

Kapitel L

Signatur und Determinante

*Algebra is the offer made by the devil to the mathematician.
The devil says: I will give you this powerful machine, it will answer
any question you like. All you need to do is give me your soul:
give up geometry and you will have this marvelous machine.*

Sir Michael Atiyah (1929–2019)

Vollversion

eiserm.de/lehre/LinA

05.03.2022

Inhalt dieses Kapitels L

L002

- 1 Die Signatur
 - Permutationen, Inversionen und Parität
 - Die Signatur einer Selbstabbildung
 - Die alternierende Gruppe
- 2 Die Determinante
 - Geometrische Motivation als orientiertes Volumen
 - Die drei Axiome: multilinear, alternierend, normiert
 - Der Hauptsatz zu Determinanten und erste Beispiele
 - Existenz und Eindeutigkeit und Multiplikativität
 - Cramersche Regel, Adjunkte und Inverse
 - Effiziente Berechnung der Determinante
 - Die rekursive Laplace–Entwicklung
- 3 Erste Anwendungen
 - Invarianz der Dimension über kommutativen Ringen
 - Die Determinante eines Endomorphismus
 - Die spezielle lineare Gruppe
 - Volumen und Orientierung

Wir diskutieren in diesem Kapitel zwei grundlegende Konstruktionen:
 (1) Die Signatur $\text{sign}(f) \in \{\pm 1, 0\}$ einer Selbstabbildung $f: X \rightarrow X$, zunächst für die Modellmenge $X = \{1 < 2 < \dots < n\}$, dann allgemein für jede endliche Menge X . Die Signatur ist multiplikativ, genauer ein Homomorphismus von Monoiden bzw. Gruppen:

$$\begin{array}{ccc} (\mathbb{E}_X, \circ, \text{id}_X) & \xrightarrow{\text{sign}=\text{sign}_X} & (\{\pm 1, 0\}, \cdot, 1) \\ \cup & & \cup \\ (\mathbb{S}_X, \circ, \text{id}_X) & \xrightarrow{f \mapsto \text{sign}(f)} & (\{\pm 1\}, \cdot, 1) \end{array}$$

(2) Im Anschluss an die Signatur konstruieren wir ihre große Schwester, die Determinante $\det(f) \in K$ einer linearen Selbstabbildung $f: V \rightarrow V$ über einem kommutativen Ring K . Dies gelingt zunächst leichter für den Modellraum $V = K^n$, dann für jeden K -linearen Raum V mit endlicher Basis. Auch die Determinante ist multiplikativ, wir erhalten so:

$$\begin{array}{ccc} (\text{End}_K(V), \circ, \text{id}_V) & \xrightarrow{\det=\det_V} & (K, \cdot, 1) \\ \cup & & \cup \\ (\text{Aut}_K(V), \circ, \text{id}_V) & \xrightarrow{f \mapsto \det(f)} & (K^\times, \cdot, 1) \end{array}$$

Die Analogie zwischen diesen beiden Konstruktionen ist frappierend. Wir beginnen zunächst mit der Signatur; sie ist leichter zu verstehen, einfacher herzustellen und anschließend für die Determinante hilfreich.

Ich erkläre das Vorgehen für die Signatur betont ausführlich, in Zeitlupe. Anschließend führen wir es für die Determinante dann genauso aus. Daher ist es gut, mit der leichter verständlichen Signatur zu üben.

Für die Determinante beginne ich mit der geometrischen Motivation als orientiertes Volumen. Das ist besonders anschaulich und leicht fasslich (und so nutzt die Analysis später die Determinante für die Integration).

Daraus extrahieren wir die algebraische Definition und beweisen dann die Existenz und die Eindeutigkeit sowie die wichtigsten Eigenschaften. Es entsteht eine wunderschöne, harmonische und elegante Theorie!

Erste Beispiele, Rechnungen und Anwendungen runden das Bild ab. Die Vorlesung legt die Fundamente. Zum tieferen Verständnis und zur routinierten Rechenfertigkeit empfehle ich nachdrücklich die Übungen!

Die Signatur ist eine allgegenwärtige kombinatorische Invariante. Ich begnüge mich hier knapp mit einer spektakulären Anwendung, der Lösung des berühmt-berüchtigten 15-Puzzles (Satz L1s).

Ebenso spielt die Determinante nahezu überall eine prominente Rolle, wo lineare Gleichungssysteme gelöst (L2P), Matrizen invertiert (L2s) oder lineare Abbildungen von Vektorräumen untersucht werden (L3D).

Determinanten sind ein wunderbares theoretisches Werkzeug, doch in hoher Dimension zunächst schwer zu berechnen. Ihre Kraft entfalten sie daher erst im Zusammenspiel mit und als Ergänzung zu praktischen Methoden, insbesondere dem Gauß-Algorithmus und seinen Varianten.

Meist sind es gerade die individuellen Stärken verschiedener Ansätze, die sich bestens ergänzen und das Zusammenwirken zum Erfolg führen. Sie werden dies hier in der Linearen Algebra des Öfteren erleben, und darüber hinaus sehr häufig in der Mathematik.

Determinanten sind ein elegantes und weitreichendes Werkzeug. Zur Erkundung dieses Gebiets wähle ich das folgende Vorgehen, das hier mustergültig zelebriert wird:

- 1 Motivation: Was wollen wir erreichen?
- 2 Konstruktion: Existenz einer Lösung
- 3 Charakterisierung: Eindeutigkeit der Lösung
- 4 Eigenschaften: Beziehungen und Formeln
- 5 Berechnung: effiziente Algorithmen
- 6 Erste Beispiele und Anwendungen

Diese verschiedenen Aspekte und Argumente stützen und ergänzen sich gegenseitig. Es wäre töricht, nur auf Algorithmen zu schielen, ohne die Fundamente zu legen, oder umgekehrt eine Theorie aufzubauen, die kaum einer Berechnung zugänglich ist. Auch das kann man tun, in der Not frisst der Teufel bekanntlich Fliegen, doch ideal ist es nicht.

Für Determinanten hingegen spielt alles glücklich zusammen!

Ich gehe in dieser Vorlesung zur Linearen Algebra ganz bewusst und angemessen ausführlich auch auf algorithmische Aspekte ein. Mathematik findet nicht nur, aber eben auch auf dem Computer statt. Ich präzisiere dazu Datenstrukturen und Algorithmen soweit möglich. Unser treues Arbeitspferd ist der extrem nützliche Gauß–Algorithmus: Wir nutzen ihn erfolgreich sowohl zu Rechnungen als auch für Beweise! Seine guten Dienste leistet das Gauß–Verfahren auch in diesem Kapitel, Sie dürfen sich freuen, dass Ihre Investition weiter reiche Früchte trägt.

Die algorithmische Sichtweise ist für Programmierung und Anwendung unverzichtbar, daran besteht kein Zweifel. Ich bin zudem überzeugt, dass sie auch für das mathematische Verständnis vorteilhaft ist.

Das mag überraschen, hat aber ganz naheliegende Gründe:

Die Formulierung als Computerprogramm zwingt uns zur Präzision.

Das ist in den meisten Situationen ein strenger, doch guter Test.

Manche sagen: „Du hast es erst dann verstanden, wenn du es einem Computer beibringen kannst.“ Das ist etwas extrem, aber doch nützlich.

Die Mathematik ist wunderschön und nützlich, und dies gilt meiner Überzeugung nach sowohl für theoretische Grundlagen als auch für praktische Umsetzungen, ebenso für Theoreme wie für Algorithmen. Beide arbeiten zusammen wie linke und rechte Hand.

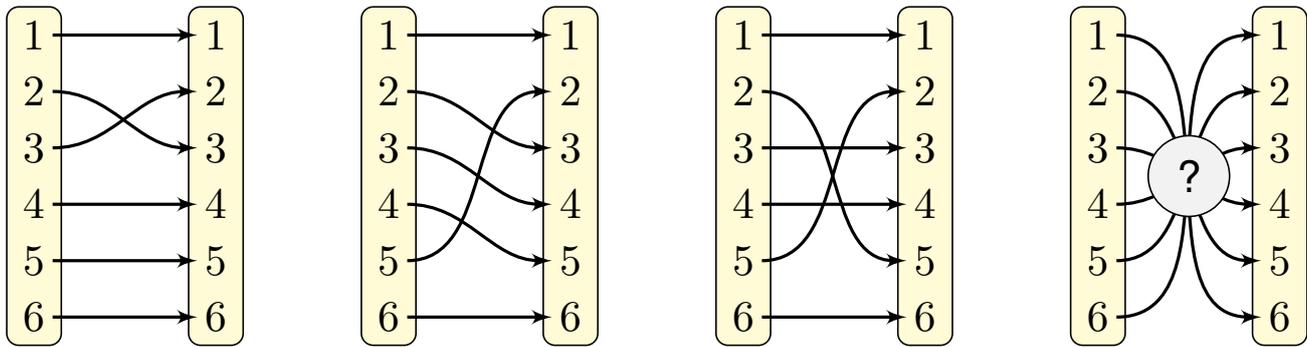
Genau besehen ist die Unterscheidung nur eine Frage des fachlichen Schwerpunkts und der persönlichen Präferenz: Auch Algorithmen wollen bewiesen werden, auch Sätze wollen angewendet werden.

Bitte begreifen Sie daher beides als integralen Teil der Mathematik.

Diese Grundphilosophie führe ich auch in diesem Kapitel fort und suche eine ehrliche Balance zwischen Theorie und Praxis.

Beim ersten Kontakt mag Ihnen alles theoretisch vorkommen, doch wir legen zugleich die praktischen Werkzeuge bereit.

Zu Ihrer erfolgreichen Arbeit benötigen Sie immer beides: präzise Begriffe und effiziente Methoden. Sie werden dies spüren und in Ihren eigenen Rechnungen gut nutzen können, angefangen in den Übungen zur Linearen Algebra und anschließend weit darüber hinaus.



Aufgabe: Nach dem Rennen sind für jeden Kart die Startposition $i \in X = \{1, \dots, n\}$ und zudem die Zielposition $\sigma(i) \in X$ bekannt.

- (1) Wie viele Überholmanöver gab es mindestens?
- (2) Wie viele Überholmanöver gab es tatsächlich?

Lösung: Wir betrachten die Menge der **Inversionen** aka **Fehlstände**:

$$\text{Inv}(\sigma) := \{ \{i, j\} \subseteq X \mid i < j \wedge \sigma(i) > \sigma(j) \}$$

Mit $\text{inv}(\sigma) := \#\text{Inv}(\sigma)$ bezeichnen wir die Anzahl der Inversionen.

- (1) Es gab mindestens $\text{inv}(\sigma)$ Überholmanöver! Warum? Siehe (2)!

Wir treffen hier stillschweigend ein paar vereinfachende Annahmen:

(a) Die Zuordnung $\sigma : X \rightarrow X$ von Start zu Ziel ist eine Permutation.

- Alle Karts haben eine feste Startreihenfolge (Pole-Position) und die Reihenfolge beim Zieleinlauf ist eindeutig (keine Gleichzeitigkeit).
- Es gilt Erhaltung: Während des Rennens gehen keine Karts verloren, und es kommen natürlich auch keine neuen hinzu.

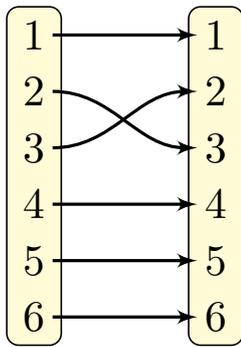
(b) Wir gehen davon aus, dass jeweils nur paarweise überholt wird, so dass wir nur paarweise Überholmanöver zählen müssen und können.

Das ist durchaus realistisch und anschaulich plausibel: Die Fahrbahn ist breit genug für zwei Karts nebeneinander, aber nicht für drei.

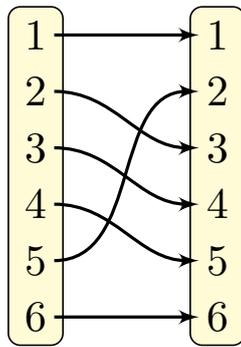
Notation: Wir schreiben kurz und bequem $\{i \neq j\}$ bzw. $\{i < j\}$ für die Menge $\{i, j\}$ mit $i \neq j$ bzw. sortiert mit der Ordnung $i < j$.

Wir nennen ein Paar $\{i \neq j\} \subseteq X$ **gerade**, falls $i < j$ und $\sigma(i) < \sigma(j)$, und **ungerade**, falls $i < j$ und $\sigma(i) > \sigma(j)$. Letzteres nennt man eine **Inversion** oder einen **Fehlstand**, manchmal auch eine **Fehlstellung**.

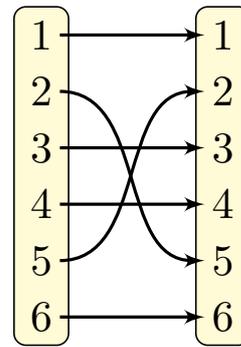
Anschauliches Beispiel: ein Kartrennen



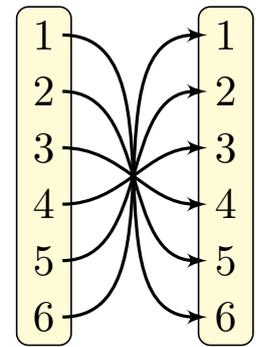
$$\text{inv} = 1$$



$$\text{inv} = 3$$



$$\text{inv} = 5$$



$$\text{inv} = \frac{n(n-1)}{2}$$

(2) Die tatsächliche Anzahl ist eventuell größer, um eine gerade Zahl!

$$\# \text{Überholmanöver} = \# \text{Inv}(\sigma) + 2n, \quad n \in \mathbb{N}$$

Beweis durch doppeltes Abzählen: Betrachte jedes Paar $\{i < j\}$.

- Für $\sigma(i) < \sigma(j)$ gab es $0 + 2n_{ij}$ Überholmanöver, wobei $n_{ij} \in \mathbb{N}$.
- Für $\sigma(i) > \sigma(j)$ gab es $1 + 2n_{ij}$ Überholmanöver, wobei $n_{ij} \in \mathbb{N}$.

Wir erhalten alle Überholmanöver, indem wir über alle Paare summieren. Die Gesamtzahl ist demnach $\# \text{Inv}(\sigma) + 2n$ mit $n = \sum_{i < j} n_{ij} \in \mathbb{N}$. QED

Anschauliches Beispiel: ein Kartrennen

Aufgabe: Ist der folgende Rennbericht glaubwürdig?

„Ein kurioses Rennen! Die Reihenfolge der sechs Wagen hat sich vom Start zum Ziel komplett umgekehrt. Dennoch war der Verlauf des Rennens eher langweilig, mit insgesamt nur 20 Überholmanövern.“

Lösung: Das ist unmöglich! Hier gilt nämlich $\text{inv}(\sigma) = \binom{6}{2} = \frac{6 \cdot 5}{2} = 15$. Möglich wären 15, 17, 19, 21, 23, ... Überholmanöver, aber niemals 20.

😊 Diese einfache Rechnung hat recht oft durchschlagende Wirkung. Genau um diese Parität geht es uns hier und in den folgenden Sätzen!

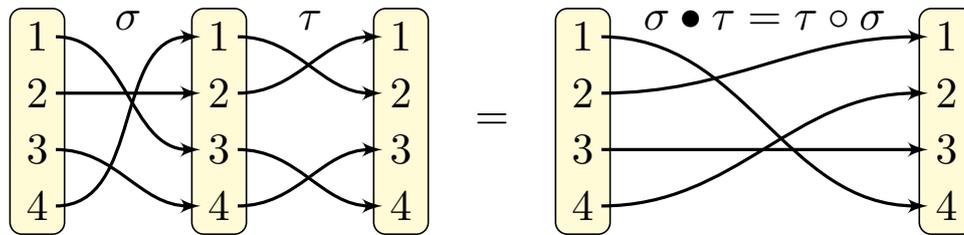
Definition L1A: Parität und Inversionen einer Permutation

Zu jeder Permutation $\sigma \in S_n$ definieren wir ihre **Parität**

$$\varepsilon : S_n \rightarrow \mathbb{Z}_2 = \{0, 1\} : \sigma \mapsto \text{inv}(\sigma) \bmod 2, \quad \text{wobei wie vereinbart}$$

$$\text{inv}(\sigma) := \# \text{Inv}(\sigma), \quad \text{Inv}(\sigma) := \{ \{i, j\} \subseteq X \mid i < j \wedge \sigma(i) > \sigma(j) \}.$$

Eine Permutation $\sigma \in S_n$ heißt **un/gerade**, falls $\text{inv}(\sigma)$ un/gerade ist.



(1) Wir betrachten eine Menge X und ihre **Selbstabbildungen**:

$$E_X = \text{End}(X) := \text{Abb}(X, X) = \{ f : X \rightarrow X \}$$

Graphisch ist die Rechtskomposition natürlicher, wie oben zu sehen; in Formeln schreiben wir $i \mapsto \sigma(i)$, da ist die Linkskomposition bequemer. Die Komposition definiert das Monoid $(E_X, \bullet, \text{id}_X)$ bzw. $(E_X, \circ, \text{id}_X)$, mit der Konvention $\sigma \bullet \tau = \tau \circ \sigma$ und $(\tau \circ \sigma)(i) = \tau(\sigma(i))$ für alle $i \in X$.

(2) Darin liegt die Gruppe der **Selbstbijektionen** aka **Permutationen**:

$$S_X = \text{Sym}(X) = \text{Aut}(X) := \text{End}(X)^\times = \text{Bij}(X, X) = \{ \sigma : X \xrightarrow{\sim} X \}.$$

Dies definiert die **symmetrische Gruppe** $(S_X, \bullet, \text{id}_X)$ bzw. $(S_X, \circ, \text{id}_X)$.

(3) Für $X = \{1, 2, \dots, n\}$ schreiben wir kurz $E_n := E_X$ und $S_n := S_X$.

Fehlstände der inversen Permutation

L106
Erläuterung

Beispiel L1B: Fehlstände der inversen Permutation

Für jede Permutation $\sigma \in S_n$ gilt $\text{Inv}(\sigma^{-1}) = \sigma(\text{Inv}(\sigma))$.

Die Anzahl der Fehlstände ist daher gleich: $\text{inv}(\sigma^{-1}) = \text{inv}(\sigma)$.

In Worten: Die Fehlstände $\text{Inv}(\sigma) \subseteq \binom{X}{2}$ notieren wir im Start von σ . Die Fehlstände von σ^{-1} sind das Bild der Fehlstände von σ . Ausführlich:

Ist $\sigma : X \xrightarrow{\sim} X$ bijektiv, so auch die Abbildung auf Paaren:

$$\sigma_2 : \binom{X}{2} \xrightarrow{\sim} \binom{X}{2} : \{i \neq j\} \mapsto \{k \neq l\} = \{\sigma(i) \neq \sigma(j)\}$$

Dazu stiftet die inverse Permutation σ^{-1} die Umkehrabbildung:

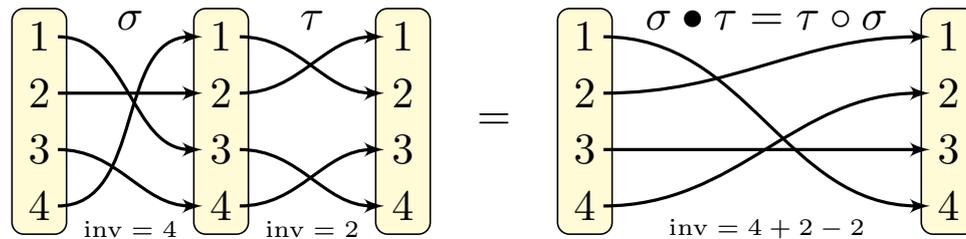
$$\sigma_2^{-1} : \binom{X}{2} \xrightarrow{\sim} \binom{X}{2} : \{k \neq l\} \mapsto \{i \neq j\} = \{\sigma^{-1}(i) \neq \sigma^{-1}(j)\}$$

Für jede Teilmenge $A \subseteq \binom{X}{2}$ schreiben wir dann kurz (siehe D233)

$$\sigma(A) = (\sigma_2)_*(A) = \{ \{\sigma(i), \sigma(j)\} \mid \{i, j\} \in A \},$$

$$\sigma^{-1}(A) = (\sigma_2^{-1})_*(A) = \{ \{\sigma^{-1}(k), \sigma^{-1}(l)\} \mid \{k, l\} \in A \}.$$

Die Parität ist ein Gruppenhomomorphismus.



Satz L1c: Die Parität ist ein Gruppenhomomorphismus.

(1) Bei Komposition von zwei Permutationen $\sigma, \tau \in S_n$ gilt:

$$\text{Inv}(\sigma \bullet \tau) = \text{Inv}(\tau \circ \sigma) = \text{Inv}(\sigma) \Delta \sigma^{-1}(\text{Inv}(\tau))$$

Hier steht Δ für die symmetrische Differenz $A \Delta B = (A \cup B) \setminus (A \cap B)$.

(2) Die Anzahl der Fehlstände ist additiv minus paarweise Auslöschung:

$$\text{inv}(\tau \circ \sigma) = \text{inv}(\sigma) + \text{inv}(\tau) - 2 \cdot \#[\text{Inv}(\sigma) \cap \sigma^{-1}(\text{Inv}(\tau))]$$

Jede Auslöschung entspricht zwei Inversionen, die sich aufheben.

(3) Die Parität ist somit ein Gruppenhomomorphismus:

$$\varepsilon : (S_n, \circ, \text{id}_X) \rightarrow (\mathbb{Z}_2, +, 0) : \sigma \mapsto \text{inv}(\sigma) \bmod 2$$

Die Parität ist ein Gruppenhomomorphismus.

Aufgabe: Erklären Sie diese Gleichungen in Worten und in Skizzen. Beweisen Sie diese Aussagen anschließend formal und ausführlich.

Lösung: (1) Das Paar $\{i \neq j\}$ wird invertiert von $\sigma \bullet \tau = \tau \circ \sigma$, wenn es entweder von σ oder anschließend von τ invertiert wird. Wird es zweimal invertiert, so endet es in gerader Reihenfolge.

(2) Die Anzahl der Fehlstände ist additiv minus der nötigen Korrektur: Jede Auslöschung entspricht zwei Inversionen, die sich aufheben.

(3) Daher ist die Anzahl $\text{inv}(\tau \circ \sigma)$ additiv modulo 2.

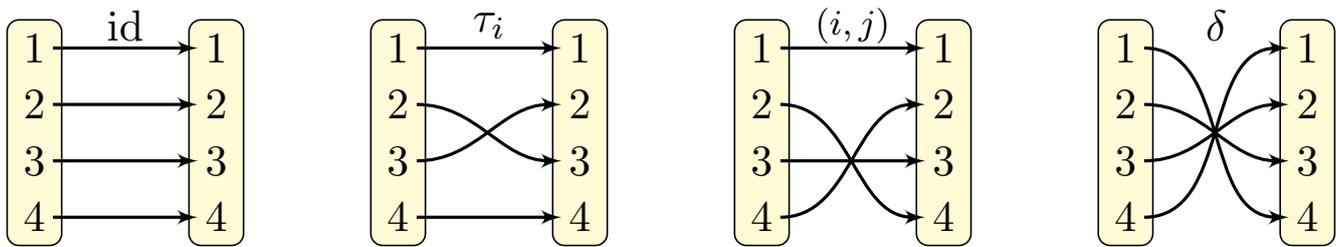
Beweis: (1) Es gilt $\{i \neq j\} \mapsto \{\sigma(i) \neq \sigma(j)\} \mapsto \{\tau(\sigma(i)) \neq \tau(\sigma(j))\}$. Genau dann endet dies in einem Fehlstand für $\sigma \bullet \tau = \tau \circ \sigma$, wenn *entweder* $\{i, j\}$ durch σ invertiert *oder* $\{\sigma(i), \sigma(j)\}$ durch τ invertiert.

(2) Für die symmetrische Differenz gilt $A \Delta B = (A \cup B) \setminus (A \cap B)$. Im endlichen Fall folgt $\#(A \Delta B) = \#A + \#B - 2 \cdot \#(A \cap B)$, siehe E2B.

(3) Additivität modulo 2 folgt sofort aus Aussage (2).

□ QED

Die extremen Permutationen



Lemma L1D: die extremen Permutationen

(0) Für jede Permutation $\sigma \in S_n$ gilt $\text{Inv}(\sigma) \subseteq \binom{X}{2}$, und somit

$$0 \leq \text{inv}(\sigma) \leq \binom{n}{2} = \frac{n(n-1)}{2}.$$

(1) Die beiden Extreme sind eindeutig:

(a) Genau dann gilt $\text{inv}(\sigma) = 0$, wenn $\sigma = \text{id} : i \mapsto i$.

(b) Genau dann gilt $\text{inv}(\sigma) = \binom{n}{2}$, wenn $\sigma = \delta : i \mapsto n + 1 - i$.

(2) Genau dann gilt $\text{inv}(\sigma) = 1$, wenn $\sigma = \tau_i := (i, i + 1)$ für ein i gilt.

Dies nennen wir eine **elementare** oder **fundamentale Transposition**.

(3) Für jede beliebige Transposition $\sigma = (i, j)$ gilt $\text{inv}(\sigma) = 2|i - j| - 1$, denn für $i < j$ haben wir $\text{Inv}(\sigma) = \{ \{i, j\} \} \cup \{ \{i, k\}, \{k, j\} \mid i < k < j \}$.

Die extremen Permutationen

Beweis: (0) Fehlstände sind Paare $\{i \neq j\} \subseteq X$. Dank E2I gilt:

$$\#\binom{X}{2} = \binom{n}{2} = \frac{n(n-1)}{2}$$

Wir charakterisieren die beiden Extreme:

(a) „ \Leftarrow “: Es gilt $\text{Inv}(\text{id}) = \emptyset$, also $\text{inv}(\text{id}) = 0$.

„ \Rightarrow “: Im Falle $\text{inv}(\sigma) = 0$ gibt es keine Fehlstände, also gilt $\sigma(1) = 1$, dann $\sigma(2) = 2$, usw. bis $\sigma(n) = n$.

(b) „ \Leftarrow “: Es gilt $\text{Inv}(\delta) = \binom{X}{2}$, also $\text{inv}(\delta) = \binom{n}{2}$.

„ \Rightarrow “: Im Falle $\text{inv}(\sigma) = \binom{n}{2}$ ist jedes Paar ein Fehlstand, also gilt $\sigma(1) = n$, dann $\sigma(2) = n - 1$, usw. bis $\sigma(n) = 1$.

(2) „ \Leftarrow “: Es gilt $\text{Inv}(\tau_i) = \{ \{i, i + 1\} \}$, also $\text{inv}(\tau_i) = 1$.

„ \Rightarrow “: Wir haben $\text{inv}(\sigma) = 1$, also $\text{Inv}(\sigma) = \{ \{i < j\} \}$.

Demnach gilt $\text{Inv}(\sigma \circ (i, j)) = \emptyset$, also $\sigma = (i, j)$ dank (1a).

Zudem wissen wir $\text{inv}(\sigma) \stackrel{(3)}{=} 2(j - i) - 1 \stackrel{!}{=} 1$, also $j = i + 1$.

(3) Die Berechnung von $\text{Inv}(\tau)$ und $\text{inv}(\tau)$ ist klar.

QED

Die Fundamentaltranspositionen erzeugen die symmetrische Gruppe:

$$S_n = \langle \tau_1 = (1, 2), \tau_2 = (2, 3), \dots, \tau_{n-1} = (n-1, n) \rangle$$

Satz L1E: Erzeugung durch Fundamentaltranspositionen

(0) Sei $\sigma \in S_n$ eine Permutation. Es gilt $\text{inv}(\tau_i) = 1$, dank L1C also

$$\text{inv}(\sigma \circ \tau_i) = \text{inv}(\sigma) \pm 1 \quad \text{und} \quad \text{inv}(\tau_i \circ \sigma) = \text{inv}(\sigma) \pm 1.$$

(1) Im Falle $\text{inv}(\sigma) > 0$ existieren $i, j \in \{1, \dots, n-1\}$ mit

$$\text{inv}(\sigma \circ \tau_i) = \text{inv}(\sigma) - 1 \quad \text{und} \quad \text{inv}(\tau_j \circ \sigma) = \text{inv}(\sigma) - 1.$$

(2) Jede Permutation $\sigma \in S_n$ ist ein Produkt der Form $\sigma = \tau_{i_1} \tau_{i_2} \cdots \tau_{i_\ell}$. Die minimale Länge $\ell \in \mathbb{N}$ ist $\text{inv}(\sigma)$. Allgemein gilt $\ell \in \text{inv}(\sigma) + 2\mathbb{N}$.

Beweis: (1a) Gilt $\sigma(1) < \sigma(2) < \dots < \sigma(n)$, so folgt $\sigma = \text{id}$, dank L1D. Im Falle $\text{inv}(\sigma) > 0$ gilt $\sigma \neq \text{id}$. Also existiert $i \in \{1, \dots, n-1\}$ mit $\sigma(i) > \sigma(i+1)$. Damit erreichen wir $\text{inv}(\sigma \circ \tau_i) = \text{inv}(\sigma) - 1$.

Erzeugung durch Fundamentaltranspositionen

(1b) Gilt $\sigma^{-1}(1) < \sigma^{-1}(2) < \dots < \sigma^{-1}(n)$, so folgt $\sigma = \text{id}$, dank L1D. Im Falle $\text{inv}(\sigma) > 0$ gilt $\sigma \neq \text{id}$. Also existiert $j \in \{1, \dots, n-1\}$ mit $\sigma^{-1}(j) > \sigma^{-1}(j+1)$. Damit erreichen wir $\text{inv}(\tau_j \circ \sigma) = \text{inv}(\sigma) - 1$.

(2) Dies folgt per Induktion über $\text{inv}(\sigma)$ dank (1). Die Ungleichung $\ell \geq \text{inv}(\sigma)$ und die Parität $\ell = \text{inv}(\sigma) + 2n$ folgen aus (0). □

😊 Das ist der mathematische Satz hinter unserem Kartrennen: Jede Zielreihenfolge σ kann durch Überholmanöver erreicht werden. Dazu sind mindestens $\text{inv}(\sigma)$ Überholmanöver $\tau_1, \dots, \tau_{n-1}$ notwendig. Die tatsächliche Anzahl ist eventuell größer, um eine gerade Zahl.

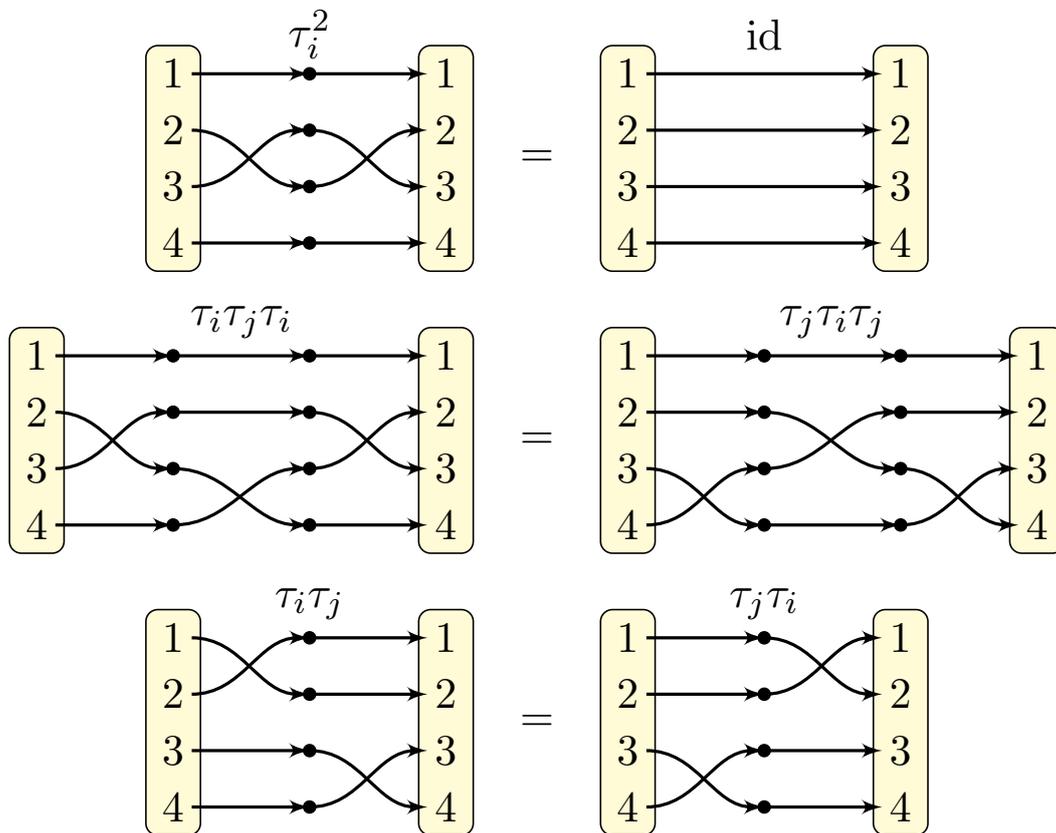
😊 Zur Beschreibung und Analyse dieser Situation haben wir nun eine gute Notation: bequem und genau. Der Satz präzisiert die Aussagen.

😊 Die Fundamentaltranspositionen $\tau_1, \tau_2, \dots, \tau_{n-1} \in S_n$ erzeugen die gesamte symmetrische Gruppe S_n . Zudem können wir für jede Permutation σ die benötigte Länge genau angeben.

Übung: (3) Bestimmen Sie Inv und inv zu $\delta \circ \sigma$ und $\sigma \circ \delta$.

(4) Existieren i, j mit $\text{inv}(\sigma \circ \tau_i) = \text{inv}(\tau_j \circ \sigma) = \text{inv}(\sigma) + 1$?

Die fundamentalen Relationen



Für die Fundamentaltranspositionen $\tau_1, \dots, \tau_{n-1}$ gelten die Relationen $\tau_i^2 = \text{id}$ sowie $\tau_i \tau_j \tau_i = \tau_j \tau_i \tau_j$ für $|i - j| = 1$ und $\tau_i \tau_j = \tau_j \tau_i$ für $|i - j| \geq 2$.

Die fundamentalen Relationen

Übung: Schreiben Sie diese Graphiken in Zykelschreibweise aus und rechnen Sie so nach, dass diese Relationen allgemein gelten.

😊 Die Relation $\tau_i^2 = \text{id}$ besagt lediglich, dass τ_i die Ordnung 2 hat. Dies gilt für jede beliebige Transposition, also insbesondere auch hier.

😊 Die zweite Relation $\tau_i \tau_j \tau_i = \tau_j \tau_i \tau_j$ für $|i - j| = 1$ ist Artins berühmte Zopfrelation; sie tritt hier natürlich für benachbarte Transpositionen auf.

😊 Die letzte Relation kennen Sie bereits im allgemeineren Kontext: Je zwei disjunkte Permutationen kommutieren (E1B).

Übung: Diese Relationen respektieren die Parität: Modulo 2 ist die Anzahl der Kreuzungen / Transpositionen auf beiden Seiten gleich! Das zeigt graphisch-anschaulich den Ursprung dieser Invariante.

Übung: Sei $h : (S_n, \circ, \text{id}_X) \rightarrow (A, \cdot, 1)$ ein Homomorphismus in eine abelsche Gruppe und $a = h(\tau_1) \in A$ das Bild von τ_1 . Dann gilt $a^2 = 1$ und $h(\sigma) = a^{\varepsilon(\sigma)}$ für alle $\sigma \in S_n$. **Hinweis:** Nutzen Sie die fundamentalen Relationen und zeigen Sie $h(\tau_i) = a$. Schließen Sie mit Satz L1E.

