

# LINEARE ALGEBRA MIT GRUNDLAGEN

Wolfgang Soergel

25. April 2024

Diese Zusammenstellung ist ergänzt um einen Abschnitt mit Grundlagen. Alle in der farbigen Darstellung grünen Referenzen beziehen sich auf die [öffentliche Werkbank](#). Lädt man diese Datei in denselben Ordner, funktionieren bei modernen Programmen zur Darstellung von pdf-Dateien auch die Hyperlinks.

# Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>1 Einstimmung</b>   | <b>7</b>  |
| 1.1 Einstimmung . . . . .                                    | 8         |
| 1.1.1 Vollständige Induktion und binomische Formel . . . . . | 8         |
| 1.1.2 Fibonacci-Folge und Vektorraumbegriff . . . . .        | 16        |
| <b>2 Mengen und Verknüpfungen</b>                            | <b>27</b> |
| 2.1 Naive Mengenlehre und Kombinatorik . . . . .             | 29        |
| 2.1.1 Mengen . . . . .                                       | 29        |
| 2.1.2 Teilmengen . . . . .                                   | 32        |
| 2.1.3 Mengenoperationen . . . . .                            | 34        |
| 2.1.4 Abbildungen . . . . .                                  | 42        |
| 2.1.5 Verknüpfung von Abbildungen . . . . .                  | 45        |
| 2.1.6 Ergänzungen zur Mengenlehre* . . . . .                 | 50        |
| 2.1.7 Logische Symbole und Konventionen . . . . .            | 54        |
| 2.2 Algebraische Grundbegriffe . . . . .                     | 57        |
| 2.2.1 Mengen mit Verknüpfung . . . . .                       | 57        |
| 2.2.2 Gruppen . . . . .                                      | 65        |
| 2.2.3 Homomorphismen . . . . .                               | 70        |
| 2.2.4 Körper . . . . .                                       | 78        |
| 2.2.5 Aufbau des Zahlensystems* . . . . .                    | 83        |
| 2.2.6 Verbände und Boole'sche Algebren* . . . . .            | 84        |
| 2.3 Zur Darstellung von Mathematik* . . . . .                | 86        |
| 2.3.1 Herkunft einiger Symbole . . . . .                     | 86        |
| 2.3.2 Grundsätzliches zur Formulierung . . . . .             | 86        |
| 2.3.3 Sprache und Mathematik . . . . .                       | 88        |
| 2.3.4 Terminologisches zur leeren Menge* . . . . .           | 91        |
| 2.4 Philosophisches und Didaktisches . . . . .               | 93        |
| 2.4.1 Was ist Mathematik? . . . . .                          | 93        |
| 2.4.2 Didaktische Gedanken . . . . .                         | 96        |
| 2.5 Danksagung . . . . .                                     | 98        |

|  |           |
|--|-----------|
| <b>3 Lineare Algebra 1</b>   | <b>99</b> |
| 3.1 Gleichungssysteme und Vektorräume . . . . .                        | 101       |
| 3.1.1 Lösen linearer Gleichungssysteme . . . . .                       | 101       |
| 3.1.2 Vektorräume . . . . .  | 111       |
| 3.1.3 Endliche Produkte von Mengen . . . . .                           | 116       |
| 3.1.4 Ordnungen und Teilordnungen* . . . . .                           | 121       |
| 3.1.5 Untervektorräume . . . . .                                       | 123       |
| 3.1.6 Lineare Unabhängigkeit und Basen . . . . .                       | 127       |
| 3.1.7 Dimension eines Vektorraums . . . . .                            | 132       |
| 3.1.8 Austauschsatz von Steinitz* . . . . .                            | 137       |
| 3.1.9 Auswahlaxiom und Zorn'sches Lemma* . . . . .                     | 138       |
| 3.2 Lineare Abbildungen . . . . .                                      | 146       |
| 3.2.1 Homomorphismen und Isomorphismen . . . . .                       | 146       |
| 3.2.2 Dimensionsformel für lineare Abbildungen . . . . .               | 151       |
| 3.2.3 Räume von linearen Abbildungen . . . . .                         | 155       |
| 3.2.4 Lineare Abbildungen $K^n \rightarrow K^m$ und Matrizen . . . . . | 160       |
| 3.2.5 Eigenschaften von Matrizen . . . . .                             | 168       |
| 3.2.6 Lineare Abbildungen und Matrizen . . . . .                       | 174       |
| 3.2.7 Komplexe Zahlen . . . . .  | 179       |
| 3.2.8 Möbiusfunktion* . . . . .  | 187       |
| 3.2.9 Dualräume und transponierte Abbildungen . . . . .                | 188       |
| 3.2.10 Ergänzungen zu linearen Abbildungen* . . . . .                  | 198       |
| 3.3 Affine Räume . . . . .   | 199       |
| 3.3.1 Affine Räume und affine Abbildungen . . . . .                    | 199       |
| 3.3.2 Affine Teileräume . . . . .                                      | 204       |
| 3.3.3 Affine Räume und ihre Geraden . . . . .                          | 208       |
| 3.3.4 Baryzentrische Koordinaten* . . . . .                            | 213       |
| 3.3.5 Lineare und affine Ungleichungen* . . . . .                      | 216       |
| 3.3.6 Endlich erzeugte Kegel* . . . . .                                | 227       |
| 3.4 Zahlen . . . . .   | 234       |
| 3.4.1 Konstruktion der natürlichen Zahlen* . . . . .                   | 234       |
| 3.4.2 Äquivalenzrelationen und ganze Zahlen . . . . .                  | 243       |
| 3.4.3 Untergruppen der Gruppe der ganzen Zahlen . . . . .              | 246       |
| 3.4.4 Primfaktorzerlegung . . . . .                                    | 248       |
| 3.5 Ringe und Polynome . . . . .                                       | 255       |
| 3.5.1 Ringe . . . . .  | 255       |
| 3.5.2 Restklassenringe des Rings der ganzen Zahlen . . . . .           | 258       |
| 3.5.3 Polynome . . . . .   | 266       |
| 3.5.4 Polynome als Funktionen* . . . . .                               | 275       |
| 3.5.5 Quotientenkörper und Partialbruchzerlegung . . . . .             | 280       |
| 3.5.6 Quaternionen* . . . . .  | 287       |

|          |   |            |
|----------|---|------------|
| 3.6      | Determinanten und Eigenwerte . . . . .                    | 291        |
| 3.6.1    | Das Signum einer Permutation . . . . .                    | 291        |
| 3.6.2    | Determinante und ihre Bedeutung . . . . .                 | 295        |
| 3.6.3    | Charakterisierung der Determinante . . . . .              | 301        |
| 3.6.4    | Rechenregeln für Determinanten . . . . .                  | 305        |
| 3.6.5    | Orientierung . . . . .                                    | 310        |
| 3.6.6    | Eigenwerte und Eigenvektoren . . . . .                    | 316        |
| 3.7      | Danksagung . . . . .                                      | 326        |
| 3.8      | Die Vorlesung LA1 im Wintersemester 14/15 . . . . .       | 327        |
| <b>4</b> | <b>Lineare Algebra 2</b>                                  | <b>331</b> |
| 4.1      | Skalarprodukt und Geometrie . . . . .                     | 332        |
| 4.1.1    | Skalarprodukt und die Ebene von Euklid . . . . .          | 332        |
| 4.1.2    | Invariante Skalarprodukte zu Drehspiegelgruppen . . . . . | 339        |
| 4.1.3    | Geometrie von Skalarprodukträumen . . . . .               | 344        |
| 4.1.4    | Orthogonale und unitäre Abbildungen . . . . .             | 353        |
| 4.1.5    | Euklidische Räume . . . . .                               | 357        |
| 4.1.6    | Euklidischer Raum und Anschauung* . . . . .               | 361        |
| 4.1.7    | Zweistrahlen und Winkel . . . . .                         | 367        |
| 4.1.8    | Winkelmaße und Winkel im Dreieck . . . . .                | 372        |
| 4.1.9    | Kreuzprodukt und Spatprodukt . . . . .                    | 379        |
| 4.1.10   | Abstandserhaltende Abbildungen . . . . .                  | 381        |
| 4.1.11   | Normalformen und Matrixzerlegungen . . . . .              | 387        |
| 4.1.12   | Selbstadjungierte Endomorphismen . . . . .                | 394        |
| 4.2      | Allgemeine Bilinearformen . . . . .                       | 410        |
| 4.2.1    | Fundamentalmatrix . . . . .                               | 410        |
| 4.2.2    | Hauptachsentransformation . . . . .                       | 413        |
| 4.2.3    | Klassifikation symmetrischer Bilinearformen . . . . .     | 416        |
| 4.2.4    | Satz von Witt* . . . . .                                  | 428        |
| 4.2.5    | Alternierende Bilinearformen . . . . .                    | 429        |
| 4.2.6    | Relativistische Raumzeit* . . . . .                       | 431        |
| 4.2.7    | Relativistische Längeneinheiten* . . . . .                | 437        |
| 4.2.8    | Affine Struktur durch Lichtkegel* . . . . .               | 439        |
| 4.3      | Hauptraumzerlegung und Jordanzerlegung . . . . .          | 444        |
| 4.3.1    | Motivation durch Differentialgleichungen* . . . . .       | 444        |
| 4.3.2    | Hauptraumzerlegung . . . . .                              | 445        |
| 4.3.3    | Jordanzerlegung . . . . .                                 | 451        |
| 4.3.4    | Jordan'sche Normalform . . . . .                          | 455        |
| 4.4      | Quotienten . . . . .                                      | 464        |
| 4.4.1    | Nebenklassen . . . . .                                    | 464        |
| 4.4.2    | Normalteiler und Nebenklassengruppen . . . . .            | 467        |

|        |  |     |
|--------|--|-----|
| 4.4.3  | Zyklische Gruppen . . . . .                          | 472 |
| 4.4.4  | Endlich erzeugte abelsche Gruppen . . . . .          | 478 |
| 4.4.5  | Quotientenvektorräume . . . . .                      | 490 |
| 4.4.6  | Exakte Sequenzen . . . . .                           | 493 |
| 4.4.7  | Mehr zu exakten Sequenzen*                           | 496 |
| 4.5    | Symmetrie* . . . . .                                 | 500 |
| 4.5.1  | Gruppenwirkungen . . . . .                           | 500 |
| 4.5.2  | Bahnformel . . . . .                                 | 510 |
| 4.5.3  | Konjugationsklassen . . . . .                        | 512 |
| 4.5.4  | Endliche Untergruppen von Bewegungsgruppen . . . . . | 514 |
| 4.5.5  | Diskussion der Eulerformel* . . . . .                | 530 |
| 4.5.6  | Bruhatzerlegung* . . . . .                           | 532 |
| 4.6    | Multilineare Algebra . . . . .                       | 536 |
| 4.6.1  | Tensorprodukte . . . . .                             | 536 |
| 4.6.2  | Multiverknüpfung multilinearer Abbildungen*          | 548 |
| 4.6.3  | Bezug zur physikalischen Terminologie*               | 550 |
| 4.6.4  | Geometrie in euklidischen Vektorräumen . . . . .     | 553 |
| 4.6.5  | Alternierende Tensoren und äußere Potenzen . . . . . | 559 |
| 4.7    | Kategorien und Funktoren* . . . . .                  | 570 |
| 4.7.1  | Kategorien . . . . .                                 | 570 |
| 4.7.2  | Funktoren . . . . .                                  | 577 |
| 4.7.3  | Objekte mit Zusatzstrukturen*                        | 582 |
| 4.7.4  | Transformationen . . . . .                           | 585 |
| 4.7.5  | Natürliche Konstruktionen in der Geometrie . . . . . | 592 |
| 4.7.6  | Köcher*  | 594 |
| 4.7.7  | Produkte und Koprodukte in Kategorien . . . . .      | 598 |
| 4.7.8  | Produkte und Summen von Vektorräumen*                | 603 |
| 4.7.9  | Algebren*  | 606 |
| 4.7.10 | Yonedalemma*   | 609 |
| 4.7.11 | Universen*   | 613 |
| 4.8    | Danksagung . . . . .                                 | 615 |
| 4.9    | Die Vorlesung LA2 im Sommersemester 2015 . . . . .   | 616 |
| 4.10   | Die Vorlesung Elementargeometrie im SS 18 . . . . .  | 619 |
|        | Literaturverzeichnis . . . . .                       | 621 |
|        | Indexvorwort . . . . .                               | 623 |
|        | Index . . . . .                                      | 625 |

# **Kapitel 1**

## **Einstimmung**

## 1.1 Einstimmung

### 1.1.1 Vollständige Induktion und binomische Formel

**Satz 1.1.1.1.** Für jede natürliche Zahl  $n \geq 1$  gilt  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ .

*Beispiel 1.1.1.2.* Im Fall  $n = 5$  behauptet unser Satz  $1 + 2 + 3 + 4 + 5 = 5 \times 6/2$  und in diesem Fall stimmt das schon mal: Beide Seiten sind 15. Man bemerke, daß wir beim Rechnen mit Symbolen wie etwa  $n(n+1)$  die Multiplikationssymbole weggelassen haben, die nur beim Rechnen mit durch Ziffern dargestellten Zahlen wichtig sind.

*Beweis.* Bei diesem Beweis sollen Sie gleichzeitig das Beweisprinzip der **vollständigen Induktion** lernen. Wir bezeichnen mit  $A(n)$  die Aussage, daß die Formel im Satz für ein gegebenes  $n$  gilt, und zeigen:

**Induktionsbasis:** Die Aussage  $A(1)$  ist richtig. In der Tat gilt  $1 = \frac{1(1+1)}{2}$ .

**Induktionsschritt:** Aus der Aussage  $A(n)$  folgt die Aussage  $A(n+1)$ . In der Tat, unter der Annahme, daß unsere Formel für ein gegebenes  $n$  gilt, der sogenannten **Induktionsannahme** oder **Induktionsvoraussetzung**, rechnen wir

$$\begin{aligned} 1 + 2 + \dots + n + (n+1) &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

und folgern so, daß die Formel auch für  $n+1$  gilt.

Es ist damit klar, daß unsere Aussage  $A(n)$  richtig ist alias daß unsere Formel gilt für alle  $n = 1, 2, 3, \dots$  □

1.1.1.3. Das Zeichen □ deutet in diesem Text das Ende eines Beweises an und ist in der neueren Literatur weit verbreitet. Buchstaben in Formeln werden in der Mathematik üblicherweise kursiv notiert, so wie etwa das  $n$  oder auch das  $A$  im vorhergehenden Beweis. Nur Buchstaben oder Buchstabenkombinationen, die stets dasselbe bedeuten sollen, schreibt man nicht kursiv, wie etwa  $\sin$  für den Sinus oder  $\log$  für den Logarithmus.

1.1.1.4. Der vorhergehende Beweis stützt sich auf unser intuitives Verständnis der natürlichen Zahlen. Man kann das Konzept der natürlichen Zahlen auch formal einführen und so die natürlichen Zahlen in gewisser Weise „besser“ verstehen. Das wird in 2.1.6.11 und ausführlicher in 3.4.1.6 diskutiert. Das Wort „Induktion“ meint eigentlich „Hervorrufen“, so wie etwa das Betrachten einer Wurst die

Ausschüttung von Spucke induziert alias uns den Mund wässrig macht. Im Zusammenhang der vollständigen Induktion ist es dahingehend zu verstehen, daß die Richtigkeit unserer Aussage  $A(1)$  die Richtigkeit von  $A(2)$  induziert, die Richtigkeit von  $A(2)$  hinwiederum die Richtigkeit von  $A(3)$ , die Richtigkeit von  $A(3)$  die Richtigkeit von  $A(4)$ , und immer so weiter.

1.1.1.5. Es herrscht keine Einigkeit in der Frage, ob man die Null eine natürliche Zahl nennen soll. In diesem Text ist stets die Null mit gemeint, wenn von natürlichen Zahlen die Rede ist. Wollen wir die Null dennoch ausschließen, so sprechen wir wie oben von einer „natürlichen Zahl  $n \geq 1$ “.

1.1.1.6. Ich will kurz begründen, warum es mir natürlich scheint, auch die Null eine natürliche Zahl zu nennen: Hat bildlich gesprochen jedes Kind einer Klasse einen Korb mit Äpfeln vor sich und soll seine Äpfel zählen, so kann es ja durchaus vorkommen, daß in seinem Korb gar kein Apfel liegt, weil es zum Beispiel alle seine Äpfel bereits gegessen hat. In der Begrifflichkeit der Mengenlehre ausgedrückt, die wir in 2.1.1 einführen werden, muß man die leere Menge endlich nennen, wenn man erreichen will, daß jede Teilmenge einer endlichen Menge wieder endlich ist. Will man dann zusätzlich erreichen, daß die Kardinalität jeder endlichen Menge eine natürliche Zahl ist, so darf man die Null nicht aus den natürlichen Zahlen herauslassen.

1.1.1.7. Man kann sich den Satz anschaulich, wie in nebenstehendem Bild ange deutet, klar machen als eine Formel für die Fläche des Querschnitts durch eine Treppe der Länge  $n$  mit Stufenabstand und Stufenhöhe Eins. In der Tat bedeckt ein derartiger Querschnitt ja offensichtlich ein halbes Quadrat der Kantenlänge  $n$  nebst  $n$  halben Quadraten der Kantenlänge Eins. Ein weiterer Beweis geht so:

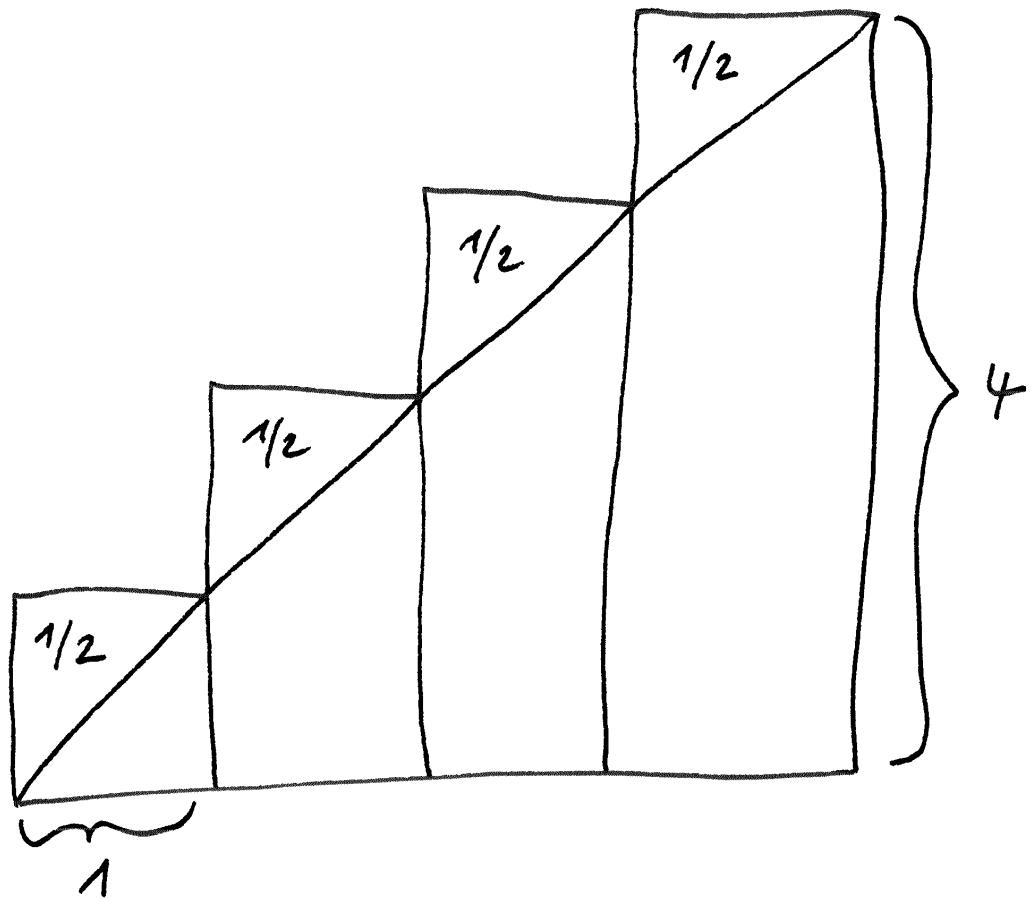
$$\begin{aligned} 1 + 2 + 3 + \dots + n &= \frac{1}{2} + \frac{2}{2} + \frac{3}{2} + \dots + \frac{n}{2} \\ &\quad + \frac{n}{2} + \frac{(n-1)}{2} + \frac{(n-2)}{2} + \dots + \frac{1}{2} \\ &= \frac{\frac{n+1}{2}}{2} + \frac{\frac{n+1}{2}}{2} + \frac{\frac{n+1}{2}}{2} + \dots + \frac{\frac{n+1}{2}}{2} \\ &= n(n+1)/2 \end{aligned}$$

Ich will letzteren Beweis benutzen, um eine neue Notation einzuführen.

**Definition 1.1.1.8.** Gegeben  $a_1, a_2, \dots, a_n$  schreiben wir

$$\sum_{i=1}^n a_i := a_1 + a_2 + \dots + a_n$$

Das Symbol  $\sum$  ist ein großes griechisches S und steht für „Summe“. Das Symbol  $:=$  deutet an, daß die Bedeutung der Symbole auf der doppelpunktbehafteten Seite des Gleichheitszeichens durch den Ausdruck auf der anderen Seite unseres



Die Gesamtfläche dieses Treppenquerschnitts ist offensichtlich  
 $4^2/2 + 4/2 = 4 \cdot 5/2$

Gleichheitszeichens definiert ist. Im obigen und ähnlichen Zusammenhängen heißen  $a_1, \dots, a_n$  die **Summanden** und  $i$  der **Laufindex**, da er eben etwa in unserem Fall von 1 bis  $n$  läuft und anzeigt alias „indiziert“, welcher Summand gemeint ist.

**1.1.1.9 (Zur Sprache in der Mathematik).** Das Wort „Definition“ kommt aus dem Lateinischen und bedeutet „Abgrenzung“. In Definitionen versuchen wir, die Bedeutung von Symbolen und Begriffen so klar wie möglich festzulegen. Sie werden merken, daß man in der Mathematik die Angewohnheit hat, in Definitionen Worte der Umgangssprache wie Menge, Gruppe, Körper, Unterkörper, Abbildung etcetera „umzuwidmen“ und ihnen ganz spezielle und meist nur noch entfernt mit der umgangssprachlichen Bedeutung verwandte neue Bedeutungen zu geben. In mathematischen Texten sind dann überwiegend diese umgewidmeten Bedeutungen gemeint. In dieser Weise baut die Mathematik also wirklich ihre eigene Sprache auf, bei der jedoch die Grammatik und auch nicht ganz wenige Wörter doch wieder von den uns geläufigen Sprachen übernommen werden. Das muß insbesondere für den Anfänger verwirrend sein, der sich auch bei ganz harmlos daherkommenden Wörtern stets fragen mussen, ob sie denn nun umgangssprachlich gemeint sind oder vielmehr bereits durch eine Definition auf eine mehr oder weniger andere und viel genauere Bedeutung festgelegt wurden. Um hier zu helfen, habe ich mir große Mühe mit dem Index gegeben, den Sie ganz am Schluß dieses Skriptums finden und in dem alle an verschiedenen Stellen eingeführten oder umgewidmeten und dort fett gedruckten Begriffe verzeichnet sein sollten. Und an dieser Stelle muß ich Sie schon bitten, das Wort „Index“ nicht als Laufindex mißzuverstehen!

*Beispiel 1.1.1.10.* In der  $\sum$ -Notation liest sich der in 1.1.1.7 gegebene Beweis so:

$$\begin{aligned}
 \sum_{i=1}^n i &= \sum_{i=1}^n \frac{i}{2} + \sum_{i=1}^n \frac{i}{2} \\
 &\quad \text{und nach Indexwechsel } i = n + 1 - k \text{ hinten} \\
 &= \sum_{i=1}^n \frac{i}{2} + \sum_{k=1}^n \frac{n+1-k}{2} \\
 &\quad \text{dann mache } k \text{ zu } i \text{ in der zweiten Summe} \\
 &= \sum_{i=1}^n \frac{i}{2} + \sum_{i=1}^n \frac{n+1-i}{2} \\
 &\quad \text{und nach Zusammenfassen beider Summen} \\
 &= \sum_{i=1}^n \frac{n+1}{2} \\
 &\quad \text{ergibt sich offensichtlich} \\
 &= n\left(\frac{n+1}{2}\right)
 \end{aligned}$$

*Beispiel 1.1.1.11.* Einen anderen Beweis derselben Formel liefert die Gleichungskette:

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

**Definition 1.1.1.12.** In einer ähnlichen Bedeutung wie das Symbol  $\sum$  verwendet man auch das Symbol  $\prod$ , ein großes griechisches  $P$ , für „Produkt“ und schreibt

$$\prod_{i=1}^n a_i := a_1 a_2 \dots a_n$$

Die  $a_1, \dots, a_n$  heißen in diesem und ähnlichen Zusammenhängen die **Faktoren** des Produkts.

**Definition 1.1.1.13.** Für jede natürliche Zahl  $n \geq 1$  definieren wir die Zahl  $n!$  (sprich:  $n$  **Fakultät**) durch die Formel

$$n! := 1 \cdot 2 \cdot \dots \cdot n = \prod_{i=1}^n i$$

Wir treffen zusätzlich die Vereinbarung  $0! := 1$  und haben also  $0! = 1$ ,  $1! = 1$ ,  $2! = 2$ ,  $3! = 6$ ,  $4! = 24$  und so weiter.

**1.1.1.14 (Allgemeinere Summen und Produkte).** Wir vereinbaren, daß Produkte, bei denen die obere Grenze des Laufindex um Eins kleiner ist als seine untere Grenze, der Wert 1 zugewiesen werden soll, also etwa  $1 = \prod_{i=1}^0 i = 0!$ . Ebenso vereinbaren wir auch, daß Summen, bei denen die obere Grenze des Laufindex um Eins kleiner ist als seine untere Grenze, der Wert 0 zugewiesen werden soll, so daß wir in Erweiterung unserer Formel 1.1.1.1 etwa schreiben könnten  $0 = \sum_{i=1}^0 i$ . Der Sinn dieser Erweiterungen zeigt sich darin, daß damit Formeln wie  $\sum_{i=k}^l a_i = \sum_{i=k}^m a_i + \sum_{i=m+1}^l a_i$  auch für  $m = k - 1$  richtig bleiben. Man mag sogar noch weiter gehen und die Definition von Summen und Produkten auf beliebige untere und obere Grenzen so erweitern, daß diese Formeln richtig bleiben, zumindest wenn alle Summanden ein Negatives beziehungsweise alle Faktoren einen Kehrwert haben. In dieser Allgemeinheit ist die fragliche Notation jedoch nur beim kontinuierlichen Analogon  $\int$  des Summenzeichens üblich, wie in ?? ausgeführt werden wird.

**Satz 1.1.1.15 (Bedeutung der Fakultät).** *Es gibt genau  $n!$  Möglichkeiten,  $n$  von einander verschiedene Objekte in eine Reihenfolge zu bringen.*

*Beispiel 1.1.1.16.* Es gibt genau  $3! = 6$  Möglichkeiten, die drei Buchstaben  $a$ ,  $b$  und  $c$  in eine Reihenfolge zu bringen, nämlich

$$\begin{array}{lll} abc & bac & cab \\ acb & bca & cba \end{array}$$

In gewisser Weise stimmt unser Satz sogar für  $n = 0$ : In der Terminologie, die wir in ?? einführen, gibt es genau eine Anordnung der leeren Menge.

*Beweis.* Hat man  $n$  voneinander verschiedene Objekte, so hat man  $n$  Möglichkeiten, ein Erstes auszusuchen, dann  $(n-1)$  Möglichkeiten, ein Zweites auszusuchen und so weiter, bis schließlich nur noch eine Möglichkeit bleibt, ein Letztes auszusuchen. Insgesamt haben wir also wie behauptet  $n!$  mögliche Reihenfolgen.  $\square$

**Definition 1.1.1.17.** Wir definieren für beliebiges  $n$  und jede natürliche Zahl  $k$  den **Binomialkoeffizienten**  $\binom{n}{k}$  (sprich:  $n$  über  $k$ ) durch die Regeln

$$\binom{n}{k} := \prod_{j=0}^{k-1} \frac{n-j}{k-j} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots1} \text{ für } k \geq 1 \text{ und } \binom{n}{0} := 1.$$

Der Sonderfall  $k = 0$  wird im Übrigen auch durch unsere allgemeine Formel gedeckt, wenn wir unsere Konvention 1.1.1.14 beherzigen. Im Lichte des folgenden Satzes schlage ich vor, die Binomialkoeffizienten  $\binom{n}{k}$  statt „ $n$  über  $k$ “ inhaltsreicher „ $k$  aus  $n$ “ zu sprechen.

1.1.1.18. Die Bezeichnung als Binomialkoeffizienten leitet sich von dem Auftreten dieser Zahlen als Koeffizienten in der „binomischen Formel“ 1.1.1.23 ab.

**Satz 1.1.1.19 (Bedeutung der Binomialkoeffizienten).** *Gegeben natürliche Zahlen  $n$  und  $k$  gibt es genau  $\binom{n}{k}$  Möglichkeiten, aus  $n$  voneinander verschiedenen Objekten  $k$  Objekte auszuwählen.*

*Beispiel 1.1.1.20.* Es gibt genau  $\binom{4}{2} = \frac{4 \cdot 3}{2 \cdot 1} = 6$  Möglichkeiten, aus den vier Buchstaben  $a, b, c, d$  zwei auszuwählen, nämlich

$$\begin{array}{lll} a, b & b, c & c, d \\ a, c & b, d \\ a, d \end{array}$$

*Beweis.* Wir haben  $n$  Möglichkeiten, ein erstes Objekt auszuwählen, dann  $n - 1$  Möglichkeiten, ein zweites Objekt auszuwählen, und so weiter, also insgesamt  $n(n - 1) \dots (n - k + 1)$  Möglichkeiten,  $k$  Objekte *der Reihe nach* auszuwählen. Auf die Reihenfolge, in der wir ausgewählt haben, kommt es uns aber gar nicht an, jeweils genau  $k!$  von unseren  $n(n - 1) \dots (n - k + 1)$  Möglichkeiten führen nach 1.1.1.15 also zur Auswahl derselben  $k$  Objekte. Man bemerke, daß unser Satz auch im Extremfall  $k = 0$  noch stimmt, wenn wir ihn geeignet interpretieren: In der Terminologie, die wir gleich einführen werden, besitzt in der Tat jede Menge genau eine nullelementige Teilmenge, nämlich die leere Menge.  $\square$

1.1.1.21. Offensichtlich gilt für alle natürlichen Zahlen  $n$  mit  $n \geq k$  die Formel

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

Das folgt einerseits sofort aus der formalen Definition und ist andererseits auch klar nach der oben erklärten Bedeutung der Binomialkoeffizienten: Wenn wir aus  $n$  Objekten  $k$  Objekte auswählen, so bleiben  $n - k$  Objekte übrig. Es gibt demnach gleichviele Möglichkeiten,  $k$  Objekte auszuwählen, wie es Möglichkeiten gibt,  $n - k$  Objekte auszuwählen. Wir haben weiter  $\binom{n}{n} = \binom{n}{0} = 1$  für jede natürliche Zahl  $n \geq 0$  sowie  $\binom{n}{1} = \binom{n}{n-1} = n$  für jede natürliche Zahl  $n \geq 1$ .

**Definition 1.1.1.22.** Wie in der Schule setzen wir  $a^k := \prod_{i=1}^k a$  und sprechen diesen Ausdruck „ $a$  hoch  $k$ “. In Worten ist also gemeint „das Produkt von  $k$ -mal dem Faktor  $a$ “. Im Lichte von 1.1.1.14 verstehen wir insbesondere  $a^0 := 1$ .

**Satz 1.1.1.23.** Für jede natürliche Zahl  $n$  gilt die **binomische Formel**

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

1.1.1.24. Man beachte, wie wichtig unsere Konvention  $a^0 = 1$  und insbesondere auch ihr Spezialfall  $0^0 = 1$  für die Gültigkeit dieser Formel ist.

1.1.1.25. Die Bezeichnung „binomische Formel“ leitet sich ab von der Vorsilbe „bi“ für Zwei, wie etwa in englisch „bicycle“ für „Zweirad“ alias „Fahrrad“, und dem lateinischen Wort „nomen“ für „Namen“. Mit den beiden „Namen“ sind hier  $a$  und  $b$  gemeint. Mehr dazu wird in ?? erklärt.

*Erster Beweis.* Beim Ausmultiplizieren erhalten wir das Monom  $a^k b^{n-k}$  so oft, wie es Möglichkeiten gibt, aus unseren  $n$  Faktoren  $(a + b)$  die  $k$  Faktoren auszusuchen, „in denen wir beim Ausmultiplizieren das  $a$  nehmen“. Dieses Argument werden wir in 2.1.2.11 noch besser formulieren. □

*Zweiter Beweis.* Dieser Beweis ist eine ausgezeichnete Übung im Umgang mit unseren Symbolen und mit der vollständigen Induktion. Er scheint mir jedoch auch in einer für Beweise durch vollständige Induktion typischen Weise wenig durchsichtig. Zunächst prüfen wir für beliebiges  $n$  und jede natürliche Zahl  $k \geq 1$  die Formel

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

durch explizites Nachrechnen. Dann geben wir unserer Formel im Satz den Namen  $A(n)$  und prüfen die Formel  $A(0)$  und zur Sicherheit auch noch  $A(1)$  durch Hinsehen. Schließlich gilt es, den Induktionsschritt durchzuführen, als da heißtt,

$A(n+1)$  aus  $A(n)$  zu folgern. Dazu rechnen wir

$$\begin{aligned}
 (a+b)^{n+1} &= (a+b)(a+b)^n \\
 &\quad \text{und mit der Induktionsvoraussetzung} \\
 &= (a+b) \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\
 &\quad \text{und durch Ausmultiplizieren} \\
 &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\
 &\quad \text{und Indexwechsel } k = i - 1 \text{ in der ersten Summe} \\
 &= \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n-i+1} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\
 &\quad \text{dann mit } k \text{ statt } i \text{ und Absondern von Summanden} \\
 &= a^{n+1} b^0 + \sum_{k=1}^n \binom{n}{k-1} a^k b^{n-k+1} + \\
 &\quad + \sum_{k=1}^n \binom{n}{k} a^k b^{n-k+1} + a^0 b^{n+1} \\
 &\quad \text{und nach Zusammenfassen der mittleren Summen} \\
 &= a^{n+1} b^0 + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n-k+1} + a^0 b^{n+1} \\
 &\quad \text{und Einbeziehen der abgesonderten Summanden} \\
 &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
 \end{aligned}$$

und folgern so tatsächlich  $A(n+1)$  aus  $A(n)$ .  $\square$

1.1.1.26. Die Formel  $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$  für  $k \geq 1$  kann man zur effektiven Berechnung der Binomialkoeffizienten mit dem sogenannten **Pascal'schen Dreieck** benutzen: Im Schema

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & & 1 & 1 & & \\
 & & & 1 & 2 & 1 & \\
 & & & 1 & 3 & 3 & 1 \\
 & & & 1 & 4 & 6 & 4 & 1
 \end{array}$$

seien die Einsen an den Rändern vorgegeben und eine Zahl in der Mitte berechne sich als die Summe ihrer beiden oberen „Nachbarn“. Dann stehen in der  $(n+1)$ -ten Zeile der Reihe nach die Binomialkoeffizienten  $\binom{n}{0} = 1, \binom{n}{1} = n, \dots$ , bis  $\binom{n}{n-1} = n, \binom{n}{n} = 1$ . Wir haben also zum Beispiel nach der untersten Zeile in obigem Ausschnitt des Pascal'schen Dreiecks

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

## Übungen

*Ergänzende Übung 1.1.1.27.* Man zeige: Ist  $p$  eine Primzahl und  $n$  nicht durch  $p$  teilbar und  $e \geq 0$  eine natürliche Zahl, so ist

$$\binom{p^e n}{p^e}$$

auch nicht durch  $p$  teilbar. Hinweis: Man möge bei der Lösung dieser Übung bereits die Erkenntnis verwenden, daß eine Primzahl ein Produkt nur teilen kann, wenn sie einen der Faktoren teilt. Ein Beweis dieser Tatsache wird in 3.4.4.15 nachgeholt.

*Übung 1.1.1.28.* Man finde und beweise eine Formel für  $\sum_{i=1}^n i^2$ . Hinweis: Man suche zunächst eine Formel für  $\sum_{i=1}^n i^3 - (i-1)^3$  und beachte  $i^3 - (i-1)^3 = 3i^2 - 3i + 1$ .

*Ergänzende Übung 1.1.1.29.* Man zeige, daß für jedes  $k \in \mathbb{N}$  eine Formel der Gestalt  $\sum_{i=1}^n i^k = \frac{1}{k+1}n^{k+1} + a_k n^k + \dots + a_1 n + a_0$  gilt mit  $a_\kappa \in \mathbb{Q}$ .

## 1.1.2 Fibonacci-Folge und Vektorraumbegriff

1.1.2.1. Ich beginne mit einigen Beispielen für eine mathematische Struktur, die ihnen im weiteren Verlauf des Studiums als „Vektorraum“ geläufig werden wird.

### Beispiel 1.1.2.2. Die Fibonacci-Folge

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

entsteht, indem man mit  $f_0 = 0$  und  $f_1 = 1$  beginnt und dann jedes weitere Folgenglied als die Summe seiner beiden Vorgänger bildet, in Formeln

$$f_{i+2} := f_{i+1} + f_i$$

Wir suchen nun für die Glieder  $f_i$  dieser Folge eine geschlossene Darstellung. Dazu vereinbaren wir, daß wir Folgen  $x_0, x_1, x_2, \dots$  mit  $x_n = x_{n-1} + x_{n-2}$  für  $n = 2, 3, 4, \dots$  **Folgen vom Fibonacci-Typ** nennen wollen. Kennen wir die beiden ersten Glieder einer Folge vom Fibonacci-Typ, so legt das natürlich bereits die gesamte Folge fest. Nun bemerken wir, daß für jede Folge  $x_0, x_1, x_2, \dots$  vom Fibonacci-Typ und jedes  $\alpha$  auch die Folge  $\alpha x_0, \alpha x_1, \alpha x_2, \dots$  vom Fibonacci-Typ ist, und daß für jede weitere Folge  $y_0, y_1, y_2, \dots$  vom Fibonacci-Typ auch die gliedweise Summe  $(x_0 + y_0), (x_1 + y_1), (x_2 + y_2), \dots$  eine Folge vom Fibonacci-Typ ist. Der Trick ist dann, danach zu fragen, für welche  $\beta$  die Folge  $x_i := \beta^i$  vom Fibonacci-Typ ist. Das ist ja offensichtlich genau dann der Fall, wenn gilt

$\beta^2 = \beta + 1$ , als da heißt für  $\beta_{\pm} = \frac{1}{2}(1 \pm \sqrt{5})$ . Für beliebige  $c, d$  ist mithin die Folge

$$x_i = c\beta_+^i + d\beta_-^i$$

vom Fibonacci-Typ, und wenn wir  $c$  und  $d$  bestimmen mit  $x_0 = 0$  und  $x_1 = 1$ , so ergibt sich eine explizite Darstellung unserer Fibonacci-Folge. Wir suchen also  $c$  und  $d$  mit

$$\begin{aligned} 0 &= c + d \\ 1 &= c\left(\frac{1}{2}(1 + \sqrt{5})\right) + d\left(\frac{1}{2}(1 - \sqrt{5})\right) \end{aligned}$$

und folgern leicht  $c = -d$  und  $1 = c\sqrt{5}$  alias  $c = 1/\sqrt{5} = -d$ . Damit ergibt sich schließlich für unsere ursprüngliche Fibonacci-Folge die explizite Darstellung

$$f_i = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^i - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^i$$

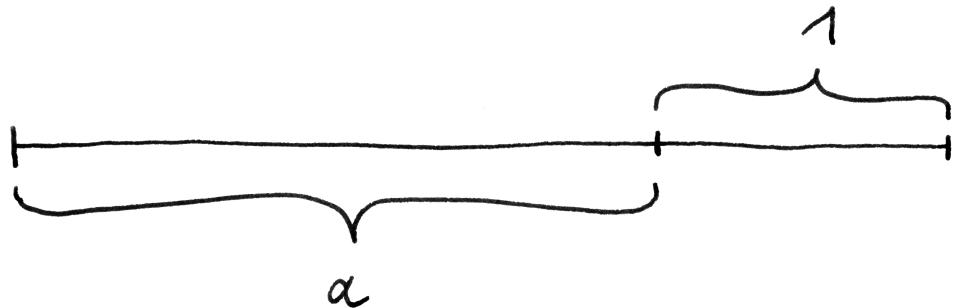
Im übrigen ist der zweite Summand hier immer kleiner als  $1/2$ , so daß wir  $f_i$  auch beschreiben können als diejenige ganze Zahl, die am nächsten am ersten Summanden liegt. Es wäre rückblickend natürlich ein Leichtes gewesen, diese Formel einfach zu „raten“, um sie dann mit vollständiger Induktion 1.1.1.1 zu beweisen. Diese Art mathematischer Zaubertricks halte ich jedoch für unehrenhaft. Ich denke, unsere Aufgabe als Mathematiker besteht darin, Verständnis zu erzeugen und nicht Bewunderung. Ich werde deshalb stets nach Kräften versuchen, das Tricksen zu vermeiden, auch wenn die Beweise dadurch manchmal etwas länger werden sollten. Eine Möglichkeit, auch den letzten verbleibenden Trick aus den vorhergehenden Überlegungen zu eliminieren, zeigt 3.5.5.18. Die bei unserer Lösung auftretende reelle Zahl  $\frac{1}{2}(1 + \sqrt{5})$  ist im Übrigen auch bekannt als „goldener Schnitt“ aus Gründen, die in nebenstehendem Bild diskutiert werden. In ?? dürfen Sie dann zur Übung zeigen, daß der Quotient zweier aufeinanderfolgender Fibonacci-Zahlen gegen den goldenen Schnitt strebt, daß also genauer und in Formeln für unsere Fibonacci-Folge  $f_0, f_1, f_2, \dots$  von oben gilt

$$\lim_{i \rightarrow \infty} \frac{f_{i+1}}{f_i} = \frac{1 + \sqrt{5}}{2}$$

*Beispiel 1.1.2.3.* Wir betrachten das Gleichungssystem

$$\begin{aligned} 3x + 3y + 7z &= 0 \\ 4x + y + 5z &= 0 \end{aligned}$$

Wie man die Menge  $L$  aller Lösungen  $(x, y, z)$  ermittelt, sollen sie später in dieser Vorlesung lernen. Zwei Dinge aber sind a priori klar:



Der **goldene Schnitt** ist das Verhältnis, in dem eine Strecke geteilt werden muß, damit das Verhältnis vom größeren zum kleineren Stück gleich dem Verhältnis des Ganzen zum größeren Stück ist, also die positive Lösung der Gleichung  $a/1 = (1+a)/a$  alias  $a^2 - a - 1 = 0$ , also  $a = (1 + \sqrt{5})/2$ .

1. Sind  $(x, y, z)$  und  $(x', y', z')$  Lösungen, so ist auch ihre komponentenweise Summe  $(x + x', y + y', z + z')$  eine Lösung;
2. Ist  $(x, y, z)$  eine Lösung und  $\alpha$  eine reelle Zahl, so ist auch das komponentenweise Produkt  $(\alpha x, \alpha y, \alpha z)$  eine Lösung.

*Beispiel 1.1.2.4.* Wir betrachten die Menge aller Funktionen  $f : \mathbb{R} \rightarrow \mathbb{R}$ , die zweimal differenzierbar sind und der Differentialgleichung

$$f'' = -f$$

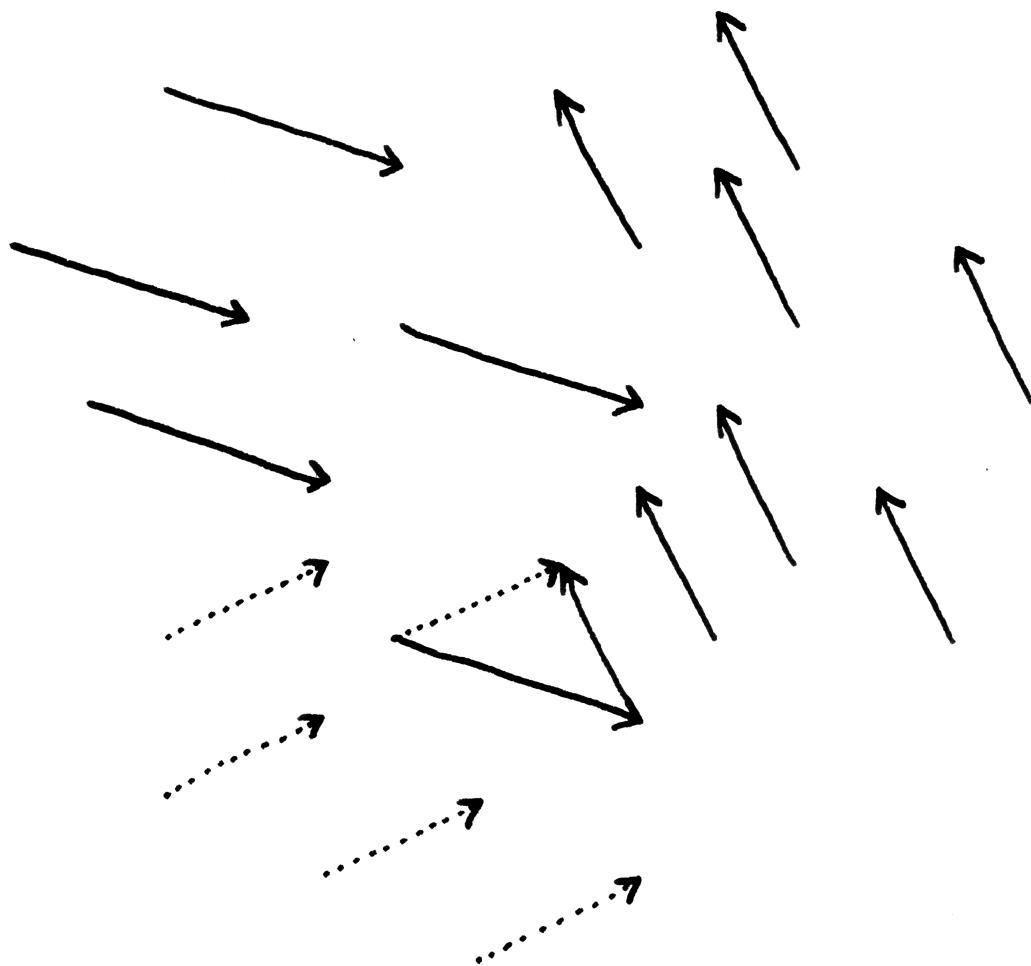
genügen. Lösungen sind zum Beispiel die Funktionen  $\sin$ ,  $\cos$ , die Nullfunktion oder auch die Funktionen  $f(x) = \sin(x + a)$  für konstantes  $a$ . Wie man die Menge  $L$  aller Lösungen beschreiben kann, sollen Sie in der Analysis lernen. Zwei Dinge aber sind a priori klar:

1. Mit  $f$  und  $g$  ist auch die Funktion  $f + g$  eine Lösung;
2. Ist  $f$  eine Lösung und  $\alpha$  eine reelle Zahl, so ist auch  $\alpha f$  eine Lösung.

