Theorem 2.7.42

Jeder Vektorraum hat eine Basis $(b_i)_{i\in I}$. Für jede weitere Basis $(b'_j)_{j\in J}$ gibt es eine Bijektion $\pi : I \longrightarrow J$.

Zwei Mengen I und J heißen **gleichmächtig**, wenn es eine Bijektion $\pi : I \longrightarrow J$ gibt.

Beweis. Sei V ein K-Vektorraum und $(b_i)_{i\in I}$ eine Basis. Sei $(b'_j)_{j\in J}$ eine weitere Basis. Wegen Theorem 2.7.38 gilt
$\mid I \mid = \mid J \mid$. Deshalb kann man eine Bijektion zwischen den Basen finden. □

Satz 2.7.43

Zwei Vektorräume sind genau dann isomorph, wenn sie gleichmächtige Basen haben.

Beweis. Seien V, W zwei K-Vektorräume.

(1) $\Rightarrow$ (2) Es gibt einen Isomorphismus $\varphi : V \to W$. Sei $B = (b_i)_{i\in I}$ eine Basis von V. Man versucht nun zu zeigen, dass $\varphi(B)$ eine Basis von W ist. Angenommen,

$$0 = \sum_{i\in I} \lambda_i \varphi(b_i)$$

für $\lambda_i \in K$. Dann gilt auf Grund der Linearität

$$0 = \sum_{i\in I} \varphi(\lambda_i b_i) = \varphi\left(\sum_{i\in I} \lambda_i b_i\right) \overset{\varphi \text{ Isomorphismus}}{\Rightarrow} 0 = \sum_{i\in I} \lambda_i b_i.$$

Da B eine Basis ist, müssen die λ_i alle Null sein. Also ist $\varphi(B)$ linear unabhängig.

Sei $w \in W$ beliebig, aber fest. Da φ ein Isomorphismus ist, gibt es ein $v \in V$, sodass $\varphi(v) = w$. Für v gibt es wiederum $\lambda_i \in K$, sodass

$$v = \sum_{i \in I} \lambda_i b_i,$$

womit

$$w = \varphi(v) = \sum_{i \in I} \lambda_i \varphi(b_i).$$

Da w beliebig war, ist $\varphi(B)$ ein Erzeugendensystem und insgesamt eine Basis. Weil φ ein Isomorphismus ist, gilt $|\varphi(B)| = |B|$ und damit $\dim W = \dim V$.

(2) $\Rightarrow$ (1) Es seien $(b_i)_{i \in I}$ eine Basis von V und $(c_j)_{j \in J}$ eine Basis von W. Da diese gleichmächtig sind, gibt es eine Bijektion $\pi : I \to J$. Man definiert somit einen Isomorphismus, was die geneigten Lesenden überprüfen können.

$$\varphi : V \to W : \sum_{i \in I} \lambda_i b_i \mapsto \sum_{i \in I} \lambda_i c_{\pi(i)}$$

□

Proposition 2.7.44

Es sei V ein Vektorraum der Dimension $n < \infty$. Dann bilden n linear unabhängige Vektoren immer eine Basis.

Beweis (Proposition 2.7.44): Seien V ein Vektorraum der Dimension $n < \infty$, B eine Basis von V und $v_1, \ldots, v_n \in V$ linear unabhängige Vektoren.

Angenommen, $v_1, \ldots, v_n$ bilden keine Basis von V, dann kann es sich bei diesen nicht um ein Erzeugendensystem handeln. Da B ein Erzeugendensystem ist, können $v_1, \ldots, v_n$ wegen Theorem 2.7.22 zu einer Basis von V erweitert werden. Dabei muss jedoch mindestens ein Element aus B hinzugefügt werden, womit man eine Basis mit Länge echt größer n erhält, was im Widerspruch zu $\dim V = n$ steht.

Per Beweis durch Widerspruch folgt also, dass $v_1, \ldots, v_n$ eine Basis von V bildet. □

Korollar 2.7.45

Es sei W ein Unterraum von V. Dann gilt

1. $\dim W \leq \dim V$.
2. $\dim W = \dim V < \infty \Longrightarrow W = V$.

Beweis (Korollar 2.7.45): Es sei W ein Unterraum von einem Vektorraum V.

1. Sei B eine Basis von W. Nach Korollar 2.7.24 existiert ein Komplement $U \subset V$, sodass $W \oplus U = V$. Sei C eine Basis von U, dann ist $B \cup C$ eine Basis von V. Insgesamt gilt wegen $B \cap C = \emptyset$, dass

$$\dim W + \dim U = | B | + | C | = | B \cup C | = \dim V.$$

Da $\dim U \geq 0$,

$$\dim W = \dim V - \dim U \leq \dim V.$$

2. Gilt $\dim W = \dim V$, dann gilt wegen Obigem $\dim U = 0$ und damit $U = 0$, womit

$$V = W \oplus U = W \oplus 0 = W.$$

□

Proposition 2.7.46

Es seien $V_1, \ldots, V_r$ K-Vektorräume. Dann gilt $\dim(V_1 \times \ldots \times V_r) = \dim V_1 + \ldots + \dim V_r$.

Beweis (Proposition 2.7.46): Seien $V_1, \ldots, V_r$ K-Vektorräume und $B_1, \ldots, B_r$ Basen dieser Vektorräume. Es sei den geneigten Lesenden überlassen zu zeigen, dass

$$\bigcup_{i=1}^{r} \left(\bigtimes_{j=1}^{i-1} \{0\} \right) \times B_i \times \left(\bigtimes_{j=i+1}^{r} \{0\} \right)$$

eine Basis von $V_1 \times \ldots \times V_n$ ist. Damit folgt die Formel sofort. □

Korollar 2.7.47

Es seien U_1, U_2 Unterräume von V mit $U_1 \cap U_2 = \{0\}$. Dann gilt

$$\dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2.$$

Beweis (Korollar 2.7.47): Seien U_1, U_2 Unterräume von V mit $U_1 \cap U_2 = \{0\}$. Dann ist

$$W = U_1 \oplus U_2$$

ein Vektorraum. Seien B, C Basen von U_1, U_2. Wegen $U_1 \cap U_2 = \{0\}$ ist $B \cap C = \emptyset$, womit $B \cup C$ Basis von W und

$$\dim(U_1 \oplus U_2) = \dim W = |B \cup C| = |B| + |C| = \dim U_1 + \dim U_2.$$

□

Korollar 2.7.48

Es sei U ein Unterraum von V. Dann gilt $\dim V = \dim U + \dim V/U$.

Beweis (Korollar 2.7.48): Es sei U ein Unterraum von V. Nach Korollar 2.7.24 existiert ein Komplement $W \subset V$, sodass $U \oplus W = V$. Man betrachtet nun die Abbildung

$$\pi : V \to V : u + w \mapsto w.$$

Es ist bereits bekannt, dass $\operatorname{Ker} \pi = U$ und $\operatorname{Im} \pi = W$. Nach dem Isomorphiesatz für lineare Abbildungen gilt, dass

$$V/U = V/\operatorname{Ker} \pi \simeq \operatorname{Im} \pi = W,$$

womit

$$\dim V/U = \dim W.$$

Insgesamt ergibt sich

$$\dim V = \dim U + \dim W = \dim U + \dim V/U.$$

□

Korollar 2.7.49

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Dann gilt

$$\dim V = \dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi.$$

Beweis (Korollar 2.7.49): Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Nach dem Isomorphiesatz gilt

$$V/\operatorname{Ker} \varphi \simeq \operatorname{Im} \varphi,$$

womit nach Korollar 2.7.48

$$\begin{aligned} \dim V &= \dim \operatorname{Ker} \varphi + \dim V/\operatorname{Ker} \varphi \\ &= \dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi \end{aligned}$$

gilt. □

2.8 Lineare Abbildungen - extended

Wir setzen hier die im Kapitel zu Dimensionstheorie begonnene Reduktion auf Basiselemente fort. Während im Kapitel zur Dimensionstheorie Vektorräume auf eine Basis reduziert wurden, betrachten wir nun, wie man lineare Abbildungen mit Hilfe von Basen reduzieren kann. Darüber hinaus werden wir einige andere Eigenschaften linearer Abbildungen diskutieren.

2.8.1 Darstellungsmatrix

Proposition 2.8.1

Es sei $b_1, \ldots, b_n$ eine Basis des K-Vektorraums V und $w_1, \ldots, w_n$ beliebige Elemente des K-Vektorraums W. Dann gibt es genau eine K-lineare Abbildung

$$\varphi : V \longrightarrow W, \quad \varphi(b_i) = w_i.$$

Beweis (Proposition 2.8.1): Sei $b_1, \ldots, b_n$ eine Basis des K-Vektorraums V und $w_1, \ldots, w_n$ beliebige Elemente des K-Vektorraums W. Man konstruiert

$$\varphi : \quad V \to W : \quad v = \sum_{i=1}^{n} \lambda_i b_i \mapsto \sum_{i=1}^{n} \lambda_i w_i.$$

Per Definition erfüllt φ die geforderte Eigenschaft. Angenommen, es gäbe eine zweite Abbildung ψ, die ebenfalls diese Eigenschaft erfüllt. Da φ und ψ auf dem Erzeugendensystem von V übereinstimmen, muss $\varphi = \psi$. Es gibt also genau eine lineare Abbildung, die die geforderte Eigenschaft erfüllt. □

Die zu Grunde liegende Idee besteht darin, dass eine lineare Abbildung $\varphi : V \to W$ eindeutig durch die Bilder der Basiselemente festgelegt wird. Da alle anderen Elemente $v \in V$ als Linearkombination der Basiselemente dargestellt werden können, ergeben sich die Bilder der $v \in V$ durch die Linearität von φ.

Es sei $b_1, \ldots, b_n$ eine Basis von V, $c_1, \ldots, c_m$ eine Basis von W und $\varphi : V \longrightarrow W$ eine lineare Abbildung. Es sei $v \in V$. Wir wollen den Koordinatenvektor von $\varphi(v)$ bezüglich der Basis von W bestimmen. Es sei

$$v = \lambda_1 b_1 + \ldots + \lambda_n b_n$$

und

$$\varphi(b_j) = a_{1j} c_1 + \ldots + a_{mj} c_m.$$

Dann ist

$$\varphi(v) = \sum_{j=1}^{n} \lambda_j \varphi(b_j) = \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{m} a_{ij} c_i \right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \lambda_j a_{ij} \right) c_i.$$

Dann ist der **Koordinatenvektor** von $\varphi(v)$ bezüglich der Basis $c_1, \ldots, c_n$ genau

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = (a_{\bullet,1} \cdots a_{\bullet,n}) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

Definition 2.8.2

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, $B = (b_1, \ldots, b_n)$ eine Basis von V und $C = (c_1, \ldots, c_m)$ eine Basis von W. Dann nennen wir die vorher konstruierte $m \times n$-Matrix ${}^C A_\varphi^B$ die ***Darstellungsmatrix* von φ bezüglich B und C.**

Beispiel 2.8.3

Es seien $V = \mathbb{R}^3$, $W = \mathbb{R}^2$, $B = (e_1, e_2, e_3)$, $C = (e_1, e_2)$ und

$$\varphi : V \to W : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} x + y + z \\ 2y - z \end{pmatrix}.$$

Dann gilt

$$\varphi(e_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ \varphi(e_2) = \begin{pmatrix} 1 \\ 2 \end{pmatrix},\ \varphi(e_3) = \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

wobei dies schon die Koordinatenvektoren bezüglich der Basis C sind. Damit ergibt sich

$${}^C A_\varphi^B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \end{pmatrix}$$

für die Darstellungsmatrix.

Proposition 2.8.4

Für festgewählte Basen B (resp. C) von V (resp. W) induziert die Zuordnung $\varphi \mapsto {}^C A_\varphi^B$ eine kanonische Bijektion zwischen $\mathrm{Hom}_K(V, W)$ und $K^{m \times n}$.

Der Beweis von Proposition 2.8.4 sei den geneigten Lesenden überlassen, da im Grunde nicht mehr viel zu zeigen ist. Das Resultat ist jedoch ein erheblicher Fortschritt in unserem Bemühen, lineare Abbildungen durch Basiselemente darzustellen. Wir können also durch Wahl von Basen alle linearen Abbildungen zwischen Vektorräumen mit endlicher Dimension mit der Menge der Matrizen des jeweils passenden Formats identifizieren.

Wenn wir für K^n und K^m die Standardbasen wählen, dann schreiben wir nur A_φ für die Darstellungsmatrix.
Wir haben schon gesehen, dass $A \in K^{m \times n}$ eine lineare Abbildung $\varphi_A : K^n \longrightarrow K^m$ induziert und es gilt

$$A_{(\varphi_A)} = A.$$

Wie man im obigen Beispiel beobachten kann, sind die Spalten der Darstellungsmatrix immer die Koordinatenvektoren der Bilder der Ursprungsbasis bezüglich der neuen Basis im Zielraum. Also gilt für eine lineare Abbildung $\varphi : V \to W$, wobei V und W Basen $B = (b_1, \ldots, b_n)$ und $C = (c_1, \ldots, c_m)$ haben,

$${}^C A_\varphi^B = \begin{pmatrix} | & & | \\ (\varphi(b_1))_C & \cdots & (\varphi(b_n))_C \\ | & & | \end{pmatrix}.$$

Es ist auch zu beobachten, dass ${}^{C}A_{\varphi}^{B}$ das Format $m \times n = \dim W \times \dim V$ hat. Um das Bild für ein beliebiges $v \in V$ zu berechnen, bildet man den Koordinatenvektor v_B und braucht nur noch zu multiplizieren:

$$\varphi(v) = {}^{C}A_{\varphi}^{B} \cdot v_B$$

Der "Beweis" hierzu ist bereits in der Konstruktion der Darstellungsmatrix enthalten.

Bemerkung 2.8.5

Es seien B, C, D Basen von V, W, X, $\varphi : V \longrightarrow W$, $\psi : W \longrightarrow X$ lineare Abbildungen, dann gilt

$${}^{D}A_{\psi\circ\varphi}^{B} = {}^{D}A_{\psi}^{C} \circ {}^{C}A_{\varphi}^{B}.$$

Beispiel 2.8.6

Man setzt die Situation aus dem letzten Beispiel fort.

1. Man betrachtet $B' = (e_1, -2e_1 + e_2 + e_3, -3e_1 + e_2 + 2e_3) \subset V$ als eine andere Basis von V. Damit ergibt sich

   $$\varphi(e_1) = \begin{pmatrix}1\\0\end{pmatrix},\ \varphi(e_2) = \begin{pmatrix}0\\1\end{pmatrix},\ \varphi(e_3) = \begin{pmatrix}0\\0\end{pmatrix}$$

   und

   $${}^{C}A_{\varphi}^{B'} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}.$$

2. Es sei $C' = (2e_1 + e_2, e_1 + e_2) \subset W$. Dann ist

   $${}^{C'}A_{\varphi}^{B'} = \begin{pmatrix}1 & -1 & 0\\ -1 & 2 & 0\end{pmatrix}.$$

2.8.2 Eigenwerte

Definition 2.8.7

Es sei $f : V \longrightarrow V$ eine lineare Abbildung eines K-Vektorraums in sich selbst. Ein Vektor $v \in V$ heißt **Eigenvektor** von f, falls

E1 $v \neq 0$.

E2 $\exists\, \lambda \in K$ mit $f(v) = \lambda \cdot v$.

In diesem Fall nennen wir v einen Eigenvektor zum Eigenwert λ. Für jeden **Eigenwert** definieren wir den **Eigenraum**

$$\mathrm{Eig}_f(\lambda) = \{v \in V \mid f(v) = \lambda \cdot v\}.$$

Beispiel 2.8.8

1. Es sei $V = \mathbb{R}^2$ und φ die Spiegelung an der y-Achse. Also

$$\varphi : \mathbb{R}^2 \to \mathbb{R}^2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x \\ y \end{pmatrix}.$$

   Für die y-Achse gilt:

$$\text{für alle } v \in \mathbb{R}^2, (\exists\, \mu \in \mathbb{R} : v = \mu \cdot e_2), v \neq 0 : \varphi(v) = v.$$

   Diese v sind Eigenvektoren zum Eigenwert 1. Der Eigenraum von φ bezüglich 1 ist die y-Achse also $\text{Eig}_\varphi(1) =$ 'y-Achse'.

   Für die x-Achse gilt:

$$\text{für alle } v \in \{w \in V \mid \exists\, \mu \in \mathbb{R} : w = \mu e_1\}, v \neq 0 : \varphi(v) = -v.$$

   Diese v sind dann Eigenvektoren zum Eigenwert -1. Der Eigenraum von φ bezüglich -1 ist die x-Achse.

2. Es sei φ die Drehung um $\frac{\pi}{2}$ im $\mathbb{R}^2$. Hier gibt es keine Eigenvektoren.

Bemerkung 2.8.9

$\text{Eig}_f(\lambda)$ ist ein Unterraum von V.