Satz L1F: Präsentation durch Erzeuger und Relationen

Die symmetrische Gruppe S_n lässt sich wie folgt präsentieren durch Erzeuger und Relationen:

$$S_n = \left\langle \tau_1, \dots, \tau_{n-1} \mid \begin{array}{ll} \tau_i^2 = 1 & \text{für alle } i \\ \tau_i \tau_j \tau_i = \tau_j \tau_i \tau_j & \text{für } |i - j| = 1 \\ \tau_i \tau_j = \tau_j \tau_i & \text{für } |i - j| \geq 2 \end{array} \right\rangle$$

Das beinhaltet zwei Aussagen: (1) Jede Permutation $\sigma \in S_n$ ist ein Produkt der Fundamentaltranspositionen $\tau_1, \dots, \tau_{n-1}$ (Satz L1E).

(2) Eine solche Darstellung ist nicht eindeutig: Genau dann stellen zwei solche Produkte dieselbe Permutation σ dar, wenn sie sich durch die angegebenen Relationen ineinander überführen lassen.

Dieser Satz lässt sich graphisch sehr direkt und anschaulich verstehen und so auch beweisen! (Genauso formuliert und beweist man Artins Präsentation der Zopfgruppe in der Geometrischen Topologie.)

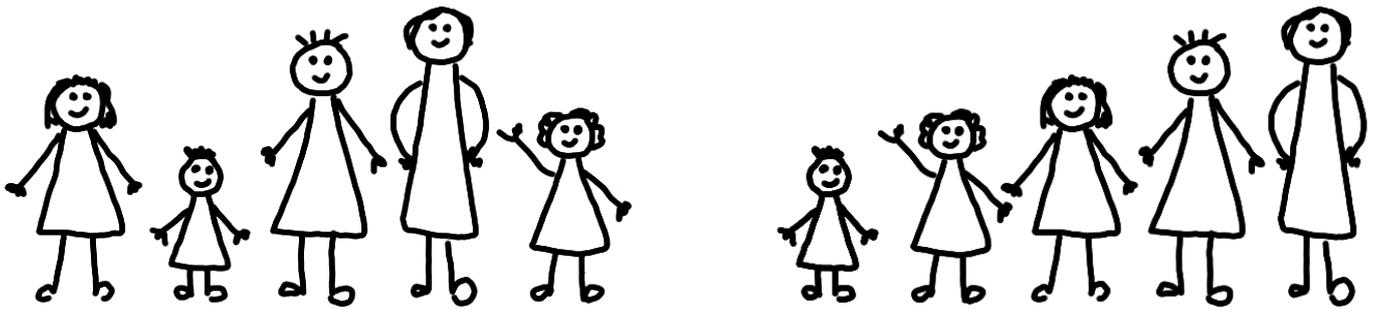
Anschaulich gesagt: Ein Wort in den elementaren Transpositionen $\tau_1, \dots, \tau_{n-1}$, das sie hier graphisch ablesen, beschreibt den Verlauf des Rennens. Der Rennverlauf legt das Ergebnis σ eindeutig fest.

Umgekehrt legt das Ergebnis σ den Rennverlauf *nicht* eindeutig fest, und den Unterschied sehen Sie hier: Er entsteht genau durch die hier gezeigten Relationen; diese führen vom einen zum anderen Verlauf.

Sie sehen also: In unserem anschaulichen Beispiel des Kartrennens steckt elementare, doch wunderschöne Mathematik: die Theorie der symmetrischen Gruppe und der elementaren Transpositionen.

😊 Das ist schön und nützlich, damit können Sie wunderbar rechnen.

In Zukunft werden Sie ein Rennen nie mehr mit denselben Augen sehen, sondern den mathematischen Kern durchschauen können.



Probleme mit Unordnung und Umordnung begegnen Ihnen sicher öfters!

Nehmen Sie zum Beispiel an, dass Sie eine bestehende Reihenfolge sortieren wollen und dabei nur Nachbarn vertauschen wollen / können. Wie stellen Sie das an? mit möglichst wenigen Vertauschungen? Vermutlich lösen Sie das Problem intuitiv genau richtig!

In diesem Fall misst die Anzahl der Fehlstände die Komplexität des Problems. Der Satz L1E sagt Ihnen genau, wie es geht, und dass es nicht besser gehen kann. Damit ist dieses Problem vollständig gelöst.

Wozu brauchen wir die Theorie, wenn alles so anschaulich gelingt?

Erstens: Wir brauchen eine gute Notation, um Daten und Operationen präzise zu beschreiben, hier also Permutationen und Vertauschungen. Nur so können wir die Strukturen klären und dazu Aussagen beweisen.

Zweitens: Meist möchten Sie Ihr Vorgehen einem Computer übertragen, einen allgemein gültigen Algorithmus entwickeln und programmieren. Hier hilft Mathematik durch gute Notation und beweisbare Aussagen.

Drittens: Wer garantiert Ihnen, dass die Sortierung durch einen Trick nicht doch mit weniger Nachbarschaftsvertauschungen möglich ist? Für kleine Daten scheint alles klar, doch für große Datenmengen wird das Problem schnell unübersichtlich. Satz L1E schafft Sicherheit.

Bemerkung: Ein guter Sortieralgorithmus, der auf Vertauschung von Nachbarn beruht, benötigt schlimmstenfalls $n(n-1)/2$ Vertauschungen. Noch besser gelingt es, wenn wir beliebige Vertauschungen zulassen. Hier sind $\approx n \ln n$ paarweise Vergleiche das Optimum.

Satz L1G: Erzeugendensysteme für S_n .

Die Transpositionen in S_n erzeugen die symmetrische Gruppe S_n .
Ebenso gilt $S_n = \langle E_n^s \rangle$ für jede der folgenden Familien:

$$E_n^1 = \{ (i, j) \mid i < j \}$$

$$E_n^2 = \{ (1, 2), (1, 3), \dots, (1, n) \}$$

$$E_n^3 = \{ (1, 2), (2, 3), \dots, (n-1, n) \}$$

$$E_n^4 = \{ (1, 2), (1, 2, \dots, n) \}$$

Insbesondere lässt sich die Gruppe S_n durch zwei Elemente erzeugen.

Aufgabe: Beweisen Sie diese Aussagen!

Hinweis: Wir betrachten die symmetrischen Gruppen als Teilmengen $\{\text{id}\} = S_0 = S_1 \subset S_2 \subset \dots \subset S_n \subset \dots$ und nutzen Induktion über $n \in \mathbb{N}$.
Formal gelingt dies durch $S_n = \{ \sigma : \mathbb{N} \xrightarrow{\sim} \mathbb{N} \mid \text{supp}(\sigma) \subseteq \{1, \dots, n\} \}$.

Beweis: (1) Sei $G_n = \langle E_n^s \rangle \leq S_n$ die erzeugte Untergruppe.

Die entscheidenden zwei Eigenschaften der Familie E_n^s sind:

- 1 Zu jedem Element $i \in \{1, \dots, n\}$ existiert $\rho \in G_n$ mit $\rho(i) = n$.
- 2 Es gilt $G_{n-1} \leq G_n$, so dass wir induktiv vorgehen können.

Das ist jeweils sorgsam zu prüfen und gelingt meist leicht.

Für $s = 1, 2, 3$ gilt sogar $E_{n-1}^s \subseteq E_n^s$, somit $\langle E_{n-1}^s \rangle \subseteq \langle E_n^s \rangle$.

Lediglich für $s = 4$ ist die Eigenschaft (2) nicht offensichtlich.

(2) Wir zeigen nun $S_n \leq G_n$ per Induktion über n .

Die Aussage ist trivial für $n \leq 1$. Sei also $n \geq 2$.

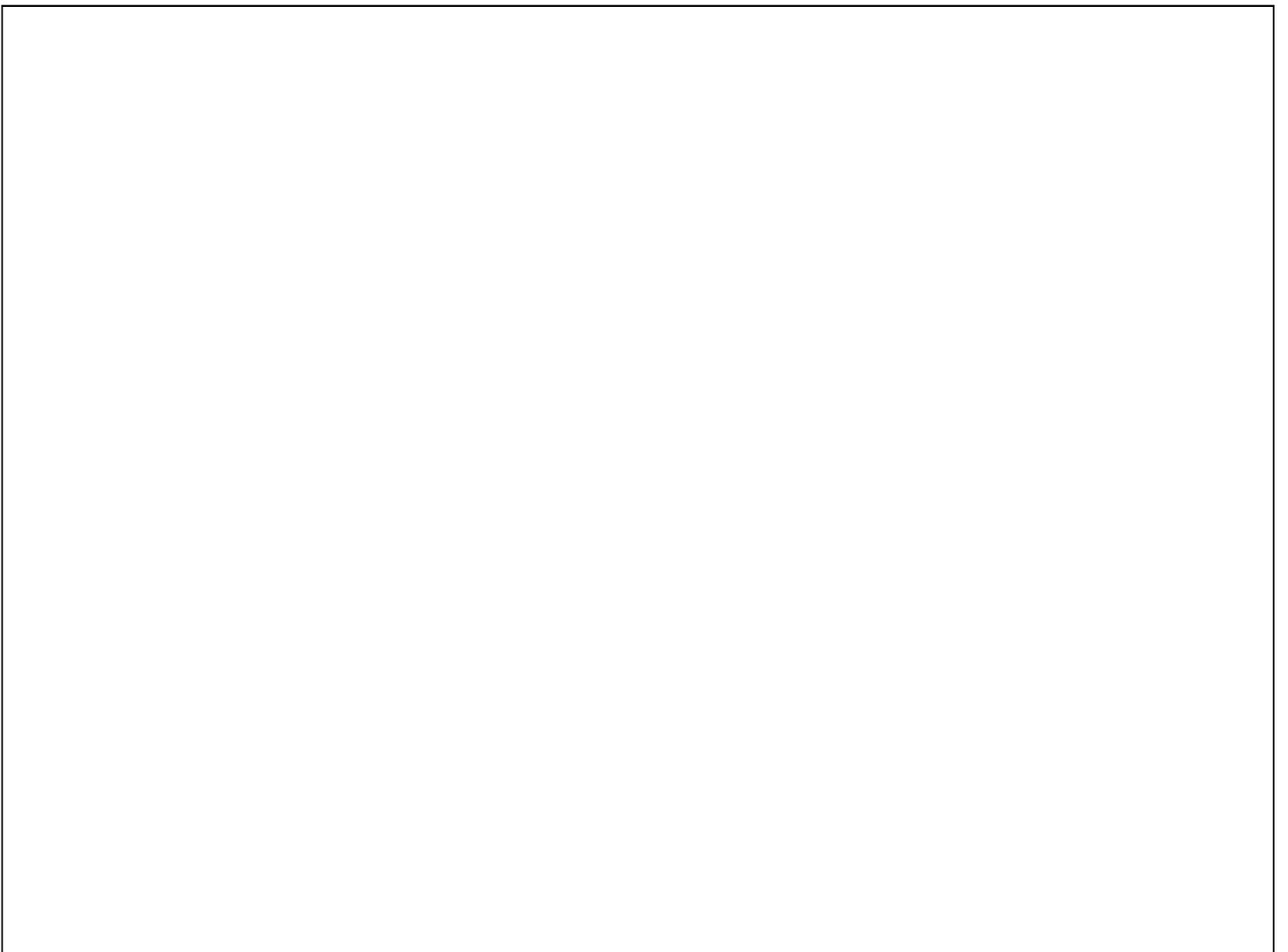
Die Aussage $S_{n-1} \leq G_{n-1}$ sei bereits bewiesen.

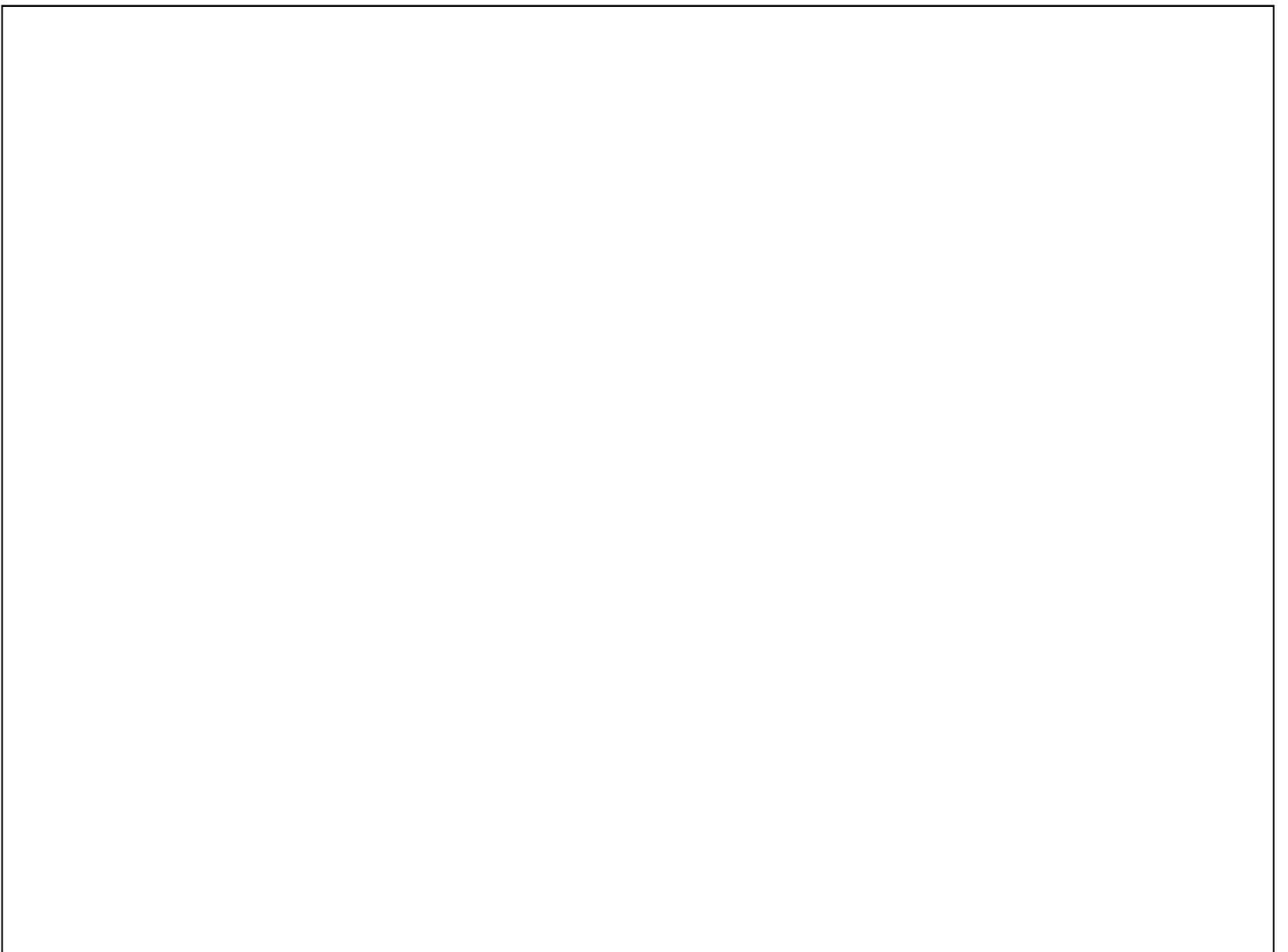
Sei $\sigma \in S_n$. Zu $i := \sigma(n)$ wählen wir $\rho \in G_n \leq S_n$ mit $\rho(i) = n$.

Somit gilt $(\rho \circ \sigma)(n) = n$, also $\rho \circ \sigma \in S_{n-1} \leq G_{n-1} \leq G_n$.

Daraus folgt $\sigma \in \rho^{-1} \circ G_n = G_n$. Wir schließen $S_n \leq G_n$.

□ QED





Die Signatur einer Selbstabbildung

Satz L1H: die Signatur einer Selbstabbildung

Zu $n \in \mathbb{N}$ betrachten wir die endliche Menge $X = \{1, \dots, n\} \subset \mathbb{N} \subset \mathbb{Q}$.

(0) Zu jeder Selbstabbildung $f : X \rightarrow X$ definieren wir die **Signatur**

$$\text{sign}(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \in \{\pm 1, 0\}.$$

Dies heißt auch **Signum** oder **Vorzeichen** von f .

(1) Die Signatur ist multiplikativ, das heißt $\text{sign}(g \circ f) = \text{sign}(g) \cdot \text{sign}(f)$ für alle $f, g : X \rightarrow X$. Wir haben also einen Monoidhomomorphismus

$$\text{sign} = \text{sign}_X : (\mathbb{E}_X, \circ, \text{id}_X) \rightarrow (\{\pm 1, 0\}, \cdot, 1) : f \mapsto \text{sign}(f)$$

(2) Genau dann ist $f \in \mathbb{E}_X$ invertierbar, wenn $\text{sign}(f) \in \{\pm 1, 0\}$ dies ist. Durch Einschränkung erhalten wir so den Gruppomorphismus

$$\text{sign} = \text{sign}_X : (\mathbb{S}_X, \circ, \text{id}_X) \rightarrow (\{\pm 1\}, \cdot, 1) : \sigma \mapsto \text{sign}(\sigma).$$

Die Signatur einer Selbstabbildung

Die bequeme Kurzschreibweise $\{i \neq j\}$ bedarf der Erläuterung.

$$\text{sign}(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j}$$

Das Produkt erstreckt sich über alle (ungeordneten) Paare $\{i, j\} \in \binom{X}{2}$, also zweielementige Mengen $\{i, j\} \subseteq X$, und das bedeutet $i \neq j$.

Jeder Faktor ist wohldefiniert, da invariant unter Vertauschung:

$$\{i, j\} \mapsto \frac{f(i) - f(j)}{i - j} = \frac{f(j) - f(i)}{j - i}$$

Wir können jede Paarmenge $\{i, j\}$ sortieren und erhalten

$$\text{sign}(f) = \prod_{\{i < j\}} \frac{f(i) - f(j)}{i - j}.$$

Das ist dasselbe Produkt wie oben: Die Indexmenge ist dieselbe und die Faktoren sind dieselben. Nur die Schreibweise hat sich geändert.

Beide Schreibweisen haben jeweils ihre Vorteile.

Die Signatur einer Selbstabbildung

Beweis: (0) Zur Wohldefiniertheit müssen wir zeigen:

$$\text{sign}(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \in \{\pm 1, 0\}$$

Für $f : X \rightarrow X$ sind bijektiv, surjektiv, injektiv äquivalent (Zahlsatz E1H).

(0a) Ist f nicht injektiv, so gibt es $i \neq j$ mit $f(i) = f(j)$, also:

$$\text{sign}(f) = 0$$

(0b) Ist $f : X \xrightarrow{\sim} X$ bijektiv, so auch die Abbildung auf Paaren (E2I):

$$f_2 : \binom{X}{2} \xrightarrow{\sim} \binom{X}{2} : \{i \neq j\} \mapsto \{k \neq \ell\} = \{f(i) \neq f(j)\}$$

Die Umkehrfunktion zu f_2 ist $(f_2)^{-1} = (f^{-1})_2$. Daraus folgt:

$$|\text{sign}(f)| = \prod_{\{i \neq j\}} \frac{|f(i) - f(j)|}{|i - j|} = \frac{\prod_{\{k \neq \ell\}} |k - \ell|}{\prod_{\{i \neq j\}} |i - j|} = 1$$

Die Signatur einer Selbstabbildung

(1) Wir zeigen nun für alle $f, g : X \rightarrow X$ die Multiplikativität

$$\text{sign}(g \circ f) = \text{sign}(g) \cdot \text{sign}(f).$$

(1a) Ist f nicht injektiv, so ist auch $g \circ f$ nicht injektiv, also gilt

$$\text{sign}(g \circ f) = 0 \quad \text{und} \quad \text{sign}(g) \cdot \text{sign}(f) = 0.$$

(1b) Ist $f : X \xrightarrow{\sim} X$ hingegen bijektiv, so finden wir

$$\begin{aligned} \text{sign}(g \circ f) &= \prod_{\{i \neq j\}} \frac{g(f(i)) - g(f(j))}{i - j} \\ &= \prod_{\{i \neq j\}} \frac{g(f(i)) - g(f(j))}{f(i) - f(j)} \cdot \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \\ &= \prod_{\{k \neq \ell\}} \frac{g(k) - g(\ell)}{k - \ell} \cdot \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \\ &= \text{sign}(g) \cdot \text{sign}(f) \end{aligned}$$

Das gigantische Produkt aus L1H dient zur *Konstruktion* der Signatur, zur *Berechnung* nutzen Sie es lieber nicht, das wäre zu aufwändig. Dazu entwickeln wir gleich effizientere Methoden, siehe Satz L1K. Zuvor diskutieren wir eine konzise Beschreibung der Signatur:

Satz L1I: Charakterisierung der Signatur

Sei $n \in \mathbb{N}_{\geq 2}$ und $X = \{1, \dots, n\}$ und hierauf $\tau_1 = (1, 2)$.

(1) Die Signatur $\text{sign} : (\mathbb{E}_X, \circ, \text{id}_X) \rightarrow (\mathbb{C}, \cdot, 1)$ ist multiplikativ und erfüllt $\text{sign}(\tau_1) = -1$. Diese Eigenschaft charakterisiert die Signatur eindeutig!

(2) Die Signatur ist der einzige surjektive Gruppenhomomorphismus

$$\text{sign} : (S_X, \circ, \text{id}_X) \twoheadrightarrow (\{\pm 1\}, \cdot, 1).$$

(3) Sei $h : (S_X, \circ, \text{id}_X) \rightarrow (A, \cdot, 1)$ ein Gruppenhomomorphismus in eine abelsche Gruppe und $a = h(\tau_1)$. Dann gilt $h(\sigma) = a^{\varepsilon(\sigma)}$ für alle $\sigma \in S_X$.

Aufgabe: Beweisen Sie diese Aussagen. *Tipp:* Beginnen Sie mit (3).

Lösung: (3) Zu je zwei Punkten $i \neq j$ in X existiert eine Permutation $\tau \in S_X$ mit $\tau(i) = 1$ und $\tau(j) = 2$. Somit gilt $(i, j) = \tau^{-1} \circ (1, 2) \circ \tau$, also $h(i, j) = h(\tau)^{-1} \cdot h(1, 2) \cdot h(\tau) = h(1, 2)$, da $(A, \cdot, 1)$ abelsch ist.

Wegen $(1, 2)^2 = \text{id}$ in S_X gilt $a^2 = 1$ in A , demnach hat a die Ordnung 2. Jede Permutation $\sigma \in S_X$ ist ein Produkt von ℓ Transpositionen (L1E). Demnach gilt $h(\sigma) = a^\ell = a^{\varepsilon(\sigma)}$ für die Parität $\varepsilon(\sigma) = \ell \pmod 2$.

(1) Die Existenz der Signatur $\text{sign} : (\mathbb{E}_X, \circ, \text{id}_X) \rightarrow (\mathbb{C}, \cdot, 1)$ haben wir in Satz L1H geklärt. Sie ist multiplikativ und erfüllt $\text{sign}(\tau_1) = -1$.

Die Eindeutigkeit folgt aus (3): Sei $h : (\mathbb{E}_X, \circ, \text{id}_X) \rightarrow (\mathbb{C}, \cdot, 1)$ multiplikativ mit $h(\tau_1) = -1$. Dann gilt $h(\sigma) = (-1)^{\varepsilon(\sigma)} = \text{sign}(\sigma)$ für alle $\sigma \in S_X$.

Zu $\sigma \in \mathbb{E}_X \setminus S_X$ existieren $i \neq j$ in X mit $\sigma(i) = \sigma(j)$, also $\sigma = \sigma \circ (i, j)$. Somit gilt $h(\sigma) = h(\sigma) \cdot h(i, j) = -h(\sigma)$, also $h(\sigma) = 0 = \text{sign}(\sigma)$.

(2) Sei $h : (S_X, \circ, \text{id}_X) \twoheadrightarrow (\{\pm 1\}, \cdot, 1)$ ein Gruppenhomomorphismus.

Wir unterscheiden die beiden Fälle $h(\tau_1) \in \{\pm 1\}$ und nutzen (3):

(2a) Im Falle $h(\tau_1) = 1$ ist h trivial, denn $h(\sigma) = 1^{\varepsilon(\sigma)} = 1$ für alle $\sigma \in S_X$.

(2b) Im Falle $h(\tau_1) = -1$ gilt $h = \text{sign}$, denn $h(\sigma) = (-1)^{\varepsilon(\sigma)} = \text{sign}(\sigma)$.

Zu $n \in \mathbb{N}_{\geq 2}$ existieren genau zwei Gruppenhomomorphismen

$$1, \text{sign} : (S_n, \circ, \text{id}) \rightarrow (\{\pm 1\}, \cdot, 1),$$

nämlich neben der konstanten Einsabbildung nur die Signatur.

Korollar L1J: Signatur als Abelschmachung

Die Signatur $\text{sign} : (S_n, \circ, \text{id}) \rightarrow (\{\pm 1\}, \cdot, 1)$ ist ein Homomorphismus in die abelsche Gruppe $(\{\pm 1\}, \cdot, 1)$ und in folgendem Sinne universell:

$$\begin{array}{ccc} (S_n, \circ, \text{id}) & & \\ \text{sign} \downarrow & \searrow h & \\ (\{\pm 1\}, \cdot, 1) & \xrightarrow{\exists! g} & (A, \cdot, 1) \end{array}$$

Zu jedem Homomorphismus $h : (S_n, \circ, \text{id}) \rightarrow (A, \cdot, 1)$ in eine abelsche Gruppe existiert genau ein Homomorphismus $g : (\{\pm 1\}, \cdot, 1) \rightarrow (A, \cdot, 1)$ mit $h = g \circ \text{sign}$. Das heißt, g macht das obige Diagramm kommutativ.

Beweis: (1) Eindeutigkeit: Sei g ein Homomorphismus mit $h = g \circ \text{sign}$. Es folgt $g(+1) = 1$ und $g(-1) = g(\text{sign}(\tau)) = h(\tau)$ für jede Transposition $\tau \in S_n$. Transpositionen existieren dank der Voraussetzung $n \geq 2$. Das legt g eindeutig fest, also gibt es höchstens eine Lösung g .

(2) Wir zeigen die Existenz von g durch die folgende Konstruktion. Wir setzen $a := h(\tau)$ und damit $g(+1) = 1$ sowie $g(-1) = a$. Wegen $\tau^2 = \text{id}$ in S_n gilt $a^2 = 1$ in A , also ist g ein Gruppenhomomorphismus. Dank L1I gilt dann $h(\sigma) = a^{\varepsilon(\sigma)} = g(\text{sign}(\sigma))$ für alle $\sigma \in S_n$. □

Satz L1K: effiziente Berechnung der Signatur

- (1) Für jede Permutation $\sigma \in S_X$ gilt $\text{sign}(\sigma) = (-1)^{\text{inv}(\sigma)} = (-1)^{\varepsilon(\sigma)}$.
- (2) Für jede Transposition $\tau = (a, b) \in S_X$ gilt somit $\text{sign}(\tau) = -1$.
- (3) Für jeden ℓ -Zykel $\sigma = (a_1, a_2, \dots, a_\ell) \in S_X$ gilt $\text{sign}(\sigma) = (-1)^{\ell-1}$.

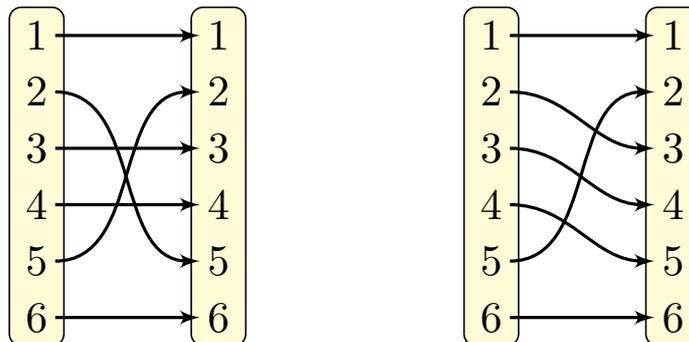
Beispiel: Aus der Zykelzerlegung E1C lässt sich die Signatur ablesen.

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 3 & 8 \end{bmatrix} = \underset{+}{(1)} \underset{-}{(2, 5, 4, 7)} \underset{+}{(6)} \underset{+}{(3, 9, 8)}$$

- 😊 Das ist die bequemste und effizienteste Berechnung der Signatur. (Jedes Produkt von Zykeln genügt hier, es muss nicht disjunkt sein.)
- 😊 Die Untersuchung aller Paare $\{i \neq j\}$ hat quadratischen Aufwand, denn $\binom{n}{2} = \frac{n(n-1)}{2}$. Die Konstruktion der Zykel hat linearen Aufwand.
- 😊 Zykelregel L1K und Multiplikativität L1H kommen auch ganz ohne Hilfsstruktur aus und gelten allgemein auf jeder Menge Y (Satz L1O).

Effiziente Berechnung der Signatur

Beispiele:



Beweis: (1) Wir wissen bereits $\text{sign}(\sigma) \in \{\pm 1\}$, daher gilt:

$$\text{sign}(\sigma) = \prod_{\{i \neq j\}} \underbrace{\frac{\sigma(i) - \sigma(j)}{i - j}}_{< 0 \text{ gdw } \{i, j\} \in \text{Inv}(\sigma)} = (-1)^{\text{inv}(\sigma)}$$

(2) Für $\tau = (a, b)$ gilt $\text{inv}(\tau) = 2 |a - b| - 1$, siehe L1D. Dank (1) folgt

$$\text{sign}(\tau) = (-1)^{\text{inv}(\tau)} = -1.$$

(3) Wir haben $\sigma = (a_1, a_2, \dots, a_\ell) = (a_1, a_2) \circ (a_2, a_3) \circ \dots \circ (a_{\ell-1}, a_\ell)$. Dank (2) und Multiplikativität L1H folgt $\text{sign}(\sigma) = (-1)^{\ell-1}$. QED

Aufgabe: Formulieren Sie einen effizienten Algorithmus (wie E1c) zur Berechnung der Signatur $\text{sign}(\sigma)$ von $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. Gelingt es mit linearem Aufwand in n ? Aufwand $\binom{n}{2}$ ist nicht optimal!

Algo L1L: Berechnung der Signatur

Eingabe: eine Abbildung $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$

Ausgabe: die Signatur $\text{sign}(\sigma) = s \in \{\pm 1, 0\}$

```

1:  $s \leftarrow +1$ ;  $\text{visited} \leftarrow (0, \dots, 0) \in \{0, 1\}^n$  // markiere besuchte Punkte
2: for  $i$  from 1 to  $n$  do // durchlaufe alle Punkte
3:   if  $\text{visited}[i] = 0$  then // falls neuer Zykel...
4:      $j \leftarrow i$ ;  $s \leftarrow -s$  // eröffne den Zykel
5:     repeat // durchlaufe den Zykel...
6:        $j \leftarrow \sigma(j)$ ;  $s \leftarrow -s$  // nächster Punkt des Zyklus
7:       if  $\text{visited}[j] = 1$  then return 0 //  $\sigma$  ist nicht injektiv
8:        $\text{visited}[j] \leftarrow 1$  // markiere als besucht
9:     until  $j = i$  // schließe den Zykel
10: return  $s$  // Signatur mitgezählt

```

Bemerkung L1M: die Signatur und ihre Hilfsstrukturen

Zur **Konstruktion** der Signatur nutzen wir zusätzliche Struktur:

- Eine totale Ordnung $(X, \leq) = \{1 < 2 < \dots < n\}$: Damit definieren wir die Menge $\text{Inv}(\sigma)$ der Fehlstände und zeigen kombinatorisch, dass die Parität (L1A) ein Gruppenhomomorphismus ist (L1C).
- Eine Einbettung $X \hookrightarrow K$ in einen Körper K , etwa $X \subset \mathbb{Q}$: Damit stellen wir die Signatur als ein Produkt dar (L1H) und weisen algebraisch ihre Multiplikativität in K nach.

Im geordneten Körper (\mathbb{Q}, \leq) treffen beide Methoden zusammen.

Zur effizienten **Berechnung** der Signatur jedoch sind diese Strukturen schließlich gar nicht mehr notwendig, wie der obige Algorithmus zeigt. Die Ordnung auf $X = \{1, 2, \dots, n\}$ nutzen wir nur noch zur Organisation der Schleife und zu unserer Buchhaltung. Der folgende Satz erklärt dies.

Die Signatur einer Selbstabbildung

Gegeben sei eine beliebige endliche Menge Y mit $n = \#Y < \infty$.

Wie definieren wir die Signatur $\text{sign}_Y : (\mathbb{E}_Y, \circ, \text{id}_Y) \rightarrow (\{\pm 1, 0\}, \cdot, 1)$?

Wir wählen willkürlich irgendeine Abzählung $\nu : X = \{1, \dots, n\} \xrightarrow{\sim} Y$.

$$\begin{array}{ccc}
 X & \xrightarrow{\quad f \quad} & X \\
 \left. \begin{array}{c} \uparrow \\ \nu \cong \\ \downarrow \end{array} \right\} \nu^{-1} & & \left. \begin{array}{c} \uparrow \\ \nu \cong \\ \downarrow \end{array} \right\} \nu^{-1} \\
 & \begin{array}{c} \varphi \updownarrow \psi \\ g \end{array} & \\
 Y & \xrightarrow{\quad g \quad} & Y
 \end{array}$$

Lemma L1N: $X \cong Y$ impliziert $S_X \cong S_Y$

Jede Bijektion $\nu : X \xrightarrow{\sim} Y$ stiftet einen Isomorphismus

$$\begin{aligned}
 (\varphi, \psi) : (\mathbb{E}_X, \circ, \text{id}_X) &\cong (\mathbb{E}_Y, \circ, \text{id}_Y) \\
 &: (S_X, \circ, \text{id}_X) \cong (S_Y, \circ, \text{id}_Y)
 \end{aligned}$$

mit $\varphi : f \mapsto g = \nu \circ f \circ \nu^{-1}$ und $\psi : g \mapsto f = \nu^{-1} \circ g \circ \nu$.

Die Signatur einer Selbstabbildung

Beweis: Die Aussage ist klar. Falls nicht, so ist es eine gute Übung: Alle Daten liegen explizit vor, es genügt sorgsames Nachrechnen!

Aufgabe: Führen Sie den behaupteten Isomorphismus aus.

Lösung: Es gilt $\psi(\varphi(f)) = \nu^{-1} \circ (\nu \circ f \circ \nu^{-1}) \circ \nu = f$ und ebenso $\varphi(\psi(g)) = g$. Wir haben also ein Bijektionspaar $(\varphi, \psi) : \mathbb{E}_X \cong \mathbb{E}_Y$.

Die Abbildung φ respektiert die Komposition: Es gilt $\varphi(\text{id}_X) = \text{id}_Y$ und

$$\varphi(f' \circ f) = \nu \circ f' \circ f \circ \nu^{-1} = \nu f' \nu^{-1} \circ \nu f \nu^{-1} = \varphi(f') \circ \varphi(f).$$

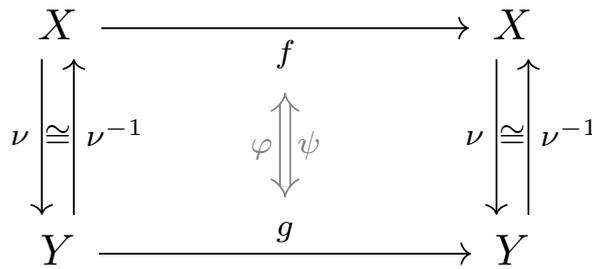
Gleiches gilt für ψ . Also haben wir ein Isomorphismenpaar (φ, ψ) . QED

😊 Auf der „nackten“ Menge Y haben wir zunächst keinerlei Struktur; diese führen wir durch unsere „Koordinaten“ $\nu : X \xrightarrow{\sim} Y$ erst ein.