*Beispiel 1.1.2.5.* Wir betrachten die Gesamtheit aller Parallelverschiebungen der Tafeloberfläche. Graphisch stellen wir solch eine Parallelverschiebung dar durch einen Pfeil von irgendeinem Punkt zu seinem Bild unter der Verschiebung. Im nebenstehenden Bild stellen etwa alle gepunkteten Pfeile dieselbe Parallelverschiebung dar. Was für ein Ding diese Gesamtheit  $P$  aller Parallelverschiebungen eigentlich ist, scheint mir recht undurchsichtig, aber einiges ist a priori klar:

1. Sind  $p$  und  $q$  Parallelverschiebungen, so ist auch ihre „Hintereinanderausführung“  $p \circ q$ , sprich „ $p$  nach  $q$ “, eine Parallelverschiebung.
2. Ist  $\alpha$  eine reelle Zahl und  $p$  eine Parallelverschiebung, so können wir eine neue Parallelverschiebung  $\alpha p$  bilden, das „ $\alpha$ -fache von  $p$ “. Bei negativen Vielfachen vereinbaren wir hierzu, daß damit eine entsprechende Verschiebung in die Gegenrichtung gemeint ist.
3. Führen wir eine neue Notation ein und schreiben für die Hintereinanderausführung  $p + q := p \circ q$ , so gelten für beliebige Parallelverschiebungen  $p, q, r$  der Tafeloberfläche und beliebige reelle Zahlen  $\alpha, \beta$  die Formeln

$$\begin{aligned} (p + q) + r &= p + (q + r) \\ p + q &= q + p \\ \alpha(\beta p) &= (\alpha\beta)p \\ (\alpha + \beta)p &= (\alpha p) + (\beta p) \\ \alpha(p + q) &= (\alpha p) + (\alpha q) \end{aligned}$$



Die Hintereinanderausführung der beiden Parallelverschiebungen der Tafel- oder hier vielmehr der Papierebene, die durch die durchgezogenen Pfeile dargestellt werden, wird die durch die gepunkteten Feile dargestellt.

Will man sich die Gesamtheit aller Parallelverschiebungen der Tafelebene anschaulich machen, so tut man im Übrigen gut daran, einen Punkt als „Ursprung“ auszuzeichnen und jede Parallelverschiebung mit dem Punkt der Tafelebene zu identifizieren, auf den unsere Parallelverschiebung diesen Ursprung abbildet.

*Beispiel* 1.1.2.6. Analoges gilt für die Gesamtheit der Parallelverschiebung des Raums unserer Anschauung und auch für die Gesamtheit aller Verschiebungen einer Geraden und, mit noch mehr Mut, für die Gesamtheit aller Zeitspannen.

1.1.2.7. Die Formeln unserer kleinen Formelsammlung von 1.1.2.5.3 gelten ganz genauso auch für die Lösungsmenge unserer Differentialgleichung  $f'' = -f$ , wenn wir  $f + g := f + g$  verstehen, für die Lösungsmenge unseres linearen Gleichungssystems, wenn wir

$$(x, y, z) \dotplus (x', y', z') := (x + x', y + y', z + z')$$

als „komponentenweise Addition“ verstehen, und für die Menge aller Folgen vom Fibonacci-Typ, wenn wir ähnlich die Summe  $\dotplus$  zweier Folgen erklären. Ein wesentliches Ziel der Vorlesungen über lineare Algebra ist es, einen abstrakten Formalismus aufzubauen, dem sich alle diese Beispiele unterordnen. Dadurch soll Zweierlei erreicht werden:

1. Unser abstrakter Formalismus soll uns dazu verhelfen, die uns als Augentieren und Nachkommen von Ästehüpfen angeborene räumliche Anschauung nutzbar zu machen zum Verständnis der bis jetzt gegebenen Beispiele und der vielen weiteren Beispiele von Vektorräumen, denen Sie im Verlauf Ihres Studiums noch begegnen werden. So werden sie etwa lernen, daß man sich die Menge aller Folgen vom Fibonacci-Typ durchaus als Ebene vorstellen darf und die Menge aller Folgen mit einem vorgegebenem Folgenglied an einer vorgegebenen Stelle als eine Gerade in dieser Ebene. Suchen wir also alle Folgen vom Fibonacci-Typ mit zwei vorgegebenen Folgengliedern, so werden wir im allgemeinen genau eine derartige Lösung finden, da sich eben zwei Geraden aus einer Ebene im allgemeinen in genau einem Punkt schneiden. In diesem Licht betrachtet soll der abstrakte Formalismus uns also helfen, a priori unanschauliche Fragestellungen der Anschauung zugänglich zu machen. Ich denke, diese Nähe zur Anschauung ist auch der Grund dafür, daß die lineare Algebra meist an den Anfang des Studiums gestellt wird: Von der Schwierigkeit des Formalismus her gesehen gehört sie nämlich keineswegs zu den einfachsten Gebieten der Mathematik. Hier würde ich eher an Gruppentheorie oder Graphentheorie oder dergleichen denken.

2. Unser abstrakter Formalismus soll so unmöglich verständlich sein und seine Spielregeln so klar, daß Sie in die Lage versetzt werden, alles nachzuvollziehen und mir im Prinzip und vermutlich auch in der Realität Fehler nachzuweisen. Schwammige Begriffe wie „Tafelebene“ oder „Parallelverschiebung des Raums“ haben in

einem solchen Formalismus keinen Platz mehr. In diesem Licht betrachtet verfolgen wir mit dem Aufbau des abstrakten Formalismus auch das Ziel einer großen Vereinfachung durch die Reduktion auf die Beschreibung einiger weniger Aspekte der uns umgebenden in ihrer Komplexität schwer faßbaren Wirklichkeit.

Die lineare Algebra hat in meinen Augen mindestens drei wesentliche Aspekte: Einen **geometrischen Aspekt**, wie ihn das Beispiel 1.1.2.5 der Gesamtheit aller Parallelverschiebungen illustriert; einen **algorithmischen Aspekt**, unter den ich das Beispiel 1.1.2.3 der Lösungsmenge eines linearen Gleichungssystems und insbesondere explizite Verfahren zur Bestimmung dieser Lösungsmenge einordnen würde; und einen **abstrakt-algebraischen Aspekt**, zu dem etwa die folgende Definition 1.1.2.8 gehört, eine Art gedankliches Skelett, das Algorithmik und Geometrie verbindet und Brücken zu vielen weiteren Anwendungen schafft, die man dann als das Fleisch auf diesem Gerippe ansehen mag. Ich will im Verlauf meiner Vorlesungen zur linearen Algebra versuchen, diese drei Aspekte zu einer Einheit zu fügen. Ich hoffe, daß Sie dadurch in die Lage versetzt werden, eine Vielzahl von Problemen mit den verbundenen Kräften Ihrer räumlichen Anschauung, Ihrer algorithmischen Rechenfähigkeiten und Ihres abstrakt-logischen Denkens anzugehen. Als Motivation für den weiteren Fortgang der Vorlesungen über lineare Algebra beschreibe ich nun das „Rückgrat unseres Skeletts“ und formuliere ohne Rücksicht auf noch unbekannte Begriffe und Notationen die abstrakte Definition eines reellen Vektorraums.

**Definition 1.1.2.8.** Ein **reeller Vektorraum** ist ein Tripel bestehend aus den folgenden drei Dingen:

1. Einer Menge  $V$ ;
2. Einer Verknüpfung  $V \times V \rightarrow V$ ,  $(v, w) \mapsto v + w$ , die die Menge  $V$  zu einer abelschen Gruppe macht;
3. Einer Abbildung  $\mathbb{R} \times V \rightarrow V$ ,  $(\alpha, v) \mapsto \alpha v$ ,

derart, daß für alle  $\alpha, \beta \in \mathbb{R}$  und alle  $v, w \in V$  gilt:

$$\begin{aligned}\alpha(\beta v) &= (\alpha\beta)v \\ (\alpha + \beta)v &= (\alpha v) + (\beta v) \\ \alpha(v + w) &= (\alpha v) + (\alpha w) \\ 1v &= v\end{aligned}$$

Hier ist nun viel zu klären: Was ist eine Menge? Eine Verknüpfung? Eine abelsche Gruppe? Eine Abbildung? Was bedeuten die Symbole  $\times$ ,  $\rightarrow$ ,  $\mapsto$ ,  $\in$ ,  $\mathbb{R}$ ? Wir beginnen in der nächsten Vorlesung mit der Klärung dieser Begriffe und Notationen.

1.1.2.9. Bereits hier will ich die Symbole  $\alpha$  und  $\beta$  erklären: Sie heißen „Alpha“ und „Beta“ und sind die beiden ersten Buchstaben des griechischen Alphabets, das ja hinwiederum selbst nach ihnen benannt ist. Bei der Darstellung von Mathematik hilft es, viele verschiedene Symbole und Symbolfamilien zur Verfügung zu haben. Insbesondere werden die griechischen Buchstaben oft und gerne verwendet. Ich schreibe deshalb hier zum Nachschlagen das griechische Alphabet auf. In der ersten Spalte stehen der Reihe nach die griechischen Kleinbuchstaben, dahinter die zugehörigen Großbuchstaben, dann ihr lateinisches Analogon soweit vorhanden, und schließlich, wie man diesen griechischen Buchstaben auf Deutsch benennt und spricht.

|                         |            |    |                     |
|-------------------------|------------|----|---------------------|
| $\alpha$                | A          | a  | alpha               |
| $\beta$                 | B          | b  | beta                |
| $\gamma$                | $\Gamma$   | g  | gamma               |
| $\delta$                | $\Delta$   | d  | delta               |
| $\epsilon, \varepsilon$ | E          | e  | epsilon             |
| $\zeta$                 | Z          | z  | zeta                |
| $\eta$                  | H          | ä  | eta                 |
| $\theta, \vartheta$     | $\Theta$   | th | theta               |
| $\iota$                 | I          | i  | iota                |
| $\kappa$                | K          | k  | kappa               |
| $\lambda$               | $\Lambda$  | l  | lambda              |
| $\mu$                   | M          | m  | my, sprich „mü“     |
| $\nu$                   | N          | n  | ny, sprich „nü“     |
| $\xi$                   | $\Xi$      | x  | xi                  |
| $\o$                    | O          | o  | omikron, „kurzes o“ |
| $\pi$                   | $\Pi$      | p  | pi                  |
| $\rho, \varrho$         | P          | r  | rho                 |
| $\sigma, \varsigma$     | $\Sigma$   | s  | sigma               |
| $\tau$                  | T          | t  | tau                 |
| $\upsilon$              | $\Upsilon$ | y  | upsilon             |
| $\phi, \varphi$         | $\Phi$     | f  | phi                 |
| $\chi$                  | X          | ch | chi                 |
| $\psi$                  | $\Psi$     | ps | psi                 |
| $\omega$                | $\Omega$   | oh | omega, „langes o“   |

## Übungen

Übung 1.1.2.10. Ein Kredit von 10000 Euro wird am Ende jeden Jahres mit einem jährlichen Zinssatz von 5% auf die jeweilige Restschuld verzinst und der Kreditnehmer zahlt zu Beginn jeden Jahres 1000 Euro zurück. Man finde eine ge-

schlossene Formel für die Restschuld am Ende des  $n$ -ten Jahres. Hinweis: Man mag es mit dem Ansatz  $x_n = c\beta^n + \alpha$  versuchen.

*Übung 1.1.2.11.* Kann man für jede Folge  $x_0, x_1, \dots$  vom Fibonacci-Typ Zahlen  $c, d$  finden mit  $x_i = c\beta_+^i + d\beta_-^i$  für alle  $i$ ? Finden Sie eine geschlossene Darstellung für die Glieder der Folge, die mit  $0, 0, 1$  beginnt und dem Bildungsgesetz  $x_n = 2x_{n-1} + x_{n-2} - 2x_{n-3}$  gehorcht.

*Übung 1.1.2.12.* Die Fibonacci-Folge erfüllt die Identität  $f_0^2 + f_1^2 + \dots + f_k^2 = f_k f_{k+1}$  für alle  $k \geq 0$ .

*Übung 1.1.2.13.* Wer Alles mit φl μ kaπrt, hat eine gρβηt gηn.  
Wer Hausis nur koπrt, steht am Pρβg hintan.

Gestern standen wir noch vor einem tiefen Abgrund,  
aber heute haben wir einen gρßen Schritt nach vorne gηn

Liebe ist, wenn sich der τsendste Kuss noch wie der erste anφlt.

Nach dem Takt, den man tρmmelt, wird auch gηnzt.

Vorgηn und nachβcht  
hat manchem schon gρß Leid gebracht.

Was mit wenigem abgηn werden kann,  
muss nicht mit φlem gηn werden.

Als ich eine ρse brach,  
und mir in den φnger stach...

τsend Freunde sind zu wenig,  
ein Feind jedoch ist zu φl



## **Kapitel 2**

# **Mengen und Verknüpfungen**

In diesen Abschnitten habe ich Notationen und Begriffsbildungen zusammengefaßt, von denen ich mir vorstelle, daß sie zu Beginn des Studiums in enger Abstimmung zwischen den beiden Grundvorlesungen erklärt werden könnten.

## 2.1 Naive Mengenlehre und Kombinatorik

### 2.1.1 Mengen

2.1.1.1. Beim Arbeiten mit reellen Zahlen oder räumlichen Gebilden reicht auf der Schule ein intuitives Verständnis meist aus, und wenn die Intuition in die Irre führt, ist ein Lehrer zur Stelle. Wenn Sie jedoch selbst unterrichten oder etwas beweisen wollen, reicht dieses intuitive Verständnis nicht mehr aus. Im folgenden werden deshalb zunächst der Begriff der reellen Zahlen und der Begriff des Raums zurückgeführt auf Grundbegriffe der Mengenlehre, den Begriff der rationalen Zahlen und elementare Logik. Bei der Arbeit mit diesen Begriffen führt uns die Intuition nicht so leicht in die Irre, wir geben uns deshalb mit einem intuitiven Verständnis zufrieden und verweisen jeden, der es noch genauer wissen will, auf eine Vorlesung über Logik. Wir beginnen mit etwas naiver Mengenlehre, wie sie von Georg Cantor in den Jahren 1874 bis 1897 begründet wurde und von der berühmten Mathematiker David Hilbert einmal sagte: „Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können“. Natürlich gab es auch vor der Mengenlehre schon hoch entwickelte Mathematik: Beim Tod von Carl Friedrich Gauß im Jahre 1855 gab es diese Theorie noch gar nicht und Fourier fand seine „Fourierentwicklung“ sogar bereits zu Beginn des 19.-ten Jahrhunderts. Er behauptete auch gleich in seiner „Théorie analytique de la chaleur“, daß sich jede beliebige periodische Funktion durch eine Fouriereihe darstellen lasse, aber diese Behauptung stieß bei anderen berühmten Mathematikern seiner Zeit auf Ablehnung und es entstand darüber ein heftiger Disput. Erst in besagtem „Paradies der Mengenlehre“ konnten die Fourier's Behauptung zugrundeliegenden Begriffe soweit geklärt werden, daß dieser Disput nun endgültig beigelegt ist. Ähnlich verhält es sich auch mit vielen anderen Fragestellungen. Da die Mengenlehre darüber hinaus auch vom didaktischen Standpunkt aus eine äußerst klare und durchsichtige Darstellung mathematischer Sachverhalte ermöglicht, hat sie sich als Grundlage der höheren Mathematik und der Ausbildung von Mathematikern an Universitäten schnell durchgesetzt und ist nun weltweit das „Alphabet der Sprache der Mathematik“. Man wird an Universitäten sogar geradezu dazu erzogen, alle Mathematik in der Sprache der Mengenlehre zu fassen und geometrischen Argumenten keine Beweiskraft zuzugestehen. Ich halte das bei der Ausbildung von Mathematikern auch für angemessen. Bei der Mathematik-Ausbildung im allgemeinen scheint mir dieses Vorgehen dahingegen nicht zielführend: In diesem Kontext sollte man meines Erachtens nicht mit demselben Maß messen, auch ohne alle Mengenlehre geometrisch erklärte Begriffe wie Gerade und Kreis, Ebene und Raum, als wohldefinierte Objekte der Mathematik zulassen und geometrischen Argumenten Beweiskraft zugestehen.

2.1.1.2. Im Wortlaut der ersten Zeilen des Artikels „Beiträge zur Begründung der

transfiniten Mengenlehre (Erster Aufsatz)“ von Georg Cantor, erschienen im Jahre 1895, hört sich die Definition einer Menge so an:

Unter einer **Menge** verstehen wir jede Zusammenfassung  $M$  von bestimmten wohlunterschiedenen Objekten  $m$  unserer Anschauung oder unseres Denkens (welche die **Elemente** von  $M$  genannt werden) zu einem Ganzen.

Verbinden wir mit einer Menge eine geometrische Vorstellung, so nennen wir ihre Elemente auch **Punkte** und die Menge selbst einen **Raum**. Ein derartiges Herumgerede ist natürlich keine formale Definition und birgt durchaus verschiedene Fallstricke, vergleiche 2.1.3.9. Das Ziel dieser Vorlesung ist aber auch nicht eine formale Begründung der Mengenlehre, wie Sie sie in der Logik kennenzulernen können. Sie sollen vielmehr die Bedeutung dieser Worte intuitiv erfassen wie ein Kleinkind, das Sprechen lernt: Indem sie mir und anderen Mathematikern zuhören, wie wir mit diesen Worten sinnvolle Sätze bilden, uns nachahmen, und beobachten, welchen Effekt Sie damit hervorrufen. Unter anderem dazu sind die Übungsgruppen da.

*Ergänzung 2.1.1.3.* Bei der Entwicklung der Mathematik aus der Umgangssprache durch fortgesetztes Zuspitzen und Umwidmen des Wortschatzes muß ich an den Baron von Münchhausen denken, wie er sich an seinen eigenen Haaren aus dem Sumpf zieht. Schon verblüffend, daß es klappt. Aber bei Kleinkindern, die Sprechen lernen, ist es ja noch viel verblüffender, wie sie die Bedeutung von Wörtern erfassen, ohne daß man sie ihnen in Worten erklären kann.

*Beispiele 2.1.1.4.* Endliche Mengen kann man durch eine vollständige Liste ihrer Elemente in geschweiften Klammern angeben, zum Beispiel in der Form

$$X = \{x_1, x_2, \dots, x_n\}$$

Diese geschweiften Klammern heißen auch **Mengenklammern**. Die Elemente dürfen mehrfach genannt werden und es kommt nicht auf die Reihenfolge an, in der sie genannt werden. Wir haben also  $\{1, 1, 2\} = \{2, 1\}$ . Die Aussage „ $x$  ist Element von  $X$ “ wird mit  $x \in X$  abgekürzt, ihre Verneinung „ $x$  ist nicht Element von  $X$ “ mit  $x \notin X$ . Zum Beispiel gilt  $1 \in \{2, 1\}$  und  $3 \notin \{2, 1\}$ . Es gibt auch die sogenannte **leere Menge**  $\emptyset = \{\}$ , die gar kein Element enthält. Andere Beispiele sind die Mengen

$\mathbb{N} := \{0, 1, 2, \dots\}$  der **natürlichen Zahlen**,

$\mathbb{Z} := \{0, 1, -1, 2, -2, \dots\}$  der **ganzen Zahlen** und

$\mathbb{Q} := \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$  der **rationalen Zahlen**.

Der Name letzterer Menge kommt von lateinisch „ratio“ für „Verhältnis“, der Buchstabe  $\mathbb{Q}$  steht für „Quotient“. Man beachte, daß wir auch hier Elemente mehrfach genannt haben, es gilt ja  $p/q = p'/q'$  genau dann, wenn  $pq' = p'q$ . Auf Deutsch bezeichnet man die rationalen Zahlen auch als **Bruchzahlen**, da man sich etwa ein Viertel eines Kekses als den Anteil denken kann, der entsteht, wenn man besagten Keks in vier gleiche Teile zerbricht. Einen Leitfaden zu einem formaleren Aufbau des Zahlensystems können Sie in 2.2.5.1 finden.

*Ergänzung 2.1.1.5 (Herkunft des Gleichheitszeichens).* Das Gleichheitszeichen = scheint auf ein 1557 von Robert Recorde publiziertes Buch zurückzugehen und soll andeuten, daß das, was auf der linken und rechten Seite dieses Zeichens steht, so gleich ist wie die beiden Strichlein, die das uns heute so selbstverständliche Gleichheitszeichen bilden. Davor schrieb man statt einem Gleichheitszeichen meist *ae* für „äquivalent“.

*Ergänzung 2.1.1.6 (Diskussion der Notation).* In Texten, in deren Konventionen die Null keine natürliche Zahl ist, verwendet man meist die abweichenden Notationen  $\mathbb{N}$  für die Menge  $\{1, 2, \dots\}$  und  $\mathbb{N}_0$  für die Menge  $\{0, 1, 2, \dots\}$ . Die in diesem Text verwendete Notation  $\mathbb{N} = \{0, 1, 2, \dots\}$  stimmt mit der internationalen Norm ISO 31-11 überein.

2.1.1.7. Die Bedeutung der Symbole  $\mathbb{Z}$  und  $\mathbb{Q}$  ist in der Mathematik weitgehend einheitlich. Man verwendet diesen Schrifttypus auch sonst gerne für Symbole, die in ihrer Bedeutung über große Teile der Mathematik hinweg einheitlich verwendet werden. Bei der Bedeutung von  $\mathbb{N}$  ist man allerdings nie ganz sicher, ob die Null mitgemeint ist. In den Konventionen dieses Textes gilt  $0 \in \mathbb{N}$ .

2.1.1.8. Eine Menge, die nur endlich viele Elemente hat, nennen wir eine **endliche Menge**. Eine präzisere Definition dieses Konzepts wird in 3.4.1.2 gegeben. Wir vereinbaren bereits hier, daß wir auch die leere Menge endlich nennen. Die Zahl der Elemente einer endlichen Menge  $X$  nennen wir ihre **Kardinalität** oder **Mächtigkeit** und notieren sie

$$|X|$$

oder  $\text{card}(X)$ . In der Literatur findet man auch die Notation  $\sharp X$ . Für endliche Mengen  $X$  ist demnach ihre Kardinalität stets eine natürliche Zahl  $|X| \in \mathbb{N}$  und  $|X| = 0$  ist gleichbedeutend zu  $X = \emptyset$ . Ist  $X$  unendlich, so schreiben wir bis auf weiteres kurzerhand  $|X| = \infty$  und ignorieren in unserer Notation, daß auch unendliche Mengen „verschieden groß“ sein können. Für ein Beispiel für „verschieden große unendliche Mengen“ siehe ?? und für eine genauere Diskussion des Begriffs der Kardinalität vergleiche ??.

### 2.1.2 Teilmengen

**Definition 2.1.2.1.** Eine Menge  $Y$  heißt **Teilmenge** einer Menge  $X$ , wenn jedes Element von  $Y$  auch ein Element von  $X$  ist. Man schreibt dafür  $Y \subset X$  oder  $X \supset Y$ .

*Beispiel 2.1.2.2.* Die leere Menge Teilmenge jeder Menge, in Formeln  $\emptyset \subset X$ .  $\{x\} \subset X$  ist gleichbedeutend zu  $x \in X$ . Es gilt  $\emptyset \subset \{2, 1\} \subset \mathbb{Z} \subset \mathbb{Q}$ .

**2.1.2.3 (Elemente und Teilmengen).** Es ist im Kontext der Mengenlehre wichtig, bei einer Menge  $X$  sorgfältig zu unterscheiden zwischen ihren Elementen und ihren Teilmengen. Gegeben ein Element  $x \in X$  ist für uns das Element  $x \in X$  etwas anderes als die Teilmenge  $\{x\} \subset X$ , die nur aus dem einzigen Element  $x$  besteht. Gegeben eine Menge  $X$  mit einer Teilmenge  $Y \subset X$  sage ich auch,  $X$  **umfaßt**  $Y$ . Gegeben ein Element  $x \in X$  sage ich,  $x$  **gehört zu**  $X$ . Andere Sprechweisen möchte ich ungern auf eine so präzise Bedeutung festlegen. Gegeben eine Teilmenge  $Y \subset X$  kann man sagen, „ $Y$  sei enthalten in  $X$ “ oder „ $Y$  liege in  $X$ “, und gegeben ein Element  $x \in X$  kann man auch sagen, „ $x$  sei enthalten in  $X$ “ oder „ $x$  liege in  $X$ “. Was genau gemeint ist, gilt es dann aus dem Kontext zu erschließen.

**2.1.2.4 (Diskussion der Notation).** Gegeben eine Menge  $X$  verwenden wir die Schreibweise  $Y \subsetneq X$  als Abkürzung für ( $Y \subset X$  und  $Y \neq X$ ). Eine von der ganzen Menge verschiedene Teilmenge  $Y$  einer Menge  $X$  nennen wir auch eine **echte Teilmenge von**  $X$ . Bei diesen Notationen folgen wir Cantor und Bourbaki, die sehr viel später festgelegte internationalen Norm ISO 31-11 weicht jedoch davon ab. In der folgenden Tabelle stellen wir diese beiden Konventionen einander gegenüber.

| Cantor und Bourbaki | Norm ISO 31-11 | Bedeutung               |
|---------------------|----------------|-------------------------|
| $\subset$           | $\subseteq$    | ist Teilmenge von       |
| $\subsetneq$        | $\subset$      | ist echte Teilmenge von |

Ich ziehe die Konvention von Cantor und Bourbaki vor, weil ich sie gewohnt bin und weil man sehr oft Teilmengen zu betrachten hat und nur vergleichsweise selten echte Teilmengen. Ich muß jedoch zugeben, daß die in diesem Text gewählte Notation  $\subset, \subsetneq$  mit den üblichen Notationen  $\leq, <$  für Ungleichungen weniger gut zusammenpaßt als die Konvention nach ISO 31-11.

**2.1.2.5.** Oft bildet man neue Mengen als Teilmengen bestehender Mengen. Gebräuchlich ist dazu eine Notation, bei der man zwischen den Mengenklammern hinter einem senkrechten Strich dazuschreibt, welche zusätzliche Eigenschaft die

Elemente einer Teilmenge haben sollte, so daß man Teilmengen  $Y$  einer Menge  $X$  angeben kann in der Form

$$Y = \{x \in X \mid x \text{ hat eine zusätzlich noch gewisse Eigenschaft}\}$$

Zum Beispiel gilt  $\mathbb{N} = \{a \in \mathbb{Z} \mid a \geq 0\}$ , lies „die Menge der natürlichen Zahlen ist die Teilmenge der Menge der ganzen Zahlen bestehend aus allen ganzen Zahlen, die  $\geq 0$  sind“, und  $\{0, 1\} = \{a \in \mathbb{N} \mid a^2 = a\}$ .

**Definition 2.1.2.6.** Es ist auch erlaubt, die „Menge aller Teilmengen“ einer gegebenen Menge  $X$  zu bilden. Sie heißt die **Potenzmenge von  $X$**  und wird  $\mathcal{P}(X)$  oder  $\text{Pot}(X)$  notiert.

*Beispiel 2.1.2.7.* Die Potenzmenge  $\mathcal{P}(\{1, 2, 3\})$  kann man als die Menge aller möglichen Ausgänge einer Versuchsanordnung interpretieren, bei der man dreimal eine Münze wirft. Dazu mag man etwa jedem Ausgang die Menge der Wurfnummern zuordnet, bei denen Wappen herauskam. So würde etwa dem Ausgang WZW die Teilmenge  $\{1, 3\}$  zugeordnet.

**2.1.2.8 (Kardinalität der Potenzmenge).** Ist  $X$  eine endliche Menge, so ist auch ihre Potenzmenge endlich und es gilt die Formel  $|\mathcal{P}(X)| = 2^{|X|}$ . Für die drei-elementige Menge  $X = \{1, 2, 3\}$  besteht ihre Potenzmenge  $\mathcal{P}(X)$  zum Beispiel aus  $8 = 2^3$  Elementen und wir haben genauer

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

Die Teilmenge  $\{1\} \subset \{1, 2, 3\}$ , die nur aus dem Element 1 besteht, ist also ein Element der Potenzmenge  $\{1\} \in \mathcal{P}(\{1, 2, 3\})$ . Das Element 1 ist dahingegen kein Element der Potenzmenge, sondern ein Element der ursprünglichen Menge  $1 \in \{1, 2, 3\}$ .

**Satz 2.1.2.9 (Bedeutung der Binomialkoeffizienten).** Gegeben natürliche Zahlen  $n, k \in \mathbb{N}$  gibt der Binomialkoeffizient  $\binom{n}{k}$  die Zahl der  $k$ -elementigen Teilmengen einer  $n$ -elementigen Menge an. In Formeln ausgedrückt haben wir unter der Annahme  $|X| = n$  also

$$|\{Y \subset X \mid |Y| = k\}| = \binom{n}{k}$$

*Beweis.* Vollständige Induktion über  $n$ . Für  $n = 0$  gilt die Aussage, denn eine nullelementige Menge hat genau eine  $k$ -elementige Teilmenge falls  $k = 0$  und keine  $k$ -elementige Teilmenge falls  $k \geq 1$ . Nehmen wir nun an, die Aussage sei für ein  $n$  schon bewiesen. Eine  $(n + 1)$ -elementige Menge  $X$  schreiben wir als  $X = M \cup \{x\}$  mit dem gleich in 2.1.3.1 formal eingeführten Vereinigungszeichen  $\cup$ , wo  $M$  eine  $n$ -elementige Menge ist und  $x \notin M$ . Ist  $k = 0$ , so gibt es genau

eine  $k$ -elementige Teilmenge von  $M \cup \{x\}$ , nämlich die leere Menge. Ist  $k \geq 1$ , so gibt es in  $M \cup \{x\}$  nach Induktionsannahme genau  $\binom{n}{k}$   $k$ -elementige Teilmengen, die  $x$  nicht enthalten. Die  $k$ -elementigen Teilmengen dahingegen, die  $x$  enthalten, ergeben sich durch Hinzunehmen von  $x$  aus den  $(k-1)$ -elementigen Teilmengen von  $M$ , von denen es gerade  $\binom{n}{k-1}$  gibt. Insgesamt hat  $M \cup \{x\}$  damit also genau  $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$  Teilmengen mit genau  $k$  Elementen.  $\square$

2.1.2.10. Wieder scheint mir dieser Beweis in der für vollständige Induktion typischen Weise undurchsichtig. Ich ziehe deshalb den in 1.1.1.19 gegebenen weniger formellen Beweis vor. Man kann auch diesen Beweis formalisieren und verstehen als Spezialfall der sogenannten „Bahnformel“, vergleiche 4.5.2.3.

2.1.2.11 (**Variante zum Beweis der binomischen Formel**). Wir geben nun die versprochene präzise Formulierung unseres ersten Beweises der binomischen Formel 1.1.1.23. Wir rechnen dazu

$$(a+b)^n = \sum_{Y \subset \{1, 2, \dots, n\}} a^{|Y|} b^{n-|Y|}$$

Die rechte Seite soll hier in Verallgemeinerung der in 1.1.1.8 eingeführten Notation bedeuten, daß wir für jede Teilmenge  $Y$  von  $\{1, 2, \dots, n\}$  den angegebenen Ausdruck  $a^{|Y|} b^{n-|Y|}$  nehmen und alle diese Ausdrücke aufsummieren. Dann fassen wir gleiche Summanden zusammen und erhalten mit 2.1.2.9 die binomische Formel.

### Übungen

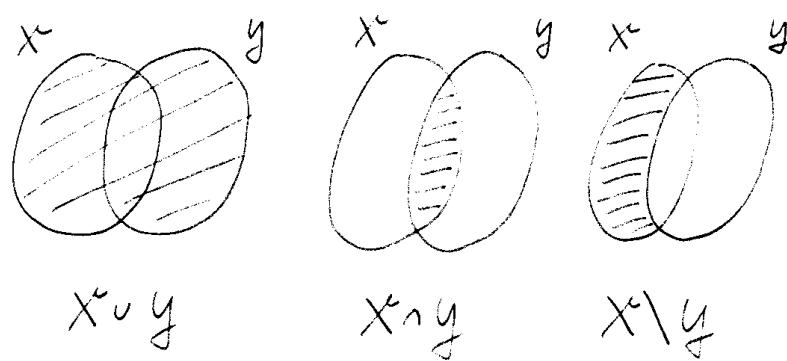
*Übung 2.1.2.12.* Es gilt  $\sum_k \binom{n}{k} = 2^n$ .

*Übung 2.1.2.13.* Man zeige  $(a+b+c)^n = \sum_{i+j+k=n} \frac{n!}{i!j!k!} a^i b^j c^k$ .

## 2.1.3 Mengenoperationen

**Definition 2.1.3.1.** Wir erinnern, daß wir := als Abkürzung für „ist definiert als“ verwenden und daß „oder“ in der Mathematik stets das „nichtausschließende oder“ meint. Gegeben zwei Mengen  $X, Y$  können wir unter anderem auf folgende Weisen neue Mengen bilden:

1. Die **Vereinigung**  $X \cup Y := \{z \mid z \in X \text{ oder } z \in Y\}$ , zum Beispiel ist  $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$ ;
2. Den **Schnitt** oder auch **Durchschnitt**  $X \cap Y := \{z \mid z \in X \text{ und } z \in Y\}$ , zum Beispiel ist  $\{1, 2\} \cap \{2, 3\} = \{2\}$ ;



Van-de-Ven-Diagramme für Vereinigung, Schnitt und Differenz

3. Die **Differenz**  $X \setminus Y := \{z \in X \mid z \notin Y\}$ , zum Beispiel haben wir  $\{1, 2\} \setminus \{2, 3\} = \{1\}$ . Man schreibt statt  $X \setminus Y$  auch  $X - Y$ . Ist  $Y$  eine Teilmenge von  $X$ , so heißt  $X \setminus Y$  das **Komplement** von  $Y$  in  $X$  oder ausführlicher die **Komplementmenge**;
4. Das **Produkt**  $X \times Y := \{(x, y) \mid x \in X, y \in Y\}$  oder ausführlicher **kartesische Produkt**. Es gilt also  $(x, y) = (x', y')$  genau dann, wenn gilt  $x = x'$  und  $y = y'$ . Zum Beispiel haben wir

$$\{1, 2\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$$

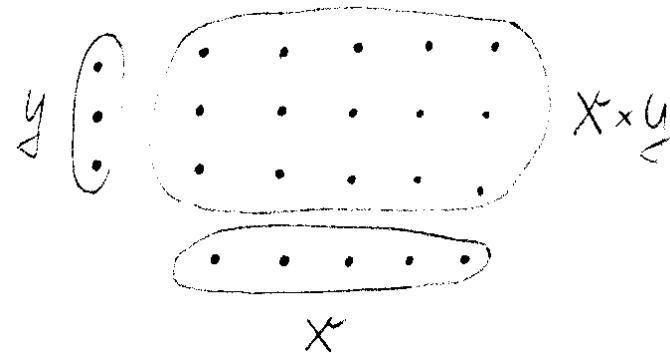
Oft benutzt man für das Produkt  $X \times X$  einer Menge  $X$  mit sich selbst die Abkürzung  $X^2 := X \times X$  und nennt das die Menge aller **angeordneten Paare** von Elementen von  $X$ .

2.1.3.2. Eine gute Anschauung für die ersten drei Operationen liefern die sogenannten **van-de-Ven-Diagramme**, wie sie die nebenstehenden Bilder zeigen. Sie sind allerdings nicht zu genau zu hinterfragen, denn ob die Punkte auf einem Blatt Papier im Sinne von Cantor „bestimmte wohlunterschiedene Objekte unserer Anschauung“ sind, scheint mir nicht ohne weiteres so klar. Wenn man jedoch jedes der schraffierten Gebiete im Bild als die Menge aller darin liegenden Kreuzungspunkte auf einem dazugedachten Millimeterpapier auffaßt und keine dieser Kreuzungspunkte auf den Begrenzungslinien liegen, so können sie wohl schon als eine Menge im Cantor'schen Sinne angesehen werden.

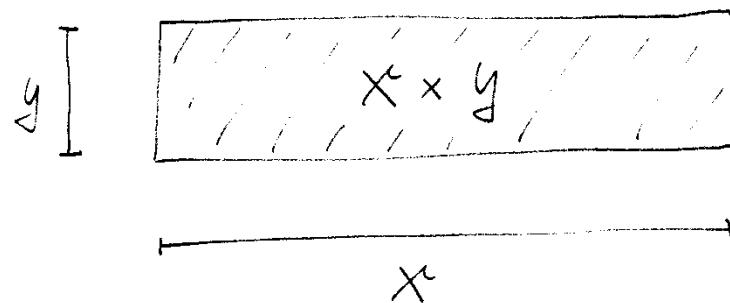
2.1.3.3. Zwei Teilmengen einer gegebenen Menge, die kein gemeinsames Element haben, heißen **disjunkt**. Äquivalent dazu ist die Bedingung, daß ihr Schnitt die leere Menge ist.

2.1.3.4 (**Mehrdeutigkeiten mit dem Komma als Trenner**). Die Verwendung des Kommas als Trenner ist hier problematisch, da  $(1, 2)$  nun zweierlei bedeuten kann: Zum einen ein Element des kartesischen Produkts  $\mathbb{N} \times \mathbb{N}$ , zum anderen aber auch den eingeklammerten Dezimalbruch  $1,2$ . Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen. In diesem Text werden Dezimalbrüche nur selten vorkommen. In deutschen Schulbüchern verwendet man für angeordnete Paare meist die abweichende Notation  $(x|y)$ , um auch Paare von Dezimalbrüchen unmissverständlich notieren zu können.

2.1.3.5 (**Diskussion der Terminologie**). Die Bezeichnung als „Schnitt“ kommt wohl her von der Vorstellung des Schnitts zweier Geraden, wenn man sie als Teilmengen der Ebene denkt und diese hinwiederum als ein Blatt Papier, das man längs der einen Gerade entzweischneiden kann. Der Punkt, an dem die andere Gerade entzweigeschnitten wird, ist dann der Schnittpunkt und der Schnitt unserer beiden Geraden besteht genau aus diesem einen Punkt.



Anschauliche Darstellung des Produkts einer Menge mit fünf und einer Menge mit drei Elementen. Hier wird ein Paar  $(x, y)$  dargestellt durch einen Punkt, der über  $x$  und neben  $y$  liegt.



Dies Bild muß anders interpretiert werden als das Vorherige. Die Mengen  $X$  und  $Y$  sind nun zu verstehen als die Mengen der Punkte der vertikalen und horizontalen Geradensegmente und ein Punkt des Quadrats meint das Element  $(x, y) \in X \times Y$ , das in derselben Höhe wie  $y \in Y$  senkrecht über  $x \in X$  liegt.

**2.1.3.6 (Mengenlehre und das Bilden von Begriffen).** Wir werden in unserer naiven Mengenlehre die ersten drei Operationen „Vereinigung“, „Schnitt“ und „Differenz“ aus 2.1.3.1 nur auf Teilmengen einer gemeinsamen Obermenge anwenden, die uns in der einen oder anderen Weise bereits zur Verfügung steht. Die Potenzmenge und das kartesische Produkt dahingegen benutzen wir, um darüber hinaus neue Mengen zu erschaffen. Diese Konstruktionen erlauben es, im Rahmen der Mengenlehre so etwas wie Abstraktionen zu bilden: Wenn wir uns etwa die Menge  $T$  aller an mindestens einem Tag der Weltgeschichte lebenden oder gelebt habenden Tiere als eine Menge im Cantor'schen Sinne denken, so würden wir Konzepte wie „männlich“ oder „Hund“ oder „Fleischfresser“ formal als Teilmengen dieser Menge alias als Elemente von  $\mathcal{P}(T)$  formalisieren. Das Konzept „ist Kind von“ würde dahingegen formalisiert als eine Teilmenge  $K \subset T \times T$  des kartesischen Produkts unserer Menge  $T$  mit sich selbst alias als ein Element  $K \in \mathcal{P}(T \times T)$ , nämlich als die Teilmenge

$$K := \{(x, y) \in T \times T \mid x \text{ ist Kind von } y\}$$

**2.1.3.7.** Für das Rechnen mit Mengen überlegt man sich die folgenden Regeln, die ich gleich mit ihren üblichen Bezeichnungen angebe:

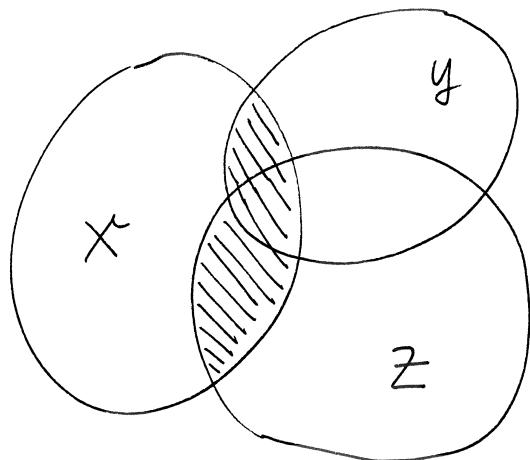
|                                       |   |
|---------------------------------------|---|
| <b>Assoziativgesetze:</b>             | $X \cap (Y \cap Z) = (X \cap Y) \cap Z$                         |
|                                       | $X \cup (Y \cup Z) = (X \cup Y) \cup Z$                         |
| <b>Distributivgesetze:</b>            | $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$                |
|                                       | $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$                |
| <b>de Morgan'sche Regeln:</b>         | $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$ |
|                                       | $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$ |
| <b>Komplement der Differenzmenge:</b> | $X \setminus (X \setminus Y) = X \cap Y$                        |

Eine gute Anschauung für diese Regeln liefern die van-de-Ven-Diagramme, wie die nebenstehenden Bilder zeigen. Das liegt daran, daß alle acht möglichen Lagen in Bezug auf unsere drei Mengen in diesen Diagrammen als Flächen zu sehen sind.

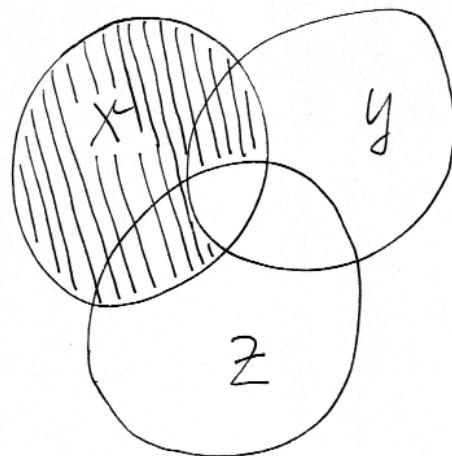
**2.1.3.8.** Ich zeige beispielhaft die Regel  $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ . Es reicht, statt der Gleichheit die beiden Inklusionen  $\subset$  und  $\supset$  zu zeigen.

Ich beginne mit  $\subset$ . Sicher gilt  $(Y \cap Z) \subset Y$ , also auch  $X \cup (Y \cap Z) \subset X \cup Y$ . Ebenso zeigt man  $X \cup (Y \cap Z) \subset X \cup Z$  und damit folgt schon mal  $\subset$ .

Bleibt noch  $\supset$  zu zeigen. Das will mir nur durch Betrachtung von Elementen gelingen. Gegeben  $a \in (X \cup Y) \cap (X \cup Z)$  gilt entweder  $a \in X$  oder  $a \notin X$ . Falls  $a \in X$  haben wir eh  $a \in X \cup (Y \cap Z)$ . Falls  $a \notin X$  folgt aus  $a \in (X \cup Y) \cap (X \cup Z)$



$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

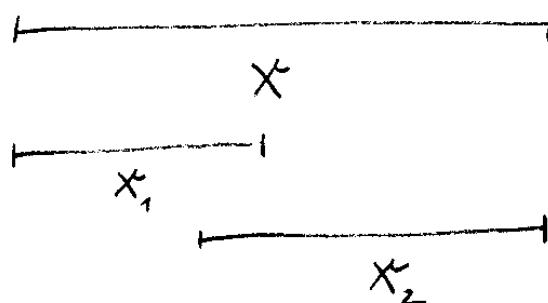
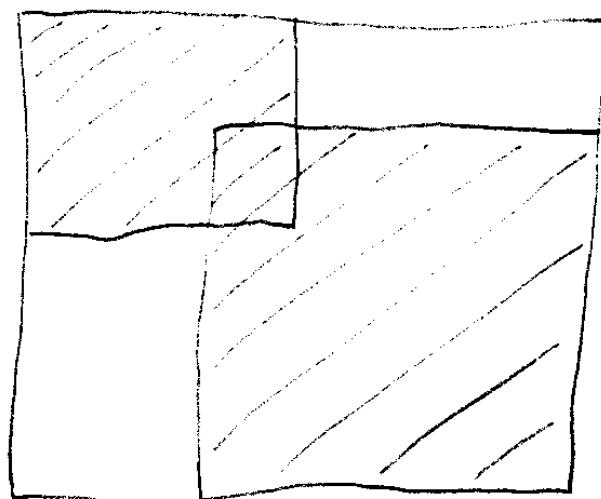
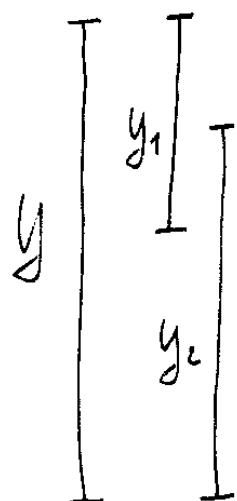


$$X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$$

erst  $a \in (X \cup Y)$  und dann  $a \in Y$  und weiter erst  $a \in (X \cup Z)$  und dann  $a \in Z$ , also  $a \in Y \cap Z \subset X \cup (Y \cap Z)$ . Wir haben somit gezeigt, daß jedes Element  $a$  von  $(X \cup Y) \cap (X \cup Z)$  auch zu  $X \cup (Y \cap Z)$  gehört. Damit folgt die behauptete Inklusion  $\supset$ .

*Ergänzung 2.1.3.9 (Das Russell'sche Paradoxon).* Ich will nicht verschweigen, daß der in diesem Abschnitt dargestellte naive Zugang zur Mengenlehre durchaus begriffliche Schwierigkeiten mit sich bringt: Zum Beispiel darf die Gesamtheit  $\mathcal{M}$  aller Mengen nicht als Menge angesehen werden, da wir sonst die „Menge aller Mengen, die sich nicht selbst als Element enthalten“, gegeben durch die formelle Beschreibung  $\mathcal{N} = \{A \in \mathcal{M} \mid A \notin A\}$ , bilden könnten. Für diese Menge kann aber weder  $\mathcal{N} \in \mathcal{N}$  noch  $\mathcal{N} \notin \mathcal{N}$  gelten. Diese Art von Schwierigkeiten kann erst ein formalerer Zugang klären und auflösen, bei dem man unsere naiven Vorstellungen durch Ketten von Zeichen aus einem wohlbestimmten endlichen Alphabet ersetzt und unsere Vorstellung von Wahrheit durch die Verifizierbarkeit mittels rein algebraischer „erlaubter Manipulationen“ solcher Zeichenketten, die in „Axiomen“ festgelegt werden. Diese Verifikationen kann man dann durchaus auch einer Rechenmaschine überlassen, so daß wirklich auf „objektivem“ Wege entschieden werden kann, ob ein „Beweis“ für die „Richtigkeit“ einer unserer Zeichenketten in einem vorgegebenen axiomatischen Rahmen stichhaltig ist. Allerdings kann in derartigen Systemen von einer Zeichenkette algorithmisch nur entschieden werden, ob sie eine „sinnvolle Aussage“ ist, nicht aber, ob sie „bewiesen“ werden kann. Noch viel stärker zeigt der Unvollständigkeitssatz von Gödel, daß es in einem derartigen axiomatischen Rahmen, sobald er reichhaltig genug ist für eine Beschreibung des Rechnens mit natürlichen Zahlen, stets sinnvolle Aussagen gibt derart, daß entweder sowohl die Aussage als auch ihre Verneinung oder aber weder die Aussage noch ihre Verneinung bewiesen werden können. Mit diesen und ähnlichen Fragestellungen beschäftigt sich die Logik.

*Vorschau 2.1.3.10 (Weitere Konstruktionen der Mengenlehre).* Um mich nicht dem Vorwurf auszusetzen, während des Spiels die Spielregeln ändern zu wollen, sei bereits hier erwähnt, was noch hinzukommen soll. Die einzigen grundlegenden Konstruktionen, die noch fehlen, sind das Bilden der „disjunkten Vereinigung“ und des „kartesischen Produkts“ zu einer „beliebigen Mengenfamilie“ in 4.7.7.17 und 4.7.7.7. In ?? besprechen wir weiter Schnitt und Vereinigung einer „beliebigen Familie von Teilmengen einer gegebenen Menge“. In 3.1.9 werden einige weniger offensichtliche Argumentationen im Zusammenhang mit dem sogenannten „Zorn'schen Lemma“ erläutert, die meines Erachtens bereits an den Rand dessen gehen, was man in unserem informellen Rahmen der naiven Mengenlehre als Argumentation noch vertreten kann. In 3.4.1 wird die Konstruktion der natürlichen Zahlen im Rahmen der Mengenlehre diskutiert, insbesondere geben wir erst dort eine formale Definition des Begriffs einer endlichen Menge. Sicher ist es in



Aus  $X = X_1 \cup X_2$  und  $Y = Y_1 \cup Y_2$  folgt noch lange nicht  
 $X \times Y = (X_1 \times Y_1) \cup (X_2 \times Y_2)$

gewisser Weise unbefriedigend, das Fundament des Hauses der Mathematik erst fertigzustellen, wenn bereits erste Stockwerke stehen und bewohnt sind. Andererseits will ich aber auch vermeiden, daß Sie mir auf einem gewaltigen Fundament, das die ganze Mathematik tragen kann, im ersten Winter(semester) jämmerlich erfrieren.