Für die Bestimmung von Eigenwerten, -vektoren, -räumen benötigen wir derzeit noch den Gauß-Algorithmus. Wir werden noch eine effizientere Methode kennenlernen.

Beispiel 2.8.10

Eigenwert und Abbildungsmatrix:

1. Es sei $B = (e_1, e_2) \subset \mathbb{R}^2$. Man betrachtet die lineare Abbildung mit

$$\varphi(e_1) = -e_1, \;\; \varphi(e_2) = e_2,$$

   also die Spiegelung an der y-Achse. Es ergibt sich

$${}^B A_\varphi^B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

   als Darstellungsmatrix. Die Eigenwerte finden wir auf der Diagonalen der Darstellungsmatrix wieder. Später werden wir untersuchen, ob wir immer eine solche passende Darstellungsmatrix finden. Das nächste Beispiel gibt uns bereits ein notwendiges Kriterium.

2. Sei V ein K-Vektorraum und $B = (b_1, \ldots, b_n)$ eine Basis aus Eigenvektoren zu den Eigenwerten λ_i. Da für alle $1 \leq i \leq n$

$$\varphi(b_i) = \lambda_i b_i \Rightarrow (\varphi(b_i))_B = \lambda_i,$$

gilt

$$ {}^{B}A_{\varphi}^{B} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}. $$

Aus dem Beispiel erkennt man, dass uns Eigenwerte helfen werden, Darstellungsmatrizen auf eine "schönere" Form zu bringen.

2.8.3 Äquivalenzrelationen auf Matrizen

Definition 2.8.11

Zwei Matrizen $A, B \in K^{m\times n}$ heißen **äquivalent** genau dann, wenn $\exists\, S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ so, dass $B = S \cdot A \cdot T^{-1}$.
Zwei Matrizen $A, B \in K^{n\times n}$ heißen **ähnlich** genau dann, wenn $\exists\, S \in \mathrm{GL}_n(K)$ so, dass $B = S \cdot A \cdot S^{-1}$.

Proposition 2.8.12

Beides sind Äquivalenzrelationen auf $K^{m\times n}$ bzw. $K^{n\times n}$.

Beweis (Proposition 2.8.12). Seien K Körper und $m, n \in \mathbb{N}$.

Reflexivität: Seien $A \in K^{m\times n}$ und $B \in K^{n\times n}$, dann

$$ \begin{aligned} E_m \cdot A \cdot E_n &= A \\ E_n \cdot B \cdot E_n &= B \end{aligned} $$

,

wobei bekanntlich $E_m \in \mathrm{GL}_m(K)$ und $E_n \in \mathrm{GL}_n(K)$. Damit ist A zu sich selbst äquivalent und B zu sich ähnlich.

Symmetrie: Seien $A, C \in K^{m\times n}$ äquivalent und $B, D \in K^{n\times n}$ ähnlich. Das heißt, es gibt $S \in \mathrm{GL}_m(K)$ und $T, U \in \mathrm{GL}_n(K)$, sodass

$$ \begin{aligned} A &= S \cdot C \cdot T^{-1} \\ B &= U \cdot D \cdot U^{-1}. \end{aligned} $$

Aufgrund der Definition der allgemeinen linearen Gruppen sind $S^{-1} \in \mathrm{GL}_m(K)$ und $T^{-1}, U^{-1} \in \mathrm{GL}_n(K)$, sodass

$$ \begin{aligned} C &= S^{-1} \cdot A \cdot T = S^{-1} \cdot A \cdot (T^{-1})^{-1} \\ D &= U^{-1} \cdot B \cdot U = U^{-1} \cdot B \cdot (U^{-1})^{-1} \end{aligned} $$

gilt. Also sind auch C äquivalent zu A und D ähnlich zu B.

Transitivität: Hier wird nur die Ähnlichkeit betrachtet. Der Fall der Äquivalenz folgt aber analog. Seien $A, B, C \in K^{n\times n}$ mit A ähnlich zu B und B ähnlich zu C. Es gibt also $S, T \in \mathrm{GL}_n(K)$, sodass $A = SBS^{-1}$ und $C = TBT^{-1}$.

Es gilt

$$S^{-1}T^{-1} \cdot TS = S^{-1}S = E_n,$$

also $S^{-1}T^{-1} = (TS)^{-1}$. Da das Produkt zweier invertierbarer Matrizen wieder invertierbar ist, gilt $TS \in \mathrm{GL}_n(K)$.

Insgesamt ergibt sich

$$C = T \cdot B \cdot T^{-1} = T \cdot (S \cdot B \cdot S^{-1}) \cdot T^{-1} = (TS) \cdot B \cdot (TS)^{-1},$$

womit A ähnlich zu C ist.

□

Die in Definition 2.8.11 eingeführten Äquivalenzenrelationen scheinen erst einmal willkürlich zu sein. Sie werden später jedoch sehr nützlich sein, wenn wir Basiswechsel betrachten. Wir haben schließlich bereits das Phänomen festgestellt, dass ein und dieselbe lineare Abbildung bezüglich unterschiedlicher Basen unterschiedliche Darstellungsmatrizen hat. Es wird sich zeigen, dass gerade die zur gleichen Abbildung gehörenden Darstellungsmatrizen äquivalent bzw. ähnlich zueinander sind.

2.8.4 Basiswechselmatrizen

Bei der Äquivalenz und Ähnlichkeit von Matrizen wurde bereits der Basiswechsel thematisiert. Man wird diesen nun genauer betrachten, wir gehen zurück zu den Koordinatenvektoren:

Proposition 2.8.13

Es seien B und C Basen von V, wobei $\dim V = n < \infty$. Für $v \in V$ seien $v_B, v_C \in K^n$ die Koordinatenvektoren bezüglich B und C. Dann gibt es genau eine Matrix $T \in \mathrm{GL}_n(K)$ so, dass für jedes $v \in V$ gilt

$$v_C = Tv_B.$$

Beweis (Proposition 2.8.13): Seien B und C Basen von V, wobei V ein endlich-dimensionaler Vektorraum sei. Man betrachtet nun die Identität $\mathrm{id} : V \to V$, welche eine lineare Abbildung ist und setzt $T = {}^{C}A^{B}_{\mathrm{id}}$. Diese Matrix erfüllt per Definition für alle $v \in V$:

$$(v)_C = (\mathrm{id}(v))_C = {}^{C}A^{B}_{\mathrm{id}} \cdot (v)_B = T \cdot (v)_B$$

Außerdem muss $T \in \mathrm{GL}_n(K)$ sein, da id ein Isomorphismus ist.

Sei $D \in K^{n\times n}$ eine beliebige Matrix, die für alle $v \in V$:

$$(v)_C = D \cdot (v)_B$$

erfüllt. Dann gilt dies insbesondere für die Basisvektoren $b_1, \ldots, b_n$, deren Koordinatenvektoren bezüglich B die Vektoren $e_1, \ldots, e_n \in K^n$ sind. Damit gilt für alle $1 \le i \le n$:

$$T_{\bullet,i} = T \cdot e_i = T \cdot (b_i)_B = (b_i)_C = D \cdot (b_i)_B = D_{\bullet,i},$$

also $T = D$, womit die Proposition gezeigt ist. □

Definition 2.8.14

Die Matrix T nennen wir ***Basiswechselmatrix*** und schreiben ${}^{C}\mathrm{id}_{V}^{B}$ dafür (wenn der Vektorraum außer Frage steht, schreiben wir auch einfach ${}^{C}\mathrm{id}^{B}$).

Beispiel 2.8.15

[Definition 2.8.14] Sei $V = \mathbb{R}^2$ und $C = (c_1, c_2) = (e_1, e_2)$, $B = (b_1, b_2) = (e_1 + e_2, -e_1 + 2e_2)$ seien Basen. Es gilt

$$\begin{aligned}\mathrm{id}(b_1) &= e_1 + e_2 = c_1 + c_2\\ \mathrm{id}(b_2) &= -e_1 + 2e_2 = -c_1 + 2c_2,\end{aligned}$$

womit

$$(b_1)_C = \begin{pmatrix}1\\1\end{pmatrix}, \quad (b_2)_C = \begin{pmatrix}-1\\2\end{pmatrix}.$$

Also hat die Basiswechselmatrix von B nach C die Form

$${}^{C}\mathrm{id}^{B} = {}^{C}A_{\mathrm{id}}^{B} = \begin{pmatrix}1 & -1\\1 & 2\end{pmatrix}.$$

Möchte man nun von C nach B, so hilft der Zusammenhang

$${}^{B}\mathrm{id}^{C}\,{}^{C}\mathrm{id}^{B} = {}^{B}A_{\mathrm{id}}^{C}\,{}^{C}A_{\mathrm{id}}^{B} = {}^{B}A_{\mathrm{id}\circ\mathrm{id}}^{B} = {}^{B}A_{\mathrm{id}}^{B} = E_n,$$

womit ${}^{B}\mathrm{id}^{C} = \left({}^{C}\mathrm{id}^{B}\right)^{-1}$. Nach der Formel zur Invertierung von 2×2 Matrizen wissen wir, dass

$${}^{B}\mathrm{id}^{C} = \frac{1}{1 \cdot 2 - 1 \cdot (-1)} \cdot \begin{pmatrix}2 & 1\\-1 & 1\end{pmatrix} = \frac{1}{3} \cdot \begin{pmatrix}2 & 1\\-1 & 1\end{pmatrix}.$$

Proposition 2.8.13 liefert die Wohldefiniertheit der Basiswechselmatrizen.

Proposition 2.8.16

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, $\dim V, \dim W < \infty$, B, B' und B'' Basen von V, C und C' Basen von W. Dann gilt

$${}^{C'}A_{\varphi}^{B'} = {}^{C'}\mathrm{id}^{C}\ {}^{C}A_{\varphi}^{B}\ {}^{B}\mathrm{id}^{B'}.$$

Insbesondere ist ${}^{B''}\mathrm{id}^{B} = {}^{B''}\mathrm{id}^{B'}\ {}^{B'}\mathrm{id}^{B}$.

Beweis (Proposition 2.8.16): Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, $\dim V = n$, $\dim W = m$ mit $m, n < \infty$, B und B' Basen von V, C und C' Basen von W. Es gilt

für alle $1 \leq i \leq n$:

$$\begin{aligned}\left({}^{C'}\mathrm{id}^{C}\,{}^{C}A_{\varphi}^{BB}\mathrm{id}^{B'}\right)_{\bullet,i} &= {}^{C'}\mathrm{id}^{C}\,{}^{C}A_{\varphi}^{BB}\mathrm{id}^{B'}\cdot\left(b_i'\right)_{B'} = {}^{C'}\mathrm{id}^{C}\,{}^{C}A_{\varphi}^{B}\cdot\left(b_i'\right)_{B}\\ &= {}^{C'}\mathrm{id}^{C}\cdot\left(\varphi\left(b_i'\right)\right)_{C} = \left(\varphi\left(b_i'\right)\right)_{C'}\\ &= \left({}^{C'}A_{\varphi}^{B'}\right)_{\bullet,i},\end{aligned}$$

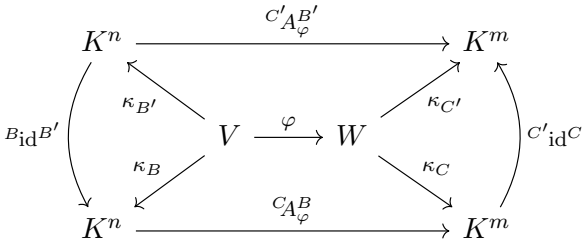
womit

$${}^{C'}\mathrm{id}^{C}\,{}^{C}A_{\varphi}^{BB}\mathrm{id}^{B'} = {}^{C'}A_{\varphi}^{B'}.$$

□

Mit Proposition 2.8.16 wird ein Teil des Zusammenhanges zwischen der Äquivalenz von Matrizen und Darstellungsmatrizen hergestellt. Da sowohl ${}^{B}\mathrm{id}^{B'}$ als auch ${}^{C'}\mathrm{id}^{C}$ invertierbar sind, sind ${}^{C'}A_{\varphi}^{B'}$ und ${}^{C}A_{\varphi}^{B}$ äquivalent.

Wir fassen nun die durch Koordinatenabbildungen, Abbildungsmatrizen und Basiswechselmatrizen gewonnen Zusammenhänge für die Situation aus Proposition 2.8.16 in einem kommutativen Diagramm zusammen:



Dabei sind die κ die Koordinatenabbildungen, die A_φ verschiedene Darstellungsmatrizen von φ und die id die Basiswechselmatrizen.

Beispiel 2.8.17

Seien

$$\varphi : \mathbb{R}^3 \to \mathbb{R}^2 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} x + 2y - z \\ -x - z \end{pmatrix}$$

eine lineare Abbildung und $B = (e_1, 2e_2 + e_3, e_1 + e_2 + e_3)$, $C = (-e_2, e_1 + e_2)$ Basen. Dann

$$\varphi(b_1) = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad \varphi(b_2) = \begin{pmatrix} 3 \\ -1 \end{pmatrix}, \quad \varphi(b_3) = \begin{pmatrix} 2 \\ -2 \end{pmatrix}$$

und

$$\left(\begin{array}{cc|c} 0 & 1 & x \\ -1 & 1 & y \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & -1 & -y \\ 0 & 1 & x \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 0 & x - y \\ 0 & 1 & x \end{array}\right),$$

womit

$$(\varphi(b_1))_C = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \quad (\varphi(b_2))_C = \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \quad (\varphi(b_3))_C = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

und

$$ {}^{C}A_{\varphi}^{B} = \begin{pmatrix} 2 & 4 & 4 \\ 1 & 3 & 2 \end{pmatrix}. $$

Man betrachtet nun Basen $B' = (e_1 + e_2, e_1 - e_2, e_1 - e_2 - e_3)$, $C' = (3e_1 - e_2, -e_1 - e_2)$. Um auf die Basiswechselmatrizen zu kommen, führt man den Gauß-Algorithmus parallel aus.

B' zu B:

$$ \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 & -1 & -1 \\ 0 & 1 & 1 & 0 & 0 & -1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 & -1 & -1 \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{array}\right) $$

$$ \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 & -1 & -1 \\ 0 & 0 & 1 & -1 & 1 & -1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 & -2 & 0 \\ 0 & 0 & 1 & -1 & 1 & -1 \end{array}\right) $$

$$ \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 1 & -1 \end{array}\right), $$

womit

$$ \left(b_1'\right)_B = \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}, \quad \left(b_2'\right)_B = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \quad \left(b_1'\right)_B = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} $$

und

$$ {}^{B}\mathrm{id}^{B'} = \begin{pmatrix} 2 & 0 & 2 \\ 1 & -1 & 0 \\ -1 & 1 & -1 \end{pmatrix}. $$

C zu C':

$$ \left(\begin{array}{cc|cc} 3 & -1 & 0 & 1 \\ -1 & -1 & -1 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 3 & -1 & 0 & 1 \\ -3 & -3 & -3 & 3 \end{array}\right) $$

$$ \rightsquigarrow \left(\begin{array}{cc|cc} 3 & -1 & 0 & 1 \\ 0 & -4 & -3 & 4 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 3 & -1 & 0 & 1 \\ 0 & 1 & \frac{3}{4} & -1 \end{array}\right) $$

$$ \rightsquigarrow \left(\begin{array}{cc|cc} 3 & 0 & \frac{3}{4} & 0 \\ 0 & 1 & \frac{3}{4} & -1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{4} & 0 \\ 0 & 1 & \frac{3}{4} & -1 \end{array}\right), $$

womit

$$ {}^{C'}\mathrm{id}^{C} = \begin{pmatrix} \frac{1}{4} & 0 \\ \frac{3}{4} & -1 \end{pmatrix}. $$

Mit Proposition 2.8.16 folgert man

$$ {}^{C'}A_{\varphi}^{B'} = {}^{C'}\mathrm{id}^{C} \cdot A_{C,B}^{\varphi} \cdot {}^{B}\mathrm{id}^{B'} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. $$

Korollar 2.8.18

Es sei V ein K-Vektorraum mit $\dim V = n < \infty$. Zwei Matrizen $A, A' \in K^{n\times n}$ sind genau dann ähnlich, wenn es eine lineare Abbildung $\varphi : V \longrightarrow V$ und Basen B, B' von V gibt, so dass $A = {}^{B}A_{\varphi}^{B}$ und $A' = {}^{B'}A_{\varphi}^{B'}$.

Beweis (Korollar 2.8.18): Seien V ein K-Vektorraum mit $\dim V = n < \infty$ und zwei Matrizen $A, A' \in K^{n\times n}$. Die Rückrichtung wurde bereits in einer obigen Bemerkung gezeigt. Es bleibt also nur die Hinrichtung zu zeigen.