😊 Ich erkläre dieses Vorgehen hier betont ausführlich, in Zeitlupe. Wir werden dies später für die Determinante genauso ausführen. Daher ist es gut, mit der leichter fasslichen Signatur zu üben.

Die Signatur einer Selbstabbildung

Als Hilfskonstrukt wählen wir eine Abzählung $\nu : X = \{1, \dots, n\} \xrightarrow{\sim} Y$.



Satz L10: die Signatur einer Selbstabbildung

(0) Mit der Abzählung $\nu : X = \{1, \dots, n\} \xrightarrow{\sim} Y$ definieren wir

$$\text{sign}_Y : E_Y \rightarrow \{\pm 1, 0\} : g \mapsto \text{sign}_Y(g) := \text{sign}_X(\nu^{-1} \circ g \circ \nu).$$

Diese Abbildung sign_Y ist wohldefiniert, das heißt unabhängig von ν .

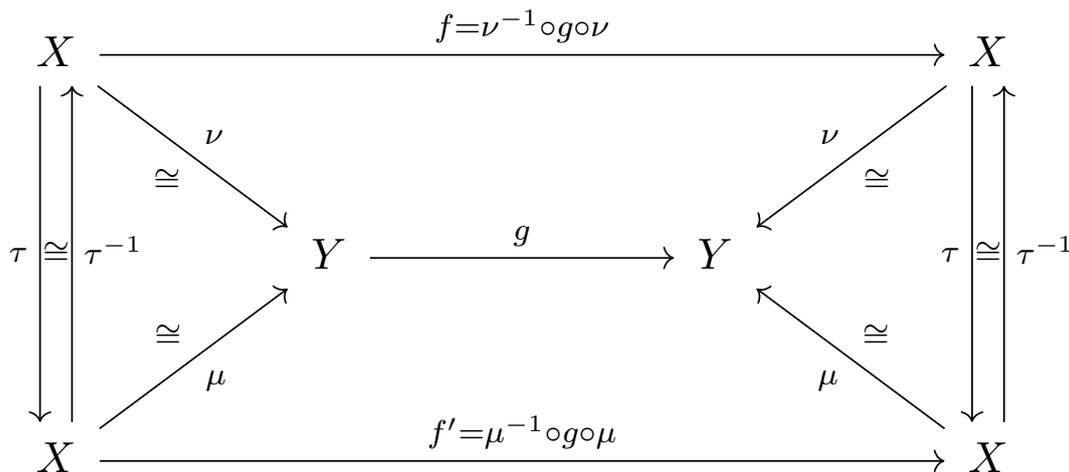
(1) Wir erhalten so den ersehnten Monoidhomomorphismus

$$\text{sign}_Y = \text{sign}_X \circ \psi : (E_Y, \circ, \text{id}_Y) \rightarrow (\{\pm 1, 0\}, \cdot, 1).$$

Weiterhin gilt die Zykelregel L1k zur effizienten Berechnung.

Invarianz der Signatur

Beweis: (0) Wir vergleichen zwei Bijektionen $\mu, \nu : X \xrightarrow{\sim} Y$:



Wir haben $f' = \tau \circ f \circ \tau^{-1}$ mit $\tau = \mu^{-1} \circ \nu : X \xrightarrow{\sim} X$, also:

$$\text{sign}_X(f') = \text{sign}_X(\tau) \cdot \text{sign}_X(f) \cdot \text{sign}_X(\tau)^{-1} = \text{sign}_X(f)$$

Somit ist die Signatur $\text{sign}_Y(g) := \text{sign}_X(f) = \text{sign}_X(f')$ wohldefiniert, da unabhängig von den willkürlich gewählten Abzählungen ν, μ . QED

Die alternierende Gruppe

Sei X eine endliche Menge, etwa $X = \{1, \dots, n\}$ als Standardmodell. Für Selbstabbildungen $f : X \rightarrow X$ haben wir die **Signatur** (L1H/L1O), und sie ist ein Homomorphismus von Monoiden bzw. Gruppen:

$$\begin{aligned} \text{sign} = \text{sign}_X & : (\mathbb{E}_X, \circ, \text{id}_X) \rightarrow (\{\pm 1, 0\}, \cdot, 1) : f \mapsto \text{sign}(f) \\ & : (\mathbb{S}_X, \circ, \text{id}_X) \rightarrow (\{\pm 1\}, \cdot, 1) : \sigma \mapsto \text{sign}(\sigma) \end{aligned}$$

Dabei gilt $\text{sign}(\sigma) = (-1)^{\text{inv}(\sigma)} = (-1)^{\varepsilon(\sigma)}$ dank der **Parität** (L1C/L1K)

$$\varepsilon : (\mathbb{S}_n, \circ, \text{id}_X) \rightarrow (\mathbb{Z}_2, +, 0) : \sigma \mapsto \text{inv}(\sigma) \bmod 2.$$

Jede Permutation $\sigma \in \mathbb{S}_X$ ist ein Produkt von Transpositionen (L1E):

0 Im Falle $\text{sign}(\sigma) = +1$ hat jedes solche Produkt gerade Länge.

1 Im Falle $\text{sign}(\sigma) = -1$ hat jedes solche Produkt ungerade Länge.

Definition L1P: die alternierende Gruppe

Die geraden Permutationen bilden die **alternierende Gruppe**

$$A_X = \text{Alt}(X) := \ker(\text{sign}_X) = \{ \sigma \in \mathbb{S}_X \mid \text{sign}(\sigma) = +1 \} \leq \mathbb{S}_X.$$

Die alternierende Gruppe

😊 Die traditionelle Benennung ist ein grandioser Etikettenschwindel: Die symmetrische Gruppe ist nicht symmetrisch, und die alternierende Gruppe alterniert nicht, aber so wurden die Namen nun mal vergeben.

Beispiel: Für $X = \{1\}$ haben wir:

$$S_1 = \text{Sym}(X) = \{ \text{id}_X \}$$

$$A_1 = \text{Alt}(X) = \{ \text{id}_X \}$$

Beispiel: Für $X = \{1, 2\}$ haben wir:

$$S_2 = \text{Sym}(X) = \{ \text{id}_X, (1, 2) \}$$

$$A_2 = \text{Alt}(X) = \{ \text{id}_X \}$$

Beispiel: Für $X = \{1, 2, 3\}$ haben wir:

$$S_3 = \text{Sym}(X) = \{ \text{id}_X, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3) \}$$

$$A_3 = \text{Alt}(X) = \{ \text{id}_X, (1, 2, 3), (1, 3, 2) \}$$

Übung: Schreiben Sie ebenso S_4 und A_4 explizit aus!

Satz L1Q: Ordnung der alternierenden Gruppe

Sei X eine endliche Menge mit Elementezahl $n = \#X \geq 2$.

(0) Die Signatur definiert eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow A_X \xrightarrow{\text{inc}} S_X \xrightarrow{\text{sign}_X} \{\pm 1\} \longrightarrow 1$$

(1) Für jede ungerade Permutation $\tau \in S_X$, mit $\text{sign}(\tau) = -1$, gilt

$$S_X = A_X \sqcup (\tau \circ A_X) = A_X \sqcup (A_X \circ \tau).$$

(2) Für die Gruppenordnung (Elementezahl) gilt demnach:

$$\#S_X = n! \quad \text{und} \quad \#A_X = n!/2$$

Beweis: (0) Die Signatur $\text{sign}_X : S_X \rightarrow \{\pm 1\}$ ist surjektiv mit Kern A_X .

(1) Dies haben wir in Satz G1R nachgerechnet. (2) Wir nutzen hier die Bijektion $A_X \cong \tau \circ A_X$ mit $\sigma \mapsto \rho = \tau \circ \sigma$ und $\sigma = \tau^{-1} \circ \rho \leftarrow \rho$. QED

Exakte Sequenzen kennen Sie bereits für lineare Abbildungen (I2H). Allgemein für Gruppen definieren wir Exaktheit durch *Bild gleich Kern*: An jeder Stelle ist das Bild von links gleich dem Kern nach rechts.

Im vorliegenden Beispiel bündelt die Exaktheit drei Aussagen:

- 1 Die Signatur $\text{sign}_X : S_X \rightarrow \{\pm 1\}$ ist surjektiv.
- 2 Der Kern ist die alternierende Gruppe $\ker(\text{sign}_X) = A_X$.
- 3 Die Inklusion $A_X \hookrightarrow S_X$ in die symmetrische Gruppe ist injektiv.

Daraus folgt die Zerlegung (1) in die Fasern der Abbildung sign_X .

Dies kann man hier auch direkt sehen: Für jede Permutation $\sigma \in S_X$ gilt entweder $\sigma \in A_X$, nämlich im Falle $\text{sign}(\sigma) = +1$, oder $\tau^{-1} \circ \sigma \in A_X$, im verbleibenden Falle $\text{sign}(\sigma) = -1$, also $\sigma \in \tau \circ A_X$.

Bei disjunkter Vereinigung addieren sich die Elementezahlen (E2A).

Zudem haben wir eine Bijektion $A_X \cong \tau \circ A_X$ wie oben gezeigt.

Also gilt $2 \cdot \#A_X = \#S_X = n!$, siehe E2H.

| | | | | | | | | | | | | | | | | | |
|-----|--|----|----|---|---|---|---|---|---|---|----|----|----|----|----|----|---|
| A : | <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>1</td><td>2</td><td>3</td><td>4</td></tr> <tr><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr><td>9</td><td>10</td><td>11</td><td>12</td></tr> <tr><td>13</td><td>14</td><td>15</td><td>+</td></tr> </table> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | + |
| 1 | 2 | 3 | 4 | | | | | | | | | | | | | | |
| 5 | 6 | 7 | 8 | | | | | | | | | | | | | | |
| 9 | 10 | 11 | 12 | | | | | | | | | | | | | | |
| 13 | 14 | 15 | + | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | |
|-----|--|----|----|---|---|---|---|----|---|---|----|---|----|---|----|----|---|
| B : | <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>10</td><td>1</td><td>3</td><td>–</td></tr> <tr><td>6</td><td>2</td><td>11</td><td>4</td></tr> <tr><td>7</td><td>14</td><td>8</td><td>12</td></tr> <tr><td>9</td><td>15</td><td>13</td><td>5</td></tr> </table> | 10 | 1 | 3 | – | 6 | 2 | 11 | 4 | 7 | 14 | 8 | 12 | 9 | 15 | 13 | 5 |
| 10 | 1 | 3 | – | | | | | | | | | | | | | | |
| 6 | 2 | 11 | 4 | | | | | | | | | | | | | | |
| 7 | 14 | 8 | 12 | | | | | | | | | | | | | | |
| 9 | 15 | 13 | 5 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | |
|-----|--|----|----|---|---|---|---|---|---|---|----|----|----|----|----|----|---|
| C : | <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>1</td><td>2</td><td>3</td><td>4</td></tr> <tr><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr><td>9</td><td>10</td><td>11</td><td>12</td></tr> <tr><td>13</td><td>15</td><td>14</td><td>+</td></tr> </table> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 15 | 14 | + |
| 1 | 2 | 3 | 4 | | | | | | | | | | | | | | |
| 5 | 6 | 7 | 8 | | | | | | | | | | | | | | |
| 9 | 10 | 11 | 12 | | | | | | | | | | | | | | |
| 13 | 15 | 14 | + | | | | | | | | | | | | | | |

Aufgabe: (1) Wie / Kommen Sie von B zurück zur Anfangsposition A ?
 (2) Können Sie von Position C jemals zur Anfangsposition gelangen?

| | | | | | | | | | | | | | | | | | |
|-----|---|----|----|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| A : | <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>1</td><td>2</td><td>3</td><td>4</td></tr> <tr><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr><td>9</td><td>10</td><td>11</td><td>12</td></tr> <tr><td>13</td><td>14</td><td>15</td><td>16</td></tr> </table> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 | 2 | 3 | 4 | | | | | | | | | | | | | | |
| 5 | 6 | 7 | 8 | | | | | | | | | | | | | | |
| 9 | 10 | 11 | 12 | | | | | | | | | | | | | | |
| 13 | 14 | 15 | 16 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | |
|---|--------------|--------------|--------------|-------------|-------------|-------------|-------------|-------------|-------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>$\sigma(1)$</td><td>$\sigma(2)$</td><td>$\sigma(3)$</td><td>$\sigma(4)$</td></tr> <tr><td>$\sigma(5)$</td><td>$\sigma(6)$</td><td>$\sigma(7)$</td><td>$\sigma(8)$</td></tr> <tr><td>$\sigma(9)$</td><td>$\sigma(10)$</td><td>$\sigma(11)$</td><td>$\sigma(12)$</td></tr> <tr><td>$\sigma(13)$</td><td>$\sigma(14)$</td><td>$\sigma(15)$</td><td>$\sigma(16)$</td></tr> </table> | $\sigma(1)$ | $\sigma(2)$ | $\sigma(3)$ | $\sigma(4)$ | $\sigma(5)$ | $\sigma(6)$ | $\sigma(7)$ | $\sigma(8)$ | $\sigma(9)$ | $\sigma(10)$ | $\sigma(11)$ | $\sigma(12)$ | $\sigma(13)$ | $\sigma(14)$ | $\sigma(15)$ | $\sigma(16)$ |
| $\sigma(1)$ | $\sigma(2)$ | $\sigma(3)$ | $\sigma(4)$ | | | | | | | | | | | | | |
| $\sigma(5)$ | $\sigma(6)$ | $\sigma(7)$ | $\sigma(8)$ | | | | | | | | | | | | | |
| $\sigma(9)$ | $\sigma(10)$ | $\sigma(11)$ | $\sigma(12)$ | | | | | | | | | | | | | |
| $\sigma(13)$ | $\sigma(14)$ | $\sigma(15)$ | $\sigma(16)$ | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | |
|--|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| <table style="text-align: center;"> <tr><td>+</td><td>–</td><td>+</td><td>–</td></tr> <tr><td>–</td><td>+</td><td>–</td><td>+</td></tr> <tr><td>+</td><td>–</td><td>+</td><td>–</td></tr> <tr><td>–</td><td>+</td><td>–</td><td>+</td></tr> </table> | + | – | + | – | – | + | – | + | + | – | + | – | – | + | – | + |
| + | – | + | – | | | | | | | | | | | | | |
| – | + | – | + | | | | | | | | | | | | | |
| + | – | + | – | | | | | | | | | | | | | |
| – | + | – | + | | | | | | | | | | | | | |

Invariante: Das Produkt $s(\sigma) \cdot \text{sign}(\sigma)$ ist konstant und anfangs gleich 1.

Erfunden hat dieses Schiebe-Puzzle Noyes Chapman aus New York. Im Jahr 1880 hat es weltweit einen phänomenalen Hype ausgelöst, vor allem in den USA, Kanada und Europa. Weiter befeuert wurde die Hysterie, als Sam Lloyd für die Lösung des 14-15-Puzzles (C) einen Preis von 1000 Dollar auslobte, das entspricht heute etwa 25 000 Dollar.

Es wurde sogar davon berichtet, dass Arbeitnehmer nicht zu ihrer Arbeit erschienen, und Ladenbesitzer ihre Läden nicht öffneten, weil alle wie besessen einer Lösung dieser logischen Knobelei nachjagten.

😊 Ausbezahlt wurde der Preis jedoch nie, und Sam Lloyd wusste das vermutlich schon im Vorhinein. Genau darum geht es in der Aufgabe!

Fun fact: Recht genau hundert Jahre später errang Rubik's Cube eine ähnliche Popularität. Rubik selbst erklärte, seine Erfindung wurde vom 15-Puzzle inspiriert. Beide sind bis heute sehr beliebt.

😊 In beiden Rätseln steckt eine ganze Menge Mathematik, genauer die Theorie von Permutationsgruppen, in unterhaltsamer Einkleidung.

😊 Wenn Sie Spaß an solchen Klobeleien und Geduldspielen haben, so lösen Sie das Beispiel *B*. Formulieren Sie ein allgemeines Verfahren, mit dem Sie jede (mögliche?) Problemstellung des 15-Puzzles lösen.

Lösung: (1) Ja, das Problem B ist lösbar: Es gibt eine Zugfolge von B nach A . Hierzu benötigen Sie vor allem Geduld. Mathematik hilft (L1s).

(2) Nein, das ist unmöglich. Hier hilft keine Geduld, nur Mathematik!

Ausführlich: Jede Spielposition ist eine Permutation $\sigma \in S_{16}$, wobei die Nummer 16 das leere Feld darstellt. Jeder Spielzug $\sigma \mapsto \sigma' = (i, j) \circ \sigma$ ist die Nachschaltung einer Transposition (i, j) : Sie dürfen die Nummern $i = \sigma(a)$ und $j = \sigma(b)$ vertauschen, wenn die Felder a und b benachbart sind und zudem $i = 16$ oder $j = 16$ gilt. Das freie Feld 16 wandert dabei um genau eine Position. Wir beginnen in der Anfangsposition A mit der Permutation id und Signatur $+$. Nach jedem Zug sehen Sie die Signatur $\text{sign}(\sigma)$ direkt am angegebenen Schachbrettmuster $s(\sigma)$. Genial!

Beispiel: In Position B zeigt das freie Feld $s = -$, die Permutation β sollte also ungerade sein. Probieren Sie es aus! Die Rechnung ist eine sehr gute praktische Übung, am besten effizient dank Zykelregel L1k.

Die tatsächliche Ausführung der Lösung ist damit noch nicht vollbracht, aber immerhin wissen wir, dass eine Lösung existiert (dank Satz L1s), und sich die Suche lohnt. Vor dem Start der fieberhaften Suche ist dies die entscheidende Information, der Rest ist dann Geduldsarbeit.

Beispiel: In Position C zeigt das freie Feld $s = +$, die Permutation γ müsste also gerade sein. Das ist sie aber offensichtlich nicht!

Auch dies ist eine hilfreiche Information: Wir brauchen die Suche gar nicht starten, denn es gibt nachweislich keine Lösung.

Zusammengefasst und noch eleganter formuliert:

Sei $s(\sigma)$ das Vorzeichen $+/-$ des freien Feldes im obigen Muster.
Weiterhin sei $\text{sign}(\sigma)$ die Signatur der Permutation σ , wie zuvor erklärt.

Lemma L1R: die Invariante des 15-Puzzles

Das Produkt $I(\sigma) = s(\sigma) \cdot \text{sign}(\sigma)$ bleibt bei jedem Zug unverändert, da jedesmal beide Faktoren ihr Vorzeichen wechseln.

☺ Ist diese Paritätsbedingung verletzt, so ist das Puzzle unlösbar: Die Positionen α, γ mit $I(\alpha) \neq I(\gamma)$ lassen sich nicht ineinander überführen.

☺ Es ist viel besser, ein Stündchen in das Erlernen der Signatur zu stecken als Monate einer Lösung nachzujagen, die gar nicht existiert!

Interessanterweise gilt die Umkehrung: Ist die Paritätsbedingung erfüllt, so ist das Puzzle lösbar. Das ist etwas mühsamer zu konstruieren. Algebraisch bedeutet es, die alternierende Gruppe zu erzeugen!

Satz L1s: Lösung des 15-Puzzles

Beim 15-Puzzle ist genau die Hälfte der Spielpositionen σ von der Startposition α aus erreichbar, nämlich solche, mit $I(\sigma) = I(\alpha)$.

Beweis: (1) „Höchstens die Hälfte“ folgt aus der Invariante I .
(2) „Mindestens die Hälfte“ zeigen wir durch folgende Konstruktion.
Zur Vereinfachung nummerieren wir die Felder neu wie gezeigt.

| | | | |
|-------------|--------------|--------------|--------------|
| $\sigma(9)$ | $\sigma(10)$ | $\sigma(13)$ | $\sigma(14)$ |
| $\sigma(8)$ | $\sigma(11)$ | $\sigma(12)$ | $\sigma(15)$ |
| $\sigma(7)$ | $\sigma(4)$ | $\sigma(3)$ | $\sigma(1)$ |
| $\sigma(6)$ | $\sigma(5)$ | $\sigma(2)$ | $\sigma(16)$ |

| | | | |
|---|----|----|----|
| 9 | 10 | 13 | 14 |
| 8 | 11 | 12 | 15 |
| 7 | 4 | 3 | 1 |
| 6 | 5 | 2 | |

| | | | |
|---|----|----|----|
| 9 | 10 | 13 | 14 |
| 8 | 11 | 12 | 15 |
| 7 | 4 | 3 | 1 |
| 6 | 5 | 2 | |

Wir können die Zyklen $(1, 2, 3)$ und $(1, 2, \dots, 15)$ realisieren, wie gezeigt. Diese erzeugen die gesamte alternierende Gruppe A_{15} (Satz L1T). QED

Analog zur symmetrischen Gruppe S_n (L1G) und motiviert durch das 15-Puzzle untersuchen wir nun Erzeugendensysteme für A_n .

Satz L1T: Erzeugendensysteme für A_n .

Die 3-Zykel in A_n erzeugen die alternierende Gruppe A_n .

Ebenso gilt $A_n = \langle E_n^s \rangle$ für jede der folgenden Familien:

$$E_n^1 = \{ (i, j, k) \mid i < j < k \}$$

$$E_n^2 = \{ (1, 2, 3), (1, 2, 4), \dots, (1, 2, n) \}$$

$$E_n^3 = \{ (1, 2, 3), (1, 3, 4), \dots, (1, n-1, n) \}$$

$$E_n^4 = \{ (1, 2, 3), (2, 3, 4), \dots, (n-2, n-1, n) \}$$

$$E_n^5 = \{ (1, 2)(2, 3), (1, 2)(3, 4), \dots, (1, 2)(n-1, n) \}$$

$$E_n^6 = \begin{cases} \{ (1, 2, 3), (1, 2, \dots, n) \} & \text{falls } n \text{ ungerade,} \\ \{ (1, 2, 3), (2, 3, \dots, n) \} & \text{falls } n \text{ gerade.} \end{cases}$$

Insbesondere lässt sich die Gruppe A_n durch zwei Elemente erzeugen.

Beweis: (1) Sei $G_n = \langle E_n^s \rangle \leq S_n$ die erzeugte Untergruppe.

Die entscheidenden drei Eigenschaften der Familie E_n^s sind:

1 Alle Permutationen sind gerade, $E_n^s \subseteq A_n$, somit gilt $G_n \leq A_n$.

2 Zu jedem Element $i \in \{1, \dots, n\}$ existiert $\rho \in G_n$ mit $\rho(i) = n$.

3 Es gilt $G_{n-1} \leq G_n$, so dass wir induktiv vorgehen können.

Das ist jeweils sorgsam zu prüfen und gelingt meist leicht.

Für $s = 1, \dots, 5$ gilt sogar $E_{n-1}^s \subseteq E_n^s$, somit $\langle E_{n-1}^s \rangle \subseteq \langle E_n^s \rangle$.

Lediglich für $s = 6$ ist die Eigenschaft (3) nicht offensichtlich.

(2) Wir zeigen nun $A_n \leq G_n$ per Induktion über n .

Die Aussage ist trivial für $n \leq 2$. Sei also $n \geq 3$.

Die Aussage $A_{n-1} \leq G_{n-1}$ sei bereits bewiesen.

Sei $\sigma \in A_n$. Zu $i := \sigma(n)$ wählen wir $\rho \in G_n \leq A_n$ mit $\rho(i) = n$.

Somit gilt $(\rho \circ \sigma)(n) = n$, also $\rho \circ \sigma \in A_{n-1} \leq G_{n-1} \leq G_n$.

Daraus folgt $\sigma \in \rho^{-1} \circ G_n = G_n$. Wir schließen $A_n \leq G_n$.

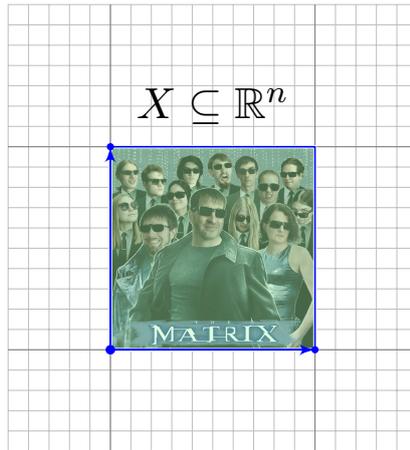
QED

Erzeugendensysteme für die alternierende Gruppe

L155
Erläuterung

Erzeugendensysteme für die alternierende Gruppe

L156
Erläuterung



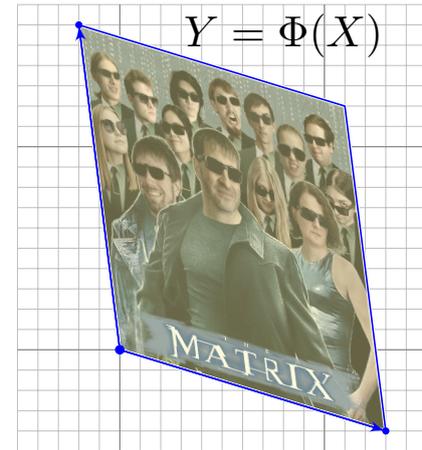
lineare Abbildung

$$\Phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$$

$$x \mapsto y = Ax$$

Zahlenbeispiel:

$$A = \begin{bmatrix} 1.3 & -0.2 \\ -0.4 & 1.6 \end{bmatrix}$$

Wie verhält sich das Volumen unter der linearen Abbildung Φ ?

$$\text{vol}_n(Y) = \text{vol}_n(X) \cdot |\det(A)|$$

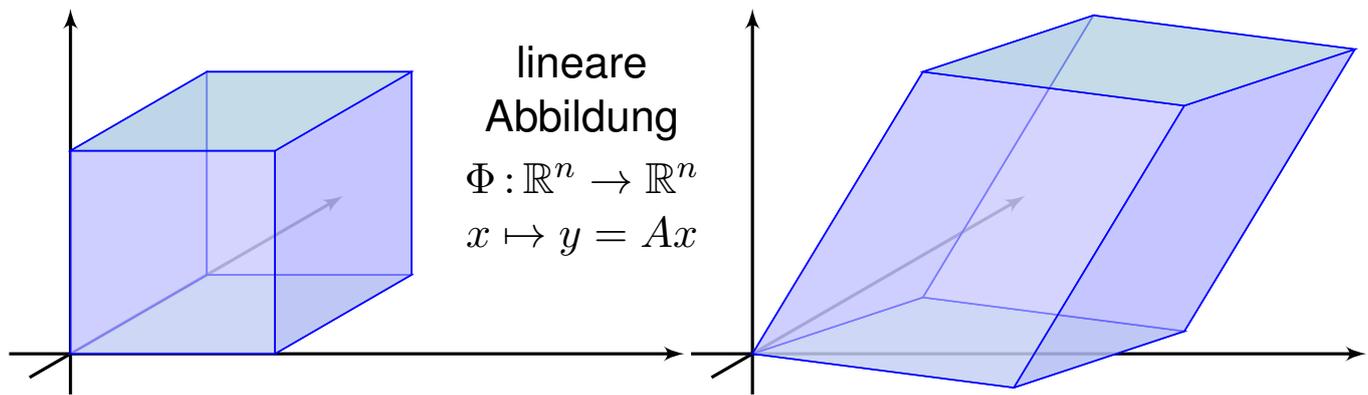
Jede lineare Abbildung $\Phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ können wir als Matrix $A \in \mathbb{R}^{n \times n}$ darstellen (K1E). Die Determinante $\det(A)$ misst die Volumenänderung.

Wie verhält sich das Volumen von $X \subseteq \mathbb{R}^n$ unter Transformationen?
Der einfachste und grundlegende Fall sind lineare Abbildungen.
Hier liefert die Determinante die Antwort, kurz und elegant.

Determinanten sind ein wunderschönes Thema mit vielen Facetten.
Es hat zahlreiche Anwendungen, theoretischer und praktischer Natur,
innerhalb der (Linearen) Algebra, und außerhalb sogar noch mehr.

Mit Determinanten können Sie nicht nur Volumina berechnen, sondern
auch lineare Gleichungssysteme lösen und Matrizen invertieren und
noch vieles mehr. Die Determinante ist ein Universalwerkzeug.

Dazu später... zunächst nutzen wir die geometrische Anschauung.



Je n Vektoren $\mathcal{A} = (a_1, \dots, a_n)$ im \mathbb{R}^n spannen ein **Parallelotop** auf:

$$P = \{ a_1x_1 + \dots + a_nx_n \mid x_1, \dots, x_n \in [0, 1] \} = A \cdot [0, 1]^n$$

Dies ist das Bild des **Einheitswürfels** $[0, 1]^n$ unter der Abbildung Φ .

Wir untersuchen nun das **orientierte Volumen**

$$v : \mathbb{R}^{n \times n} \rightarrow \mathbb{R} : A \mapsto v(A) \quad \text{sodass} \quad \text{vol}_n(P) = |v(A)|.$$

Ziele: präzise Definition? gute Eigenschaften? effiziente Berechnung?

Ich nenne P hier allgemein ein **Parallelotop**. In Dimension $n = 2$ ist dies ein **Parallelogramm**, in Dimension $n = 3$ nennt man dies auch ein **Parallelepipiped** oder einen **Spat**. Die Rechnungen sehen in jeder Dimension gleich aus, daher lege ich die Dimension n hier nicht fest.

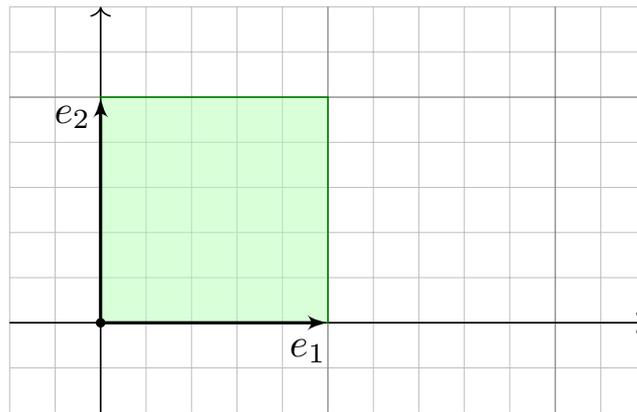
Die **Volumenverzerrung** spielt in der Analysis eine wichtige Rolle bei der Transformationsformel der mehrdimensionalen Integration. Die Matrix ist dort die **Jacobi-Matrix** der Koordinatentransformation und die Determinante ist die sogenannte **Funktionaldeterminante**. Den algebraischen Teil dieser Theorie bereiten wir hier vor.

Notation: Wir fassen die Familie $\mathcal{A} = (a_1, \dots, a_n)$ der Spaltenvektoren $a_1, \dots, a_n \in \mathbb{R}^n$ als die Spalten der Matrix $A \in \mathbb{R}^{n \times n}$ zusammen.

Im Folgenden unterscheide ich daher nicht penibel zwischen der Familie $\mathcal{A} = (a_1, \dots, a_n) \in (\mathbb{R}^n)^n$ und der Matrix $A = (a_1, \dots, a_n) \in \mathbb{R}^{n \times n}$.

Das vereinfacht uns etwas die Schreib- und Sprechweise.

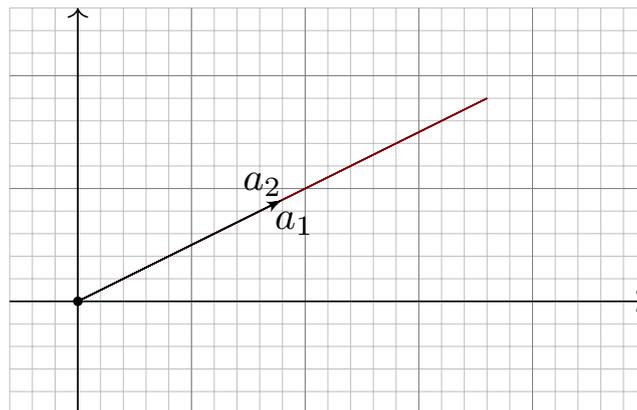
Die Indizes ergeben sich jeweils aus dem Kontext.



1. Normierung: Für die Standardbasis (e_1, \dots, e_n) gilt

$$v(e_1, \dots, e_n) = 1.$$

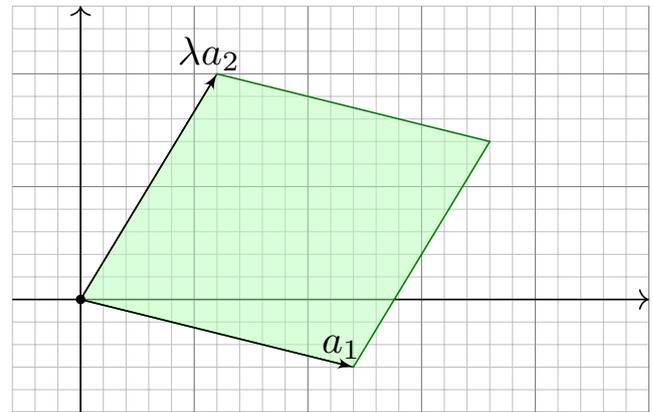
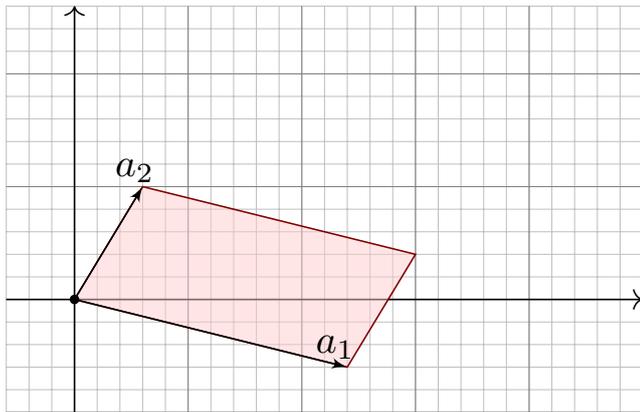
Wir sagen hierzu, die Abbildung v ist **normiert**.



2. Degenerierung: Gilt $a_i = a_j$ für ein Paar $i \neq j$, so folgt

$$v(a_1, \dots, a_i, \dots, a_j, \dots, a_n) = 0.$$

Wir sagen hierzu, die Abbildung v ist **alternierend**.



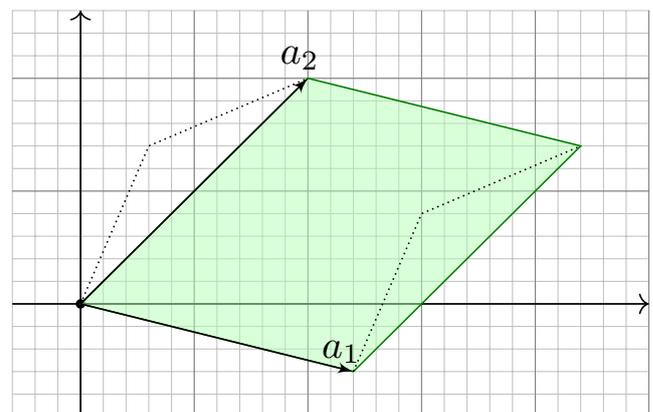
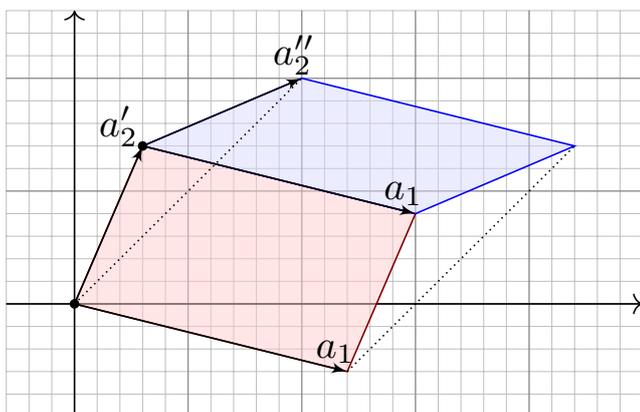
3. Skalierung: Für alle $\lambda \in \mathbb{R}$ gilt

$$v(a_1, \dots, \lambda a_i, \dots, a_n) = \lambda v(a_1, \dots, a_i, \dots, a_n).$$

Für $\lambda < 0$ kehrt sich das Vorzeichen um: orientiertes Volumen!