**2.1.3.11 (Der Sinn von Genauigkeit und sorgfältiger Sprache).** Ich könnte mir gut vorstellen, daß verschiedene meiner Leser denken, diese ganze Pedanterie sei doch eigentlich überflüssig und jetzt sollten wir doch einfach mal fröhlich losrechnen wie das in der Schule ja auch sehr gut ging. Ich will hier erklären, warum Pedanterie in diesem Zusammenhang wichtig ist. Viele von Ihnen werden wissen, wie man mit einem einfachen Blatt Papier zum Mond kommt: 42-mal Falten und draufsteigen, das war's schon. So ähnlich ist es in der Mathematik: Etwas völlig Banales wie die naive Mengenlehre wird in den etwa dreißig Vorlesungsdoppelstunden des Wintersemesters jedes Mal von neuem gefaltet und wenn Sie dann am Ende des Wintersemesters zurückblicken, kann Ihnen schon leicht schwindlig werden. Das funktioniert mit wirklichem Papier nur eingeschränkt, aber wenn man sehr festes und glattes „Gedankenpapier“ nimmt, und solches Gedankenpapier ist eben gerade die Mengenlehre, dann klappt es verblüffend gut. Man muß dazu aber mit der Herstellung dieses Gedankenpapiers ebenso wie beim Falten sorgfältig sein bis zur Pedanterie, denn auch die kleinste Ungeschicklichkeit vervielfacht sich bei diesem Vorgehen mit derselben Schnelligkeit wie die gedankliche Höhe und bringt, eh man sich's versieht, alles zum Einsturz.

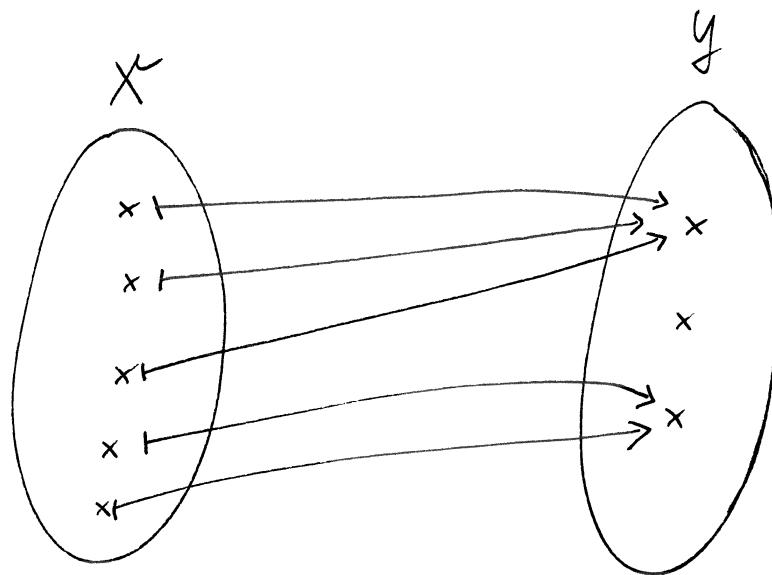
### Übungen

*Übung 2.1.3.12.* Sind  $X$  und  $Y$  endliche Mengen, so gilt für die Kardinalitäten  $|X \times Y| = |X| \cdot |Y|$  und  $|X \cup Y| = |X| + |Y| - |X \cap Y|$ .

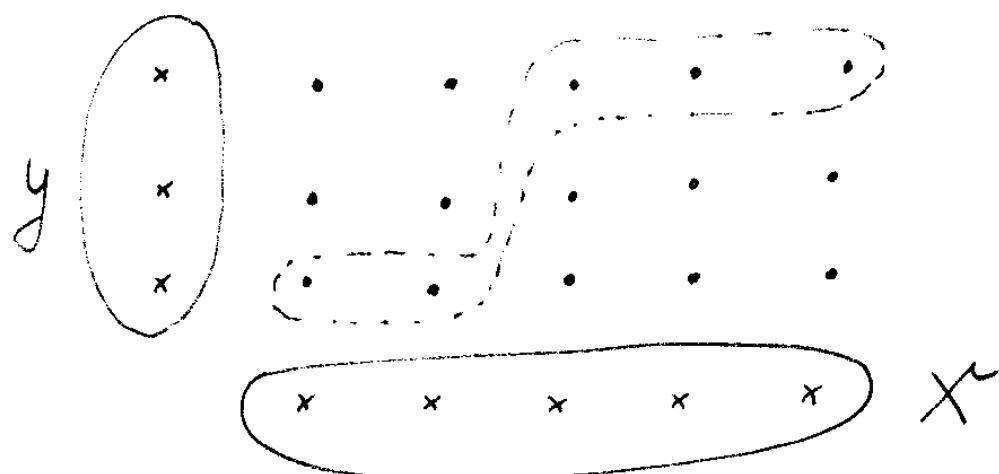
## 2.1.4 Abbildungen

**Definition 2.1.4.1.** Seien  $X, Y$  Mengen. Eine **Abbildung**  $f : X \rightarrow Y$  ist eine Zuordnung, die jedem Element  $x \in X$  genau ein Element  $f(x) \in Y$  zuordnet, das **Bild** von  $x$  unter  $f$ , auch genannt der **Wert** von  $f$  an der Stelle  $x$ . Man spricht dann auch vom **Auswerten** der Funktion  $f$  an der Stelle  $x$  oder vom **Einsetzen** von  $x$  in  $f$  und schreibt manchmal abkürzend  $f(x) = fx$ .

**2.1.4.2.** Wem das zu vage ist, der mag die alternative Definition vorziehen, nach der eine **Abbildung**  $f : X \rightarrow Y$  eine Teilmenge  $f \subset X \times Y$  ist derart, daß es für jedes  $x \in X$  genau ein  $y \in Y$  gibt mit  $(x, y) \in f$ . Dies eindeutig bestimmte  $y$  schreiben wir dann  $f(x)$  und sind auf einem etwas formaleren Weg wieder an



Eine Abbildung einer Menge mit fünf in eine mit drei Elementen



Der Graph der oben angegebenen Abbildung, wobei das  $X$  oben mit dem  $X$  hier identifiziert wurde durch „Umkippen nach Rechts“

demselben Punkt angelangt. In unseren Konventionen nennen wir besagte Teilmenge den **Graphen von  $f$**  und notieren sie mit dem Symbol  $\Gamma$  (sprich: Gamma), einem großen griechischen G, und schreiben

$$\Gamma(f) := \{(x, f(x)) \mid x \in X\} \subset X \times Y$$

**Definition 2.1.4.3.** Ist  $f : X \rightarrow Y$  eine Abbildung, so nennen wir  $X$  ihren **Definitionsreich** und  $Y$  ihren **Wertebereich**. Zwei Abbildungen nennen wir gleich, wenn sie denselben Definitionsbereich  $X$ , denselben Wertebereich  $Y$  und dieselbe Abbildungsvorschrift  $f \subset X \times Y$  haben.

2.1.4.4 (**Die Notationen → und ↪**). Wir notieren Abbildungen oft in der Form

$$\begin{array}{rcl} f : & X & \rightarrow & Y \\ & x & \mapsto & f(x) \end{array}$$

und in verschiedenen Verkürzungen dieser Notation. Zum Beispiel sprechen wir von „einer Abbildung  $\mathbb{N} \rightarrow \mathbb{N}$  von der Menge der natürlichen Zahlen in sich selber“ oder „der Abbildung  $n \mapsto n^3$  von der Menge der natürlichen Zahlen in sich selber“. Wir benutzen unsere zwei Arten von Pfeilen  $\rightarrow$  und  $\mapsto$  auch im allgemeinen in derselben Weise.

*Beispiel 2.1.4.5.* Für jede Menge  $X$  haben wir die **identische Abbildung** oder **Identität**

$$\begin{array}{rcl} \text{id} = \text{id}_X : & X & \rightarrow & X \\ & x & \mapsto & x \end{array}$$

Ein konkreteres Beispiel für eine Abbildung ist das Quadrieren

$$\begin{array}{rcl} q : & \mathbb{Z} & \rightarrow & \mathbb{Z} \\ & n & \mapsto & n^2 \end{array}$$

*Beispiel 2.1.4.6.* Gegeben zwei Mengen  $X, Y$  erklärt man die **Projektionsabbildungen** oder **Projektionen**  $\text{pr}_X : X \times Y \rightarrow X$  beziehungsweise  $\text{pr}_Y : X \times Y \rightarrow Y$  durch die Vorschrift  $(x, y) \mapsto x$  beziehungsweise  $(x, y) \mapsto y$ . In manchen Zusammenhängen notiert man sie auch abweichend  $\text{pr}_1$  und  $\text{pr}_2$  für die „Projektion auf die erste beziehungsweise zweite Komponente“.

**Definition 2.1.4.7.** Sei  $f : X \rightarrow Y$  eine Abbildung.

1. Gegeben eine Teilmenge  $A \subset X$  erklären wir das **Bild von  $A$  unter  $f$** , eine Teilmenge  $f(A) \subset Y$ , durch

$$f(A) := \{y \in Y \mid \text{Es gibt } x \in A \text{ mit } f(x) = y\}$$

2. Gegeben eine Teilmenge  $B \subset Y$  erklären wir das **Urbild von  $B$  unter  $f$** , eine Teilmenge von  $f^{-1}(B) \subset X$ , durch

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}$$

2.1.4.8. Das Bild von ganz  $X$  nennen wir das **Bild von  $f$**  und notieren es  $\text{im}(f) := f(X)$ . Das Kürzel  $\text{im}$  steht für französisch und englisch **image**.

*Beispiel 2.1.4.9.* Für unsere Abbildung  $q : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $n \mapsto n^2$  des Quadrierens von eben könnten wir die Menge aller Quadratzahlen schreiben als

$$q(\mathbb{Z}) = \{a^2 \mid a \in \mathbb{Z}\}$$

Ebenso wäre  $\{2a \mid a \in \mathbb{N}\}$  eine mögliche formelmäßige Darstellung der Menge aller geraden natürlichen Zahlen, und  $\{ab \mid a, b \in \mathbb{N}, a \geq 2, b \geq 2\}$  wäre eine formelmäßige Darstellung der Menge aller natürlichen Zahlen, die nicht prim und auch nicht Null oder Eins sind.

2.1.4.10. Eine Abbildung, deren Bild aus höchstens einem Element besteht, nennen wir eine **konstante Abbildung**. Eine Abbildung, deren Bild aus genau einem Element besteht, nennen wir eine **einwertige Abbildung**. Eine einwertige Abbildung ist also eine konstante Abbildung mit nichtleerem Definitionsbereich.

2.1.4.11 (**Konstanten und konstante Abbildungen**). Gegeben ein festes  $c \in Y$  schreiben wir oft auch kurz  $c$  für die konstante Abbildung  $X \rightarrow Y$  gegeben durch  $x \mapsto c$  für alle  $x \in X$ . Damit verbunden ist die Hoffnung, daß aus dem Kontext klar wird, ob im Einzelfall die Abbildung  $c : X \rightarrow Y$  oder das Element  $c \in Y$  gemeint sind.

2.1.4.12. Gegeben eine Abbildung  $f : X \rightarrow Y$  ist formal  $f^{-1}$  eine Abbildung  $f^{-1} : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$  in der Gegenrichtung auf den Potenzmengen. Besteht  $B$  nur aus einem Element  $x$ , so schreiben wir auch  $f^{-1}(x)$  statt  $f^{-1}(\{x\})$  und nennen diese Menge die **Faser von  $f$  über  $x$**  oder **bei  $x$** . Das Quadrieren  $q$  aus 2.1.4.9 hat etwa die Faser  $q^{-1}(1) = \{1, -1\}$  bei 1 und die Faser  $q^{-1}(-1) = \emptyset$  bei -1.

2.1.4.13 (**Diskussion der Notation**). Die Notation  $f^{-1}(B)$  für das Urbild einer Menge unter einer Abbildung führt leicht zu Verwirrung, da man  $a^{-1}$  aus der Schule als alternative Notation für den Bruch  $a^{-1} = 1/a$  gewohnt ist. Diese beiden Notationen sind nur entfernt verwandt und werden beide in der Mathematik durchgehend verwendet. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen.

## 2.1.5 Verknüpfung von Abbildungen

**Definition 2.1.5.1.** Sind drei Mengen  $X, Y, Z$  gegeben und dazwischen Abbildungen  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$ , so definieren wir die **Verknüpfung** unserer

Abbildungen  $f$  und  $g$ , eine Abbildung  $g \circ f : X \rightarrow Z$ , durch die Vorschrift

$$\begin{array}{rcl} g \circ f : & X & \rightarrow Z \\ & x & \mapsto g(f(x)) \end{array}$$

**2.1.5.2 (Diskussion der Notation).** Die Notation  $g \circ f$ , sprich „ $g$  nach  $f$ “, für „erst  $f$ , dann  $g$ “ ist gewöhnungsbedürftig, erklärt sich aber durch die offensichtliche Formel  $(g \circ f)(x) = g(f(x))$ . Ich sage,  $g \circ f$  entstehe aus  $g$  durch **Vorschalten von  $f$**  und aus  $f$  durch **Nachschalten von  $g$** . Oft kürzt man auch  $g \circ f$  mit  $gf$  ab. Mit dieser Abkürzung muß man jedoch sorgsam umgehen, da im Fall von zwei Abbildungen  $f, g$  von derselben Menge in einen Zahlbereich, etwa  $f, g : X \rightarrow \mathbb{Q}$ , der Ausdruck  $fg$  vielmehr für die Abbildung  $x \mapsto f(x)g(x)$  reserviert ist, das sogenannte „punktweise Produkt“ unserer beiden Funktionen.

*Beispiel 2.1.5.3.* Betrachten wir zusätzlich zum Quadrieren  $q : \mathbb{Z} \rightarrow \mathbb{Z}$  die Abbildung  $t : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $x \mapsto x + 1$ , so gilt  $(q \circ t)(x) = (x + 1)^2$  aber  $(t \circ q)(x) = x^2 + 1$ .

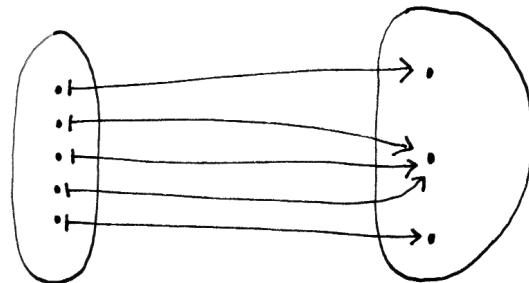
**Definition 2.1.5.4.** Sei  $f : X \rightarrow Y$  eine Abbildung.

1.  $f$  heißt **injektiv** oder eine **Injektion**, wenn aus  $x \neq x'$  folgt  $f(x) \neq f(x')$ . Gleichbedeutend ist die Forderung, daß es für jedes  $y \in Y$  höchstens ein  $x \in X$  gibt mit  $f(x) = y$ . Injektionen schreibt man oft  $\hookrightarrow$ .
2.  $f$  heißt **surjektiv** oder eine **Surjektion**, wenn es für jedes  $y \in Y$  mindestens ein  $x \in X$  gibt mit  $f(x) = y$ . Surjektionen schreibt man manchmal  $\rightarrow\!\!\rightarrow$ .
3.  $f$  heißt **bijektiv** oder eine **Bijektion**, wenn  $f$  injektiv und surjektiv ist. Gleichbedeutend ist die Forderung, daß es für jedes  $y \in Y$  genau ein  $x \in X$  gibt mit  $f(x) = y$ . Bijektionen schreibt man oft  $\tilde{\rightarrow}$ .

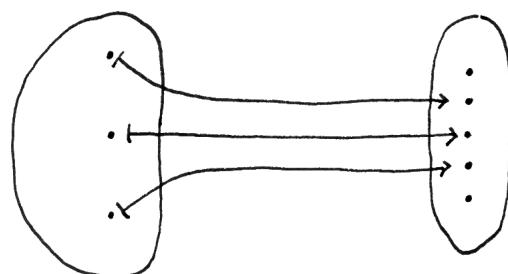
**2.1.5.5.** Ist  $X \subset Y$  eine Teilmenge, so ist die **Einbettung** oder **Inklusion**  $i : X \rightarrow Y$ ,  $x \mapsto x$  stets injektiv. Ist  $g : Y \rightarrow Z$  eine Abbildung und  $X \subset Y$  eine Teilmenge, so nennen wir die Verknüpfung  $g \circ i$  von  $g$  mit der Inklusion auch die **Einschränkung** von  $g$  auf  $X$  und notieren sie

$$g \circ i =: g|_X = g|_X : X \rightarrow Z$$

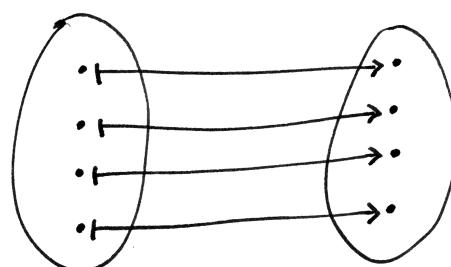
Oft bezeichnen wir eine Einschränkung aber auch einfach mit demselben Buchstaben  $g$  in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, welche Abbildung genau gemeint ist. Das ist nicht ganz unproblematisch: So ist etwa unsere Abbildung  $q : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $n \mapsto n^2$  nicht injektiv, ihre Restriktion zu einer Abbildung  $q : \mathbb{N} \rightarrow \mathbb{Z}$  ist aber durchaus injektiv.



Eine Surjektion



Eine Injektion



Eine Bijektion

**2.1.5.6 (Surjektion auf das Bild).** Ist  $f : X \rightarrow Y$  eine Abbildung, so ist die Abbildung  $f : X \rightarrow f(X)$ ,  $x \mapsto f(x)$  stets surjektiv. Der Leser möge entschuldigen, daß wir hier zwei verschiedene Abbildungen mit demselben Symbol  $f$  bezeichnet haben. Das wird noch öfter vorkommen. Überhaupt ignorieren wir, gegeben Mengen  $X, Y$  und eine Teilmenge  $Z \subset Y$ , im folgenden meist den Unterschied zwischen einer „Abbildung von  $X$  nach  $Y$ , deren Bild in  $Z$  enthalten ist“ und einer „Abbildung von  $X$  nach  $Z$ “.

**Beispiele 2.1.5.7.** Unsere Abbildung  $q : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $n \mapsto n^2$  ist weder injektiv noch surjektiv. Die Identität  $\text{id} : X \rightarrow X$  ist stets bijektiv. Sind  $X$  und  $Y$  endliche Mengen, so gibt es genau dann eine Bijektion von  $X$  nach  $Y$ , wenn  $X$  und  $Y$  dieselbe Kardinalität haben, in Formeln  $|X| = |Y|$ .

**Satz 2.1.5.8.** Seien  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  Abbildungen.

1. Ist  $g \circ f$  injektiv, so ist  $f$  injektiv;
2. Sind  $g$  und  $f$  injektiv, so auch  $g \circ f$ ;
3. Genau dann ist  $g$  injektiv, wenn für beliebige Abbildungen  $f_1, f_2 : X \rightarrow Y$  aus  $g \circ f_1 = g \circ f_2$  schon folgt  $f_1 = f_2$ .

*Beweis.* Übung. Besonders elegant ist es, zunächst die letzte Aussage zu zeigen, und dann die vorderen Aussagen ohne weitere Betrachtung von Elementen zu folgern.  $\square$

**2.1.5.9 (Universelle Eigenschaft von Injektionen).** Sei  $i : Y \hookrightarrow X$  eine injektive Abbildung und  $\varphi : Z \rightarrow X$  eine beliebige Abbildung. Genau dann gibt es eine Abbildung  $\tilde{\varphi} : Z \rightarrow Y$  mit  $i \circ \tilde{\varphi} = \varphi$ , wenn gilt  $\text{im}(\varphi) \subset \text{im}(i)$ . Nach dem Vorhergehenden ist diese Abbildung  $\tilde{\varphi}$  dann sogar eindeutig bestimmt.

**Satz 2.1.5.10.** Seien  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  Abbildungen.

1. Ist  $g \circ f$  surjektiv, so ist  $g$  surjektiv;
2. Sind  $g$  und  $f$  surjektiv, so auch  $g \circ f$ ;
3. Genau dann ist  $f$  surjektiv, wenn für beliebige Abbildungen  $g_1, g_2 : Y \rightarrow Z$  aus  $g_1 \circ f = g_2 \circ f$  schon folgt  $g_1 = g_2$ .

*Beweis.* Übung. Besonders elegant ist es, zunächst die letzte Aussage zu zeigen, und dann die vorderen Aussagen ohne weitere Betrachtung von Elementen zu folgern.  $\square$

2.1.5.11 (**Universelle Eigenschaft von Surjektionen**). Sei  $s : X \twoheadrightarrow Y$  eine surjektive Abbildung und  $\varphi : X \rightarrow Z$  eine beliebige Abbildung. Offensichtlich gibt es genau dann eine Abbildung  $\bar{\varphi} : Y \rightarrow Z$  mit  $\bar{\varphi} \circ s = \varphi$ , wenn  $\varphi$  auf den **Fasern** von  $s$  konstant ist. Nach dem Vorhergehenden ist diese Abbildung  $\bar{\varphi}$  dann sogar eindeutig bestimmt. Diese Erkenntnis ist insbesondere für die Algebra relevant.

2.1.5.12. Ist  $f : X \xrightarrow{\sim} Y$  eine bijektive Abbildung, so ist offensichtlich die Menge  $\{(f(x), x) \in Y \times X \mid x \in X\}$  im Sinne von 2.1.4.2 eine Abbildung oder, vielleicht klarer, der Graph einer Abbildung  $Y \rightarrow X$ . Diese Abbildung in die Gegenrichtung heißt die **Umkehrabbildung** oder **Umkehrfunktion** auch die **inverse Abbildung** zu  $f$  und wird mit  $f^{-1} : Y \rightarrow X$  bezeichnet. Offensichtlich ist mit  $f$  auch  $f^{-1}$  eine Bijektion.

2.1.5.13 (**Diskussion der Notation**). Mit dem vorhergehenden haben wir schon eine dritte mögliche Bedeutung für das Symbol  $f^{-1}$  kennengelernt. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen.

*Beispiel 2.1.5.14.* Die Umkehrabbildung unserer Bijektion  $t : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $x \mapsto x + 1$  ist die Abbildung  $t^{-1} : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $x \mapsto x - 1$ .

**Satz 2.1.5.15 (Bedeutung der Fakultät).** *Sind  $X$  und  $Y$  zwei Mengen mit je  $n$  Elementen, so gibt es genau  $n!$  bijektive Abbildungen  $f : X \xrightarrow{\sim} Y$ .*

*Beweis.* Sei  $X = \{x_1, \dots, x_n\}$ . Wir haben  $n$  Möglichkeiten, ein Bild für  $x_1$  auszusuchen, dann noch  $(n - 1)$  Möglichkeiten, ein Bild für  $x_2$  auszusuchen, und so weiter, bis schließlich nur noch 1 Element von  $Y$  als mögliches Bild von  $x_n$  in Frage kommt. Insgesamt gibt es also  $n(n - 1) \cdots 1 = n!$  Möglichkeiten für  $f$ . Da wir  $0! = 1$  vereinbart hatten, stimmt unser Satz auch für  $n = 0$ .  $\square$

## Übungen

*Übung 2.1.5.16.* Gegeben eine Bijektion  $f : X \rightarrow Y$  ist  $g = f^{-1}$  die einzige Abbildung  $g : Y \rightarrow X$  mit  $f \circ g = \text{id}_Y$ . Ebenso ist auch  $h = f^{-1}$  die einzige Abbildung  $h : Y \rightarrow X$  mit  $h \circ f = \text{id}_X$ .

*Ergänzende Übung 2.1.5.17.* Gegeben endliche Mengen  $X, Y$  gibt es genau  $|Y|^{|X|}$  Abbildungen von  $X$  nach  $Y$  und unter diesen Abbildungen sind genau  $|Y|(|Y| - 1)(|Y| - 2) \dots (|Y| - |X| + 1)$  Injektionen.

*Übung 2.1.5.18.* Sind Abbildungen  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  gegeben, so haben wir  $(g \circ f)(A) = g(f(A))$  für jede Teilmenge  $A \subset X$  und umgekehrt auch  $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$  für jede Teilmenge  $C \subset Z$ .

*Ergänzende Übung 2.1.5.19.* Sei  $X$  eine Menge mit  $n$  Elementen und seien natürliche Zahlen  $\alpha_1, \dots, \alpha_r \in \mathbb{N}$  gegeben mit  $n = \alpha_1 + \dots + \alpha_r$ . Man zeige: Es

gibt genau  $n! / (\alpha_1! \cdots \alpha_r!)$  Abbildungen  $f : X \rightarrow \{1, \dots, r\}$ , die jedes  $i$  genau  $\alpha_i$ -mal als Wert annehmen, in Formeln

$$\frac{n!}{\alpha_1! \cdots \alpha_r!} = \text{card}\{f \mid |f^{-1}(i)| = \alpha_i \text{ für } i = 1, \dots, r\}$$

*Ergänzung 2.1.5.20.* Manche Autoren bezeichnen die Zahlen aus der vorherigen Übung 2.1.5.19 als **Multinomialkoeffizienten** und verwenden die Notation

$$\binom{n}{\alpha_1; \dots; \alpha_r} := \frac{n!}{\alpha_1! \cdots \alpha_r!}$$

Mich überzeugt diese Notation nicht, da sie im Gegensatz zur Notation für Binomialkoeffizienten nichts kürzer macht.

*Ergänzende Übung 2.1.5.21.* Man zeige die Formel

$$(x_1 + \dots + x_r)^n = \sum_{\alpha_1 + \dots + \alpha_r = n} \frac{n!}{\alpha_1! \cdots \alpha_r!} x_1^{\alpha_1} \cdots x_r^{\alpha_r}$$

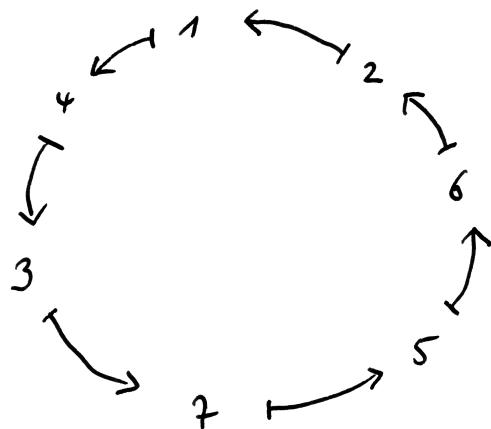
Hier ist zu verstehen, daß wir für alle  $\alpha_1, \dots, \alpha_r \in \mathbb{N}$  mit  $\alpha_1 + \dots + \alpha_r = n$  den angegebenen Ausdruck nehmen und alle diese Ausdrücke aufsummieren.

*Ergänzende Übung 2.1.5.22.* Eine **zyklische Anordnung** einer endlichen Menge  $M$  ist eine Abbildung  $z : M \rightarrow M$  derart, daß wir durch mehrmaliges Anwenden von  $z$  auf ein beliebiges Element  $x \in M$  jedes Element  $y \in M$  erhalten können. Man zeige, daß es auf einer  $n$ -elementigen Menge mit  $n \geq 1$  genau  $(n-1)!$  zyklische Anordnungen gibt. Die Terminologie „zyklische Anordnung“ ist etwas unglücklich, da unsere Struktur nun beim besten Willen keine Anordnung im Sinne von ?? ist. Andererseits ist aber das Angeben einer Anordnung auf einer endlichen Menge  $M$  schon auch etwas Ähnliches.

*Ergänzende Übung 2.1.5.23.* Sei  $X$  eine Menge mit  $n \geq 1$  Elementen und sei  $m$  eine natürliche Zahl. Man zeige, daß es genau  $\binom{n+m-1}{n-1}$  Abbildungen  $f : X \rightarrow \mathbb{N}$  gibt mit  $\sum_{x \in X} f(x) = m$ . Hinweis: Man denke sich  $X = \{1, 2, \dots, n\}$  und veranschauliche sich dann  $f$  als eine Folge auf  $f(1)$  Punkten gefolgt von einem Strich gefolgt von  $f(2)$  Punkten gefolgt von einem Strich und so weiter, insgesamt also eine Folge aus  $n+m-1$  Symbolen, davon  $m$  Punkten und  $n-1$  Strichen.

## 2.1.6 Ergänzungen zur Mengenlehre\*

2.1.6.1 (**Kommutativität kartesischer Produkte**). Ich insistiere darauf, daß gegeben Mengen  $X, Y$  die kartesischen Produkte  $X \times Y$  und  $Y \times X$  für uns verschiedene Mengen sind. Es gibt zwischen diesen kartesischen Produkten zwar die ausgezeichneten Bijektionen  $\tau_{X,Y} : X \times Y \xrightarrow{\sim} Y \times X$  mit  $(x, y) \mapsto (y, x)$  und  $\tau_{Y,X}$  ist stets die Umkehrabbildung zu  $\tau_{X,Y}$ , aber  $\tau_{X,X}$  muß keineswegs die Identität auf  $X^2$  sein, das gilt vielmehr nur für  $|X| \leq 1$ .



Versuch der graphischen Darstellung einer zyklischen Anordnung auf der Menge  $\{1, 2, \dots, 7\}$ . Die Pfeile  $\mapsto$  sollen jeweils den Effekt der Abbildung  $z$  veranschaulichen.

|        |   |   |   |   |   |   |
|--------|---|---|---|---|---|---|
| $x$    | 1 | 2 | 3 | 4 | 5 | 6 |
| $f(x)$ | 2 | 0 | 0 | 4 | 4 | 0 |

|    |             |
|----|-------------|
| 11 | 4444 5555   |
| .. | ..... ..... |

Eine Abbildung  $f : \{1, 2, \dots, n\} \rightarrow \mathbb{N}$  im Fall  $n = 6$  mit Wertesumme  $m = 10$  und die Veranschaulichung nach der Vorschrift aus Übung 2.1.5.23 als Folge bestehend aus  $m$  Punkten und  $n - 1$  Strichen.

*Vorschau 2.1.6.2.* In ?? zeigen wir den Satz von Schröder-Bernstein: Sind  $X$  und  $Y$  Mengen und gibt es sowohl eine Injektion  $f : X \hookrightarrow Y$  als auch eine Injektion  $g : Y \hookrightarrow X$ , so gibt es sogar eine Bijektion  $b : X \xrightarrow{\sim} Y$ .

**Definition 2.1.6.3.** Die Menge aller Abbildungen von  $X$  nach  $Y$  bezeichne ich mit

$$\text{Ens}(X, Y)$$

nach der französischen Übersetzung **ensemble** des deutschen Begriffs „Menge“.

**2.1.6.4 (Diskussion der Terminologie).** Üblicher ist statt unserem  $\text{Ens}(X, Y)$  die Notation  $Y^X$ . Noch gebräuchlicher ist in der deutschen Literatur die Bezeichnung  $\text{Abb}(X, Y)$  für die Menge aller Abbildungen von  $X$  nach  $Y$ . Ich will jedoch in 4.7.1.4 die „Kategorie aller Mengen“ wie Gabriel [Gab62] mit  $\text{Ens}$  bezeichnen und für je zwei Objekte  $X, Y$  einer Kategorie  $\mathcal{C}$  die Menge aller „Morphismen“ von  $X$  nach  $Y$  mit  $\mathcal{C}(X, Y)$ . Das erklärt die hier gewählte Bezeichnung für Mengen von Abbildungen.

**2.1.6.5 (Exponentialgesetz).** Gegeben drei Mengen  $X, Y, Z$  erhalten wir eine Bijektion

$$\text{Ens}(X \times Y, Z) \xrightarrow{\sim} \text{Ens}(X, \text{Ens}(Y, Z))$$

durch die Vorschrift  $f \mapsto f(x, \quad)$  mit der Notation  $f(x, \quad)$  für die Abbildung  $y \mapsto f(x, y)$ . Etwas vage formuliert ist also eine Abbildung  $X \times Y \rightarrow Z$  von einem kartesischen Produkt  $X \times Y$  in eine weitere Menge  $Z$  dasselbe wie eine Abbildung, die jedem  $x \in X$  eine Abbildung  $Y \rightarrow Z$  zuordnet, und umgekehrt natürlich auch dasselbe wie eine Abbildung, die jedem  $y \in Y$  eine Abbildung  $X \rightarrow Z$  zuordnet. In der exponentiellen Notation liest sich das besonders suggestiv als kanonische Bijektion  $Z^{(X \times Y)} \xrightarrow{\sim} (Z^X)^Y$ . Wegen dieser Notation zitiert man diese Aussage auch als das **Exponentialgesetz**. In wieder anderen Worten sind also die in der Schule derzeit so beliebten „Funktionen mit Parameter“ nichts anderes als „Funktionen von zwei Variablen, bei denen eine der beiden Variablen als Parameter bezeichnet wird“.

*Vorschau 2.1.6.6.* Später bezeichnen wir eine Abbildung  $X \times Y \rightarrow Z$  auch als eine **2-Multiabbildung** und notieren sie  $X \curlyvee Y \rightarrow Z$  mit dem als reinem Trenner zu verstehenden Symbol  $\curlyvee$  und erklären allgemeiner „ $r$ -Multiabbildungen“ für beliebiges  $r \in \mathbb{N}$  sowie deren „Multiverknüpfung“, aber alles zu seiner Zeit.

*Ergänzung 2.1.6.7 (Unmögliche Surjektionen).* Eine Abbildung  $f : X \rightarrow \mathcal{P}(X)$  von einer Menge in ihre Potenzmenge kann nie surjektiv sein. In der Tat, betrachten wir in  $X$  die Teilmenge  $A = \{x \in X \mid x \notin f(x)\}$ , so kann es kein  $y \in X$  geben mit  $f(y) = A$ , denn für solch ein  $y$  hätten wir entweder  $y \in A$  oder  $y \notin A$ , und aus  $y \in A$  alias  $y \in f(y)$  folgte  $y \notin A$ , wohingegen aus  $y \notin A$  alias  $y \notin f(y)$  folgte  $y \in A$ . Ordnen wir etwa jedem Menschen die Menge aller der Menschen

zu, die er liebt, und betrachten die Menge aller Menschen, die sich nicht selbst lieben, so wird diese Menge für keinen Menschen genau aus all den Menschen bestehen, die er liebt.

*Ergänzung 2.1.6.8.* Gegeben eine Menge  $X$  mag man sich eine Abbildung  $X \rightarrow \mathbb{N}$  veranschaulichen als eine „Menge von Elementen von  $X$ , in der jedes Element mit einer wohlbestimmten Vielfachheit vorkommt“. Aufgrund dieser Vorstellung nennen wir eine Abbildung  $X \rightarrow \mathbb{N}$  auch eine **Multimenge** von Elementen von  $X$ . Unter der **Kardinalität einer Multimenge** verstehen wir die Summe über die Werte der entsprechenden Abbildung an allen Stellen  $x \in X$ , aufgefaßt als ein Element von  $\mathbb{N} \sqcup \{\infty\}$ . Ich notiere Multimengen durch Mengenklammern mit einem vorgestellten unteren Index  $\mu$ . So wäre etwa  $\mu\{5, 5, 5, 7, 7, 1\}$  eine Multimenge von natürlichen Zahlen der Kardinalität 6. Diese Notation ist aber nicht gebräuchlich. Die Gesamtheit aller endlichen Multimengen von Elementen einer Menge  $X$  notiere ich auch  $\mathbb{N}X$ . Eine Multimenge der Kardinalität Zwei von Elementen einer Menge  $X$  nenne ich ein **ungeordnetes Paar** von Elementen von  $X$ .

2.1.6.9. Gegeben  $S \supset T$  eine Menge mit einer Teilmenge und  $f : S \rightarrow S$  eine Selbstabbildung von  $S$  sagen wir,  $T$  sei **stabil unter**  $f$  und  $f$  **stabilisiert**  $T$ , wenn gilt  $f(T) \subset T$ . Gilt sogar  $f(T) = T$ , so sagen wir,  $T$  **werde von**  $f$  **festgehalten**. Gilt noch stärker  $f(t) = t \forall t \in T$ , so sagen wir,  $T$  **werde von**  $f$  **punktweise festgehalten**.

*Beispiel 2.1.6.10.* Für jede Menge  $X$  mag man die **Mengenabbildung**  $X \hookrightarrow \mathcal{P}(X)$ ,  $x \mapsto \{x\}$  betrachten. Ihr Bild ist die Menge

$$\mathcal{P}_1(X) \subset \mathcal{P}(X)$$

aller einteiligen Teilmengen von  $X$ . Die Umkehrabbildung der so entstehenden Bijektion  $X \xrightarrow{\sim} \mathcal{P}_1(X)$  notieren wir  $\text{elt} : \mathcal{P}_1(X) \rightarrow X$  und nennen sie die **Elementabbildung**. Sie ordnet jeder einteiligen Teilmenge von  $X$  ihr einziges Element zu.

*Vorschau 2.1.6.11 (Formalisierung des Begriffs der natürlichen Zahlen).* Wir werden in 3.4.1 zeigen, daß es Paare  $(N, s)$  gibt bestehend aus einer Menge  $N$  und einer injektiven Abbildung  $s : N \rightarrow N$  derart, daß  $N \setminus s(N)$  aus genau einem Element  $o$  besteht und daß jede  $s$ -stabile Teilmenge von  $N$ , die  $o$  enthält, bereits ganz  $N$  sein muß. Weiter werden wir zeigen, daß solch ein Paar im Wesentlichen eindeutig bestimmt ist in dem Sinne, daß es für jedes weitere derartige Paar  $(N', s')$  genau eine Bijektion  $\varphi : N \xrightarrow{\sim} N'$  gibt mit  $s'\varphi = \varphi s$ . Im Rahmen der ganz naiven Mengenlehre kann man solch ein Paar unmittelbar angeben als  $(\mathbb{N}, s)$  mit  $s : n \mapsto (n + 1)$ . Bei einem etwas formaleren Aufbau der Mathematik aus der Mengenlehre mag man umgekehrt von derartigen Paaren ausgehen und so zu

einer Definition von  $\mathbb{N}$  und der Addition auf  $\mathbb{N}$  gelangen, vergleiche 3.4.1 folgende. Hier liegt auch der Schlüssel für eine formale Rechtfertigung des Prinzips der vollständigen Induktion.

*Vorschau 2.1.6.12.* Sie sehen bereits an dieser Stelle, wie problematisch der Begriff der Gleichheit im Grunde genommen ist und wie nah er an der Wurzel mathematischen Denkens liegt. Um ein besonders einfaches Beispiel zu bemühen, mag man sich fragen, ob je zwei einelementige Mengen gleich sind. Unsere Antwort hier muß lauten: Natürlich nicht, zwei einelementige Teilmengen einer gegebenen Menge etwa sind genau dann gleich, wenn sie dasselbe Element enthalten. Allerdings gibt es andererseits zwischen je zwei einelementigen Mengen genau eine Bijektion, eine einelementige Menge ist also „eindeutig bis auf eindeutige Bijektion“.

### Übungen

*Ergänzende Übung 2.1.6.13.* Gegeben eine fest gedachte Menge  $Y$  können wir für jede weitere Menge  $A$  eine Abbildung  $\text{ev}_A : A \rightarrow \text{Ens}(\text{Ens}(A, Y), Y)$ , genannt die **Evaluations- oder Auswertungsabbildung**, erklären durch die Vorschrift  $\text{ev}_A : a \mapsto (f \mapsto f(a))$ . Man zeige, daß für jede Menge  $X$  die Komposition

$$\text{Ens}(X, Y) \rightarrow \text{Ens}(\text{Ens}(\text{Ens}(X, Y), Y), Y) \rightarrow \text{Ens}(X, Y)$$

von  $\text{ev}_{\text{Ens}(X, Y)}$  mit dem Vorschalten ( $\circ \text{ev}_X$ ) von  $\text{ev}_X$  die Identität auf  $\text{Ens}(X, Y)$  ist. Später werden Sie diese Aussage möglicherweise als die „Dreiecksidentität“ im Kontext „adjungierter Funktoren“ in ?? verstehen lernen.

## 2.1.7 Logische Symbole und Konventionen

2.1.7.1. In der mathematischen Fachsprache meint **oder** immer, daß auch beides erlaubt ist. Wir haben diese Konvention schon benutzt bei der Definition der Vereinigung in 2.1.3.1 durch die Vorschrift  $X \cup Y = \{z \mid z \in X \text{ oder } z \in Y\}$ . Zum Beispiel haben wir  $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$ . In diesem Zusammenhang muß ich die schöne Geschichte erzählen von dem Logiker, der seinem Freund erzählt, er habe ein Kind bekommen. Der Freund fragt: „Ist es ein Junge oder ein Mädchen?“ worauf der Logiker antwortet: „Ja!“

*Ergänzung 2.1.7.2 (Herkunft des Vereinigungssymbols).* In den „Arithmetes principia“ von Giuseppe Peano scheint das Symbol  $\cup$  zum ersten Mal vorzukommen, allerdings als Symbol für „oder“. Peano schreibt: „Signum  $\cup$  legitur *vel*“ und „*vel*“ heißt „oder“ auf lateinisch. Der Kontext legt nahe, daß  $\cup$  an den Buchstaben

$v$  erinnern soll. Das Symbol  $\vee$  hatte Peano schon als Symbol für „verum“ verbraucht. In der Bedeutung der Vereinigung zweier Mengen habe ich das Symbol zuerst bei Bourbaki gesehen.

2.1.7.3. Sagt man der mathematischen Fachsprache, es gebe ein Objekt mit diesen und jenen Eigenschaften, so ist stets gemeint, daß es *mindestens ein* derartiges Objekt geben soll. Hätten wir diese Sprachregelung rechtzeitig vereinbart, so hätten wir zum Beispiel das Wörtchen „mindestens“ in Teil 2 von 2.1.5.4 bereits weglassen können. Sagt ihnen also ein Mathematiker, er habe einen Bruder, so kann es auch durchaus sein, daß er noch weitere Brüder hat! Will man in der mathematischen Fachsprache Existenz und Eindeutigkeit gleichzeitig ausdrücken, so sagt man, es gebe **genau ein** Objekt mit diesen und jenen Eigenschaften. Sagt ihnen also ein Mathematiker, er habe genau einen Bruder, so können sie sicher sein, daß er nicht noch weitere Brüder hat.

2.1.7.4. Die folgenden Abkürzungen erweisen sich als bequem und werden häufig verwendet:

|                               |   |
|-------------------------------|---|
| $\forall$                     | für alle (ein umgedrehtes A wie „alle“)     |
| $\exists$                     | es gibt (ein umgedrehtes E wie „existiert“) |
| $\exists!$                    | es gibt genau ein                           |
| $\dots \Rightarrow \dots$     | aus ... folgt ...                           |
| $\dots \Leftarrow \dots$      | ... folgt aus ...                           |
| $\dots \Leftrightarrow \dots$ | ... ist gleichbedeutend zu ...              |

Ist zum Beispiel  $f : X \rightarrow Y$  eine Abbildung, so können wir unsere Definitionen injektiv, surjektiv, und bijektiv etwas formaler so schreiben:

$$\begin{aligned} f \text{ injektiv} &\Leftrightarrow ((f(x) = f(z)) \Rightarrow (x = z)) \\ f \text{ surjektiv} &\Leftrightarrow \forall y \in Y \exists x \in X \text{ mit } f(x) = y \\ f \text{ bijektiv} &\Leftrightarrow \forall y \in Y \exists !x \in X \text{ mit } f(x) = y \end{aligned}$$

2.1.7.5. In den Zeiten des Bleisatzes war es nicht einfach, neue Symbole in Druck zu bringen. Irgendwelche Buchstaben verdreht zu setzen, war jedoch unproblematisch. So entstanden die Symbole  $\forall$  und  $\exists$ . Sie heißen **Quantoren**.

2.1.7.6. Bei den „für alle“ und „es gibt“ kommt es in der mathematischen Fachsprache, anders als in der weniger präzisen Umgangssprache, entscheidend auf die Reihenfolge an. Man betrachte zum Beispiel die beiden folgenden Aussagen:

„Für alle  $n \in \mathbb{N}$  gibt es  $m \in \mathbb{N}$  so daß gilt  $m \geq n$ “

„Es gibt  $m \in \mathbb{N}$  so daß für alle  $n \in \mathbb{N}$  gilt  $m \geq n$ “

Offensichtlich ist die Erste richtig, die Zweite aber falsch. Weiter mache man sich klar, daß die „für alle“ und „es gibt“ bei Verneinung vertauscht werden. Äquivalent sind zum Beispiel die beiden folgenden Aussagen

„Es gibt kein  $n \in \mathbb{N}$  mit  $n^2 = 2$ “

„Für alle  $n \in \mathbb{N}$  gilt nicht  $n^2 = 2$ “

2.1.7.7. Wollen wir zeigen, daß aus einer Aussage  $A$  eine weitere Aussage  $B$  folgt, so können wir ebensogut zeigen: Gilt  $B$  nicht, so gilt auch  $A$  nicht. In formelhafter Schreibweise haben wir also

$$(A \Rightarrow B) \Leftrightarrow ((\text{nicht } B) \Rightarrow (\text{nicht } A))$$

Wollen wir zum Beispiel zeigen ( $g \circ f$  surjektiv)  $\Rightarrow$  ( $g$  surjektiv), so reicht es, wenn wir uns überlegen: Ist  $g$  nicht surjektiv, so ist  $g \circ f$  erst recht nicht surjektiv. Oder ein Beispiel aus dem täglichen Leben: Die Aussage (Wenn ein Mensch ein Kind gebiert, ist er eine Frau) ist gleichbedeutend zur Aussage (Wenn ein Mensch keine Frau ist, gebiert er auch keine Kinder). Nicht folgern kann man dahingegen die Aussage (Wenn ein Mensch kein Kind gebiert, ist er keine Frau).

2.1.7.8. In der Literatur findet man oft die Abkürzung **oBdA** für „ohne Beschränkung der Allgemeinheit“.

## 2.2 Algebraische Grundbegriffe

Auf der Schule versteht man unter einer „reellen Zahl“ meist einen unendlichen Dezimalbruch, wobei man noch aufpassen muß, daß verschiedene unendliche Dezimalbrüche durchaus dieselbe reelle Zahl darstellen können, zum Beispiel gilt in den reellen Zahlen ja

$$0,99999\dots = 1,00000\dots$$

Diese reellen Zahlen werden dann addiert, subtrahiert, multipliziert und dividiert ohne tiefes Nachdenken darüber, wie man denn zum Beispiel mit den eventuell unendlich vielen Überträgen bei der Addition und Subtraktion umgehen soll, und warum dann Formeln wie  $(a + b) - c = a + (b - c)$  wirklich gelten, zum Beispiel für  $a = b = c = 0,999\dots$ . Dieses tiefe Nachdenken wollen wir im Folgenden vom Rest der Vorlesung abkoppeln und müssen dazu sehr präzise formulieren, welche Eigenschaften für die Addition, Multiplikation und Anordnung in „unseren“ reellen Zahlen gelten sollen. In der Terminologie, die in den folgenden Abschnitten eingeführt wird, werden wir die reellen Zahlen charakterisieren als einen angeordneten Körper, in dem jede nichtleere Teilmenge mit einer unteren Schranke sogar eine größte untere Schranke besitzt. Von dieser Charakterisierung ausgehend erklären wir dann, welche reelle Zahl ein gegebener unendlicher Dezimalbruch darstellt, und errichten das Gebäude der Analysis. In demselben Begriffsgebäude modellieren wir auch den Anschauungsraum, vergleiche 3.3.1.9 und 4.1.6.4. Um diese Charakterisierungen und Modellierungen verständlich zu machen, führen wir zunächst einige grundlegende algebraische Konzepte ein, die Ihnen im weiteren Studium der Mathematik noch oft begegnen werden.