Seien also A, A' ähnlich mit $S \in \mathrm{GL}_n(K) : A' = SAS^{-1}$. Man setzt $B = (e_1, \ldots, e_n)$, $B' = \left(S^{-1}_{\bullet,i}\right)_{1\le i\le n}$ und $\varphi = \varphi_A$. Es ist klar, dass

$$A = {}^{B}A_{\varphi}^{B}.$$

Weiterhin gilt für alle $1 \le i \le n$:

$$\left({}^{B}\mathrm{id}^{B'}\right)_{\bullet,i} = \left(b_i'\right)_B = b_i' = S^{-1}_{\bullet,i},$$

womit ${}^{B}\mathrm{id}^{B'} = S^{-1}$ und

$$A' = SAS^{-1} = {}^{B'}\mathrm{id}^{B} \cdot {}^{B}A_{\varphi}^{B} \cdot {}^{B}\mathrm{id}^{B'} = {}^{B'}A_{\varphi}^{B'}.$$

Damit ist die Proposition gezeigt. □

2.8.5 Duale Abbildung

Bemerkung 2.8.19

Erinnerung an die Bilinearform: $V^* \times V \longrightarrow K, \quad \langle f, v\rangle \mapsto f(v)$.

Zu einer Basis $B = (b_1, \ldots, b_n)$ von V gibt es genau eine Basis $b_1^*, \ldots, b_n^*$ von V^* mit

$$\langle b_j^*, b_i\rangle = \delta_{i,j}.$$

Diese Basis nennen wir die **duale Basis** zu B.

Beispiel 2.8.20

1. Sei K ein Körper. Man betrachtet den K^n für $n \in \mathbb{N}$. Sei $B = (b_1, \ldots, b_n)$ eine Basis. Dann gilt für die Darstellungsmatrizen der $b_i^* : K^n \to K$

   $${}^{C}A_{b_i^*}^{B} = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix},$$

   wobei $C = (1)$ eine Basis von K ist und die 1 an der i-ten Stelle steht.

2. Sei $V = \mathbb{R}^3$ und die Basis $B = (e_1 + 2e_2 + e_3, 2e_1 + e_2, 3e_1 + 2e_3)$. Die geneigten Lesenden zeigen, dass es sich bei

   $$B^* = (-\frac{2}{9}e_1^* + \frac{4}{9}e_2^* + \frac{1}{3}e_3^*, \frac{4}{9}e_1^* + \frac{1}{9}e_2^* - \frac{2}{3}e_1^*, \frac{1}{9}e_1^* - \frac{2}{9}e_2^* + \frac{1}{3}e_3^*)$$

   um die duale Basis handelt.

Satz 2.8.21

Es sei V ein endlich-dimensionaler K-Vektorraum. Dann ist die kanonische Abbildung $V \longrightarrow V^{**}, \quad v \mapsto \langle\ , v\rangle$ ein Isomorphismus von K-Vektorräumen.

Beweis (Satz 2.8.5): Sei V ein endlich-dimensionaler K-Vektorraum. Es ist bereits bekannt, dass es sich bei der kanonischen Abbildung um eine lineare Abbildung handelt. Sei $B = (b_1, \ldots, b_n)$ eine Basis von V und $B^* = (b_1^*, \ldots, b_n^*)$ die duale Basis. Dann ist $B^{**} = (\langle -, b_1\rangle, \ldots, \langle -, b_n\rangle)$ die duale Basis von B^*. Wie die geneigten Lesenden zeigen, gibt es eine Bijektion zwischen B^{**} und B, womit V^{**} und V wegen der Linearität der kanonischen Abbildung isomorph zueinander sind. □

Definition 2.8.22

Es sei $A \in K^{m\times n}$, dann definieren wir die **Transponierte Matrix** $A^t \in M_{n,m}(K)$ durch

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{m,n} \end{pmatrix} \Longrightarrow A^t := \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}.$$

Beispiel 2.8.23

1. $$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \Rightarrow A^t = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}$$

2. $$A = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix} \Rightarrow A^t = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}$$

Proposition 2.8.24

Es gilt dann für $A, B \in K^{m\times n}$, $C \in M_{n,p}(K)$, $\lambda \in K$:

1. $(A + B)^t = A^t + B^t$.
2. $(\lambda A)^t = \lambda A^t$.
3. $(AC)^t = C^t A^t$.

Beweis (Proposition 2.8.24): Seien K ein Körper, $A, B \in K^{m\times n}$, $C \in K^{n\times p}$ und $\lambda \in K$.

1. Es gilt für alle $1 \leq i \leq n, 1 \leq j \leq m$:
$$(A + B)^t_{i,j} = (A + B)_{j,i} = A_{j,i} + B_{j,i} = A^t_{i,j} + B^t_{i,j},$$
womit $(A + B)^t = A^t + B^t$.

2. Es gilt für alle $1 \leq i \leq n, 1 \leq j \leq m$:

$$(\lambda A)^t_{i,j} = (\lambda A)_{j,i} = \lambda A_{j,i} = \lambda A^t_{i,j},$$

also $(\lambda A)^t = \lambda A^t$.

3. Es gilt für alle $1 \leq i \leq p, 1 \leq j \leq m$:

$$\begin{aligned}(A \cdot C)^t_{i,j} = (A \cdot C)_{j,i} &= \sum_{k=1}^{n} a_{j,k} \cdot c_{k,i} = \sum_{k=1}^{n} A^t_{k,j} \cdot C^t_{i,k} = \sum_{k=1}^{n} C^t_{i,k} \cdot A^t_{k,j} \\ &= (C^t \cdot A^t)_{i,j},\end{aligned}$$

also $(A \cdot C)^t = C^t \cdot A^t$.

□

Man kann das Transponieren auch als eine Abbildung $\varphi : K^{m \times n} \to K^{n \times m} : A \mapsto A^t$ auffassen. Nach Proposition 2.8.24 ist diese sogar linear. Man kann also auch eine Abbildungsmatrix aufstellen.

Beispiel 2.8.25

Seien $K = \mathbb{R}$ und $m = n = 2$. Dann sind

$$\begin{aligned}B &= (E_{11}, E_{22}, E_{12}, E_{21}) \\ C &= (E_{11}, E_{22}, E_{21}, E_{12})\end{aligned}$$

Basen von $\mathbb{R}^{2\times 2}$, womit die Abbildungsmatrix bezüglich der Transpositionsabbildung

$${}^{C}A^{B}_{\varphi} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

lautet, obwohl es sich bei φ *nicht* um die Identität handelt!

Proposition 2.8.26

Es seien V, W endlich-dimensionale Vektorräume sowie $\varphi : V \longrightarrow W$ eine lineare Abbildung, B eine Basis von V, C eine Basis von W, B^* und C^* die dualen Basen. Es sei ${}^{C}A^{B}_{\varphi}$ die Abbildungsmatrix bezüglich B und C, ${}^{C^*}A^{B^*}_{\varphi^*}$ die Abbildungsmatrix der dualen Abbildung bezüglich C^* und B^*. Dann gilt

$${}^{B^*}A^{C^*}_{\varphi^*} = ({}^{C}A^{B}_{\varphi})^t$$

Der Beweis von Proposition 2.8.26 ist als Übungsaufgabe vorgesehen.

2.8.6 Invertierbarkeit von Matrizen

Definition 2.8.27

Eine Matrix $A \in K^{n\times n}$ heißt **invertierbar** genau dann, wenn $\exists\, A^{-1} \in K^{n\times n}$ mit

$$A \cdot A^{-1} = A^{-1} \cdot A = E_n.$$

Die Menge der invertierbaren Matrizen wird mit $\mathrm{GL}_n(K)$ bezeichnet und heißt **allgemeine lineare Gruppe**.

Beispiel 2.8.28

Es sei

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

Man bestimmt das Inverse, indem man das Problem als drei lineare Gleichungssysteme auffasst. Es werden schließlich die Spalten der Inversen

$$A^{-1} = \begin{pmatrix} | & | & | \\ x_1 & x_2 & x_3 \\ | & | & | \end{pmatrix}$$

gesucht, welche sich durch für alle $1 \le i \le 3$:

$$A \cdot x_i = e_i$$

definieren. Um also das Inverse zu bestimmen, löst man die Gleichungssysteme parallel auf. Dies geschieht, indem man den Gauß-Algorithmus auf die größere Koeffizientenmatrix $(A \mid E_n)$ anwendet. Im Fall des Beispiels gilt:

$$\begin{aligned}
(A \mid E_n) &= \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -2 & 1 & 0 \\ 0 & -2 & -1 & -1 & 0 & 1 \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -2 & 1 & 0 \\ 0 & 0 & 3 & \frac{1}{3} & -\frac{2}{3} & 1 \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & \frac{2}{3} & \frac{2}{3} & -1 \\ 0 & -3 & 0 & -\frac{4}{3} & -\frac{1}{3} & 2 \\ 0 & 0 & 3 & \frac{1}{3} & -\frac{2}{3} & 1 \end{array}\right)
\end{aligned}$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{2}{9} & \frac{4}{9} & \frac{1}{3} \\ 0 & -3 & 0 & -\frac{4}{3} & -\frac{1}{3} & 2 \\ 0 & 0 & 3 & \frac{1}{3} & -\frac{2}{3} & 1 \end{array}\right)$$
$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{2}{9} & \frac{4}{9} & \frac{1}{3} \\ 0 & 1 & 0 & \frac{4}{9} & \frac{1}{9} & -\frac{2}{3} \\ 0 & 0 & 1 & \frac{1}{9} & -\frac{2}{9} & \frac{1}{3} \end{array}\right),$$

womit das Inverse

$$A^{-1} = \begin{pmatrix} -\frac{2}{9} & \frac{4}{9} & \frac{1}{3} \\ \frac{4}{9} & \frac{1}{9} & -\frac{2}{3} \\ \frac{1}{9} & -\frac{2}{9} & \frac{1}{3} \end{pmatrix}$$

ist.

An dieser Stelle sollte man bemerken, dass sich eine allgemeine Formel für 2×2 invertierbare Matrizen herleiten lässt:

Beispiel 2.8.29

Sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K^{m \times n}$$

invertierbar, wobei K ein Körper ist. Wäre eine Zeile von A nur mit Nullen gefüllt, dann wäre A nicht mehr invertierbar, weil

$$\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \cdot x_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot x_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

nicht lösbar sind. Weiterhin gilt, dass es in A mindestens ein Element ungleich null geben muss, da A ansonsten auch nicht invertierbar wäre. Damit kann man für die Spalten argumentieren, dass diese auch ungleich null sein müssen, damit A invertierbar ist:

$$\left(\begin{array}{cc|cc} a & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} a & 0 & 1 & 0 \\ 0 & 0 & -c \cdot a^{-1} & 1 \end{array}\right) \vee \left(\begin{array}{cc|cc} 0 & 0 & 1 & -a \cdot c^{-1} \\ c & 0 & 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{cc|cc} 0 & b & 1 & 0 \\ 0 & d & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 0 & b & 1 & 0 \\ 0 & 0 & -d \cdot b^{-1} & 1 \end{array}\right) \vee \left(\begin{array}{cc|cc} 0 & 0 & 1 & -b \cdot d^{-1} \\ 0 & d & 0 & 1 \end{array}\right)$$

Angenommen, es wäre $a \cdot d - c \cdot b = 0$. O.B.d.A. $a \neq 0$. Dann würde man mit der Rechnung

$$\left(\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ ac & ad & 0 & a \end{array}\right)$$
$$\rightsquigarrow \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & ad - cb & -c & a \end{array}\right)$$

auf einen Widerspruch zur Invertierbarkeit von A stoßen.
Man wendet nun den Gauß-Algorithmus an o.B.d.A $a \neq 0$ (ansonsten $c \neq 0$):

$$\begin{aligned}
\left(\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \end{array}\right) &\rightsquigarrow \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & ad-cb & -c & a \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & 1 & -c(ad-cb)^{-1} & a(ad-cb)^{-1} \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{cc|cc} a & 0 & 1+cb(ad-cb)^{-1} & -ba(ad-cb)^{-1} \\ 0 & 1 & -c(ad-cb)^{-1} & a(ad-cb)^{-1} \end{array}\right) \\
&\rightsquigarrow (ad-cb)^{-1} \cdot \left(\begin{array}{cc|cc} a & 0 & ad-cb+cb & -ba \\ 0 & 1 & -c & a \end{array}\right) \\
&\rightsquigarrow (ad-cb)^{-1} \cdot \left(\begin{array}{cc|cc} a & 0 & ad & -ba \\ 0 & 1 & -c & a \end{array}\right) \\
&\rightsquigarrow (ad-cb)^{-1} \cdot \left(\begin{array}{cc|cc} 1 & 0 & d & -b \\ 0 & 1 & -c & a \end{array}\right)
\end{aligned}$$

So erhält man für invertierbare 2×2 Matrizen eine relativ einfache Formel. Wir werden in Kapitel über Determinanten sehen, dass $ad - cb \neq 0$ sogar eine hinreichende Bedingung für die Invertierbarkeit ist.

Zur Definition der Invertierbarkeit ist es wichtig zu bemerken, dass diese nur auf quadratische Matrizen angewandt wird. Für nicht-quadratische Matrizen unterscheidet man zwischen Links- und Rechtsinversen. Gilt für zwei Matrizen A, B die Beziehung

$$A \cdot B = E_n,$$

dann ist A ein **Linksinverses** von B und B ein **Rechtsinverses** von A. Man nimmt diese Unterscheidung vor, da im Allgemeinen (wenn überhaupt definiert) die Relation

$$B \cdot A \neq E_m$$

gilt. Erst wenn eine Matrix sowohl ein Links- als auch ein Rechtsinverses hat und diese identisch sind, nennt man diese Matrix invertierbar.

2.8.7 Der Rang einer Abbildung

Definition 2.8.30

Es sei $A \in K^{m \times n}$. Dann ist

1. der **Spaltenrang** von A die Dimension des von den Spaltenvektoren erzeugten Unterraums in K^m,
2. der **Zeilenrang** von A die Dimension des von den Zeilenvektoren erzeugten Unterraums im K^n.

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, dann ist der **Rang** von φ die Dimension von $\varphi(V)$.

Beispiel 2.8.31

Man betrachtet die Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & -1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Wie man an der Zeilenstufenform direkt ablesen kann, haben der Spaltenraum und der Zeilenraum Dimension Drei. Die Dimensionen ergeben sich schließlich durch die Anzahl der linear unabhängigen Zeilen / Spalten, da diese die anderen erzeugen und somit eine Basis bilden.

Bemerkung 2.8.32

Falls $\varphi = \varphi_A$, dann ist

$$\text{Spaltenrang } A = \text{Rang } \varphi_A$$

und

$$\text{Zeilenrang } A = \text{Rang } \varphi_{A^t}.$$

Proposition 2.8.33

Für $A \in K^{n\times n}$ sind folgende Aussagen äquivalent:

1. A ist invertierbar;
2. $\exists\, B \in K^{n\times n}$ mit $A \cdot B = E_n$;
3. $\exists\, B \in K^{n\times n}$ mit $B \cdot A = E_n$;
4. Die lineare Abbildung $\varphi_A : K^n \longrightarrow K^n$ ist ein Isomorphimus;
5. Die lineare Abbildung $\varphi_A : K^n \longrightarrow K^n$ ist surjektiv;
6. Die lineare Abbildung $\varphi_A : K^n \longrightarrow K^n$ ist injektiv;
7. Der Spaltenrang von A ist n;
8. Der Zeilenrang von A ist n;
9. A^t ist invertierbar.

Beweis (Proposition 2.8.33): Es sei K ein Körper, $n \in \mathbb{N}$ und $A \in K^{n\times n}$.

(1) $\Rightarrow$ (2): Die Aussage folgt mit $B = A^{-1}$.

(2) $\Rightarrow$ (3): Wegen $AB = E_n$ erzeugen die Spalten von A die kanonische Basis des K^n, sind damit also ein Erzeugendensystem.

Wären die Spalten von A nicht linear unabhängig, dann könnte man die Spalten auf ein Erzeugendensystem mit weniger als n Vektoren reduzieren, was jedoch

durch $\dim K^n = n$ ausgeschlossen wird. Also sind die Spalten von A linear unabhängig und es gilt

$$\mathrm{Ker}(A) = \{0\}.$$

Daraus schließt man

$$A(BA - E_n) = (AB)A - A = A - A = 0 \overset{\mathrm{Ker}(A)=\{0\}}{\Rightarrow} BA - E_n = 0,$$

womit $BA = E_n$.

(3) $\Rightarrow$ (4): Man betrachtet hierzu φ_B. Aus (3) kann man auf die gleiche Weise auf (2) schließen, wie man von (2) auf (3) geschlossen hat. Damit gilt für alle $x \in K^n$:

$$\begin{aligned}\varphi_B(\varphi_A(x)) &= \varphi_B(A \cdot x) = B \cdot (A \cdot x) = (B \cdot A) \cdot x = E_n \cdot x \\ &= (A \cdot B) \cdot x = \varphi_A(\varphi_B(x))\end{aligned}$$

Also $\varphi_B \circ \varphi_A = \varphi_A \circ \varphi_B = \mathrm{id}_{K^n}$, womit φ_A ein Isomorphismus ist.

(4) $\Rightarrow$ (5) Da Isomorphismen bijektiv sind, ist φ_A insbesondere surjektiv.