😊 Der Absolutbetrag $|v(A)|$ misst das geometrische Volumen des Parallelotops, also die Volumenverzerrung der Abbildung $\Phi_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$.

😊 Das Vorzeichen $\text{sign } v(A)$ misst, ob die Familie $\mathcal{A} = (a_1, \dots, a_n)$ rechtshändig oder linkshändig ist (bzgl. der Standardbasis des \mathbb{R}^n).



4. Additivität: Für $a_i = a'_i + a''_i$ in \mathbb{R}^n gilt

$$v(a_1, \dots, a'_i + a''_i, \dots, a_n) = v(a_1, \dots, a'_i, \dots, a_n) + v(a_1, \dots, a''_i, \dots, a_n)$$

Zusammenfassend: Die Abbildung v ist \mathbb{R} -linear in jeder Spalte a_i .

Eindeutigkeit? Können wir das Volumen damit eindeutig bestimmen? und effizient berechnen? Oder fehlen noch weitere Forderungen?

Existenz? Sind unsere Wünsche erfüllbar, also widerspruchsfrei? Oder haben wir hier bereits zu viele Forderungen erhoben?

Multilinear, alternierend, normiert

Definition L2A: multilinear, alternierend, normiert

Sei K ein kommutativer Ring und $v : K^{n \times \ell} \rightarrow K$ eine Abbildung,

$$v : (a_1, \dots, a_i, \dots, a_\ell) \mapsto v(a_1, \dots, a_i, \dots, a_\ell).$$

(1) Wir nennen v **multilinear** über K , falls v linear in jeder Spalte ist:

$$\begin{aligned} v(a_1, \dots, a'_i + a''_i, \dots, a_\ell) &= v(a_1, \dots, a'_i, \dots, a_\ell) + v(a_1, \dots, a''_i, \dots, a_\ell), \\ v(a_1, \dots, \lambda \cdot a_i, \dots, a_\ell) &= \lambda \cdot v(a_1, \dots, a_i, \dots, a_\ell) \end{aligned}$$

für alle $a_1, \dots, a_i, a'_i, a''_i, \dots, a_\ell \in K^n$ und $\lambda \in K$.

(2) Wir nennen v **alternierend**, falls aus der Gleichheit $a_i = a_j$ zweier Spalten $i \neq j$ stets $v(a_1, \dots, a_i, \dots, a_j, \dots, a_\ell) = 0$ folgt.

Wir nennen v **antisymmetrisch**, falls Vertauschung das Vorzeichen wechselt gemäß $v(\dots, a_i, \dots, a_j, \dots) = -v(\dots, a_j, \dots, a_i, \dots)$.

Wir nennen v **symmetrisch**, falls Vertauschung nichts ändert.

(3) Im Falle $n = \ell$ nennen wir v **normiert**, falls $v(e_1, \dots, e_n) = 1$ gilt.

Multilinear, alternierend, normiert

Hier und im Folgenden sei K ein kommutativer Ring.

- Wir betrachten die linearen Räume K^n und $K^{n \times \ell}$ über K .
- Skalare $\lambda \in K$ multiplizieren wir wahlweise von links oder rechts.

Jede Matrix $A \in K^{n \times \ell}$ können wir auffassen als Familie $\mathcal{A} = (a_1, \dots, a_\ell)$ von Spaltenvektoren $a_1, \dots, a_\ell \in K^n$. Wir nutzen also $K^{n \times \ell} \cong (K^n)^\ell$.

Die Abbildung $v : K^{n \times \ell} \rightarrow K$ nimmt als Eingabe ℓ Spaltenvektoren $a_1, \dots, a_\ell \in K^n$ und liefert als Ausgabe einen Skalar $v(a_1, \dots, a_\ell) \in K$.

Für A nutzen wir die traditionelle Indizierung: erst Zeile, dann Spalte. Der Eintrag $a_{ki} = a_{k,i}$ bezeichnet den k ten Eintrag der i ten Spalte a_i . Die Familie der Zeilen wäre in dieser Hinsicht hier etwas bequemer.

Die Familie (a_1, \dots, a_ℓ) suggeriert umgekehrt: erst Spalte, dann Zeile. In dieser Sichtweise als Spaltenvektoren haben wir also $(a_i)_k = a_{ki}$. Das ist leider nicht besonders elegant, aber nicht weiter tragisch.

😊 Die Determinante, auf die wir zuarbeiten, erweist sich als invariant unter Transposition $A \mapsto A^T$, also geben beide Sichtweisen dasselbe.

Einmal Null, immer Null

Uns interessiert hier vor allem der Fall $n = \ell$. Wir wollen zeigen: Es existiert genau eine multilineare, alternierende und normierte Abbildung $v: K^{n \times n} \rightarrow K$, und diese nennen wir **die Determinante**. Das ist die Aussage des Hauptsatzes L2G zu Determinanten.

Zur Vorbereitung stellen wir einfache Rechenregeln zusammen. Wir beginnen mit der folgenden, sehr einfachen Beobachtung:

Bemerkung L2B: einmal Null, immer Null

Allein mit der Additivität folgt aus $a_i = 0$ bereits $v(A) = 0$, denn

$$\begin{aligned} v(\dots, a_{i-1}, 0, a_{i+1}, \dots) &= v(\dots, a_{i-1}, 0 + 0, a_{i+1}, \dots) \\ &= v(\dots, a_{i-1}, 0, a_{i+1}, \dots) + v(\dots, a_{i-1}, 0, a_{i+1}, \dots). \end{aligned}$$

Dasselbe folgt ebenso aus der K -Homogenität für $\lambda = 0$:

$$v(\dots, a_{i-1}, 0 \cdot 0, a_{i+1}, \dots) = 0 \cdot v(\dots, a_{i-1}, 0, a_{i+1}, \dots)$$

Der Skalar $0 = 0_K$ und der Vektor $0 = 0_{K^n}$ haben hier dasselbe Symbol. Das ist schon arg knausrig, aber daran haben Sie sich schon gewöhnt.

Transvektion ändert nichts.

Lemma L2C: Transvektion ändert nichts.

Ist $v: K^{n \times \ell} \rightarrow K$ multilineare und alternierend so gilt

$$v(\dots, a_i, \dots, a_j + \lambda a_i, \dots) = v(\dots, a_i, \dots, a_j, \dots)$$

Beweis: Wir nutzen die Linearität in Spalte j :

$$\begin{aligned} &v(\dots, a_i, \dots, a_j + \lambda a_i, \dots) \\ &= v(\dots, a_i, \dots, a_j, \dots) + \lambda v(\dots, a_i, \dots, a_i, \dots) \end{aligned}$$

Da v alternierend ist, verschwindet der letzte Summand. □

Das ist eine einfache Rechnung, doch die Konsequenzen sind enorm: Das Lemma zeigt, dass wir den Gauß-Algorithmus anwenden können: Bei Transvektionen ändert sich der Wert von v nicht, wie hier zu sehen. Bei Skalierung einer Spalte nutzen wir die Linearität (K -Homogenität). Es bleiben noch Vertauschungen, die untersuchen wir als nächstes...

Aus alternierend folgt antisymmetrisch.

Lemma L2D: Aus alternierend folgt antisymmetrisch.

(1) Sei v multilinear. Ist v alternierend, so auch antisymmetrisch.

$$(\star) \quad v(\dots, a_i, \dots, a_j, \dots) = -v(\dots, a_j, \dots, a_i, \dots)$$

(2) Über jedem Körper K der Charakteristik $\neq 2$ gilt die Umkehrung.

Beweis: (1) Wir nutzen die Additivität in den Spalten $i \neq j$:

$$\begin{aligned} 0 &\stackrel{\text{alt}}{=} v(\dots, a_i + a_j, \dots, a_i + a_j, \dots) \\ &\stackrel{\text{add}}{=} + v(\dots, a_i, \dots, a_i, \dots) + v(\dots, a_i, \dots, a_j, \dots) \\ &\quad + v(\dots, a_j, \dots, a_i, \dots) + v(\dots, a_j, \dots, a_j, \dots) \end{aligned}$$

(2) Aus (\star) und $a_i = a_j$ mit $i \neq j$ folgt $2v(\dots, a_i, \dots, a_j, \dots) = 0$.

Nach Division durch 2 erhalten wir $v(\dots, a_i, \dots, a_j, \dots) = 0$. QED

Gegenbeispiel: Die Multiplikation $\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \rightarrow \mathbb{F}_2 : (a, b) \mapsto a \cdot b$ ist anti/symmetrisch, aber nicht alternierend, da $1 \cdot 1 = 1 \neq 0$.

Permutationsmatrizen und Signatur

Jede Abbildung $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ definiert eine Matrix

$$P_\sigma := (e_{\sigma(1)}, \dots, e_{\sigma(n)}) \in K^{n \times n}.$$

Im Falle $\sigma \in S_n$ nennen wir P_σ die **Permutationsmatrix** zu σ .

Beispiel: Für $\sigma = (1, 2, 3) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ und $\tau = (2, 3) = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$ in S_3 gilt

$$P_\sigma = (e_2, e_3, e_1) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{und} \quad P_\tau = (e_1, e_3, e_2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Lemma L2E: Permutationsmatrix und Signatur

Ist $v : K^{n \times n} \rightarrow K$ multilinear und alternierend, so gilt

$$v(P_\sigma) = \text{sign}(\sigma) \cdot v(E).$$

Ist v zudem normiert durch $v(E) = 1$, so folgt $v(P_\sigma) = \text{sign}(\sigma)$.

Beweis: Ist σ nicht injektiv, so gilt $v(P_\sigma) = 0$ (L2A) und $\text{sign}(\sigma) = 0$ (L1H). Jede Permutation $\sigma \in S_n$ ist Produkt $\sigma = \tau_1 \tau_2 \cdots \tau_\ell$ von Transpositionen (L1E), also $\text{sign}(\sigma) = (-1)^\ell$ (L1K) und $v(P_\sigma) = (-1)^\ell \cdot v(E)$ (L2D). QED

Permutationsmatrizen und Signatur

Die Matrix P_σ entspricht der linearen Abbildung

$$K^n \rightarrow K^n : e_i \mapsto e_{\sigma(i)}.$$

Dabei gilt $P_\sigma \cdot P_\tau = P_{\sigma \circ \tau}$ und $P_{\sigma^{-1}} = P_\sigma^{-1} = P_\sigma^\top$. Wir haben also:

$$\begin{aligned} P : (E_n, \circ, \text{id}) &\hookrightarrow (K^{n \times n}, \cdot, 1_{n \times n}) : \sigma \mapsto P_\sigma \\ (S_n, \circ, \text{id}) &\hookrightarrow (\text{GL}_n K, \cdot, 1_{n \times n}) \end{aligned}$$

Ist $v : K^{n \times n} \rightarrow K$ multilinear, alternierend und normiert, so haben wir:

$$\begin{array}{ccc} (E_n, \circ, \text{id}) & \xrightarrow{\sigma \mapsto P_\sigma} & (K^{n \times n}, \cdot, 1_{n \times n}) \\ \text{sign} \downarrow & & \downarrow v \text{ det} \\ (\{\pm 1, 0\}, \cdot, 1) & \xrightarrow{s \mapsto s \cdot 1_K} & (K, \cdot, 1) \end{array}$$

Wir interpretieren hier und im Folgenden die Signatur $\text{sign}(\sigma) \in \{\pm 1, 0\}$ als Element des Rings K , genauer könnten wir schreiben $\text{sign}(\sigma) \cdot 1_K$.

Die Kommutativität des Grundrings K ist notwendig.

L216
Erläuterung

Der Unterschied zwischen alternierend und antisymmetrisch ist recht subtil und spielt vor allem in Charakteristik 2 eine ernsthafte Rolle. Wir wollen alle Fälle einheitlich behandeln und wählen daher bewusst den stärkeren Begriff: alternierend. Damit passt alles zusammen.

Die Kommutativität von K fordern wir nicht nur aus Bequemlichkeit:

Bemerkung L2F: Die Kommutativität von K ist notwendig.

Eine multilineare normierte Abbildung $v : K^{n \times n} \rightarrow K$ kann es für $n \geq 2$ nur über einem *kommutativen* Ring K geben. Für $a, b \in K$ gilt nämlich

$$\begin{aligned} v \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} &= a \cdot v \begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} = a \cdot b \cdot v \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = a \cdot b, \\ v \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} &= b \cdot v \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = b \cdot a \cdot v \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = b \cdot a. \end{aligned}$$

😊 Der folgende Satz besagt, dass die Kommutativität von K bereits ausreicht, um die Existenz und die Eindeutigkeit einer multilinearen, alternierenden, normierten Abbildung $K^{n \times n} \rightarrow K$ sicherzustellen.

Der Hauptsatz zu Determinanten

Satz L2G: Existenz, Eindeutigkeit, Eigenschaften

Sei K ein kommutativer Ring. In jeder Dimension $n \in \mathbb{N}$ existiert genau eine multilineare, alternierende, normierte Abbildung $v: K^{n \times n} \rightarrow K$.

Diese Abbildung nennen wir die **Determinante** und schreiben hierfür

$$\det = \det_K^n : K^{n \times n} \rightarrow K.$$

- 1 Es gilt $\det A = \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}$. (Leibniz)
- 2 Die Determinante ist transpositionsinvariant: $\det(A^T) = \det(A)$.
- 3 Die Determinante ist multiplikativ: $\det(A \cdot B) = \det(A) \cdot \det(B)$.
- 4 Genau dann ist $A \in K^{n \times n}$ invertierbar, wenn $\det(A) \in K$ dies ist.
- 5 Es gilt $AA' = A'A = \det(A)E$, also $A^{-1} = \det(A)^{-1} A'$. (Cramer)

Zu $A = (a_1, \dots, a_n)$ definieren wir die **adjunkte Matrix** $A' = \text{adj}(A)$ durch die Cofaktoren $a'_{ij} := \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n)$.

😊 Explizite polynomielle Formeln. 😊 Sofort praktisch für kleine n .

Definition und Eigenschaften der Determinante

L218
Erläuterung

Ich fasse hier die wichtigsten Aussagen zu Determinanten übersichtlich zusammen und nenne dies daher den **Hauptsatz zu Determinanten**. Er dient als Zusammenfassung und Vorschau; alles Wesentliche steckt bereits kurz & knapp drin, wir packen es anschließend sorgfältig aus.

Ich möchte dies an den Anfang stellen, um Ihnen einen ersten Überblick zu geben. So können Sie schon sehen, oder besser erahnen, wozu die Determinante so alles gut ist. Die Details, Beweise und Beispiele folgen. Es gibt noch mehr Schönes zu berichten, hier das Wichtigste in Kürze.

Ich betone hier, dass die Determinante durch ein Polynom gegeben ist, zwar ein großes Polynom, doch recht simpel und übersichtlich gebaut. Insbesondere zur Inversion $A \mapsto A^{-1}$ bietet $A^{-1} = \det(A)^{-1} \text{adj}(A)$ eine geschlossene Formel, als rationale Funktion: stetig, differenzierbar.

Für kleine n ist dies sofort praktisch einsetzbar, für große n jedoch ist die naive Anwendung der Leibniz-Formel rasch zu aufwändig ($n!$). Dazu entwickeln wir ergänzend noch weit effizientere Verfahren, allen voran geht hier natürlich der Gauß-Algorithmus (n^3).

Beispiel $n = 2$: Inversion von 2×2 -Matrizen

Notation: Man schreibt oft kurz $|A| := \det(A)$. Vorsicht! Hier droht die Gefahr einer Verwechslung mit Beträgen, Längen und Normen.

Für $n = 0$ haben wir $K^{0 \times 0} = \{()\}$ und $\det_K^0 : K^{0 \times 0} \rightarrow K : () \mapsto 1$.

Für $n = 1$ ist $\det_K^1 : K^{1 \times 1} \xrightarrow{\simeq} K : (a) \mapsto a$ ein Isomorphismus.

Der erste interessante Fall entsteht in Dimension $n = 2$:

Beispiel L2H: Determinante und Inversion von 2×2 -Matrizen

Für 2×2 -Matrizen ist die Determinante gegeben durch

$$\det = \det_K^2 : K^{2 \times 2} \rightarrow K : \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mapsto \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc.$$

Genau dann ist A in $K^{2 \times 2}$ invertierbar, wenn $\det A$ in K invertierbar ist.

Für die Inversion haben wir eine einfache, rationale Adjunktenformel:

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

Beispiel $n = 2$: Inversion von 2×2 -Matrizen

Übung: (1) Lesen Sie den Hauptsatz L2G nochmal genaustens durch und folgern Sie daraus für $n = 2$ die obigen Formeln in Beispiel L2H.

(2) Die explizit gegebene Inversionsformel können Sie direkt prüfen: Multiplizieren Sie die Matrizen A und A^{-1} , dies muss $1_{2 \times 2}$ ergeben!

Lösung: (1a) Die Leibniz-Formel summiert über $S_2 = \{\text{id}, (1, 2)\}$.

(1b) Für die Adjunkte finden wir z.B. $a'_{12} = \det(e_2, a_2) = \begin{vmatrix} 0 & c \\ 1 & d \end{vmatrix} = -c$.

Probieren Sie es selbst: So finden Sie alle Terme der Inversionsformel!

(2) Sie kennen diese schöne Formel bereits aus Kapitel B, Satz B1E. Dies gelingt auch ganz direkt, fast ohne Theorie: Stehen die expliziten Formeln einmal vor Ihnen, so genügt Nachrechnen (oder Anwenden).

Im jetzigen Kontext erweist sich der Fall $n = 2$ als der erste Schimmer einer allgemeinen Theorie der Determinanten. Alles fügt sich.

😊 Determinante und Inversion von 2×2 -Matrizen wird Ihnen häufig nützen, daher sollten Sie beides im Schlaf beherrschen.

Beispiel $n = 3$: Sarrus–Regel aka Jägerzaun

😊 Im Fall $n = 2$ können Sie noch alles direkt per Hand nachrechnen. Ab $n \geq 3$ sorgt die allgemeine Theorie für Ordnung und Übersicht.

Beispiel L21: Determinante und Inversion von 3×3 –Matrizen

Jede 3×3 –Matrix $A \in K^{3 \times 3}$ ist die Determinante gegeben durch

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

Diese **Regel von Sarrus** lässt sich als **Jägerzaunregel** merken.

Genau dann ist A in $K^{3 \times 3}$ invertierbar, wenn $\det A$ in K invertierbar ist. Für die Inversion haben wir eine explizite, rationale Adjunktenformel:

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}$$

Ab $n \geq 4$ ist die Leibniz–Formel aufwändiger, mit $n!$ Summanden.

Beispiel $n = 3$: Sarrus–Regel aka Jägerzaun

Übung: Lesen Sie den Hauptsatz L2G nochmal genaustens durch und folgern Sie daraus für $n = 3$ die obigen Formeln in Beispiel L21. (Sie können gerne später mit mehr Erfahrung darauf zurückkommen, in jedem Falle sollten Sie viel rechnen, um Zutrauen zu gewinnen.)

Die explizit gegebene Inversionsformel können Sie direkt nachprüfen. Das ist allerdings wenig erquicklich. Schon hier scheint es mir viel effizienter und auch lehrreicher, den allgemeinen Fall zu verstehen. Allgemeine Theorie und konkrete Zahlenbeispiele ergänzen sich!

😊 Die Jägerzaunregel ist in Rechnungen oft hilfreich, daher sollten Sie die ganz einfachen Formeln auswendig und fehlerfrei beherrschen.

Schon die Inversionsformel in Dimension $n = 3$ scheint mir zu vertrackt, um sie stur auswendig zu lernen. Mit System geht es viel besser!

Investieren Sie Ihre kostbare Zeit lieber in das genaue Verständnis des Hauptsatzes L2G: Aus diesem können Sie je nach Bedarf alle weiteren Formeln ableiten, wie hier gezeigt. Das ist ein allgemeines Prinzip.

Aufgabe: Für welche Werte $\lambda \in \mathbb{R}$ ist die folgende Matrix invertierbar?

$$A(\lambda) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{3 \times 3}$$

Lösung: Wir berechnen die Determinante und finden:

$$\det A(\lambda) = \begin{vmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{vmatrix} = 60 - 12\lambda$$

Für alle $\lambda \in \mathbb{R} \setminus \{5\}$ ist die Matrix $A(\lambda)$ in $\mathbb{R}^{3 \times 3}$ invertierbar.

$$A(5) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \notin \text{GL}_3 \mathbb{R}$$

Für $\lambda = 5$ erhalten wir die Telefonmatrix; diese hat nur Rang 2.

😊 Dieses Phänomen gilt für jeden der neun Einträge der Telefonmatrix: Wenn wir beliebig wenig daran wackeln, so wird die Matrix invertierbar!

Die drei Spalten der Telefonmatrix ($\lambda = 5$) sind linear abhängig, sie spannen im \mathbb{R}^3 nur einen Unterraum der Dimension 2 auf.

Für $\lambda \neq 5$ hingegen sind die drei Spalten linear unabhängig und bilden somit eine Basis des \mathbb{R}^3 . Die Determinante hilft!

Übrigens geht dieses System um $\lambda = 5$ von einer rechtshändigen in eine linkshändige Basis über, dazwischen kann es keine Basis sein.

Übung: (1) Platzieren Sie die Variable λ an verschiedene Stellen der Telefonmatrix und untersuchen Sie die Determinante wie oben.

(2) Untersuchen Sie dieses Beispiel genauso über $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$.

😞 Im Gauß-Algorithmus müssen Sie Fallunterscheidungen treffen: null oder nicht? Das ist für eine einzelne Rechnung kein Problem, erschwert aber den Überblick für eine Familie $\lambda \mapsto A(\lambda)$ wie hier.

😊 Die Determinante ist ein sympathisches Polynom und erfordert keine Fallunterscheidungen: Alles gelingt einheitlich, alle Fälle gleich.

Die einzige Entscheidung $\det A \stackrel{?}{=} 0$ entsteht erst ganz zum Schluss!

Konstruktion der Determinante

Weiterhin sei K ein kommutativer Ring und $n \in \mathbb{N}$ eine natürliche Zahl.

Definition L2J: Konstruktion der Determinante

Wir konstruieren $\det = \det_K^n : K^{n \times n} \rightarrow K$ durch die **Leibniz-Formel**

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot \prod_{j=1}^n a_{\sigma(j),j} \\ &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n} \end{aligned}$$

und nennen diese Abbildung die **Determinante** in Dimension n über K .

- 😊 Explizite polynomielle Formel. 😊 Direkt anwendbar für kleine n .
 - 😊 Daraus folgern wir alle weiteren Eigenschaften und Rechenregeln.
- Die Leibniz-Formel ist ein guter Startpunkt, aber noch nicht das Ende:
- 😞 Naive Anwendung der Leibniz-Formel ist für große n aufwändig ($n!$).
 - 😊 Eine effiziente Berechnung gelingt mit dem Gauß-Algorithmus (n^3).

Invarianz unter Transposition

Satz L2K: Invarianz unter Transposition

Die Determinante ist invariant unter Transposition: $\det(A^T) = \det(A)$.

Beweis: Für jede Permutation $\sigma \in S_n$ gilt dank Sortierung der Faktoren

$$a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n} = a_{1,\sigma^{-1}(1)} \cdot a_{2,\sigma^{-1}(2)} \cdots a_{n,\sigma^{-1}(n)}.$$

Zudem gilt $\text{sign}(\sigma) = \text{sign}(\sigma^{-1})$. Durchläuft σ alle Elemente von S_n , so durchläuft auch das Inverse σ^{-1} alle Elemente von S_n . Wir erhalten:

$$\begin{aligned} \det(A^T) &\stackrel{\text{Def}}{=} \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1}^T \cdot a_{\sigma(2),2}^T \cdots a_{\sigma(n),n}^T \\ &\stackrel{\text{Def}}{=} \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} \\ &\stackrel{\text{Inv}}{=} \sum_{\sigma \in S_n} \text{sign}(\sigma^{-1}) \cdot a_{1,\sigma^{-1}(1)} \cdot a_{2,\sigma^{-1}(2)} \cdots a_{n,\sigma^{-1}(n)} \\ &\stackrel{\text{Sort}}{=} \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n} \stackrel{\text{Def}}{=} \det(A) \end{aligned}$$

Somit ist die Determinante transpositionsinvariant. QED

Die Determinante tut, was eine Determinante tun muss.

Satz L2L: Die Determinante erfüllt die Axiome.

Die Determinante $\det = \det_K^n$ ist normiert, multilinear und alternierend.

Beweis: (1) Für die Einheitsmatrix $E = 1_{n \times n}$ und $\sigma \in S_n$ gilt

$$\text{sign}(\sigma) \cdot e_{\sigma(1),1} \cdot e_{\sigma(2),2} \cdots e_{\sigma(n),n} = \begin{cases} 1 & \text{für } \sigma = \text{id}, \\ 0 & \text{für } \sigma \neq \text{id}. \end{cases}$$

(2) Die Determinante $A \mapsto \det(A)$ ist linear in jeder Spalte:

$$\begin{aligned} & \det(a_1, \dots, a'_i + \lambda a''_i, \dots, a_n) \\ &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots (a'_{\sigma(i),i} + \lambda a''_{\sigma(i),i}) \cdots a_{\sigma(n),n} \\ &= \dots = \det(a_1, \dots, a'_i, \dots, a_n) + \lambda \det(a_1, \dots, a''_i, \dots, a_n) \end{aligned}$$

(3) Sei $A \in K^{n \times n}$ mit $a_i = a_j$ für ein Paar $i \neq j$. Zu $\tau = (i, j)$ haben wir $S_n = A_n \sqcup \tau \circ A_n$. Für jede Permutation $\sigma \in A_n$ und $\sigma' = \tau \circ \sigma$ gilt:

$$a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} = a_{1,\sigma'(1)} \cdot a_{2,\sigma'(2)} \cdots a_{n,\sigma'(n)}$$

In der Leibniz-Formel löschen sich so alle Terme paarweise aus. QED

Die Determinante tut, was eine Determinante tun muss.

Axiome sind grundlegende Annahmen, Forderungen, Wünsche, ...
Damit haben wir die wesentlichen Eigenschaften knapp und präzise zusammengefasst, die wir von der Determinante erwarten / erhoffen.

😊 Das Wünschen ist immer erlaubt, doch nicht alles ist erfüllbar.
Der vorige Satz L2L garantiert, dass unsere Wünsche tatsächlich erfüllt werden können; der folgende Satz L2M sichert zudem die Eindeutigkeit.

😊 Ich habe die drei Axiome (multilinear, alternierend, normiert) hier zunächst für die Spalten formuliert. Das ist etwas willkürlich:
Für Spalten scheint mir die Notation (a_1, \dots, a_n) etwas bequemer.

😊 Alles gilt genauso für Zeilen, dank Invarianz unter Transposition.
Die Determinante ist also multilinear, alternierend, normiert in den Spalten (nach Definition) und ebenso in den Zeilen (dank Satz).

Andere Autoren gehen umgekehrt vor, das Ergebnis ist dasselbe...
Zum Glück! Es gibt eben nur eine Determinante, für alle dieselbe.
Dies bringt uns schließlich zum folgenden Eindeutigkeitssatz.

Der Eindeutigkeitsatz

Satz L2M: Eindeutigkeitsatz für die Determinante

Ist $v : K^{n \times n} \rightarrow K$ multilinear und alternierend, so gilt

$$v(A) = v(E) \cdot \det(A)$$

für alle Matrizen $A \in K^{n \times n}$. Ist v zudem normiert, so folgt $v = \det$.

Beweis: Jeder Spaltenvektor $a_j \in K^n$ ist eine Linearkombination $a_j = \sum_{i=1}^n e_i a_{ij}$ der Standardbasis $e_1, \dots, e_n \in K^n$. Daraus folgt:

$$\begin{aligned} v(a_1, \dots, a_n) &= v\left(\sum_{i_1=1}^n e_{i_1} a_{i_1,1}, \dots, \sum_{i_n=1}^n e_{i_n} a_{i_n,n}\right) \\ &\stackrel{(1)}{=} \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n a_{i_1,1} \cdots a_{i_n,n} v(e_{i_1}, \dots, e_{i_n}) \\ &= \sum_{\sigma \in E_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} v(P_\sigma) \quad \text{mit } \sigma : k \mapsto i_k \\ &\stackrel{(2)}{=} \sum_{\sigma \in S_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \text{sign}(\sigma) v(E) \end{aligned}$$

Wir nutzen hier: v ist (1) multilinear und (2) alternierend (L2E).

QED

Der Multiplikationssatz

Satz L2N: Die Determinante ist multiplikativ.

Für alle quadratischen Matrizen $A, B \in K^{n \times n}$ gilt:

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Wir erhalten so den Monoidhomomorphismus

$$\det : (K^{n \times n}, \cdot, 1_{n \times n}) \rightarrow (K, \cdot, 1).$$

Beweis: Wir halten $A \in K^{n \times n}$ fest und betrachten die Abbildung

$$v : K^{n \times n} \rightarrow K : B \mapsto \det(A \cdot B) = \det(Ab_1, \dots, Ab_n).$$

Diese ist multilinear und alternierend in den Spalten b_1, \dots, b_n von B .

Dank des Eindeutigkeitsatzes L2M gilt $v(B) = v(E) \cdot \det(B)$, also

$$\det(A \cdot B) \stackrel{\text{Def}}{=} v(B) \stackrel{\text{L2M}}{=} v(E) \cdot \det(B) \stackrel{\text{Def}}{=} \det(A) \cdot \det(B).$$

Somit ist die Determinante multiplikativ für alle $A, B \in K^{n \times n}$.

QED

😊 Dieses Vorgehen ist einfach genial, raffiniert und effizient! Aus dem Eindeutigkeitssatz L2M folgt mit einem Schlag die Multiplikativität L2N.

An dieser Stelle bin ich jedesmal aufs Neue erstaunt und begeistert. Wieder einmal gilt: Kaum macht man es richtig, schon funktioniert's!

In manchen Büchern zur Linearen Algebra wird die Multiplikativität auf anderen Wegen bewiesen, zum Beispiel mit dem Gauß-Algorithmus. Das ist möglich, doch unser obiges Argument ist unschlagbar elegant.

Ich versuche daher bewusst, obskur-stumpfsinnige Rechnungen durch klar-scharfsinnige Argumente zu ersetzen, soweit dies hier möglich ist. Ab und an müssen wir tapfer durchrechnen, da führt kein Weg vorbei.

😊 Unsere sorgsamten Rechnungen haben sich wieder einmal gelohnt. Zugegeben, auch wir mussten uns einigen Index-Schlachten stellen, doch wir haben obsiegt und tragen nun reiche Beute davon. Darauf können wir im Folgenden weiter aufbauen.

Die Determinante ist nicht additiv!

L232

Bemerkung L2O: Warnung, die Determinante ist nicht additiv!

(0) In Dimension $n \geq 2$ ist die Determinante

$$\det = \det_K^n : (K^{n \times n}, \cdot, 1_{n \times n}) \rightarrow (K, \cdot, 1)$$

ein Monoidhomomorphismus, aber **kein Ringhomomorphismus!**

(1) Die Determinante ist multiplikativ, aber **nicht additiv**:

Ein besonders einfaches Gegenbeispiel ist

$$\det \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0 \quad \text{und} \quad \det \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = 0 \quad \text{aber} \quad \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1.$$

(2) Die Determinante \det_K^n ist insgesamt **K -homogen vom Grad n** :

Für jede Matrix $A \in K^{n \times n}$ und jeden Skalar $\lambda \in K$ gilt

$$\det(\lambda A) = \lambda^n \det(A).$$

Insbesondere gilt $\det(-A) = (-1)^n \det(A)$.

Satz L2P: Cramersche Regel / Determinantenverfahren

Gegeben seien die Matrix $A \in K^{n \times n}$ und zwei Vektoren $x, b \in K^n$.

(1) Gilt $Ax = b$, also $b = \sum_{i=1}^n a_i x_i$, so folgt für alle $j \in \{1, \dots, n\}$:

$$\det(\dots, a_{j-1}, b, a_{j+1}, \dots) = \det(A) \cdot x_j$$

(2) Ist $\det(A)$ in K invertierbar, so lösen wir $Ax = b$ eindeutig durch

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \frac{1}{\det A} \begin{bmatrix} \det(b, a_2, \dots, a_n) \\ \det(a_1, b, \dots, a_n) \\ \vdots \\ \det(a_1, a_2, \dots, b) \end{bmatrix}.$$

Beweis: (1) Die Determinante ist multilinear und alternierend (L2L):

$$\det(\dots, a_{j-1}, b, a_{j+1}, \dots) = \sum_{i=1}^n \det(\dots, a_{j-1}, a_i, a_{j+1}, \dots) \cdot x_i$$

Alle Terme mit $i \neq j$ verschwinden, es bleibt nur $\det(A) \cdot x_j$. QED

Die Cramersche Regel und das Determinantenverfahren

😊 Die Determinante filtert den gewünschten Koeffizienten x_j heraus! Die **Cramersche Regel** bietet eine geschlossene Formel zur Lösung linearer Gleichungssysteme – unter der Voraussetzung $\det A \in K^\times$. Diese Lösungsmethode heißt daher auch **Determinantenverfahren**.

😊 In kleiner Dimension n kann dieses Verfahren direkt eingesetzt werden und liefert die eindeutige Lösung x mit vertretbarem Aufwand.

😞 Zur Berechnung müssen $n + 1$ Determinanten bestimmt werden; in Spezialfällen ist das leicht, aber allgemein für große n zu aufwändig. Daher sind andere Lösungsmethoden meist vorzuziehen, etwa das Gauß–Verfahren oder algorithmische Verfeinerungen der Numerik.

😊 Dennoch ist die Cramersche Regel aus theoretischer Sicht hilfreich: Sie garantiert (im klassischen Fall $K = \mathbb{R}, \mathbb{C}$), dass die gesuchte Lösung x stetig von den Eingabedaten A und b abhängt (sogar differenzierbar). Wenn wir A und b nur wenig ändern, so bewegt auch x sich nur wenig.

😊 Genauer haben wir für x eine explizite rationale Funktion in den Koeffizienten von A und b , also einen Quotienten von Polynomen.

Aufgabe: Wir betrachten zu jedem Parameter $\lambda \in \mathbb{R}$ die reelle Matrix

$$A(\lambda) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{3 \times 3}.$$

Bestimmen Sie alle Lösungen $x \in \mathbb{R}^3$ der Gleichung $A(\lambda)x = e_1$.

Lösung: Wir wissen bereits $\det A(\lambda) = 60 - 12\lambda$, siehe L223.

Für $\lambda \neq 5$ können wir das Determinantenverfahren L2P nutzen.