### 2.2.1 Mengen mit Verknüpfung

**Definition 2.2.1.1.** Eine **Verknüpfung**  $\top$  auf einer Menge  $X$  ist eine Abbildung

$$\begin{array}{rcl} X \times X & \rightarrow & X \\ (x, y) & \mapsto & x \top y \end{array}$$

Jedem angeordneten Paar  $(x, y)$  mit  $x, y \in X$  wird also ein Element  $(x \top y) \in X$  zugeordnet.

2.2.1.2. Das unverfängliche Symbol  $\top$  benutze ich, um mich an dieser Stelle noch nicht implizit auf einen der Standardfälle Addition oder Multiplikation festlegen zu müssen. Das Wort „Verknüpfung“ erhält damit eine gegenüber 2.1.5.1 erweiterte Bedeutung: Statt der Verknüpfung von zwei Abbildungen kann damit auch allgemeiner eine abstrakte Verknüpfung auf einer beliebigen Menge gemeint sein. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen.

|   | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 2 | 0 | 1 | 2 | 2 | 2 |
| 3 | 0 | 1 | 2 | 3 | 3 |
| 4 | 0 | 1 | 2 | 3 | 4 |

Man kann Verknüpfungen auf endlichen Mengen darstellen durch ihre **Verknüpfungstafel**. Hier habe ich etwa die Verknüpfungstafel der Verknüpfung min auf der Menge  $\{0, 1, 2, 3, 4\}$  angegeben. Eigentlich muß man sich dazu einigen, ob im Kästchen aus der Spalte  $m$  und der Zeile  $n$  nun  $m \top n$  oder vielmehr  $n \top m$  stehen soll, aber bei einer kommutativen Verknüpfung wie min kommt es darauf zum Glück nicht an.

| (und)  | Wahr   | Falsch |
|--------|--------|--------|
| Wahr   | Wahr   | Falsch |
| Falsch | Falsch | Falsch |

| (oder) | Wahr | Falsch |
|--------|------|--------|
| Wahr   | Wahr | Wahr   |
| Falsch | Wahr | Falsch |

Die Wahrheitstafeln für „und“ und „oder“. Gemeint ist hier wie stets in der Mathematik das „nichtausschließende oder“. Sagen wir, es gelte  $A$  oder  $B$ , so ist insbesondere auch erlaubt, daß beides gilt. Bei der Wahrheitstafel für das „ausschließende oder“ müßte oben links als Verknüpfung von „Wahr“ mit „Wahr“ ein „Falsch“ stehen.

*Beispiele 2.2.1.3.* 1. Die Addition von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \rightarrow & \mathbb{Z} \\ (m, n) & \mapsto & m + n \end{array}$$

2. Die Multiplikation von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \rightarrow & \mathbb{Z} \\ (m, n) & \mapsto & m \cdot n \end{array}$$

3. Die Zuordnung  $\min$ , die jedem Paar von natürlichen Zahlen die kleinere zuordnet, wenn sie verschieden sind, und eben diese Zahl  $\min(n, n) = n$ , wenn sie gleich sind, ist eine Verknüpfung

$$\begin{array}{ccc} \min : \mathbb{N} \times \mathbb{N} & \rightarrow & \mathbb{N} \\ (m, n) & \mapsto & \min(m, n) \end{array}$$

4. Eine Abbildung  $Z \rightarrow Z$  von einer Menge  $Z$  in sich selbst nennen wir eine **Selbstabbildung von  $Z$** . Wir kürzen die Menge aller Selbstabbildungen einer Menge  $Z$  mit  $\text{Ens}(Z) := \text{Ens}(Z, Z)$  ab. Die Verknüpfung von Abbildungen liefert eine Verknüpfung auf der Menge  $\text{Ens}(Z)$  aller Selbstabbildungen von  $Z$ , in Formeln

$$\begin{array}{ccc} \text{Ens}(Z) \times \text{Ens}(Z) & \rightarrow & \text{Ens}(Z) \\ (f, g) & \mapsto & f \circ g \end{array}$$

5. Die Subtraktion von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \rightarrow & \mathbb{Z} \\ (m, n) & \mapsto & m - n \end{array}$$

6. Jede Verknüpfung  $\top$  auf einer Menge induziert eine Verknüpfung auf ihrer Potenzmenge mittels der Vorschrift

$$U \top V := \{u \top v \mid u \in U, v \in V\}$$

7. Gegeben Mengen mit Verknüpfung  $(X, \top)$  und  $(Y, \perp)$  erklären wir die **komponentenweise Verknüpfung** auf ihrem Produkt  $X \times Y$  durch die Vorschrift  $((x, y), (x', y')) \mapsto ((x \top x'), (y \perp y'))$ .

8. Logische Operationen wie „und“, „oder“, „impliziert“ können als Verknüpfungen auf der zweielementigen Menge  $\{\text{Wahr}, \text{Falsch}\}$  aufgefaßt werden. Die zugehörigen Verknüpfungstabellen heißen **Wahrheitstafeln**. Bei einem formalen Zugang werden diese Tafeln, wie sie für „und“ und „oder“ auf der vorhergehenden Seite zu finden sind, zur Definition der jeweiligen Begriffe.

2.2.1.4. Sei  $(X, \top)$  eine Menge mit Verknüpfung.

1. Gegeben Elemente  $a, b \in X$  sagen wir,  $a$  ist ein **Linksteiler** von  $b$ , wenn es  $d \in X$  gibt mit  $a \top d = b$ . Analog erklären wir **Rechtsteiler**;
2. Ein Element  $a \in X$  heißt **linkskürzbar**, wenn die Verknüpfung mit  $a$  eine Injektion  $(a \cdot) : X \hookrightarrow X$  liefert. Analog erklären wir die Eigenschaft **rechtskürzbar**. Ein Element, das linkskürzbar und rechtskürzbar ist, nennen wir **kürzbar**. Ein nicht kürzbares Element nennen wir **nichtkürzbar**.

*Beispiel 2.2.1.5.* Die kürzbaren Elemente von  $(\mathbb{Z}, \cdot)$  sind alle von Null verschiedenen Elemente. In  $(\mathbb{Z}, +)$  sind alle Elemente kürzbar. Die linkskürzbaren Elemente von  $\text{Ens}(Z)$  sind die Surjektionen. Die rechtskürzbaren Elemente von  $\text{Ens}(Z)$  sind die Injektionen.

2.2.1.6. Sei  $(X, \top)$  eine Menge mit Verknüpfung. Eine Teilmenge  $U \subset X$  heißt **abgeschlossen unter der Verknüpfung**, wenn aus  $x, y \in U$  folgt  $x \top y \in U$ . Natürlich ist in diesem Fall auch  $(U, \top)$  eine Menge mit Verknüpfung. Man spricht dann von der **auf  $U$  induzierten Verknüpfung**. Zum Beispiel ist  $\mathbb{N} \subset \mathbb{Z}$  abgeschlossen unter der Addition, aber  $\mathbb{Z} \setminus \{0\} \subset \mathbb{Q} \setminus \{0\}$  ist nicht abgeschlossen unter der durch die Division gegebenen Verknüpfung  $(m, n) \mapsto m/n$ .

**Definition 2.2.1.7.** Eine Verknüpfung  $\top$  auf einer Menge  $X$  heißt **assoziativ**, wenn gilt  $x \top (y \top z) = (x \top y) \top z \quad \forall x, y, z \in X$ . Sie heißt **kommutativ** oder **abelsch**, wenn gilt  $x \top y = y \top x \quad \forall x, y \in X$ . Gilt für zwei vorgegebene Elemente die Identität  $x \top y = y \top x$ , so sagen wir, daß diese beiden Elemente **kommutieren**.

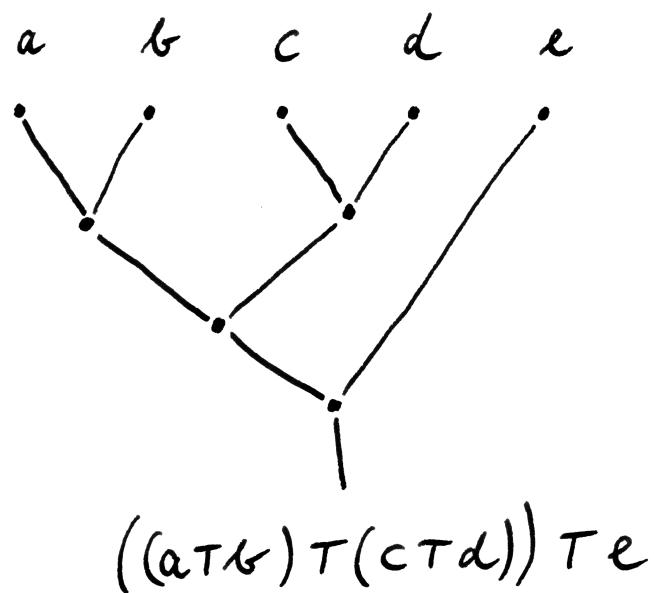
2.2.1.8 (**Diskussion der Terminologie**). Die Bezeichnung „abelsch“ ehrt den norwegischen Mathematiker Nils Henrik Abel.

*Beispiele 2.2.1.9.* Von unseren Beispielen sind die ersten Drei assoziativ und kommutativ, das Vierte ist assoziativ aber nicht kommutativ falls  $Z$  mehr als ein Element hat, das Fünfte ist weder assoziativ noch kommutativ.

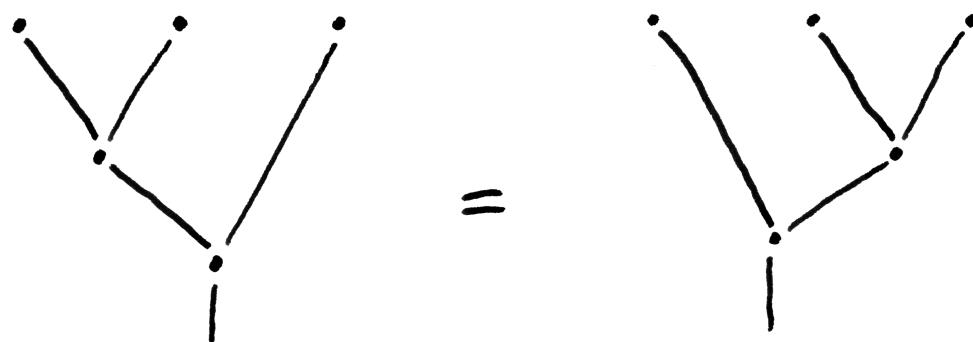
2.2.1.10. Ist eine Verknüpfung  $\top$  auf einer Menge  $A$  assoziativ, so liefern auch ungeklammerte Ausdrücke der Form  $a_1 \top a_2 \top \dots \top a_n$  wohlbestimmte Elemente von  $A$ , und zwar ist genauer das Resultat unabhängig davon, wie wir die Klammern setzen. Um diese Erkenntnis zu formalisieren, vereinbaren wir für einen ungeklammerten Ausdruck die „von hinten hochgeklammerte“ Interpretation

$$a_1 \top a_2 \top \dots \top a_n := a_1 \top (a_2 \top (\dots (a_{n-1} \top a_n) \dots))$$

und zeigen dann das folgende Lemma.



Mögliche „Klammerungen“ mag man sich graphisch wie oben angedeutet veranschaulichen. Die Assoziativität bedeutet dann graphisch so etwas wie



Das Gleichheitszeichen meint nur, daß beide Klammerungen stets dasselbe liefern, wenn wir oben drei Elemente unserer Menge mit Verknüpfung einfüllen.

**Lemma 2.2.1.11 (Assoziativität macht Klammern überflüssig).** *Gegeben eine Menge mit einer assoziativen Verknüpfung  $(A, \top)$  und  $a_1, \dots, a_n, b_1, \dots, b_m \in A$  gilt mit der von hinten hochgeklammerten Interpretation für ungeklammerte Ausdrücke*

$$(a_1 \top \dots \top a_n) \top (b_1 \top \dots \top b_m) = a_1 \top \dots \top a_n \top b_1 \top \dots \top b_m$$

*Beweis.* Wir folgern mit den Definitionen für die erste Gleichheit und dem Assoziativgesetz für die zweite Gleichheit die Identität

$$\begin{aligned} (a_1 \top \dots \top a_n) \top (b_1 \top \dots \top b_m) &= (a_1 \top (a_2 \top \dots \top a_n)) \top (b_1 \top \dots \top b_m) \\ &= a_1 \top ((a_2 \top \dots \top a_n) \top (b_1 \top \dots \top b_m)) \end{aligned}$$

und sind fertig mit vollständiger Induktion über  $n$ .  $\square$

2.2.1.12. Das Wort „Lemma“, im Plural „Lemmata“, kommt vom griechischen Wort  $\lambda\alpha\mu\beta\alpha\nu\epsilon\nu$  für „nehmen“ und bezeichnet in der Mathematik kleinere Resultate oder auch Zwischenschritte von größeren Beweisen, denen der Autor außerhalb ihres engeren Kontexts keine größere Bedeutung zumäßt.

*Vorschau* 2.2.1.13. Die Zahl der Möglichkeiten, einen Ausdruck in  $n+1$  Faktoren so zu klammern, daß in jedem Schritt nur die Verknüpfung von je zwei Elementen zu berechnen ist, heißt die  **$n$ -te Catalan-Zahl** und wird  $C_n$  notiert. Die ersten Catalan-Zahlen sind  $C_0 = C_1 = 1$ ,  $C_2 = 2$  und  $C_3 = 5$ : Die fünf möglichen Klammerungen von 4 Elementen sind etwa  $(ab)(cd)$ ,  $a(b(cd))$ ,  $a((bc)d)$ ,  $((ab)c)d$  und  $(a(bc))d$ . Im allgemeinen zeigen wir in ??, daß sich die Catalan-Zahlen durch die Binomial-Koeffizienten 1.1.1.17 ausdrücken lassen vermittels der amüsanten Formel

$$C_n = \frac{1}{n+1} \binom{2n}{n}$$

2.2.1.14. Gegeben eine Menge mit assoziativer und kommutativer Verknüpfung  $(A, \top)$  kommt es beim Verknüpfen noch nicht einmal auf die Reihenfolge an. Sind genauer  $a_1, \dots, a_n$  mit  $n \geq 1$  gegeben und ist  $\sigma : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}$  eine bijektive Abbildung, so gilt

$$a_1 \top \dots \top a_n = a_{\sigma(1)} \top \dots \top a_{\sigma(n)}$$

Wir betrachten das als offensichtlich und schreiben keinen Beweis aus.

**Definition 2.2.1.15 (Iterierte Verknüpfungen).** Sei  $(X, \top)$  eine Menge mit Verknüpfung. Ist  $n \in \{1, 2, \dots\}$  eine von Null verschiedene natürliche Zahl und  $x \in X$ , so schreiben wir

$$\underbrace{x \top x \top \dots \top x}_{n\text{-mal}} =: n^\top x$$

Ich erinnere daran, daß wir in 2.2.1.10 für derartige Ausdrücke im Zweifelsfall die Interpretation als „von hinten hochgeklammerte Verknüpfung“ vereinbart hatten.

2.2.1.16. Wird unsere Verknüpfung  $+$  notiert, so schreibt man statt  $n^+x$  meist kurz  $nx$ . Wird unsere Verknüpfung mit einem runden Symbol wie etwa  $*$  notiert, so schreibt man statt  $n^*x$  meist kurz  $x^n$  oder etwas ausführlicher  $x^{*n}$  oder  $x^{(*n)}$ .

2.2.1.17 (**Iterationsregeln**). Sei  $(A, \top)$  eine Menge mit assoziativer Verknüpfung. Sind  $m, n$  zwei von Null verschiedene natürliche Zahlen, so erhalten wir mithilfe unseres Lemmas 2.2.1.11 zur Überflüssigkeit von Klammern bei assoziativen Verknüpfungen die Regeln  $(n + m)^\top a = (n^\top a) \top (m^\top a)$  und  $(nm)^\top a = n^\top(m^\top a)$ . Ist unsere Verknüpfung außerdem auch noch kommutativ, so gilt zusätzlich die Regel  $n^\top(a \top b) = (n^\top a) \top (n^\top b)$ . Wenn man es ganz genau nimmt, muß man für einen formalen Beweis die formale Einführung der natürlichen Zahlen 3.4.1.5 abwarten, wo Sie das dann als Übung 3.4.1.39 behandeln dürfen.

**Definition 2.2.1.18.** Gegeben eine Menge mit Verknüpfung  $(X, \top)$  heißt ein Element  $e \in X$  ein **neutrales Element** von  $(X, \top)$ , wenn gilt

$$e \top x = x \top e = x \quad \forall x \in X$$

2.2.1.19 (**Eindeutigkeit neutraler Elemente**). In einer Menge mit Verknüpfung  $(X, \top)$  kann es höchstens ein neutrales Element  $e$  geben, denn für jedes weitere Element  $e'$  mit  $e' \top x = x \top e' = x \quad \forall x \in X$  haben wir  $e' = e' \top e = e$ . Wir dürfen also den bestimmten Artikel verwenden und in einer Menge mit Verknüpfung von *dem* neutralen Element reden und es mit  $e_X$  bezeichnen.

**Definition 2.2.1.20.** Ein **Monoid** ist eine Menge mit einer assoziativen Verknüpfung, in der es ein neutrales Element gibt.

2.2.1.21. Das Wort „Monoid“ ist wohl von griechisch „μονος“ für „allein“ abgeleitet: Ein Monoid besitzt nur eine einzige Verknüpfung. Für ein kommutatives Monoid schlage ich die abkürzende Bezeichnung **Abmonoid** vor, mit der Vorsilbe „Ab“ für „abelsch“.

2.2.1.22 (**Additiv und multiplikativ notierte Monoide**). Notiert man in einem Monoid  $M$  die Verknüpfung mit dem Symbol  $+$ , so notiert man das neutrale Element meist  $0_M$  oder abkürzend 0 und nennt es das **Null-Element** oder abkürzend die **Null** und spricht von einem **additiv notierten Monoid**. Nur kommutative Monoide werden additiv notiert. Notiert man in einem Monoid  $M$  die Verknüpfung mit einem eher runden Symbol wie  $\cdot$  oder  $\circ$  oder  $*$  oder auch einfach durch Hintereinanderschreiben, so notiert man das neutrale Element oft  $1_M$  oder abkürzend 1 und nennt es das **Eins-Element** oder abkürzend die **Eins** und spricht von einem **multiplikativ notierten Monoid**.

*Beispiele* 2.2.1.23. Die natürlichen Zahlen bilden mit der Addition ein Monoid  $(\mathbb{N}, +)$  mit neutralem Element 0. Sie bilden auch mit der Multiplikation ein Monoid  $(\mathbb{N}, \cdot)$  mit neutralem Element 1. Für jede Menge  $Z$  ist die Menge  $\text{Ens}(Z)$  der

Selbstabbildungen von  $Z$  mit der Verknüpfung  $\circ$  von Abbildungen als Verknüpfung ein Monoid mit neutralem Element  $\text{id}_Z$ . Die leere Menge ist *kein* Monoid, ihr fehlt das neutrale Element. Jede einelementige Menge ist mit der einzigen möglichen Verknüpfung ein Monoid.

**2.2.1.24 (Nullfach iterierte Verknüpfung in Monoiden).** Ist  $(M, \top)$  ein Monoid, so erweitern wir unsere Notation  $n^\top a$  aus 2.2.1.15 auf alle natürlichen Zahlen  $n \in \mathbb{N}$ , indem wir

$$0^\top a := e_M$$

als das neutrale Element  $e_M$  von  $M$  verstehen, für alle  $a \in M$ . Damit gelten unsere Iterationsregeln 2.2.1.17 dann sogar für alle  $n, m \in \mathbb{N}$ , vergleiche 3.4.1.29.

**2.2.1.25 (Notationen für nullfach iterierte Verknüpfung).** Sei ein Monoid  $M$  gegeben. Wird seine Verknüpfung  $+$  notiert, so schreibt man auch für  $n = 0$  statt  $n^+x$  meist kurz  $nx$  und meint also mit  $0x$  das neutrale Element von  $M$ , in Formeln

$$0x := 0_M$$

Wird seine Verknüpfung mit einem runden Symbol wie etwa  $*$  notiert, so schreibt man auch für  $n = 0$  statt  $n^*x$  meist kurz  $x^n$  oder etwas ausführlicher  $x^{*n}$  oder  $x^{(*n)}$  und meint insbesondere mit  $x^0$  das neutrale Element von  $M$ , in Formeln

$$x^0 := 1_M$$

**2.2.1.26 (Summen- und Produktzeichen).** Gegeben eine Abbildung  $I \rightarrow M$ ,  $i \mapsto a_i$  von einer endlichen Menge in ein additiv beziehungsweise multiplikativ notiertes Abmonoid  $M$  vereinbaren wir die Notationen

$$\sum_{i \in I} a_i \quad \text{beziehungsweise} \quad \prod_{i \in I} a_i$$

für die „Verknüpfung aller  $a_i$  mit  $i \in I$ “. Ist  $I$  die leere Menge, so vereinbaren wir, daß dieser Ausdruck das neutrale Element von  $M$  bedeuten möge, also 0 beziehungsweise 1. Für die konstante Abbildung  $I \rightarrow \mathbb{N}$ ,  $i \mapsto 1$  haben wir zum Beispiel

$$\sum_{i \in I} 1 = |I|$$

Unsere Konvention 1.1.1.14 für mit einem Laufindex notierte Summen beziehungsweise Produkte verwenden wir bei kommutativen Monoiden analog.

*Ergänzung 2.2.1.27.* Gegeben eine Menge mit Verknüpfung  $(M, \top)$  kann man die Assoziativität und die Existenz eines neutralen Elements dahingehend zusammenfassen, daß wir für jedes  $r \geq 0$  ausgezeichnete „Multiverknüpfungen“  $M^{\times r} \rightarrow M$  zur Verfügung haben, die eine gewisse „Multiassoziativität“ erfüllen,

die ich hier nicht genauer ausschreiben will. Das neutrale Element ist dabei die „Multiverknüpfung des Nulltupels“. In diesem Licht betrachtet gehören bei einer Verknüpfung die Forderungen der Assoziativität und der Existenz eines neutralen Elements zusammen. Ich schlage vor, eine Verknüpfung mit diesen beiden Eigenschaften **unitärassoziativ** zu nennen. Ein Monoid ist damit eine Menge mit einer unitärassoziativen Verknüpfung.

## Übungen

*Übung 2.2.1.28.* Sei  $Z$  eine Menge. Das Schneiden von Teilmengen ist eine Verknüpfung

$$\begin{aligned}\cap : \mathcal{P}(Z) \times \mathcal{P}(Z) &\rightarrow \mathcal{P}(Z) \\ (A, B) &\mapsto A \cap B\end{aligned}$$

auf der Potenzmenge. Dasselbe gilt für die Vereinigung und das Bilden der Differenzmenge. Welche dieser Verknüpfungen sind kommutativ oder assoziativ? Welche besitzen neutrale Elemente?

*Ergänzende Übung 2.2.1.29.* Man gebe die Wahrheitstafeln für  $\Rightarrow$  und  $\Leftrightarrow$  an. Bezeichne weiter  $\neg : \{\text{Wahr}, \text{Falsch}\} \rightarrow \{\text{Wahr}, \text{Falsch}\}$  die „Verneinung“. Man zeige, daß die Formel

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

beim Einsetzen beliebiger Wahrheitswerte aus  $\{\text{Wahr}, \text{Falsch}\}$  für  $A$  und  $B$  stets den Wert Wahr ausgibt, in Übereinstimmung mit unseren eher intuitiven Überlegungen in 2.1.7.7.

## 2.2.2 Gruppen

2.2.2.1. Ich empfehle, bei der Lektüre dieses Abschnitts die Tabelle nach 2.2.2.13 gleich mitzulesen, die die Bedeutungen der nun folgenden Formalitäten in den zwei gebräuchlichsten Notationssystemen angibt. In diesen Notationssystemen sollten alle Formeln aus der Schulzeit vertraut sein. Ich erinnere daran, daß wir ein Monoid definiert hatten als eine Menge mit einer assoziativen Verknüpfung, für die es in unserer Menge ein neutrales Element gibt.

**Definition 2.2.2.2.** 1. Ist  $(M, \top)$  ein Monoid und  $a \in M$  ein Element, so nennen wir ein weiteres Element  $\bar{a} \in M$  **invers zu**  $a$ , wenn gilt  $a \top \bar{a} = e = \bar{a} \top a$  für  $e \in M$  das neutrale Element unseres Monoids. Ein Element eines Monoids, das ein Inverses besitzt, heißt **invertierbar**;

2. Eine **Gruppe** ist ein Monoid, in dem jedes Element ein Inverses besitzt;

3. Eine **kommutative Gruppe** oder **abelsche Gruppe** ist eine Gruppe, deren Verknüpfung kommutativ ist.

*Beispiele 2.2.2.3.* Von unseren Beispielen 2.2.1.3 für Mengen mit Verknüpfung oben ist nur  $(\mathbb{Z}, +)$  eine Gruppe, und diese Gruppe ist kommutativ. Ein anderes Beispiel für eine kommutative Gruppe ist die Menge  $\mathbb{Q}$  der rationalen Zahlen mit der Addition als Verknüpfung, ein weiteres die Menge  $\mathbb{Q} \setminus \{0\}$  der von Null verschiedenen rationalen Zahlen mit der Multiplikation als Verknüpfung. Auch jedes einelementige Monoid ist eine Gruppe.

2.2.2.4. Der Begriff einer „Gruppe“ wurde von Évariste Galois (1811-1832) in die Mathematik eingeführt. Er verwendet den Begriff „Gruppe von Transformationen“ sowohl in der Bedeutung einer „Menge von bijektiven Selbstabbildungen einer gegebenen Menge“ als auch in der Bedeutung einer „Menge von bijektiven Selbstabbildungen einer gegebenen Menge, die abgeschlossen ist unter Verknüpfung und Inversenbildung“, und die damit in der Tat ein Beispiel für eine Gruppe im Sinne der obigen Definition bildet. Unsere obige Definition 2.2.2 geht auf eine Arbeit von Arthur Cayley aus dem Jahre 1854 mit dem Titel „On the theory of groups as depending on the symbolic equation  $\theta^n = 1$ “ zurück und wurde damit formuliert, bevor Cantor die Sprache der Mengenlehre entwickelte. Die Terminologie „abelsche Gruppe“ wurde zu Ehren des norwegischen Mathematikers Niels Hendrik Abel eingeführt.

**Lemma 2.2.2.5.** *Jedes Element eines Monoids besitzt höchstens ein Inverses.*

*Beweis.* Aus  $a \top \bar{a} = e$  und  $b \top a = e$  folgt durch Anwenden von  $b \top$  auf die erste Gleichung mit dem Assoziativgesetz sofort  $\bar{a} = b$ .  $\square$

2.2.2.6. Wir dürfen also den bestimmten Artikel benutzen und von nun an von *dem Inversen* eines Elements eines Monoids und insbesondere auch einer Gruppe reden. Gegeben ein invertierbares Element ist offensichtlich auch sein Inverses invertierbar und das Inverse des Inversen ist wieder das ursprüngliche Element, in Formeln  $\bar{\bar{a}} = a$ .

2.2.2.7. Beim Beweis von Lemma 2.2.2.5 haben wir stärker gezeigt: Besitzt ein Element eines Monoids ein „Rechtsinverses“ und ein „Linksinverses“, so stimmen diese überein.

**Lemma 2.2.2.8.** *Sind  $a$  und  $b$  invertierbare Elemente eines Monoids, so ist auch  $a \top b$  invertierbar mit Inversem  $\overline{(a \top b)} = \bar{b} \top \bar{a}$ .*

*Beweis.* In der Tat rechnen wir schnell  $(a \top b) \top (\bar{b} \top \bar{a}) = e = (\bar{b} \top \bar{a}) \top (a \top b)$ . Diese Formel ist auch aus dem täglichen Leben vertraut: Wenn man sich morgends zuerst die Strümpfe anzieht und dann die Schuhe, so muß man abends zuerst die Schuhe ausziehen und dann die Strümpfe.  $\square$

|     | 123 | 213 | 312 | 321 | 132 | 231 |  |
|-----|-----|-----|-----|-----|-----|-----|--|
| 123 | 123 | 213 | 312 | 321 | 132 | 231 |  |
| 213 | 213 | 123 | 321 | 312 | 231 | 132 |  |
| 312 | 312 | 132 | 231 | 213 | 321 | 123 |  |
| 321 | 321 | 231 | 132 | 123 | 312 | 213 |  |
| 132 | 132 | 312 | 213 | 231 | 123 | 321 |  |
| 231 | 231 | 321 | 123 | 132 | 213 | 312 |  |
|     |     |     |     |     |     |     |  |

Die Verknüpfungstafel der Gruppe aller Permutationen der Menge  $\{1, 2, 3\}$ . Eine solche Permutation  $\sigma$  habe ich dargestellt durch das geordnete Zahlentripel  $\sigma(1)\sigma(2)\sigma(3)$ , und im Kästchen aus der Zeile  $\tau$  und der Spalte  $\sigma$  steht  $\tau \circ \sigma$ .

**2.2.2.9 (Gruppe der invertierbaren Elemente eines Monoids).** Die invertierbaren Elemente eines Monoids bilden insbesondere stets eine unter der Verknüpfung abgeschlossene Teilmenge. Diese Teilmenge enthält offensichtlich das neutrale Element und ist folglich mit der induzierten Verknüpfung eine Gruppe. Für die Gruppe der invertierbaren Elemente eines multiplikativ notierten Monoids  $M$  verwenden wir die Notation  $M^\times$ . Zum Beispiel haben wir  $\mathbb{Z}^\times = \{1, -1\}$ . Dieses Kreuz soll nicht als  $x$  gelesen werden, es ist vielmehr ein mißbrauchtes Multiplikationssymbol.

*Beispiel 2.2.2.10.* Für jede Menge  $Z$  ist die Menge aller Bijektionen von  $Z$  auf sich selbst eine Gruppe, mit der Komposition von Abbildungen als Verknüpfung. Wir notieren diese Gruppe  $\text{Ens}^\times(Z)$  in Übereinstimmung mit unserer Konvention 2.2.2.9, schließlich handelt es sich um die Gruppe der invertierbaren Elemente des Monoids  $\text{Ens}(Z)$ . Ihre Elemente heißen die **Permutationen von  $Z$** . Die Gruppe der Permutationen einer Menge  $Z$  ist für  $|Z| > 2$  nicht kommutativ. Das Inverse einer Bijektion ist ihre Umkehrabbildung.

**Definition 2.2.2.11 (Negativ iterierte Verknüpfung invertierbarer Elemente).**

Ist  $(M, \top)$  ein Monoid und  $a \in M$  invertierbar, so erweitern wir unsere Notation  $n^\top a$  aus 2.2.1.24 weiter auf alle ganzen Zahlen  $n \in \mathbb{Z}$ , indem wir für  $n$  negativ setzen  $n^\top a := (-n)^\top \bar{a}$ .

**2.2.2.12 (Iterationsregeln).** Gegeben ein invertierbares Element  $a$  eines Monoids gelten offensichtlich sogar für alle ganzen Zahlen  $n \in \mathbb{Z}$  die Regeln  $(n+m)^\top a = (n^\top a) \top (m^\top a)$  und  $(nm)^\top a = n^\top (m^\top a)$ . Sind  $a, b$  invertierbare Elemente eines Monoids mit  $ab = ba$ , so gilt zusätzlich  $n^\top (a \top b) = (n^\top a) \top (n^\top b)$  für alle  $n \in \mathbb{Z}$ . Wenn man es ganz genau nehmen will, muß man hierfür die formale Einführung der ganzen Zahlen 3.4.2.12 abwarten.

**2.2.2.13.** Bei additiv geschriebenen Monoiden bezeichnet man das Inverse von  $a$ , sofern es existiert, meist als das **Negative** von  $a$  und notiert es  $-a$ . Bei multiplikativ notierten kommutativen Monoiden verwendet man die Bruchnotation  $1/a$  und  $b/a$  aus nebenstehender Tabelle, falls  $a$  invertierbar ist. Bei nichtkommutativen multiplikativ notierten Monoiden benutzt man für das Inverse von  $a$  die von der im folgenden erklärten allgemeinen Notation  $a^n$  abgeleitete Notation  $a^{-1}$ . Die nebenstehende Tabelle faßt die üblichen Notationen für unsere abstrakten Begriffsbildungen in diesem Kontext zusammen und gibt unsere allgemeinen Resultate und Konventionen in diesen Notationen wieder.

**2.2.2.14 (Notationen für negativ iterierte Verknüpfung).** Sei ein Monoid  $M$  gegeben und sei  $x \in M$  invertierbar. Wird unser Monoid additiv notiert, so schreibt man auch für negatives  $n \in \mathbb{Z}$  statt  $n^+x$  meist kurz  $nx$  und meint also mit  $nx$  das Negative von  $(-n)x$ . Wird unser Monoid multiplikativ notiert, also mit einem

| abstrakt   | additiv                         | multiplikativ  |
|--|---------------------------------|--|
| $a \top b$                                       | $a + b$                         | $a \cdot b, a \circ b, ab$   |
| $e$  | $\hat{0}$                       | $\hat{1}$  |
| $\bar{b}$  | $-b$                            | $\hat{1}/b, b^{-1}$  |
| $a \top \bar{b}$                                 | $a - b$                         | $a/b, ab^{-1}$   |
| $n^\top a$                                       | $na$                            | $a^n$  |
| $e \top a = a \top e = a$                        | $\hat{0} + a = a + \hat{0} = a$ | $\hat{1} \cdot a = a \cdot \hat{1} = a$                              |
| $a \top \bar{a} = e$                             | $a - a = \hat{0}$               | $a/a = \hat{1}$  |
| $\bar{\bar{a}} = a$                              | $-(-a) = a$                     | $\hat{1}/(\hat{1}/a) = a$  |
| $(-1)^\top a = \bar{a}$                          | $(-1)a = -a$                    | $a^{-1} = \hat{1}/a$   |
| $\overline{(a \top b)} = \bar{b} \top \bar{a}$   | $-(a + b) = (-b) + (-a)$        | $(ab)^{-1} = b^{-1}a^{-1},$<br>$\hat{1}/ab = (\hat{1}/b)(\hat{1}/a)$ |
| $\overline{(a \top \bar{b})} = b \top \bar{a}$   | $-(a - b) = b - a$              | $\hat{1}/(a/b) = b/a$  |
| $n^\top (m^\top a) = (nm)^\top a$                | $n(ma) = (nm)a$                 | $(a^m)^n = a^{nm}$   |
| $(m + n)^\top a = (m^\top a) \top (n^\top a)$    | $(m + n)a = (ma) + (na)$        | $a^{(m+n)} = (a^m)(a^n)$   |
| $\overline{n^\top a} = (-n)^\top a$              | $-(na) = (-n)a$                 | $(a^n)^{-1} = a^{-n}$  |
| $0^\top a = e$                                   | $0a = \hat{0}$                  | $a^0 = \hat{1}$  |
| $n^\top (a \top b) = (n^\top a) \top (n^\top b)$ | $n(a + b) = (na) + (nb)$        | $(ab)^n = (a^n)(b^n)$  |

Konventionen und Formeln in verschiedenen Notationssystemen. Bereits diese Tabelle muß mit einigen Hintergedanken gelesen werden, weil die Symbole  $+$ ,  $-$  darin in zweierlei Bedeutung vorkommen: Manchmal meinen sie konkrete Operationen in  $\mathbb{Z}$ , manchmal stehen sie aber auch für Verknüpfung, Inversenbildung und neutrale Elemente in abstrakten Monoiden. Ich habe den Symbolen  $0, 1$  einen Hut aufgesetzt und  $\hat{0}, \hat{1}$  geschrieben, wenn sie neutrale Elemente in abstrakten Monoiden bedeuten. Das werde ich aber nicht durchhalten.

runden Symbol wie etwa  $*$ , so schreibt man auch für negatives  $n \in \mathbb{Z}$  statt  $n^*x$  meist kurz  $x^n$  oder etwas ausführlicher  $x^{*n}$  oder  $x^{(*)n}$  und meint also mit  $x^n$  das Inverse von  $x^{-n}$ .

*Beispiel 2.2.2.15.* Im Fall einer bijektiven Abbildung  $f : Z \xrightarrow{\sim} Z$  ist die Umkehrabbildung  $f^{-1} : Z \xrightarrow{\sim} Z$  das Inverse  $f^{-1}$  des invertierbaren Elements  $f$  des Monoids  $\text{Ens}(Z)$ . Ebenso ist im Fall einer von Null verschiedenen rationalen Zahl  $a \in \mathbb{Q}$  ihr Inverses im multiplikativen Monoid  $\mathbb{Q}$  der Kehrbruch  $1/a = a^{-1}$ . Unsere Konvention verträgt sich also recht gut mit verschiedenen anderen Konventionen, die Sie bereits kennen mögen.

### Übungen

*Übung 2.2.2.16.* Ein Element  $a$  eines Monoids  $M$  ist invertierbar genau dann, wenn es  $b, c \in M$  gibt mit  $b \top a = e = a \top c$  für  $e$  das neutrale Element.

*Übung 2.2.2.17 (Kürzen).* Sind  $a, b, c$  Elemente einer Gruppe, so folgt aus  $a \top b = a \top c$  bereits  $b = c$ . Ebenso folgt aus  $b \top a = c \top a$  bereits  $b = c$ . Dasselbe gilt allgemeiner in einem beliebigen Monoid, wenn wir  $a$  invertierbar annehmen.

*Ergänzende Übung 2.2.2.18.* Seien  $M$  ein Monoid und  $e$  sein neutrales Element. Man zeige: Unser Monoid ist genau dann eine Gruppe, wenn es für jedes  $a \in M$  ein  $\bar{a} \in M$  gibt mit  $\bar{a} \top a = e$ , und dies Element  $\bar{a}$  ist dann notwendig das Inverse von  $a$  in  $M$ . Noch Mutigere zeigen: Ist  $A$  eine Menge mit assoziativer Verknüpfung und existiert ein  $e \in M$  mit  $e \top a = a \forall a \in M$  sowie für jedes  $a \in M$  ein  $\bar{a} \in M$  mit  $\bar{a} \top a = e$ , so ist  $M$  eine Gruppe. Hinweis: Man zeige, daß  $\bar{a} \top$  bijektiv ist.

*Ergänzende Übung 2.2.2.19.* Gegeben eine Menge  $Z$  ist ihre Potenzmenge  $\mathcal{P}(Z)$  mit der Verknüpfung  $A + B := (A \cup B) \setminus (A \cap B)$  eine abelsche Gruppe.

*Ergänzende Übung 2.2.2.20.* Gegeben Gruppen  $G, H$  können wir das kartesische Produkt  $G \times H$  zu einer Gruppe machen, indem wir darauf die komponentenweise Verknüpfung  $(g, h)(g', h') := (gg', hh')$  betrachten.

*Übung 2.2.2.21.* Ein endliches Monoid  $(M, \top)$ , in dem für jedes Element  $a \in M$  die Multiplikationsabbildung eine Injektion  $(a \top) : M \hookrightarrow M$  ist, muß bereits eine Gruppe sein.

### 2.2.3 Homomorphismen

*Didaktische Anmerkung 2.2.3.1.* Ich habe diesen Abschnitt einmal erst später im Zusammenhang mit der Diskussion von linearen Abbildungen besprochen und habe es bereut.

**Definition 2.2.3.2.** Eine Menge mit einer völlig beliebigen, nicht notwendig assoziativen Verknüpfung heißt ein **Magma**. Gegeben Magmas  $(X, \top)$  und  $(Y, \perp)$  verstehen wir unter einem **Homomorphismus von Mengen mit Verknüpfung** oder auch **Homomorphismus von Magmas** eine Abbildung  $\varphi : X \rightarrow Y$  derart, daß gilt  $\varphi(a \top b) = \varphi(a) \perp \varphi(b)$  für alle  $a, b \in X$ . Die Menge aller solchen Homomorphismen von Magmas bezeichnen wir mit

$$\text{Mag}(X, Y)$$

*Beispiel 2.2.3.3.* Sei  $Z$  eine Menge und  $\mathcal{P}(Z)$  ihre Potenzmenge. Wir betrachten auf  $\mathcal{P}(Z)$  die Verknüpfung  $(A, B) \mapsto A \setminus B$ . Ist  $Z \hookrightarrow W$  eine Injektion, so ist die auf den Potenzmengen induzierte Abbildung ein Homomorphismus von Magmas

$$(\mathcal{P}(Z), \setminus) \rightarrow (\mathcal{P}(W), \setminus)$$

2.2.3.4. Sind unsere beiden Mengen mit Verknüpfung Monoide, so verstehen wir unter einem **Monoidhomomorphismus** einen Homomorphismus von Mengen mit Verknüpfung, der das neutrale Element auf das neutrale Element abbildet. Gegeben Monoide  $M$  und  $N$  bezeichnen wir die Menge aller Monoidhomomorphismen von  $M$  nach  $N$  mit

$$\text{Mon}(M, N) := \{\varphi \in \text{Mag}(M, N) \mid \varphi(e_M) = e_N\}$$

*Ergänzung 2.2.3.5.* Die beiden Bedingungen an einen Monoidhomomorphismus  $\varphi : M \rightarrow N$  können in der in 2.2.1.27 eingeführten Terminologie dahingehend zusammengefaßt werden, daß die beiden Abbildungen  $M^{\times r} \rightarrow M \rightarrow N$  und  $M^{\times r} \rightarrow N^{\times r} \rightarrow N$ , die durch  $\varphi$  und unsere Multiverknüpfungen gegeben werden, für alle  $r \geq 0$  übereinstimmen sollen.

*Beispiel 2.2.3.6.* Gegeben Monoide  $M, N$  kann  $\text{Mon}(M, N) \subset \text{Mag}(M, N)$  eine echte Teilmenge sein. Zum Beispiel ist die Abbildung  $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, \cdot)$ , die jede ganze Zahl auf die Null wirft, ein Homomorphismus von Mengen mit Verknüpfung, aber kein Monoidhomomorphismus.

2.2.3.7. Gegeben ein Monoid  $M$  und eine Gruppe  $G$  gilt stets

$$\text{Mag}(M, G) = \text{Mon}(M, G)$$

Jeder Homomorphismus  $\varphi$  von Mengen mit Verknüpfung von einem Monoid in eine Gruppe bildet also das neutrale Element auf das neutrale Element ab. In der Tat folgt das aus  $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$  durch Kürzen. Einen Homomorphismus zwischen zwei Gruppen, in Formeln eine Abbildung  $\varphi : H \rightarrow G$  mit  $\varphi(ab) = \varphi(a)\varphi(b)$  für alle  $a, b \in H$ , nennen wir einen **Gruppenhomomorphismus**. Gegeben Gruppen  $H$  und  $G$  bezeichnen wir die Menge aller Gruppenhomomorphismen von  $H$  nach  $G$  mit

$$\text{Grp}(H, G)$$

Die neue Notation hat gegenüber den beiden bereits eingeführten alternativen Notationen  $\text{Mag}(H, G)$  und  $\text{Mon}(H, G)$  den Vorteil, uns daran zu erinnern, daß wir es mit Gruppen zu tun haben.

**Definition 2.2.3.8.** Ein **Isomorphismus** ist ein Homomorphismus  $\phi$  mit der Eigenschaft, daß es einen Homomorphismus  $\psi$  in die Gegenrichtung gibt derart, daß beide Kompositionen  $\psi \circ \phi$  und  $\phi \circ \psi$  die Identität sind. Zwei Gruppen oder Monoide oder Magmas heißen **isomorph**, wenn es zwischen ihnen einen Isomorphismus gibt.

2.2.3.9. Die Terminologie kommt von griechisch „*μορφη*“ für „Gestalt, Struktur“ und griechisch „*ομοιος*“ für „gleich, ähnlich“. Auf deutsch könnte man statt Homomorphismus auch „strukturerhaltende Abbildung“ sagen. Das Wort „Isomorphismus“ wird analog gebildet mit griechisch „*ισος*“ für „gleich“.

2.2.3.10. In den Fällen der obigen Definition ist offensichtlich jeder bijektive Homomorphismus bereits ein Isomorphismus. Im weiteren Verlauf dieser Vorlesungen werden Ihnen aber auch Arten von Homomorphismen begegnen, für die das nicht mehr richtig oder nicht einmal eine sinnvolle Aussage ist. Der erste derartige Fall wird Ihnen in diesen Vorlesungen in 3.1.4.8 begegnen: Im Kontext teilgeordneter Mengen muß eine bijektive monoton wachsende Abbildung keineswegs ein „Isomorphismus von teilgeordneten Mengen“ sein alias eine monoton wachsende Umkehrabbildung besitzen.

*Ergänzung* 2.2.3.11. Den Begriff eines Homomorphismus verwendet man auch im Fall von Mengen ohne Verknüpfung: Unter einem **Homomorphismus von Mengen** versteht man schlicht eine Abbildung, unter einem **Isomorphismus von Mengen** eine Bijektion.

*Beispiel 2.2.3.12 (Gruppen mit höchstens zwei Elementen).* Je zwei Gruppen mit genau einem Element sind isomorph und es gibt zwischen ihnen genau einen Isomorphismus. Je zwei Gruppen mit genau zwei Elementen sind isomorph und es gibt zwischen ihnen genau einen Isomorphismus, der eben das neutrale Element auf das neutrale Element wirft und das nichtneutrale Element auf das nichtneutrale Element.

*Beispiel 2.2.3.13 (Dreielementige Gruppen).* Je zwei Gruppen mit genau drei Elementen sind isomorph und es gibt zwischen ihnen genau zwei Isomorphismen. Um das zu sehen, beschreiben wir eine endliche Menge mit Verknüpfung durch ihre Verknüpfungstabelle, die im Fall einer Gruppe auch **Gruppentafel** heißt. Zum Beispiel bilden diejenigen Permutationen der Menge  $\{1, 2, 3\}$ , die nicht genau eines unserer drei Elemente festhalten, unter der Hintereinanderausführung eine

Gruppe mit der Gruppentafel

|         | 1       | $\zeta$ | $\eta$  |
|---------|---------|---------|---------|
| 1       | 1       | $\zeta$ | $\eta$  |
| $\zeta$ | $\zeta$ | $\eta$  | 1       |
| $\eta$  | $\eta$  | 1       | $\zeta$ |

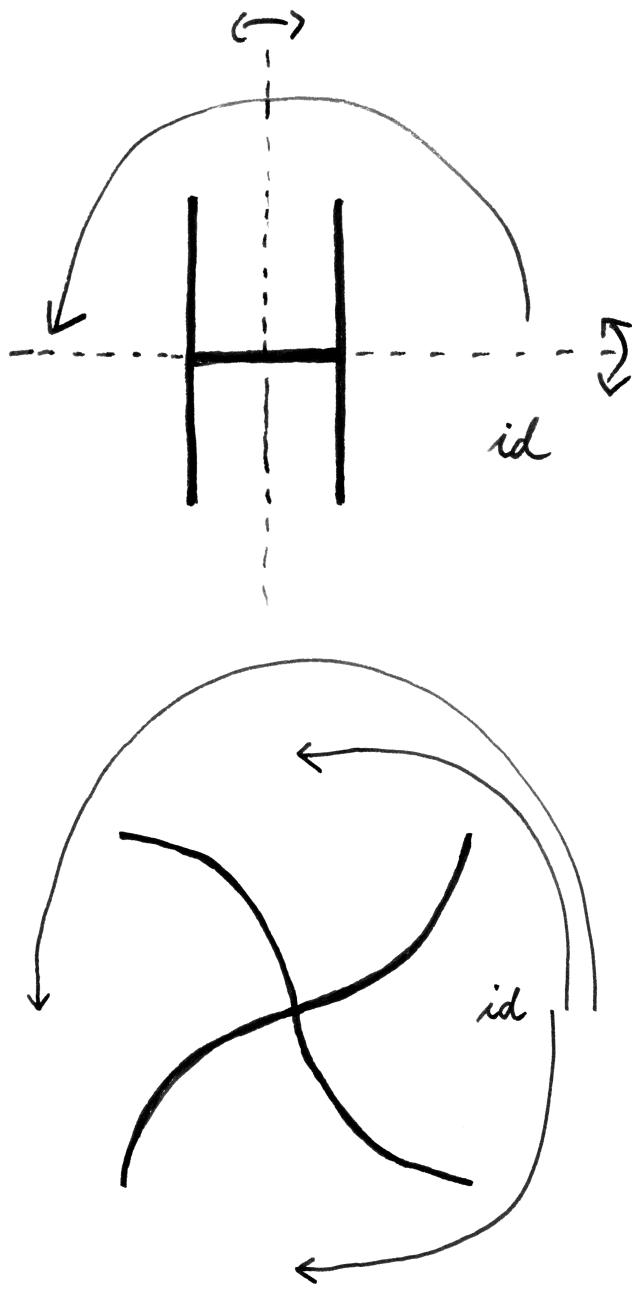
Bei einer Gruppentafel muß nach der Kürzungsregel 2.2.2.17 in jeder Spalte und in jeder Zeile jedes Element genau einmal vorkommen. Man sieht so recht leicht, daß jede weitere Gruppe  $G$  mit genau drei Elementen zu der durch die obige Verknüpfungstafel gegebenen Gruppe isomorph sein muß. Anschaulich denke ich mir diese Gruppe meist als die Gruppe aller Drehungen der Ebene, die ein gleichseitiges Dreieck in sich selbst überführen. Der Nachweis, daß es zwischen je zwei dreielementigen Gruppen genau zwei Isomorphismen gibt, sei dem Leser zur Übung überlassen.