(5) $\Rightarrow$ (6) Wegen der Dimensionsformel für lineare Abbildungen gilt

$$\dim \mathrm{Ker}\, \varphi_A = \dim K^n - \dim \mathrm{Im}\, \varphi_A \overset{\varphi_A \text{ surj.}}{=} n - n = 0,$$

womit $\mathrm{Ker}\, \varphi_A = \{0\}$ und φ_A schließlich injektiv ist.

(6) $\Rightarrow$ (7) Es gilt

$$\mathrm{Im}\, \varphi_A = \langle (A_{\bullet,i})_{1 \le i \le n} \rangle$$

aufgrund der Definition der Matrix-Vektor Multiplikation. Damit gilt aber wegen der Dimensionsformel

$$\begin{aligned}\dim \langle (A_{\bullet,i})_{1 \le i \le n} \rangle = \dim \mathrm{Im}\, \varphi_A &= \dim K^n - \dim \mathrm{Ker}\, \varphi_A \\ \overset{\varphi_A \text{ injektiv}}{=} \quad & n - 0 = n.\end{aligned}$$

Also ist der Spaltenrang von A gleich n.

(7) $\Rightarrow$ (8) Da die Spalten von A linear unabhängig sind, gibt es eine Reihe elementarer Operationen, die sich so in einer invertierbaren Matrix $G \in \mathrm{GL}_n(K)$ zusammenfassen lassen, dass

$$E_n = A \cdot G$$

gilt, womit

$$E_n = G^t \cdot A^t.$$

G^t ist schließlich invertierbar wegen

$$G^t \cdot (G^{-1})^t = (G^{-1} \cdot G)^t = E_n^t = E_n,$$

also

$$E_n = G^t \cdot E^t \Leftrightarrow \left(G^t\right)^{-1} = A^t \Leftrightarrow E_n = A^t \cdot \left(G^t\right).$$

Aus der letzten Gleichung folgt jedoch, dass die Spalten von A^t linear unabhängig sind, womit die Zeilen von A linear unabhängig sind und A den Zeilenrang n hat.

(8) $\Rightarrow$ (9) Wenn der Zeilenrang von A gleich n ist, dann ist der Spaltenrang von A^t ebenfalls gleich n. Also sind die Spalten von A^t linear unabhängig, was mit Gauß für ein $G \in \mathrm{GL}_n(K)$ zu

$$E_n = G \cdot A^t$$

führt, womit A^t invertierbar ist.

(9) $\Rightarrow$ (1) Wenn A^t invertierbar ist, dann gilt

$$((A^t)^{-1})^t \cdot A = (A^t \cdot (A^t)^{-1})^t = E_n^t = E_n.$$

Also ist A invertierbar.

□

Proposition 2.8.34

Der Spaltenrang von äquivalenten Matrizen ist gleich, ebenso der Zeilenrang.

Beweis (Proposition 2.8.34): Sei $A = S \cdot B \cdot T^{-1}$ für $A, B \in K^{m\times n}$, $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$. Nach Definition des Spaltenranges ist zu zeigen, dass

$$\dim \mathrm{Im}(\varphi_A) = \dim \mathrm{Im}(\varphi_B)$$

gilt. Man beobachtet

$$\begin{aligned}\dim \mathrm{Im}(\varphi_A) &= \dim \mathrm{Im}(\varphi_{SBT^{-1}}) = \dim \mathrm{Im}(\varphi_S \circ \varphi_B \circ \varphi_{T^{-1}}) \\ &= \dim \varphi_S(\varphi_B(\varphi_{T^{-1}}(K^n))) \overset{\varphi_{T^{-1}} \text{ Iso.}}{=} \dim \varphi_S(\varphi_B(K^n)) \\ &\overset{\varphi_S \text{ Iso.}}{=} \dim \varphi_B(K^n) = \dim \mathrm{Im}(\varphi_B).\end{aligned}$$

Also ist der Spaltenrang gleich. Es gilt

$$A^t = (SBT^{-1})^t = (T^t)^{-1} B^t ((S^t)^{-1})^{-1},$$

womit A^t und B^t äquivalent sind. Nach Obigem haben A^t und B^t den gleichen Spaltenrang und damit A und B den gleichen Zeilenrang. □

Proposition 2.8.35

Es sei $A \in K^{m\times n}$, dann ist $\mathcal{L}(A \mid 0) = \ker \varphi_A$ und

$$\dim \mathcal{L}(A \mid 0) = n - \mathrm{Rang}\ \varphi_A.$$

Damit ist

$$\mathcal{L}(A \mid 0) = \{0\} \Leftrightarrow \text{Spaltenrang } A = n.$$

Beweis (Proposition 2.8.35): Sei $A \in K^{m\times n}$. Es gilt für alle $x \in K^n$:

$$x \in \mathrm{Ker}\, \varphi_A \Leftrightarrow A \cdot x = 0 \Leftrightarrow x \in \mathcal{L}(A \mid 0)$$

Damit gilt nach der Dimensionsformel für lineare Abbildungen

$$\begin{aligned}\dim \mathcal{L}(A \mid 0) &= \dim \mathrm{Ker}(\varphi_A) = \dim K^n - \dim \mathrm{Im}(\varphi_A) \\ &= n - \mathrm{Rg}\ \varphi_A.\end{aligned}$$

Die Äquivalenz ist eine direkte Folgerung. □

Proposition 2.8.36

Für das lineare Gleichungssystem $Ax = b$ mit $A \in K^{m\times n}$ und $b \in K^m$ sind äquivalent:

1. Es gibt mindestens eine Lösung.
2. Der Spaltenrang von $(A \mid b)$ ist der Spaltenrang von A.
3. b ist im Bild von φ_A.

Beweis (Proposition 2.8.36): Seien $A \in K^{m\times n}$ und $b \in K^m$ beliebig, aber fest.

(1) $\Rightarrow$ (2): Es sei $x \in K^n$ mit $Ax = b$. Damit gilt

$$\sum_{i=1}^{n} x_i \cdot A_{\bullet,i} = Ax = b.$$

b ist also eine Linearkombination der Spalten von A und somit bereits im Spann der Spalten von A enthalten und verändert somit nicht die Dimension.

(2) $\Rightarrow$ (3): Es gilt $\operatorname{Rg}(A|b) = \operatorname{Rg}(A)$. Der Vektor b ist linear abhängig von den Spalten von A. Also ist $b \in \operatorname{Im}\varphi_A$.

(3) $\Rightarrow$ (1): Es gilt $b \in \operatorname{Im}\varphi_A$. Also gibt es ein $x \in K^n$, sodass $A \cdot x = \varphi_A(x) = b$, womit das LGS eine Lösung hat.

□

Korollar 2.8.37

Für $A \in K^{m\times n}$ sind folgende Aussagen äquivalent:

1. Für jedes $b \in K^m$ hat $Ax = b$ eine Lösung.
2. Der Spaltenrang von A ist m.
3. φ_A ist surjektiv.

Beweis (Korollar 2.8.37): Sei $A \in K^{m\times n}$ eine beliebige, aber feste Matrix.

(1) $\Rightarrow$ (2): Sei $B \subset K^m$ eine Basis, dann ist B insbesondere ein Erzeugendensystem. Da für alle $b \in B : \exists\, x \in K^n : Ax = b$, erzeugen die Spalten von A ein Erzeugendensystem vom K^m. Damit sind die Spalten von A selbst ein Erzeugendensystem und der Spaltenrang ist $\dim K^m = m$.

(2) $\Rightarrow$ (1): Dadurch, dass der Spaltenrang von A gleich m ist, erzeugen die Spalten von A den K^m. Damit gibt es für alle $b \in K^m$ Koeffizienten $x_1, \ldots, x_n \in K$, sodass

$$b = \sum_{i=1}^{n} x_i \cdot A_{\bullet,i} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \varphi_A\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right).$$

Damit ist φ_A surjektiv.

(3) $\Rightarrow$ (1) Da φ_A surjektiv ist, gilt für alle $b \in K^m$, dass ein $x \in K^n$ existiert, sodass

$$b = \varphi_A(x) = A \cdot x,$$

womit das LGS $Ax = b$ eine Lösung hat.

□

Korollar 2.8.38

Folgende Aussagen sind äquivalent für $A \in K^{n \times n}$:

1. A ist invertierbar.
2. Für jedes $b \in K^n$ hat $Ax = b$ eine Lösung.
3. Für jedes $b \in K^n$ hat $Ax = b$ genau eine Lösung.

Wenn (3) erfüllt ist, so ist $x = A^{-1} \cdot b$.

Beweis (Korollar 2.8.38): Sei $A \in K^{n \times n}$ beliebig, aber fest.

(1) $\Rightarrow$ (2): Sei $b \in K^n$ beliebig, aber fest. Dann ist $x := A^{-1}b \in K^n$. Man sieht, dass

$$A \cdot x = A \cdot (A^{-1} \cdot b) = (A \cdot A^{-1}) \cdot b = E_n \cdot b = b$$

ergibt, womit das LGS eine Lösung hat.

(2) $\Rightarrow$ (3): Nach Korollar 2.8.37 ist φ_A surjektiv, was mit der Dimensionsformel

$$\dim \operatorname{Ker} \varphi_A = \dim K^n - \dim \operatorname{Im} \varphi_A = n - n = 0$$

ergibt. Also besteht der Kern nur aus der Null. Sei $b \in K^n$ beliebig, aber fest. Seien $x, x' \in K^n$ zwei Lösungen des LGS. Dann gilt

$$0 = b - b = Ax - Ax' = A(x - x') \quad \Rightarrow \quad x - x' \in \operatorname{Ker} \varphi_A = \{0\}.$$

Also ist $x = x'$ und die Lösung des LGS eindeutig.

(3) $\Rightarrow$ (1) Da $Ax = b$ für alle $b \in K^n$ genau eine Lösung hat, existieren insbesondere Lösungen für $b = e_1, \ldots, e_n$. Damit existieren aber die Spalten der Inversen und damit die Inverse selbst.

□

Bemerkung 2.8.39

Bestimmung des Lösungsraums eines homogenen LGS? Einmal mehr der Gauß-algorithmus.

Was bringen uns die obigen Aussagen für das Lösen von linearen Gleichungssystemen? Wir können nun unter günstigen Umständen, ohne den ganzen Gauß-Algorithmus durchzuführen, Aussagen über die Lösbarkeit treffen. Zur Bestimmung des Lösungsraum muss jedoch weiterhin der Gauß-Algorithmus verwendet werden, insbesondere, um die Inverse zu gewinnen, falls diese existiert.

Theorem 2.8.40

Es sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, $\dim V = n < \infty$, $\dim W = m < \infty$. Dann existieren B, eine Basis von V, und C, eine Basis von W, sodass

$$ {}^{C}A_{\varphi}^{B} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in K^{m \times n}, $$

wobei $r = \dim \varphi(V) = \operatorname{Rang} \varphi$. Insbesondere ist jede Matrix äquivalent zu genau so einer Matrix, also zwei Matrizen sind äquivalent genau dann, wenn sie den gleichen Spaltenrang haben.

Beweis. Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung mit $\dim V = n$, $\dim W = m$ und $m, n < \infty$.

Man setzt $r = \dim \operatorname{Im} \varphi$ und wählt eine Basis $C = (c_1, \ldots, c_n)$ von $\operatorname{Im} \varphi$. Als nächstes wählt man für alle $1 \leq i \leq r$ ein Element aus $\varphi^{-1}(\{c_i\})$ und definiert dieses als b_i.

Die $b_1, \ldots, b_n$ sind linear unabhängig, denn für alle $\lambda_1, \ldots, \lambda_r$, die

$$ \sum_{i=1}^{r} \lambda_i b_i = 0 $$

erfüllen, gilt, dass

$$ 0 = \varphi(\sum_{i=1}^{r} \lambda_i b_i) = \sum_{i=1}^{r} \lambda_i \varphi(b_i) = \sum_{i=1}^{r} \lambda_i c_i \overset{C \text{ Basis}}{\Rightarrow} \lambda_1 = \cdots = \lambda_r = 0. $$

Damit gilt insbesondere, dass $\langle b_1, \ldots, b_r \rangle \cap \operatorname{Ker} \varphi = \{0\}$.

Sei nun $(b_{r+1}, \ldots, b_n)$ eine Basis von $\operatorname{Ker} \varphi$. Man setzt $B = (b_1, \ldots, b_n)$ und ergänzt C mit $c_{r+1}, \ldots, c_m$ zu einer Basis von W. Da $\langle b_1, \ldots, b_r \rangle \cap \operatorname{Ker} \varphi = \{0\}$, $\dim \langle b_1, \ldots, b_r \rangle = r$ und $\dim \operatorname{Ker} \varphi = n - r$, ist $V = \langle b_1, \ldots, b_r \rangle \oplus \operatorname{Ker} \varphi$. Somit ist B eine Basis von V. Also gilt

$$ \begin{cases} \varphi(b_i) = c_i, & \text{für alle } 1 \leq i \leq r \\ \varphi(b_i) = 0, & \text{für alle } r+1 \leq i \leq n \end{cases} \Rightarrow \begin{cases} (\varphi(b_i))_C = e_i, & \text{für alle } 1 \leq i \leq r \\ (\varphi(b_i))_C = 0, & \text{für alle } r+1 \leq i \leq n \end{cases}, $$

womit

$$ {}^{C}A_{\varphi}^{B} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}. $$

Also ist der erste Teil der Aussage gezeigt.

Sei $A \in K^{m \times n}$ beliebig, dann ist φ_A eine lineare Abbildung und es existieren Basen B', C' von K^n bzw. K^m, sodass

$$ {}^{C'}A_{\varphi}^{B'} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, $$

wobei $r = \dim \operatorname{Im} \varphi_A = \operatorname{SRg} A$. Wählt man B, C als die Standardbasen vom K^n bzw. K^m, dann gilt

$$ A = {}^{C}A_{\varphi_A}^{B} = {}^{C}\mathrm{id}^{C'} \, {}^{C'}A_{\varphi_A}^{B'} \, {}^{B'}\mathrm{id}^{B} = {}^{C}\mathrm{id}^{C'} \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} {}^{B'}\mathrm{id}^{B}. $$

Da ${}^{B'}\mathrm{id}^{B} \in \mathrm{GL}_n(K)$ und ${}^{C}\mathrm{id}^{C'} \in \mathrm{GL}_m(K)$, ist A äquivalent zu

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Der Rest folgt mit der Transitivität der Äquivalenzrelation. □

Lemma 2.8.41

Für jedes $A \in K^{m\times n}$ ist der Spaltenrang gleich dem Zeilenrang.

Beweis (Lemma 2.8.7). Sei $AK^{m\times n}$ beliebig, aber fest. Man setzt $r := \mathrm{SRg}\ A$. Nach Theorem 2.8.40, gibt es $S \in \mathrm{GL}_m(K), T \in \mathrm{GL}_n(K)$, sodass

$$SAT^{-1} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Dann

$$T^{-t}A^t(S^{-t})^{-1} = (SAT^{-1})^t = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}^t = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Der Spaltenrang von A^t ist also r und da der Spaltenrang von A^t der Zeilenrang von A ist, sind Spaltenrang und Zeilenrang von A identisch. □

Wir können nun endlich zeigen, dass der Spaltenrang und der Zeilenrang identisch sind. Damit macht es auch Sinn, von *dem* Rang einer Matrix bzw. Abbildung zu sprechen.

2.9 Determinanten

Wir werden uns in diesem Kapitel mit Determinanten beschäftigen und diese als wichtiges Werkzeug bei der Untersuchung linearer Abbildungen nutzen. Interessanterweise können wir die Determinante auf der einen Seite durch Formeln beschreiben aber auf der anderen Seite auch durch Eigenschaften

Hier wäre ein kurzer Blick in das Kapitel über Gruppen sinnvoll, lesen Sie nochmal alles zur symmetrischen Gruppe durch.

Im weiteren betrachten wir kommutative Ringe mit 1. Das mag mit Hinblick auf lineare Abbildungen ungewöhnlich sein, da wir bisher dort immer Körper betrachtet haben, aber Determinanten für Polynomringe werden in der Zukunft eine erhebliche Rolle spielen.

2.9.1 Leibniz-Regel

Definition 2.9.1

Es sei R ein kommutativer Ring mit 1 ist. Dann ist die **Determinante** die Abbildung $\det : R^{n\times n} \longrightarrow R$ definiert durch

$$A = (a_{i,j}) \mapsto \det A = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Die Formel aus der Definition wird auch **Leibniz-Formel**enannt. In dieser wird über die Elemente der n-ten symmetrischen Gruppe S_n alternierend (mit Hilfe des Signum) summiert. Seien nun R,n und A wie in 2.9.1. Die Determinante von A ergibt sich also, indem man damit beginnt, alle Kombinationen aufzuschreiben, in denen aus jeder Zeile genau ein Element ausgewählt wird. Man bildet dann innerhalb der Kombinationen die entsprechenden Produkte und multipliziert das Signum der Auswahl an das Produkt heran. Alle so gewonnenen Ergebnisse werden aufaddiert und man erhält die Determinante.