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & \lambda & 6 \\ 0 & 8 & 9 \end{vmatrix} \stackrel{\text{L2I}}{=} 9\lambda - 48, \quad \begin{vmatrix} 1 & 1 & 3 \\ 4 & 0 & 6 \\ 7 & 0 & 9 \end{vmatrix} \stackrel{\text{L2I}}{=} 6, \quad \begin{vmatrix} 1 & 2 & 1 \\ 4 & \lambda & 0 \\ 7 & 8 & 0 \end{vmatrix} \stackrel{\text{L2I}}{=} 32 - 7\lambda.$$

Zu jedem Parameter $\lambda \in \mathbb{R} \setminus \{5\}$ finden wir so die einzige Lösung:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \stackrel{\text{L2P}}{=} \frac{1}{\det A} \begin{bmatrix} \det(b, a_2, a_3) \\ \det(a_1, b, a_3) \\ \det(a_1, a_2, b) \end{bmatrix} \stackrel{\text{L2I}}{=} \frac{1}{60 - 12\lambda} \begin{bmatrix} 9\lambda - 48 \\ 6 \\ 32 - 7\lambda \end{bmatrix}$$

Für $\lambda = 5$ nutzen wir Gauß B2C... Die Lösungsmenge ist hier leer.

Sie können nun konkrete Werte einsetzen, etwa $\lambda = \dots, 3, 4, 6, 7, \dots$, oder allgemein die geforderte Gleichung $A(\lambda)x = e_1$ nachprüfen.

😊 Die Lösung ist eine **rationale Funktion** der Eingabedaten.

Sie sehen an diesem Zahlenbeispiel klar die Vor- und Nachteile, die ich oben bereits zum Determinantenverfahren erläutert habe.

⚠️ Im Sonderfall $\lambda = 5$ gilt $\det A(5) = 0$, die Matrix ist also **singulär**: Das Determinantenverfahren bricht hier zusammen! Wir müssen daher separat rechnen: Das Gauß-Verfahren B2C nützt immer, so auch hier.

$$\left[\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 4 & 5 & 6 & 0 \\ 7 & 8 & 9 & 0 \end{array} \right] \xrightarrow[\text{B2C}]{\text{Gauß}} \left[\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 4/3 \\ 0 & 0 & 0 & 1 \end{array} \right]$$

😊 Da $\det A(5) \in \mathbb{R}$ nicht invertierbar ist, ist auch $A(5) \in \mathbb{R}^{3 \times 3}$ nicht invertierbar (L2G), demnach gilt $\ker A(5) \neq \{0\}$ (B2D). Die Gleichung $Ax = b$ hat also entweder gar keine Lösung oder aber unendlich viele. Das Gauß-Verfahren zeigt hier: e_1 liegt nicht im Bild von $A(5)$.

Satz L2Q: Determinante und Kern einer Matrix

Sei K ein Integritätsring, etwa \mathbb{Z} oder ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Für jede quadratische Matrix $A \in K^{n \times n}$ gilt dann:

$$\det(A) = 0 \iff \ker(A) \neq \{0\}$$

$$\det(A) \neq 0 \iff \ker(A) = \{0\}$$

In Worten: Genau dann gilt $\det A = 0$, wenn die Spalten der Matrix A linear abhängig sind. Dasselbe gilt für die Zeilen der Matrix A (L2K).

Beweis: (1) Für $x \in K^n$ mit $Ax = 0$ gilt dank Cramerscher Regel L2P $\det(A) \cdot x_j = \det(\dots, a_{j-1}, 0, a_{j+1}, \dots) = 0$. Aus $x \neq 0$ folgt $\det(A) = 0$.
 (2) Sei $\ker A = \{0\}$. (a) Ist K ein Körper, dann ist A invertierbar (B2D): Es existiert $B \in K^{n \times n}$ mit $AB = BA = 1_{n \times n}$, somit $\det(A) \det(B) = 1$.
 (b) Wir nutzen den Bruchkörper $\mathbb{Q} \geq K$ (E3L), im Beispiel \mathbb{Z} also $\mathbb{Q} \geq \mathbb{Z}$. Dank (a) gilt $\det_{\mathbb{Q}}^n(A) \neq 0$, dank Leibniz $\det_K^n(A) = \det_{\mathbb{Q}}^n(A)$. QED

😊 Der letzte Schritt des Beweises von Körper zu Integritätsringen ist etwas trickreich. Im konkreten Beispiel $\mathbb{Z} \leq \mathbb{Q}$ ist das Argument leicht: Wir setzen $\ker_{\mathbb{Z}}(A) = \{0\}$ voraus und wollen $\det_{\mathbb{Z}}(A) \neq 0$ zeigen.

Aus $\ker_{\mathbb{Z}}(A) = \{0\}$ folgern wir zunächst $\ker_{\mathbb{Q}}(A) = \{0\}$. Beweis per Kontraposition: Für $0 \neq x \in \mathbb{Q}^n$ mit $Ax = 0$ multiplizieren wir mit einem gemeinsamen Nenner $m \in \mathbb{N}_{\geq 1}$ der Koordinaten $x_1, \dots, x_n \in \mathbb{Q}$ und erhalten $0 \neq mx \in \mathbb{Z}^n$ mit $A(mx) = m(Ax) = 0$, also $mx \in \ker_{\mathbb{Z}}(A)$.

Dank $\ker_{\mathbb{Q}}(A) = \{0\}$ können wir (a) anwenden und schließen, dass A über \mathbb{Q} invertierbar ist (dank Gauß B2D): Es existiert $B \in \mathbb{Q}^{n \times n}$ mit $AB = BA = 1_{n \times n}$, somit $\det_{\mathbb{Q}}^n(A) \det_{\mathbb{Q}}^n(B) = 1$, also $\det_{\mathbb{Q}}^n(A) \neq 0$. Dank Leibniz-Formel L2G folgt schließlich $\det_{\mathbb{Z}}^n(A) = \det_{\mathbb{Q}}^n(A) \neq 0$.

⚠ Wir benötigen für Satz L2Q wirklich einen Integritätsring.

Gegenbeispiel: Die Matrix $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{Z}_6^{2 \times 2}$ hat nicht-verschwindende Determinante $\det A = 2$, doch nicht-trivialen Kern $\ker A = \{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \end{bmatrix} \}$.

Der Beweis zeigt allgemein: Ist $\ker A \neq \{0\}$, so ist $\det A$ ein Nullteiler. In einem Integritätsring, insbesondere Körper, bedeutet das $\det A = 0$.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{Z}^{3 \times 3}.$$

Beispiel: Die drei Spalten der Telefonmatrix $A \in \mathbb{Z}^{3 \times 3}$ sind linear abhängig über \mathbb{Z} , denn $\det A = 0$. Die ersten beiden Spalten sind jedoch linear unabhängig, denn $|\begin{smallmatrix} 4 & 5 \\ 7 & 8 \end{smallmatrix}| = -3$, $|\begin{smallmatrix} 1 & 2 \\ 4 & 5 \end{smallmatrix}| = -3$, $|\begin{smallmatrix} 1 & 2 \\ 7 & 8 \end{smallmatrix}| = -6$.

Satz L2R: Determinantenkriterium für lineare Unabhängigkeit

Sei K ein Integritätsring, etwa \mathbb{Z} oder ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Genau dann sind die Spalten von $A \in K^{n \times r}$ linear unabhängig, wenn es eine Untermatrix M der Größe $r \times r$ gibt mit $\det M \neq 0$.

Beweis: Analog zu Satz L2Q. Versuchen Sie es als Übung!

😊 Im klassischen Fall $K = \mathbb{R}, \mathbb{C}$ ist die Determinante zudem stetig: Wenn wir $a_1, \dots, a_r \in K^n$ nur wenig ändern, so bleiben sie unabhängig!

Zunächst sollten wir den Begriff „Untermatrix“ präzise ausformulieren: Sei $A: I \times J \rightarrow K$ eine Matrix mit $I = \{1, \dots, n\}$ und $J = \{1, \dots, r\}$. Eine **Untermatrix** $M = A|_{I' \times J'}$ der Größe $r \times r$ ist die Einschränkung auf r Zeilen $I' = \{i_1 < \dots < i_r\}$ und r Spalten $J' = \{j_1 < \dots < j_r\}$.

Lösung: „ \Leftarrow “: Sei $M = A|_{I' \times J}$ eine $r \times r$ -Untermatrix mit $\det M \neq 0$. Wir projizieren die Vektoren $a_1, \dots, a_r \in K^I$ vermöge $p: K^I \rightarrow K^{I'}$ durch Einschränkung $a \mapsto a|_{I'}$ der Koordinaten von I auf I' . Sie sind linear unabhängig im Bild $K^{I'}$ (L2Q), also auch in K^I (J1I).

„ \Rightarrow “: (a) Wie im vorigen Beweis von L2Q sei K zunächst ein Körper. Der Gauß-Algorithmus B2C überführt A in Spaltenstufenform A' vom Rang r (K2J). Die Untermatrix M der r Pivotzeilen erfüllt $\det M \neq 0$. (Alternativ kann man A^T in Zeilenstufenform überführen dank L2K.)

(b) Wir nutzen den Bruchkörper $\mathbb{Q} \geq K$ (E3L), im Beispiel \mathbb{Z} also $\mathbb{Q} \geq \mathbb{Z}$. Dank (a) gilt $\det_{\mathbb{Q}}^r(M) \neq 0$, dank Leibniz $\det_K^r(M) = \det_{\mathbb{Q}}^r(M)$. ◻

Adjunkte und Inversionsformel

Wir wenden die Cramersche Regel auf $AX = 1_{n \times n}$ an und erhalten:

Satz L2s: Adjunkte und Inversionsformel

Zu jeder Matrix $A = (a_1, \dots, a_n) \in K^{n \times n}$ definieren wir ihre **adjunkte Matrix** $A' = \text{adj}(A) \in K^{n \times n}$ oder **komplementäre Matrix** durch

$$a'_{ij} := \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n).$$

(1) Die Matrix A und ihre Adjunkte A' erfüllen

$$A' \cdot A = A \cdot A' = \det(A) \cdot 1_{n \times n}.$$

(2) Ist $\det(A)$ in K invertierbar, so auch A in $K^{n \times n}$ dank

$$A^{-1} = \det(A)^{-1} \text{adj}(A).$$

😊 Zur Inversion $A \mapsto A^{-1}$ bietet somit $A^{-1} = \det(A)^{-1} \text{adj}(A)$ eine geschlossene Formel, als rationale Funktion: stetig, differenzierbar.

Adjunkte und Inversionsformel

Beweis: (1a) Wir berechnen $D = A' \cdot A$ koeffizientenweise:

$$\begin{aligned} d_{ik} &\stackrel{\text{Def}}{=} \sum_{j=1}^n a'_{ij} a_{jk} \\ &\stackrel{\text{Def}}{=} \sum_{j=1}^n \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n) a_{jk} \\ &\stackrel{\text{Lin}}{=} \det(a_1, \dots, a_{i-1}, \sum_{j=1}^n e_j a_{jk}, a_{i+1}, \dots, a_n) \\ &\stackrel{\text{Def}}{=} \det(a_1, \dots, a_{i-1}, a_k, a_{i+1}, \dots, a_n) \stackrel{\text{Alt}}{=} \begin{cases} \det(A) & \text{falls } k = i, \\ 0 & \text{falls } k \neq i. \end{cases} \end{aligned}$$

Demnach gilt $A' \cdot A = \det(A) 1_{n \times n}$, wie behauptet.

(1b) Ebenso finden wir $A \cdot A' = \det(A) \cdot 1_{n \times n}$. (Übung!)

Am geschicktesten gelingt dies so: Für die Transponierte $B = A^\top$ finden wir $\text{adj}(B) = \text{adj}(A)^\top$, siehe L275 und L276. Daraus folgt:

$$A \cdot A' = B^\top \cdot B'^\top = (B' \cdot B)^\top = (\det(B) \cdot 1_{n \times n})^\top = \det(A) \cdot 1_{n \times n}$$

(2) Im Falle $\det(A) \in K^\times$ erhalten wir $A^{-1} = \det(A)^{-1} \cdot A'$. □ QED

Determinante und Inversion

Korollar L2T: Determinante und Inversion

Sei K ein kommutativer Ring.

(1) Genau dann ist $A \in K^{n \times n}$ invertierbar, wenn $\det(A) \in K^\times$ dies ist.

$$\mathrm{GL}_n(K) = \{ A \in K^{n \times n} \mid \det(A) \in K^\times \}$$

Für jede invertierbare Matrix $A \in \mathrm{GL}_n(K)$ gilt $\det(A^{-1}) = \det(A)^{-1}$.

(2) Die Matrixinversion ist eine explizit gegebene, rationale Funktion:

$$\iota : \mathrm{GL}_n(K) \rightarrow \mathrm{GL}_n(K) : A \mapsto A^{-1} = \det(A)^{-1} \mathrm{adj}(A)$$

Alle Operationen der Gruppe $(\mathrm{GL}_n(K), \cdot, 1_{n \times n}, \iota)$ sind rational über K , also jeweils ein Bruch von Polynomen in den Matrixkoeffizienten.

Beweis: (1) „ \Rightarrow/\subseteq “: Sei $A \in K^{n \times n}$ invertierbar, das heißt, es existiert $B \in K^{n \times n}$ mit $A \cdot B = B \cdot A = 1_{n \times n}$. Dank Multiplikativität L2N folgt $\det(A) \cdot \det(B) = \det(A \cdot B) = \det(1_{n \times n}) = 1$, also $\det(A) \in K^\times$.

„ \Leftarrow/\supseteq “ und (2): Die Inversionsformel verdanken wir Satz L2s. ◻

Determinante und Inversion

Beispiel: In Dimension $n = 2$ haben wir (L2H):

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

Beispiel: In Dimension $n = 3$ haben wir (L2I):

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

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}$$

😊 Im klassischen Fall $K = \mathbb{R}, \mathbb{C}$ können wir die Stetigkeit nutzen: Wenn wir $A \in \mathrm{GL}_n(K)$ nur wenig ändern, so bleibt $A + \varepsilon S$ invertierbar!

😊 Die Inversion $A \mapsto A^{-1}$ ist rational, und somit nicht nur stetig (\mathcal{C}^0), sondern differenzierbar (\mathcal{C}^1), sogar glatt (\mathcal{C}^∞), gar analytisch (\mathcal{C}^ω), ...

Bemerkung L2U

Sei K ein Körper. In $K^{n \times n}$ ist $GL_n(K) = \{ A \in K^{n \times n} \mid \det(A) \neq 0 \}$ die Nicht-Nullstellen-Menge eines Polynoms in den Koeffizienten.

Über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ folgt daraus (dank Analysis / Topologie): Die Teilmenge $GL_n \mathbb{K} \subset \mathbb{K}^{n \times n}$ ist offen und dicht, und ihr Komplement hat Maß 0:

- 1 Fast alle Matrizen sind invertierbar (volles Lebesgue–Maß),
- 2 nicht-invertierbare werden invertierbar durch kleine Störung,
- 3 invertierbare Matrizen bleiben invertierbar bei kleiner Störung.

Anschaulich bedeutet (1): Wenn Sie zufällig (stetig verteilt) eine Matrix $A \in \mathbb{R}^{n \times n}$ wählen, dann ist diese invertierbar mit Wkt 100%. Das ist klar in Dimension $n = 1$; in Dimension $n \geq 2$ folgt es aus der Determinante.

Ich nenne dies hier als schönen Ausblick. Die nötigen Begriffe und Techniken hierzu lernen Sie in der Analysis und in der Topologie.

Wir ahnen dies bereits im endlichen Fall über \mathbb{F}_q für $q \rightarrow \infty$ (Satz J2H), denn der Anteil der invertierbaren Matrizen konvergiert gegen 100%:

$$\begin{aligned} \frac{\# GL_n \mathbb{F}_q}{\# \mathbb{F}_q^{n \times n}} &= \frac{q^n - 1}{q^n} \cdot \frac{q^n - q}{q^n} \cdots \frac{q^n - q^{n-1}}{q^n} \\ &= (1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n}) \rightarrow 1 \end{aligned}$$

Über einem großen endlichen Körper \mathbb{F}_q ist eine zufällige Matrix also „nahezu sicher“ invertierbar. Über dem unendlichen Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ist dies tatsächlich der Fall, im Sinne des Lebesgue–Maßes.

😊 Die nicht-invertierbaren Matrizen in $\mathbb{K}^{n \times n}$ sind topologisch und maßtheoretisch gesehen also vernachlässigbar. Ihre algebraische Untersuchung ist selbstverständlich trotzdem wichtig, um alle Fälle zu behandeln. Nicht alle Matrizen sind zufällig, ganz im Gegenteil!

Determinante von Dreiecksmatrizen

Aufgabe: Berechnen Sie die Determinante jeder oberen Dreiecksmatrix

$$A = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{bmatrix}$$

(1) mit Spaltenoperationen L2C sowie (2) mit der Leibniz-Formel L2J.

Lösung: (1) Die Determinante ist multilinear, alternierend und normiert (L2L), somit insbesondere invariant unter Transvektionen (L2C). Also:

$$\begin{vmatrix} \lambda_1 & * & * \\ 0 & * & * \\ 0 & 0 & \lambda_n \end{vmatrix} \stackrel[\text{L2C}]{\text{L2L}}{=} \lambda_1 \begin{vmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & 0 & \lambda_n \end{vmatrix} \stackrel[\text{L2C}]{\text{L2L}}{=} \cdots \stackrel[\text{L2C}]{\text{L2L}}{=} \lambda_1 \cdots \lambda_n \begin{vmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{vmatrix} \stackrel{\text{L2L}}{=} \lambda_1 \cdots \lambda_n$$

(2) Nur die Identität $\sigma = \text{id}$ liefert einen Beitrag in der Summe

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}.$$

Auch hier finden wir also $\det(A) = \lambda_1 \cdots \lambda_n$.

Determinante von Dreiecksmatrizen

In der Rechnung (1) nutzen wir die drei definierenden Eigenschaften. Sie sehen hier noch einmal sehr schön, wie diese zusammenwirken:

(a) Aus der i ten Spalte können wir den Faktor λ_i herausziehen.

(b) Durch Transvektionen können wir dann die i te Zeile aufräumen.

Die Schritte (a) und (b) wiederholen wir für alle $i = 1, 2, \dots, n$.

(c) Die Determinante der Einheitsmatrix ist $\det(1_{n \times n}) = 1$.

😊 Wir setzen die Skalare $\lambda_1, \dots, \lambda_n \in K$ nicht als invertierbar voraus. Bitte beachten Sie die sorgsam gewählte Reihenfolge der Operationen in den Schritten (a) und (b), die ganz ohne Divisionen auskommen.

Für solche Rechnungen nutzen wir allgemein die Bemerkung L2W zur Determinante unter Spalten- und Zeilenoperationen.

😊 Die einfache, elegante Rechnung in (2) gelingt sofort. Hier bietet die Leibniz-Formel gewisse Vorteile.

Satz L2v: Determinante einer Dreiecksmatrix

(1) Sei $A \in K^{n \times n}$ eine (obere/untere) Dreiecksmatrix:

$$A = \begin{bmatrix} \lambda_1 & * & * & * \\ 0 & \lambda_2 & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \lambda_n \end{bmatrix} \quad \text{oder} \quad \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ * & \lambda_2 & 0 & 0 \\ * & * & \ddots & 0 \\ * & * & * & \lambda_n \end{bmatrix}$$

In diesem Fall gilt $\det(A) = \lambda_1 \lambda_2 \cdots \lambda_n$ dank Leibniz-Formel L2J.

(2) Entsprechendes gilt für jede (obere/untere) Block-Dreiecksmatrix:

$$A = \begin{bmatrix} A_{11} & * & * & * \\ 0 & A_{22} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & A_{\ell\ell} \end{bmatrix} \quad \text{oder} \quad \begin{bmatrix} A_{11} & 0 & 0 & 0 \\ * & A_{22} & 0 & 0 \\ * & * & \ddots & 0 \\ * & * & * & A_{\ell\ell} \end{bmatrix}$$

In diesem Fall gilt $\det(A) = \det(A_{11}) \cdot \det(A_{22}) \cdots \det(A_{\ell\ell})$ dank L2J.

Beispiel: eine Block-Dreiecksmatrix

Aufgabe: Bestimmen Sie die Determinante der folgenden 9×9 -Matrix:

$$A = \begin{bmatrix} 1 & 2 & * & * & * & * & * & * & * \\ 3 & 4 & * & * & * & * & * & * & * \\ 0 & 0 & 2 & * & * & * & * & * & * \\ 0 & 0 & 0 & 3 & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 4 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 5 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & \lambda & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 & 8 & 9 \end{bmatrix}$$

Lösung: Dies ist eine Block-Dreiecksmatrix (L2v). Daher erhalten wir:

$$\det(A) = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \cdot \begin{vmatrix} 2 & * & * & * \\ 0 & 3 & * & * \\ 0 & 0 & 4 & * \\ 0 & 0 & 0 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{vmatrix} = (-2) \cdot 120 \cdot (60 - 12\lambda) = -2880 \cdot (5 - \lambda)$$

Beweis des Satzes: (1) Wir betrachten eine obere Dreiecksmatrix A und berechnen die Determinante mit der Leibniz-Formel L2J:

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}$$

Gilt $\sigma(i) > i$ für einen Index i , so ist dieser Summand gleich Null.

Die einzige Permutation $\sigma \in S_n$ mit $\sigma(i) \leq i$ für alle i ist $\sigma = \text{id}$.

Daraus folgt $\det(A) = \lambda_1 \lambda_2 \cdots \lambda_n$, wie im Satz angegeben.

😊 Alternativ zur Leibniz-Formel können wir Spaltenoperationen oder Zeilenoperationen nutzen, wie in der vorigen Aufgabe L249 ausgeführt. Beide Sichtweisen sind lehrreich und führen zum ersehnten Ergebnis.

(2) Die allgemeine Formel für Block-Dreiecksmatrizen beweisen wir ganz genauso, lediglich die Buchführung der Summe ist aufwändiger.

😊 Die Idee ist ganz anschaulich: Eine Permutationen $\sigma \in S_n$ trägt nur dann etwas bei, wenn Sie auf den diagonalen Matrizen gefangen ist.

(a) Wir betrachten eine obere Block-Dreiecksmatrix, auf der Diagonalen stehen die Matrizen $A_{11}, \dots, A_{\ell\ell}$ mit $A_{jj} \in K^{n_j \times n_j}$ der Größe $n_j \in \mathbb{N}_{\geq 1}$.

Wir zerlegen die Indexmenge $I = \{1, \dots, n\}$ mit $n = n_1 + \dots + n_\ell$ in $I = I_1 \sqcup \dots \sqcup I_\ell$ mit $I_1 = \{1, \dots, n_1\}$ und $I_j = \max I_{j-1} + \{1, \dots, n_j\}$.

Gilt $\sigma(i) > I_j$ für einen Index $i \in I_j$, so ist dieser Summand gleich Null. Es bleiben nur die Permutationen $\sigma \in S_n$ mit $\sigma(I_j) = I_j$ für $j = 1, \dots, \ell$.

(b) Wir nutzen die Untergruppe $U = \text{Sym}(I_1) \times \dots \times \text{Sym}(I_\ell) \leq \text{Sym}(I)$. Für $\sigma \in U$ haben wir die Zerlegung $\sigma = \sigma_1 \sqcup \dots \sqcup \sigma_\ell$ mit $\sigma_j \in \text{Sym}(I_j)$.

Die Signatur ist multiplikativ gemäß $\text{sign}(\sigma) = \text{sign}(\sigma_1) \cdots \text{sign}(\sigma_\ell)$; dies sehen wir an den Fehlständen oder der Zykelzerlegung.

(c) Mit diesen Vorbereitungen berechnen wir die Determinante:

$$\begin{aligned}
 \det(A) &\stackrel{\text{Def}}{=} \sum_{\sigma \in \text{Sym}(I)} \text{sign}(\sigma) \prod_{i \in I} a_{\sigma(i),i} \\
 &\stackrel{(a)}{=} \sum_{\sigma \in U} \text{sign}(\sigma) \prod_{i \in I} a_{\sigma(i),i} \\
 &\stackrel{(b)}{=} \sum_{\sigma \in U} \prod_{j=1}^{\ell} \text{sign}(\sigma_j) \prod_{i \in I_j} a_{\sigma_j(i),i} \\
 &\stackrel{(b)}{=} \prod_{j=1}^{\ell} \sum_{\sigma_j \in \text{Sym}(I_j)} \text{sign}(\sigma_j) \prod_{i \in I_j} a_{\sigma_j(i),i} \\
 &\stackrel{\text{Def}}{=} \prod_{j=1}^{\ell} \det(A_{jj})
 \end{aligned}$$

Wir erhalten also $\det(A) = \det(A_{11}) \cdot \det(A_{22}) \cdots \det(A_{\ell\ell})$.

QED

Die Idee ist anschaulich klar: Eine Permutationen $\sigma \in S_n$ trägt nur dann etwas bei, wenn Sie auf den diagonalen Matrizen gefangen ist, $\sigma \in U$.

Damit können wir die Summe der Leibniz-Formel nun umformen. Hier sehen Sie, wie es geht. Wie immer gilt: Gute Notation hilft!

Bemerkung: Alternativ zur Leibniz-Formel können wir auch für jede Block-Dreiecksmatrix A Zeilenoperationen bzw. Spaltenoperationen nutzen, um A auf Dreiecksform $A' = SA$ bzw. $A'' = AT$ zu bringen.

Dies geschieht separat in jedem Block A_{jj} , also erhalten wir auch hier

$$\det(A) = \det(A_{11}) \cdot \det(A_{22}) \cdots \det(A_{\ell\ell}).$$

Übung: Führen Sie auch diese zweite Beweisidee sorgfältig aus. Vergleichen Sie beide Beweise: Welcher gefällt Ihnen besser?

😊 Bei diesen Rechnungen nutzen wir die Bemerkung L2w zur Determinante unter Spalten- und Zeilenoperationen.

Bemerkung L2w: Spalten- und Zeilenoperationen

Elementare Spaltenoperationen ändern die Determinante wie folgt:

- 1 Transvektion $T_{ij}(\lambda)$ ändert nichts (L2c), $\det(T_{ij}(\lambda)) = 1$.
- 2 Skalierung $S_i(\mu)$ multipliziert mit μ (L2L), $\det(S_i(\mu)) = \mu$.
- 3 Vertauschung P_{ij} multipliziert mit -1 (L2E), $\det(P_\sigma) = \text{sign}(\sigma)$.

Dasselbe gilt für Zeilenoperationen, dank Transpositionsinvarianz L2k.

Über jedem Körper K erhalten wir daraus den folgenden Algorithmus:

Algo L2x: Berechnung der Determinante

Eingabe: eine Matrix $A \in K^{n \times n}$ über einem Körper K

Ausgabe: die Determinante $\det(A) \in K$

- 1: Bringe A in Dreiecksform $B = SA$, etwa mit Gauß B2c
- 2: **return** $\det(A) = \det(S)^{-1} \det(B)$ dank L2N und L2w

😊 Die Berechnung gelingt mit höchstens n^3 Operationen in K .

Wir nutzen gerne und erfolgreich die Umformung von Matrizen mittels elementarer Zeilen- und Spaltenoperationen. Bemerkung L2w fasst zusammen, wie sich die Determinante bei diesen Umformungen verhält.

😊 Insbesondere können wir über einem Körper das Gauß–Verfahren anwenden, um die Determinante zu berechnen. Beides sind starke Methoden, und sie fügen sich hier nun wunderbar zusammen.

😊 Das Gauß–Verfahren B2c ist sehr effizient: Es benötigt $\leq n^2$ Zeilenoperationen und $\leq n^3$ arithmetische Operationen in K .

Das ist eine gigantische Verbesserung gegenüber den fatalen $n \cdot n!$ Operationen, die eine naive Anwendung der Leibniz–Formel erfordert. Um diesen Unterschied möglichst eindrücklich zu illustrieren, stelle ich die ersten Werte von n^3 und $n \cdot n!$ in der folgenden Tabelle gegenüber.

Übung: Wie lange benötigt ein Rechner mit einer Billion Operationen pro Sekunde? (TerraFlops = 10^{12} floating point operations per second)

Vergleich von Gauß–Verfahren und Leibniz–Formel:

| Größe n | Aufwand n^3 | Aufwand $n \cdot n!$ |
|-----------|---------------|---------------------------|
| 1 | 1 | 1 |
| 2 | 8 | 4 |
| 3 | 27 | 18 |
| 4 | 64 | 96 |
| 5 | 125 | 600 |
| 6 | 216 | 4320 |
| 7 | 343 | 35 280 |
| 8 | 512 | 322 560 |
| 9 | 729 | 3 265 920 |
| 10 | 1000 | 36 288 000 |
| 20 | 8000 | $\approx 5 \cdot 10^{19}$ |
| 30 | 27000 | $\approx 8 \cdot 10^{33}$ |
| 40 | 64000 | $\approx 3 \cdot 10^{49}$ |

Sie sehen an dieser Tabelle: Für $n = 2, 3$ liegen beide Verfahren gleich auf, je nach Zählung noch mit leichtem Vorteil für die Leibniz–Formel.

Ab $n = 4$ macht sich die Bürde der Fakultät in $n \cdot n!$ bemerkbar, und für $n \geq 5$ explodiert dieser Term geradezu, während n^3 moderat wächst.

Das erklärt eindrücklich, warum die Berechnung der Determinante mit der Leibniz–Formel für $n = 2, 3$ recht beliebt ist, aber danach nicht mehr!

 Wählen Sie Ihren Rechenweg immer mit Bedacht und Umsicht! Egal ob Sie selbst per Hand rechnen oder den Computer rechnen lassen, die Anzahl der Rechenschritte ist eine wichtige Ressource.

Das Ergebnis ist zwar *theoretisch* auf beiden Wegen dasselbe, doch diese Garantie nützt Ihnen *praktisch* herzlich wenig, wenn Sie Jahre, Jahrtausende oder Jahrmillionen auf das Ergebnis warten müssen.

 Es ist schön und nützlich, dass wir dank Leibniz für die Determinante über eine polynomielle Darstellung verfügen. Diese Formel hat viele gute Eigenschaften, effiziente Berechenbarkeit gehört nicht dazu. Diesen Teil übernimmt Gauß. Gemeinsam sind sie stark!

Aufgabe: Berechnen Sie die Determinante der folgenden Matrix:

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{bmatrix}$$

- (0) Ist die Leibniz–Formel hier geeignet? (1) Wie effizient ist Gauß?
 (2) Geht es mit Umsicht und Geschick noch besser? Anleitung:
 (3) Subtrahiere die i te Zeile von der $(i - 1)$ ten Zeile für $i = 2, \dots, 10$.
 Anschließend addiere die erste Spalte zu jeder weiteren Spalte.

Manche Menschen behaupten, die Determinante großer Matrizen könne man nicht mit vertretbarem Aufwand berechnen. Das ist nicht wahr! Hier sehen Sie eine 10×10 –Matrix, die Sie per Hand ausrechnen. Wenn Sie geschickt vorgehen, dann ist die Rechnung sogar leicht.

😊 Gauß geht immer, diese Methode löst das allgemeine Problem. Dieses universelle Verfahren ist weiterhin unser treues Arbeitspferd. Das stumpfsinnige Rechnen macht dem Computer rein gar nichts aus — mir schon! Und ich bin mir sicher, Ihnen geht es ganz ähnlich.

😊 Wenn Sie von Hand rechnen, dann möchten Sie genauer hinsehen und Vereinfachungen nutzen, um den Aufwand weiter zu reduzieren. Daher ist die sture Anwendung des Gauß–Algorithmus zwar möglich, sie führt immer zum Ziel, aber sie ist nicht immer der beste Weg.

Typische Strategie: Wie kommen wir schnell zu einer Dreiecksmatrix? Im vorliegenden Beispiel gibt die Aufgabenstellung eine Anleitung.

Lösung: (3) Wir gehen geschickt vor und/oder folgen der Anleitung.
Wir subtrahieren die i te Zeile von der $(i - 1)$ ten Zeile für $i = 2, \dots, 10$:

$$\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix}$$

Die Determinante bleibt dabei gleich: Transvektion ändert nichts (L2w).
Dass dies ein Schritt in die richtige Richtung ist, sehen wir gleich...

 Ausprobieren
mit Gaël!

Wir addieren die erste Spalte zu jeder weiteren Spalte:

$$\begin{vmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & -2 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & -2 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & -2 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & -2 & 0 & 0 \\ * & * & * & * & * & * & * & * & -2 & 0 \\ * & * & * & * & * & * & * & * & * & 9 \end{vmatrix}$$

So gewinnen wir eine Dreiecksmatrix (L2v). Nun lesen wir mühelos ab:

$$\det(A) = -9 \cdot (-2)^8 = -2304$$

Sie können die Matrix A auch stur nach Gauß-Algorithmus behandeln.
Probieren Sie es aus, am besten mit unserem Online-Tool Gaël!

Die Vandermonde–Determinante

Aufgabe: Berechnen Sie die Determinante der Vandermonde–Matrix

$$V = V(x_0, \dots, x_n) := (x_i^j)_{i=0,1,\dots,n}^{j=0,1,\dots,n} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix}.$$

Diese berühmte Matrix tritt häufig auf, insbesondere bei der Polynominterpolation, siehe B309. Ihre Invertierbarkeit haben wir in Satz B3A bereits geklärt, nun berechnen wir explizit ihre Determinante $\det V$.

Lösung: Wir berechnen die kleinen Fälle und suchen nach Mustern. Diese wollen wir anschließend für alle $n \in \mathbb{N}$ per Induktion beweisen. Der Fall $n = 0$ ist trivial, der Fall $n = 1$ sehr einfach:

$$|1| = 1, \quad \begin{vmatrix} 1 & x_0 \\ 1 & x_1 \end{vmatrix} = x_1 - x_0$$

Hieran erkennen wir leider noch keine allgemeine Regel.

Die Vandermonde–Determinante

Für $n = 2$ suchen wir insbesondere nach einer Rekursion:

$$\begin{vmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{vmatrix} \stackrel{(1)}{=} \begin{vmatrix} 1 & x_0 & x_0^2 \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 \\ 0 & x_2 - x_0 & x_2^2 - x_0^2 \end{vmatrix}$$

(1) Spalte 0 aufräumen: Wir subtrahieren Zeile 0 von jeder Zeile $i > 0$.

(2) Wir ziehen den Faktor $(x_i - x_0)$ aus jeder Zeile $i > 0$ (dank G2D):

$$\begin{vmatrix} 1 & x_0 & x_0^2 \\ 0 & 1 & x_1 + x_0 \\ 0 & 1 & x_2 + x_0 \end{vmatrix} \stackrel{(3)}{=} \begin{vmatrix} 1 & x_0 & 0 \\ 0 & 1 & x_1 \\ 0 & 1 & x_2 \end{vmatrix}$$

(3) Aufräumen: Wir subtrahieren x_0 mal Spalte 1 von Spalte 2.

Wir erhalten so eine Block-Dreiecksmatrix aus 1 und $V(x_1, x_2)$.

Nun können wir den vorigen Fall $n = 1$ anwenden! Wir erhalten:

$$\begin{vmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{vmatrix} = (x_1 - x_0)(x_2 - x_0)(x_2 - x_1) = \prod_{i < j} (x_j - x_i)$$

Die Vandermonde–Determinante

Satz L2Y: die Vandermonde–Matrix und ihre Determinante

Sei K ein kommutativer Ring und $x_0, x_1, \dots, x_n \in K$. Dann gilt:

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix} \implies \det V = \prod_{i < j} (x_j - x_i)$$

Beweis: Dies folgt per Induktion über n nach dem obigen Vorbild. QED

Aufgabe: Führen Sie den nächsten Fall $n = 3$ aus, dann allgemein.