*Beispiel 2.2.3.14 (Vierelementige Gruppen).* Man sieht durch die Untersuchung von Verknüpfungstafeln recht leicht, daß es bis auf Isomorphismus höchstens zwei vierelementige Magmas mit neutralem Element gibt, in denen die Kürzungsregeln gelten in dem Sinne, daß in jeder Zeile und Spalte der Verknüpfungstafel jedes Element genau einmal vorkommt. Durch Betrachtung der nebenstehenden Bilder oder Interpretation als spezielle Permutationen einer geeigneten endlichen Menge überzeugt man sich auch leicht, daß diese Magmas sogar Gruppen sind, die sich dadurch unterscheiden, ob jedes Element sein eigenes Inverses ist oder nicht. Sie heißen im ersten Fall die **Klein'sche Vierergruppe** und im zweiten Fall die **vier-elementige zyklische Gruppe**. Man mag zur Übung zeigen, daß es zwischen je zwei Klein'schen Vierergruppen genau sechs Isomorphismen gibt und zwischen zwei vierelementigen zyklischen Gruppen genau zwei Isomorphismen.

**Definition 2.2.3.15.** Eine Teilmenge eines Monoids heißt ein **Untermonoid**, wenn sie abgeschlossen ist unter der Verknüpfung und wenn sie zusätzlich das neutrale Element enthält.

**Definition 2.2.3.16.** Eine Teilmenge einer Gruppe heißt eine **Untergruppe**, wenn sie abgeschlossen ist unter der Verknüpfung und der Inversenbildung und wenn sie zusätzlich das neutrale Element enthält. Ist  $G$  eine multiplikativ geschriebene Gruppe, so ist eine Teilmenge  $U \subset G$  also eine Untergruppe genau dann, wenn in Formeln gilt:  $a, b \in U \Rightarrow ab \in U$ ,  $a \in U \Rightarrow a^{-1} \in U$  sowie  $1 \in U$ .

*Ergänzung 2.2.3.17 (Unter-was-auch-immer).* Die Begriffsbildungen eines Untermonoids und einer Untergruppe können als Spezialfälle eines allgemeineren Begriffsschemas verstanden werden. Danach wäre ein Untermonoid zu definieren



Die vier Symmetrien des Buchstabens H und des Sonnenrads, das wohl nicht zuletzt auch wegen seiner Symmetriegruppe so unvermittelt an furchtbare Zeiten der deutschen Geschichte erinnert.

als eine Teilmenge eines Monoids, die so mit einer Monoidstruktur versehen werden kann, daß die Einbettung ein Monoidhomomorphismus ist. Ebenso wäre eine Untergruppe zu definieren als eine Teilmenge einer Gruppe, die so mit einer Gruppenstruktur versehen werden kann, daß die Einbettung ein Gruppenhomomorphismus ist. Da diese Definitionen jedoch für Anwendungen erst aufgeschlüsselt werden müssen, haben ich die aufgeschlüsselten Fassungen als Definition genommen und überlasse den Nachweis der Äquivalenz zu den eben gegebenen Definitionen dem Leser zur Übung. Mehr dazu wird in 4.7.3.12 erklärt.

*Beispiele* 2.2.3.18. In jeder Gruppe ist die einelementige Teilmenge, die nur aus dem neutralen Element besteht, eine Untergruppe. Wir nennen sie die **triviale Untergruppe**. Ebenso ist natürlich die ganze Gruppe stets eine Untergruppe von sich selber. Unsere kleinen Gruppen von eben lassen sich formal gut beschreiben als Untergruppen von Permutationsgruppen. Stellt man eine Permutation  $\sigma$  der Menge  $\{1, 2, \dots, n\}$  dar, indem man  $\sigma(1)\sigma(2)\dots\sigma(n)$  hintereinander schreibt – bei  $n \leq 9$  mag das angehen – so ist unsere dreielementige Gruppe die Untergruppe  $\{123, 231, 312\}$  der entsprechenden Permutationsgruppe, oder ganz pedantisch isomorph dazu, unsere Klein'sche Vieregruppe die Untergruppe  $\{1234, 2143, 4321, 3412\}$  der entsprechenden Permutationsgruppe und unsere vierelementige zyklische Gruppe die Untergruppe  $\{1234, 4123, 3412, 2341\}$ .

*Ergänzung* 2.2.3.19. Eine Menge mit einer assoziativen Verknüpfung heißt auch **Halbgruppe**. Gegeben Halbgruppen  $A$  und  $B$  schreiben wir  $\text{Halb}(A, B)$  statt  $\text{Mag}(A, B)$  für die Menge aller mit der Verknüpfung verträglichen Abbildungen von  $A$  nach  $B$ , als da heißt, aller **Halbgruppenhomomorphismen**. Wieder hat diese Notation den Vorteil, uns daran zu erinnern, daß wir es mit Halbgruppen zu tun haben. Für jede Halbgruppe  $A$  liefert die Vorschrift  $\varphi \mapsto \varphi(1)$  eine Bijektion

$$\text{Halb}(\mathbb{N}_{\geq 1}, A) \xrightarrow{\sim} A$$

Hierbei fassen wir  $\mathbb{N}_{\geq 1}$  mittels der Addition als Halbgruppe auf. Ein formaler Beweis muß auf eine formale Definition der natürlichen Zahlen warten und ist in 3.4.1.5 enthalten.

*Ergänzung* 2.2.3.20. Betrachten wir die Menge  $\mathbb{M}$  „aller möglichen Klammerungen von einem oder mehr Symbolen“ im Sinne von 2.2.1.13 und darauf die durch „Hintereinanderschreiben“ erklärte Verknüpfung sowie das Element  $*$   $\in \mathbb{M}$ , das die einzige mögliche Verkammerung von einem einzigen Symbol meint, so liefert für jedes Magma  $X$  die Vorschrift  $\varphi \mapsto \varphi(*)$  eine Bijektion

$$\text{Mag}(\mathbb{M}, X) \xrightarrow{\sim} X$$

## Übungen

*Übung 2.2.3.21 (Injektivität und Kern).* Gegeben ein Gruppenhomomorphismus oder allgemeiner ein Monoidhomomorphismus  $\varphi : G \rightarrow H$  erklärt man den **Kern von  $\varphi$**  als das Urbild des neutralen Elements, in Formeln

$$\ker \varphi := \{g \in G \mid \varphi(g) = e\}$$

Man zeige, daß  $\ker \varphi$  stets eine Untergruppe beziehungsweise ein Untermonoid von  $G$  ist. Man zeige weiter, daß im Gruppenfall  $\varphi$  genau dann injektiv ist, wenn sein Kern nur aus dem neutralen Element besteht.

*Übung 2.2.3.22.* Das Bild eines Monoids unter einem Monoidhomomorphismus ist stets ein Untermonoid. Das Urbild eines Untermonoids unter einem Monoidhomomorphismus ist stets ein Untermonoid.

*Übung 2.2.3.23.* Jeder Monoidhomomorphismus  $M \rightarrow N$  bildet invertierbare Elemente auf invertierbare Elemente ab und induziert so einen Gruppenhomomorphismus  $M^\times \rightarrow N^\times$ .

*Übung 2.2.3.24.* Das Bild einer Untergruppe unter einem Gruppenhomomorphismus ist stets eine Untergruppe. Das Urbild einer Untergruppe unter einem Gruppenhomomorphismus ist stets eine Untergruppe.

*Übung 2.2.3.25.* Gegeben eine Menge  $Z$  ist das Bilden des Komplements ein Monoidhomomorphismus  $(\mathcal{P}(Z), \cap) \rightarrow (\mathcal{P}(Z), \cup)$ .

*Übung 2.2.3.26.* Die Multiplikation mit 5 ist ein Gruppenhomomorphismus von additiven Gruppen  $(5 \cdot) : \mathbb{Z} \rightarrow \mathbb{Z}$ .

*Übung 2.2.3.27 (Induzierte Verknüpfung).* Sei  $(X, \top)$  eine Menge mit Verknüpfung. Gegeben eine Injektion  $U \hookrightarrow X$  gibt es höchstens eine Verknüpfung auf  $U$  derart, daß unsere Injektion ein Homomorphismus ist. Wenn es solch eine Verknüpfung gibt, heißt unsere Injektion **an die Verknüpfung angepaßt** und die fragliche Verknüpfung auf  $U$  die **auf  $U$  induzierte Verknüpfung**. Die Einbettung einer Teilmenge ist genau dann angepaßt, wenn unsere Teilmenge abgeschlossen ist unter der Verknüpfung im Sinne von 2.2.1.6. Die Eigenschaften der Assoziativität und Kommutativität übertragen sich auf die induzierte Verknüpfung.

*Übung 2.2.3.28 (Koinduzierte Verknüpfung).* Sei  $(X, \top)$  eine Menge mit Verknüpfung. Gegeben eine Surjektion  $X \twoheadrightarrow Q$  gibt es höchstens eine Verknüpfung auf  $Q$  derart, daß unsere Surjektion ein Homomorphismus ist. Wenn es solch eine Verknüpfung gibt, heißt unsere Surjektion **an die Verknüpfung angepaßt** und die fragliche Verknüpfung auf  $Q$  die **auf  $Q$  koinduzierte Verknüpfung**. Zum Beispiel ist die Surjektion  $\mathbb{N} \twoheadrightarrow \{0, 1, \dots, 9\}$ , die jeder Zahl die letzte Ziffer ihrer Dezimaldarstellung zuordnet, angepaßt sowohl an die Addition als auch an die Multiplikation. Mehr dazu in 3.5.2.4.

*Übung 2.2.3.29 (Eigenschaften einer koinduzierten Verknüpfung).* Die Eigenschaften der Assoziativität und Kommutativität übertragen sich auf die koindizierte Verknüpfung. Das Bild des Einselementes ist ein Einselement für die koindizierte Verknüpfung, das Bild des Inversen ein Inverses. Jede koindizierte Verknüpfung zu einer angepaßten Surjektion von einer Gruppe auf eine Menge macht besagte Menge zu einer Gruppe.

*Ergänzende Übung 2.2.3.30 (Universelle Eigenschaft der natürlichen Zahlen).* Man zeige, daß für jedes Monoid  $M$  die Vorschrift  $\varphi \mapsto \varphi(1)$  eine Bijektion

$$\text{Mon}(\mathbb{N}, M) \xrightarrow{\sim} M$$

liefert. Ein Monoidhomomorphismus vom additiven Monoid der natürlichen Zahlen in ein beliebiges weiteres Monoid ist also in Worten festgelegt und festlegbar durch das Bild des Elements  $1 \in \mathbb{N}$ . Hinweis: Man erinnere 2.2.1.24. Wenn man es ganz genau nimmt, muß man für diese Übung die formale Einführung der natürlichen Zahlen 3.4.1.5 abwarten.

*Übung 2.2.3.31 (Universelle Eigenschaft der ganzen Zahlen).* Man zeige, daß für jede Gruppe  $G$  die Vorschrift  $\varphi \mapsto \varphi(1)$  eine Bijektion

$$\text{Grp}(\mathbb{Z}, G) \xrightarrow{\sim} G$$

liefert. Ein Gruppenhomomorphismus von der additiven Gruppe der ganzen Zahlen in irgendeine weitere Gruppe ist also in Worten festgelegt und festlegbar durch das Bild des Elements  $1 \in \mathbb{Z}$ . Hinweis: Man erinnere 2.2.2.12. Man beachte, daß die 1 nicht das neutrale Element der Gruppe  $\mathbb{Z}$  meint, die hier vielmehr als additive Gruppe zu verstehen ist. Man gebe explizit den Gruppenhomomorphismus  $\mathbb{Z} \rightarrow \mathbb{Z}$  mit  $1 \mapsto 5$  an. Man gebe explizit den Gruppenhomomorphismus  $\mathbb{Z} \rightarrow \mathbb{Q} \setminus \{0\}$  mit  $1 \mapsto 5$  an. Wenn man es ganz genau nehmen will, muß man für diese Übung die formale Einführung der ganzen Zahlen 3.4.2.12 abwarten.

*Übung 2.2.3.32.* Jeder Gruppenhomomorphismus  $\varphi : G \rightarrow H$  vertauscht mit Inversenbildung, in Formeln  $\varphi(a^{-1}) = (\varphi(a))^{-1} \forall a \in G$ .

*Ergänzende Übung 2.2.3.33.* Gegeben eine Verknüpfung  $X \times X \rightarrow X$ ,  $(x, y) \mapsto xy$  auf einer Menge  $X$  erklärt man die **opponierte Verknüpfung** durch die Vorschrift  $(x, y) \mapsto yx$ . Oft schreibt man auch  $X^{\text{opp}}$  für die Menge  $X$ , versehen mit der opponierten Verknüpfung, und  $x^\circ$  für das Element  $x \in X$ , aufgefaßt als Element von  $X^{\text{opp}}$ . Das hat den Vorteil, daß man sich das Verknüpfungssymbol sparen kann, die Definition der opponierten Verknüpfung läßt sich schreiben als  $y^\circ x^\circ := (xy)^\circ$ . Man zeige: Gegeben eine Gruppe  $G$  liefert das Bilden des Inversen stets einen Gruppenisomorphismus  $G^{\text{opp}} \xrightarrow{\sim} G$ ,  $g^\circ \mapsto g^{-1}$  zwischen der **opponierten Gruppe** und der ursprünglichen Gruppe.

*Ergänzende Übung 2.2.3.34.* Jede Halbgruppe  $A$  kann man zu einem Monoid  $\tilde{A}$  erweitern, indem man noch ein Element hinzunimmt und ihm die Rolle des neutralen Elements zuweist. Für jedes weitere Monoid  $M$  liefert dann das Vorschalten der Einbettung  $A \hookrightarrow \tilde{A}$  eine Bijektion

$$\text{Mon}(\tilde{A}, M) \xrightarrow{\sim} \text{Halb}(A, M)$$

*Übung 2.2.3.35.* Eine Abbildung  $\varphi : G \rightarrow H$  von Gruppen ist genau dann ein Gruppenhomomorphismus, wenn ihr Graph  $\Gamma(\varphi) \subset G \times H$  eine Untergruppe des Produkts ist.

*Übung 2.2.3.36.* Jede Verknüpfung von Homomorphismen von Magmas ist wieder ein Homomorphismus von Magmas. Sind also in Formeln  $g : U \rightarrow V$  und  $f : V \rightarrow W$  Homomorphismen, so ist auch  $f \circ g : U \rightarrow W$  ein Homomorphismus.

*Übung 2.2.3.37.* Gegeben ein surjektiver Homomorphismus  $g : U \twoheadrightarrow V$  von Magmas und eine Abbildung  $f : V \rightarrow W$  in ein weiteres Magma ist  $f$  genau dann ein Homomorphismus, wenn die Verknüpfung  $f \circ g : U \rightarrow W$  ein Homomorphismus ist. Gegeben ein injektiver Homomorphismus von Magmas  $f : V \hookrightarrow W$  und eine Abbildung  $g : U \twoheadrightarrow V$  von einem weiteren Magma nach  $V$  ist  $g$  genau dann ein Homomorphismus, wenn die Verknüpfung  $f \circ g : U \rightarrow W$  ein Homomorphismus ist.

## 2.2.4 Körper im Sinne der Algebra

2.2.4.1. Die algebraische Struktur eines Körpers wird den Hauptbestandteil unseres Axiomensystems für die reellen Zahlen in ?? bilden. Gleichzeitig bildet sie die Grundlage für die Modellierung des Raums unserer Anschauung in der linearen Algebra.

**Definition 2.2.4.2.** Ein **Körper**  $(K, +, \cdot)$  (englisch **field**, französisch **corps**) ist eine Menge  $K$  mit zwei kommutativen assoziativen Verknüpfungen, genannt die **Addition**  $+$  und die **Multiplikation**  $\cdot$  des Körpers, derart daß die folgenden drei Bedingungen erfüllt sind:

1.  $(K, +)$  ist eine Gruppe, die **additive Gruppe** des Körpers;
2. Die vom neutralen Element der Addition  $0_K \in K$  verschiedenen Elemente von  $K$  bilden eine unter der Multiplikation abgeschlossene Teilmenge, und diese Teilmenge  $K \setminus \{0_K\}$  ist unter der Multiplikation ihrerseits eine Gruppe, die **multiplikative Gruppe** des Körpers;

### 3. Es gilt das **Distributivgesetz**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \forall a, b, c \in K$$

*Beispiele 2.2.4.3.* Ein erstes Beispiel ist der Körper der rationalen Zahlen  $(\mathbb{Q}, +, \cdot)$ . Ein anderes Beispiel ist der zweielementige Körper mit den durch die Axiome erzwungenen Rechenregeln, der fundamental ist in der Informatik. Die ganzen Zahlen  $(\mathbb{Z}, +, \cdot)$  bilden keinen Körper, da  $(\mathbb{Z} \setminus \{0\}, \cdot)$  keine Gruppe ist, da es nämlich in  $\mathbb{Z} \setminus \{0\}$  nur für 1 und  $-1$  ein multiplikatives Inverses gibt. Es gibt keinen einelementigen Körper, da das Komplement seines Nullelements die leere Menge sein müßte: Dies Komplement kann dann aber unter der Multiplikation keine Gruppe sein, da es kein neutrales Element haben könnte.

*Ergänzung 2.2.4.4 (Ursprung der Terminologie).* Der Begriff „Körper“ ist in diesem Zusammenhang wohl zu verstehen als „besonders gut unter den verschiedenen Rechenoperationen abgeschlossener Zahlbereich“, in Analogie zu geometrischen Körpern wie Kugeln oder Zylindern, die man entsprechend als „besonders gut in sich geschlossene Bereiche des Raums“ ansehen könnte. Die Bezeichnung als „Distributivgesetz“ röhrt daher, daß uns dieses Gesetz erlaubt, beim Multiplizieren eines Elements mit einer Summe den „Faktor auf die Summanden zu verteilen“. Das Wort „distribution“ für Verteilung von Nahrungsmitteln und dergleichen auf Französisch und Englisch kommt von demselben lateinischen Wortstamm, auf die auch unsere Bezeichnung „Distributivgesetz“ zurückgeht.

**2.2.4.5 (Weglassen von Multiplikationssymbolen).** Beim Rechnen mit Buchstaben werden wir meist  $ab := a \cdot b$  abkürzen. Das wäre beim Rechnen mit durch Ziffernfolgen dargestellten Zahlen wenig sinnvoll, da man dann nicht wissen könnte, ob 72 nun als „Zweiundsiebzig“ oder vielmehr als „Sieben mal Zwei“ zu verstehen sein soll. Beim Einsetzen von Zahlen für die Buchstaben müssen also wieder Multiplikationssymbole eingefügt werden.

*Ergänzung 2.2.4.6 (Weglassen von Additionssymbolen).* In der Schule und außerhalb der Mathematik ist es üblich,  $1 + \frac{1}{2}$  mit  $1\frac{1}{2}$  abzukürzen und „Anderthalb Stunden“ zu sagen oder „Dreieinviertel Pfund“. In diesem Fall wird also ein Additionssymbol weggelassen. Das ist jedoch in der höheren Mathematik nicht üblich. In der gesprochenen Sprache ist es ja noch viel merkwürdiger: Neunzehnhundertvierundachtzig versteht jeder, in Symbolen geschrieben sieht  $9\ 10\ 100\ 4 + 80$  dahingegen ziemlich sinnlos aus, und statt der üblichen Interpretation  $((9+10)100)+4+80$  wären durchaus auch andere Interpretationen denkbar. In der gesprochenen Sprache scheint eher eine Konvention befolgt zu werden, nach der die Operationen der Reihe nach auszuführen sind wie bei einem Taschenrechner, wobei eine Multiplikation gemeint ist, wenn die zuerst genannte Zahl die kleinere ist, und eine Addition, wenn sie die Größere ist. Nur die Zahlen von 13 bis

19 scheinen dieser Regel nicht zu gehorchen. Kein Wunder, daß es Erstklässlern schwer fällt, sich den Zahlenraum zu erschließen, wenn sie zuvor dieses Dickicht von Konventionen durchdringen müssen.

**2.2.4.7 (Punkt vor Strich).** Wir vereinbaren zur Vermeidung von Klammern die Regel „Punkt vor Strich“, so daß also zum Beispiel unter zusätzlicher Beachtung unserer Konvention des Weglassens von Multiplikationssymbolen, in diesem Fall das Weglassen des Punktes, das Distributivgesetz kürzer in der Form  $a(b + c) = ab + ac$  geschrieben werden kann.

**2.2.4.8 (Multiplikation mit Null).** In jedem Körper  $K$  gilt  $a0_K = 0_K \quad \forall a \in K$ . Man folgert das aus  $a0_K + a0_K = a(0_K + 0_K) = a0_K$  durch Hinzuaddieren von  $-(a0_K)$  auf beiden Seiten. Für das neutrale Element der multiplikativen Gruppe des Körpers vereinbaren wir die Bezeichnung  $1_K$ . Nach dem Vorhergehenden gilt  $1_K b = b$  auch für  $b = 0_K$ , mithin für alle  $b \in K$ . Folglich ist  $(K, \cdot)$  ein Monoid mit neutralem Element  $1_K$  und der Menge aller von Null verschiedenen Elemente als Gruppe der invertierbaren Elementen, in Formeln  $K \setminus \{0_K\} = K^\times$ .

**2.2.4.9 (Binomische Formel).** Für alle  $a, b$  in einem Körper  $K$  und alle  $n \geq 0$  gilt die binomische Formel

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

Um das einzusehen prüft man, daß wir bei der Herleitung nach 1.1.1.23 nur Körperiaksiome verwandt haben. Man beachte hierbei unsere Konvention  $0_K^0 = 1_K$  aus 2.2.1.25, angewandt auf das Monoid  $(K, \cdot)$ . Die Multiplikation mit den Binomialkoeffizienten in dieser Formel ist zu verstehen als wiederholte Addition im Sinne der Bezeichnungskonvention  $na$  aus 2.2.1.16, angewandt auf den Spezialfall der additiven Gruppe unseres Körpers.

**Lemma 2.2.4.10 (Folgerungen aus den Körperaxiomen).** *In jedem Körper  $K$  gelten die folgenden Aussagen und Formeln:*

1.  $ab = 0_K \Rightarrow (a = 0_K \text{ oder } b = 0_K);$
2.  $-a = (-1_K)a \quad \forall a \in K;$
3.  $(-1_K)(-1_K) = 1_K;$
4.  $(-a)(-b) = ab \quad \forall a, b \in K;$
5.  $\frac{a}{b} \frac{c}{d} = \frac{ac}{bd} \text{ für alle } a, c \in K \text{ und } b, d \in K^\times;$
6.  $\frac{ac}{bc} = \frac{a}{b} \text{ für alle } a \in K \text{ und } b, c \in K^\times;$
7.  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ für alle } a, c \in K \text{ und } b, d \in K^\times;$
8.  $m(ab) = (ma)b \text{ für alle } m \in \mathbb{Z} \text{ und } a, b \in K.$

*Beweis.* 1. In der Tat folgt aus  $(a \neq 0_K \text{ und } b \neq 0_K)$  schon  $(ab \neq 0_K)$  nach den Körperaxiomen.

2. In der Tat gilt  $a + (-1_K)a = 1_Ka + (-1_K)a = (1_K + (-1_K))a = 0_Ka = 0_K$ , und  $-a$  ist ja gerade definiert als das eindeutig bestimmte Element von  $K$  mit der Eigenschaft  $a + (-a) = 0_K$ .
3. In der Tat gilt nach dem Vorhergehenden  $(-1_K)(-1_K) = -(-1_K) = 1_K$ .
4. Um das nachzuweisen ersetzen wir einfach  $(-a) = (-1_K)a$  und  $(-b) = (-1_K)b$  und verwenden  $(-1_K)(-1_K) = 1_K$ .
5. Das ist klar.
6. Das ist klar.
7. Das wird bewiesen, indem man die Brüche auf einen Hauptnenner bringt und das Distributivgesetz anwendet.
8. Das folgt durch wiederholtes Anwenden des Distributivgesetzes.

□

**2.2.4.11 (Minus mal Minus gibt Plus).** Die Frage, wie das Produkt zweier negativer Zahlen zu bilden sei, war lange umstritten. Mir scheint der vorhergehende Beweis das überzeugendste Argument für „Minus mal Minus gibt Plus“: Es sagt salopp gesprochen, daß man diese Regel vereinbaren muß, wenn man beim Rechnen das Ausklammern ohne alle Einschränkungen erlauben will.

**2.2.4.12 (Ganze Zahlen und allgemeine Körper).** Für jeden Körper  $K$  und  $n \in \mathbb{Z}$  setzen wir  $n_K := n^+1_K = n1_K$  in unserer Notation 2.2.2.11 beziehungsweise ihrer für additiv notierte Monoide vereinbarten Abkürzung. Für  $n \in \mathbb{N}$  bedeutet das explizit  $n_K := 1_K + \dots + 1_K$  mit  $n$  Summanden. Nach der ersten Iterationsregel in 2.2.2.12 gilt stets  $(n+m)_K = n_K + m_K$  und aus dem Distributivgesetz folgt leicht  $n_K \cdot a = n^+a$  oder abgekürzt  $n_K a = na$  für alle  $n \in \mathbb{Z}$  und  $a \in K$ . Mit der zweiten Iterationsregel in 2.2.2.12 folgt weiter für alle  $m, n \in \mathbb{Z}$  die Identität  $n_K m_K = (nm)_K$  über die Gleichungskette

$$n_K \cdot m_K = n^+m_K = n^+(m^+1_K) = (nm)^+1_K = (nm)_K$$

Oft schreibt man deshalb kurz  $n$ , wenn eigentlich  $n_K$  gemeint ist, und insbesondere kürzt man eigentlich immer  $0_K$  ab durch 0 und  $1_K$  durch 1. Man beachte jedoch, daß für verschiedene ganze Zahlen  $n \neq m$  durchaus  $n_K = m_K$  gelten kann: Ist etwa  $K$  ein Körper mit zwei Elementen, so gilt  $n_K = 0_K$  für gerades  $n$  und  $n_K = 1_K$  für ungerades  $n$ . Vom höheren Standpunkt wird das alles noch einmal in 3.5.1.11 ausführlicher diskutiert werden.

*Ergänzung 2.2.4.13.* Den Begriff eines Homomorphismus verwendet man bei Mengen mit mehr als einer Verknüpfung analog. Zum Beispiel ist ein **Körperhomomorphismus**  $\varphi$  von einem Körper  $K$  in einen Körper  $L$  definiert als eine Abbildung  $\varphi : K \rightarrow L$  derart, daß gilt  $\varphi(a+b) = \varphi(a)+\varphi(b)$  und  $\varphi(ab) = \varphi(a)\varphi(b)$  für alle  $a, b \in K$  sowie  $\varphi(1) = 1$ . Die Bedingung  $\varphi(1) = 1$  ist nur nötig, um den Fall der Nullabbildung auszuschließen. In anderen Worten mag man einen Körperhomomorphismus auch definieren als eine Abbildung, die sowohl für die Addition als auch für die Multiplikation ein Monoidhomomorphismus ist. Unter einem **Körperisomorphismus** verstehen wir wieder einen Körperhomomorphismus  $\phi$  mit der Eigenschaft, daß es einen Körperhomomorphismus  $\psi$  in die Gegenrichtung gibt mit  $\phi \circ \psi = \text{id}$  und  $\psi \circ \phi = \text{id}$ . Wieder ist jeder bijektive Körperhomomorphismus bereits ein Körperisomorphismus.

## Übungen

*Übung 2.2.4.14.* Ist  $K$  ein Körper derart, daß es kein  $x \in K$  gibt mit  $x^2 = -1$ , so kann man die Menge  $K \times K = K^2$  zu einem Körper machen, indem man die Addition und Multiplikation definiert durch

$$\begin{aligned} (a, b) + (c, d) &:= (a+c, b+d) \\ (a, b) \cdot (c, d) &:= (ac - bd, ad + bc) \end{aligned}$$

Die Abbildung  $K \rightarrow K^2$ ,  $a \mapsto (a, 0)$  ist dann ein Körperhomomorphismus. Kürzen wir  $(a, 0)$  mit  $a$  ab und setzen  $(0, 1) = i$ , so gilt  $i^2 = -1$  und  $(a, b) = a + bi$  und die Abbildung  $a + bi \mapsto a - bi$  ist ein Körperisomorphismus  $K^2 \xrightarrow{\sim} K^2$ .

2.2.4.15. Auf die in der vorhergehenden Übung 2.2.4.14 erklärte Weise können wir etwa aus dem Körper  $K = \mathbb{R}$  der „reellen Zahlen“, sobald wir ihn kennengelernt haben, direkt den Körper  $\mathbb{C}$  der **komplexen Zahlen** konstruieren. Unser Körperisomorphismus gegeben durch die Vorschrift  $a + bi \mapsto a - bi$  heißt in diesem Fall die **komplexe Konjugation** und wird auch  $z \mapsto \bar{z}$  notiert. Man beachte, wie mühelos das alles in der Sprache der Mengenlehre zu machen ist. Als die komplexen Zahlen erfunden wurden, gab es noch keine Mengenlehre und beim Rechnen beschränkte man sich auf das Rechnen mit „reellen“ Zahlen, ja selbst das Multiplizieren zweier negativer Zahlen wurde als eine fragwürdige Operation angesehen, und das Ziehen einer Quadratwurzel aus einer negativen Zahl als eine rein imaginäre Operation. In gewisser Weise ist es das ja auch geblieben, aber die Mengenlehre liefert eben unserer Imagination eine wunderbar präzise Sprache, in der wir uns auch über imaginierte Dinge unmißverständlich austauschen können. Man kann dieselbe Konstruktion auch allgemeiner durchführen, wenn man statt  $-1$  irgendein anderes Element eines Körpers  $K$  betrachtet, das kein Quadrat ist. Noch allgemeinere Konstruktionen zur „Adjunktion höherer Wurzeln“ oder sogar der „Adjunktion von Nullstellen polynomiauer Gleichungen“ können Sie in der Algebra kennenlernen, vergleiche etwa [??](#). In 3.2.7 diskutieren wir die komplexen Zahlen ausführlicher.

*Ergänzende Übung 2.2.4.16.* Ein Körperhomomorphismus ist stets injektiv.

## 2.2.5 Aufbau des Zahlensystems\*

### 2.2.5.1. Der Aufbau des Zahlensystems

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

erscheint in diesem Text nur in einer Abfolge von Nebenbemerkungen und soll an dieser Stelle zusammenfassend dargestellt werden.

1. Die Konstruktion der natürlichen Zahlen  $\mathbb{N}$  aus Grundbegriffen der Mengenlehre diskutiere ich in 3.4.1.5. Kurz wurde das auch schon in 2.1.6.11 angerissen. Eine vollständig überzeugende Diskussion dieser Struktur ist meines Erachtens nur im Rahmen der Logik möglich.
2. Die Konstruktion der ganzen Zahlen  $\mathbb{Z}$  aus den natürlichen Zahlen  $\mathbb{N}$ , ja der einhüllenden Gruppe eines beliebigen kommutativen Monoids wird in 3.4.2.12 erklärt. Nach [??](#) gibt es dann genau eine Multiplikation auf  $\mathbb{Z}$ , die unsere Multiplikation auf  $\mathbb{N}$  fortsetzt und  $\mathbb{Z}$  zu einem Ring macht.
3. Die Konstruktion des Körpers der rationalen Zahlen  $\mathbb{Q}$  aus dem Integritätsbereich der ganzen Zahlen  $\mathbb{Z}$ , ja des Quotientenkörpers eines beliebigen

kommutativen Integritätsbereichs wird in 3.5.5.2 ausgeführt. Die Anordnung auf  $\mathbb{Q}$  dürfen Sie selbst in 3.5.5.19 konstruieren.

4. Die Konstruktion des angeordneten Körpers der reellen Zahlen  $\mathbb{R}$  aus dem angeordneten Körper der rationalen Zahlen  $\mathbb{Q}$  wird zur Beginn der Analysis in ?? erklärt.
5. Die Konstruktion des Körpers der komplexen Zahlen  $\mathbb{C}$  aus dem Körper der reellen Zahlen  $\mathbb{R}$  wurde in 2.2.4.14 angerissen und wird in 3.2.7 ausführlicher behandelt.

**2.2.5.2 (Gewinne und Verluste beim Aufbau des Zahlensystems).** Oft wird der Aufbau des Zahlensystems als eine Geschichte immer neuer Gewinne erzählt: Beim Übergang von  $\mathbb{N}$  zu  $\mathbb{Z}$  gewinnt man die Lösbarkeit aller Gleichungen des Typs  $a + x = b$ , beim Übergang von  $\mathbb{Z}$  zu  $\mathbb{Q}$  die Lösbarkeit aller Gleichungen des Typs  $ax = b$  für  $a \neq 0$ , beim Übergang von  $\mathbb{Q}$  zu  $\mathbb{R}$  die Lösbarkeit aller Gleichungen des Typs  $x^a = b$  für  $a, b > 0$ , und nach Übergang von  $\mathbb{R}$  zu  $\mathbb{C}$  besitzen sogar alle nichtkonstanten Polynome Nullstellen. Hier ist nur anzumerken, daß man die Lösbarkeit aller Gleichungen des Typs  $x^a = b$  für  $a, b > 0$  auch schon in einem abzählbaren Unterkörper von  $\mathbb{R}$  erreichen könnte und daß der eigentliche Grund für den Übergang zu  $\mathbb{R}$  analytischer Natur ist: Man gewinnt so den Zwischenwertsatz ?. Man kann den Aufbau des Zahlensystems aber auch als eine Geschichte immer neuer Verluste erzählen: Beim Übergang von  $\mathbb{N}$  zu  $\mathbb{Z}$  verliert man die Existenz eines kleinsten Elements, beim Übergang von  $\mathbb{Z}$  zu  $\mathbb{Q}$  die Existenz unmittelbarer Nachfolger, beim Übergang von  $\mathbb{Q}$  zu  $\mathbb{R}$  die Abzählbarkeit, und beim Übergang von  $\mathbb{R}$  zu  $\mathbb{C}$  die Anordnung. Man kann noch weiter gehen zum Schiefkörper der sogenannten Quaternionen  $\mathbb{H} \supset \mathbb{C}$  aus 3.5.6.3, dabei verliert man die Kommutativität der Multiplikation, oder sogar zu den sogenannten Oktaven  $\mathbb{O} \supset \mathbb{H}$  aus ??, bei denen die Multiplikation nicht einmal mehr assoziativ ist.

## 2.2.6 Verbände und Boole'sche Algebren\*

**Definition 2.2.6.1.** Eine **Boole'sche Algebra** ist ein Tripel  $(B, \wedge, \vee)$  bestehend aus einer Menge mit zwei assoziativen kommutativen Verknüpfungen derart, daß gilt:

1. Mit jeder unserer Verknüpfungen wird  $B$  ein Monoid. Man notiert 1 das neutrale Element zu  $\wedge$  und 0 das neutrale Element zu  $\vee$ ;
2. Jede unserer beiden Verknüpfungen ist „distributiv über der anderen“, in Formeln  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$  und  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ;

3. Zu jedem  $a \in B$  existiert  $c \in B$  mit  $a \wedge c = 0$  und  $a \vee c = 1$ . Man zeigt mühelos, daß dies Element  $c$  durch  $a$  eindeutig bestimmt ist, und notiert es  $c = \neg a$  oder  $c = \bar{a}$ .

Ein **Homomorphismus von Boole'schen Algebren** ist eine Abbildung, die für beide Monoidstrukturen ein Homomorphismus von Monoiden ist. Gegeben Boole'sche Algebren  $B, C$  notieren wir  $\text{Boole}(B, C)$  die Menge aller Homomorphismen von  $B$  nach  $C$ .

2.2.6.2. Ein typisches Beispiel einer Boole'schen Algebra erhält man, indem man für eine beliebige Menge  $X$  das Tripel  $(\text{Pot}(X), \cap, \cup)$  bestehend aus ihrer Potenzmenge mit den Operationen Schnitt und Vereinigung betrachtet. In dieser Situation haben wir  $1 = X$  sowie  $0 = \emptyset$  und  $\neg A = X \setminus A$  ist die Komplementmenge.

**Definition 2.2.6.3.** Ein **Verband** ist ein Tripel  $(B, \wedge, \vee)$  bestehend aus einer Menge mit zwei assoziativen kommutativen Verknüpfungen derart, daß die **Absorptionsgesetze**  $a \wedge (a \vee b) = a$  und  $a \vee (a \wedge b) = a$  gelten für alle  $a, b \in B$ .

*Beispiel 2.2.6.4.* Als Übung 2.2.6.7 dürfen Sie zeigen, daß jede Boole'sche Algebra ein Verband ist.

*Vorschau 2.2.6.5.* Wir werden in ?? sehen, daß eine teilgeordnete Menge, in der jede zweielementige Teilmenge ein Supremum und ein Infimum hat, zu einem Verband wird, wenn wir  $a \vee b := \sup\{a, b\}$  und  $a \wedge b := \inf\{a, b\}$  setzen, und daß wir so genau alle Verbände erhalten.

## Übungen

*Übung 2.2.6.6.* Man zeige für jedes Element  $a$  einer Boole'schen Algebra die Identitäten  $a \wedge 0 = 0$  und  $a \vee 1 = 1$ . Hinweis: Man gehe von  $1 = a \vee (\bar{a} \wedge 1)$  aus und verwende Distributivität.

*Übung 2.2.6.7.* Man zeige, daß jede Boole'sche Algebra ein Verband ist. Hinweis: Man gehe von  $(b \wedge 0) \vee a = a$  nach 2.2.6.6 aus und verwende die Distributivität.

*Übung 2.2.6.8.* Man zeige für jedes Element  $a$  eines Verbandes  $a \wedge a = a$  und  $a \vee a = a$ . Hinweis: Absorptionsgesetze mit  $b = a \wedge a$  oder  $b = a \vee a$ .

## 2.3 Zur Darstellung von Mathematik\*

### 2.3.1 Herkunft einiger Symbole

2.3.1.1. Ich habe versucht, etwas über die Herkunft einiger mathematischer Symbole in Erfahrung zu bringen, die schon aus der Schule selbstverständlich sind.

2.3.1.2. Das Pluszeichen + ist wohl ein Auschnitt aus dem Symbol &, das hinwie-derum entstanden ist durch Zusammenziehen der beiden Buchstaben im Wörtchen „et“, lateinisch für „und“.

2.3.1.3. Die Dezimaldarstellung der natürlichen Zahlen kam Mitte des vorigen Jahrtausends aus Indien über die Araber nach Italien. Bis dahin rechnete man in Europa in römischer Notation. Sie müssen nur versuchen, in dieser Notation zwei größere Zahlen zu multiplizieren, um zu ermessen, welchen wissenschaftlichen und auch wirtschaftlichen Fortschritt der Übergang zur Dezimaldarstellung bedeutete. Das Beispiel der Dezimaldarstellung zeigt in meinen Augen auch, wie entscheidend das sorgfältige Einbeziehen trivialer Spezialfälle, manchmal als „Theorie der leeren Menge“ verspottet, für die Eleganz der Darstellung mathematischer Sachverhalte sein kann: Sie wurde ja eben dadurch erst ermöglicht, daß man ein eigenes Symbol für „gar nichts“ erfand! Ich denke, daß der Aufbau eines effizienten Notationssystems, obwohl er natürlich nicht denselben Stellenwert einnehmen kann wie die Entwicklung mathematischer Inhalte, dennoch in der Lehre ein wichtiges Ziel sein muß. In diesem Text habe ich mir die größte Mühe gegeben, unter den gebräuchlichen Notationen diejenigen auszuwählen, die mir am sinnvollsten schienen, und sie soweit wie möglich aufzuschlüsseln. Wo es mir sinnvoll schien, habe ich auch nicht gezögert, neue Notationen einzuführen.

2.3.1.4. Das Wort von der „Theorie der leeren Menge“ scheint auf Carl Ludwig Siegel zurückzugehen, der einmal gesagt haben soll: „Ich habe Angst, dass die Mathematik vor dem Ende des Jahrhunderts zugrunde geht, wenn dem Trend nach sinnloser Abstraktion – die Theorie der leeren Menge, wie ich es nenne – nicht Einhalt geboten wird“.

2.3.1.5. Die Herkunft der logischen Symbole  $\exists$  und  $\forall$  als umgedrehte E und A haben wir bereits in 2.1.7.4 erwähnt. Sie wurden von Cantor in seiner Mengenlehre zuerst verwendet. Die Symbole  $\mathbb{R}$ ,  $\mathbb{Q}$ ,  $\mathbb{N}$ ,  $\mathbb{Z}$  wurden früher als fette Buchsta-ben gedruckt und zunächst nur beim Tafelanschrieb in der hier gegebenen Gestalt wiedergegeben, da man fetten Druck an der Tafel nicht gut darstellen kann.

### 2.3.2 Grundsätzliches zur Formulierung

2.3.2.1 (**Redundanz**). Es scheint mir wichtig, sich beim Schreiben über Mathe-matik immer vor Augen zu halten, daß die mathematische Terminologie und For-

melsprache sehr wenig Redundanz aufweisen. Auch kleinste Fehler oder Ungenauigkeiten können dadurch schon zu den größten Mißverständnissen führen. Ich plädiere deshalb dafür, die Redundanz künstlich zu erhöhen und nach Möglichkeit alles dreimal zu sagen: Einmal in mathematischer Terminologie, einmal in Formeln, und dann noch einmal in weniger formellen Worten und mit Bildern.

**2.3.2.2 (Versprachlichung).** Ich halte es für ebenso wichtig wie delikat, den mathematischen Inhalten griffige Bezeichnungen zu geben. Wir wollen uns ja auch mit anderen Mathematikern unterhalten können, die nicht dasselbe Buch gelesen haben. Sogar dann, wenn ich nur mit mir selbst und einem einzigen Buch beschäftigt bin und bei einem Beweis, den ich gerade verstehen will, ganz präzise „Theorem 4.2“ zitiert wird, stört es mich: Ich muß blättern, bin abgelenkt und mein Verstehen wird gebremst. Darüber hinaus kann ich mir Dinge viel besser merken, die griffige Bezeichnungen haben. Diese Bezeichnungen wirken wie Garderobenhaken im Kopf, an denen man Inhalte aufhängen und wiederfinden kann. Delikat ist, daß die Wahl einer Bezeichnung oft auch eine politische und historische Dimension hat. Delikat ist weiter, daß bei vielen üblichen Bezeichnungen verschiedene Varianten für ihre genaue Bedeutung im Umlauf sind. Ich versuche beides nach bestem Wissen und Gewissen offenzulegen.

**2.3.2.3 (Generalvoraussetzungen).** Ich selber lese keineswegs immer alles von vorne bis hinten durch und merke mir das bereits Gelesene. Vielmehr suche oft, um nicht zu sagen meist, nur gezielt spezielle Resultate, und lese dazu eher diagonal. Ich habe es deshalb nach Kräften vermieden, Generalvoraussetzungen einzustreuen, von der Art „von nun an bis zum Ende des Abschnitts sind alle unsere topologischen Räume Hausdorff“ und dergleichen. Wenn das einmal bei speziellen Themen zu umständlich werden sollte, will ich strikt die Regel befolgen, daß Generalvoraussetzungen für eine Gliederungsstufe entweder direkt nach der Überschrift besagter Gliederungsstufe stehen müssen, oder aber direkt vor dem Beginn des ersten Abschnitts der nächsttieferen Gliederungsstufe, im Anschluß an die Vorrede, und dann als eigener Abschnitt „Generalvoraussetzungen“.

**2.3.2.4 (Definition-Satz-Beweis).** Das Schema Definition-Satz-Beweis scheint mir für die Darstellung von Mathematik sehr gut geeignet und auch zum Lesen und Lernen äußerst effektiv, wenn es richtig angewendet wird: Wenn nämlich die Sätze so formuliert werden, daß ihre Aussagen auch für sich genommen schon sinnvoll und verständlich sind, sofern man die entsprechenden Definitionen parat hat. Dann kann man dieses Schema verstehen als eine Anleitung zum diagonalen Lesen. Demselben Ziel dient die Abstufung der Sätze durch die Bezeichnung als Satz, Korollar, Proposition, Lemma und dergleichen: Sie soll dem Leser zu erlauben, etwa durch Konzentration auf die Sätze eine schnelle Orientierung über die wesentlichen Aussagen und Resultate zu gewinnen. Diese Form ersetzt zu einem gewissen Maße, was man im Deutschunterricht lernt. Ich empfehle, mathemati-

sche Texte und Vorträge nicht mit einer Gliederung zu beginnen und auch nicht mit einem Schlußwort zu beenden, da das in Anbetracht der in der Mathematik eh üblichen Strukturierung durch das Schema „Definition-Satz-Beweis“ leicht dazu führt, daß die strukturellen Elemente im Vergleich zum eigentlichen Inhalt unverhältnismäßig viel Raum einnehmen.

**2.3.2.5 (Andere nummerierte Passagen).** In diesem Text gibt es auch viele Passagen, die einfach nur nummeriert sind. Hier handelt es sich meist um kleinere Aussagen mit Beweis, die mir für die „große Form“ Definition-Satz-Beweis zu unbedeutend oder zu offensichtlich schienen. Andere Textpassagen sind als *Ergänzung* oder *Ergänzende Übung* ausgewiesen: Damit ist gemeint, daß sie im unmittelbaren Zusammenhang ohne Schaden übersprungen werden können, daß sie jedoch aus dem vorhergehenden heraus verständlich sein sollten. Wieder andere Textpassagen sind als *Vorschau* oder *Weiterführende Übung* ausgewiesen: Damit ist gemeint, daß sie im unmittelbaren Zusammenhang ohne Schaden übersprungen werden können und daß ihr Verständnis Kenntnisse voraussetzt, bei denen nicht davon ausgehe, daß sie dem Leser an der entsprechenden Stelle bereits zur Verfügung stehen.

**2.3.2.6 (Satzzeichen in mathematischen Texten).** Satzzeichen wie Punkt und Komma stören aus meiner Sicht die Ästhetik von aus dem Text herausgestellten Formeln. Ich will deshalb die Regel aufstellen und befolgen, daß eine aus dem Text herausgestellte Formel stets mit einem nicht gedruckten Punkt dahinter zu denken ist, wenn der Text mit ihr aufhört oder wenn es darunter mit einem Großbuchstaben weitergeht. Ich werde den Fall vermeiden, daß hinter einer aus dem Text herausgestellten Formel nach den Regeln der Grammatik ein Komma gehören müßte.

**2.3.2.7 (Eigennamen in mathematischen Texten).** Ich übernehme aus dem Englischen den Apostroph bei Eigennamen und schreibe also zum Beispiel Zorn'sches Lemma. In der deutschen Literatur sind stattdessen Kapitälchen üblich, wie etwa ZORNSches Lemma, aber diese Hervorhebung im Schriftbild scheint mir unbührlich viel Aufmerksamkeit zu binden.

### 2.3.3 Sprache und Mathematik

2.3.3.1. In diesem Abschnitt habe ich gesammelt, was mir beim Erklären von Mathematik und Schreiben über Mathematik besonders schwer fällt.