Beispiel 2.9.2

1.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$\begin{aligned} \det(A) &= \sum_{\sigma\in S_2} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \\ &= \operatorname{sgn}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \cdot a_{1,1} \cdot a_{2,2} + \operatorname{sgn}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot a_{1,2} \cdot a_{2,1} \\ &= 1 \cdot a_{1,1} \cdot a_{2,2} + (-1) \cdot a_{1,2} \cdot a_{2,1} \\ &= 1 \cdot 4 - 2 \cdot 3 = 4 - 6 \\ &= -2 \end{aligned}$$

2.

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

$$\begin{aligned} \det(A) &= a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} \\ &\quad - a_{3,1}a_{2,2}a_{1,3} - a_{3,2}a_{2,3}a_{1,1} - a_{3,3}a_{2,1}a_{1,2} \\ &= 2 + 2 + 0 - (-2) - 1 - 0 = 5 \end{aligned}$$

Im letzten Beispiel haben wir bereits eine Regel für die Bestimmung der Determinante angewendet, nämlich die sogenannte ***Regel von Sarrus***. Diese soll es bequemer machen 3×3 Matrizen zu berechnen.

Algorithmus 2.9.3

Die ***Regel von Sarrus*** gilt nur für $3x3$ Matrizen und lautet wie folgt: Sei

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix},$$

dann berechnet sich die Determinante nach dem Schema:

$$\left(\begin{array}{ccc|cc} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,1} & a_{3,2} \end{array} \right)$$

Also

$$\begin{aligned} \det(A) &= a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} \\ &\quad - a_{3,1}a_{2,2}a_{1,3} - a_{3,2}a_{2,3}a_{1,1} - a_{3,3}a_{2,1}a_{1,2}. \end{aligned}$$

Beispiel 2.9.4

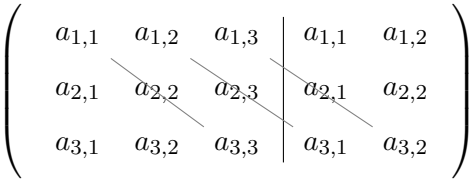
Etwas ausführlicher gestaltet sich die Regel für eine gegebene Matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

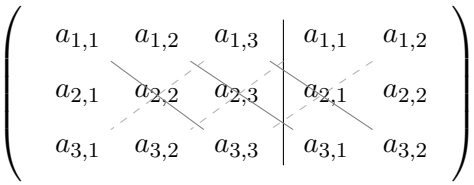
wie folgt. Man erweitert diese auf der rechten Seite mit den ersten beiden Spalten zu

$$\left(\begin{array}{ccc|cc} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,1} & a_{3,2} \end{array}\right)$$

und multipliziert die Elemente auf den von links oben nach rechts unten gehenden Diagonalen und addiert die Produkte.



Danach wiederholt man den selben Prozess mit den von links unten nach rechts oben gehenden Diagonalen.



Man subtrahiert die zweite Summe von der ersten Summe. Es ergibt sich die folgende Formel:

$$\begin{aligned} \det(A) = {} & a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} \\ & - a_{3,1}a_{2,2}a_{1,3} - a_{3,2}a_{2,3}a_{1,1} - a_{3,3}a_{2,1}a_{1,2}. \end{aligned}$$

Um diese Formel zu beweisen, muss man lediglich die Leibnizformel für $n = 3$ ausschreiben und die Kommutativität in R nutzen.

Wie Sie gesehen haben, ist bereits die Berechnung der Determinanten von 3×3 Matrizen aufwändig. Für Matrizen höherer Dimension steigt der Rechenaufwand über die Leibnizformel nochmals stark an. Schließlich hat man $n!$ Summanden mit jeweils $(n-1)$ Produkten.

Abgesehen davon erweist sich die Struktur der Leibnizformel für allgemeine Beweise als unhandlich. Deshalb zeigen wir im Folgenden einige Eigenschaften der Determinante, sodass wir eben diese Eigenschaften in weiteren Beweisen verwenden können anstelle der Formel selbst.

Proposition 2.9.5

Für alle $A \in R^{n\times n}$ gilt: $\det A = \det A^T$.

Beweis. Sei $n \in \mathbb{N}$, R ein kommutativer Ring mit 1 und $A \in R^{n\times n}$. Sei nun $\sigma \in S_n$ beliebig.

Hat σ keine Fehlstellungen, so ist $\sigma = \mathrm{id} = \mathrm{id}^{-1} = \sigma^{-1}$. Für alle anderen σ gibt es also mindestens eine Fehlstellung und diese betrachtet man nun.

Seien nun $i < j \in \{1, ..., n\}$ mit $\sigma(i) > \sigma(j)$. Also ist $\sigma(j) < \sigma(i) \in \{1, ..., n\}$ und damit $\sigma^{-1}(\sigma(j)) = j > i = \sigma^{-1}(\sigma(i))$. Das bedeutet, dass eine Fehlstellung in σ eine Fehlstellung in σ^{-1} impliziert und umgekehrt.

Daraus ergibt sich, dass die Anzahl der Fehlstellungen für σ und σ^{-1} gleich groß ist, womit:

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1}).$$

Außerdem ist

$$a_{1,\sigma^{-1}(1)} \cdot \ldots \cdot a_{n,\sigma^{-1}(n)} = a_{\sigma(1),1} \cdot \ldots \cdot a_{\sigma(n),n}.$$

Da σ beliebig war, gilt:

$$\begin{aligned}
\det\left(A^T\right) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left((A^T)_{1,\sigma(1)} \cdot \ldots \cdot (A^T)_{n,\sigma(n)} \right) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \cdot \ldots \cdot a_{\sigma(n),n} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{\sigma(1),1} \cdot \ldots \cdot a_{\sigma(n),n} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{1,\sigma^{-1}(1)} \cdot \ldots \cdot a_{n,\sigma^{-1}(n)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} = \det(A)
\end{aligned}$$

Die vorletzte Gleichheit gilt, da für alle $\sigma \in S_n$ auch $\sigma^{-1} \in S_n$ und man somit in der Summe den σ^{-1}-Term an die Stelle des σ-Terms stellen kann und umgekehrt.

□

2.9.2 Charakterisierung der Determinante

Bevor wir uns der versprochenen Charakterisierung der Determinante zuwenden können, welche in Satz 2.9.12 gegeben wird, müssen wir noch zwei Begriffe einführen.

Definition 2.9.6

Sei R ein kommutativer Ring und V, W seien R-Moduln (Sie können hier an Körper und Vektorräume denken). Eine Abbildung $\varphi : V \times \cdots \times V \to W$ heißt R-multilinear genau dann, wenn φ auf jedem V linear ist. D.h. $\forall (v_1, \cdots, v_n) \in V \times \cdots \times V :$ für alle $u \in V :$ für alle $\lambda \in R :$ für alle $1 \leq i \leq n :$

$$\begin{aligned}
&\varphi((v_1, \cdots, v_{i-1}, \lambda \cdot v_i + u, v_{i+1}, \cdots, v_n)) = \\
&\qquad \lambda \cdot \varphi((v_1, \cdots, v_{i-1}, v_i, v_{i+1}, \cdots, v_n)) + \varphi((v_1, \cdots, v_{i-1}, u, v_{i+1}, \cdots, v_n))
\end{aligned}$$

Definition 2.9.7

Sei φ mit den Voraussetzungen aus 2.9.6. Die Abbildung φ heißt alternierend genau dann, wenn φ auf jedem n-Tupel mit mindestens zwei gleichen Einträgen null ist.

Proposition 2.9.8

Sei φ wie in 2.9.6, K ein Körper mit $1+1 \neq 0$ und φ multilinear. Dann ist φ genau dann alternierend, wenn für jedes n-Tupel $A \in V^n$ gilt, dass $\varphi(A) = -\varphi(A')$ wenn A' durch Vertauschung zweier Komponenten aus A entsteht.

Beweis. Es reicht die Proposition für $n = 2$ zu betrachten, da wegen der Multilinearität nur auf den beiden vertauschten Einträgen operiert werden muss.

Seien $v, w \in V$, V und W K-Vektorräume und $\varphi : V \times V \to W$ eine multilineare Abbildung, dann gilt:

$$\begin{aligned}\varphi(v+w, v+w) = 0 \overset{\varphi \text{ multilin.}}{\Leftrightarrow} \varphi(v,v) + \varphi(v,w) + \varphi(w,v) + \varphi(w,w) = 0 \\ \Leftrightarrow \varphi(v,w) + \varphi(w,v) = 0 \Leftrightarrow \varphi(v,w) = -\varphi(w,v),\end{aligned}$$

wobei sich die mittlere Äquivalenz aus der Definition ergibt: Ist φ alternierend, dann gilt:

$$\varphi(v,v) = \varphi(w,w) = 0.$$

Umgekehrt gilt nach Voraussetzung

$$\varphi(v,v) = -\varphi(v,v),$$

womit

$$0 = (1+1) \cdot \varphi(v,v).$$

Da $1 + 1 \neq 0$ und Körper nullteilerfrei sind, gilt $\varphi(v,v) = 0$. □

Wir beachten, dass die eine Implikation auch für beliebige Ringe gilt, alternierend impliziert ein Multiplikation mit -1 bei Vertauschung zweier Komponenten.

Beispiel 2.9.9

Sei K ein Körper und $V = K^2$. Dann ist die Abbildung

$$\begin{aligned}\varphi : V \times V &\to K \\ (v,w) &\mapsto v_1 \cdot w_2\end{aligned}$$

multilinear. Seien $v, w, u \in V$ und $\lambda \in K$:

$$\varphi(v, \lambda w + u) = v_1 \cdot (\lambda w_2 + u_2) = \lambda \cdot v_1 \cdot w_2 + v_1 \cdot u_2 = \lambda\varphi(v,w) + \varphi(v,u)$$

Man kann analog im 1. Argument vorgehen.

Es ist sehr wichtig zu verstehen, dass multilinear etwas anderes ist als linear. Multilinearität ist Linearität in jedem einzelnen Argument, aber nicht zusammen für alle Argumente.

Beispiel 2.9.10

Wir wählen φ wie oben. Wäre φ linear, dann könnte man für $v, w, u, p \in V$ folgendes tun:

$$\varphi(v+w, u+p) = \varphi(v,u) + \varphi(w,p).$$

Da φ aber multilinear ist, gilt:

$$\varphi(v+w, u+p) = \varphi(v,u) + \varphi(v,p) + \varphi(w,u) + \varphi(w,p)$$

Im Allgemeinen ist aber

$$\varphi(v,u) + \varphi(w,p) \neq \varphi(v,u) + \varphi(v,p) + \varphi(w,u) + \varphi(w,p).$$

Beispiel 2.9.11

Ein Beispiel für eine Abbildung, die nicht multilinear ist, ist:

$$\begin{aligned} \varphi : V \times V &\to V \\ (v,w) &\mapsto v - w \end{aligned}$$

betrachten. Es sollte offensichtlich sein, dass für alle $v \in V$ gilt, dass $\varphi(v,v) = 0$.

Nun kann die Determinante mit den soeben gewonnenen Begriffen charakterisiert werden.

Satz 2.9.12

Sei K ein Körper. Dann gibt es genau eine Abbildung $f : K^{n\times n} \longrightarrow K$, für die gilt:

1. f ist multilinear, und
2. f ist alternierend, und
3. $f(E_n) = 1$.

Diese Abbildung ist die Determinante.

Beweis. Sei R ein kommutativer Ring mit 1 und $n \in \mathbb{N}$. Wir interpretieren hier die Determinante als eine Abbildung $\det(R^n)^n \longrightarrow R$. Also fassen wir eine $n \times n$ Matrix als ein n-Tupel von n Spaltenvektoren auf.

1. Man beginnt damit zu zeigen, dass die Determinante tatsächlich multilinear und alternierend ist und außerdem $\det(E_n) = 1$ gilt.

a) Normiertheit: Es ist $E_n = (e_1, \cdots, e_n)$. Daraus folgt aber, dass

$$\begin{aligned}
\det(E_n) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)(E_n)_{1,\sigma(1)} \cdot \ldots \cdot (E_n)_{n,\sigma(n)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\delta_{1,\sigma(1)} \cdot \ldots \cdot \delta_{n,\sigma(n)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \begin{cases} 1 & , \text{ für alle } 1 \leq i \leq n : \delta_{i,\sigma(i)} = 1 \\ 0 & , \text{sonst} \end{cases} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \begin{cases} 1 & , \text{ für alle } 1 \leq i \leq n : i = \sigma(i) \\ 0 & , \text{sonst} \end{cases} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \begin{cases} 1 & , \sigma = \mathrm{id} \\ 0 & , \text{sonst} \end{cases} \\
&= \operatorname{sgn}(\mathrm{id}) = 1.
\end{aligned}$$

b) Alternierend: Sei A' eine Matrix, die durch Tauschen der i-ten und j-ten Spalte in $A = (a_{\bullet,1}, \cdots, a_{\bullet,n})$ entstanden ist, dann gilt $A' = \left(a_{\bullet,\tau(1)}, \cdots, a_{\bullet,\tau(n)}\right)$ für $\tau \in S_n$ mit $\tau(i) = j, \tau(j) = i$ und für alle $k \neq i, j : \tau(k) = k$. Damit ist

$$\begin{aligned}
\det\left(A'\right) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left((A')_{1,\sigma(1)} \cdot \ldots \cdot (A')_{n,\sigma(n)}\right) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left((A)_{\tau(1),\sigma(1)} \cdot \ldots \cdot (A)_{\tau(n),\sigma(n)}\right) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left((A)_{1,\sigma(\tau^{-1}(1))} \cdot \ldots \cdot (A)_{n,\sigma(\tau^{-1}(n))}\right) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma \circ \tau^{-1} \circ \tau) \left((A)_{1,\sigma(\tau^{-1}(1))} \cdot \ldots \cdot (A)_{n,\sigma(\tau^{-1}(n))}\right) \\
&\overset{\sigma' = \sigma \circ \tau^{-1}}{=} \sum_{\sigma' \in S_n} \operatorname{sgn}(\sigma' \circ \tau) \left((A)_{1,\sigma'(1)} \cdot \ldots \cdot (A)_{n,\sigma'(n)}\right) \\
&= \operatorname{sgn}(\tau) \sum_{\sigma' \in S_n} \operatorname{sgn}(\sigma') \left((A)_{1,\sigma'(1)} \cdot \ldots \cdot (A)_{n,\sigma'(n)}\right) \\
&= \operatorname{sgn}(\tau) \cdot \det(A).
\end{aligned}$$

c) Multilinearität: Seien $A \in R^{n \times n}$,$\lambda \in R$, $w \in R^n$ und $j \in \{1, \ldots, n\}$. Man definiert $A' \in R^{n \times n}$ durch für alle $i \neq j : (A')_{\bullet,i} := a_{\bullet,i}$ und $(A')_{\bullet,j} := \lambda \cdot a_{\bullet,j} + w$.

$$
\begin{aligned}
\det\big(A'\big) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (A')_{i,\sigma(i)} \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) (A')_{j,\sigma(j)} \prod_{\substack{i=1,\\ i\neq j}}^{n} (A')_{i,\sigma(i)} \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) (\lambda \cdot a_{j,\sigma(j)} + w_{\sigma(j)}) \prod_{\substack{i=1,\\ i\neq j}}^{n} (A')_{i,\sigma(i)} \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) (\lambda \cdot a_{j,\sigma(j)} + w_{\sigma(j)}) \prod_{\substack{i=1,\\ i\neq j}}^{n} a_{i,\sigma(i)} \\
&= \lambda \cdot \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} + \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) w_{\sigma(j)} \prod_{i=1}^{n} a_{i,\sigma(i)} \\
&= \lambda \cdot \det(A) + \det((a_{\bullet,1}, \cdots, a_{\bullet,i-1}, w, a_{\bullet,i+1}, \cdots, a_{\bullet,n}))
\end{aligned}
$$

2. Eindeutigkeit: Sei $\varphi : (R^n)^n \to R$ eine multilineare, alternierende normierte Abbildung. Dann ist

$$
\begin{aligned}
\varphi(A) &= \sum_{j=1}^{n} a_{j,1} \varphi(e_j, A_{\bullet,2,}, \ldots, A_{\bullet,n}) \\
\text{multilinear} &= \sum_{j_1,\ldots,j_n=1}^{n} a_{j_1,1} \cdots a_{j_n,n} \varphi(e_{j_1}, \ldots, e_{j_n}) \\
\text{alternierend} &= \sum_{\sigma\in S_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \varphi(e_{j_1}, \ldots, e_{j_n}) \\
\text{alternierend} &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} \varphi(e_1, \ldots, e_n) \\
&= \det A.
\end{aligned}
$$

□

2.9.3 Multiplikationssatz

Satz 2.9.13

Es sei R ein kommutativer Ring und $A, B \in R^{n\times n}$, dann gilt

$$\det(A \cdot B) = \det A \cdot \det B.$$

Beweis. Seien $n \in \mathbb{N}$, R ein kommutativer Ring und $A, B \in R^{n\times n}$. Wir erinnern uns

$$S_n := \{\tau | \tau \text{ Abbildung von } \{1, \ldots, n\} \text{ nach } \{1, \ldots, n\}$$

und notieren für den Beweis noch $T_n = \{1, \ldots, n\}^{\{1,\ldots,n\}}$:

$$T_n := \{\tau | \tau \text{ Abbildung von } \{1, \ldots, n\} \text{ nach } \{1, \ldots, n\}\}.$$

Das n-fache Produkt von n-fachen Summen lässt sich auch als Summe von Produkten schreiben:
Es sei $C = (c_{i,j}) \in R^{n \times n}$:

$$\prod_{i=1}^{n} \sum_{j=1}^{n} c_{i,j} = \sum_{(p_1,\ldots,p_n) \in \{1,\ldots,n\}^n} \prod_{i=1}^{n} c_{i,p_i} = \sum_{\tau \in T_n} \prod_{i=1}^{n} c_{i,\tau(i)}$$

Der Beweis sei den geneigten Lesenden überlassen.