Das ist eine gute Übung zur Rechenfertigkeit mit Determinanten.

Wie so oft verstehen Sie es erst, wenn Sie es selbst tun!

Erkläre es mir, und ich werde es vergessen.

Zeige es mir, und ich werde mich erinnern.

Lass es mich tun, und ich werde es verstehen.

(Konfuzius, 551–497 v.Chr.)

Die Vandermonde–Determinante

Lösung: Für $n = 3$ verfahren wir nach obigem Muster:

$$\begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \end{vmatrix} \stackrel{(1)}{=} \begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 & x_1^3 - x_0^3 \\ 0 & x_2 - x_0 & x_2^2 - x_0^2 & x_2^3 - x_0^3 \\ 0 & x_3 - x_0 & x_3^2 - x_0^2 & x_3^3 - x_0^3 \end{vmatrix}$$

(1) Spalte 0 aufräumen: Wir subtrahieren Zeile 0 von jeder Zeile $i > 0$.

(2) Wir ziehen den Faktor $(x_i - x_0)$ aus jeder Zeile $i > 0$ (dank G2D):

$$\begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 0 & 1 & x_1 + x_0 & x_1^2 + x_1 x_0 + x_0^2 \\ 0 & 1 & x_2 + x_0 & x_2^2 + x_2 x_0 + x_0^2 \\ 0 & 1 & x_3 + x_0 & x_3^2 + x_3 x_0 + x_0^2 \end{vmatrix} \stackrel{(3)}{=} \begin{vmatrix} 1 & x_0 & 0 & 0 \\ 0 & 1 & x_1 & x_1^2 \\ 0 & 1 & x_2 & x_2^2 \\ 0 & 1 & x_3 & x_3^2 \end{vmatrix}$$

(3) Aufräumen: Wir subtrahieren x_0 mal Spalte 1 von Spalte 2, dann x_0^2 mal Spalte 1 von Spalte 3, und x_0 mal Spalte 2 von Spalte 3. Voilà!

😊 Der allgemeine Induktionsbeweis verläuft ganz genau so.

Die Vandermonde–Determinante

L271
Erläuterung

Die Vandermonde–Determinante

L272
Erläuterung

Die Streichungsmatrix A_{ij}

Aus $A \in K^{n \times n}$ bilden wir die **Streichungsmatrix** $A_{ij} \in K^{(n-1) \times (n-1)}$:

$$A_{ij} = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i,1} & \dots & a_{i,j-1} & a_{i,j} & a_{i,j+1} & \dots & a_{i,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}$$

Wir löschen aus A die i te Zeile und die j te Spalte und erhalten A_{ij} . Die so entstehende Matrix hat eine Zeile und eine Spalte weniger.

Diese Streichungsmatrix A_{ij} können wir recht häufig zur rekursiven Berechnung nutzen, wie die folgenden typischen Beispiele zeigen.

Die Ersetzungsmatrix A_{ij}^+

Beispiel: Aus der Matrix $A \in K^{n \times n}$ bilden wir die **Ersetzungsmatrix**

$$A_{ij}^+ = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}.$$

Wir tauschen (i, j) nach $(1, 1)$ und erhalten eine Block-Diagonalmatrix:

$$\det A_{ij}^+ = (-1)^{i+j} \det A_{ij}$$

Von unserer Matrix A_{ij}^+ zur Block-Diagonalmatrix $\text{diag}(1, A_{ij})$ tauschen wir $i - 1$ mal benachbarte Zeilen und $j - 1$ mal benachbarte Spalten, daher das Vorzeichen $(-1)^{i+j-2} = (-1)^{i+j}$. In Blockform können wir schließlich Satz L2v anwenden und erhalten $\det \text{diag}(1, A_{ij}) = \det A_{ij}$.

Beispiel: In der Matrix $A \in K^{n \times n}$ ersetzen wir die j te Spalte durch e_i :

$$A_{ij}^! = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i,1} & \dots & a_{i,j-1} & 1 & a_{i,j+1} & \dots & a_{i,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}$$

Wir tauschen (i, j) nach $(1, 1)$ zu einer oberen Block-Dreiecksmatrix:

$$\det A_{ij}^! = (-1)^{i+j} \det A_{ij}$$

Das Vorzeichen entsteht genau wie zuvor für die Matrix A_{ij}^+ erklärt.

Alternativ: $\det A_{ij}^! = \det A_{ij}^+$ durch Leerräumen der i ten Zeile (L2w).

Beispiel: In der Matrix $A \in K^{n \times n}$ ersetzen wir die i te Zeile durch e_j^T :

$$A_{ij}^- = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}$$

Wir tauschen (i, j) nach $(1, 1)$ zu einer unteren Block-Dreiecksmatrix:

$$\det A_{ij}^- = (-1)^{i+j} \det A_{ij}$$

Das Vorzeichen entsteht genau wie zuvor für die Matrix A_{ij}^+ erklärt.

Alternativ: $\det A_{ij}^- = \det A_{ij}^+$ durch Leerräumen der j ten Spalte (L2w).

Die rekursive Laplace–Entwicklung

Satz L2z: Entwicklungssatz von Laplace

Die Determinante von $A \in K^{n \times n}$ lässt sich rekursiv berechnen durch Entwicklung nach der j ten Spalte oder nach der i ten Zeile:

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

Hierbei entsteht A_{ij} durch Streichen der i ten Zeile und der j ten Spalte.

Beweis: (1) Die j te Spalte ist $a_j = \sum_{i=1}^n e_i a_{ij}$, also gilt:

$$\begin{aligned} \det A &= \det(a_1, \dots, a_{j-1}, \sum_{i=1}^n e_i a_{ij}, a_{j+1}, \dots, a_n) \\ &= \sum_{i=1}^n a_{ij} \det(a_1, \dots, a_{j-1}, e_i, a_{j+1}, \dots, a_n) \\ &= \sum_{i=1}^n a_{ij} \det A_{ij} = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det A_{ij} \end{aligned}$$

(2) Entsprechend entwickeln wir nach der i ten Zeile (L2k). □

Notation: Das Produkt $\tilde{a}_{ij} := (-1)^{i+j} \det A_{ij}$ heißt der **Cofaktor** zu a_{ij} . Die Cofaktormatrix $\tilde{A} = (\tilde{a}_{ij})_{ij}$ ist transponiert zur Adjunkten $\text{adj}(A)$.

Die rekursive Laplace–Entwicklung

Das hier auftretende Vorzeichen $(-1)^{i+j}$ bildet ein Schachbrettmuster:

$$\begin{bmatrix} + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \end{bmatrix}$$

Die Laplace–Entwicklung ist eine Umformulierung der Leibniz–Formel, die Summe über alle Permutationen in S_n wird nur anders durchlaufen. Beide haben zunächst denselben Aufwand und sind gleich in/effizient.

😊 Die Laplace–Entwicklung lohnt sich, wenn A viele Nullen enthält: Diese Terme fallen sofort weg, und die Rechnung vereinfacht sich.

Die rekursive Laplace–Entwicklung

Aufgabe: Entwickeln Sie geschickt die Determinante von

$$A = \begin{bmatrix} 7 & 3 & 0 \\ 2 & 1 & 5 \\ 4 & 2 & 0 \end{bmatrix} \quad \text{und} \quad B = \begin{bmatrix} 3 & 1 & 2 & 2 \\ 4 & 0 & 0 & 2 \\ 7 & 2 & 1 & 0 \\ 0 & 5 & 8 & 3 \end{bmatrix}.$$

Lösung: (1) Wir entwickeln $\det(A)$ nach der dritten Spalte:

$$\begin{vmatrix} 7 & 3 & 0 \\ 2 & 1 & 5 \\ 4 & 2 & 0 \end{vmatrix} = +0 \cdot \begin{vmatrix} 2 & 1 \\ 4 & 2 \end{vmatrix} - 5 \cdot \begin{vmatrix} 7 & 3 \\ 4 & 2 \end{vmatrix} + 0 \cdot \begin{vmatrix} 7 & 3 \\ 2 & 1 \end{vmatrix} = (-5) \cdot 2 = -10$$

(2) Wir entwickeln $\det(B)$ nach der zweiten Zeile:

$$\begin{vmatrix} 3 & 1 & 2 & 2 \\ 4 & 0 & 0 & 2 \\ 7 & 2 & 1 & 0 \\ 0 & 5 & 8 & 3 \end{vmatrix} = -4 \begin{vmatrix} 1 & 2 & 2 \\ 7 & 1 & 0 \\ 0 & 8 & 3 \end{vmatrix} + 0 \begin{vmatrix} 3 & 2 & 2 \\ 7 & 1 & 0 \\ 0 & 8 & 3 \end{vmatrix} + 0 \begin{vmatrix} 3 & 1 & 2 \\ 7 & 2 & 0 \\ 0 & 5 & 3 \end{vmatrix} + 2 \begin{vmatrix} 3 & 1 & 2 \\ 7 & 2 & 1 \\ 0 & 5 & 8 \end{vmatrix} \\ = -4 \cdot [2 \cdot 11 + 3 \cdot (-3)] + 2 \cdot [3 \cdot 11 - 7 \cdot (-2)] = 42$$

Die rekursive Laplace–Entwicklung

Ausprobieren
mit Gaël!

Das Beispiel A ist sehr klein und einfach, Sie durchschauen es sofort. Als Service und zur Betonung habe ich auch die Nullterme angegeben; sie fallen weg, und normalerweise würde man sie direkt übergehen. Sie dienen hier allein zur graphischen Erklärung des Verfahrens.

Beim Beispiel B hingegen müssen wir schon etwas länger rechnen. Insbesondere spüren Sie, dass es sich um eine Rekursion handelt: Die 3×3 –Streichungsmatrizen müssen ebenfalls berechnet werden. Die Einsparung entsteht allein durch die Nullterme!

😊 Es lohnt sich für B bereits, den Gauß–Algorithmus zu nutzen!

Übung: Berechnen Sie $\det(A)$ und $\det(B)$ zum direkten Vergleich durch Zeilen- und Spaltenumformungen wie im Gauß–Algorithmus.

Wie viele Operationen in K benötigen Sie jeweils?

Übung: Ohne Einsparungen durch Nulleinträge hat die rekursive Laplace–Entwicklung denselben Aufwand wie die Leibniz–Formel: Beide benötigen $n \cdot n!$ Operationen im Grundkörper K .

Ist jede invertierbare Matrix quadratisch?

$$\begin{array}{ccc}
 \begin{array}{|c|c|c|c|} \hline 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ \hline \end{array} & \cdot & \begin{array}{|c|c|c|} \hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline \end{array} & \stackrel{!}{=} & \begin{array}{|c|c|c|} \hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline \end{array} \\
 \\
 \begin{array}{|c|} \hline A \\ \hline \end{array} & \cdot & \begin{array}{|c|} \hline B \\ \hline \end{array} & \stackrel{?}{=} & \begin{array}{|c|c|c|c|} \hline 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \\ \hline \end{array}
 \end{array}$$

Gibt es invertierbare Matrizen $A \in R^{n \times m}$, die nicht quadratisch sind?

- Ja, klar, über dem Nullring $R = \{0\}$ mit $0 = 1$ ist das trivial.
- Es gibt weitere Beispiele (J10), etwa über $R = \text{End}_K(K[X])$.

Damit gilt $R^m \cong R^n$; der Begriff „Dimension“ hat dann keinen Sinn.

Viele „vernünftige“ Ringe erfüllen die Invarianz der Dimension (J1L):

- Über jedem Divisionsring haben wir den Gauß–Algorithmus (B2D).
- Über jedem kommutativen Ring haben wir die Determinante (L2G).

Ist jede invertierbare Matrix quadratisch?

😊 Erst die Invarianz der Dimension, wie in J1L definiert, erlaubt es uns, jedem freien R –linearen Raum V eine Dimension $\dim_R(V)$ zuzuordnen.

⚠ Über manchen Ringen hat der Begriff „Dimension“ keinen Sinn!

Zur Erinnerung (J10): Sei K ein Körper. Im Ring $R = \text{End}_K(K[X])$ haben wir die Elemente $a: P(X) \mapsto P(X^2)$ und $b: P(X) \mapsto XP(X^2)$ sowie $(c, d): P \mapsto (P_0, P_1)$ mit $P = P_0(X^2) + XP_1(X^2)$, also explizit

$$\begin{aligned}
 a(P) &= (p_0, 0, p_1, 0, p_2, 0, \dots), & c(P) &= (p_0, p_2, p_4, p_6, p_8, \dots), \\
 b(P) &= (0, p_0, 0, p_1, 0, p_2, \dots), & d(P) &= (p_1, p_3, p_5, p_7, p_9, \dots).
 \end{aligned}$$

Überraschenderweise gelten damit die Gleichungen

$$\begin{pmatrix} c \\ d \end{pmatrix} (a \ b) = \begin{pmatrix} ca & cb \\ da & db \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad (a \ b) \begin{pmatrix} c \\ d \end{pmatrix} = ac + bd = 1.$$

Die Matrizen $\begin{pmatrix} c \\ d \end{pmatrix}$ und $(a \ b)$ stiften somit einen Isomorphismus $R^1 \cong R^2$. Wider die Intuition haben wir also die verblüffende Gleichung

$$\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Satz L3A: invertierbare Matrizen

Gegeben sei ein kommutativer Ring K mit $0 \neq 1$. Seien $m, n \in \mathbb{N}$.

- (1) Für alle $A \in K^{n \times m}$ und $B \in K^{m \times n}$ mit $A \cdot B = 1_{n \times n}$ gilt $m \geq n$.
 (2) Ist die Matrix $A \in K^{n \times m}$ invertierbar, so folgt $n = m$.

Beweis: (1) Angenommen, es gäbe ein Gegenbeispiel mit $m < n$.

Wir ergänzen A, B zu $A', B' \in K^{n \times n}$ durch Nullspalten bzw. Nullzeilen:

$$\begin{array}{|c|c|} \hline A & 0 \\ \hline \end{array} \cdot \begin{array}{|c|} \hline B \\ \hline 0 \\ \hline \end{array} = \begin{array}{|cccc|} \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline \end{array}$$

Weiter gilt $A' \cdot B' = 1_{n \times n}$. Auf quadratische (!) Matrizen können wir die Determinante anwenden. Die Determinante ist multiplikativ (L2N), also:

$$\det(A') \cdot \det(B') = \det(A' \cdot B') = \det(1_{n \times n}) = 1$$

Andererseits gilt $\det(A') = \det(B') = 0$ (L2B), ein Widerspruch!

QED

😊 Es gibt weitere Beweise für diese fundamentale Eigenschaft (1). Über jedem Divisionsring gilt (1) dank Gauß-Algorithmus (B2D).

Satz L3B: Transferprinzip

Sei $\varphi: S \rightarrow R$ ein Homomorphismus von Ringen (hier immer mit Eins). Gilt die Aussage (1) über dem Ring R , so auch über dem Ring S .

Beweis: Wir setzen φ komponentenweise fort zu $\varphi: S^{p \times q} \rightarrow R^{p \times q}$. Dies respektiert die Addition und die Multiplikation von Matrizen.

Gegeben seien Matrizen $A \in S^{n \times m}$ und $B \in S^{m \times n}$ mit $A \cdot B = 1_{n \times n}$. Daraus folgt $\varphi(A) \cdot \varphi(B) = \varphi(A \cdot B) = \varphi(1_{n \times n}) = \varphi(1_{n \times n})$ über R . Nach Voraussetzung über R gilt demnach $m \geq n$. **QED**

Beispiel: Für den Ring \mathbb{Z} können wir die Einbettung $\text{inc}: \mathbb{Z} \hookrightarrow \mathbb{Q}$ nutzen und ebenso den Quotienten $q: \mathbb{Z} \twoheadrightarrow \mathbb{F}_p$ für eine Primzahl $p \in \mathbb{N}_{\geq 2}$:

😊 So können wir für den Ring \mathbb{Z} neben der Determinante L3A auch den Gauß-Algorithmus B2D nutzen, indirekt über $\mathbb{Z} \hookrightarrow \mathbb{Q}$ oder $\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$.

Satz L3C: Invarianz der Dimension

Sei K ein kommutativer Ring mit $0 \neq 1$. Für alle $m, n \in \mathbb{N}$ gilt:

- 1 Ist $f : K^m \twoheadrightarrow K^n$ eine K -lineare Surjektion, so gilt $m \geq n$.
- 2 Ist $f : K^m \hookrightarrow K^n$ eine K -lineare Injektion, so gilt $m \leq n$.
- 3 Ist $f : K^m \xrightarrow{\sim} K^n$ eine K -lineare Bijektion, so gilt $m = n$.

Somit erfüllt der Ring K die Invarianz der Dimension (J1L).

Beweis: (1) Zu jedem $i = 1, \dots, n$ wählen wir $v_i \in K^m$ mit $f(v_i) = e_i$. Sei $g : K^n \rightarrow K^m$ die lineare Abbildung mit $g(e_i) = v_i$ (PLF, Satz K1B). Damit gilt $f \circ g = \text{id}_{K^n}$ (K1A). Die darstellenden Matrizen $A \in K^{n \times m}$ zu f und $B \in K^{m \times n}$ zu g erfüllen $A \cdot B = 1_{n \times n}$. Daraus folgt $m \geq n$ (L3A).
 (3) Dank (1) gilt $m \geq n$. Mit $f^{-1} : K^n \xrightarrow{\sim} K^m$ (I1G) folgt $n \geq m$. □

Aussage (2) ist algebraisch raffinierter und wird hier nicht bewiesen. Zwecks Symmetrie will ich jedoch alle drei Aussagen beisammen halten.

Die Aussage des Satzes ist die vertraute Invarianz der Dimension, die Sie bereits aus Kapitel J kennen, nun über kommutativen Ringen. Der Satz gilt auch über Divisionsringen dank Gauß-Algorithmus (J1K). Beide Versionen beinhalten kommutative Divisionsringe, also Körper

Zum Beweis benötigen wir stichhaltige Argumente, und dies gelingt mit starken Werkzeugen: über kommutativen Ringen die Determinante, über Divisionsringen der Gauß-Algorithmus.

Bemerkung: Zur Dimension $\dim_R(V)$ benötigen wir zwei Zutaten:

- 1 Der R -lineare Raum V muss frei sein, also mindestens eine Basis haben; das gilt leider nicht immer, siehe J1B. Es gilt für alle Vektorräume, siehe J2B und J2C.
- 2 Der Ring R muss die Invarianz der Dimension erfüllen: Je zwei Basen von V haben dann dieselbe Länge. Dazu haben wir die Sätze J1K und L3C.

Ein erstes Anwendungsbeispiel

- Aufgabe:** (1) Sind die Gruppen $(\mathbb{Z}^m, +)$ und $(\mathbb{Z}^n, +)$ isomorph?
 (2) Wie viele Homomorphismen $(\mathbb{Z}^n, +) \rightarrow (\mathbb{Z}/a, +)$ gibt es für $a \in \mathbb{N}_{\geq 2}$?
 (3) Lösen Sie mit der Rechnung (2) erneut das Isomorphieproblem (1).

Lösung: (1) Jede abelsche Gruppe ist ein \mathbb{Z} -linearer Raum (I1K), und jeder Gruppenhomomorphismus ist automatisch linear über \mathbb{Z} . Dank Invarianz der Dimension L3C gilt: Aus $\mathbb{Z}^m \cong \mathbb{Z}^n$ folgt $m = n$.

(2) Glücklicherweise ist \mathbb{Z}^n frei über \mathbb{Z} , mit Basis e_1, \dots, e_n (J1C). Dank Prinzip der linearen Fortsetzung (K1B) haben wir die Bijektion

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}/a) \xrightarrow{\sim} \text{Abb}(\{e_1, \dots, e_n\}, \mathbb{Z}/a) : f \mapsto f|_B.$$

Demnach gilt $\sharp \text{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}/a) = a^n$. Anschaulich: Wir müssen für jeden der Basisvektoren e_1, \dots, e_n ein Bildelement $f(e_k) \in \mathbb{Z}/a$ vorgeben.

(3) Aus der Isomorphie $(\mathbb{Z}^m, +) \cong (\mathbb{Z}^n, +)$ folgt die Gleichheit von $\sharp \text{Hom}_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}/a) = a^m$ und $\sharp \text{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}/a) = a^n$, also $m = n$ (A1B).

Ein erstes Anwendungsbeispiel

😊 Dieser einfache Trick (2) beantwortet die Frage (1) direkt durch Abzählen, ohne Determinante oder Gauß-Algorithmus.

Für je zwei natürliche Zahlen $m \neq n$ gilt demnach $\mathbb{Z}^m \not\cong \mathbb{Z}^n$.

Für diese grundlegende Tatsache gibt es viele schöne Beweise...

Den ersten Beweis (1) habe ich zur Illustration des Invarianzsatzes L3C angeführt. Er schießt zwar mit Kanonen auf Spatzen... doch er trifft.

Auch der zweite Beweis (2) ist lehrreich, denn er betont das Prinzip der linearen Fortsetzung und ist ansonsten vollkommen elementar.

Bemerkung: Der wohl einfachste Beweis gelingt mit der Spur (B1I):

$$\text{tr} = \text{tr}_n : \mathbb{Z}^{n \times n} \rightarrow \mathbb{Z} : A \mapsto \sum_{k=1}^n a_{kk} = a_{11} + a_{22} + \dots + a_{nn}$$

Aus $(f, g) : \mathbb{Z}^n \cong \mathbb{Z}^m$ erhalten wir Matrizen $A \in \mathbb{Z}^{m \times n}$ und $B \in \mathbb{Z}^{n \times m}$ mit $AB = 1_{m \times m}$ und $BA = 1_{n \times n}$. Daraus folgt $\text{tr}(AB) = m$ und $\text{tr}(BA) = n$. Dank Satz B1J gilt $\text{tr}(AB) = \text{tr}(BA)$ über \mathbb{Z} , also $m = n$.

Die Determinante eines Endomorphismus

Über jedem kommutativen Ring K haben wir die Determinante (L2G)

$$\det = \det_K^n : (K^{n \times n}, \cdot, 1_{n \times n}) \rightarrow (K, \cdot, 1) : A \mapsto \det(A).$$

Allgemeiner sei V ein linearer Raum mit einer endlichen Basis über K .
Wie definieren wir die Determinante für lineare Abbildungen $f : V \rightarrow V$?

$$\det_V : (\text{End}_K(V), \circ, \text{id}_V) \rightarrow (K, \cdot, 1) : f \mapsto \det_V(f)$$

Wir wählen willkürlich irgendeine Basis \mathcal{B} von V (J2B):

$$\begin{array}{ccc} K^n & \xrightarrow{x \mapsto Ax} & K^n \\ & \downarrow f_A & \\ \Phi_{\mathcal{B}} \downarrow \cong & \updownarrow & \Phi_{\mathcal{B}} \downarrow \cong \\ V & \xrightarrow{f} & V \end{array}$$

Aufgabe: Können wir $\det_V(f) := \det_K^n(A)$ so wohl definieren?
Ist das Ergebnis unabhängig von der willkürlich gewählten Basis \mathcal{B} ?

Die Determinante eines Endomorphismus

Lösung: Wir vergleichen zwei Basen \mathcal{B} und \mathcal{C} des Raums V über K :
Dank Invarianz der Dimension L3C haben beide dieselbe Länge n .

$$\begin{array}{ccccc} K^n & \xrightarrow{A = M_{\mathcal{B}}^{\mathcal{B}}(f)} & K^n & & \\ & \searrow \Phi_{\mathcal{B}} \cong & & \swarrow \Phi_{\mathcal{B}} \cong & \\ & & V & \xrightarrow{f} & V \\ & \swarrow \Phi_{\mathcal{C}} \cong & & \searrow \Phi_{\mathcal{C}} \cong & \\ K^n & \xrightarrow{A' = M_{\mathcal{C}}^{\mathcal{C}}(f)} & K^n & & \\ & \uparrow T_{\mathcal{B}}^{\mathcal{C}} \cong & & \downarrow T_{\mathcal{C}}^{\mathcal{B}} \cong & \end{array}$$

In $K^{n \times n}$ haben wir $A' = T \cdot A \cdot T^{-1}$ mit $T = T_{\mathcal{B}}^{\mathcal{C}}$ und $T^{-1} = T_{\mathcal{C}}^{\mathcal{B}}$.
Dank Multiplikatивität L2N der Determinante gilt:

$$\det(A') = \det(T) \cdot \det(A) \cdot \det(T)^{-1} = \det(A)$$

Somit ist die Determinante $\det_V(f) := \det(A) = \det(A')$ wohldefiniert,
da unabhängig von den willkürlich gewählten Basen \mathcal{B} und \mathcal{C} .

Satz L3D: die Determinante eines Endomorphismus

(0) Sei K ein kommutativer Ring und V ein linearer Raum mit einer endlichen Basis über K . Mit der Wahl einer Basis \mathcal{B} definieren wir

$$\det_V : \text{End}_K(V) \rightarrow K : f \mapsto \det_V(f) := \det(M_{\mathcal{B}}^{\mathcal{B}}(f)).$$

Diese Abbildung \det_V ist wohldefiniert, das heißt basisunabhängig: Jede andere Wahl einer Basis führt zu demselben Ergebnis.

(1) Wir erhalten so den ersehnten Monoidhomomorphismus

$$\det_V : (\text{End}_K(V), \circ, \text{id}_V) \rightarrow (K, \cdot, 1) : f \mapsto \det_V(f).$$

Genau dann ist $f \in \text{End}_K(V)$ invertierbar, wenn $\det(f) \in K$ dies ist.

(2) Ist K ein Integritätsring, etwa ein Körper, so gilt:

$$\det(f) = 0 \iff \ker(f) \neq \{0\}$$

$$\det(f) \neq 0 \iff \ker(f) = \{0\}$$

Die Determinante eines Endomorphismus

Beweis: Die Wohldefiniertheit (0) haben wir in der vorigen Aufgabe nachgerechnet. Die weiteren Aussagen kennen wir bereits für die Determinante von Matrizen (L2T, L2Q) und übertragen diese nun auf Endomorphismen vermöge des Ringisomorphismus K1K:

$$(L_{\mathcal{B}}^{\mathcal{B}}, M_{\mathcal{B}}^{\mathcal{B}}) : (K^{n \times n}, +, \cdot) \cong (\text{End}_K(V), +, \circ)$$

😊 Wir setzen hier voraus, dass V frei und von endlicher Dimension ist. Über einem Körper K müssen wir die Existenz einer Basis nicht fordern, sie folgt aus dem Basisauswahlsatz J2B. In diesem Fall vereinfacht sich die Voraussetzung zu: K ist ein Körper und $\dim_K(V) < \infty$.

😊 Die Matrixdarstellung $A = M_{\mathcal{B}}^{\mathcal{B}}(f)$ ist ein Hilfskonstrukt zur Definition der Determinante auf V . Sie dient ebenso zur effizienten Berechnung, denn für die Matrix $A \in K^{n \times n}$ halten wir alle Werkzeuge bereit! Das Ergebnis jedoch ist von der Basiswahl unabhängig.

Anwendungsbeispiel zur Determinante

Beispiel: Wir betrachten die Ableitung ∂ auf dem \mathbb{C} -Vektorraum

$$\begin{aligned} V &= \langle \cos(2t), \sin(2t), \cos(3t), \sin(3t) \rangle_{\mathbb{C}} \\ &= \langle e^{2it}, e^{-2it}, e^{3it}, e^{-3it} \rangle_{\mathbb{C}} \leq \mathbb{C}^{\mathbb{R}}. \end{aligned}$$

Gemeint ist $f_1: \mathbb{R} \rightarrow \mathbb{C}: t \mapsto \cos(2t)$ usw. und $g_1: \mathbb{R} \rightarrow \mathbb{C}: t \mapsto e^{2it}$ usw.

Aufgabe: Berechnen Sie die Determinante $\det_V(\partial: V \rightarrow V)$.

Lösung: Wir wählen eine Basis von V , etwa \mathcal{A} oder \mathcal{B} wie oben, und stellen den Endomorphismus ∂ bezüglich dieser Basis als Matrix dar:

$$M_{\mathcal{A}}^{\mathcal{A}}(\partial) = \begin{bmatrix} 0 & 2 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & -3 & 0 \end{bmatrix} \quad \text{bzw.} \quad M_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 2i & 0 & 0 & 0 \\ 0 & -2i & 0 & 0 \\ 0 & 0 & 3i & 0 \\ 0 & 0 & 0 & -3i \end{bmatrix}$$

Damit finden wir $\det_V(\partial) = \det M_{\mathcal{A}}^{\mathcal{A}}(\partial) = \det M_{\mathcal{B}}^{\mathcal{B}}(\partial) = 36$.

😊 Jede Basiswahl führt zu demselben Ergebnis.

Anwendungsbeispiel zu Eigenräumen

Wir führen Beispiel K257 fort: Zu $v = \begin{bmatrix} -1 \\ 1 \end{bmatrix} \in \mathbb{R}^2$ betrachten wir

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}^2: x \mapsto x - v \cdot v^T \cdot x.$$

Aufgabe: (1) Finden Sie alle $\lambda \in \mathbb{R}$ mit nicht-trivialem **Eigenraum**

$$E(\lambda) := \{ x \in \mathbb{R}^2 \mid f(x) = \lambda x \} = \ker(f - \lambda \text{id}).$$

(2) Bestimmen Sie die Eigenräume. (3) Finden Sie eine Eigenbasis.

Lösung: (1) Zur Bestimmung von λ nutzen wir die **Determinante**:

$$\ker(f - \lambda \text{id}) \neq \{0\} \iff \det(f - \lambda \text{id}) = 0$$

Zur Berechnung wählen wir eine Basis, etwa $\mathcal{E} = (e_1, e_2)$, und finden

$$A = M_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \det(A - \lambda \cdot 1_{2 \times 2}) = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - 1.$$

Dies ist das **charakteristische Polynom** von A bzw. von f .

Seine Nullstellen sind in diesem Beispiel $\lambda = +1$ und $\lambda = -1$.

Dies sind die **Eigenwerte** der Matrix A bzw. der Abbildung f .

Anwendungsbeispiel zu Eigenräumen

Zur Erinnerung wiederhole ich die weitere Rechnung von Seite K257:

(2) Wir bestimmen die Eigenräume $E(+1)$ und $E(-1)$ wie folgt:

$$E(+1) = \ker(f - \text{id}) = \ker \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbb{R} b_1 \quad \text{mit} \quad b_1 := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$E(-1) = \ker(f + \text{id}) = \ker \begin{bmatrix} +1 & 1 \\ 1 & +1 \end{bmatrix} = \mathbb{R} b_2 \quad \text{mit} \quad b_2 := \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

Für alle weiteren $\lambda \in \mathbb{R} \setminus \{\pm 1\}$ gilt $E(\lambda) = \{0\}$ dank Satz L3D.

(3) Wir erhalten $\mathbb{R}^2 = E(+1) \oplus E(-1)$ und die Basis $\mathcal{B} = (b_1, b_2)$ von \mathbb{R}^2 . Nach Konstruktion gilt $f(b_1) = +1 \cdot b_1$ und $f(b_2) = -1 \cdot b_2$, und somit

$$M_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Auf Seite K237 haben wir bereits die Basiswechsellmatrizen bestimmt:

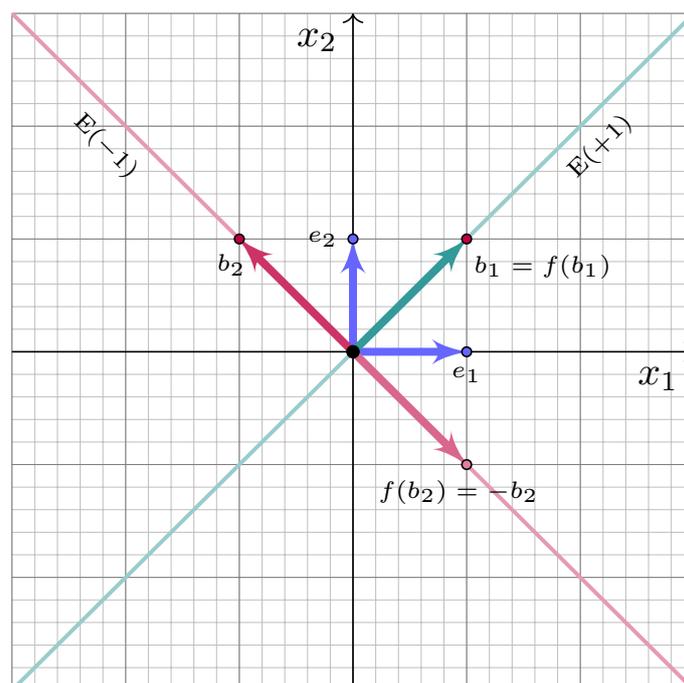
$$T_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \text{und} \quad T_{\mathcal{E}}^{\mathcal{B}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Anwendungsbeispiel zu Eigenräumen

😊 In der angepassten Basis $\mathcal{B} = (b_1, b_2)$ können wir die Abbildung f besonders einfach darstellen... Den Eigenräumen sei Dank!

$$M_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$M_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Die Abbildung $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ist die Spiegelung an der Hauptdiagonalen.

Die spezielle lineare Gruppe

Über jedem kommutativen Ring K haben wir die Determinante (L2G)

$$\det = \det_K^n : (K^{n \times n}, \cdot, 1_{n \times n}) \rightarrow (K, \cdot, 1) : A \mapsto \det(A).$$

Die invertierbaren Matrizen bilden die **allgemeine lineare Gruppe**

$$\mathrm{GL}_n(K) \stackrel{\text{L2T}}{=} \{ A \in K^{n \times n} \mid \det_K^n(A) \in K^\times \}$$

Ist V ein linearer Raum mit endlicher Basis über K , so haben wir:

$$\mathrm{GL}(V) \stackrel{\text{L3D}}{=} \{ f : V \rightarrow V \mid \det_V(f) \in K^\times \}$$

Definition L3E: die spezielle lineare Gruppe

Die Matrizen mit Determinante 1 bilden die **spezielle lineare Gruppe**

$$\mathrm{SL}_n(K) := \ker(\det_K^n) = \{ A \in K^{n \times n} \mid \det_K^n(A) = 1 \}.$$

Ebenso definieren wir die Gruppe der **speziellen Automorphismen**

$$\mathrm{SL}(V) := \ker(\det_V) = \{ f : V \rightarrow V \mid \det_V(f) = 1 \}.$$

Die spezielle lineare Gruppe

Die allgemeine lineare Gruppe $\mathrm{GL}(V)$ besteht aus den K -linearen Automorphismen $f : V \xrightarrow{\sim} V$, daher sind die folgenden Bezeichnungen ebenso üblich:

$$\mathrm{GL}(V) = \mathrm{Aut}_K(V)$$

$$\mathrm{SL}(V) = \mathrm{SAut}_K(V)$$

Beide Schreibweisen bedeuten dasselbe, jede hat ihre eigenen Vorteile. In der Nähe zu Matrizen schreibe ich hier lieber $\mathrm{GL}(V)$; in der Nähe zu Gruppen und ähnlichen Strukturen schreibe ich entsprechend $\mathrm{Aut}_K(V)$.

Die Determinante hat diese ganz besondere Eigenschaft (L2T):

Genau dann ist $A \in K^{n \times n}$ invertierbar, wenn $\det A \in K$ invertierbar ist

Daher können wir $\mathrm{GL}_n(K)$ durch die Determinante charakterisieren.