**2.3.3.2 (Umgangssprache versus mathematische Fachsprache).** Die mathematische Terminologie widmet freimütig Worte der Umgangssprache um und gibt ihnen präzise mathematische Bedeutungen, die mal mehr und mal weniger zur Ursprungsbedeutung verwandt sind. Man denke zum Beispiel an die Worte Menge, Abbildung, Gruppe, Ring, Körper. Mit dem Adjektiv **schmutzig** betone ich,

daß ein Wort umgangssprachlich zu verstehen ist und nicht als ein Begriff der allein auf der Mengenlehre basierenden aseptisch steril perfekten Ideenwelt der reinen Mathematik.

2.3.3.3. Im Gegensatz zu dem, was in der Schule im Deutschunterricht gelernt wird, ist Wortwiederholung beim mathematischen Schreiben und Reden richtig und wichtig.

2.3.3.4 (**Erweiterung oder Zusitzung durch Ergänzungen**). Bereits erklärte Begriffe werden in der mathematischen Fachsprache durch Ergänzungen mal spezifiziert, mal abgeschwächt, und manchmal sogar beides zugleich. Der noch wenig informierte Leser kann nur schwer erraten, was im Einzelfall zutrifft. So ist ein Primkörper etwas Spezielleres als ein Körper, ein Schiefkörper etwas Allgemeineres, und ein Erweiterungskörper „etwas mit zusätzlichen Daten“. Ein lokal kompakter Raum ist etwas allgemeineres als ein kompakter Raum. Eine universelle Überlagerung ist etwas Spezielleres als eine Überlagerung und eine verzweigte Überlagerung etwas Allgemeineres, das aber nur im Spezialfall von Flächen überhaupt sinnvoll definiert ist. Ein Borelmaß ist etwas Spezielleres als ein Maß und ein signiertes Maß etwas Allgemeineres. Eine Mannigfaltigkeit mit Rand ist etwas Allgemeineres als eine Mannigfaltigkeit, eine glatte Mannigfaltigkeit dahingegen eine spezielle Art von Mannigfaltigkeit, und ich könnte noch lange so fortfahren. Das führt leicht zu Verwirrung, aber ich habe auch keine Lösung.

2.3.3.5 (**Bestimmte und unbestimmte Artikel**). Problematisch scheint mir in mathematischen Texten die Verwendung bestimmter und unbestimmter Artikel, und ich bin fast neidisch auf die russische Sprache, die diese Unterscheidung nicht kennt. Sind mathematische Strukturen „eindeutig bis auf eindeutigen Isomorphismus“, wie Gruppen mit zwei Elementen oder Mengen mit einem Element, so fällt mir die Verwendung des bestimmten Artikels leicht. Häufig sind mathematische Strukturen jedoch nur „eindeutig bis auf nicht-eindeutigen Isomorphismus“: Etwa Mengen mit fünf Elementen, Gruppen mit drei Elementen oder Vektorräume gegebener Dimension über einem vorgegebenen Körper. Soll man dann den bestimmten oder den unbestimmten Artikel verwenden? Hier ist die Terminologie uneinheitlich: Man sagt üblicherweise „ein fünfdimensionaler reeller Vektorraum, eine abzählbar unendliche Menge“ aber „die euklidische Ebene, der Zerfällungskörper, der algebraische Abschluß, die universelle Überlagerung“, ohne daß ich dafür triftige Gründe ausmachen könnte. Vielleicht wäre es eine gute Idee, für nur bis auf nichteindeutigen Isomorphismus eindeutig bestimmte mathematische Objekte die bestimmten Artikel mit einer „abschwächenden Schlange“ in der Form „dér, dīe, dās“ zu verwenden.

2.3.3.6 (**Existenz in Definitionen**). Ich plädiere dafür, in mathematischen Texten die Formulierungen „Es existiert“ und „Es gibt“ ausschließlich in ihrer Bedeutung als Quantoren zu verwenden, da es sonst leicht zu Mißverständnissen kommen

kann. Insbesondere plädiere ich sehr dafür, diese Formulierungen zu vermeiden, wenn es in Definitionen um die Vorstellung der „Ausgangsdaten“ geht. Die folgenden Beispiele mögen das illustrieren.

**Mißverständlich:** Eine Gruppe ist eine Menge, auf der es eine assoziative Verknüpfung gibt derart, daß es ein neutrales Element gibt und zu jedem Element ein Inverses.

**Klarer:** Eine Gruppe ist eine Menge mit einer assoziativen Verknüpfung derart, daß es ein neutrales Element gibt und zu jedem Element ein Inverses.

**Pedantisch:** Eine Gruppe ist ein Paar bestehend aus einer Menge und einer assoziativen Verknüpfung auf dieser Menge derart, daß es ein neutrales Element gibt und zu jedem Element ein Inverses.

In der Tat gibt es ja auf jeder nichtleeren Menge eine assoziative Verknüpfung, die sie zu einer Gruppe macht. Eine Gruppe ist aber keineswegs eine Menge mit gewissen Eigenschaften, sondern eine Menge mit Verknüpfung mit gewissen Eigenschaften. Das Ausgangsdatum bei dieser Definition ist in anderen Worten und ganz pedantisch formuliert ein Paar bestehend aus einer Menge zusammen mit einer Verknüpfung auf dieser Menge. Ich gebe zu, daß man auch die „klare“ Definition falsch verstehen könnte, aber an dieser Stelle würde ich dieser Formulierung wegen ihrer Kürze doch der Vorzug gegenüber der „pedantischen“ Formulierung einräumen.

**Mißverständlich:** Ein Körper heißt angeordnet, wenn es auf ihm eine Anordnung gibt derart, daß...

**Klarer:** Ein angeordneter Körper ist ein Körper mit einer Anordnung derart, daß...

**Pedantisch:** Ein angeordneter Körper ist ein Paar bestehend aus einem Körper mit einer Anordnung auf der ihm zugrundeliegenden Menge derart, daß...

Zur Verdeutlichung zum Abschluß noch ein Beispiel, in dem die mißverständliche Formulierung die korrekte Formulierung einer anderen Eigenschaft ist:

**Mißverständlich:** Eine Mannigfaltigkeit heißt orientiert, wenn es auf ihr eine Orientierung gibt.

**Klarer:** Eine orientierte Mannigfaltigkeit ist eine Mannigfaltigkeit mit einer Orientierung.

**Pedantisch:** Eine orientierte Mannigfaltigkeit ist ein Paar bestehend aus einer Mannigfaltigkeit mit einer Orientierung auf unserer Mannigfaltigkeit.

Hier ist die erste Formulierung in der Tat bei der üblichen Interpretation von „es gibt“ als Quantor die Definition einer orientierbaren, nicht die einer orientierten Mannigfaltigkeit.

**2.3.3.7 (Kampf dem Index).** Beim Schreiben von Mathematik in Formeln hat man oft mit der Schwierigkeit zu kämpfen, daß die wesentliche Information sich in Indizes verstecken will und die besonders wesentliche Information in Subindizes. Dem gilt es bewußt entgegenzuarbeiten.

### 2.3.4 Terminologisches zur leeren Menge\*

*Vorschau* 2.3.4.1. Ich finde es oft schwierig, die leere Menge terminologisch korrekt einzubinden. Das ist aber ebenso wichtig wie der Beckenrand beim Schwimmbad, den man ja auch nicht wegläßt, obwohl man nachher nur im Wasser schwimmen will. Ich finde auch, daß das Bourbaki, den ich an sich sehr schätze, oft mißlungen ist. Meine Konventionen sind wie folgt:

1. Die leere Menge ist nach ?? ein Intervall. So sind beliebige Schnitte von Intervallen wieder Intervalle;
2. Die leere Menge ist nach 3.3.5.2 konvex. So sind beliebige Schnitte konvexer Mengen wieder konvex;
3. Die leere Menge ist *nicht* zusammenhängend. Die Zusammenhangskomponenten eines topologischen Raums sind seine maximalen zusammenhängenden Teilmengen und die leere Menge hat gar keine Zusammenhangskomponente. So hat für einen topologischen Raum mit nur endlich vielen Zusammenhangskomponenten der Vektorraum der stetigen Abbildungen in den Körper mit zwei Elementen als Dimension gerade die Zahl der Zusammenhangskomponenten. Die zusammenhängenden Teilmengen von  $\mathbb{R}$  sind damit genau die *nichtleeren* Intervalle und nur jede *nichtleere* konvexe Teilmenge eines endlichdimensionalen reellen affinen Raums ist zusammenhängend;
4. Die Wirkung einer Gruppe  $G$  auf der leeren Menge ist nach 4.5.1.7 *nicht* transitiv. Damit läßt sich jede  $G$ -Menge bis auf Reihenfolge und Isomorphismus eindeutig als eine disjunkte Vereinigung von transitiven  $G$ -Mengen darstellen;
5. Die leere Menge ist nach 3.3.1.1 *kein* affiner Raum. Sie läßt ja nach der vorhergehenden Konvention auch keine transitive Operation eines Vektorraums zu. Daß damit der Schnitt zweier affiner Teilräume nicht notwendig wieder ein affiner Teilraum ist, nehme ich als kleineres Übel in Kauf;

6. Eine Abbildung von der leeren Menge in eine beliebige weitere Menge ist konstant, aber nicht einwertig, vergleiche 2.1.4.10;

## 2.4 Philosophisches und Didaktisches

In diesen Abschnitten habe ich einige Gedanken zur Mathematik und zum Unterrichten von Mathematik gesammelt, die nicht zum logisch kohärenten Aufbau des Stoffes selber beitragen und teilweise auch stark persönlich gefärbt sind.

### 2.4.1 Was ist Mathematik?

2.4.1.1. Das Wort „Mathematik“ kommt vom griechischen „μαθηματικός“, das sich hinwiederum ableitet von „μαθημα“ für „der Lerngegenstand, die Wissenschaft“ nach dem Verb „μανθάνω“ für „lernen, verstehen“. Das Anhängen der Endung „-ικός“ oder im Anschluß an einen Vokal „-τικός“ hat eine ähnliche Bedeutung wie im Deutschen das Anhängen von „-ig“ oder „-lich“ beziehungsweise „-tlich“, etwa wie in Mut  $\mapsto$  mutig, Haar  $\mapsto$  haarig, wohnen  $\mapsto$  wohnlich oder eigen  $\mapsto$  eigentlich. In diesem Sinne wäre die wörtliche Übersetzung von „μαθηματικός“ also „das Lernige“ oder „das Verständliche“. Platon verwendet den Begriff „τὸ μαθηματικὸν“ im Sinne von „der Forschungsgegenstand“ in Sophista 219c:2 und Timaeus 88c:1. In der hellenistischen Zeit verengte sich die Bedeutung ein erstes Mal und bezeichnete etwas, was wir heute eher als „Mathematik und Naturwissenschaften“ bezeichnen würden. Erst in neuerer Zeit verengte sich die Bedeutung weiter auf das, was wir heute unter Mathematik verstehen

2.4.1.2. Ich würde die heutige Mathematik in einem ersten Ansatz beschreiben als die „Wissenschaft von den einfachsten Begriffen“: Wieviel einfacher sind doch Zahlen und ihre Rechenregeln, Geraden und Ebenen, selbst Abbildungen zwischen Mengen im Vergleich zu Pflanzen und Menschen, Hass und Liebe, ja selbst Luft und Wasser! Diese einfachsten Begriffe müssen nun jedoch mit der größten Vorsicht und Präzision gehandhabt werden, damit uns unsere an den Umgang mit Pflanzen und Menschen, Hass und Liebe, Luft und Wasser gewöhnnte Intelligenz nicht in die Irre führt. Die eigentliche Mathematik besteht dann darin, diese einfachsten Begriffe zu größeren Theorien zu kombinieren, und die eigentlichen Einsichten entstehen auch erst in dieser Gesamtschau. Ich sehe darin eine Affinität zur Musik, in der man ja auch von einfachsten Geräuschen, in der Klassik etwa von den Tönen der Tonleiter, ausgeht und diese einfachsten Grundbausteine zu Kompositionen kombiniert, deren Sinnhaftigkeit sich erst in der Gesamtschau erschließt. Auf einen Gegensatz zur Musik will ich im nächsten Absatz noch ausführlicher zu sprechen kommen: Während auch die schönste Musik meines Erachtens vom Komponisten nicht entdeckt sondern vielmehr erschaffen wird, scheint es sich mir bei der Mathematik gerade umgekehrt zu verhalten. Sicher gibt es sozusagen „komponierte“ mathematische Artikel, aber die mathematischen Inhalte selbst lassen sich von Menschenhand nicht formen und wollen entdeckt werden.

2.4.1.3. In diesem Zusammenhang will ich auf eine gerne diskutierte Frage eingehen: Wird Mathematik eigentlich entdeckt oder entwickelt? Aus meiner eigenen Erfahrung mit dieser widerspenstigen Materie und auch der Erfahrung beim Erklären von Beweisen scheint es mir offensichtlich, daß mathematische Inhalte „objektiv da sind“, also unabhängig vom menschlichen Subjekt existieren und entdeckt werden. Was jedoch entwickelt werden muß ist eine Sprache, die es uns ermöglicht, uns über diese Inhalte zu verständigen und sie zu nutzen. Hier kam und kommt es durchaus zu parallelen Entwicklungen, man denke etwa an die beiden Notationen  $x$  und  $\frac{dx}{dt}$  für die Ableitung, an den Erwartungswert  $E(X)$  einer Zufallsvariable  $X$  in der Wahrscheinlichkeitstheorie, der ja nichts anderes ist als das Integral  $\int f$  einer Funktion  $f$  in der Analysis, und nicht zuletzt an die verschiedenen Notationen für die natürlichen Zahlen durch römische Buchstaben oder arabische Ziffern.

2.4.1.4. Bildlich gesprochen scheint mir die Mathematik wie eine weitverzweigte Höhle, voller Wunder und wertvoller Mineralien, die wir Mathematiker einerseits erkunden und andererseits erschließen. Die Höhle selbst ist objektiv vorhanden und es gilt, immer weiter in sie vorzudringen und Neues zu entdecken und Neues wie Bekanntes nutzbar zu machen. Wo und wie dann jedoch Treppen und Wege und Lampen angebracht werden und eventuell sogar eine kleine Eisenbahn zum Transport der Mineralien, darin haben wir große Freiheit und in diesem Sinne wird Mathematik auch entwickelt. Natürlich sind diese beiden Aufgaben eng miteinander verwoben und wie weit wir selbst vordringen können hängt ganz wesentlich davon ab, wie weit unsere Vorfäher gekommen sind und wie weit sie die Höhle bereits zugänglich gemacht haben.

2.4.1.5. Die im vorhergehenden dargelegte Auffassung vom Sinn und Wesen der Mathematik bezeichnet man wegen ihrer engen Verwandtschaft mit Plato's Ideenlehre auch als „platonisch“. Barry Mazur fordert in seinem Aufsatz [Maz08] die Platoniker auf, zu erklären, warum Beweise denn uns als Mathematikern so wichtig sein sollten, wenn es nur um das Erkennen einer unabhängig von uns existierenden Wirklichkeit geht. Dieser Aufforderung will ich gerne nachkommen. Ich fasse Beweise auf als Beiträge zum großen Projekt, die Welt der mathematischen Inhalte dem menschlichen Verstand zugänglich zu machen. Mir scheint es in diesem Sinne eine wichtige Aufgabe, auch für bereits bewiesene Erkenntnisse möglichst glatte und für menschliche Gehirne transparente Beweise zu finden, aufzuschreiben und öffentlich zugänglich zu machen. Was das Beweisen angeht, gibt es auch durchaus verschiedene Ansätze: Anschauliche Beweise aus der Schulgeometrie, etwa für den Satz des Pythagoras oder andere elementargeometrische Sätze, wären um im Bild zu bleiben eher ein Art Wegesystem für Fußgänger, wohingegen sich professionelle Mathematiker seit etwa 1900 meist auf einem aus Mengenlehre aufgebauten Schienennetz bewegen, das zwar große an-

fängliche Investitionen erfordert, danach aber dem Verstand ein sehr schnelles, sicheres und tiefes Eindringen ermöglicht. Allerdings fällt es unseren durch die Bequemlichkeit dieses Zugangs verwöhnten Studenten meist bitter schwer, dann an interessanten und noch nicht erschlossenen Stellen wieder auszusteigen und sich zu Fuß weiter fortzubewegen oder gar selbst Schienen zu legen. Rechnergestützte Beweise sind für mich wie eine Erkundung mit Robotern nicht in derselben Weise befriedigend wie der persönliche Augenschein, aber wenn man an interessante Stellen partout nicht selbst hingelangen kann, sind doch schöne von Robotern geschossene Bilder allemal besser als gar nichts.

2.4.1.6. Die Mathematik wird insbesondere von Außenstehenden oft als eine tote Wissenschaft erlebt, in der „alles schon seit dreihundert Jahren bekannt sei“. Dieser Eindruck mag damit zusammenhängen, daß Mathematik durchaus „verholzt“ in dem Sinne, daß sie einen festen Stamm an Wissen und kodifizierter Sprache ausbildet. Das aber ermöglicht es unserer Wissenschaft auch gerade wieder, hoch hinaus zu wachsen, und damit das gelingen kann, müssen wir uns alle Mühe geben, in der mathematischen Terminologie keine Sprachverwirrung einreißen zu lassen.

2.4.1.7. Beim Erlernen dieser Wissenschaft soll man, so denke ich, nach Kräften versuchen, sich aller seiner gedanklichen Fähigkeiten zu bedienen. Geeignet für das Durchdringen mathematischer Sachverhalte scheinen mir insbesondere die räumliche oder noch besser die räumlich-zeitliche Anschauung, das abstrakte logische Denken und das formale Umformen von Zeichenketten auf Papier. Hilfreich kann auch unsere sprachliche Intelligenz sein: Bereits kleine Kinder lernen ja das Zählen, indem sie zunächst „Eins-Zwei-Drei-Vier-Fünf“ memorieren wie „Abrakadabra Simsalabim“, und ältere lernen ähnlich den Satz des Pythagoras oder die binomischen Formeln.

2.4.1.8. Die Mathematik schöpft große Kraft aus abstrakten Theorien, und nur allzuoft wollen diese ihre Herkunft verbergen und verkleiden sich als zufällig zusammengewürfelte Haufen aus Daten und Axiomen. Man darf sich davon nicht in die Irre führen lassen. Meist sind das vielmehr sehr sorgfältig konstruierte und in immer neuen Versionen an zahlreichen Beispielen erprobte Maschinen, die es einem erlauben, wie in einem Flugzeug mit großer Bequemlichkeit große Wegstrecken zurückzulegen und dabei die meisten konkreten Schwierigkeiten am Boden zu ignorieren. Das alles ist jedoch nur sinnvoll, wenn auch das Starten und das Landen gelingt, und das Herrichten von Start- und Landebahnen kann auch leicht so viel Arbeit bedeuten, daß das ganze Fliegen dadurch uninteressant wird. Bei mancher Theorie habe ich sogar den Eindruck, daß man nur startet aber nie mehr landet, oder noch schlimmer, daß man weder starten noch landen kann, sondern einfach nur sinnlos herumfliegt, aber das mag auch an meiner mangelnden Kenntnis der jeweiligen Theorie liegen – ich nenne besser keine Beispiele.

### 2.4.2 Didaktische Gedanken

2.4.2.1 (**Warum Vorlesungen?**). Warum hören und halten wir in der Mathematik eigentlich Vorlesungen? In der Zeit, in der das Drucken von Büchern noch nicht möglich oder zumindest schwierig und teuer war, mag es sinnvoll gewesen sein, einfach ein Buch vorzulesen, das dann in mehreren Kopien mitgeschrieben werden konnte: In Klöstern wurden etwa die Schriften der Antike und des Christentums lange Zeit auf diese Weise vor dem Vergessen und dem Zerfall gerettet. In der Zeit von Internet und Kopiergeräten kann es jedoch nicht mehr das Ziel einer Vorlesung sein, daß die beteiligten Studenten Mitschriften anfertigen, aus denen sie dann den Stoff lernen: Zu viel wird in solchen Vorlesungen falsch verstanden und falsch abgeschrieben, als daß ich nicht eher das Lernen aus Büchern empfehlen würde. Für den andauernden Erfolg der Vorlesung als Unterrichtsform fallen mir verschiedene Gründe ein.

1. Der Mensch ist nicht gern allein. Es lernt sich besser gemeinsam, man kann sich in der Pause und nach der Vorlesung untereinander über das Gelernte und das nicht Verstandene unterhalten und auch einfach so mal treffen. Die Pause dient insbesondere nicht allein zum Pinkeln oder zum Aufrechterhalten der Konzentration, und es ist doppelt schade, wenn sie ausfällt.
2. Die Vorlesung gibt einen gewissen Rhythmus vor, in dem gelernt und nicht Gelerntes ignoriert und auf später verschoben wird. Anfänger lernen aus Büchern leicht so, wie ganz kleine Kinder spaziergehen: Jeder Kieselstein ist interessant und eine Pause zur ausführlichen Betrachtung wert. Ganz zu Anfang ist das ja auch richtig so, aber dann muß doch die Vorlesung etwas schieben, damit es auch vorangeht.
3. Die Studenten müssen, insbesondere in der Mathematik, regelmäßig davon überzeugt werden, daß prinzipiell durchaus verständlich ist, was sie da lernen sollen, daß es sich nicht um eine Art Zauberformeln handelt, die von Generation zu Generation nur abgeschrieben werden. Sie von der Verständlichkeit des Stoffes zu überzeugen gelingt besonders gut durch das Entwickeln aus dem Kopf an der Tafel. Ein Beamer oder das Auflegen vorbereiteter Folien oder das Ablesen eines vorbereiteten Manuskripts wirken im Vergleich wesentlich weniger überzeugend.

2.4.2.2 (**Welche Übungen?**). Ich denke, daß man die Mathematik nicht erlernen kann, ohne Übungsaufgaben zu lösen. Allerdings sollten diese zu großen Teilen viel elementarer sein als die in diesem und den folgenden Texten vorgeschlagenen Übungen. Diese dienen eher dazu, ergänzenden Stoff in knapper Form zu präsentieren und sollen auf den Übungsblättern nur einen Teil der Übungen ausmachen.

Insbesondere in den Grundvorlesungen müssen ihnen auch nicht wenig mehr algorithmische Übungen zur Seite gestellt werden, von der Art: Löse dieses lineare Gleichungssystem, invertiere jene Matrix, zerlege dieses Polynom in irreduzible Faktoren und dergleichen mehr.

## **2.5 Danksagung**

Für Korrekturen und Verbesserungen danke ich Markus Junker, Dominic Maier, Dimitri Guefack, Pascal Soergel.

# **Kapitel 3**

## **Lineare Algebra 1**

Die Bezeichnung „Algebra“ kommt von arabisch „al-jabr“, das in der Medizin das Wiedereinrenken eines Gelenks bezeichnete und in der Mathematik für eine Umformung stand, die man heute das „Herüberschaffen durch Subtraktion“ eines Terms von der einen auf die andere Seite einer Gleichung nennen würde. In diesem Zusammenhang wurde wohl auch das Rechnen mit negativen Zahlen entwickelt. Der im folgenden vorgestellte Teil der Algebra heißt „linear“, da das einfachste der darin untersuchten Gleichungssysteme dem geometrischen Problem entspricht, den Schnittpunkt zweier Geraden alias Linien zu bestimmen. Ich habe mir bei der Darstellung die größte Mühe gegeben, die abstrakte Sprache der Mengenlehre und unsere räumliche Anschauung zu einer Einheit zu fügen, ohne dabei die algorithmischen Aspekte zu kurz kommen zu lassen.

## 3.1 Gleichungssysteme und Vektorräume

In diesem Abschnitt will ich aufzeigen, inwiefern uns die räumliche Anschauung beim Verständnis der Theorie linearer Gleichungssysteme helfen kann und in welcher Weise die Theorie abstrakter Vektorräume eine Brücke zwischen diesen beiden Begriffswelten schafft.

### 3.1.1 Lösen linearer Gleichungssysteme

3.1.1.1. Ich erinnere aus 2.2.4.2 die Definition eines Körpers, die dort in größerer Ausführlichkeit besprochen wird.

**Definition 3.1.1.2.** Ein **Körper** ( $K, +, \cdot$ ) ist eine Menge  $K$  mit zwei kommutativen assoziativen Verknüpfungen, genannt die **Addition**  $+$  und die **Multiplikation**  $\cdot$  des Körpers, die meist schlicht durch Zusammenschreiben  $a \cdot b = ab$  notiert wird, derart daß mit der Konvention „Punkt vor Strich“ die folgenden drei Bedingungen erfüllt sind:

1.  $(K, +)$  ist eine Gruppe, die **additive Gruppe** des Körpers;
2. Die vom neutralen Element der Addition  $0_K \in K$  verschiedenen Elemente von  $K$  bilden eine unter der Multiplikation abgeschlossene Teilmenge und diese Teilmenge  $K \setminus \{0_K\}$  ist unter der Multiplikation ihrerseits eine Gruppe, die **multiplikative Gruppe** des Körpers;
3. Es gilt das **Distributivgesetz**

$$a(b + c) = ab + ac \quad \forall a, b, c \in K$$

*Ergänzung 3.1.1.3.* Fordert man hier nicht die Kommutativität der Multiplikation und fordert zusätzlich das „Distributivgesetz für die Multiplikation von rechts“  $(b+c)a = ba+ca \quad \forall a, b, c \in K$ , das im Fall einer kommutativen Multiplikation ja schon aus den anderen Axiomen folgte, so heißt unsere Struktur ein **Schiefkörper**.

3.1.1.4. Sei  $K$  ein Körper. Ich rate, zunächst einmal an den Körper  $K = \mathbb{Q}$  der rationalen Zahlen oder den Körper  $K = \mathbb{R}$  der reellen Zahlen zu denken. Ich werde im folgenden, weil ich selber meist an diese beiden Fälle denke, Elemente eines allgemeinen Körpers  $K$  oft als „Zahlen“ bezeichnen. Gegeben seien  $n$  Gleichungen in  $m$  Unbekannten alias **Variablen**  $x_1, \dots, x_m$  von der Gestalt

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m &= b_2 \\ \vdots &\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m &= b_n \end{aligned}$$

$$x_1 + 3x_2 = 1$$

$$2x_1 + 2x_2 + x_3 = 2$$

$$4x_1 + 6x_2 + x_3 = 8$$

Ein lineares Gleichungssystem mit drei Gleichungen und drei Unbekannten.

Hierbei denken wir uns  $a_{ij}, b_i \in K$  fest vorgegeben und  $x_j \in K$  gesucht. Der in mathematischer Formelsprache geübte Leser wird das bereits erkannt haben, denn es ist allgemeine Konvention, Buchstaben vom Anfang des Alphabets für „bekannte Unbestimmte“ zu verwenden und Buchstaben vom Ende des Alphabets für „gesuchte Unbestimmte“. Eine Gesamtheit von mehreren zu erfüllenden Gleichungen bezeichnet man als **Gleichungssystem**. Ein Gleichungssystem des obigen Typs nennt man ein **lineares Gleichungssystem**. Linear heißt es, weil darin keine komplizierteren Ausdrücke in den Variablen wie Quadrate  $x_1^2$  oder Produkte von Variablen  $x_1 x_2 x_3$  vorkommen. Die  $a_{ij}$  heißen in diesem und ähnlichen Zusammenhängen **Koeffizienten** von lateinisch „coefficientes“ für deutsch „mitwirken“. Gesucht ist eine Beschreibung aller  $m$ -Tupel  $(x_1, \dots, x_m)$  von Elementen von  $K$  derart, daß alle  $n$  obigen Gleichungen gleichzeitig erfüllt sind. In der Begrifflichkeit und Notation, wie wir sie gleich in 3.1.3.8 einführen, bildet die Gesamtheit aller  $m$ -Tupel  $(x_1, \dots, x_m)$  von Elementen von  $K$  eine neue Menge  $K^m$ . In dieser Terminologie suchen wir also eine möglichst explizite Beschreibung der Teilmenge  $L \subset K^m$  derjenigen  $m$ -Tupel, die alle unsere  $n$  Gleichungen erfüllen. Sie heißt die **Lösungsmenge**  $L$  unseres Gleichungssystems.

3.1.1.5. Sind alle  $b_i$  auf der rechten Seite unserer Gleichungen Null, so heißt unser lineares Gleichungssystem **homogen**. Das lineare Gleichungssystem, das aus einem inhomogenen System in der oben angegebenen Notation entsteht, indem man alle  $b_i$  zu Null setzt, heißt das zugehörige **homogenisierte** Gleichungssystem.

3.1.1.6 (**Schwierigkeiten der Notation**). In obigem Gleichungssystem ist  $a_{12}$  nicht als  $a$ -Zwölf zu verstehen, sondern als  $a$ -Eins-Zwei. Sicher wäre es präziser gewesen, die beiden Bestandteile unserer Doppelindizes durch ein Komma zu trennen und  $a_{1,2}$  und dergleichen zu schreiben. Das hätte unser Gleichungssystem aber weniger übersichtlich gemacht. Man muß beim Schreiben und Verstehen von Mathematik oft einen Ausgleich zwischen einer präzisen aber unübersichtlichen und einer übersichtlichen aber unpräzisen Darstellung suchen. An dieser Stelle schien mir das Weglassen der Kommata der bessere Weg. Einem Menschen etwas verständlich zu machen ist eben eine andere Aufgabe als einen Computer zu programmieren. Beim Programmieren eines Computers kommt es an erster Stelle auf die Eindeutigkeit der Anweisungen an und alles andere ist nebensächlich. Beim Schreiben und Erklären für Menschen kommt es dahingegen eher auf die Übersichtlichkeit an und bei Mehrdeutigkeiten kann man erwarten, daß sie vom Leser aus dem Kontext heraus aufgelöst werden und oft noch nicht einmal auffallen. Insbesondere in der Physik ist es üblich, einen der Indizes hochzustellen, also  $a_1^2$  statt  $a_{12}$  zu schreiben, aber das kann auch wieder leicht als das Quadrat  $(a_1)^2$  einer Zahl  $a_1$  mißverstanden werden. Ich würde am liebsten  ${}^1 a_2$  schreiben und eine Zeile unseres Gleichungssystems entsprechend als  ${}^1 a_1 {}^1 x + {}^1 a_2 {}^2 x + \dots + {}^1 a_m {}^m x = {}^1 b$ , aber das schien mir zu viel Umgewöhnung auf einmal. Man beachte auch, daß bei Ma-

$$2y - 17z = 0$$

$$4x + 22y + z = 0$$

Ein homogenes lineares Gleichungssystem, mit zwei Gleichungen und drei Unbekannten, bei dem ich die Unbekannten statt mit  $x_1, x_2, x_3$  zur Abwechslung einmal  $x, y, z$  notiert habe. Es ist beim Rechnen meist sinnvoll, eine Notation mit möglichst wenig Indizes zu verwenden.

$$0x = 1$$

Ein inhomogenes lineares Gleichungssystem mit einer Gleichung und einer Unbekannten und leerer Lösungsmenge.

trizen die Konventionen anders bei Koordinaten. Bei Matrizen wächst üblicherweise der erste Index nach unten der zweite Index nach rechts, bei Koordinaten dahingegen der erste Index nach rechts und der zweite Index nach oben.

3.1.1.7. Um die Lösungsmenge eines linearen Gleichungssystems zu bestimmen, kann man den **Gauß-Algorithmus** verwenden. Er basiert auf der elementaren Erkenntnis, daß sich die Lösungsmenge nicht ändert, wenn wir in einer der beiden folgenden Weisen zu einem neuen Gleichungssystem übergehen:

1. Wir ersetzen eine unserer Gleichungen durch ihre Summe mit einem Vielfachen einer anderen unserer Gleichungen;
2. Wir vertauschen zwei unserer Gleichungen.

Der noch zu besprechende Gauß-Algorithmus beschreibt, wie wir mithilfe dieser beiden Operationen, also ohne die Lösungsmenge zu ändern, zu einem Gleichungssystem übergehen können, das **Zeilenstufenform** hat. Nebenstehendes Bild mag aufschlüsseln, was das anschaulich bedeuten soll. Formal sagen wir, ein Gleichungssystem „habe Zeilenstufenform“, wenn man ein  $r \geq 0$  und Indizes  $1 \leq s(1) < s(2) < \dots < s(r) \leq m$  so angeben kann, daß in unserem Gleichungssystem gilt  $a_{i,s(i)} \neq 0$  für  $1 \leq i \leq r$  und daß  $a_{\nu\mu} \neq 0$  nur gelten kann, wenn es ein  $i$  gibt mit  $\nu \leq i$  und  $\mu \geq s(i)$ .

3.1.1.8. Es ist üblich und erspart Schreibarbeit, die Symbole für die Variablen sowie die Pluszeichen und Gleichheitszeichen bei Rechnungen im Zusammenhang mit linearen Gleichungssystemen wegzulassen und stattdessen ein Gleichungssystem der oben beschriebenen Art abzukürzen durch seine **erweiterte Koeffizientenmatrix**

$$\left( \begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1m} & b_1 \\ a_{21} & a_{22} & & a_{2m} & b_2 \\ \vdots & & & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} & b_n \end{array} \right)$$

Die Spezifikation „erweitert“ weist auf die letzte Spalte der  $b_i$  hin. Die Matrix der  $a_{ij}$  für sich genommen heißt die **Koeffizientenmatrix** unseres Gleichungssystems.

3.1.1.9 (**Gauß-Algorithmus**). Der Gauß-Algorithmus zum Bestimmen der Lösungsmenge eines linearen Gleichungssystems funktioniert so: Sind alle Koeffizienten in der ersten Spalte Null, so ignorieren wir die erste Spalte und machen mit der auf diese Weise entstehenden Matrix weiter. Ist ein Koeffizient in der ersten Spalte von Null verschieden, so bringen wir ihn durch eine Zeilenvertauschung an die oberste Stelle. Ziehen wir dann geeignete Vielfache der obersten Zeile von den anderen Zeilen ab, so gelangen wir zu einem System, bei dem in der ersten

$$\begin{array}{cccc}
 & \neq 0 & & * \\
 & \neq 0 & \neq 0 & \\
 & & \neq 0 & \\
 & & & \neq 0 \\
 & & & * \\
 \hline
 A(1) & A(2) & A(3) & A(4) \\
 " & " & " & " \\
 3 & 5 & 6 & 9
 \end{array}$$

Ein System in Zeilenstufenform ist ein System der obigen Gestalt, bei dem im Teil mit den Koeffizienten  $a_{ij}$  wie angedeutet unterhalb solch einer „Treppe mit der Stufenhöhe Eins aber mit variabler Breite der Stufen“ nur Nullen stehen, vorn an den Stufenabsätzen aber von Null verschiedene Einträge. Hier ist  $r$  die Zahl der Stufen. An die durch den senkrechten Strich abgetrennte letzte Spalte mit den gewünschten Ergebnissen  $b_i$  werden hierbei keinerlei Bedingungen gestellt. Das Symbol unten links ist eine Null. Die Symbole \* oben rechts deuten an, daß unerheblich ist, was dort steht.

Spalte unterhalb des obersten Eintrags nur noch Nullen stehen. Für das weitere ignorieren wir dann die oberste Zeile und die erste Spalte und machen mit der auf diese Weise entstehenden Matrix weiter. Offensichtlich können wir so jedes lineare Gleichungssystem auf Zeilenstufenform bringen, ohne seine Lösungsmenge zu ändern.

**3.1.1.10 (Lösungsmenge bei Zeilenstufenform).** Die Lösungsmenge eines linearen Gleichungssystems in Zeilenstufenform ist schnell bestimmt: Ist eine der Zahlen  $b_{r+1}, \dots, b_n$  nicht Null, so besitzt es gar keine Lösung. Gilt dahingegen  $b_{r+1} = \dots = b_n = 0$ , so können wir Zahlen  $x_\mu$  für  $\mu$  verschieden von den Spaltenindizes  $s(1), \dots, s(r)$  der Stufen beliebig vorgeben und finden für jede solche Vorgabe der Reihe nach eindeutig bestimmte Zahlen  $x_{s(r)}, x_{s(r-1)}, \dots, x_{s(1)}$  derart, daß das entstehende  $m$ -Tupel  $(x_1, \dots, x_m)$  eine Lösung unseres Gleichungssystems ist.

**3.1.1.11.** Eine Abbildung  $A : \{1, \dots, n\} \times \{1, \dots, m\} \rightarrow Z$  der Produktmenge in eine Menge  $Z$  heißt ganz allgemein eine  **$(n \times m)$ -Matrix mit Einträgen in  $Z$** . Gegeben solch eine Matrix  $A$  schreibt man meist  $A_{ij}$  oder  $a_{ij}$  statt  $A(i, j)$  und veranschaulicht sich die Abbildung  $A$  als ein rechteckiges Arrangement von Elementen von  $Z$  wie eben im Fall  $Z = K$ . Das  $a_{ij}$  heißt dann der **Eintrag** unserer Matrix in der  $i$ -ten Zeile und  $j$ -ten Spalte. Das  $i$  heißt der **Zeilenindex**, da es angibt alias „indiziert“, in welcher Zeile unser Eintrag  $a_{ij}$  steht. Entsprechend nennt man das  $j$  den **Spaltenindex** unseres Matrixeintrags. Ich erinnere daran, daß wir für beliebige Mengen  $X, Y$  die Menge aller Abbildungen von  $X$  nach  $Y$  mit  $\text{Ens}(X, Y)$  bezeichnen. Die Menge aller  $(n \times m)$ -Matrizen mit Koeffizienten in einer Menge  $Z$  notieren wir

$$\text{Mat}(n \times m; Z) := \text{Ens}(\{1, \dots, n\} \times \{1, \dots, m\}, Z)$$

Im Fall  $n = m$  sprechen wir von einer **quadratischen Matrix** und kürzen unsere Notation ab zu  $\text{Mat}(n; Z) := \text{Mat}(n \times n; Z)$ . Manchmal werden wir sogar für beliebige Mengen  $X, Y, Z$  eine Abbildung  $X \times Y \rightarrow Z$  als eine  **$(X \times Y)$ -Matrix mit Einträgen in  $Z$**  ansprechen.

*Ergänzung 3.1.1.12 (Ursprung der Terminologie).* Die Bezeichnung „Matrix“ wurde meines Wissens vom englischen Mathematiker Joseph Sylvester in einem 1851 bei George Bell, Fleet Street erschienenen Artikel mit dem Titel „An essay on canonical forms, supplement to a sketch of a memoir on elimination, transformation and canonical forms“ in die Mathematik eingeführt. Die Bezeichnung scheint auf das lateinische Wort „matrix“ für deutsch „Gebärmutter“ hinzugezogen. Sylvester benutzt Matrizen mit einer Zeile mehr als Spalten und betrachtet die „Determinanten“ der quadratischen Matrizen, die durch Streichen je einer Zeile entstehen. Die Determinante führen wir erst in 3.6.2.1 ein.

$$\left( \begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 2 & 2 & 1 & 2 \\ 4 & 6 & 1 & 8 \end{array} \right) \rightsquigarrow \begin{aligned} x_1 + 3x_2 &= 1 \\ 2x_1 + 2x_2 + x_3 &= 2 \\ 4x_1 + 6x_2 + x_3 &= 8 \end{aligned}$$



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



$$\left( \begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 0 & -4 & 1 & 0 \\ 0 & 0 & -\frac{1}{2} & 4 \end{array} \right) \rightsquigarrow \begin{aligned} x_3 &= -8 \\ x_2 &= -2 \\ x_1 &= 7 \end{aligned}$$

Ein lineares Gleichungssystem mit drei Gleichungen und drei Unbekannten und seine Lösung mit dem Gauß-Algorithmus. Für gewöhnlich wird beim Anwenden des Gauß-Algorithmus ein Vertauschen der Zeilen gar nicht nötig sein. Gibt es weiter genausoviele Gleichungen wie Unbekannte, so werden wir für gewöhnlich so wie in obigem Beispiel genau eine Lösung erwarten dürfen.

**Satz 3.1.1.13 (Lösungsmengen inhomogener linearer Gleichungssysteme).** Ist die Lösungsmenge eines linearen Gleichungssystems nicht leer, so erhalten wir alle Lösungen, indem wir zu einer fest gewählten Lösung unseres Systems eine beliebige Lösung des zugehörigen homogenisierten Systems komponentenweise addieren.

*Beweis.* Ist  $c = (c_1, \dots, c_m)$  eine Lösung unseres linearen Gleichungssystems und  $d = (d_1, \dots, d_m)$  eine Lösung des homogenisierten Systems, so ist offensichtlich die komponentenweise Summe  $c + d = (c_1 + d_1, \dots, c_m + d_m)$  eine Lösung des ursprünglichen Systems. Ist andererseits  $c' = (c'_1, \dots, c'_m)$  eine weitere Lösung unseres linearen Gleichungssystems, so ist offensichtlich die komponentenweise Differenz  $d = (c'_1 - c_1, \dots, c'_m - c_m)$  eine Lösung des homogenisierten Systems, für die gilt  $c' = c + d$  mit unserer komponentenweisen Addition  $+$  aus 1.1.2.7.  $\square$

**3.1.1.14 (Unabhängigkeit der Stufenzahl vom Lösungsweg).** Die vorstehenden Überlegungen zeigen, wie man die Lösungsmenge jedes linearen Gleichungssystems bestimmen kann. Man erhält dabei nach 3.1.1.10 im Fall einer nichtleeren Lösungsmenge durch die Transformation auf Zeilenstufenform sogar eine ausgezeichnete Bijektion zwischen  $t$ -Tupeln von Elementen von  $K$  und besagter Lösungsmenge, für  $t = m - r$  die Zahl der Variablen abzüglich der „Zahl der Stufen“, die eben jeder Vorgabe von  $x_j$  für  $j$  verschieden von den „Spaltenindizes der Stufen“  $j \neq s(1), \dots, s(r)$  die durch diese Vorgabe eindeutig bestimmte Lösung zuordnet. Der Gauß-Algorithmus gibt uns allerdings nicht vor, welche Zeilenvertauschungen wir unterwegs verwenden sollen. Damit stellt sich die Frage, ob wir unabhängig von der Wahl dieser Zeilenvertauschungen stets bei derselben Matrix in Zeilenstufenform ankommen. Das ist nun zwar nicht richtig, aber dennoch sind die „Breiten der einzelnen Stufen“ alias die Spaltenindizes  $s(i)$  der Stufen unabhängig von allen Wahlen. In der Tat lassen sie sich auch direkt beschreiben, indem wir im zugehörigen homogenisierten Gleichungssystem unsere Variablen von hinten durchgehen und jeweils fragen: Gibt es für jedes  $(x_{j+1}, x_{j+2}, \dots, x_m)$ , das zu einer Lösung  $(x_1, x_2, \dots, x_m)$  ergänzbar ist, nur ein  $x_j$  derart, daß auch  $(x_j, x_{j+1}, x_{j+2}, \dots, x_m)$  zu einer Lösung  $(x_1, x_2, \dots, x_m)$  ergänzbar ist? Genau dann lautet die Antwort „ja“, wenn in der  $j$ -ten Spalte eine neue Stufe beginnt.

**3.1.1.15 (Unabhängigkeit der Stufenzahl von der Variablenreihung).** Nun könnten wir auch vor dem Anwenden des Gauß-Algorithmus zuerst unsere Variablen umnummerieren alias die Spalten unserer Koeffizientenmatrix vertauschen. Wir erhielten wieder eine Bijektion zwischen  $u$ -Tupeln von Elementen von  $K$  mit der Lösungsmenge wie eben. Die Frage, der wir uns als nächstes zuwenden wollen, lautet nun: Gilt stets  $u = t$ , in anderen Worten, landen wir bei einer Zeilenstufenform mit derselben Zahl von Stufen, wenn wir zuerst die Spalten unseres Systems

$$\left( \begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 2 & 2 & 1 & 2 \end{array} \right) \xrightarrow{\text{Sub}} \begin{array}{l} x_1 + 3x_2 = 1 \\ 2x_1 + 2x_2 + x_3 = 2 \end{array}$$

$\downarrow$

$$\left( \begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 0 & -4 & 1 & 0 \end{array} \right) \xrightarrow{\text{Sub}} \begin{array}{l} x_3 \text{ f\"ur Parameter,} \\ x_2 = x_3/4 \\ x_1 = 1 - (3/4)x_3 \end{array}$$

Ein lineares Gleichungssystem mit zwei Gleichungen und drei Unbekannten, dessen L\"osungsmenge nach unserer allgemeinen Theorie f\"ur jedes  $x_3$  genau einen Punkt  $(x_1, x_2, x_3)$  enth\"alt, und zwar haben wir wegen der zweiten Gleichung  $x_2 = x_3/4$  und dann wegen der ersten Gleichung  $x_1 = 1 - (3/4)x_3$ , so daß die allgemeine L\"osung lautet  $(1 - (3/4)\lambda, \lambda/4, \lambda)$  f\"ur variables  $\lambda$ .

willkürlich vertauschen, bevor wir den Gauß-Algorithmus durchführen? Die Antwort lautet wieder „Ja“, aber hierzu ist mir kein ganz elementares Argument mehr eingefallen. Darauf war ich sogar ganz froh: Diese Frage kann so nämlich zur Motivation der Entwicklung der abstrakten Theorie der Vektorräume dienen, mit der wir an dieser Stelle beginnen. Wir führen in diesem Rahmen den auch in vielen anderen Zusammenhängen äußerst nützlichen Begriff der „Dimension“ eines „Vektorraums“ ein, und zeigen in 3.2.1.11, daß die Stufenzahl unabhängig von allen Wahlen als die „Dimension des Lösungsraums“ des zugehörigen homogenisierten Gleichungssystems beschrieben werden kann. Zunächst jedoch führen wir einige weitere Begriffe ein, die wir dabei und auch darüber hinaus noch oft brauchen werden.

### 3.1.2 Vektorräume

**Definition 3.1.2.1.** Ein Vektorraum  $V$  über einem Körper  $K$  ist ein Paar bestehend aus einer abelschen Gruppe  $V = (V, +)$  und einer Abbildung

$$\begin{array}{ccc} K \times V & \rightarrow & V \\ (\lambda, \vec{v}) & \mapsto & \lambda \vec{v} \end{array}$$

derart, daß für alle  $\lambda, \mu \in K$  und  $\vec{v}, \vec{w} \in V$  die folgenden Identitäten gelten:

$$\begin{aligned} \lambda(\vec{v} + \vec{w}) &= (\lambda\vec{v}) + (\lambda\vec{w}) \\ (\lambda + \mu)\vec{v} &= (\lambda\vec{v}) + (\mu\vec{v}) \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1_K \vec{v} &= \vec{v} \end{aligned}$$

Wie bei der Axiomatik eines Körpers 2.2.4.2 heißen die ersten beiden Gesetze die **Distributivgesetze**. In Analogie zu der Sprechweise bei Mengen mit Verknüpfung heißt das dritte Gesetz das **Assoziativgesetz**.