Man erhält:

$$\begin{aligned}
\det(A \cdot B) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (AB)_{i,\sigma(i)} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} \cdot b_{j,\sigma(i)} \\
&\overset{\text{s.o.}}{=} \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \sum_{\tau \in T_n} \prod_{i=1}^{n} a_{i,\tau(i)} \cdot b_{\tau(i),\sigma(i)} \\
&= \sum_{\sigma \in S_n, \tau \in T_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\tau(i)} \cdot b_{\tau(i),\sigma(i)} \\
&= \sum_{\tau \in T_n} \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \left(\prod_{i=1}^{n} b_{\tau(i),\sigma(i)} \right) \\
&= \sum_{\tau \in T_n} \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} b_{\tau(i),\sigma(i)} \right) \\
&= \sum_{\tau \in T_n} \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \det\left(b_{\tau(1)}, \cdots, b_{\tau(n)}\right) \\
&= \sum_{\tau \in T_n} \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \det(\tau(B))
\end{aligned}$$

Da die Determinante alternierend ist, gilt $\det(\tau(B)) = 0$ genau dann, wenn $\tau \notin S_n$:

$$\begin{aligned}
\det(A \cdot B) &= \sum_{\tau \in T_n} \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \det(\tau(B)) = \sum_{\tau \in S_n} \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \det(\tau(B)) \\
&\overset{\text{alt.}}{=} \sum_{\tau \in S_n} \left(\prod_{i=1}^{n} a_{i,\tau(i)} \right) \operatorname{sgn}(\tau) \det(B) = \det(B) \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \prod_{i=1}^{n} a_{i,\tau(i)} \\
&= \det(A) \cdot \det(B)
\end{aligned}$$

□

Es ist wichtig anzumerken, dass es für die Determinante zwar einen Multiplikationssatz, aber keinen Additionssatz gibt. Man findet für die Addition ein einfaches Gegenbeispiel:

$$1 = \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \neq \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) + \det\left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) = 0 + 0 = 0$$

Eine andere Formulierung für den Multiplikationssatz lautet:

Proposition 2.9.14

Die Abbildung $\det : \mathrm{GL}_n(R) \longrightarrow R^\times$ ist ein Gruppenhomomorphismus.

Wir erhalten damit insbesondere, dass für alle $A \in \mathrm{GL}_n(R)$:

$$\det A^{-1} = (\det A)^{-1}.$$

Die folgende Aussage hätten wir schon aus den definierenden Eigenschaften ableiten können, aber mit Hilfe des Multiplikationssatzes können wir die elegant beweisen. Erinnern Sie sich an die Zeilenoperationen des Gauss-Algorithmus und wie wir diese durch Linksmultiplikation mit Elementarmatrizen darstellen konnten.

Proposition 2.9.15

Es sei R ein kommutativer Ring und $A \in^{n\times n}$. Es seien $i \neq j$ und $\lambda \in R$ gegeben, dann gilt:

1. $\det E^{i,j} A = -\det A$.
2. $\det E^{\lambda,i} A = \lambda \det A$.
3. $\det E^{\lambda,i,j} A = \det A$.

Beweis. Folgt direkt aus dem Multiplikationssatz. □

Wir können also den Gauss-Algorithmus verwenden um A auf eine "einfachere" Gestalt zu bringen und müssen dabei nur darauf achten, dass die Determinante sich entsprechend ändert.

Satz 2.9.16

Für einen Körper K und $A \in K^{n\times n}$ gilt:

$$A \text{ ist invertierbar in } K^{n\times n} \Leftrightarrow \det A \text{ ist invertierbar in } K.$$

Beweis. Es sei $A \in K^{n\times n}$.

- " $\Rightarrow$": Sei A invertierbar. Es gilt per Definition $A \cdot A^{-1} = E_n$, womit

  $$1 = \det(E_n) = \det\big(A \cdot A^{-1}\big) \overset{\text{Satz } 2.9.13}{=} \det(A) \cdot \det\big(A^{-1}\big)$$

  Dann gilt $\det(A) \in K^\times$, also invertierbar.

- " $\Leftarrow$": Angenommen A ist nicht invertierbar. Dann ist insbesondere A nicht surjektiv, also sind die Spalten von A nicht linear unabhängig.

  Wenn nun aber die Spalten linear abhängig sind, dann ist mindestens eine Spalte eine Linearkombination aus den anderen Spalten. Formal ausgedrückt:

  $$\exists\, 1 \leq i \leq n : \exists\, \lambda_j, j \neq i : A_{\bullet,i} = \sum_{j=1, j\neq i}^{n} \lambda_j A_{\bullet,j}.$$

Mit dieser Identität folgert man:

$$\begin{aligned}
\det(A) &= \det(A_{\bullet,1}, \cdots, A_{\bullet,i-1}, \quad A_{\bullet,i}, \quad A_{\bullet,i+1}, \cdots, A_{\bullet,n}) \\
&= \det\left(A_{\bullet,1}, \cdots, A_{\bullet,i-1}, \quad \sum_{j=1,j\neq i}^{n} \lambda_j A_{\bullet,j}, \quad A_{\bullet,i+1}, \cdots, A_{\bullet,n}\right) \\
&\overset{\text{mul.}}{=} \sum_{j=1,j\neq i}^{n} \lambda_j \det(A_{\bullet,1}, \cdots, A_{\bullet,i-1}, \quad A_{\bullet,j}, \quad A_{\bullet,i+1}, \cdots, A_{\bullet,n}) \\
&\overset{\text{alt.}}{=} \sum_{j=1,j\neq i}^{n} 0 = 0
\end{aligned}$$

□

Tatsächlich sehen wir sehr schnell, dass die Implikation $\Rightarrow$ auch für kommutative Ringe mit 1 gilt. Überlegen Sie sich, ob auch $\Rightarrow$ für kommutative Ringe mit 1 gilt; der oben stehende Beweis würde nicht ausreichen.

2.9.4 Determinante einer Abbildung

Definition 2.9.17

Es sei $\varphi : V \longrightarrow V$ eine lineare Abbildung zwischen K-Vektorräumen und B eine Basis von V ($\dim V < \infty$). Dann definieren wir die Determinante von φ als

$$\det \varphi := \det({}^{B}A_{\varphi}^{B}).$$

Bemerkung 2.9.18

Das ist wohldefiniert und unabhängig von der Wahl einer Basis

Wohldefiniertheit (Definition 2.9.17): Seien die Bezeichnungen wie in der Definition.

Um die Wohldefiniertheit von $\det(\varphi)$ zu sichern, muss Unabhängigkeit von der gewählten Basis nachgewiesen werden. Seien also B und C Basen von V.

Wir wissen über die Basiswechselmatrizen, dass ${}^{B}\mathrm{id}^{C} = ({}^{C}\mathrm{id}^{B})^{-1}$. Damit

$$\begin{aligned}
\det({}^{B}A_{\varphi}^{B}) &= \det({}^{B}\mathrm{id}^{C} \cdot {}^{C}A_{\varphi}^{C} \cdot {}^{C}\mathrm{id}^{B}) \overset{2.9.13}{=} \det\big({}^{B}\mathrm{id}^{C}\big) \cdot \det({}^{C}A_{\varphi}^{C}) \cdot \det\big({}^{C}\mathrm{id}^{B}\big) \\
&= \det\big({}^{B}\mathrm{id}^{C} \cdot {}^{C}\mathrm{id}^{B}\big) \cdot \det({}^{C}A_{\varphi}^{C}) = \det(E_n) \cdot \det({}^{C}A_{\varphi}^{C}) \\
&= \det({}^{C}A_{\varphi}^{C}).
\end{aligned}$$

□

2.9.5 Adjunkte Matrix

Definition 2.9.19

Es sei $A \in R^{n\times n}$, R ein kommutativer Ring. Für $1 \leq i, j \leq n$ definieren wir $A^{i,j} \in M_{n-1,n-1}(R)$ als die durch das Streichen der i.-Zeile und j.-Spalte aus A entstehende Matrix.

Beispiel 2.9.20

Sei

$$A := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & -1 & -2 & -3 \\ -4 & 0 & 1 & 2 \end{pmatrix}.$$

Damit hätte man unter Anderem die Streichungsmatrizen

$$A^{2,3} = \begin{pmatrix} 1 & 2 & 4 \\ 9 & -1 & -3 \\ -4 & 0 & 2 \end{pmatrix}$$

und

$$A^{4,2} = \begin{pmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 9 & -2 & -3 \end{pmatrix}.$$

Definition 2.9.21

Es sei R ein kommutativer Ring und $A \in R^{n\times n}$. Die **adjunkte Matrix** $A^\sharp \in R^{n\times n}$ ist definiert durch die Einträge $A^\sharp_{ij} := (-1)^{i+j} \det A^{j,i}$.

Beispiel 2.9.22

Sei

$$A := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},$$

dann

$$\begin{aligned} A^{1,1} = 4 &\Rightarrow \det\left(A^{1,1}\right) = 4 \\ A^{1,2} = 3 &\Rightarrow \det\left(A^{1,2}\right) = 3 \\ A^{2,1} = 2 &\Rightarrow \det\left(A^{2,1}\right) = 2 \\ A^{2,2} = 1 &\Rightarrow \det\left(A^{2,2}\right) = 1, \end{aligned}$$

womit

$$\begin{aligned} A^\sharp_{1,1} &= (-1)^{1+1} \cdot 4 = 4 \\ A^\sharp_{2,1} &= (-1)^{1+2} \cdot 3 = -3 \\ A^\sharp_{1,2} &= (-1)^{2+1} \cdot 2 = -2 \\ A^\sharp_{2,2} &= (-1)^{2+2} \cdot 1 = 1. \end{aligned}$$

Insgesamt ist also

$$A^\sharp = \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}.$$

Satz 2.9.23

Es gilt

$$A \cdot A^\sharp = (\det A) E_n.$$

Beweis. Wir machen eine Vorüberlegung und betrachten die Matrix $A^{i,j}$. Wir ergänzen diese zu einer $n \times n$-Matrix $\hat{A}^{i,j}$ durch eine neue i.Zeile e_j und eine neue j.Spalte e_i. Also wir fügen an der Stelle (i,j) eine 1 ein und ergänzen die Zeile und Spalte jeweils durch 0. Dann gilt

$$\det \hat{A}^{i,j} = (-1)^{i+j} \det A^{i,j}.$$

Wir können wir (da die Determinante alternierend ist), Vielfache der i.Zeile auf die anderen Zeilen addieren ohne, dass wir die Determinante verändern. Also addieren wir das $a_{k,j}$-fache der i.Zeile auf die k.Zeile von $\hat{A}^{i,j}$. Wir erhalten damit die Matrix

$$\begin{pmatrix} A_{1,\bullet} \\ \vdots \\ A_{i-1,\bullet} \\ e_i \\ A_{i+1,\bullet} \\ \vdots \\ A_{n,\bullet} \end{pmatrix}$$

deren Determinante immer noch $(-1)^{i+j}\det\left(A^{i,j}\right)$ ist.

Jetzt können wir den Eintrag (i,j) der Matrix $A \cdot A^\sharp$ bestimmen.

1. $i = j$:

$$(A \cdot A^\sharp)_{i,j} = \sum_{k=1}^{n} a_{i,k} \cdot (A^\sharp)_{k,j} = \sum_{k=1}^{n} (-1)^{k+j} \cdot a_{i,k} \cdot \det\left(A^{k,j}\right)$$

$$= \sum_{k=1}^{n} (-1)^{k+j} \cdot a_{i,k} \quad \det \begin{pmatrix} A_{1,\bullet} \\ \vdots \\ A_{k-1,\bullet} \\ e_i \\ A_{k+1,\bullet} \\ \vdots \\ A_{n,\bullet} \end{pmatrix} = \quad \det \begin{pmatrix} A_{1,\bullet} \\ \vdots \\ A_{k-1,\bullet} \\ A_{i,\bullet} \\ A_{k+1,\bullet} \\ \vdots \\ A_{n,\bullet} \end{pmatrix}$$

$$= \begin{cases} \det(A) & i = j \\ 0 & i \neq j \end{cases}$$

□

Diese Relation zwischen den beiden Matrizen können wir verwenden um lineare Gleichungssystem nur mit Hilfe von Determinanten zu lösen.

Beispiel 2.9.24: Cramersche Regel

Sei $Ax = b, A \in K^{n\times n}$ ein LGS. Dieses ist genau dann lösbar, wenn $\det(A) \neq 0$, also invertierbar in K. Dann

$$\begin{aligned} & A \cdot A^\sharp = \det(A) \cdot E_n \\ \Leftrightarrow \qquad & A^\sharp = A^{-1} \cdot A \cdot A^\sharp = \det(A) \cdot A^{-1} \cdot E_n = \det(A) \cdot A^{-1} \\ \Leftrightarrow \qquad & A^{-1} = \frac{1}{\det(A)} \cdot A^\sharp. \end{aligned}$$

Damit

$$x = A^{-1} \cdot b = \frac{1}{\det(A)} \cdot A^\sharp \cdot b$$

$$\begin{aligned} \Rightarrow \text{ für alle } 1 \leq i \leq n : x_i &= \frac{1}{\det(A)} \cdot (A^\sharp \cdot b)_i = \frac{1}{\det(A)} \cdot \sum_{k=1}^{n} (A^\sharp)_{i,k} \cdot b_k \\ &= \frac{1}{\det(A)} \cdot \sum_{k=1}^{n} (-1)^{i+k} \cdot \det\left(A^{k,i}\right) \cdot b_k \\ &\overset{\text{Laplace}}{=} \frac{1}{\det(A)} \det(A_{\bullet,1}, \cdots, A_{\bullet,i-1}, b, A_{\bullet,i+1}, \cdots, A_{\bullet,n}). \end{aligned}$$

Wir haben hier nicht nur das Gleichungssystem gelöst sondern sogar die Inverse einer Matrix nur über Determinanten berechnet, statt wie bisher den Gauss-Algorithmus zu verwenden.

2.9.6 Entwicklungssatz Laplace

Satz 2.9.25

Es sei $A \in R^{n\times n}$ und $1 \leq i \leq n$, dann gilt

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A^{i,j}$$

und für $1 \leq j \leq n$

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A^{i,j}.$$

Beispiel 2.9.26

Sei

$$A := \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 7900 & 3 & 0 & 10 \\ 0 & 9\pi & 2 & 0 & 9 \\ 1 & 0 & 7 & -1 & 42070 \\ 0 & 48912 & 4 & -5 & 2 \end{pmatrix}.$$

Die Determinante von A mit der Leibnizformel zu berechnen wäre langwierig und rechenaufwändig. Mit dem Entwicklungssatz von Laplace gestaltet sich dieses aber deutlich einfacher. So sehen wir, dass die erste Spalte von A nur einen Eintrag ungleich 0 hat. Wir entwickeln also entlang dieser Spalte:

$$\begin{aligned} \det(A) \overset{j=1}{=} \sum_{i=1}^{5} (-1)^{i+1} a_{i,1} \cdot \det\left(A^{i,1}\right) &\overset{\text{für alle } i \neq 4 : a_{i,1}=0}{=} (-1)^{4+1} \cdot 1 \cdot \det\left(A^{4,1}\right) \\ &= -\det\left(A^{4,1}\right) \end{aligned}$$

Es ist

$$B := A^{4,1} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 7900 & 3 & 0 & 10 \\ 9\pi & 2 & 0 & 9 \\ 48912 & 4 & -5 & 2 \end{pmatrix}.$$

Nun sieht die 3. Spalte von B vielversprechend aus:

$$\begin{aligned} \det(B) \overset{j=3}{=} \sum_{i=1}^{4} (-1)^{i+3} b_{i,3} \cdot \det\left(B^{i,3}\right) &\overset{\text{für alle } i \neq 4 : b_{i,3}=0}{=} (-1)^{4+3} \cdot (-5) \cdot \det\left(B^{4,3}\right) \\ &= 5 \cdot \det\left(B^{4,3}\right) \end{aligned}$$

Man erhält also

$$C := B^{4,3} = \begin{pmatrix} -1 & 0 & 0 \\ 7900 & 3 & 10 \\ 9\pi & 2 & 9 \end{pmatrix}$$

Hier kann man leicht nach der ersten Zeile entwickeln:

$$\begin{aligned} \det(C) \overset{i=1}{=} \sum_{j=1}^{3} (-1)^{1+j} c_{1,j} \cdot \det\left(C^{1,j}\right) &\overset{\text{für alle } j \neq 1 : c_{1,j}=0}{=} (-1)^{1+1} \cdot (-1) \cdot \det\left(C^{1,1}\right) \\ &= -1 \cdot \det\left(C^{1,1}\right) \end{aligned}$$

Es ist

$$C^{1,1} = \begin{pmatrix} 3 & 10 \\ 2 & 9 \end{pmatrix},$$

welche bekanntlich

$$\det\left(C^{1,1}\right) = 3 \cdot 9 - 2 \cdot 10 = 27 - 20 = 7$$

hat. Damit ergibt sich aber

$$\det(A) = -\det(B) = -1 \cdot 5 \cdot \det(C) = -1 \cdot 5 \cdot (-1) \cdot \det\left(C^{1,1}\right) = -1 \cdot 5 \cdot (-1) \cdot 7 = 35.$$

Wir sehen also, dass der Entwicklungssatz sehr hilfreich ist. Nun gehen wir dazu über diesen zu beweisen.