Über einem Körper K vereinfacht sich dies weiter zu $\det(A) \neq 0$.

Für die spezielle lineare Gruppe verlangen wir nun $\det(A) = 1$.

Somit ist $\mathrm{SL}_n(K)$ durch eine polynomielle Gleichung definiert.

Die spezielle lineare Gruppe

Beispiel: In Dimension $n = 1$ gilt $GL_1(K) = K^\times$ und $SL_1(K) = \{1\}$.

Beispiel: In Dimension $n = 2$ haben wir:

$$GL_2(K) \stackrel{\text{L2T}}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mid ad - bc \in K^\times \right\}$$

$$SL_2(K) \stackrel{\text{L3E}}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mid ad - bc = 1 \right\}$$

Bemerkung: Auf $GL_n(K)$ ist die Inversion $A^{-1} = \det(A)^{-1} \text{adj}(A)$ eine rationale Funktion (L2T), speziell auf $SL_n(K)$ sogar ein Polynom!

$$A \in SL_n(K) \implies A^{-1} = \text{adj}(A), \quad \begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix},$$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}^{-1} = \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}$$

Die spezielle lineare Gruppe

Die Determinante $\det: K^{n \times n} \rightarrow K$ ist ein explizites Polynom, dank der Leibniz-Formel L2G. Gleiches gilt für die Adjunktion $\text{adj}: K^{n \times n} \rightarrow K^{n \times n}$. Daraus erhalten wir die Inversion $A \mapsto A^{-1} = \det(A)^{-1} \text{adj}(A)$ als eine geschlossene Formel: eine explizit gegebene rationale Funktion (L2s).

Ich habe bereits die Besonderheit rationaler Funktionen betont: Über $K = \mathbb{R}, \mathbb{C}$ sind diese insbesondere stetig (\mathcal{C}^0), zudem differenzierbar (\mathcal{C}^1), glatt (\mathcal{C}^∞), sogar analytisch (\mathcal{C}^ω), ... Auch Sicht der Analysis haben sie alle guten Eigenschaften, die wir uns nur wünschen können.

Für Polynome gelten all diese schönen Eigenschaften weiterhin, zudem sind Polynome noch einfacher: Wir müssen nicht einmal dividieren.

Allgemeine und spezielle lineare Gruppe

Satz L3F: allgemeine und spezielle lineare Gruppe

(0) Die Determinante definiert eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow \mathrm{SL}_n(K) \xrightarrow{\mathrm{inc}} \mathrm{GL}_n(K) \xrightarrow[\iota]{\det_K^n} K^\times \longrightarrow 1$$

(1) Zu \det_K^n existiert ein rechtsinverser Gruppenhomomorphismus

$$\iota : K^\times = \mathrm{GL}_1(K) \hookrightarrow \mathrm{GL}_n(K) : s \mapsto \mathrm{diag}(s, 1, \dots, 1).$$

(2) Daraus folgt die Bijektion (jedoch i.A. kein Gruppenisomorphismus)

$$\varphi : \mathrm{SL}_n(K) \times K^\times \xrightarrow{\sim} \mathrm{GL}_n(K) : (A, s) \mapsto A \cdot \iota(s).$$

Ihre Umkehrabbildung ist $\psi(B) = (B \cdot \iota(\det(B)^{-1}), \det(B))$.

(3) Ist $K = \mathbb{F}_q$ ein endlicher Körper der Ordnung q , so gilt

$$\#\mathrm{GL}_n \mathbb{F}_q = \prod_{k=0}^{n-1} (q^n - q^k) \quad \text{und} \quad \#\mathrm{SL}_n \mathbb{F}_q = \frac{\#\mathrm{GL}_n \mathbb{F}_q}{q-1}.$$

Allgemeine und spezielle lineare Gruppe

😊 Dieser Satz L3F zur allgemeinen und speziellen linearen Gruppe entspricht Satz L1Q zur symmetrischen und alternierenden Gruppe.

Aufgabe: Weisen Sie die Aussagen dieses Satzes sorgfältig nach! Alle Daten liegen explizit vor, es genügt geduldiges Nachrechnen.

Lösung: (0) Die Determinante ist ein Monoidhomomorphismus (L2N) $\det_K^n : (K^{n \times n}, \cdot, 1_{n \times n}) \rightarrow (K, \cdot, 1)$. Durch Einschränkung erhalten wir den Gruppenhomomorphismus $\det_K^n : (\mathrm{GL}_n(K), \cdot, 1_{n \times n}) \rightarrow (K^\times, \cdot, 1)$.

(1) Die Abbildung $\iota : (K, \cdot, 1) \hookrightarrow (K^{n \times n}, \cdot, 1_{n \times n}) : s \mapsto \mathrm{diag}(s, 1, \dots, 1)$ ist ein Monoidhomomorphismus. Durch Einschränkung erhalten wir den Gruppenhomomorphismus $\iota : (K^\times, \cdot, 1) \rightarrow (\mathrm{GL}_n(K), \cdot, 1_{n \times n})$.

Dabei gilt $\det_K^n \circ \iota = \mathrm{id}$, denn $\det_K^n(\iota(s)) = s$ für alle $s \in K$ dank L2v. Insbesondere ist \det_K^n surjektiv und ι injektiv. (Letzteres war klar.) Der Kern von \det_K^n ist $\mathrm{SL}_n(K)$, also ist die Sequenz (0) exakt.

(2) Die Abbildungen φ und ψ sind explizit gegeben.

(2a) Nach Konstruktion gilt $\psi \circ \varphi = \text{id}$, denn wir haben

$$(A, s) \mapsto B = A \cdot \iota(s) \mapsto (B \cdot \iota(\det(B)^{-1}), \det(B)) = (A, s).$$

Hierzu nutzen wird die Multiplikativität L2N der Determinante:

$$\det(B) = \det(A \cdot \iota(s)) = \det(A) \cdot \det(\iota(s)) = 1 \cdot s = s$$

(2b) Ebenso gilt $\varphi \circ \psi = \text{id}$, denn wir haben

$$B \mapsto (B \cdot \iota(\det(B)^{-1}), \det(B)) \mapsto B \cdot \iota(\det(B)^{-1}) \cdot \iota(\det(B)) = B$$

Somit ist $(\varphi, \psi) : \text{SL}_n(K) \times K^\times \cong \text{GL}_n(K)$ ein Bijektionspaar.

 **Warnung:** Das Bijektionspaar (φ, ψ) ist i.A. kein Isomorphismus! Die koordinatenweise Multiplikation auf dem kartesischen Produkt $\text{SL}_n(K) \times K^\times$ entspricht nicht der Matrixmultiplikation in $\text{GL}_n(K)$. Diese grundlegende Beobachtung führen wir in (2c) kurz aus.

(2c) Ist die Gruppe K^\times nicht trivial, so existiert $s \in K^\times \setminus \{1\}$.

Wir betrachten dann das folgende Gegenbeispiel zur Multiplikativität:

$$S = \iota(s) = \begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad SA = \begin{bmatrix} 0 & -s \\ 1 & 0 \end{bmatrix}, \quad AS = \begin{bmatrix} 0 & -1 \\ s & 0 \end{bmatrix}.$$

Also sind $\varphi((1, s) \cdot (A, 1)) = AS$ und $\varphi(1, s) \cdot \varphi(A, 1) = SA$ verschieden!

 Die richtige Gruppenstruktur auf $\text{SL}_n(K) \times \iota(K^\times)$ ist hier also nicht das direkte Produkt, sondern ein sogenanntes semidirektes Produkt:

$$\text{GL}_n(K) = \text{SL}_n(K) \rtimes \iota(K^\times)$$

Mehr hierzu lernen Sie in der Algebra / Gruppentheorie.

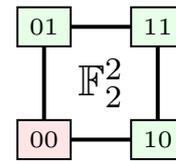
(3) Aus der Bijektion (2) folgt für die Gruppenordnungen:

$$\#\text{GL}_n(K) = \#\text{SL}_n(K) \cdot \#K^\times$$

Speziell für jeden endlichen Körper $K = \mathbb{F}_q$ wissen wir $\#K^\times = q - 1$ und kennen zudem die Gruppenordnung $\#\text{GL}_n(K)$ aus Satz J2H.

Beispiele zu linearen Gruppen

Aufgabe: (1) Wie viele Elemente haben die Gruppen $GL_2 \mathbb{F}_2$ und S_3 ?
 (2) Sind diese beiden Gruppen isomorph?



Lösung: (1) Wir finden $\# GL_2 \mathbb{F}_2 = 3 \cdot 2$ (J2H) und $\# S_3 = 3!$ (E2H).

(2) Wir nutzen die Abbildung $f : GL_n(K) \rightarrow \text{Sym}(K^n \setminus \{0\}) : A \mapsto f_A$. Sie ist ein Gruppenhomomorphismus (K1K) und zudem injektiv (K1E).

Speziell für $n = 2$ und $K = \mathbb{F}_2$ ist f bijektiv dank Elementezahl (E1H).

Somit ist $f : GL_2 \mathbb{F}_2 \xrightarrow{\sim} \text{Sym}(\mathbb{F}_2^2 \setminus \{0\})$ ein Gruppenisomorphismus.

Wir wählen eine Abzählung $(\nu, \mu) : \{1, 2, 3\} \cong \mathbb{F}_2^2 \setminus \{0\}$. Diese stiftet einen Gruppenisomorphismus $(\varphi, \psi) : S_3 \cong \text{Sym}(\mathbb{F}_2^2 \setminus \{0\})$ (L1N).

😊 Zusammengefasst erhalten wir das schöne Ergebnis:

Satz L3G: $GL_2 \mathbb{F}_2 \cong S_3$

Die Gruppen $GL_2 \mathbb{F}_2 = SL_2 \mathbb{F}_2$ und $\text{Sym}(\mathbb{F}_2^2 \setminus \{0\}) \cong S_3$ sind isomorph.

Beispiele zu linearen Gruppen

Jede Matrix $A \in K^{n \times n}$ definiert ihre zugehörige lineare Abbildung $f_A : K^n \rightarrow K^n : x \mapsto Ax$. Ist A zudem invertierbar, so ist f_A bijektiv, also eine Permutation der Menge K^n . Die Null wird dabei immer fest gehalten, wir können sie daher sofort aus der Menge K^n entfernen.

Genau diese Zuordnung $f : GL_n(K) \rightarrow \text{Sym}(K^n \setminus \{0\}) : A \mapsto f_A$ nutzen wir hier. Dieser der Konstruktion ist natürlich, ohne willkürliche Wahlen. Der letzte Teil $\text{Sym}(\mathbb{F}_2^2 \setminus \{0\}) \cong S_3$ gelingt auch leicht, doch hier müssen wir willkürliche Wahlen treffen, nämlich die Menge $\mathbb{F}_2^2 \setminus \{0\}$ abzählen.

😊 Der Satz ist in gewisser Weise ein „numerischer Zufall“ aus dem die genannte Isomorphie folgt: Die ganz kleinen Elementezahlen lassen einfach keinen Platz und erzwingen so die Isomorphie.

Bemerkung: Für den Körper $K = \mathbb{F}_2$ gilt $GL_n \mathbb{F}_2 = SL_n \mathbb{F}_2$.

Auch für den Polynomring $K = \mathbb{F}_2[X]$ über \mathbb{F}_2 gilt $K^\times = \{1\}$.

Somit haben wir auch hier die Gleichheit $GL_n(K) = SL_n(K)$.

Aufgabe: Wie viele Elemente hat der Matrixring $\mathbb{F}_3^{2 \times 2}$ sowie darin die allgemeine lineare Gruppe $GL_2 \mathbb{F}_3$ und die spezielle $SL_2 \mathbb{F}_3$?

Lösung: Dank unserer Vorbereitung L3F ist die Rechnung leicht:

$$\begin{aligned} \#\mathbb{F}_3^{2 \times 2} &= 3^4 &= 81 \\ \#GL_2 \mathbb{F}_3 &= (3^2 - 1)(3^2 - 3) = 8 \cdot 6 = 48 \\ \#SL_2 \mathbb{F}_3 &= \#GL_2 \mathbb{F}_3 / \#\mathbb{F}_3^\times = 48/2 = 24 \end{aligned}$$

😊 Zur Interpretation als Wahrscheinlichkeiten siehe J218.

Bemerkung: Die Gruppen $SL_2 \mathbb{F}_3$ und S_4 haben dieselbe Ordnung, sind aber nicht isomorph: Das Zentrum von $GL_2 \mathbb{F}_3$ ist $Z(SL_2 \mathbb{F}_3) = \{\pm E\}$. Die symmetrische Gruppe hat triviales Zentrum, $Z(S_4) = \{\text{id}\}$.

Für die Struktur der Gruppe ist ihre Elementzahl der erste Schritt, aber im Allgemeinen noch lange nicht ausreichend für Isomorphie. Die Quotientengruppe $PSL_2 \mathbb{F}_3 := SL_2 \mathbb{F}_3 / Z(SL_2 \mathbb{F}_3)$ ist isomorph zu A_4 .

Aufgabe: Wie viele Elemente hat der Matrixring $\mathbb{F}_5^{2 \times 2}$ sowie darin die allgemeine lineare Gruppe $GL_2 \mathbb{F}_5$ und die spezielle $SL_2 \mathbb{F}_5$?

Lösung: Dank unserer Vorbereitung L3F ist die Rechnung leicht:

$$\begin{aligned} \#\mathbb{F}_5^{2 \times 2} &= 5^4 &= 625 \\ \#GL_2 \mathbb{F}_5 &= (5^2 - 1)(5^2 - 5) = 24 \cdot 20 = 480 \\ \#SL_2 \mathbb{F}_5 &= \#GL_2 \mathbb{F}_5 / \#\mathbb{F}_5^\times = 480/4 = 120 \end{aligned}$$

😊 Zur Interpretation als Wahrscheinlichkeiten siehe J218.

Bemerkung: Das Zentrum $Z(SL_2 \mathbb{F}_5)$ besteht aus den beiden Matrizen $\pm E$. Die Quotientengruppe $PSL_2 \mathbb{F}_5 := SL_2 \mathbb{F}_5 / Z(SL_2 \mathbb{F}_5)$ hat demnach 60 Elemente. Die alternierende Gruppe A_5 hat ebenfalls 60 Elemente.

Hier kommt es zu einem weiteren erstaunlichen Zusammentreffen: Diese beiden Gruppen sind isomorph, es gilt also $PSL_2 \mathbb{F}_5 \cong A_5$. Mehr hierzu lernen Sie in der Algebra / Gruppentheorie.

Beispiel: Über dem Ring \mathbb{Z} der ganzen Zahlen haben wir

$$GL_2 \mathbb{Z} \stackrel{L2T}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathbb{Z}^{2 \times 2} \mid ad - bc = \pm 1 \right\},$$

$$SL_2 \mathbb{Z} \stackrel{L3E}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathbb{Z}^{2 \times 2} \mid ad - bc = +1 \right\}.$$

Hierin betrachten wir zwei Transvektionen und eine Skalierung:

$$X = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Satz L3H: Erzeuger für $SL_2 \mathbb{Z}$ und $GL_2 \mathbb{Z}$

Es gilt $SL_2 \mathbb{Z} = \langle X, Y \rangle$ und $GL_2 \mathbb{Z} = \langle X, Y, Z \rangle$.

Beweis: Die Gleichung $ad - bc = \pm 1$ bedeutet $\text{ggT}(a, b) = 1$ (A2i).

Mit den Zeilenoperationen $X^{\pm 1}$ und $Y^{\pm 1}$ führen wir den euklidischen Algorithmus auf der ersten Spalte aus, bis wir E oder Z erreichen. \square

Aufgabe: (0) Liegt die Matrix $M = \begin{bmatrix} 29 & -8 \\ 11 & -3 \end{bmatrix}$ in der Gruppe $SL_2 \mathbb{Z}$?

(1) Schreiben Sie M als ein Produkt über $X = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ und $Y = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

(2) Erfinden und lösen Sie selbst weitere Zahlenbeispiele dieser Art.

(3) Formulieren Sie Ihr Vorgehen als Algorithmus mit Induktionsbeweis.

Lösung: (0) Ja, denn $\det M = 29 \cdot (-3) - 11 \cdot (-8) = -87 + 88 = 1$.

(1) Wir nutzen X^{\pm} und Y^{\pm} als Zeilenoperationen (Operation von links) und wenden den euklidischen Algorithmus auf die erste Spalte an.

$$M = \begin{bmatrix} 29 & -8 \\ 11 & -3 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 18 & -5 \\ 11 & -3 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 7 & -2 \\ 11 & -3 \end{bmatrix} \xrightarrow{X^-} \begin{bmatrix} 7 & -2 \\ 4 & -1 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 3 & -1 \\ 4 & -1 \end{bmatrix}$$

$$\xrightarrow{X^-} \begin{bmatrix} 3 & -1 \\ 1 & 0 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \xrightarrow{X^-} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \xrightarrow{Y^+} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E$$

Zusammenfassend erhalten wir $E = YX^{-1}Y^{-2}X^{-1}Y^{-1}X^{-1}Y^{-2}M$,
und daraus die ersehnte Produktdarstellung $M = Y^2XYXY^2XY^{-1}$.

Wir konzentrieren uns hier (etwas willkürlich) auf die erste Spalte (a, b) und führen darauf den euklidischen Algorithmus A2H aus. Im Beispiel führe ich dies in Zeitlupe vor. Wenn wir gleich das k -Fache addieren möchten, so nutzen wir bequem die Potenzen X^k bzw. Y^k für $k \in \mathbb{Z}$.

Die zweite Spalte (c, d) erfüllt $ad - bc = 1$, dies sind also (bis auf die Vorzeichen) die zu (a, b) gehörigen Bézout-Koeffizienten, die wir mit denselben Operationen mitführen. Bitte schauen Sie sich hierzu nochmal Satz A2I und den Algorithmus von Euklid-Bézout an.

😊 Wir können mit Fug und Recht sagen: Die Arithmetik der Gruppe $SL_2 \mathbb{Z}$ entspricht dem guten alten euklidischen Algorithmus über \mathbb{Z} – in der besonders bequemen und effizienten Matrixschreibweise.

Aufgabe: (0) Ist die Matrix $M = \begin{bmatrix} 31 & -5 \\ 316 & -51 \end{bmatrix}$ über \mathbb{Z} invertierbar?

(1) Stellen Sie M dar als ein Produkt in den Erzeugern X, Y, Z .

Lösung: (0) Ja, es gilt $M \in GL_2 \mathbb{Z}$, denn

$$\det M = 31 \cdot (-51) - 316 \cdot (-5) = -1581 + 1580 = -1.$$

(1) Wir nutzen X^\pm und Y^\pm als Zeilenoperationen (Operation von links) und wenden den euklidischen Algorithmus auf die erste Spalte an.

$$M = \begin{bmatrix} 31 & -5 \\ 316 & -51 \end{bmatrix} \xrightarrow{X^{-10}} \begin{bmatrix} 31 & -5 \\ 6 & -1 \end{bmatrix} \xrightarrow{Y^{-5}} \begin{bmatrix} 1 & 0 \\ 6 & -1 \end{bmatrix} \xrightarrow{X^{-6}} \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = Z$$

Zusammenfassend erhalten wir $Z = X^{-6}Y^{-5}X^{-10}M$,
und daraus die ersehnte Produktdarstellung $M = X^{10}Y^5X^6Z$.

Diese Rechnung gelingt über jedem Ring K , kommutativ oder nicht. Ich habe deshalb hier umsichtig die übliche Konvention angewendet: Der Grundring operiert auf Zeilen von links und auf Spalten von rechts.

Wir dividieren hier einmal durch a , daher setzen wir $a \in K^\times$ voraus. Damit gelingen die Operationen über jedem Ring, wie hier gezeigt. Zusammenfassend erhalten wir so die gewünschte Umformung als Operation von Transvektionen (Zeilen von links, Spalten von rechts):

$$\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ (1-b)a^{-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ b-1 & 1 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}$$

Somit ist $\text{diag}(c, c^{-1}) \in SL_2(K)$ ein Produkt von vier Transvektionen:

$$\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -c^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c(1-c) & 1 \end{bmatrix}$$

Insbesondere sehen wir so, dass die spezielle lineare Gruppe $SL_n(K)$ über jedem Körper K bereits von den Transvektionen erzeugt wird.

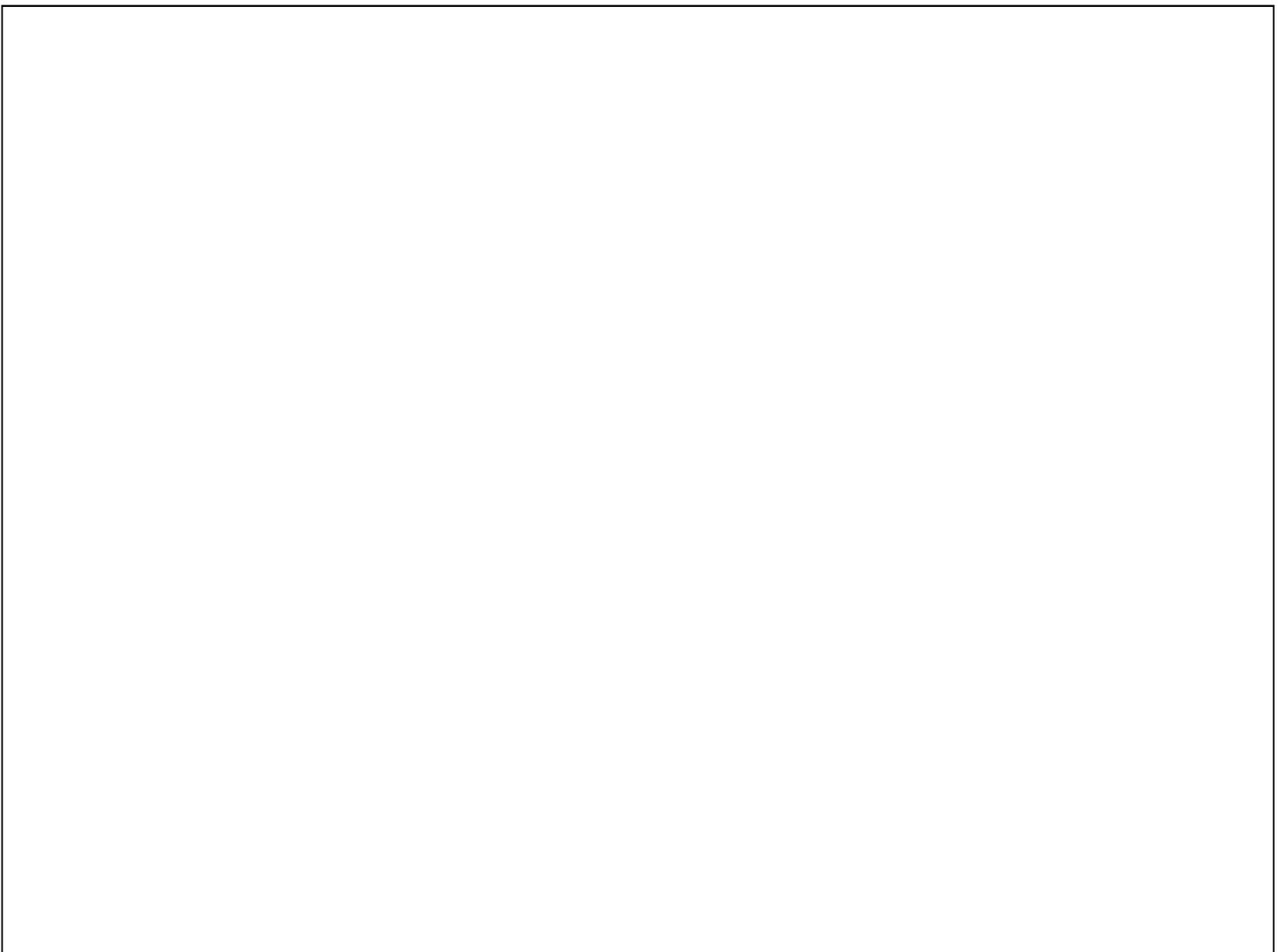
😊 Die Arithmetik und die Struktur der Gruppen $SL_n(K) \leq GL_n(K)$ entsprechen dem guten alten Gauß-Algorithmus – in der besonders bequemen und effizienten Matrixschreibweise wie in Satz L3I erklärt.

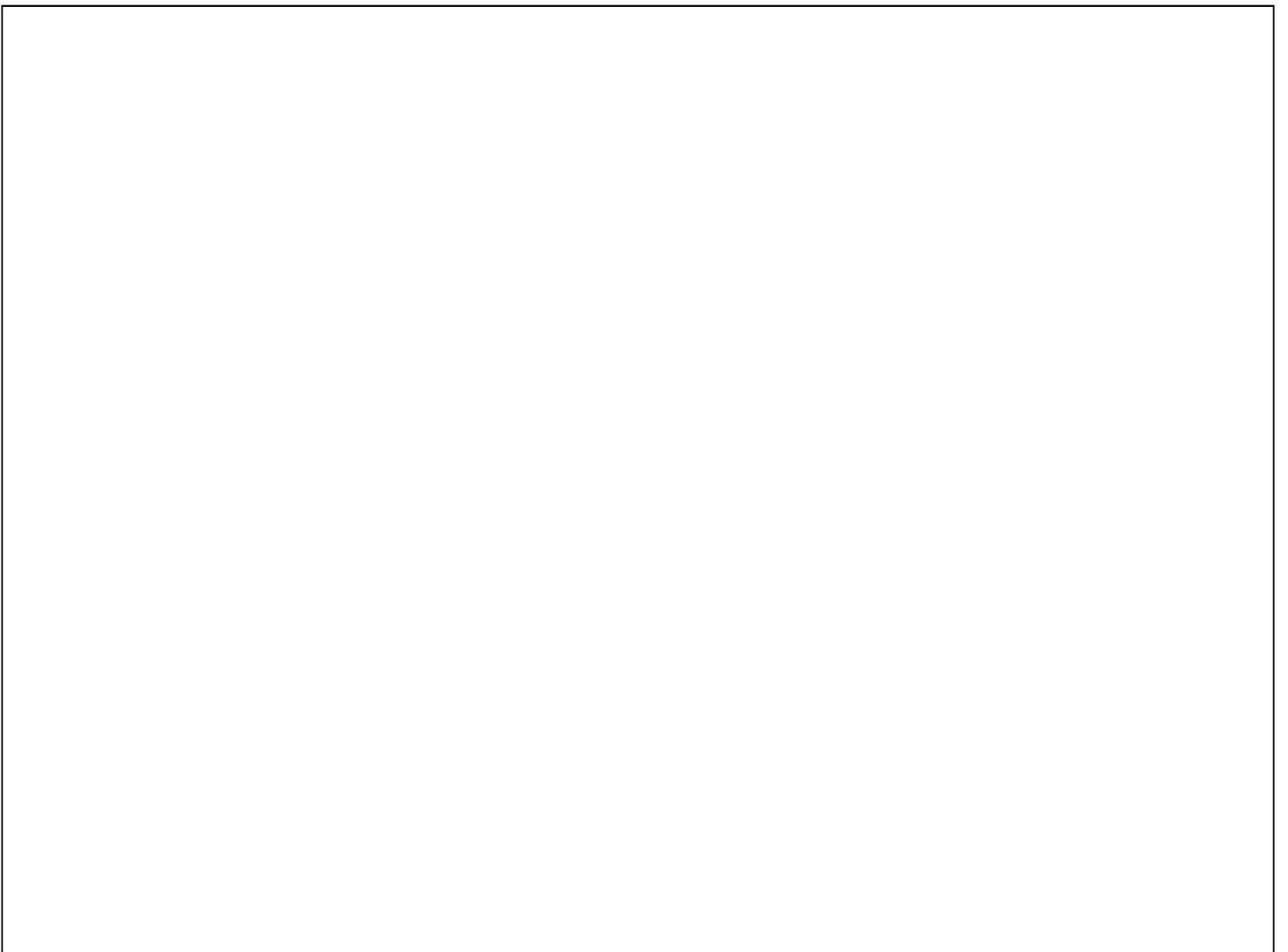
Aussagen (1) und (2) sowie ihr Beweis gelten wörtlich genauso über jedem Divisionsring. Zu Aussage (3) benötigen wir die Determinante, denn diese liegt schon der Definition der Gruppe $SL_n(K) = \ker(\det_K^n)$ zu Grunde. Die Determinante haben wir nur für kommutative Ringe!

Für einen Divisionsring R können wir nun umgekehrt vorgehen, und die spezielle lineare Gruppe über R *definieren* durch

$$SL_n(R) := \langle T_{ij}(\lambda) \mid i \neq j, \lambda \in R \rangle.$$

Diese Definition kommt demnach ganz ohne die Determinante aus. Im kommutativen Falle, also über jedem Körper, stimmt diese Setzung mit unserer vorigen Definition L3E überein. Wir können Satz L3I also auch so lesen: Beide Konstruktionen führen zu derselben Gruppe!

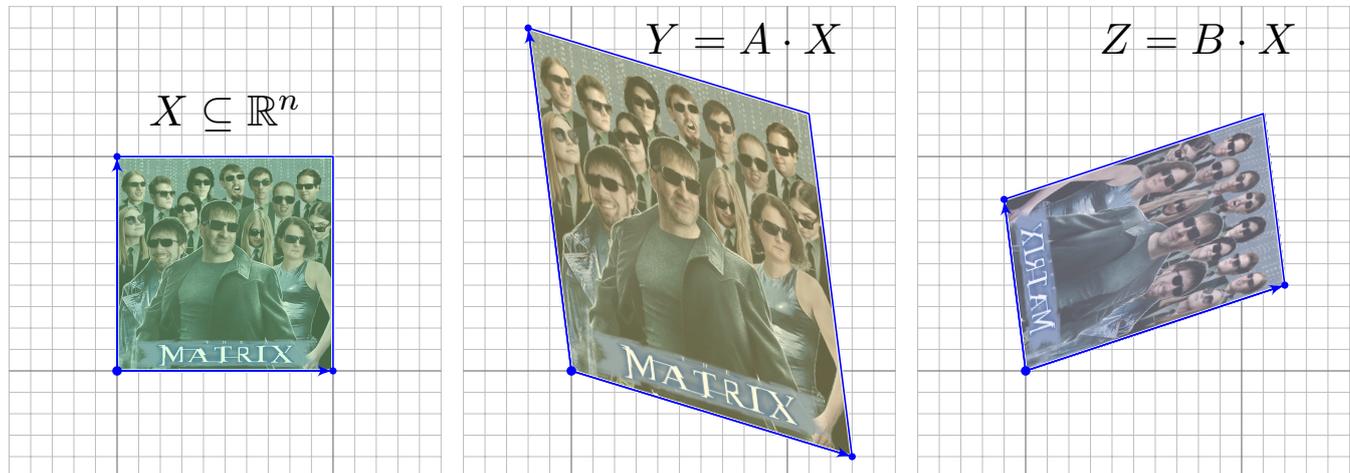




Aufgabe: Wie wirken die Matrizen

$$A = \begin{bmatrix} 1.3 & -0.2 \\ -0.4 & 1.6 \end{bmatrix} \quad \text{und} \quad B = \begin{bmatrix} -0.1 & 1.2 \\ 0.8 & 0.4 \end{bmatrix}$$

als Abbildungen $f_A, f_B : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ auf Flächeninhalt und Orientierung?



Lösung: Wir finden $\det(f_A) = \det(A) = +2$ und $\det(f_B) = \det(B) = -1$. Der Flächeninhalt wird von f_A verdoppelt, aber von f_B beibehalten. Die Orientierung wird von f_A beibehalten, aber von f_B umgekehrt.

Zum guten Abschluss dieses facettenreichen Kapitels kommen wir auf unsere ursprüngliche, geometrische Motivation zurück:

Die Determinante über \mathbb{R} misst Volumen und Orientierung.

Dies wollen wir nun illustrieren und erste Anwendungen erklären.

Die Verzerrung des geometrischen Volumens wird gemessen durch

$$\begin{aligned} v : (\mathbb{R}^{n \times n}, \cdot, 1_{n \times n}) &\xrightarrow{\det} \gg (\mathbb{R}, \cdot, 1) \xrightarrow{\text{abs}} \gg (\mathbb{R}_{\geq 0}, \cdot, 1) : A \mapsto |\det(A)|, \\ (\text{GL}_n \mathbb{R}, \cdot, 1_{n \times n}) &\xrightarrow{\det} \gg (\mathbb{R}^\times, \cdot, 1) \xrightarrow{\text{abs}} \gg (\mathbb{R}_{>0}, \cdot, 1). \end{aligned}$$

Der Kern des Gruppenhomomorphismus v ist

$$\text{SL}_n^\pm(\mathbb{R}) := \ker(v) = \{ A \in \mathbb{R}^{n \times n} \mid \det(A) = \pm 1 \}.$$

Das Orientierungsverhalten wird gemessen durch

$$\begin{aligned} \text{sign} : (\mathbb{R}^{n \times n}, \cdot, 1_{n \times n}) &\xrightarrow{\det} \gg (\mathbb{R}, \cdot, 1) \xrightarrow{\text{sign}} \gg (\{\pm 1, 0\}, \cdot, 1), \\ (\text{GL}_n \mathbb{R}, \cdot, 1_{n \times n}) &\xrightarrow{\det} \gg (\mathbb{R}^\times, \cdot, 1) \xrightarrow{\text{sign}} \gg (\{\pm 1\}, \cdot, 1). \end{aligned}$$

Dies zerlegt die Gruppe $\text{GL}_n(\mathbb{R})$ in zwei Klassen:

$$\begin{aligned} \text{GL}_n^+(\mathbb{R}) &:= \ker(\text{sign}) = \{ A \in \mathbb{R}^{n \times n} \mid \det(A) > 0 \}, \\ \text{GL}_n^-(\mathbb{R}) &:= \{ A \in \mathbb{R}^{n \times n} \mid \det(A) < 0 \}. \end{aligned}$$

Beispiele: Wir haben oben $A \in \text{GL}_n^+(\mathbb{R})$ und $B \in \text{GL}_n^-(\mathbb{R})$ gesehen. Zu $\text{GL}_n^+(\mathbb{R})$ gehören alle Drehungen (vorerst nur anschaulich). Zu $\text{GL}_n^-(\mathbb{R})$ gehören alle Spiegelungen (vorerst nur anschaulich).

Was ist eine Orientierung des Raumes \mathbb{R}^n ? Wie stellen wir fest, ob ein Automorphismus $f : \mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$ die Orientierung erhält oder umkehrt? Bemerkenswerterweise ist die zweite Frage leichter als die erste!