3.1.2.2. Die Elemente eines Vektorraums nennt man meist **Vektoren**. Die Elemente des Körpers heißen in diesem Zusammenhang oft **Skalare** und der Körper selber der **Grundkörper**. Die Abbildung  $(\lambda, \vec{v}) \mapsto \lambda \vec{v}$  heißt die **Multiplikation mit Skalaren** oder auch die **Operation des Körpers  $K$  auf  $V$** . Sie ist nicht zu verwechseln mit dem „Skalarprodukt“, das wir in 4.1.1.2 einführen und das aus zwei Vektoren einen Skalar macht. Ich habe oben aus didaktischen Gründen die Addition von Vektoren  $+$  notiert, um sie von der Addition von Körperelementen zu unterscheiden, aber das werde ich nicht lange durchhalten. Mit der auch in diesem Zusammenhang allgemein üblichen Konvention „Punkt vor Strich“ und der zu  $+$  vereinfachten Notation für die Addition von Vektoren und der Abkürzung  $1_K = 1$  für das multiplikativ neutrale Element des Grundkörpers können unsere

Vektorraumaxiome dann etwas übersichtlicher geschrieben werden als die Forderung, daß für alle Skalare  $\lambda, \mu$  und alle Vektoren  $\vec{v}, \vec{w}$  gelten möge

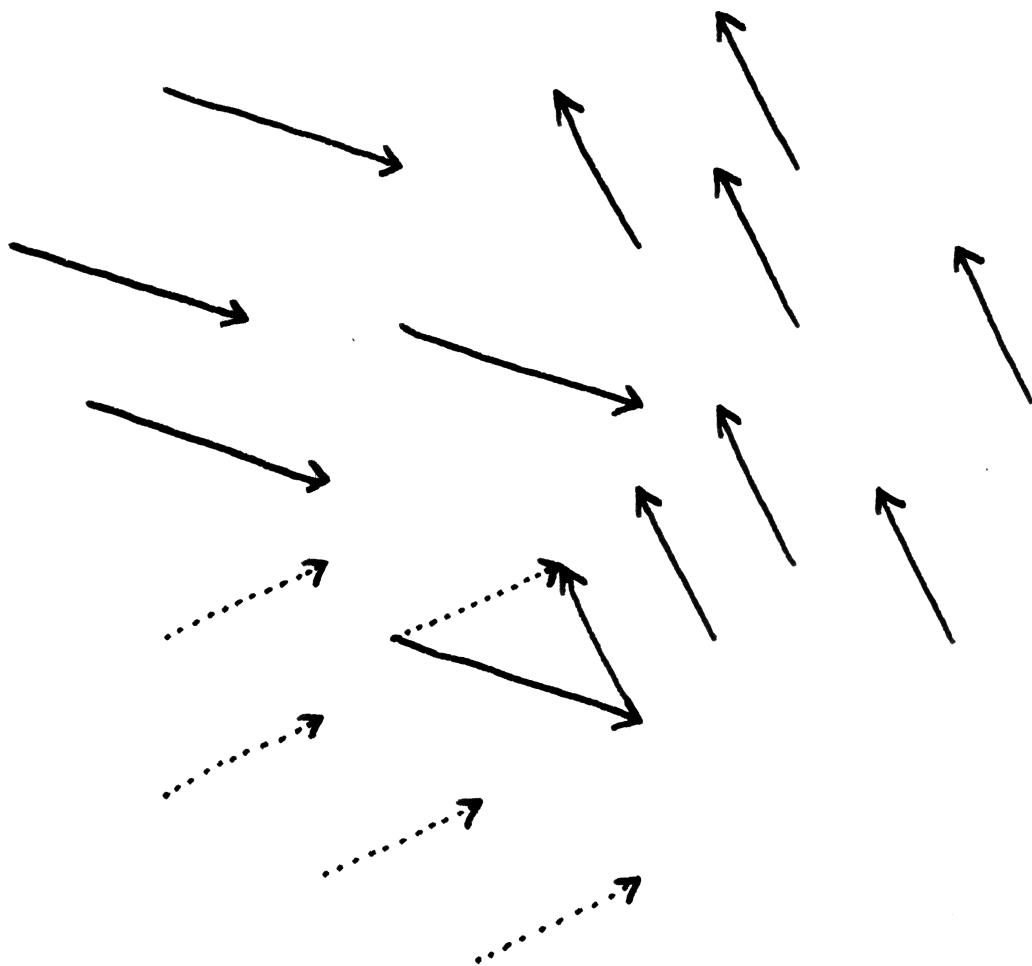
$$\begin{aligned}\lambda(\vec{v} + \vec{w}) &= \lambda\vec{v} + \lambda\vec{w} \\ (\lambda + \mu)\vec{v} &= \lambda\vec{v} + \mu\vec{v} \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1\vec{v} &= \vec{v}\end{aligned}$$

Ich habe aus didaktischen Gründen bis hierher Vektoren stets mit einem Pfeil notiert, das halte ich wohl etwas länger durch, aber auf Dauer werden Sie sich auch den Pfeil selbst dazudenken müssen. Das neutrale Element der abelschen Gruppe  $V$  notieren wir  $\vec{0}$  und nennen es den **Nullvektor**. Die letzte Bedingung  $1\vec{v} = \vec{v}$  schließt zum Beispiel den Fall aus, daß wir für  $V$  irgendeine von Null verschiedene abelsche Gruppe nehmen und dann einfach  $\lambda\vec{v} = \vec{0}$  setzen für alle  $\lambda \in K$  und  $\vec{v} \in V$ .

*Beispiel 3.1.2.3 (Die schmutzige Anschauung).* Ich stelle mir als Vektorraum gerne wie in 1.1.2.5 ausgeführt die Menge  $V$  aller Parallelverschiebungen der schmutzigen Ebene oder auch die Menge  $V$  der Parallelverschiebungen des schmutzigen Raums der Anschauung vor, mit der „Hintereinanderausführung“ als Addition und der offensichtlichen Multiplikation mit reellen Skalaren. Diese Mengen von Parallelverschiebungen nenne ich den **schmutzigen Richtungsraum** der Ebene beziehungsweise des Raums. Graphisch mag man diese Parallelverschiebungen alias Vektoren durch Pfeile in der Ebene oder oder im Raum darstellen und ihre Addition wie in nebenstehendem Bild veranschaulichen. Das ist nur leider im mathematischen Sinne kein recht eigentlich wohldefiniertes Beispiel: Schon die Frage, ob diese Parallelverschiebungen eigentlich „wohlunterschiedene Objekte unserer Anschauung oder unseres Denkens“ sind, und wie man sie eigentlich zu definieren hätte, scheint mir nicht so einfach und eindeutig zu beantworten. So bin ich in der schizophrenen Lage, daß mir dieses Beispiel einerseits besonders nahrhaft und motivierend scheint, daß es aber andererseits für unsere rein auf Mengenlehre aufgebaute aseptisch steril perfekte Mathematik zu schmutzig ist, um als echtes Beispiel durchzugehen.

*Ergänzung 3.1.2.4.* Wann immer ich einen Begriff mit dem Zusatz „der Anschauung“ oder „anschaulich“ oder „schmutzig“ versehe, soll gemeint sein, daß er nicht in einem mathematisch wie auch immer präzise definierten Sinne zu verstehen ist, also nicht als ein Gebilde der Mengenlehre, sondern eben anschaulich.

*Beispiel 3.1.2.5 (Funktionenräume als Vektorräume).* Gegeben eine Menge  $X$  und ein Körper  $K$  ist die Menge  $\text{Ens}(X, K)$  aller Abbildungen  $X \rightarrow K$  ein  $K$ -Vektorraum, wenn man die Addition durch  $(f + g)(x) := f(x) + g(x)$  erklärt und die Multiplikation mit Skalaren durch  $(\lambda f)(x) := \lambda(f(x))$ . Insbesondere erhält



Die Hintereinanderausführung der beiden Parallelverschiebungen der Tafel- oder hier vielmehr der Papierebene, die durch die durchgezogenen Pfeile dargestellt werden, wird die durch die gepunkteten Feile dargestellt.

so auch die Menge  $\text{Mat}(n \times m; K)$  aller  $(n \times m)$ -Matrizen mit Einträgen in einem Körper  $K$  aus 3.1.1.11 die Struktur eines  $K$ -Vektorraums.

**Beispiel 3.1.2.6 (Lösungsmengen als Vektorräume).** Gegeben ein homogenes lineares Gleichungssystem in  $n$  Variablen wird seine Lösungsmenge  $L$  ein  $K$ -Vektorraum, wenn wir sie mit der komponentenweisen Addition  $+$  und der komponentenweisen Multiplikation mit Skalaren versehen.

**Ergänzung 3.1.2.7.** Im Fall eines Schiefkörpers  $K$  muß man an dieser Stelle mehr aufpassen. Lösungen eines linearen Gleichungssystems bleiben dann nur nur Lösungen, wenn man sie von rechts mit Skalaren multipliziert. Das führt zur Erkenntnis, daß man in diesem Fall „Rechtsvektorräume“ und „Linksvektorräume“ unterscheiden muß und die Lösungsmenge eines linearen Gleichungssystems, bei dem die Koeffizienten von links an die Variablen daranmultipliziert werden, einen Rechtsvektorraum bildet.

**Ergänzung 3.1.2.8 (Ursprung der Terminologie).** Die Bezeichnung als „Vektor“ kommt von lateinisch „vehere“ für „fahren, transportieren“. Sie röhrt von unserem Beispiel 1.1.2.5 der Gesamtheit aller Parallelverschiebungen der Ebene oder des Raums her, die ja in gewisser Weise Punkte transportieren. Auf Deutsch könnte man diese Intuition wiedergeben, indem man statt von Vektoren etwa von „Schiebern“ redet. Beim Gedanken an eine Vorlesung über die „Lehre von der Schieberei“ bin ich aber doch glücklicher mit der gewohnten, vom Latein geprägten Terminologie. Die Bezeichnung „Skalare“ für Elemente des zugrundeliegenden Körpers kommt von dem lateinischen Wort „scala“ für „Leiter“ und hat sich von dort über eine Bezeichnung für das Metermaß entwickelt zu einer Bezeichnung für das, was man auf einer Meßskala ablesen kann, als da heißt zu einer Bezeichnung für reelle Zahlen. In Mathematik und Physik werden nun aber nicht nur reelle Vektorräume betrachtet, und so überträgt man dann dieses Wort weiter und verwendet es auch im allgemeinen als Bezeichnung für die Elemente des jeweiligen Grundkörpers.

**3.1.2.9 (Produkt mit dem Skalar Null).** Gegeben ein Vektorraum  $V$  und ein Vektor  $\vec{v} \in V$  gilt  $0_K \vec{v} = \vec{0}$ . Multipliziert man also einen beliebigen Vektor mit dem Skalar Null, erhält man stets den Nullvektor. In der Tat finden wir mit dem zweiten Distributivgesetz  $0_K \vec{v} = (0_K + 0_K) \vec{v} = 0_K \vec{v} + 0_K \vec{v}$  und Subtraktion von  $0_K \vec{v}$  alias Addition seines Negativen  $-0_K \vec{v}$  auf beiden Seiten liefert  $\vec{0} = 0_K \vec{v}$ .

**3.1.2.10 (Produkt mit dem Skalar minus Eins).** Gegeben ein Vektorraum  $V$  und ein Vektor  $\vec{v} \in V$  gilt  $(-1_K) \vec{v} = -\vec{v}$ . Multipliziert man also in Worten das Negative der Eins des Grundkörpers mit einem beliebigen Vektor, so erhält man das Negative von besagtem Vektor. In der Tat finden wir mit der letzten und der zweiten Formel aus der Definition  $\vec{v} + (-1_K) \vec{v} = 1_K \vec{v} + (-1_K) \vec{v} = (1_K + (-1_K)) \vec{v} = 0_K \vec{v} = \vec{0}$ . Damit ist  $(-1_K) \vec{v}$  in der Tat das additive Inverse von  $\vec{v}$ .

*Beispiel 3.1.2.11.* Gegeben ein Körper  $K$  ist die abelsche Gruppe  $V = K$  mit der durch die Multiplikation von  $K$  gegebenen Multiplikation mit Skalaren ein  $K$ -Vektorraum.

*Beispiel 3.1.2.12.* Gegeben ein Körper  $K$  wird jede einelementige Menge  $V$  mittels der offensichtlichen Operationen zu einem  $K$ -Vektorraum. Wir sprechen dann von einem **Nullvektorraum**, weil er eben nur aus dem Nullvektor besteht, und verwenden oft auch den bestimmten Artikel und sprechen von *dem* Nullvektorraum, da er ja „im wesentlichen“ eindeutig bestimmt ist. Wir bezeichnen diesen Vektorraum und allgemeiner die einelementige Gruppe gerne mit 0. Dieses Symbol muß in der Mathematik für die verschiedensten Dinge herhalten.

*Beispiel 3.1.2.13.* Die additive Gruppe  $\mathbb{R}$  der reellen Zahlen ist in offensichtlicher Weise ein  $\mathbb{Q}$ -Vektorraum. Ist allgemeiner  $\varphi : K \rightarrow L$  ein Körperhomomorphismus, so wird die additive Gruppe  $L$  ein  $K$ -Vektorraum mittels der Multiplikation mit Skalaren  $\lambda a := \varphi(\lambda)a$ .

*Beispiel 3.1.2.14 (Prozentrechnung).* Bei der Prozentrechnung geht man stets implizit von einem eindimensionalen reellen Vektorraum aus. Wenn man etwa sagt, 80% einer Pralinenschachtel sei Luft, so mag man sich im formalen Rahmen dieser Vorlesung einen eindimensionalen reellen Vektorraum  $V$  denken, dessen Elemente gewisse „Volumina“ sind, und darin einen Vektor  $v \in V$ , das „Volumen der Pralinenschachtel“, und will sagen, daß  $(80/100)v$  das in der Schachtel von Luft eingenommene Volumen ist. Oft gibt man den fraglichen eindimensionalen Vektorraum auh explizit an und spricht von **Volumenprozent** oder **Gewichtsprozent** oder dergleichen. Den Vektorraum der Volumina diskutieren wir noch ausführlich in 4.6.1.16. Es sollte aber auch hier schon zumindest anschaulich klar sein, daß man Volumina addieren und mit Skalaren multiplizieren kann und daß man so, wenn man formal auch noch negative Volumina zuläßt, einen eindimensionalen reellen Vektorraum erhält alias daß alle Rechenregeln aus unserer Definition eines Vektorraums 3.1.2.1 gelten.

## Übungen

*Übung 3.1.2.15 (Produkt mit dem Nullvektor).* Gegeben ein Vektorraum  $V$  über einem Körper  $K$  zeige man für alle  $\lambda \in K$  die Identität  $\lambda\vec{0} = \vec{0}$ . Weiter zeige man, daß aus  $\lambda\vec{v} = \vec{0}$  folgt  $\lambda = 0$  oder  $\vec{v} = \vec{0}$ .

*Übung 3.1.2.16.* Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  und ein Vektor  $\vec{v} \in V$  eine ganze Zahl  $n \in \mathbb{Z}$  gilt mit unserer Notation  $n_K$  aus 2.2.4.12 stets  $n_K\vec{v} = n\vec{v}$  oder ausgeschrieben in unserer Notation 2.2.2.11 für iterierte Verknüpfungen  $(n^{+1}_K)\vec{v} = n^+\vec{v}$ . Hinweis: Die Fälle  $n = 0$  und  $n = (-1)$  dieser Aussage wurden bereits in 3.1.2.9 und 3.1.2.10 besprochen.

*Ergänzende Übung 3.1.2.17.* Für eine vorgegebene abelsche Gruppe  $(V, +)$  gibt es höchstens eine Abbildung  $\mathbb{Q} \times V \rightarrow V$  derart, daß sie mit dieser Abbildung als Multiplikation mit Skalaren ein  $\mathbb{Q}$ -Vektorraum wird.

*Ergänzende Übung 3.1.2.18.* Eine Gruppe, in der jedes Element sein eigenes Inverses ist, kann auf genau eine Weise mit der Struktur eines Vektorraums über dem Körper mit zwei Elementen versehen werden. Ein Beispiel ist unsere Gruppe aus 2.2.2.19.

*Übung 3.1.2.19.* Gegeben eine Menge  $X$  und ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  ist auch die Menge  $\text{Ens}(X, V)$  aller Abbildungen  $X \rightarrow V$  ein  $K$ -Vektorraum, wenn man sie mit der Addition gegeben durch  $(f + g)(x) := f(x) + g(x)$  und mit der Multiplikation mit Skalaren gegeben durch  $(\lambda f)(x) := \lambda(f(x))$  versieht. Das verallgemeinert unser Beispiel 3.1.2.5.

*Ergänzende Übung 3.1.2.20.* Ist  $\varphi : L \rightarrow K$  ein Körperhomomorphismus und  $V$  ein  $K$ -Vektorraum, so wird die abelsche Gruppe  $V$  mit der durch die Formel  $\lambda \vec{v} := \varphi(\lambda) \vec{v}$  erklärten Multiplikation mit Skalaren aus  $L$  ein  $L$ -Vektorraum. Man sagt dann, dieser  $L$ -Vektorraum entstehe durch **Restriktion der Skalare** aus dem  $K$ -Vektorraum  $V$ .

### 3.1.3 Endliche Produkte von Mengen

3.1.3.1 (**Längere kartesische Produkte**). Bis jetzt hatten wir nur das kartesische Produkt  $X \times Y$  von zwei Mengen  $X$  und  $Y$  betrachtet. Ebenso kann man auch für mehr Mengen  $X_1, \dots, X_n$  das kartesische Produkt

$$X_1 \times \dots \times X_n := \{(x_1, \dots, x_n) \mid x_i \in X_i \text{ für } 1 \leq i \leq n\}$$

einführen. Die Elemente von so einem Produkt bezeichnet man als **angeordnete  $n$ -Tupel** oder auch einfach als **Tupel**. In diesem Zusammenhang heißen 2-Tupel auch **Paare** oder genauer **angeordnete Paare** und 3-Tupel **Tripel** oder genauer **angeordnete Tripel**. Die  $x_i$  heißen die **Komponenten** unseres Tupels  $(x_1, \dots, x_n)$ . Die Mengen  $X_i$  heißen die **Faktoren** unseres kartesischen Produkts. Wir vereinbaren, daß wir das „leere Produkt“ als die einelementige Menge interpretieren.

3.1.3.2. Im deutschsprachigen Raum verwendet man auf der Schule für Tupel vielfach auch die alternative Notation  $(x_1 | \dots | x_n)$ . Das geschieht, um Verwechslungen zwischen 2-Tupeln von natürlichen Zahlen und Dezimalbrüchen zu vermeiden, die ja im deutschsprachigen Raum als „Kommazahlen“ notiert werden.

3.1.3.3 (**Abbildungen in ein Produkt**). Für ein kartesisches Produkt von Mengen hat man stets die **Projektionsabbildungen** oder **Projektionen**

$$\begin{aligned} \text{pr}_i : X_1 \times \dots \times X_n &\rightarrow X_i \\ (x_1, \dots, x_n) &\mapsto x_i \end{aligned}$$

Wir erhalten dann für jede weitere Menge  $Z$  eine Bijektion

$$\begin{aligned} \text{Ens}(Z, X_1 \times \dots \times X_n) &\xrightarrow{\sim} \text{Ens}(Z, X_1) \times \dots \times \text{Ens}(Z, X_n) \\ f &\mapsto (\text{pr}_1 \circ f, \dots, \text{pr}_n \circ f) \end{aligned}$$

zwischen Abbildungen in das Produkt und Tupeln von Abbildungen in seine Faktoren. Die Umkehrung dieser **kanonischen Bijektion** notieren wir sozusagen gar nicht. Gegeben Abbildungen  $f_i : Z \rightarrow X_i$  notieren wir genauer die Abbildung  $f : Z \rightarrow X_1 \times \dots \times X_n$  von  $Z$  in das kartesische Produkt der  $X_i$  gegeben durch die Vorschrift  $z \mapsto (f_1(z), \dots, f_n(z))$  schlicht

$$f = (f_1, \dots, f_n)$$

In der exponentiellen Schreibweise geschrieben liest sich unsere Bijektion ganz suggestiv als eine Bijektion  $(X_1 \times \dots \times X_n)^Z \xrightarrow{\sim} X_1^Z \times \dots \times X_n^Z$ . Besonders wichtig ist die **diagonale Einbettung** oder **Diagonale**

$$\begin{aligned} \Delta := \Delta_X := (\text{id}, \text{id}) : X &\rightarrow X \times X \\ x &\mapsto (x, x) \end{aligned}$$

*Vorschau 3.1.3.4 (Abbildungen aus kartesischen Produkten).* Eine Abbildung  $f : X_1 \times \dots \times X_n \rightarrow Z$  von einem kartesischen Produkt in eine beliebige Menge  $Z$  nennen wir auch eine  **$n$ -Multiabbildung** und notieren sie gerne

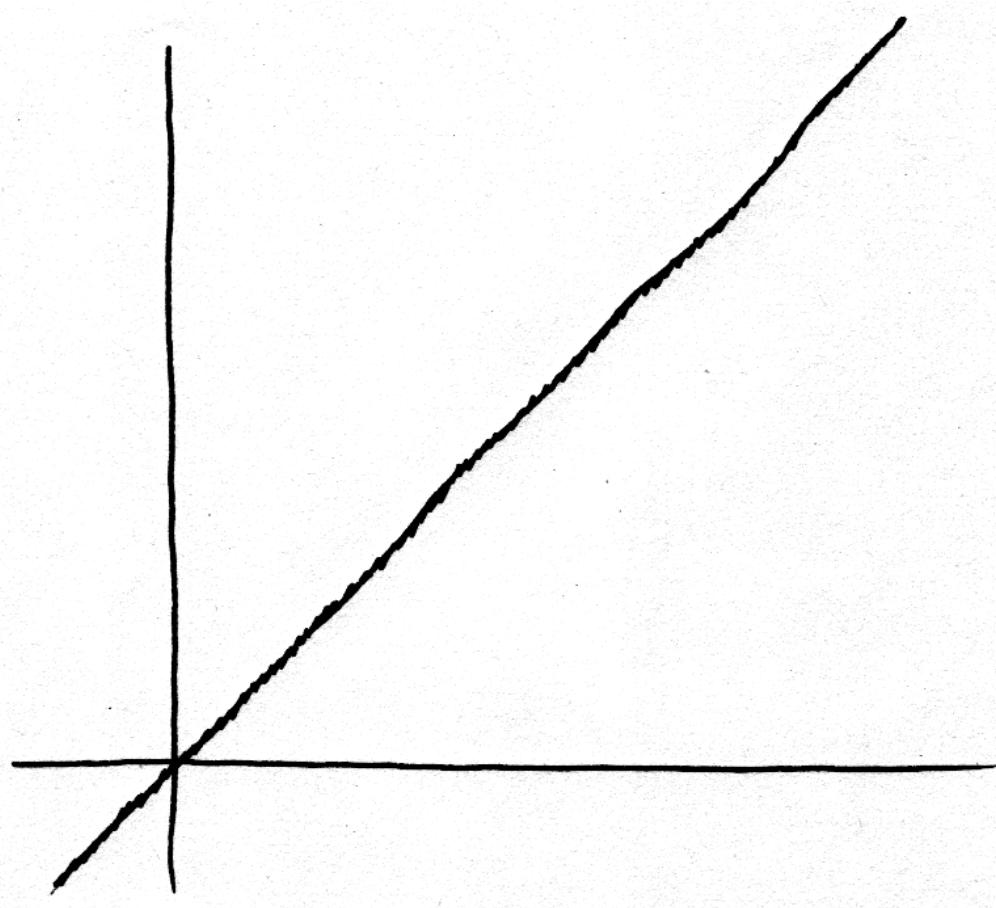
$$f : X_1 \times \dots \times X_n \rightarrow Z$$

Unter einer **0-Multiabbildung nach  $Z$**  verstehen wir in diesem Kontext ein Element von  $Z$ . Solche Multiabbildungen lassen sich dann in offensichtlicher Weise „multiverknüpfen“, aber das soll erst in ?? weiter formalisiert werden.

*Ergänzung 3.1.3.5 (Kartesisches Produkt von Abbildungen).* Sind ein weiteres Produkt von der Form  $Y = Y_1 \times \dots \times Y_n$  sowie Abbildungen  $f_i : X_i \rightarrow Y_i$  gegeben, so können wir insbesondere die Abbildung

$$\begin{aligned} X_1 \times \dots \times X_n &\rightarrow Y_1 \times \dots \times Y_n \\ (x_1, \dots, x_n) &\mapsto (f_1(x_1), \dots, f_n(x_n)) \end{aligned}$$

betrachten. Wir notieren sie  $f_1 \times \dots \times f_n := (f_1 \text{ pr}_1, \dots, f_n \text{ pr}_n)$  mit der im Sinne der in 3.1.3.3 eingeführten Notation zu verstehenden rechten Seite. Man beachte, daß im allgemeinen keineswegs alle Abbildungen  $X_1 \times \dots \times X_n \rightarrow Y_1 \times \dots \times Y_n$  von dieser Form sind. Das kartesische Produkt von Surjektionen ist stets wieder surjektiv. Das kartesische Produkt von Injektionen ist stets wieder injektiv.



Das Bild der diagonalen Einbettung  $\Delta : \mathbb{R} \rightarrow \mathbb{R}^2$ ,  $t \mapsto (t, t)$ .

*Ergänzung 3.1.3.6 (Assoziativität kartesischer Produkte).* Gegeben drei Mengen  $X, Y, Z$  mag man sich nun die Frage stellen, inwieweit die drei Mengen  $(X \times Y) \times Z$ ,  $X \times (Y \times Z)$  und  $X \times Y \times Z$  übereinstimmen, und allgemeiner, inwieweit „das kartesische Produkt  $\times$  assoziativ ist“. Wir werden derartige Fragen später im Rahmen der Kategorientheorie ausführlicher diskutieren. Hier sei nur bemerkt, daß zum Beispiel alle unsere drei Tripelprodukte wohlbestimmte Projektionen  $\text{pr}_X$ ,  $\text{pr}_Y$  und  $\text{pr}_Z$  auf  $X$ ,  $Y$  und  $Z$  haben und daß es eindeutig bestimmte Bijektionen zwischen ihnen gibt, die mit diesen drei Projektionen verträglich sind. Wegen dieser „Eindeutigkeit bis auf eindeutige Bijektionen“ werden wir uns erlauben, die drei fraglichen Tripelprodukte schlicht als gleich anzusehen. In derselben Weise verfahren wir in analogen Situationen mit mehr Faktoren.

**3.1.3.7 (Einelementige Menge).** In derselben Weise sprechen auch mit einem bestimmten Artikel von „der“ einelementigen Menge. Wir notieren sie manchmal  $\text{ens}$ , da es sich um das „finale Objekt der Kategorie Ens der Mengen“ handelt, aber das brauchen Sie hier noch nicht zu verstehen. Das einzige Element der ein-elementigen Menge notieren wir gerne  $*$  und haben also in Formeln

$$\text{ens} = \{ *\}$$

**3.1.3.8 (Tupel von Elementen einer Menge).** Das kartesische Produkt von  $n$  Kopien einer Menge  $X$  kürzt man meist ab mit

$$X^n$$

Die Elemente von  $X^n$  sind also  $n$ -Tupel von Elementen aus  $X$ . Es ist sinnvoll und allgemeine Konvention, diese Notation auf den Fall  $n = 0$  dadurch auszudehnen, daß man  $X^0$  als die einelementige Menge auffaßt, in Formeln  $X^0 = \text{ens}$ , so daß wir für alle  $n, m \geq 0$  eine kanonische Bijektion  $X^n \times X^m \xrightarrow{\sim} X^{n+m}$  erhalten. Wenn ich Verwechslungen mit anderen Notationen befürchte, die Sie später kennenlernen werden, schreibe ich statt  $X^n$  auch ausführlicher  $X^{\times n}$ .

**Beispiele 3.1.3.9 (Der Vektorraum der  $n$ -Tupel).** Einige Beispiele für Vektorräume wurden bereits in 1.1.2 diskutiert. Besonders wichtig ist das Beispiel des Vektorraums

$$V = K^n$$

über einem vorgegebenen Körper  $K$ . Hier verwenden wir die Notation 3.1.3.8, die Elemente von  $K^n$  sind also  $n$ -Tupel von Elementen des Körpers  $K$ . Wir notieren die Komponenten dieser  $n$ -Tupel im folgenden der Übersichtlichkeit halber untereinander, nicht wie zuvor nebeneinander und durch Kommata getrennt. Die

Addition von Vektoren und Multiplikation mit Skalaren seien gegeben durch

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} := \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix}$$

$$\lambda \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} := \begin{pmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{pmatrix}$$

für  $\lambda, v_1, \dots, v_n, w_1, \dots, w_n \in K$ . Die Erste unserer Gleichungen definiert die Summe zweier  $n$ -Tupel, also die Addition in unserem Vektorraum  $V = K^n$ , indem sie diese durch die Addition im Körper  $K$  ausdrückt. Die zweite Gleichung leistet dasselbe für die Multiplikation mit Skalaren. An dieser Stelle gebe ich einen ersten Teil meiner didaktischen Notation auf und schreibe von nun an  $+$  statt  $\dot{+}$ . Gegeben  $\vec{v} \in K^n$  schreibe ich seine Komponenten  $v_1, v_2, \dots, v_n$  und versehe sie nicht mit Pfeilen, da sie ja Elemente des Grundkörpers sind. Wenn irgendwo einmal  $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n$  stehen sollte, so sind nicht die  $n$  Komponenten eines  $n$ -Tupels  $\vec{v}$  gemeint, sondern vielmehr  $n$  Vektoren eines Vektorraums. Sobald ich die Pfeil-Notation aufgebe, muß der Leser aus dem Kontext erschließen, was im Einzelfall jeweils gemeint ist.

## Übungen

*Übung 3.1.3.10.* Gegeben ein Körper  $K$  und  $K$ -Vektorräume  $V_1, \dots, V_n$  können wir das kartesische Produkt  $V_1 \times \dots \times V_n$  zu einem  $K$ -Vektorraum machen, indem wir die Addition sowie die Multiplikation mit Skalaren komponentenweise definieren. In Formeln sieht das dann so aus wie 3.1.3.9, nur daß wir den  $v_i$  und  $w_i$  Pfeile aufsetzen und statt  $v_i, w_i \in K$  wie dort nun  $\vec{v}_i, \vec{w}_i \in V_i$  nehmen müssen. Den so entstehenden Vektorraum notieren wir auch

$$V_1 \oplus \dots \oplus V_n$$

und nennen ihn das **Produkt** oder auch die **direkte Summe** der  $V_i$ . Insbesondere ist  $K^n$  die direkte Summe  $K \oplus \dots \oplus K$  von  $n$  Kopien des  $K$ -Vektorraums  $K$ .

*Übung 3.1.3.11.* Seien  $f : X \rightarrow Y$  und  $g : Z \rightarrow W$  Abbildungen und

$$f \times g : X \times Z \rightarrow Y \times W$$

ihr Produkt. Ist  $f \times g$  surjektiv und gilt  $W \neq \emptyset$ , so ist  $f$  surjektiv. Ist  $f \times g$  injektiv und gilt  $Z \neq \emptyset$ , so ist  $f$  injektiv.

### 3.1.4 Ordnungen und Teilordnungen\*

3.1.4.1. Bei den Inhalten dieses Abschnitts hoffe ich, daß sie rechtzeitig in der Analysis besprochen werden, so daß sie in der linearen Algebra übersprungen werden können. Ich habe ihn aus ?? kopiert, wo zusätzlich noch Supremum und Infimum besprochen werden.

**Definition 3.1.4.2.** Eine **Relation**  $R$  auf einer Menge  $X$  ist eine Teilmenge  $R \subset X \times X$  des kartesischen Produkts von  $X$  mit sich selbst, also eine Menge von Paaren von Elementen von  $X$ . Statt  $(x, y) \in R$  schreiben wir in diesem Zusammenhang meist  $xRy$ . Eine Relation  $R$  heißt eine **Ordnungsrelation** oder eine **Teilordnung** oder eine **partielle Ordnung**, wenn für alle  $x, y, z \in X$  gilt:

1. **Transitivität:**  $(xRy \text{ und } yRz) \Rightarrow xRz$ ;
2. **Antisymmetrie:**  $(xRy \text{ und } yRx) \Rightarrow x = y$ ;
3. **Reflexivität:**  $xRx$  für alle  $x \in X$ .

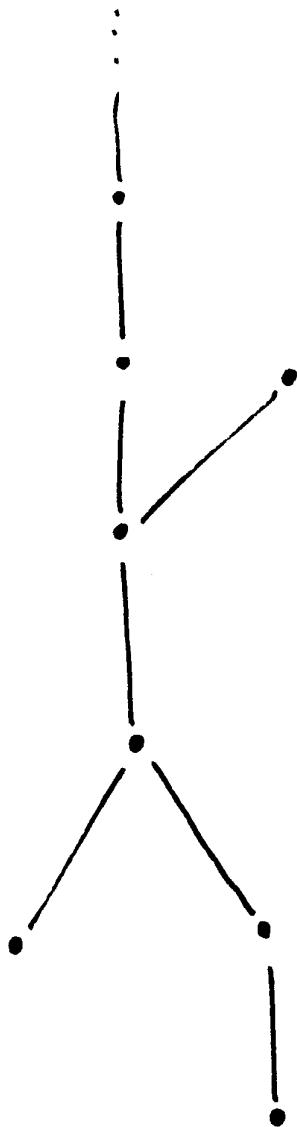
Eine Teilordnung heißt eine **Ordnung** oder **Anordnung**, wenn wir zusätzlich haben

4. **Totalität:** Für alle  $x, y \in X$  gilt  $xRy$  oder  $yRx$ .

3.1.4.3 (**Diskussion der Terminologie**). In der Literatur heißt eine Teilordnung auch eine **Halbordnung** oder kurz eine „Ordnung“. Wir verstehen jedoch unter einer Ordnung stets eine Ordnungsrelation, die auch die Eigenschaft der Totalität besitzt. Auf Englisch benutzt man für eine teilgeordnete Menge alias „partially ordered set“ gerne die Abkürzung **poset**. Eine Ordnung in unserem Sinne heißt in der Literatur auch eine **totale Ordnung** oder eine **lineare Ordnung**.

*Vorschau* 3.1.4.4. Allgemeiner versteht man unter einer **Relation  $R$  zwischen einer Menge  $X$  und einer Menge  $Y$**  eine Teilmenge  $R \subset X \times Y$ . In diesem Sinne sind dann auch unsere Abbildungen aus 2.1.4.2 spezielle Relationen. In Teilen der Literatur heißen derartige Relationen auch „Korrespondenzen“. Noch allgemeiner betrachtet man auch für  $n \geq 0$  und Mengen  $X_1, \dots, X_n$  Teilmengen  $R \subset X_1 \times \dots \times X_n$  und nennt sie  **$n$ -stellige Relationen**, aber das ist für uns vorerst noch nicht relevant.

3.1.4.5. Bei einer Ordnungsrelation  $R$  schreibt man meist  $x \leq y$  statt  $xRy$  und statt  $x \leq y$  schreibt man dann oft auch  $y \geq x$ . Weiter kürzt man  $(x \leq y \text{ und } x \neq y)$  ab mit  $x < y$  und ebenso  $(x \geq y \text{ und } x \neq y)$  mit  $x > y$ . Auf jeder angeordneten Menge definieren wir Verknüpfungen max und min in offensichtlicher Verallgemeinerung von 2.2.1.3.



Eine teilgeordnete Menge mit zwei minimalen und einem maximalen Element, die weder ein kleinstes noch ein größtes Element besitzt. Die Darstellung ist in der Weise zu verstehen, daß die fetten Punkte die Elemente unserer Menge bedeuten und daß ein Element größer ist als ein anderer genau dann, wenn es von diesem „durch einen aufsteigenden Weg erreicht werden kann“.

**Definition 3.1.4.6.** Sei  $(Y, \leq)$  eine teilgeordnete Menge.

1. Ein Element  $g \in Y$  heißt ein **größtes Element von  $Y$** , wenn gilt  $g \geq y \forall y \in Y$ . Ein Element  $g \in Y$  heißt ein **maximales Element von  $Y$** , wenn es kein  $y \in Y$  gibt mit  $y > g$ .
2. Ein Element  $k \in Y$  heißt ein **kleinstes Element von  $Y$** , wenn gilt  $k \leq y \forall y \in Y$ . Ein Element  $k \in Y$  heißt ein **minimales Element von  $Y$** , wenn es kein  $y \in Y$  gibt mit  $y < k$ .

3.1.4.7. Jede teilgeordnete Menge besitzt höchstens ein größtes und höchstens ein kleinstes Element. Wir dürfen deshalb den bestimmten Artikel verwenden und von **dem** größten beziehungsweise kleinsten Element reden. Besitzt eine teilgeordnete Menge ein größtes beziehungsweise ein kleinstes Element, so ist dies auch ihr einziges maximales beziehungsweise minimales Element. Im allgemeinen kann es jedoch maximale beziehungsweise minimale Elemente in großer Zahl geben, zumindest dann, wenn unsere Teilordnung keine Anordnung ist. Es kann auch durchaus passieren, daß es überhaupt kein minimales oder maximales Element gibt, und zwar selbst dann, wenn unsere teilgeordnete Menge nicht die leere Menge ist.

3.1.4.8. Gegeben teilgeordnete Mengen  $(X, \leq)$  und  $(Y, \leq)$  versteht man unter einem **Homomorphismus von teilgeordneten Mengen** oder gleichbedeutend einer **monoton wachsenden Abbildung** eine Abbildung  $\phi : X \rightarrow Y$  mit  $x \leq z \Rightarrow \phi(x) \leq \phi(z)$ . Wie immer erklärt man einen Isomorphismus als einen Homomorphismus  $\phi$  mit der Eigenschaft, daß es einen Homomorphismus  $\psi$  in die Gegenrichtung gibt derart, daß  $\psi \circ \phi$  und  $\phi \circ \psi$  die Identität sind. Man beachte, daß in diesem Fall ein bijektiver Homomorphismus keineswegs ein Isomorphismus zu sein braucht.

### 3.1.5 Untervektorräume

**Definition 3.1.5.1.** Eine Teilmenge  $U$  eines Vektorraums  $V$  heißt ein **Untervektorraum** oder **Teilraum**, wenn  $U$  den Nullvektor enthält und wenn aus  $\vec{u}, \vec{v} \in U$  und  $\lambda \in K$  folgt  $\vec{u} + \vec{v} \in U$  sowie  $\lambda \vec{u} \in U$ .

3.1.5.2. Statt zu fordern, daß unsere Teilmenge den Nullvektor enthält, reicht es wegen 3.1.2.9 schon aus, in obiger Definition zu fordern, daß unsere Teilmenge nicht leer ist. Diese Definitionsvariante wird oft vorgezogen, da sie zumindest prinzipiell leichter nachzuprüfen ist. Ich mag sie nicht, da sie noch ferner von der „eigentlich richtigen Definition“ ist, die ich in der folgenden Bemerkung erläutern will.

*Ergänzung 3.1.5.3 (Untervektorräume vom höheren Standpunkt).* Die vom höheren Standpunkt aus „richtige“ Definition eines Untervektorraums lautet wie folgt: Sei  $K$  ein Körper. Eine Teilmenge eines  $K$ -Vektorraums heißt ein Untervektorraum, wenn sie so mit der Struktur eines  $K$ -Vektorraums versehen werden kann, daß die Einbettung ein „Homomorphismus  $K$ -Vektorräumen“ wird. Ich kann diese „bessere“ Definition hier noch nicht geben, da wir Homomorphismen von  $K$ -Vektorräumen erst in 3.2.1.1 kennenlernen. Sie ist leider auch komplizierter. Sie scheint mir dennoch besser, da man in derselben Weise auch korrekte Definitionen von Untermonoiden, Untergruppen, Unterkörpern und Unter-was-nicht-noch-all-für-Strukturen erhält, die Sie erst später kennenlernen werden. Genaueres diskutieren wir in 4.7.3.12.

**3.1.5.4 (Lösungsmengen als Untervektorräume).** Unter einem homogenen linearen Gleichungssystem über einem gegebenen Körper  $K$  versteht man, wie in 3.1.1.5 besprochen, ein System von Gleichungen der Gestalt

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m &= 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m &= 0 \\ \vdots &\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m &= 0 \end{aligned}$$

Die Homogenität bedeutet, daß rechts nur Nullen stehen. Die Lösungsmenge eines solchen homogenen Gleichungssystems ist offensichtlich ein Untervektorraum  $L \subset K^m$ .

**3.1.5.5 (Untervektorräume des schmutzigen Richtungsraums der Ebene).** Das nun folgende Geschwafel darf nicht als Teil des formalen Aufbaus der Theorie mißverstanden werden. Ich erinnere an den schmutzigen Richtungsraum 3.1.2.3 der Ebene alias die Menge aller Parallelverschiebungen der Ebene mit ihrer Struktur als reeller Vektorraum. Seine Untervektorräume sind (1) der Nullraum, (2) die Teilmengen, die aus allen Verschiebungen bestehen, die eine vorgegebene Gerade in sich selbst überführen, und (3) der ganze Richtungsraum. Will man diese Untervektorräume graphisch darstellen, ist es hilfreich, einen festen Punkt der Ebene willkürlich als „Ursprung“ auszuzeichnen und die Menge derjenigen Punkte zu schwarz zu machen, die wir aus diesem festen Punkt durch Verschiebungen mit Vektoren unseres Untervektorraums erhalten können. Dann entsprechen die Untervektorräume den folgenden Teilmengen der Ebene: (1) Der einelementigen Teilmenge, die nur aus unserem Ursprung besteht, (2) allen Geraden, die unseren Ursprung enthalten, und (3) der ganzen Ebene.

**3.1.5.6 (Untervektorräume des schmutzigen Richtungsraums des Raums).** Das nun folgende Geschwafel darf nicht als Teil des formalen Aufbaus der Theorie mißverstanden werden. Ich erinnere an den schmutzigen Richtungsraum 3.1.2.3

des Raums alias die Menge aller Parallelverschiebungen des Raums mit ihrer Struktur als reeller Vektorraum. Seine Untervektorräume sind (1) der Nullraum, der nur aus der Identitätsverschiebung besteht, (2) die Teilmengen, die aus allen Verschiebungen bestehen, die eine vorgegebene Gerade in sich selbst überführen, (3) die Teilmengen, die aus allen Verschiebungen bestehen, die eine vorgegebene Ebene in sich selbst überführen, und (4) der ganze Richtungsraum.

**Proposition 3.1.5.7 (Von einer Teilmenge erzeugter Untervektorraum).** *Gegeben eine Teilmenge  $T$  eines Vektorraums  $V$  über einem Körper  $K$  gibt es unter allen Untervektorräumen von  $V$ , die  $T$  umfassen, einen kleinsten Untervektorraum*

$$\langle T \rangle = \langle T \rangle_{\text{lin}} = \langle T \rangle_K \subset V$$

*Er kann beschrieben werden als die Menge aller Vektoren  $\alpha_1 \vec{v}_1 + \dots + \alpha_r \vec{v}_r$  mit  $\alpha_1, \dots, \alpha_r \in K$  und  $\vec{v}_1, \dots, \vec{v}_r \in T$  zusammen mit dem Nullvektor im Fall  $T = \emptyset$ .*

3.1.5.8. Ein Ausdruck der Gestalt  $\alpha_1 \vec{v}_1 + \dots + \alpha_r \vec{v}_r$  heißt eine **Linearkombination** der Vektoren  $\vec{v}_1, \dots, \vec{v}_r$ . Hierbei sind nur endliche Summen erlaubt. Der kleinste  $T$  umfassende Untervektorraum  $\langle T \rangle \subset V$  heißt der **von  $T$  erzeugte Untervektorraum** oder der **von  $T$  aufgespannte Untervektorraum** oder auch das **Erzeugnis von  $T$**  oder der **Spann von  $T$**  oder die **lineare Hülle von  $T$** . Wenn wir den Nullvektor als die „leere Linearkombination von  $r = 0$  Vektoren“ verstehen, was hiermit vereinbart sei, so besteht das Erzeugnis von  $T$  demnach auch im Fall  $T = \emptyset$  genau aus allen Linearkombinationen von Vektoren aus  $T$ .

*Ergänzung 3.1.5.9.* Andere übliche Notationen für den von einer Teilmenge  $T$  eines Vektorraums erzeugten Untervektorraum sind  $\text{span}(T)$  und  $\text{lin}(T)$ .

*Beweis.* Es ist klar, daß die Linearkombinationen von Vektoren aus  $T$  einen Untervektorraum von  $V$  bilden, der  $T$  umfaßt. Es ist ebenso klar, daß jeder Untervektorraum von  $V$ , der  $T$  umfaßt, auch alle Linearkombinationen von Vektoren aus  $T$  enthalten muß.  $\square$

**Definition 3.1.5.10.** Eine Teilmenge eines Vektorraums heißt ein **Erzeugendensystem** unseres Vektorraums, wenn ihr Erzeugnis der ganze Vektorraum ist. Ein Vektorraum, der ein endliches Erzeugendensystem besitzt, heißt **endlich erzeugt**. Manche Autoren verwenden gleichbedeutend die vielleicht noch präzisere Terminologie **endlich erzeugbar**.

**Beispiel 3.1.5.11 (Erzeugnis in der schmutzigen Anschauung).** Ich erinnere an unsere Identifikation 3.1.5.6 des schmutzigen Vektorraums aller Parallelverschiebungen des Raums mit der Menge aller Punkte des Raums durch Auszeichnung eines festen Punktes als Ursprung. Dem Erzeugnis des Nullvektors entspricht unter dieser Identifikation die nur aus dem Ursprung bestehende Teilmenge; dem

Erzeugnis eines von Null verschiedenen Vektors entspricht die anschauliche Gerade durch den Ursprung und den Endpunkt des Pfeils, der vom Ursprung ausgehend unseren Vektor darstellt; und dem Erzeugnis zweier Vektoren, von denen keiner ein Vielfaches des anderen ist, entspricht die anschauliche Ebene, auf der unser fester Punkt und die Endpunkte der beiden Pfeile liegen, die vom Ursprung ausgehend unsere Vektoren darstellen.

**3.1.5.12 (Schnitt von Untervektorräumen).** Der Schnitt von zwei Untervektorräumen eines gegebenen Vektorraums ist offensichtlich wieder ein Untervektorraum.

**Definition 3.1.5.13.** Gegeben eine Menge  $X$  erinnere ich an die Menge aller Teilmengen  $\mathcal{P}(X) := \{U \mid U \subset X\}$  von  $X$ , die sogenannte **Potenzmenge von  $X$** . Da es mich verwirrt, über Mengen von Mengen zu reden, werde ich Teilmengen von  $\mathcal{P}(X)$  nach Möglichkeit als **Systeme von Teilmengen von  $X$**  ansprechen. Gegeben ein solches Mengensystem  $\mathcal{U} \subset \mathcal{P}(X)$  bildet man zwei neue Teilmengen von  $X$ , den **Schnitt** und die **Vereinigung** der Mengen aus unserem System  $\mathcal{U}$ , durch die Vorschriften

$$\begin{aligned}\bigcup_{U \in \mathcal{U}} U &:= \{x \in X \mid \text{Es gibt } U \in \mathcal{U} \text{ mit } x \in U\} \\ \bigcap_{U \in \mathcal{U}} U &:= \{x \in X \mid \text{Für alle } U \in \mathcal{U} \text{ gilt } x \in U\}\end{aligned}$$

Insbesondere ist der Schnitt über das leere System von Teilmengen von  $X$  ganz  $X$  und die Vereinigung über das leere System von Teilmengen von  $X$  die leere Menge. Um den Schnitt über ein leeres Mengensystem zu bilden, muß man also spezifizieren, das leere System von Teilmengen welcher Menge man nun betrachtet. Bei allen anderen Operationen kommt es dahingegen nicht darauf an.

**3.1.5.14 (Erzeugnis als Schnitt).** Jeder Schnitt von Untervektorräumen eines Vektorraums ist offensichtlich wieder ein Untervektorraum. Betrachten wir für eine Teilmenge  $T$  eines Vektorraums  $V$  über einem Körper  $K$  den Schnitt aller Untervektorräume von  $V$ , die  $T$  umfassen, so erhalten wir offensichtlich den kleinsten Untervektorraum von  $V$ , der  $T$  umfaßt. Wir erhalten so einen von 3.1.5.7 unabhängigen Beweis für die Existenz solch eines kleinsten Untervektorraums. Dieser Beweis hat den Vorteil, sich leichter auf andere Arten von Strukturen verallgemeinern zu lassen.

## Übungen

*Übung 3.1.5.15.* Sei  $K$  ein Körper. Man zeige, daß der  $K$ -Vektorraum  $K$  genau zwei Untervektorräume besitzt.

*Ergänzende Übung 3.1.5.16.* Eine Teilmenge eines Vektorraums heißt ganz allgemein eine **Hyperebene** oder präziser **lineare Hyperebene**, wenn unsere Teilmenge ein echter Untervektorraum ist, der zusammen mit einem einzigen weiteren Vektor unseren ursprünglichen Vektorraum erzeugt. Man zeige, daß eine Hyperebene sogar zusammen mit *jedem* Vektor außerhalb besagter Hyperebene unseren ursprünglichen Vektorraum erzeugt.

*Übung 3.1.5.17.* Gegeben ein Vektorraum über dem Körper mit zwei Elementen ist jede Untergruppe bereits ein Untervektorraum.

*Übung 3.1.5.18.* Sei  $V$  ein Vektorraum mit zwei Untervektorräumen  $U, W$ . Ist  $U \cup W$  ein Untervektorraum, so gilt  $U \subset W$  oder  $W \subset U$ .