Beweis. Wir bestimmen dazu den Eintrag (i, i) in $A \cdot A^\sharp$:

$$\det(A) = (A \cdot A^\sharp)_{i,i} = \sum_{k=1}^{n} a_{i,k} a^\sharp_{k,i} = \sum_{k=1}^{n} a_{i,k} (-1)^{i+j} \det\left(A^{i,k}\right).$$

□

Der Entwicklungssatz von Laplace ist besonders wichtig, weil uns dieser die Berechnung von Determinanten stark erleichtern kann. So kann man die Berechnung einer 4×4 Determinante auf die Berechnung von 4 3×3 Determinanten zurückführen, wobei man in günstigen Fällen sogar weniger als 4 Determinanten berechnen muss. Im worst-case ist der Aufwand allerdings immer noch der gleiche wie bei der Leibniz-Regel. Für vollbesetzte Matrizen ist daher erst ein Gauss-Algorithmus zur Vereinfachung zu empfehlen.

Mit dem Entwicklungssatz lassen sich direkt zwei Regeln für bestimmte Arten von Matrizen herleiten:

Beispiel 2.9.27

Sei

$$A := \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array}\right)$$

mit $A \in K^{n \times n}$, $B \in K^{l \times l}$, $C \in K^{l \times n-l}$, $D \in K^{n-l \times n-l}$ und $1 \leq l < n$. Dann gilt

$$\det(A) = \det(B) \cdot \det(D).$$

Man kann diesen Satz durch vollständige Induktion zeigen. Für $l = 1$ folgt die Aussage direkt für eine Entwicklung nach der 1. Spalte. Im Induktionsschritt entwickelt man ebenfalls entlang der 1. Spalte, wendet dann auf die $(l+1)$-Terme die Induktionsvoraussetzung an, klammert die Determinante von D aus und erhält mit dem Entwicklungssatz die Aussage.
Wichtig ist an dieser Stelle die Anmerkung, dass

$$\det\left(\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)\right) = \det(A)\det(D) - \det(C)\det(B)$$

im Allgemeinen **nicht** gilt.

Beispiel 2.9.28

Sei

$$A := \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

eine obere Dreiecksmatrix. Man zeigt, dass

$$\det(A) = \prod_{i=1}^{n} \lambda_i$$

gilt, durch vollständige Induktion:

IA) n=1:

$$A = (\lambda_1) \Rightarrow \det(A) = \lambda_1$$

IV) Angenommen die Aussage gilt für ein $n \in \mathbb{N}$.

IS) Sei

$$A := \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_{n+1} \end{pmatrix}$$

Man entwickelt entlang der 1. Spalte und erhält

$$\det(A) = (-1)^{1+1}\lambda_1 \cdot \det \begin{pmatrix} \lambda_2 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_{n+1} \end{pmatrix} \overset{\text{IV)}}{=} \lambda_1 \cdot \prod_{i=2}^{n+1} \lambda_i = \prod_{i=1}^{n+1} \lambda_i$$

Insbesondere haben damit echte obere Dreiecksmatrizen immer Determinante null.

2.10 Gruppenoperationen

2.10.1 G-Mengen

Definition 2.10.1

Es sei G eine Gruppe und X eine Menge. Dann ist eine **G-Operation** auf X eine Abbildung

$$G \times X \longrightarrow X, (g, x) \mapsto g.x$$

derart, dass für alle $g, h \in G, x \in X$ gilt $g.(h.x) = (gh).x$ und $e.x = x$, wobei $e \in G$ das neutrale Element ist. Wir nennen dann X auch eine **G-Menge**.

Beispiel 2.10.2

1. Sei $G = S_n$ und $X = \{1, \ldots, n\}$, dann definiert $(\sigma, i) \mapsto \sigma(i)$ eine Gruppenoperation der S_n auf X.
2. Sei G eine Gruppe, dann operiert G auf mehrere (natürliche) Weisen auf sich selbst, beispielsweise durch die Linksmultiplikation $(g, h) \mapsto gh$. Dadurch wird G zu einer G-Menge.
3. Sei G eine Gruppe und X eine Menge, dann wird X zu einer G-Menge durch $(g, x) \mapsto x$. Wir nennen diese auch die *triviale* Operation.
4. Es sei G eine Gruppe und X eine G-Menge, dann erhalten wir eine induzierte G-Operation auf $\mathcal{P}(X)$, der Potenzmenge von X.
5. Es sei G eine Gruppe und $H \subset G$ eine Untergruppe. Auf der Menge der Linksnebenklassen G/H ($g_1 \sim g_2 \Leftrightarrow g_1 g_2^{-1} \in H$) erhalten wir durch Linksmultiplikation $(g_1, g_2 H) \mapsto (g_1 g_2)H$ eine G-Operation.

Es sei X eine Menge und $\mathrm{Sym}(X)$ die Gruppe der Bijektionen auf X, die **symmetrische Gruppe einer Menge**.

Proposition 2.10.3

Es sei G eine Gruppe und X eine G-Menge, weiter sei $g \in G$. Dann ist die Abbildung $\sigma_g : X \longrightarrow X, x \mapsto g.x$ in der symmetrischen Gruppe von X.

Beweis. Wir müssen nur nachrechnen, dass σ_g eine Bijektion ist, aber es gilt $(\sigma_g)^{-1} = \sigma_{g^{-1}}$:

$$(\sigma_g \circ \sigma_{g^{-1}}(x) = g.(g^{-1}.x) = (gg^{-1}).x = x$$

und ebenso für $\sigma_{g^{-1}} \circ \sigma_g$. □

Proposition 2.10.4

Es sei G eine Gruppe und X eine Menge, dann gibt es eine Bijektion zwischen den G-Operationen auf X und den Gruppenhomomorphismen $G \longrightarrow \mathrm{Sym}(X)$: sei X eine G-Menge, dann ist die Zuordnung $G \longrightarrow \mathrm{Sym}(X)\, g \mapsto \sigma_g$ ein Gruppenhomomorphismus.

Beweis. Wir haben gesehen, dass $g \mapsto \sigma_g$ wohldefiniert ist von $G \longrightarrow \mathrm{Sym}(X)$. Es seien $g_1, g_2 \in G$, dann gilt

$$\sigma_{g_1 g_2}(x) = (g_1 g_2).x = g_1.(g_2.x) = (\sigma_{g_1} \circ \sigma_{g_2})(x).$$

Damit erhalten wir eine Abbildung

$$\{G - \text{Operationen auf } X\} \longrightarrow \{\text{Gruppenhomomorphismen } G \longrightarrow \mathrm{Sym}(X)\}.$$

Wir geben hierzu die inverse Abbildung an und überlassen den Beweis den Lesenden. Sei also $\phi : G \longrightarrow \mathrm{Sym}(X)$ ein Gruppenhomomorphismus, dann definieren wir

$$G \times X \longrightarrow X, (g, x) \mapsto g.x := \phi(g)(x).$$

Dann gilt $e.x = \phi(e).x = \mathrm{id}_X(x) = x$ und

$$g_1.(g_2.x) = \phi(g_1)(\phi(g_2)(x)) = \phi(g_1 g_2)(x) = (g_1 g_2).x,$$

da ϕ ein Gruppenhomomorphismus ist. □

Definition 2.10.5

Es sei $G \times M \longrightarrow M$ eine Operation auf M

1. Die **Menge der Fixpunkte** oder **Invarianten** von G in M ist
$$M^G = \{m \in M \mid g.m = m \; \forall \; g \in G\}.$$
2. Der **Stabilisator** von $m \in M$ ist die Menge
$$G_m = \{g \in G \mid g.m = m\}.$$
3. Sei $m \in M$, dann ist **die Bahn** oder **der Orbit** von m die Menge
$$G.m = \{g.m \mid g \in G\}.$$
4. Eine Operation heißt **transitiv** wenn es ein $m \in M$ gibt mit $G.m = M$. In diesem Fall nennen wir M mit dieser Operation einen **homogenen Raum**.
5. Sei $g \in G$, dann ist die **Menge der Fixpunkte von** g
$$M^g = \{m \in M \mid g.m = m\}.$$

Lemma 2.10.6

Es sei G eine Gruppe und X eine G-Menge, dann sind zwei Bahnen entweder gleich oder disjunkt.

Beweis. Es seien $x, y \in M$ und $G.x \cap G.y \neq \emptyset$, also $\exists\, g_1, g_2 \in G$ mit $g_1.x = g_2.y$. Dann ist aber auch $(g_2^{-1} g_1).x = y$, also $y \in G.x$ und damit $G.y \subseteq G.y$ (und umgekehrt). □

Korollar 2.10.7

Es sei G eine Gruppe und X eine G-Menge, dann wird durch die Bahnen eine Äquivalenzrelation auf X definiert, $x_1 \sim x_2$ genau dann, wenn x_1, x_2 in einer gemeinsamen Bahn unter der G-Operation sind.

Beweis. Der Beweis folgt direkt aus Lemma 2.10.1 □

Definition 2.10.8

Es sei G eine Gruppe und X eine G-Menge. Die Menge der Bahnen bezeichnen wir als **Bahnenraum** $X\backslash G$. Die kanonische, surjektive Abbildung $x \mapsto G.x$ bezeichnen wir mit $\text{can} : G \longrightarrow X\backslash G$.

Bemerkung 2.10.9

Der Bahnenraum ist also der Quotientenraum der Äquivalenzrelation.

Lemma 2.10.10

Es sei G eine Gruppe und X eine G-Menge. Sei $\varphi : X \longrightarrow Y$ eine Abbildung mit $\varphi(g.x) = \varphi(x)$ für alle $g \in G, x \in X$. Dann existiert genau eine Abbildung $\overline{\varphi} : X\backslash G \longrightarrow Y$ mit $\overline{\varphi} \circ \text{can} = \varphi$. Genauer ist $\overline{\varphi}(G.x) := \varphi(G.x) = \varphi(x)$.

Beweis. Das folgt aus dem Homomorphiesatz für Mengen. □

2.10.2 Drei fundamentale Beispiele von G-Mengen

In diesem Abschnitt möchten wir drei besondere G-Operationen betrachten, welche uns durch große Teile der Linearen Algebra 1 und 2 begleiten.

Beispiel 2.10.11: Rang-Theorem

Es sei $G = \text{GL}_m(\mathbb{K}) \times \text{GL}_n(\mathbb{K})$ und $X = \mathbb{K}^{m\times n}$ mit

$$((g,h), A) \mapsto gAh^{-1}.$$

Das entspricht den Basiswechseln von $\mathbb{K}^m$ und $\mathbb{K}^n$, und liefert die Darstellungsmatrix der linearen Abbildung φ_A bzgl. dieser neuen Basen definiert durch g und h. Wir kennen die davon induzierte Äquivalenzrelation schon aus Definition 2.8.11. Das erste große Ziel der Linearen Algebra war für uns die Untersuchung dieser $\text{GL}_n(\mathbb{K})$-Operation und mit Theorem 2.8.40 wissen wir, dass es genau $\min n, m+1$ Bahnen unter dieser Operation gibt.

Beispiel 2.10.12: Jordan- und Smith-Normalform

Es sei $G = \text{GL}_n(\mathbb{K})$ und $X = \mathbb{K}^{n\times n}$ mit

$$(g, A) \mapsto gAg^{-1}.$$

Das entspricht einem Basiswechsel auf dem $\mathbb{K}^n$. Auch die davon induzierte Äquivalenzrelation kennen wir schon aus Definition 2.8.11, wir sagen also zwei Ma-

trizen sind **ähnlich** wenn sie in einer gemeinsamen Bahn liegen. Die Frage nach den Bahnen ist eine viel schwierigere und wir werden diese in Lineare Algebra 2 versuchen zu beantworten, werden uns dabei aber zunächst auf algebraisch abgeschlossene Körper beschränken müssen.

Ein Beispiel, welches uns in Lineare Algebra 2 beschäftigen wird:

Beispiel 2.10.13: Trägheitssatz von Sylvester

Es sei $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$, $G = \mathrm{GL}_n(\mathbb{K})$ und $X = \{A \in \mathbb{K}^{n\times n} \mid A = \overline{A}^t\}$ (die transponierte Matrix aus Definition 2.8.22 deren Einträge komplex konjugiert sind) mit

$$(g, A) \mapsto g^t A\overline{g}.$$

Dann gilt

$$\overline{(g^t A\overline{g})}^t = \overline{(\overline{g}^t)}\overline{A^t g^t}^t = (g^t A\overline{g}),$$

also ist die Operation wohldefiniert auf X. Wieder können wir die Frage nach den Bahnen stellen und die Antwort ist das zweite große Ziel in der Linearen Algebra 2, der Trägheitssatz von Sylvester.

Sie sehen, dass wir große Teile der Linearen Algebra durch den Begriff von Gruppenoperationen motivieren können.

Mit Hilfe von Gruppenoperationen können wir auch die Aufgabe 2.11.5 nochmal anders formulieren:

Aufgabe 2.10.14

Es sei $G = \mathrm{GL}_n(\mathbb{K})\times\mathrm{GL}_n(K)\times\mathrm{GL}_n(\mathbb{K})$ und $X = \mathbb{K}^{n\times n}\times\mathbb{K}^{n\times n}$ mit der Operation

$$((g_1, g_2, g_3), (A_1, A_2)) \mapsto (g_2 A_1 g_1^{-1}, g_3 A_2 g_2^{-1}).$$

Können Sie die Bahnen unter dieser Operation beschreiben? Wie viele Bahnen gibt es und können Sie für jede Bahn einen Repräsentanten auswählen?

Hinweis: Für das Rang-Theorem benötigen Sie zwei Basiswechsel für eine Abbildung, eine für den Definitionsbereich und einen für den Wertebereich. In diesem Fall haben Sie aber nur drei Basiswechsel für zwei Abbildungen, das macht die Aufgabe etwas komplizierter.

2.10.3 Bahnformel

Lemma 2.10.15

Es sei M eine G-Menge und $x \in M$. Dann ist die Abbildung

$$G/G.x \longrightarrow G_x,\ g \cdot G_x \mapsto g.x$$

eine Bijektion.

Beweis. Wir zeigen zunächst, dass die Abbildung wohldefiniert ist. Seien dazu $g_1 \cdot G_x =$

$g_2 \cdot G_x$, also $g_2^{-1} g_1 \in G_x$. Dann ist

$$g_2.x = g_2.(g_2^{-1} g_1.x) = (g_2 g_2^{-1}).(g_1.x) = g_1.x$$

und damit ist die Abbildung unabhängig von der Wahl der Repräsentanten. Die Abbildung ist weiterhin injektiv, denn falls $g_1.x = g_2.x$, so ist $(g_1^{-1} g_2).x = x$, also $g_1^{-1} g_2 \in G_x$ und damit $g_1 \cdot G_x = g_2 \cdot G_x$. Die Surjektivität ist gegeben, da $G.x$ ein Orbit ist. □

Korollar 2.10.16

Es sei G eine endliche Gruppe und M eine G-Menge. Dann gilt für jedes $x \in M$:

$$|G| = |G.x| \cdot |G_x|.$$

Beweis. Das folgt sofort aus Lemma 2.10.15. □

Definition 2.10.17

Es sei G eine Gruppe und wir machen G zu einer G-Menge durch die **Konjugation**

$$G \times G \longrightarrow G,\ (g, h) \mapsto ghg^{-1}.$$

Die Bahnen unter dieser Operation heißen **Konjugationsklassen**.