Ist V ein \mathbb{R} -linearer Raum endlicher Dimension, so setzen wir:

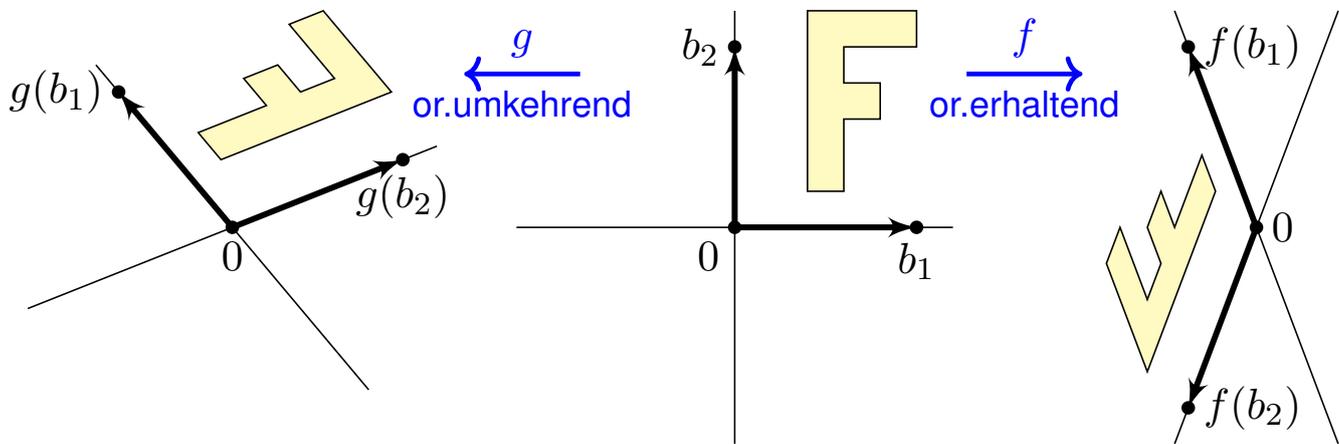
$$\begin{aligned} \text{GL}^+(V) &:= \{ f : V \rightarrow V \mid \det_V(f) > 0 \} \\ \text{GL}^-(V) &:= \{ f : V \rightarrow V \mid \det_V(f) < 0 \} \end{aligned}$$

Jeder Automorphismus $f \in \text{GL}^+(V)$ heißt **orientierungserhaltend**. Jeder Automorphismus $f \in \text{GL}^-(V)$ heißt **orientierungsumkehrend**.

Hierbei sind $\text{GL}_n^+(\mathbb{R}) \leq \text{GL}_n(\mathbb{R})$ und $\text{GL}^+(V) \leq \text{GL}(V)$ Untergruppen, nicht jedoch $\text{GL}_n^-(\mathbb{R})$ und $\text{GL}^-(V)$: Letztere sind nicht abgeschlossen unter Multiplikation, und sie enthalten auch nicht das Einselement.

Wie orientieren wir einen \mathbb{R} -Vektorraum?

Wir haben nun erklärt, wann eine \mathbb{R} -lineare Abbildung $f : V \rightarrow V$ „die Orientierung erhält“ oder aber „die Orientierung umkehrt“. Dabei haben wir noch nicht definiert, was eine Orientierung ist. Das ist kein Versehen, sondern die logisch richtige Reihenfolge!



Beispiel: Die reelle Gerade \mathbb{R} wird orientiert durch ihre Ordnung \leq . Wie orientieren wir die Ebene \mathbb{R}^2 ? oder den Raum \mathbb{R}^3 ? oder \mathbb{R}^n ? Allgemein einen \mathbb{R} -Vektorraum V endlicher Dimension?

Wie orientieren wir einen \mathbb{R} -Vektorraum?

Was eine **Orientierung** des Raums \mathbb{R}^n oder V allgemein sein soll, ist zunächst keineswegs offensichtlich. Es erfordert Scharfsinn!

Geometrische Sichtweise im \mathbb{R}^n : Zwei Basen $\mathcal{B} = (b_1, \dots, b_n)$ und $\mathcal{B}' = (b'_1, \dots, b'_n)$ des \mathbb{R}^n sind **orientierungsäquivalent**, wenn es einen Weg $\gamma : [0, 1] \rightarrow GL_n \mathbb{R}$ von \mathcal{B} nach \mathcal{B}' gibt: Die Spalten von $\gamma(t)$ sind zu jedem Zeitpunkt $t \in [0, 1]$ eine Basis des \mathbb{R}^n und deformieren \mathcal{B} in \mathcal{B}' .

Algebraische Sichtweise: In Satz L3L zeigen wir folgende Äquivalenz: Dies ist genau dann möglich, wenn die Basiswechselmatrix $A \in \mathbb{R}^{n \times n}$ von \mathcal{B} nach \mathcal{B}' eine **positive Determinante** hat, also $\det A > 0$ erfüllt. Diese algebraische Eigenschaft erheben wir nun zur Definition L3J.

Pragmatische Sichtweise: Wir benötigen ein Entscheidungsverfahren. Eine **Orientierung** sagt jeder Basis, ob sie positiv oder negativ ist, wobei orientierungsäquivalente Basen denselben Wert bekommen und orientierungsumgekehrte Basen entgegengesetzte Werte.

Definition L3J: Orientierungen eines \mathbb{R} -Vektorraums

Zwei Basen $\mathcal{B} = (b_1, \dots, b_n)$ und $\mathcal{B}' = (b'_1, \dots, b'_n)$ eines \mathbb{R} -Vektorraums V nennen wir **orientierungsäquivalent**, wenn die Basiswechselmatrix $A \in \mathbb{R}^{n \times n}$, definiert durch $b_j = \sum_{i=1}^n b'_i a_{ij}$, positive Determinante hat. Das ist eine Äquivalenzrelation: reflexiv, symmetrisch, transitiv. (Übung!)

Die Äquivalenzklasse $[\mathcal{B}]$ der Basis \mathcal{B} nennen wir eine **Orientierung** auf V , und das Paar $(V, [\mathcal{B}])$ einen **orientierten** \mathbb{R} -Vektorraum.

Es gibt genau zwei Orientierungen auf V : neben $[\mathcal{B}] = [b_1, b_2, \dots, b_n]$ die umgekehrte Orientierung $-[\mathcal{B}] = [-b_1, b_2, \dots, b_n] = [b_2, b_1, \dots, b_n]$.

Jeder \mathbb{R} -Isomorphismus $h: V \xrightarrow{\sim} V'$ transportiert die Orientierung $[\mathcal{B}] = [b_1, \dots, b_n]$ auf V zu $h_*([\mathcal{B}]) = [h(b_1), \dots, h(b_n)]$ auf V' .

Ein \mathbb{R} -linearer Isomorphismus $h: (V, [\mathcal{B}]) \xrightarrow{\sim} (V', [\mathcal{B}'])$ orientierter Vektorräume heißt **orientierungserhaltend**, falls $h_*([\mathcal{B}]) = [\mathcal{B}']$ gilt, und andernfalls **orientierungsumkehrend**, falls $h_*([\mathcal{B}]) = -[\mathcal{B}']$ gilt.

Orientierungen eines \mathbb{R} -Vektorraums

Beachten Sie das raffinierte Vorgehen, es ist logisch korrekt! Reflexivität, Symmetrie und Transitivität folgen aus der Definition K2L des Basiswechsels und der Multiplikativität L2N der Determinante.

Diese Definition teilt die Basen von V in genau zwei Klassen: Es gibt genau zwei Orientierungen, „die eine“ und „die andere“. Beide sind unterschieden, wie oben erklärt, aber gleichberechtigt.

Dimension $n = 0$ ist hierbei (technisch bedingt) eine Ausnahme.

Wenn Sie einen \mathbb{R} -Vektorraum V orientieren wollen, dann müssen Sie explizit angeben, welche der beiden Orientierungen Sie auswählen.

Dimension $n = 1$ ist klar. Der erste interessante Fall ist $n = 2$.

Ich nehme daher meist stillschweigend $n \geq 2$ an.

Ein \mathbb{R} -linearer Automorphismus $f: V \xrightarrow{\sim} V$ ist orientierungserhaltend, falls $f([\mathcal{B}]) = [\mathcal{B}]$ gilt, und orientierungsumkehrend, falls $f([\mathcal{B}]) = -[\mathcal{B}]$.

😊 Dies ist unabhängig von der Basiswahl und gleichbedeutend damit, dass die darstellende Matrix $A \in \mathbb{R}^{n \times n}$ positive / negative Determinante hat. Wir erhalten also die eingangs formulierte Vorzeichenregel.

Besonders einfach und vertraut ist der Koordinatenraum \mathbb{R}^n :

Beispiel: Der Koordinatenraum \mathbb{R}^n kommt mit seiner **Standardbasis**

$$\mathcal{E} = (e_1, \dots, e_n).$$

Diese definiert auf \mathbb{R}^n die **Standardorientierung**

$$[\mathcal{E}] = [e_1, \dots, e_n].$$

Jede Basis $\mathcal{B} = (b_1, \dots, b_n)$ des \mathbb{R}^n ist gleich oder entgegengesetzt zu \mathcal{E} orientiert, also „rechtshändig“ $[\mathcal{B}] = [\mathcal{E}]$ oder „linkshändig“ $[\mathcal{B}] = -[\mathcal{E}]$.

Für $n = 1$ ist $[e_1]$ die übliche, positive Orientierung von (\mathbb{R}, \leq) , entgegengesetzt ist die negative Orientierung $-[e_1] = [-e_1]$.

Die Standardorientierung $[e_1, e_2]$ auf \mathbb{R}^2 und $[e_1, e_2, e_3]$ auf \mathbb{R}^3 stellen wir anschaulich durch eine Rechte-Hand-Regel dar.

Anschaulich: Die Basis \mathcal{B} lässt sich stetig in \mathcal{E} überführen oder nicht.
Genauer: $GL_n \mathbb{R}$ hat zwei Wegkomponenten, $GL_n^+ \mathbb{R}$ und $GL_n^- \mathbb{R}$.

Ich betone nachdrücklich, dass „rechtshändig“ und „linkshändig“ keine absoluten Begriffe sind, sondern immer nur relativ zu einer gewählten Referenzbasis; hier ist dies die Standardbasis \mathcal{E} des Raums \mathbb{R}^n , oder allgemein eine ausgezeichnete Basis \mathcal{B} von V über \mathbb{R} .

Jeder Mensch, der schon einmal über seine Hände nachgedacht hat, wird feststellen: Beide sind eigentlich gleich, und doch auf subtile Weise verschieden. Sie sehen nun den mathematischen Grund: Der Übergang von „links“ nach „rechts“ führt über eine negative Basiswechselmatrix.

Zunächst sind beide Hände gleich gut geeignet. Wir wählen (willkürlich) eine davon als Referenz, die andere ist dann dazu entgegengesetzt. Die Natur hat uns einen Repräsentanten jeder Klasse mitgegeben! Daher sind unsere Hände sehr hilfreich für unsere Anschauung.

Als allgemeine, mathematische Erklärung taugt unsere vage Anschauung jedoch nicht; dafür haben wir die Definition L3J.

Beispiel: Wie orientieren Sie folgenden Untervektorraum $U \leq \mathbb{R}^4$?

$$U = \{ x \in \mathbb{R}^4 \mid x_1 + x_2 + x_3 + x_4 = 0 \}$$

Wie immer gibt es zwei Orientierungen, keine ist schöner als die andere. Es gilt $\dim_{\mathbb{R}}(U) = 3$, also $U \cong \mathbb{R}^3$, doch die Wahl eines Isomorphismus ist nicht eindeutig oder kanonisch. Wir müssen willkürlich eine Basis $\mathcal{B} = (b_1, b_2, b_3)$ wählen, um eine Orientierung $[\mathcal{B}]$ auf U zu vereinbaren.

Beispiel: Wie orientieren Sie folgenden Untervektorraum $V \leq \mathbb{R}^{\mathbb{R}}$?

$$V = \langle 1, \cos, \sin \rangle_{\mathbb{R}}^!$$

Die beiden möglichen Orientierungen sind

$$[1, \cos, \sin] = [\cos, \sin, 1] = \dots \quad \text{und} \quad [1, \sin, \cos] = [\cos, 1, \sin] = \dots$$

Beide Orientierungen sind verschieden, doch a priori gleichberechtigt. Kurzum: Die Orientierung $[\mathcal{B}]$ auf V ist eine zusätzliche Struktur!

Für den Koordinatenraum \mathbb{R}^n scheint alles leicht und übersichtlich. Doch es gibt viele weitere \mathbb{R} -Vektorräume, nicht nur den \mathbb{R}^n .

Ich wähle bewusst knifflige Beispiele $U \leq \mathbb{R}^4$ und $V \leq \mathbb{R}^{\mathbb{R}}$, um vom \mathbb{R}^n wegzukommen, denn da drängt sich die Standardbasis allzu sehr auf. Für U und V haben wir keine „kanonische“ Basis oder Orientierung.

Wenn Sie einen \mathbb{R} -Vektorraum V orientieren wollen, dann müssen Sie explizit angeben, welche der beiden Orientierungen Sie auswählen. Die Orientierung $[\mathcal{B}]$ auf V ist nicht etwa „naturegegeben“, sondern eine zusätzliche Struktur, ein weiteres Datum, eine ergänzende Information.

Aufgabe: Ist die Ableitung $\partial : V \rightarrow V$ auf $V = \langle \cos, \sin \rangle_{\mathbb{R}}$ orientierungserhaltend oder orientierungsumkehrend?

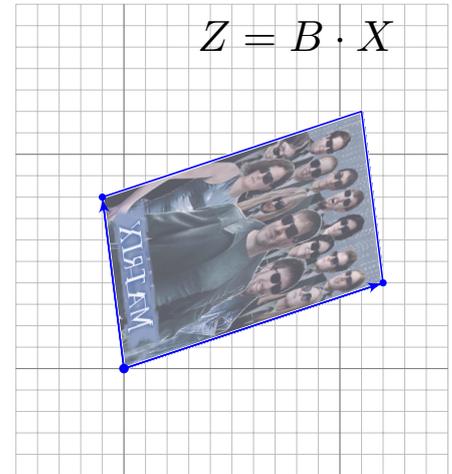
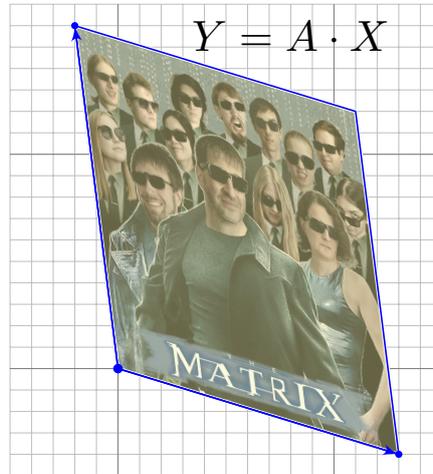
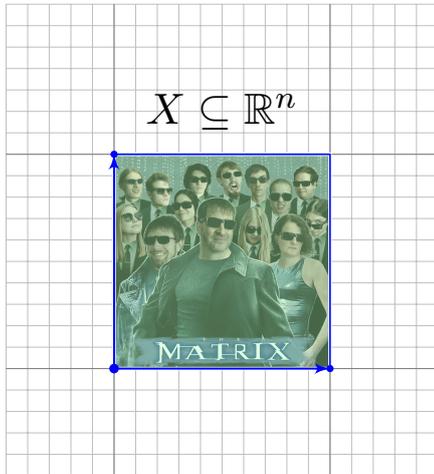
Lösung: Wir berechnen die Determinante $\det(\partial) \in \mathbb{R}$.
Hierzu wählen wir eine Basis von V , etwa $\mathcal{B} = (\cos, \sin)$.

$$A = M_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \implies \det_V(\partial) = \det_{\mathbb{R}}^2(A) = +1$$

Das bedeutet, $\partial : V \rightarrow V$ ist ein Automorphismus, zudem orientierungserhaltend und volumentreu, kurz $\partial \in \text{SL}(V)$.

😊 Diese Eigenschaften sind unabhängig von der Wahl der Basis! (L3D)

Die Determinante ist geometrisch motiviert als orientiertes Volumen. Dies hat uns direkt zur algebraischen Definition geführt: multilinear, alternierend, normiert. Daraus haben wir eine Fülle phantastischer Eigenschaften abgeleitet. Schließlich kehren wir zur Geometrie zurück.



Sie verfügen nun über die nötigen mathematischen Werkzeuge, sowohl die theoretischen Grundlagen als auch praktische Verfahren. Auf unserem Weg der präzisen Ausarbeitung hat sich wunderschöne Mathematik entfaltet, die Sie fortan gewinnbringend anwenden können.

Satz L3K: die Gruppe $GL_n^+(\mathbb{R})$

(0) Die Determinante definiert eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow SL_n(\mathbb{R}) \xrightarrow{\text{inc}} GL_n^+(\mathbb{R}) \xrightarrow[\iota]{\det} \mathbb{R}_{>0} \longrightarrow 1$$

Zudem haben wir $\iota: \mathbb{R}_{>0} \hookrightarrow GL_n^+(\mathbb{R}) : \mu \mapsto \text{diag}(\mu, 1, \dots, 1)$ wie in L3F.

(1) Die positive lineare Gruppe $GL_n^+(\mathbb{R})$ wird erzeugt von den Transvektionen und den positiven Skalierungen:

$$GL_n^+(\mathbb{R}) = \langle T_{ij}(\lambda), S_i(\mu) \mid i \neq j, \lambda \in \mathbb{R}, \mu \in \mathbb{R}_{>0} \rangle$$

(2) Genauer genügt eine einzige Skalierung, etwa $S_1(\mu)$ mit $\mu \in \mathbb{R}_{>0}$.

Beweis: (1) Analog zum Gauß-Algorithmus B2C können wir allein mit Zeilentransvektionen jede invertierbare Matrix $A \in GL_n(\mathbb{R})$ überführen in $\text{diag}(\mu_1, \mu_2, \dots, \mu_n)$ und dann (2) weiter zu $\text{diag}(\mu, 1, \dots, 1)$ (L3I). Falls wir mit $\det(A) > 0$ starten, so gilt $\mu = \det(A) > 0$ (L2W). **QED**

Ein **Weg** in $GL_n(\mathbb{R})$ ist eine stetige Abbildung $\gamma: [0, 1] \rightarrow GL_n(\mathbb{R})$ des reellen Intervalls $[0, 1]$ in den Zielraum $GL_n(\mathbb{R})$. Dabei heißt $A = \gamma(0)$ der Startpunkt und $B = \gamma(1)$ der Zielpunkt von γ . Wir sagen auch, der Weg γ verläuft von A nach B , oder γ verbindet A mit B .

Satz L3L: Die Gruppe $GL_n^+(\mathbb{R})$ ist wegzusammenhängend.

(1) Die positive lineare Gruppe $GL_n^+(\mathbb{R})$ ist wegzusammenhängend:

Je zwei Matrizen $A, B \in GL_n^+(\mathbb{R})$ lassen sich verbinden durch einen Weg $\gamma: [0, 1] \rightarrow GL_n^+(\mathbb{R})$ von $\gamma(0) = A$ nach $\gamma(1) = B$.

(2) Die Gruppe $GL_n(\mathbb{R}) = GL_n^+(\mathbb{R}) \sqcup GL_n^-(\mathbb{R})$ hat zwei Komponenten:

Genau dann lassen sich $A, B \in GL_n(\mathbb{R})$ verbinden durch einen Weg $\gamma: [a, b] \rightarrow GL_n(\mathbb{R})$, wenn beide dasselbe Vorzeichen haben.

Beispiel: Für $n = 1$ und $\mathbb{R}^\times = \mathbb{R}_{>0} \sqcup \mathbb{R}_{<0}$ ist dies sofort plausibel. Die Anschauung trügt hier nicht! Der Zwischenwertsatz garantiert: Jede stetige Funktion $f: [a, b] \rightarrow \mathbb{R}$ nimmt jeden Wert s zwischen $f(a)$ und $f(b)$ an, das heißt, es existiert $t \in [a, b]$ mit $f(t) = s$.

Beweis: (1a) Zu jedem Erzeuger $T_{ij}(\lambda)$ und $S_i(\mu)$ in $GL_n^+(\mathbb{R})$ haben wir

$$\tau : [0, 1] \rightarrow GL_n^+(\mathbb{R}) : t \mapsto T_{ij}(t\lambda),$$

$$\sigma : [0, 1] \rightarrow GL_n^+(\mathbb{R}) : t \mapsto S_i(1 + t(\mu - 1)).$$

Der Weg τ verbindet die Einheitsmatrix $\tau(0) = E$ mit $\tau(1) = T_{ij}(\lambda)$.

Der Weg σ verbindet die Einheitsmatrix $\sigma(0) = E$ mit $\sigma(1) = S_i(\mu)$.

(1b) Dank Satz L3K können wir jede Matrix $A \in GL_n^+(\mathbb{R})$ darstellen als ein Produkt $A = A_1 A_2 \cdots A_\ell$ der Erzeuger $A_k \in \{ T_{ij}(\lambda), S_i(\mu) \}$.

Zu jedem Index $k = 1, 2, \dots, \ell$ haben wir wie in (1a) erklärt einen Weg $\alpha_k : [0, 1] \rightarrow GL_n^+(\mathbb{R})$ von $\alpha_k(0) = E$ nach $\alpha_k(1) = A_k$. Wir erhalten:

$$\alpha : [0, 1] \rightarrow GL_n^+(\mathbb{R}) : \alpha(t) = \alpha_1(t)\alpha_2(t) \cdots \alpha_\ell(t)$$

Diese Abbildung ist stetig, somit ein Weg von $\alpha(0) = E$ nach $\alpha(1) = A$.

😊 Erfreulicher Nebeneffekt unserer Sorgfalt: Der so konstruierte Weg α ist eine Polynomfunktion vom Grad $\leq \ell$ in jedem Matrixeintrag.

(1c) Zu $A, B \in GL_n^+(\mathbb{R})$ existieren dank (1b) Wege $\alpha, \beta : [0, 1] \rightarrow GL_n^+(\mathbb{R})$ von der Einheitsmatrix $\alpha(0) = \beta(0) = E$ nach $\alpha(1) = A$ bzw. $\beta(1) = B$.

Daraus erhalten wir den Weg $\gamma : [0, 1] \rightarrow GL_n^+(\mathbb{R}) : \gamma(t) = \alpha(1-t)\beta(t)$ von $\gamma(0) = A$ nach $\gamma(1) = B$. Damit ist Aussage (1) bewiesen.

😊 Auch der Weg γ ist eine Polynomfunktion in jedem Matrixeintrag.

(2a) Für $A, B \in GL_n^+(\mathbb{R})$ haben wir in (1) einen Weg konstruiert.

(2b) Für $A, B \in GL_n^-(\mathbb{R})$ verbinden wir $S_1(-1)A$ und $S_1(-1)B$ durch γ in $GL_n^+(\mathbb{R})$, somit verläuft der Weg $S_1(-1)\gamma$ in $GL_n^-(\mathbb{R})$ von A nach B .

(2c) Für Matrizen $A, B \in GL_n(\mathbb{R})$ mit entgegengesetzten Vorzeichen $\text{sign } A \neq \text{sign } B$ existiert kein Weg $\gamma : [0, 1] \rightarrow GL_n(\mathbb{R})$ von A nach B .

Angenommen, $\gamma : [0, 1] \rightarrow GL_n(\mathbb{R}) \subset \mathbb{R}^{n \times n}$ verläuft von A nach B .

Da γ und $\det : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}$ stetig sind, gilt dies auch für die Komposition $f = \det \circ \gamma : [0, 1] \rightarrow \mathbb{R}$ mit $f(t) = \det(\gamma(t))$. Dank Zwischenwertsatz existiert $t_0 \in [0, 1]$ mit $f(t_0) = 0$. Somit ist die Matrix $\gamma(t_0) \in \mathbb{R}^{n \times n}$ nicht invertierbar, ein Widerspruch. □

Die Gruppe $GL_1(\mathbb{R}) = \mathbb{R} \setminus \{0\} = \mathbb{R}_{>0} \sqcup \mathbb{R}_{<0}$ hat zwei Komponenten. Hierin lassen sich die Punkte ± 1 nicht durch einen Weg verbinden. Hingegen ist die Gruppe $GL_1(\mathbb{C}) = \mathbb{C} \setminus \{0\}$ wegzusammenhängend: In der gelochten Ebene $\mathbb{C} \setminus \{0\}$ können wir je zwei Punkte verbinden.

Lemma L3M: Die Gruppe \mathbb{C}^\times ist wegzusammenhängend.

Seien $z_0, z_1 \in \mathbb{C}^\times$. In Polarkoordinaten haben wir $z_k = e^{w_k}$ mit $w_k \in \mathbb{C}$. Der Weg $\gamma: [0, 1] \rightarrow \mathbb{C}^\times: t \mapsto e^{(1-t)w_0 + tw_1}$ läuft von z_0 nach z_1 .

Diese Eigenschaft hat Konsequenzen in jeder höheren Dimension:

Satz L3N: Die Gruppe $GL_n(\mathbb{C})$ ist wegzusammenhängend.

Die allgemeine lineare Gruppe $GL_n(\mathbb{C})$ ist wegzusammenhängend: Je zwei invertierbare Matrizen $A, B \in GL_n(\mathbb{C})$ lassen sich verbinden durch einen Weg $\gamma: [0, 1] \rightarrow GL_n(\mathbb{C})$ von $\gamma(0) = A$ nach $\gamma(1) = B$.

Aufgabe: Beweisen Sie diesen Satz nach dem Vorbild von $GL_n^+(\mathbb{R})$.

Lösung: Wir nutzen Satz L3I im Spezialfall des Körpers $K = \mathbb{C}$:

$$GL_n(\mathbb{C}) = \langle T_{ij}(\lambda), S_i(\mu) \mid i \neq j, \lambda \in \mathbb{C}, \mu \in \mathbb{C}^\times \rangle$$

(a) Zu jedem Erzeuger $T_{ij}(\lambda)$ und $S_i(\mu)$ haben wir $\mu = e^w$ und somit

$$\begin{aligned} \tau &: [0, 1] \rightarrow GL_n(\mathbb{C}) : t \mapsto T_{ij}(t\lambda), \\ \sigma &: [0, 1] \rightarrow GL_n(\mathbb{C}) : t \mapsto S_i(e^{tw}). \end{aligned}$$

Der Weg τ verbindet die Einheitsmatrix $\tau(0) = E$ mit $\tau(1) = T_{ij}(\lambda)$.

Der Weg σ verbindet die Einheitsmatrix $\sigma(0) = E$ mit $\sigma(1) = S_i(\mu)$.

Ab hier verläuft der Beweis wörtlich wie (1b) und (1c) zu Satz L3L.

Bemerkung: Die Zweiteilung $\mathbb{R}^\times = \mathbb{R}_{>0} \sqcup \mathbb{R}_{<0}$ ist eine Besonderheit des Körpers \mathbb{R} . Sie beruht auf der vollständigen Ordnung von \mathbb{R} und der so definierten Orientierung auf \mathbb{R} : Diese erklärt hier „links“ und „rechts“.

Daraus gewinnen wir die Zweiteilung $GL_n(\mathbb{R}) = GL_n^+(\mathbb{R}) \sqcup GL_n^-(\mathbb{R})$ und schließlich die beiden Orientierungen des Raumes \mathbb{R}^n .

Satz L30: Jede komplexe Nichtnullstellenmenge ist wegzshgd.

Sei $P \in \mathbb{C}[Z_1, \dots, Z_n]$ ein Polynom, $P \neq 0$, und $f: \mathbb{C}^n \rightarrow \mathbb{C}: z \mapsto P(z)$ die zugehörige Polynomfunktion. Dann ist die Nichtnullstellenmenge $X := f^{-1}(\mathbb{C}^\times) = \{z \in \mathbb{C}^n \mid P(z) \neq 0\}$ wegzusammenhängend.

Beweis: (1) Für $n = 1$ ist dies leicht: Zu jedem Polynom $P \in \mathbb{C}[Z] \setminus \{0\}$ ist die Nullstellenmenge $f^{-1}(\{0\}) = \{z \in \mathbb{C} \mid P(z) = 0\}$ endlich (G3K). Das Komplement $X = \{z \in \mathbb{C} \mid P(z) \neq 0\}$ ist wegzusammenhängend, denn je zwei Punkte in X lassen sich durch einen Weg in X verbinden.

(2) Zu $a \neq b$ in X sei $g: \mathbb{C} \rightarrow \mathbb{C}^n: z \mapsto a + z(b - a)$ die komplexe Gerade durch $g(0) = a$ und $g(1) = b$. Die Polynomfunktion $h = f \circ g: \mathbb{C} \rightarrow \mathbb{C}$ hat endlich viele Nullstellen. Darauf können wir nun (1) anwenden: Es existiert ein Weg $\gamma: [0, 1] \rightarrow \mathbb{C}$ von 0 nach 1 in $h^{-1}(\mathbb{C}^\times) \subset \mathbb{C}$.

Somit läuft der Weg $g \circ \gamma: [0, 1] \rightarrow \mathbb{C}^n$ von a nach b in $f^{-1}(\mathbb{C}^\times) \subset \mathbb{C}^n$, denn zu jedem Zeitpunkt $t \in [0, 1]$ gilt $f(g(\gamma(t))) = h(\gamma(t)) \neq 0$. **QED**

Warnung: Für reelle Polynome gilt Satz L30 nicht! Zum Beispiel ist die Menge $\mathbb{R} \setminus \{0\} = \{x \in \mathbb{R} \mid x \neq 0\}$ nicht wegzusammenhängend.

Auch $\mathbb{R}^2 \setminus \mathbb{R} = \{(x, y) \in \mathbb{R}^2 \mid y \neq 0\}$ ist nicht wegzusammenhängend, doch $\mathbb{R}^2 \setminus \{0\} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \neq 0\}$ ist wegzusammenhängend.

Hingegen ist das Komplement $\mathbb{R}^2 \setminus \mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1 \neq 0\}$ der Kreislinie $\mathbb{S}^1 \subset \mathbb{R}^2$ nicht wegzusammenhängend.

Aufgabe: Beweisen Sie mit dem vorigen Satz L30 erneut, dass die Gruppe $GL_n(\mathbb{C})$ wegzusammenhängend ist.

Lösung: Dank der Determinante L2G haben wir die Mengengleichheit

$$GL_n(\mathbb{C}) = \{A \in \mathbb{C}^{n \times n} \mid \det A \neq 0\}.$$

Die Determinante ist gegeben durch die explizite, polynomielle Formel

$$\det: \mathbb{C}^{n \times n} \rightarrow \mathbb{C}: A \mapsto \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Dank Satz L30 ist daher die Menge $GL_n(\mathbb{C})$ wegzusammenhängend.

Zusammenfassung zur Determinante $\det = \det_K^n : K^{n \times n} \rightarrow K$ über einem kommutativen Ring K , etwa Integritätsring oder Körper.

Geometrische Motivation über \mathbb{R} : orientiertes Volumen.

Algebraische Definition L2A: multilinear, alternierend, normiert.

Hauptsatz L2G: Existenz (L2L) und Eindeutigkeit (L2M).

Eigenschaften: antisymmetrisch (L2D), $\det(P_\sigma) = \text{sign}(\sigma)$ (L2E), invariant unter Transvektion (L2C) und unter Transposition (L2K), multiplikativ (L2N), Inversionsformel $A^{-1} = \det(A)^{-1} \text{adj}(A)$ (L2S). Genau dann ist A invertierbar, wenn $\det A$ invertierbar ist (L2T). Cramersche Regel (L2P), $\det A = 0$ gdw $\ker(A) \neq \{0\}$ (L2Q).

Berechnung: Leibniz-Formel (L2J) und Laplace-Entwicklung (L2Z) beide mit Aufwand $n \cdot n!$, Gauß-Algorithmus (L2X) mit Aufwand n^3 , dazu Determinante unter Spalten- und Zeilenoperationen (L2W), Regel für 2×2 -Matrizen (L2H) und für 3×3 -Matrizen (L2I), Dreiecksmatrizen und Block-Dreiecksmatrizen (L2V).

Erste Anwendungen: Über jedem kommutativen Ring K mit $0 \neq 1$ ist jede invertierbare Matrix quadratisch (L3A) und daher gilt auch hier die ersehnte Invarianz der Dimension (L3C).

Auf jedem K -linearen Raum V mit endlicher Basis \mathcal{B} haben wir die Determinante $\det_V : \text{End}_K(V) \rightarrow K : f \mapsto \det_V(f) = M_{\mathcal{B}}^{\mathcal{B}}(f)$ mit allen guten Eigenschaften der Matrixdeterminante (L3D).

Der Kern der Determinante $\det : \text{GL}_n(K) \twoheadrightarrow K^\times$ ist die spezielle lineare Gruppe $\text{SL}_n(K) = \ker(\det)$. Diese wird erzeugt von Transvektionen... über jedem Körper K (L3I) und auch über dem Ring \mathbb{Z} (L3H).

Die allgemeine lineare Gruppe $\text{GL}_n(\mathbb{R}) = \text{GL}_n^+(\mathbb{R}) \sqcup \text{GL}_n^-(\mathbb{R})$ über \mathbb{R} zerfällt in zwei Komponenten, positiv und negativ (L3L).

Diese Zweiteilung definiert zwei Orientierungen auf dem Raum \mathbb{R}^n und somit auf jedem endlich-dimensionalen \mathbb{R} -Vektorraum V (L3J).

Über dem Körper \mathbb{C} ist die allgemeine lineare Gruppe $\text{GL}_n(\mathbb{C})$ hingegen wegzusammenhängend (L3N); hier tritt diese Zweiteilung nicht auf.

Inversion quadratischer Matrizen

Wir betrachten quadratische Matrizen $A, B \in R^{n \times n}$ über einem Ring R und fragen: Folgt aus $AB = 1_{n \times n}$ bereits $BA = 1_{n \times n}$, also $B = A^{-1}$?

Aufgabe: (0) Finden Sie Gegenbeispiele! Beantworten Sie die Frage (1) für jeden Divisionsring R und (2) für jeden kommutativen Ring R .

Lösung: (0) Wir nutzen unser unvergessliches Gegenbeispiel J10: Hierzu sei K ein Körper. Im Endomorphismenring $R = \text{End}_K(K[X])$ haben wir die Elemente $a: P(X) \mapsto P(X^2)$ und $b: P(X) \mapsto XP(X^2)$ sowie $(c, d): P \mapsto (P_0, P_1)$ mit $P = P_0(X^2) + XP_1(X^2)$, also explizit

$$\begin{aligned} a(P) &= (p_0, 0, p_1, 0, p_2, 0, \dots), & c(P) &= (p_0, p_2, p_4, p_6, p_8, \dots), \\ b(P) &= (0, p_0, 0, p_1, 0, p_2, \dots), & d(P) &= (p_1, p_3, p_5, p_7, p_9, \dots). \end{aligned}$$

Bemerkenswerterweise gelten damit die Gleichungen

$$\begin{aligned} \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} ca & cb \\ da & db \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} &= \begin{pmatrix} ac + bd & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Inversion quadratischer Matrizen

😊 Es ist heilsam, mit Gegenbeispielen zu beginnen: Diese bewahren Sie vor dem naiven Irrglauben, die Aussage sei „klar“ oder „trivial“. Sie sehen daran eindrucklich, dass hier wirklich etwas zu zeigen ist. So motiviert lösen wir nun die beiden wichtigsten, positiven Fälle:

(1) Über jedem Divisionsring R hilft uns der Gauß-Algorithmus!

Für jede quadratische Matrix $A \in R^{n \times n}$ gilt nämlich dank Satz B2D: A ist rechtsinvertierbar $\Leftrightarrow A$ ist linksinvertierbar $\Leftrightarrow A$ ist invertierbar. Jede Rechtsinverse zu A ist eine Linksinverse zu A und umgekehrt.

(2) Über jedem kommutativen Ring R hilft uns die Determinante!

Aus $AB = 1_{n \times n}$ folgt $1 = \det(AB) = \det(A) \det(B)$, also ist $\det(A)$ in R invertierbar. Dank Satz L2s ist die Matrix A dann in $K^{n \times n}$ invertierbar durch $A^{-1} = \det(A)^{-1} \text{adj}(A)$. Aus $AB = 1_{n \times n}$ folgt also $B = A^{-1}$.

😊 Am Ende geht alles gut aus. Es bedarf jedoch eines Beweises! Genau das ist der Nutzen des mahnenden Gegenbeispiels J10.