Bemerkung 2.10.18

Die Lesenden mögen verifizieren, dass die Konjugation tatsächlich eine G-Menge definiert.

Bemerkung 2.10.19

Wir können in Beispiel 2.10.12 die Menge X auf invertierbare Matrizen einschränken und erhalten gerade die Konjugation der $\mathrm{GL}_n(\mathbb{K})$.

Beispiel 2.10.20

Ein fundamentales Beispiel für die Konjugation ist die Operation der S_n auf sich selber

$$(\sigma, \tau) \mapsto \sigma\tau\sigma^{-1}.$$

Versuchen Sie sich mal an den Konjugationsklassen für festes n. Wie viele existieren davon (natürlich nur endlich viele) und wie lassen diese sich parametrisieren?

Lemma 2.10.21: Burnside's Lemma

Es sei G eine endliche Gruppe und M eine G-Menge. Dann gilt

$$|M \backslash G| = \frac{1}{|G|} \sum_{g \in G} |M^g|$$

Bemerkung 2.10.22

Dieses Lemma wird eigentlich Frobenius oder Cauchy-Frobenius zugeschrieben, Burnside hat, ohne böse Absicht, vergessen, die beiden zu zitieren.

Beweis. Wir betrachten für $g \in G$ die Menge M^g, die Fixpunkte von g, dann gilt

$$\sum_{g\in G} |M^g| = |\{(g,x) \in G \times M \mid g(x) = x\}| = \sum_{x\in M} |G_x| = \sum_{H\in M\backslash G} \sum_{x\in H} |G_x|.$$

Es sei $H \in M\backslash G$, $x, y \in H$, $g \in G$ mit $g.x = y$. Dann ist

$$\tau_g : G_x \longrightarrow G_y \ , \ h \mapsto ghg^{-1}.$$

erstens wohldefiniert, denn wenn $h.x = x$, dann ist $ghg^{-1}.y = gh.x = g.x = y$ und zweitens eine Bijektion, denn mit $\tau_{g^{-1}}$ umkehrbar. Also sei $x_H \in H$ fest gewählt. Dann gilt

$$\sum_{x\in H} |G_x| = \sum_{x\in H} |G_{x_H}| = |G.x_H| \cdot |G_{x_H}| = |G|,$$

wobei die letzte Gleichung aus Korollar 2.10.16 folgt. Damit gilt

$$\sum_{g\in G} |M^g| = \sum_{H\in M\backslash G} \sum_{x\in H} |G_x| = \sum_{H\in M\backslash G} |G| = |M\backslash G| \cdot |G|.$$

□

Wir sehen, dass wir nicht sehr viele Voraussetzungen benötigen um dieses Lemma zu beweisen. Tatsächlich kann dieses Lemma nur mit den Inhalten des Abschnitts über Gruppenoperationen bewiesen werden. Wir können aber dieses Lemma in Anwendungen nutzen. Wenn wir wissen möchten wie viele Objekte (in einer bestimmten Menge) wir bis auf Symmetrie (mit welcher Symmetrie auch immer, formal würden wir bis auf G-Operation für eine Gruppe G sagen) haben, so müssen wir nur für jedes Element aus der Symmetriegruppe nachrechnen, wie viele Objekte fixiert werden.

Beispiel 2.10.23

Es sei M die Menge alle Graphen (das heißt Mengen von Knoten mit je maximal einer Kante zwischen zwei Knoten) mit 4 Knoten, von solchen Graphen gibt es $2^6 = 64$. Wie viele solcher Graphen gibt es bis auf Isomorphie (also bis auf Drehung, Vertauschen, Spiegeln etc.)? Diese Isomorphien sind durch die Operation der S_4 auf den Knoten gegeben. Nach dem Lemma von Burnside müssen wir dazu nur für jedes Element $g \in S_4$ die Anzahl der Graphen bestimmen, welche invariant unter g sind.

- $g = \mathrm{id}$, dann sind alle 64 Graphen invariant.
- Es sei $g \in S_4$ ein 2-Zykel, davon gibt es 6. Es sei $g = (ab)$, dann ist die Anzahl der Kanten zwischen c und a genau die Anzahl zwischen b und a. Es bleiben also $2^4 = 16$ Graphen in M^g.
- Es sei g das Produkt zweier disjunkter 2-Zykel, davon gibt es 3. Dann ist $M^g = 16$.

- Es sei g ein 3-Zykel, davon gibt es 8. Dann ist $M^g = 4$.
- Es sei g ein 4-Zykel, davon gibt es 6. Dann ist $M^g = 4$.

Die Formel

$$M\backslash G = \frac{1}{|G|}\sum_{g\in G}|M^g|$$

übersetzt sich damit zu

$$M\backslash G = \frac{1}{24}(1\cdot 64 + 6\cdot 16 + 3\cdot 16 + 8\cdot 4 + 6\cdot 4) = \frac{1}{24}(64+96+48+32+24) = 11$$

2.10.4 Bruhatzerlegung

Definition 2.10.24

Die **Standard-Boreluntergruppe** $B_n(\mathbb{K})$ der $\mathrm{GL}_n(\mathbb{K})$ ist die Untergruppe der oberen Dreiecksmatrizen.

Bemerkung 2.10.25

Das ist tatsächlich eine Untergruppe, wie sich leicht verifizieren lässt.

Bemerkung 2.10.26

Grundsätzlich nennen wir eine Untergruppe eine **Boreluntergruppe**, wenn sie auflösbar ist und mit dieser Eigenschaft maximal, aber das würde uns hier zu weit führen. Wir merken uns nur, dass auch die Gruppe der unteren Dreiecksmatrizen eine Boreluntergruppe ist und schreiben dafür $L_n(\mathbb{K})$.

Für den folgenden Satz führen wir noch die Notation einer Permutationsmatrix ein
Es sei $w \in S_n$, dann ist die Permutationsmatrix $E_w \in \mathrm{GL}_n(\mathbb{K})$ definiert durch

$$(E_w)_{i,j} = \begin{cases} 1 & j = \sigma(i) \\ 0 & \text{sonst} \end{cases}$$

Dann gilt

$$E_w(e_i) = e_{\sigma(i)}.$$

Bemerkung 2.10.27

Wir beachten, dass die Spalten von E_w paarweise verschiedene Einheitsvektoren sind und jede Matrix dieser Gestalt genau so ein E_w ist.

Satz 2.10.28

Wir betrachten $\mathrm{GL}_n(\mathbb{K})$ als $B_n(\mathbb{K}) \times B_n(\mathbb{K})$-Menge durch

$$((b_1, b_2), g) \mapsto b_1 g b_2^{-1}.$$

Dann sind die Bahnen parametrisiert durch S_n, die Bijektion ist gegeben durch

$$w \mapsto B_n(\mathbb{K})E_wB_n(\mathbb{K}).$$

Beweis. Wir zeigen, dass die Matrizen E_w ein Repräsentantensystem bilden. Sei dazu $A \in \mathrm{GL}_n(\mathbb{K})$, es sei i maximal mit $a_{i,1} \neq 0$. Dann können wir durch Zeilenumformungen (hierbei reichen Linksmultiplikation mit Elementen aus $B_n(\mathbb{K})$) erreichen, dass A äquivalent ist zu einer Matrix A', deren erste Spalte genau e_i ist. Durch Spaltenumformungen (Rechtsmultiplikation mit Elementen aus $B_n(\mathbb{K})$), können wir annehmen, dass die i.Zeile genau e_1 ist.
Wir setzen das induktiv fort und sehen, dass A äquivalent ist zu einer Matrix deren Spalten paarweise verschiedene Einheitsvektoren sind. Dazu beachten wir, dass A invertierbar ist, also auch A' invertierbar ist und damit in der zweiten Spalte von A' wieder ein Eintrag ungleich 0 ist. Dieser Eintrag kann nicht in der i.Zeile sein.
Tatsächlich erhalten wir so zu A eine Sequenz $i_A := (i_1, i_2, \ldots, i_n)$ definiert durch

$$i_j := \max\{\ell \mid a_{\ell,j} \neq 0 \text{ und } \ell \neq i_1, \ldots, i_{j-1}\}.$$

Diese Sequenz definiert eine Permutation w durch $w(j) = i_j$ und damit ist A äquivalent zu der Matrix E_w. Tatsächlich gilt sogar (wir überlassen die Rechnung den Lesenden) für $T, S \in B_n(\mathbb{K})$:

$$i_A = i_{SAT}.$$

Daraus folgt, dass E_w und E_τ genau dann äquivalent sind, wenn $\tau = w$ und damit haben wir gezeigt, dass die Bahnen durch S_n parametrisiert werden und die E_w ein Repräsentantensystem bilden. □

Definition 2.10.29

Die Zerlegung

$$\mathrm{GL}_n(\mathbb{K}) = \coprod_{w \in S_n} B_n(\mathbb{K})E_wB_n(\mathbb{K})$$

nennen wir die **Bruhatzerlegung** der $\mathrm{GL}_n(\mathbb{K})$ und die einzelnen Bahnen nennen wir **Bruhat-Zellen**.

Es sei w_0 das *längste Element* der S_n, also $w_0(i) = n + 1 - i$ für alle i. Dann gilt

$$L_n(\mathbb{K}) = E_{w_0}B_n(\mathbb{K})E_{w_0},$$

wie Sie gerne als Übung verifizieren können. Weiter ist $BE_{w_0}B$ die *größte* Zelle, genauer ist (für einen unendlichen Körper) die Wahrscheinlichkeit gleich 1, dass eine beliebige Matrix in dieser Zelle liegt. Wenn wir diese größte Zelle mit w_0 verschieben, dann erhalten wir also

$$E_{w_0}(B_n(\mathbb{K})E_{w_0}B_n(\mathbb{K})) = L_n(\mathbb{K})B_n(\mathbb{K}).$$

Definition 2.10.30

Die Untergruppe $U_n(\mathbb{K})$ der unipotenten Matrizen ist die Menge der Matrizen in $B_n(\mathbb{K})$ deren Diagonaleinträge alle gleich 1 sind.

Bemerkung 2.10.31

Auch hier lässt sich schnell verifizieren, dass $U_n(\mathbb{K})$ tatsächlich eine Untergruppe ist und mehr noch

$$L_n(\mathbb{K}) \cap U_n(\mathbb{K}) = \{E_n\}$$

und

$$LU = LB.$$

Proposition 2.10.32

Die Abbildung

$$L_n(\mathbb{K}) \times U_n(\mathbb{K}) \longrightarrow L_n(\mathbb{K})B_n(\mathbb{K}), (l, u) \mapsto lu$$

ist eine Bijektion.

Beweis. Nach der vorherigen Bemerkung reicht es aus, die Injektivität nachzurechnen. Dafür seien $l_1, l_2 \in L_n(\mathbb{K}), u_1, u_2 \in U_n(\mathbb{K})$ mit $l_1u_1 = l_2u_2$. Es folgt

$$l_2^{-1}l_1 = u_2u_1^{-1} = E_n$$

da sowohl $L_n(\mathbb{K})$ als auch $U_n(\mathbb{K})$ jeweils Untergruppen sind und wiederum nach obiger Bemerkung der Schnitt nur E_n ist. Aber damit folgt, dass die Abbildung injektiv ist. □

Definition 2.10.33

Die Zerlegung einer Matrix aus $L_n(\mathbb{K})B_n(\mathbb{K})$ in $L_n(\mathbb{K}) \times U_N(\mathbb{K})$ heißt auch **LR-Zerlegung** oder **LU-Zerlegung** und wird Ihnen in der Numerik wieder begegnen.

Bemerkung 2.10.34

Wir bemerken hierbei, dass eine beliebige Matrix $A \in \mathrm{GL}_n(\mathbb{K})$ genau dann eine LR-Zerlegung hat, wenn sie sich durch durch Zeilenoperationen aber ohne Zeilenvertauschungen in eine obere Dreiecksmatrix umformen lässt. Diese Zeilenoperationen ergeben die Matrix l und die resultierende Matrix ist die Matrix u.

2.11 Zusatzaufgaben

Während des Semesters werden wir immer mal wieder Aufgaben jenseits der Übungsblätter stellen, die Sie ein bisschen herausfordern sollen. Diese sind, jeweils im Kontext des Wissensstand, eventuell schwieriger als die üblichen Hausaufgaben:

Aufgabe 2.11.1: Abschnitt 2.3, Gruppen, Ringe, Körper

Es sei G eine abelsche Gruppe, Sie dürfen annehmen, dass

$$G = \mathbb{Z}^m \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_s\mathbb{Z}$$

für $m \in \mathbb{N}_0$ und $a_i \in \mathbb{N}$. Beschreiben Sie alle G für die gilt:

$$\mathrm{End}_{\mathbb{Z}}(G) \text{ ist ein kommutativer Ring}$$

Aufgabe 2.11.2: Abschnitt 2.6, Vektorräume

Wir betrachten Tupel $(A, v) \in \mathbb{K}^{n\times n} \times \mathbb{K}^n$ für $n \geq 1$ und einen Körper $\mathbb{K}$. Beschreiben Sie die Tupel (A, v) so dass gilt

$$\forall\, w \in \mathbb{K}^n\ \exists\, p \in \mathbb{K}[x] : w = p(A) \cdot v.$$

Aufgabe 2.11.3: Abschnitt 2.7, Dimensionstheorie

Wir betrachten $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum. Zeigen Sie konstruktiv, dass es in $\mathbb{R}$ unendliche, linear unabhängige Teilmengen gibt.

Aufgabe 2.11.4: Abschnitt 2.6, Ringe und Moduln

Es sei $\mathbb{K}$ ein Körper und $V \neq 0$ ein $\mathbb{K}$-Vektorraum. Dann existiert eine injektive lineare Abbildung $\iota : \mathbb{K} \longrightarrow V$. Tatsächlich existiert für jedes $v \neq 0$ eine solche Abbildung, durch $\iota(1) = v$.

1. Gilt das auch für einen beliebigen Kring R und einen beliebigen R-Modul M?
2. Welche R-Moduln *verhalten* sich so wie Vektorräume? (Erzeugendensystem, lineare Unabhängigkeit, Basis)

Aufgabe 2.11.5: Abschnitt 2.8.7, Rang-Theorem

Es sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Es sei $X = (\mathbb{K}^{n\times n}, \mathbb{K}^{n\times n})$ und eine Äquivalenzrelation R auf X definiert durch

$$(A_1, B_1) \equiv (A_2, B_2) :\Leftrightarrow \exists\, S_1, S_2, S_3 \in \mathrm{GL}_n(\mathbb{K}) \text{ mit } S_2 A_1 S_1^{-1} = A_2, S_3 B_1 S_2^{-1} = B_2.$$

(eine Verallgemeinerung der Definition von äquivalenten Matrizen).

1. Zeigen Sie, dass R eine Äquivalenzrelation ist.
2. Bestimmen Sie die Anzahl der Äquivalenzklassen von R.
3. Geben Sie ein Repräsentantensystem von R an.
4. Wie sieht eine Verallgemeinerung auf $X = (\mathbb{K}^{n\times n})^m$ aus, wie sieht dann ein Repräsentantensystem aus?

Aufgabe 2.11.6: Abschnitt 2.9, Determinanten

Die Determinante ist die einzige (auf den Spalten von Elementen aus $\mathbb{K}^{n\times n}$) alternierende Multilinearform welche auf E_n normiert ist.
Wie lässt sich das auf $\mathbb{K}^{m\times n}$ verallgemeinern? Wie sehen dort die (auf den Spal-

ten) alternierenden Multilinearformen aus?

1. Zeigen Sie, dass die Menge der alternierenden Multilinearformen auf $\mathbb{K}^{m\times n}$ ein Vektorraum ist.
2. Welche Dimension hat dieser Vektorraum? Geben Sie dazu eine Basis an.

Aufgabe 2.11.7: Abschnitt 2.10, Gruppenoperationen

Es sei $n \geq 1$ und wir betrachten die Operation der S_n auf S_n durch Konjugation:

$$S_n \times S_n \longrightarrow S_n \ , \ (\sigma, \tau) \mapsto \sigma\tau\sigma^{-1}.$$

1. Wie viele Konjugationsklassen (Bahnen) hat diese Operation?
2. Geben Sie ein Repräsentantensystem an.

Literaturverzeichnis

[1] Siegfried Bosch. *Lineare Algebra*. Springer-Verlag, New York, 2014.

[2] Gerd Fischer. *Lineare Algebra*. Grundkurs Mathematik. Friedr. Vieweg & Sohn, Braunschweig, 1979.

[3] Klaus Jänich. *Lineare Algebra*. Springer-Verlag, New York, 2013.

[4] Gerhard Kowalsky, Hans-Joachim und Michler. *Lineare Algebra*. de Gruyter, 2003.

[5] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[6] Falko Lorenz. *Lineare Algebra 1+2*. Spektrum Akademischer Verlag, 2003.

[7] Hartmut Storch, Uwe und Wiebe. *Band 2: Lineare Algebra*. Springer Spektrum, 2010.

Index