### 3.1.6 Lineare Unabhängigkeit und Basen

**Definition 3.1.6.1.** Eine Teilmenge  $L$  eines Vektorraums heißt **linear unabhängig**, wenn für paarweise verschiedene Vektoren  $\vec{v}_1, \dots, \vec{v}_r \in L$  und beliebige Skalare  $\alpha_1, \dots, \alpha_r \in K$  aus  $\alpha_1\vec{v}_1 + \dots + \alpha_r\vec{v}_r = \vec{0}$  bereits folgt  $\alpha_1 = \dots = \alpha_r = 0$ .

3.1.6.2. Gleichbedeutend ist die Forderung, daß keiner der Vektoren unserer Teilmenge **redundant** ist in dem Sinne, daß er sich als eine Linearkombination der anderen schreiben läßt. Der Nullvektor ist dabei in jeder Teilmenge redundant: Selbst wenn er der einzige Vektor ist, läßt er sich noch als die leere Linearkombination schreiben.

**Definition 3.1.6.3.** Eine Teilmenge  $L$  eines Vektorraums heißt **linear abhängig**, wenn sie nicht linear unabhängig ist, wenn es also ausgeschrieben paarweise verschiedene Vektoren  $\vec{v}_1, \dots, \vec{v}_r \in L$  und Skalare  $\alpha_1, \dots, \alpha_r \in K$  gibt derart, daß nicht alle  $\alpha_i$  Null sind und dennoch gilt  $\alpha_1\vec{v}_1 + \dots + \alpha_r\vec{v}_r = \vec{0}$ .

*Beispiele 3.1.6.4.* Die leere Menge ist in jedem Vektorraum linear unabhängig. Eine einelementige Teilmenge ist linear unabhängig genau dann, wenn sie nicht aus dem Nullvektor besteht: Für das Produkt des Nullvektors mit dem Skalar 1 gilt nämlich  $1 \cdot \vec{0} = \vec{0}$ , und nach unseren Annahmen gilt in einem Körper stets  $1 \neq 0$ , also ist die aus dem Nullvektor bestehende Menge nicht linear unabhängig. Daß jede andere einelementige Teilmenge linear unabhängig ist, folgt andererseits aus unserer Erkenntnis 3.1.2.15, daß das Produkt von einem Vektor mit einem Skalar nur dann Null ist, wenn entweder der Vektor Null ist oder der Skalar.

*Beispiel 3.1.6.5.* Denken wir uns wie in 3.1.5.6 den schmutzigen Raum der Anschauung mit einem ausgezeichneten Ursprung als reellen Vektorraum, so sind drei Vektoren linear unabhängig genau dann, wenn sie nicht „zusammen mit unserem Ursprung in einer anschaulichen Ebene liegen“.

**Definition 3.1.6.6.** Eine **Basis eines Vektorraums** ist ein linear unabhängiges Erzeugendensystem.

*Beispiel 3.1.6.7.* Denken wir uns wie in 3.1.5.6 den schmutzigen Raum der Anschauung mit einem ausgezeichneten Ursprung als reellen Vektorraum, so ist jede Menge von drei Vektoren, die nicht zusammen mit unserem Ursprung in einer anschaulichen Ebene liegen, eine Basis. Die leere Menge ist eine Basis des Nullvektorraums.

3.1.6.8. Gegeben Mengen  $A$  und  $I$  bezeichnet man eine Abbildung  $I \rightarrow A$  ganz allgemein auch als eine **durch  $I$  indizierte Familie von Elementen von  $A$**  und benutzt die Notation

$$(a_i)_{i \in I}$$

Diese Sprechweise und Notation für Abbildungen verwendet man insbesondere dann, wenn man der Menge  $I$  eine untergeordnete Rolle zugeschrieben hat. Im Fall  $I = \emptyset$  spricht man von der **leeren Familie** von Elementen von  $A$ .

3.1.6.9 (**Linear unabhängige Familien**). Manchmal ist es praktisch und führt zu einer übersichtlicheren Darstellung, Varianten unserer Begriffe zu verwenden, die sich statt auf Teilmengen unseres Vektorraums auf Familien von Vektoren  $(\vec{v}_i)_{i \in I}$  beziehen. Eine derartige Familie heißt ein Erzeugendensystem, wenn die Menge  $\{\vec{v}_i \mid i \in I\}$  ein Erzeugendensystem ist. Sie heißt **linear unabhängig** oder ganz pedantisch **linear unabhängig als Familie**, wenn für beliebige paarweise verschiedene Indizes  $i(1), \dots, i(r) \in I$  und beliebige Skalare  $\alpha_1, \dots, \alpha_r \in K$  aus  $\alpha_1 \vec{v}_{i(1)} + \dots + \alpha_r \vec{v}_{i(r)} = \vec{0}$  bereits folgt  $\alpha_1 = \dots = \alpha_r = 0$ . Der wesentliche Unterschied zur Begrifflichkeit für Teilmengen liegt darin, daß bei einer Familie ja für verschiedene Indizes die zugehörigen Vektoren durchaus gleich sein könnten, was aber durch die Bedingung der linearen Unabhängigkeit dann doch wieder ausgeschlossen wird. Eine Familie von Vektoren, die nicht linear unabhängig ist, nennen wir eine **linear abhängige Familie**. Eine erzeugende und linear unabhängige Familie nennt man wieder eine **Basis** oder ausführlicher eine **durch  $i \in I$  indizierte Basis**.

3.1.6.10. Besonders oft werden wir später Basen betrachten, die durch eine Menge der Gestalt  $\{1, \dots, n\}$  mit  $n \in \mathbb{N}$  indiziert sind. Hier ist dann der wesentliche Unterschied zu einer Basis im Sinne von 3.1.6.6, daß wir zusätzlich festlegen, welcher Basisvektor der Erste, welcher der Zweite und so weiter sein soll. In der Terminologie aus 3.1.4 bedeutet das gerade, daß wir eine Anordnung auf unserer Basis festlegen. Wollen wir das besonders hervorheben, so sprechen wir von einer **angeordneten Basis**.

*Beispiel 3.1.6.11.* Seien  $K$  ein Körper und  $n \in \mathbb{N}$ . Wir betrachten in unserem Vektorraum  $K^n$  der  $n$ -Tupel die Vektoren

$$\vec{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$$

mit einer Eins an der  $i$ -ten Stelle und Nullen sonst. Dann bilden  $\vec{e}_1, \dots, \vec{e}_n$  eine angeordnete Basis von  $K^n$ , die sogenannte **Standardbasis** des  $K^n$ . Wir notieren diese Standardbasis  $\mathcal{S}(n)$ .

**Satz 3.1.6.12 (über Linearkombinationen von Basiselementen).** *Seien  $V$  ein Vektorraum über einem Körper  $K$  und  $\vec{v}_1, \dots, \vec{v}_r \in V$  Vektoren. Genau dann ist die Familie der  $\vec{v}_i$  eine Basis von  $V$ , wenn das Auswerten von Linearkombinationen eine Bijektion  $\Phi : K^r \xrightarrow{\sim} V$ ,  $(\alpha_1, \dots, \alpha_r) \mapsto \alpha_1 \vec{v}_1 + \dots + \alpha_r \vec{v}_r$  liefert.*

3.1.6.13. Bezeichnet  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_r)$  unsere angeordnete Familie, so notieren wir unsere Abbildung auch  $\Phi = \Phi_{\mathcal{A}} : K^r \rightarrow V$ .

*Beweis.* Ausführlicher gilt für unsere Abbildung  $\Phi$  sogar:

$$\begin{aligned} (\vec{v}_i)_{1 \leq i \leq r} \text{ ist Erzeugendensystem} &\Leftrightarrow \Phi \text{ ist eine Surjektion } K^r \twoheadrightarrow V \\ (\vec{v}_i)_{1 \leq i \leq r} \text{ ist linear unabhängig} &\Leftrightarrow \Phi \text{ ist eine Injektion } K^r \hookrightarrow V \\ (\vec{v}_i)_{1 \leq i \leq r} \text{ ist Basis} &\Leftrightarrow \Phi \text{ ist eine Bijektion } K^r \xrightarrow{\sim} V \end{aligned}$$

Hier folgt die erste Äquivalenz direkt aus den Definitionen. Um bei der zweiten Äquivalenz die Implikation  $\Leftarrow$  einzusehen, muß man nur bemerken, daß  $\Phi$  den Nullvektor auf Null wirft und folglich kein anderer Vektor aus  $K^r$  von  $\Phi$  auf Null geworfen werden kann. Um bei der zweiten Äquivalenz die Implikation  $\Rightarrow$  einzusehen, argumentieren wir durch Widerspruch: Wäre  $\Phi$  nicht injektiv, so gäbe es  $(\alpha_1, \dots, \alpha_r) \neq (\beta_1, \dots, \beta_r)$  mit demselben Bild  $\alpha_1 \vec{v}_1 + \dots + \alpha_r \vec{v}_r = \beta_1 \vec{v}_1 + \dots + \beta_r \vec{v}_r$ . Dann aber wäre

$$(\alpha_1 - \beta_1) \vec{v}_1 + \dots + (\alpha_r - \beta_r) \vec{v}_r = \vec{0}$$

eine nichttriviale Darstellung der Null als Linearkombination der  $\vec{v}_i$  und dann könnten unsere Vektoren nicht linear unabhängig gewesen sein. Die letzte Äquivalenz schließlich ist eine direkte Konsequenz der ersten beiden.  $\square$

**Satz 3.1.6.14 (Extremalcharakterisierungen von Basen).** *Für eine Teilmenge eines Vektorraums sind gleichbedeutend:*

1. *Unsere Teilmenge ist eine Basis alias ein linear unabhängiges Erzeugendensystem;*
2. *Unsere Teilmenge ist minimal unter allen Erzeugendensystemen;*
3. *Unsere Teilmenge ist maximal unter allen linear unabhängigen Teilmengen.*

3.1.6.15. Die Begriffe minimal und maximal sind hier zu verstehen im Sinne von 3.1.4.6 in Bezug auf Inklusionen zwischen Teilmengen, nicht etwa in Bezug auf

die Zahl der Elemente. Um das zu betonen, spricht man auch gerne von einem **verkürzbaren Erzeugendensystem**, wenn man eben daraus noch so einen Vektor weglassen kann, daß es ein Erzeugendensystem bleibt, und von einer **verlängerbaren linear unabhängigen Teilmenge**, wenn man so einen Vektor dazunehmen kann, daß sie linear unabhängig bleibt. Ein minimales Erzeugendensystem nennen wir folgerichtig auch ein **unverkürzbares Erzeugendensystem** und eine maximale linear unabhängige Teilmenge eine **unverlängerbare linear unabhängige Teilmenge**.

**3.1.6.16 (Existenz von Basen).** Unsere Minimalcharakterisierung 3.1.6.14 von Basen impliziert insbesondere, daß jeder endlich erzeugte Vektorraum eine endliche Basis besitzt: Wir lassen einfach aus einem endlichen Erzeugendensystem so lange Vektoren weg, bis wir bei einem unverkürzbaren Erzeugendensystem angekommen sind. Mit raffinierteren Methoden der Mengenlehre kann man stärker den **Basisexistenzsatz** zeigen, nach dem überhaupt jeder Vektorraum eine Basis besitzt. Wir diskutieren das in 3.1.9.20.

*Beweis.* (1 $\Leftrightarrow$ 2) Es gilt zu zeigen: Ein Erzeugendensystem ist linear unabhängig genau dann, wenn es unverkürzbar ist. Es ist gleichbedeutend zu zeigen: Ein Erzeugendensystem ist linear abhängig genau dann, wenn es verkürzbar ist. Ist  $E \subset V$  ein Erzeugendensystem und ist  $E$  linear abhängig, so gilt eine Relation  $\lambda_1 \vec{v}_1 + \dots + \lambda_r \vec{v}_r = \vec{0}$  mit  $r \geq 1$ , mit den  $\vec{v}_i \in E$  paarweise verschieden und mit allen  $\lambda_i \neq 0$ , aus der wir folgern

$$\vec{v}_1 = -\lambda_1^{-1} \lambda_2 \vec{v}_2 - \dots - \lambda_1^{-1} \lambda_r \vec{v}_r \in \langle E \setminus \vec{v}_1 \rangle$$

Damit ist auch  $E \setminus \vec{v}_1$  bereits ein Erzeugendensystem und  $E$  war verkürzbar. Ist umgekehrt  $E$  verkürzbar, so gibt es  $\vec{v} \in E$  derart, daß  $E \setminus \vec{v}$  immer noch ein Erzeugendensystem ist. Insbesondere existiert eine Darstellung

$$\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$$

mit  $n \geq 0$  und  $\vec{v}_i \in E \setminus \vec{v}$  paarweise verschieden. Daraus folgt  $\vec{v} - \lambda_1 \vec{v}_1 - \dots - \lambda_n \vec{v}_n = \vec{0}$  und  $E$  war linear abhängig.

(1 $\Leftrightarrow$ 3) Es gilt zu zeigen: Eine linear unabhängige Teilmenge ist ein Erzeugendensystem genau dann, wenn sie unverlängerbar ist. Wir argumentieren wieder durch Widerspruch. Ist  $L \subset V$  linear unabhängig und kein Erzeugendensystem, so ist für jedes  $\vec{v} \in V \setminus \langle L \rangle$  auch  $L \cup \{\vec{v}\}$  linear unabhängig und  $L$  war verlängerbar. Ist umgekehrt  $L$  verlängerbar, so gibt es einen Vektor  $\vec{v}$  derart, daß auch  $L \cup \{\vec{v}\}$  linear unabhängig ist, und dann kann  $L$  kein Erzeugendensystem gewesen sein, denn dieser Vektor  $\vec{v}$  kann nicht zu seinem Erzeugnis gehört haben.  $\square$

**Satz 3.1.6.17 (Extremalcharakterisierungen von Basen, Variante).** Sei  $V$  ein Vektorraum.

1. Ist  $L \subset V$  eine linear unabhängige Teilmenge und ist  $E$  minimal unter allen Erzeugendensystemen unseres Vektorraums mit  $E \supset L$ , so ist  $E$  eine Basis unseres Vektorraums  $V$ ;
2. Ist  $E \subset V$  ein Erzeugendensystem und ist  $L$  maximal unter allen linear unabhängigen Teilmengen unseres Vektorraums mit  $L \subset E$ , so ist  $L$  eine Basis unseres Vektorraums  $V$ .

3.1.6.18. Die Begriffe minimal und maximal sind hier genau wie in 3.1.6.14 zu verstehen im Sinne von 3.1.4.6 in Bezug auf Inklusionen zwischen Teilmengen, nicht etwa in Bezug auf die Zahl ihrer Elemente.

*Beweis.* (1) Wäre  $E$  keine Basis, so gäbe es zwischen seinen Vektoren eine nicht-triviale Relation  $\lambda_1 \vec{v}_1 + \dots + \lambda_r \vec{v}_r = \vec{0}$  mit  $r \geq 1$ , den  $\vec{v}_i \in E$  paarweise verschieden und allen  $\lambda_i \neq 0$ . Hier können nicht alle  $\vec{v}_i$  zu  $L$  gehören, da das ja linear unabhängig angenommen war. Ein  $\vec{v}_i$  gehört also zu  $E \setminus L$  und kann als Linearkombination der anderen Elemente von  $E$  geschrieben werden. Dann aber ist  $E \setminus \{\vec{v}_i\}$  auch schon ein Erzeugendensystem und  $E$  war nicht minimal.

(2) Wäre  $L$  keine Basis, so wäre  $L$  kein Erzeugendensystem und es gäbe notwendig auch einen Vektor  $\vec{v} \in E$ , der nicht im Erzeugnis von  $L$  läge. Nehmen wir ihn zu  $L$  hinzu, so erhalten wir eine echt größere linear unabhängige Teilmenge und  $L$  war nicht maximal.  $\square$

3.1.6.19 (**Lineare Unabhängigkeit und Erzeugen bei abelschen Gruppen**). In der Hoffnung, daß es zum Verständnis beiträgt, will ich kurz ausführen, inwiefern die Analoga der vorhergehenden Aussagen im Fall abelscher Gruppen im allgemeinen nicht mehr gelten. Eine Teilmenge  $L$  einer abelschen Gruppe  $M$  heißt **linear unabhängig**, wenn für beliebige paarweise verschiedene Elemente  $m_1, \dots, m_r \in L$  und beliebige ganze Zahlen  $\alpha_1, \dots, \alpha_r \in \mathbb{Z}$  aus  $\alpha_1 m_1 + \dots + \alpha_r m_r = 0$  bereits folgt  $\alpha_1 = \dots = \alpha_r = 0$ . Sie heißt ein **Erzeugendensystem**, wenn sich jedes Gruppenelement als endliche Linearkombination von Elementen von  $L$  mit ganzzahligen Koeffizienten schreiben lässt. Sie heißt eine **Basis**, wenn sie ein linear unabhängiges Erzeugendensystem ist. In der zweielementigen Gruppe ist dann die leere Menge die einzige linear unabhängige Teilmenge und das Komplement der Null das einzige minimale Erzeugendensystem und es gibt keine Basis. Weiter besitzt abelsche Gruppe  $\mathbb{Z}$  zwar eine Basis, etwa die Menge  $\{1\}$ , aber mit  $\{2, 3\}$  auch ein minimales Erzeugendensystem, das nicht linear unabhängig ist, und mit  $\{2\}$  eine maximale linear unabhängige Teilmenge, die kein Erzeugendensystem ist.

## Übungen

*Übung 3.1.6.20.* Eine zweielementige Teilmenge eines Vektorraums ist linear unabhängig genau dann, wenn keiner ihrer beiden Vektoren ein Vielfaches des anderen ist.

*Übung 3.1.6.21.* Eine Teilmenge eines Vektorraums ist linear abhängig genau dann, wenn sich mindestens einer ihrer Vektoren als eine Linearkombination der übrigen schreiben lässt.

*Übung 3.1.6.22.* Man zeige, daß im Vektorraum  $\text{Ens}(\mathbb{R}, \mathbb{R})$  das Erzeugnis der beiden Funktionen  $\sin, \cos$  aus allen Funktionen besteht, die sich in der Form  $x \mapsto A \sin(x + \varphi)$  schreiben lassen für  $A \geq 0$  und  $\varphi \in [0, 2\pi]$ . In diesem Zusammenhang ist  $A$  wohlbestimmt und heißt die **Amplitude**. Im Fall  $A \neq 0$  ist  $\varphi$  auch wohlbestimmt und heißt die **Phase**.

### 3.1.7 Dimension eines Vektorraums

**Satz 3.1.7.1 (Hauptabschätzung der linearen Algebra).** *In einem vorgegebenen Vektorraum  $V$  hat eine linear unabhängige Teilmenge nie mehr Elemente als ein Erzeugendensystem. Ist also in Formeln  $L \subset V$  eine linear unabhängige Teilmenge und  $E \subset V$  ein Erzeugendensystem, so gilt stets*

$$|L| \leq |E|$$

*Beweis.* Sei  $K$  unser Grundkörper. Seien  $E = \{\vec{w}_1, \dots, \vec{w}_m\}$  ein Erzeugendensystem und  $\vec{v}_1, \dots, \vec{v}_n$  Vektoren. Dann können wir die Vektoren  $\vec{v}_1, \dots, \vec{v}_n$  als Linearkombinationen der Vektoren unseres Erzeugendensystems schreiben. In Formeln ausgedrückt können wir also Skalare  $a_{ij} \in K$  finden mit

$$\begin{aligned} \vec{v}_1 &= a_{11}\vec{w}_1 + a_{21}\vec{w}_2 + \cdots + a_{m1}\vec{w}_m \\ &\vdots && \vdots && \vdots \\ \vec{v}_n &= a_{1n}\vec{w}_1 + a_{2n}\vec{w}_2 + \cdots + a_{mn}\vec{w}_m \end{aligned}$$

Für  $x_1, \dots, x_n \in k$  ist damit  $x_1\vec{v}_1 + \dots + x_n\vec{v}_n = \vec{0}$  gleichbedeutend zu

$$\left( \sum x_i a_{1i} \right) \vec{w}_1 + \dots + \left( \sum x_i a_{mi} \right) \vec{w}_m = \vec{0}$$

und gilt a fortiori, wenn die Koeffizienten aller  $\vec{w}_j$  verschwinden, also für jede Lösung des Gleichungssystems

$$\begin{aligned} x_1 a_{11} + x_2 a_{12} + \cdots + x_n a_{1n} &= 0 \\ &\vdots && \vdots && \vdots \\ x_1 a_{m1} + x_2 a_{12} + \cdots + x_n a_{mn} &= 0 \end{aligned}$$

Im Fall  $n > m$  hat dieses Gleichungssystem weniger Gleichungen als Unbekannte und der Gauß-Algorithmus 3.1.1.9 liefert dafür mindestens eine von Null verschiedene Lösung  $(x_1, \dots, x_n) \neq (0, \dots, 0)$ . Dann aber kann die Familie der Vektoren  $\vec{v}_1, \dots, \vec{v}_n$  nicht linear unabhängig sein.  $\square$

**3.1.7.2 (Diskussion alternativer Zugänge).** Die Terminologie „Hauptabschätzung der linearen Algebra“ für diese Aussage ist unüblich. Wir verwenden bei ihrer Formulierung unsere Konvention, nach der wir für alle unendlichen Mengen  $X$  schlicht  $|X| = \infty$  setzen. Damit macht der Satz also nur für endlich erzeugte Vektorräume überhaupt eine Aussage. Er gilt aber auch mit einer feineren Interpretation von  $|X|$  als „Kardinalität“. Genauer folgt aus dem „Zorn’schen Lemma“ die Existenz einer Injektion  $L \hookrightarrow E$ , wie in 3.1.8.3 in größerer Allgemeinheit diskutiert wird. Man benötigt dazu den „Austauschsatz von Steinitz“ 3.1.8.2, der auch einen oft gewählten alternativen Zugang zur Hauptabschätzung der linearen Algebra liefert. Der Kern des Arguments ist jedoch bei beiden Zugängen derselbe.

**Korollar 3.1.7.3 (Basisergänzungssatz).** *Ist  $M$  eine linear unabhängige Teilmenge in einem endlich erzeugten Vektorraum und  $E$  ein Erzeugendensystem, so läßt sich  $M$  durch Hinzunahme von Vektoren aus  $E$  zu einer Basis unseres Vektorraums ergänzen.*

**Vorschau 3.1.7.4.** Mit raffinierteren Methoden der Mengenlehre kann man diesen Satz sogar für jeden beliebigen, nicht notwendig endlich erzeugten Vektorraum zeigen. Wir diskutieren das in 3.1.9.20.

**Beweis.** Nach der Maximalcharakterisierung 3.1.6.17 von Basen ist jede linear unabhängige Teilmenge  $L$  unseres Vektorraums, die maximal ist unter allen linear unabhängigen Teilmengen  $L$  mit  $L \subset (M \cup E)$ , bereits eine Basis. Nach der Hauptabschätzung 3.1.7.1 kann man  $M$  auch tatsächlich zu einer maximalen linear unabhängigen Teilmenge von  $M \cup E$  vergrößern.  $\square$

**Korollar 3.1.7.5 (Kardinalitäten von Basen).** *Jeder endlich erzeugte Vektorraum besitzt eine endliche Basis, und je zwei seiner Basen haben gleich viele Elemente.*

**Vorschau 3.1.7.6.** In ?? wird mit raffinierteren Methoden der Mengenlehre gezeigt, daß es auch im Fall eines nicht notwendig endlich erzeugten Vektorraums für je zwei seiner Basen eine Bijektion zwischen der einen Basis und der anderen Basis gibt.

**Beweis.** Wie bereits in 3.1.6.16 erwähnt, erhalten wir eine endliche Basis, wenn wir ein beliebiges endliches Erzeugendensystem durch das Streichen von Vektoren zu einem unverkürzbaren Erzeugendensystem verkleinern. Gegeben zwei Basen  $B$  und  $B'$  eines Vektorraums haben wir nach der Hauptabschätzung 3.1.7.1 außerdem stets  $|B| \leq |B'| \leq |B|$ .  $\square$

**Definition 3.1.7.7.** Die Kardinalität einer und nach 3.1.7.5 jeder Basis eines endlich erzeugten Vektorraums  $V$  heißt die **Dimension** von  $V$  und wird  $\dim V$  notiert. Ist  $K$  ein Körper und wollen wir betonen, daß wir die Dimension als  $K$ -Vektorraum meinen, so schreiben wir

$$\dim V = \dim_K V$$

Ist der Vektorraum nicht endlich erzeugt, so schreiben wir  $\dim V = \infty$  und nennen  $V$  **unendlichdimensional** und ignorieren für gewöhnlich die durchaus möglichen feineren Unterscheidungen zwischen verschiedenen Unendlichkeiten. Derlei Feinheiten werden erst in ?? besprochen.

*Ergänzung 3.1.7.8 (Verschiedene Bedeutungen des Wortes „Dimension“).* In der Physik wird der Begriff der „Dimension“ leider auch noch in einer völlig anderen Bedeutung verwendet: Physikalische Dimensionen wären im physikalischen Sinne etwa die Länge, die Zeit, die Masse, die Frequenz und dergleichen mehr. In der hier entwickelten Sprache würde man so eine physikalische Dimension wohl am ehesten als einen „eindimensionalen reellen Vektorraum“ modellieren, vielleicht noch mit einer ausgezeichneten „Orientierung“. Ich kann nur hoffen, daß der Leser aus dem Kontext erschließen kann, welcher Dimensionsbegriff im Einzelfall jeweils gemeint ist.

3.1.7.9. Der Nullraum hat als Basis die leere Menge. Seine Dimension ist folglich Null. Allgemeiner hat für jeden Körper  $K$  die Standardbasis aus 3.1.6.11 des Vektorraums  $K^n$  genau  $n$  Elemente und das zeigt

$$\dim_K K^n = n$$

**Korollar 3.1.7.10 (Kardinalitätskriterien für Basen).** *Sei  $V$  ein endlich erzeugter Vektorraum.*

1. *Jede linear unabhängige Teilmenge  $L \subset V$  hat höchstens  $\dim V$  Elemente und im Fall  $|L| = \dim V$  ist  $L$  bereits eine Basis;*
2. *Jedes Erzeugendensystem  $E \subset V$  hat mindestens  $\dim V$  Elemente und im Fall  $|E| = \dim V$  ist  $E$  bereits eine Basis.*

*Beweis.* Nach der Hauptabschätzung 3.1.7.1 gilt für  $L$  eine linear unabhängige Teilmenge,  $B$  eine Basis und  $E$  ein Erzeugendensystem von  $V$  stets

$$|L| \leq |B| \leq |E|$$

Gibt es ein endliches Erzeugendensystem, so muß im Fall  $|L| = |B| = |E|$  mithin  $L$  eine unverlängerbare linear unabhängige Teilmenge und damit nach der Maximalcharakterisierung 3.1.6.14 eine Basis sein. Im Fall  $|B| = |E|$  muß  $E$  in derselben Weise ein unverkürzbares Erzeugendensystem und damit nach der Minimalcharakterisierung 3.1.6.14 eine Basis sein.  $\square$

**Korollar 3.1.7.11 (Dimensionsabschätzung für Untervektorräume).** Ein echter Untervektorraum eines endlichdimensionalen Vektorraums ist stets auch endlich erzeugt und hat darüber hinaus eine echt kleinere Dimension.

*Beweis.* Ist in Formeln  $U \subset V$  ein Untervektorraum eines endlichdimensionalen Vektorraums, so behaupten wir mithin  $\dim U \leq \dim V$  und behaupten zusätzlich, daß aus  $\dim U = \dim V < \infty$  folgt  $U = V$ . Nach der Hauptabschätzung 3.1.7.1 gibt es in  $U$  eine unverlängerbare linear unabhängige Teilmenge und jede derartige Teilmenge hat höchstens  $\dim V$  Elemente. Jede derartige Teilmenge ist aber nach der Maximalcharakterisierung 3.1.6.14 notwendig eine Basis von  $U$  und das zeigt  $\dim U \leq \dim V$ . Gilt hier Gleichheit, so ist wieder nach der Hauptabschätzung 3.1.7.1 jede Basis von  $U$  auch eine Basis von  $V$  und das zeigt  $U = V$ .  $\square$

**Satz 3.1.7.12 (Dimensionssatz).** Gegeben ein Vektorraum  $V$  und darin Teilräume  $U, W \subset V$  gilt

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$$

3.1.7.13. Wir verwenden hier die bereits in 2.2.1.3 eingeführte Notation  $U + W$  für den Teilraum  $U + W := \{\vec{u} + \vec{w} \mid \vec{u} \in U, \vec{w} \in W\}$  von  $V$ . Wir beweisen diesen Satz in 3.2.2.9 noch ein zweites Mal als Korollar der Dimensionsformel für lineare Abbildungen.

*Beispiel 3.1.7.14.* Denken wir uns wie in 3.1.5.6 den Raum der schmutzigen Anschauung mit einem ausgezeichneten festen Punkt als Vektorraum, so entsprechen die zweidimensionalen Untervektorräume den anschaulichen Ebenen durch unseren festen Punkt und je zwei verschiedene zweidimensionale Untervektorräume  $U, W$  spannen den ganzen Raum auf,  $\dim(U + W) = 3$ . Zwei verschiedene Ebenen durch unseren festen Punkt schneiden sich nun offensichtlich in einer anschaulichen Geraden, und das entspricht genau der Aussage unseres Satzes, die in diesem Fall zur Identität  $3 + 1 = 2 + 2$  spezialisiert.

*Beweis.* Sind  $U$  oder  $W$  unendlichdimensional, so ist das eh klar. Sonst wählen wir eine Basis  $s_1, \dots, s_d$  von  $U \cap W$  und ergänzen sie erst durch  $u_1, \dots, u_r \in U$  zu einer Basis von  $U$  und dann weiter durch  $w_1, \dots, w_t \in W$  zu einer Basis von  $U + W$ . Wir haben gewonnen, wenn wir zeigen können, daß bei derartigen Wahlen bereits  $s_1, \dots, s_d, w_1, \dots, w_t$  eine Basis von  $W$  ist. Dazu reicht es zu zeigen, daß diese Menge  $W$  erzeugt. Sicher können wir jedes  $w \in W$  schreiben als Linear-kombination

$$\begin{aligned} w = & \lambda_1 u_1 + \dots + \lambda_r u_r \\ & + \mu_1 s_1 + \dots + \mu_d s_d \\ & + \nu_1 w_1 + \dots + \nu_t w_t \end{aligned}$$

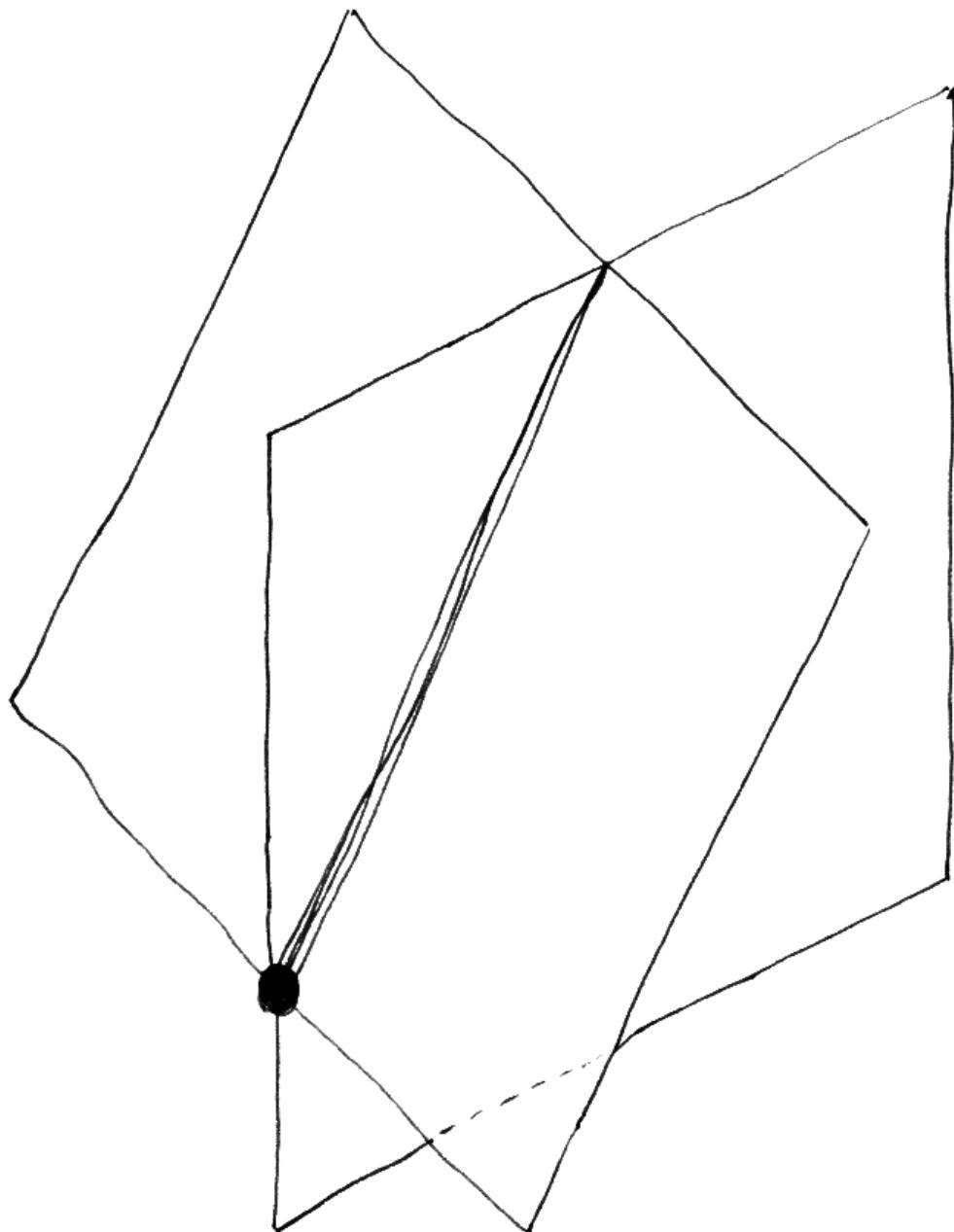


Illustration zum Dimensionssatz nach 3.1.7.14: Zwei verschiedene Ebenen im Raum, die beide einen ausgezeichneten festen Punkt enthalten, schneiden sich in einer Geraden.

Dabei gilt jedoch offensichtlich  $\lambda_1 u_1 + \dots + \lambda_r u_r \in W \cap U$ . Dieser Ausdruck läßt sich damit auch als Linearkombination der  $s_i$  schreiben, so daß  $w$  selbst auch als Linearkombination der  $s_i$  und  $w_j$  geschrieben werden kann, was zu zeigen war. Im übrigen muß dann auch bei der obigen Darstellung bereits gelten  $\lambda_1 = \dots = \lambda_r = 0$ , aber das ist für unseren Beweis schon gar nicht mehr von Belang.  $\square$

## Übungen

*Übung 3.1.7.15.* Man zeige, daß jeder eindimensionale Vektorraum genau zwei Untervektorräume besitzt.

*Übung 3.1.7.16.* Gegeben  $K$ -Vektorräume  $V$  und  $W$  mit Basen  $v_1, \dots, v_n$  und  $w_1, \dots, w_m$  zeige man, daß die Paare  $(v_i, 0)$  zusammen mit den Paaren  $(0, w_j)$  eine Basis von  $V \oplus W$  bilden. Insbesondere gilt für die Dimension des kartesischen Produkts die Formel

$$\dim(V \oplus W) = \dim(V) + \dim(W)$$

Gegeben  $K$ -Vektorräume  $V_1, \dots, V_n$  gilt allgemeiner für die Dimension ihres kartesischen Produkts die Formel

$$\dim(V_1 \oplus \dots \oplus V_n) = \dim(V_1) + \dots + \dim(V_n)$$

*Ergänzende Übung 3.1.7.17.* Wir erinnern die Körper  $\mathbb{R} \subset \mathbb{C}$  aus 2.2.4.15. Natürlich kann jeder  $\mathbb{C}$ -Vektorraum  $V$  auch als  $\mathbb{R}$ -Vektorraum aufgefaßt werden. Wir notieren diesen  $\mathbb{R}$ -Vektorraum  $V^{\mathbb{R}}$  und nennen ihn die **Reellifizierung** von  $V$ . Man zeige  $\dim_{\mathbb{R}} V^{\mathbb{R}} = 2 \dim_{\mathbb{C}} V$ .

## 3.1.8 Austauschsatz von Steinitz\*

3.1.8.1. Einen anderen Zugang zur Hauptabschätzung der linearen Algebra 3.1.7.1 liefert der folgende Austauschsatz von Steinitz, der sogar eine etwas feinere Aussage liefert. Im hier verfolgten Zugang zur linearen Algebra ist er entbehrlich. Mir scheint insbesondere seine Variante ?? relevant, da es mit ihr gelingt, auch im Fall eines nicht endlich erzeugten Vektorraums die Existenz einer Bijektion zwischen je zweien seiner Basen zu zeigen. Derlei Feinheiten gehören jedoch eher nicht in eine Grundvorlesung. Ich habe den Austauschsatz hier dennoch besprochen, da er beim üblichen Aufbau der Theorie eine wichtige Rolle spielt und deshalb auch in Prüfungen oft danach gefragt wird.

**Satz 3.1.8.2 (Austauschsatz von Steinitz).** Ist  $V$  ein Vektorraum,  $L \subset V$  eine endliche linear unabhängige Teilmenge und  $E \subset V$  ein Erzeugendensystem, so gibt es eine Injektion  $\varphi : L \hookrightarrow E$  derart, daß auch  $(E \setminus \varphi(L)) \cup L$  ein Erzeugendensystem von  $V$  ist.

3.1.8.3. Wir können also in anderen Worten die Vektoren unserer linear unabhängigen Teilmenge so in unser Erzeugendensystem hineintauschen, daß es ein Erzeugendensystem bleibt. Mit raffinierteren Methoden der Mengenlehre kann obiger Austauschsatz auch ohne die Voraussetzung  $L$  endlich gezeigt werden. Der Beweis in dieser Allgemeinheit wird in ?? skizziert.

*Beweis.* Der Austauschsatz folgt leicht induktiv aus dem Austauschlemma 3.1.8.4, das wir im Anschluß beweisen: Dies Lemma erlaubt uns nämlich, die Elemente von  $L$  der Reihe nach in  $E$  hineinzutauschen.  $\square$

**Lemma 3.1.8.4 (Austauschlemma von Steinitz).** *Seien  $V$  ein Vektorraum und darin  $E \supset M$  ein Erzeugendensystem mit einer linear unabhängigen Teilmenge. Ist  $\vec{w} \in V \setminus M$  ein Vektor außerhalb von  $M$  derart, daß auch  $M \cup \{\vec{w}\}$  linear unabhängig ist, so gibt es  $\vec{e} \in E \setminus M$  derart, daß auch  $(E \setminus \vec{e}) \cup \{\vec{w}\}$  ein Erzeugendensystem von  $V$  ist.*

*Beweis.* Da  $E$  ein Erzeugendensystem von  $V$  ist, können wir  $\vec{w}$  als Linearkombination von Vektoren aus  $E$  schreiben, sagen wir

$$\vec{w} = \lambda_1 \vec{e}_1 + \dots + \lambda_r \vec{e}_r$$

mit paarweise verschiedenen  $\vec{e}_i \in E$  und allen Koeffizienten verschieden von Null. Da  $M \cup \{\vec{w}\}$  linear unabhängig ist, können hier nicht alle  $\vec{e}_i$  bereits zu  $M$  gehören. Ohne Beschränkung der Allgemeinheit dürfen wir also  $\vec{e}_1 \notin M$  annehmen. Nun schreiben wir unsere Identität um zu

$$\vec{e}_1 = \lambda_1^{-1}(\vec{w} - \lambda_2 \vec{e}_2 - \dots - \lambda_r \vec{e}_r)$$

und sehen so, daß auch  $(E \setminus \vec{e}_1) \cup \{\vec{w}\}$  ein Erzeugendensystem ist.  $\square$

### 3.1.9 Auswahlaxiom und Zorn'sches Lemma\*

3.1.9.1. Wir erinnern an einige Begriffe im Zusammenhang mit teilgeordneten Mengen aus 3.1.4, deren genaue Bedeutung im folgenden wesentlich ist. Ein Element einer teilgeordneten Menge  $x \in X$  heißt **maximal**, wenn es keine Elemente oberhalb von  $x$  gibt. Ein Element einer teilgeordneten Menge  $x \in X$  heißt das **größte Element von  $X$** , wenn alle anderen Elemente unterhalb von  $x$  liegen.

3.1.9.2. Es kann also in einer teilgeordneten Menge viele maximale Elemente geben, aber nicht mehr als ein größtes Element. Falls es ein größtes Element gibt, so ist dies auch das einzige maximale Element. Gibt es andererseits genau ein maximales Element und ist  $X$  endlich, so ist dies maximale Element notwendig das größte Element.

3.1.9.3. Seien  $X \supset Y$  eine teilgeordnete Menge mit einer Teilmenge. Ein Element  $o \in X$  heißt eine **obere Schranke von**  $Y$ , wenn gilt  $o \geq y \forall y \in Y$ . Gibt es eine kleinste derartige obere Schranke, so heißt sie das **Supremum von**  $Y$  **in**  $X$  und wird  $\sup Y = \sup_X Y$  notiert.

3.1.9.4. Eine Teilmenge einer teilgeordneten Menge heißt eine **Kette**, wenn sie total geordnet ist, wenn also darin je zwei Elemente vergleichbar sind. Eine teilgeordnete Menge heißt **induktiv teilgeordnet**, wenn darin jede Kette eine obere Schranke besitzt, und **streu induktiv teilgeordnet**, wenn darin jede Kette eine kleinste obere Schranke besitzt.

3.1.9.5. Eine induktiv teilgeordnete Menge ist nie leer, denn die leere Menge ist stets eine Kette und besitzt folglich eine obere Schranke. In der Literatur sagt man meist einfacher „induktiv geordnet“ und „streu induktiv geordnet“.

**Satz 3.1.9.6 (Fixpunktsatz von Bourbaki).** *Gegeben eine streu induktiv teilgeordnete Menge  $(S, \leq)$  besitzt jede Abbildung  $f : S \rightarrow S$  mit der Eigenschaft  $f(s) \geq s \forall s \in S$  mindestens einen Fixpunkt.*

*Beweis.* Sicher besitzt  $S$  ein kleinstes Element  $k \in S$ , nämlich das Supremum der leeren Menge, die ja stets eine Kette ist. Eine Teilmenge  $T \subset S$  heiße ein  **$f$ -Turm** oder kurz **Turm**, wenn gilt

1. Ist  $K \subset T$  eine Kette, so gehört auch  $\sup_S K$  zu  $T$ ;
2. Aus  $t \in T$  folgt  $f(t) \in T$ , als da heißt,  $T$  ist stabil unter  $f$ .

Insbesondere gehört also das Supremum der leeren Menge alias das kleinste Element von  $S$  zu jedem Turm. Der Schnitt über alle Türme in  $S$  ist sicher der bezüglich Inklusion **kleinste Turm**  $R \subset S$ . Gegeben ein Turm  $T \subset S$  heiße weiter ein Element  $e \in T$  eine **Engstelle von**  $T$ , wenn für alle  $a \in T$  gilt  $(a < e) \Rightarrow (f(a) \leq e)$ . Ist  $e \in T$  eine Engstelle eines Turms, so ist auch

$$T_e := \{a \in T \mid a \leq e \text{ oder } f(e) \leq a\}$$

ein Turm. Hier folgt  $f(T_e) \subset T_e$  aus der Definition einer Engstelle und die Supremumseigenschaft ist auch offensichtlich erfüllt. Per definitionem gilt  $T_e \subset T$ . Für jede Engstelle  $e \in R$  des kleinsten Turms  $R$  gilt insbesondere

$$R_e = R$$

Eine Engstelle von  $R$  ist also mit jedem Element von  $R$  vergleichbar. Wir zeigen nun, daß unser kleinster Turm  $R$  überhaupt nur aus Engstellen besteht. Dazu reicht es zu zeigen, daß die Menge seiner Engstellen  $E \subset R$  auch ihrerseits wieder ein Turm ist. Prüfen wir also unsere beiden Eigenschaften. Die kleinste obere

Schranke einer Kette von Engstellen eines Turms ist offensichtlich auch selbst wieder eine Engstelle unseres Turms. Bleibt nur noch  $f(E) \subset E$  zu prüfen. Für jede Engstelle  $e \in E$  unseres kleinsten Turms  $R$  gilt jedoch wie bereits erwähnt  $R_e = R$ . Damit ist auch  $f(e)$  eine Engstelle von  $R$ , denn für  $a \in R = R_e$  folgt aus  $a < f(e)$  offensichtlich  $f(e) \not\leq a$  und so  $a \leq e$ , also entweder  $a < e$  oder  $a = e$ . Im ersten Fall  $a < e$  folgt weiter  $f(a) \leq e$ , weil  $e$  bereits als Engstelle von  $R$  angenommen war, wohingegen im zweiten Fall  $a = e$  eh klar ist, daß gilt  $f(a) \leq f(e)$ , ja sogar  $f(a) = f(e)$ . Damit gilt also  $e \in E \Rightarrow f(e) \in E$  alias  $f(E) \subset E$  und  $E$  ist in der Tat wieder ein Turm. Da  $R$  der kleinste Turm war, folgern wir

$$E = R$$

Für alle  $e \in R$  gilt folglich  $R_e = R$  und für jedes  $a \in R$  gilt damit  $a \leq e$  oder  $e \leq a$ , ja sogar  $f(e) \leq a$ . Mithin ist unser kleinerster Turm  $R$  eine Kette und deren kleinste obere Schranke ist dann notwendig das größte Element von  $R$  und ein Fixpunkt von  $f$ .  $\square$

*Ergänzung 3.1.9.7.* Anschaulich mag man sich unsere teilgeordnete Menge  $S$  mit der Abbildung  $f$  vorstellen als eine mathematische Beschreibung für mehr oder weniger geordnetes Schlangestehen, etwa um in ein Flugzeug zu gelangen. In dieser Interpretation wäre  $S$  eine Menge möglicher Standplätze und die Abbildung  $f$  wäre eine Vorschrift, die unsere Flugreisenden in jedem Zeitschritt von einem Standplatz zu einem besseren Standplatz vorrücken oder aber stehenbleiben lässt. Eine Engstelle einer beliebigen unter  $f$  stabilen Teilmenge  $R \subset S$  wäre etwa ein Standplatz direkt vor einem Drehkreuz, an dem die Bordkarten eingesammelt werden und an dem alle Reisenden, die auf Standplätzen aus  $R$  stehen, einzeln vorbeigehen müssen, wenn sie denn überhaupt ins Flugzeug kommen wollen.

*Ergänzung 3.1.9.8.* Dieser Unterabschnitt ist nur motivierendes Geschwätz und muß bei einem streng logischen Aufbau übersprungen werden. Aber sei's drum! In unserem kleinsten Turm liegen natürlich das kleinste Element  $k$  und dann auch  $f(k), f^2(k), f^3(k) \dots$  Wird diese Folge stationär, etwa bei  $f^n(k) = f^{n+1}(k)$ , so ist diese endliche Menge der kleinste Turm. Wird sie nicht stationär, so gehört ihr Supremum  $s = \sup\{f^n(k)\}$  nicht zu den Folgengliedern, gehört aber auch zu unserem kleinsten Turm, ebenso wie auch  $f(s), f^2(s), f^3(s) \dots$  Wird diese Folge stationär, etwa bei  $f^n(s) = f^{n+1}(s)$ , so ist die Vereinigung der Glieder unserer beiden Folgen der kleinste Turm. Sonst gehört das Supremum  $s_1 = \sup\{f^n(s)\}$  unserer zweiten Folge wieder nicht zu den Folgengliedern, gehört aber auch zu unserem kleinsten Turm, ebenso wie auch  $f(s_1), f^2(s_1), f^3(s_1) \dots$  Terminiert „dieser Prozess“, so liefert er den kleinsten Turm als Vereinigung endlich vieler Folgen, der letzten davon endlich. Sonst bilden wir die Folge  $s = s_0, s_1, \dots$  und auch deren Supremum  $t = \sup\{s_n\}$  gehört zu unserem kleinsten Turm, ebenso

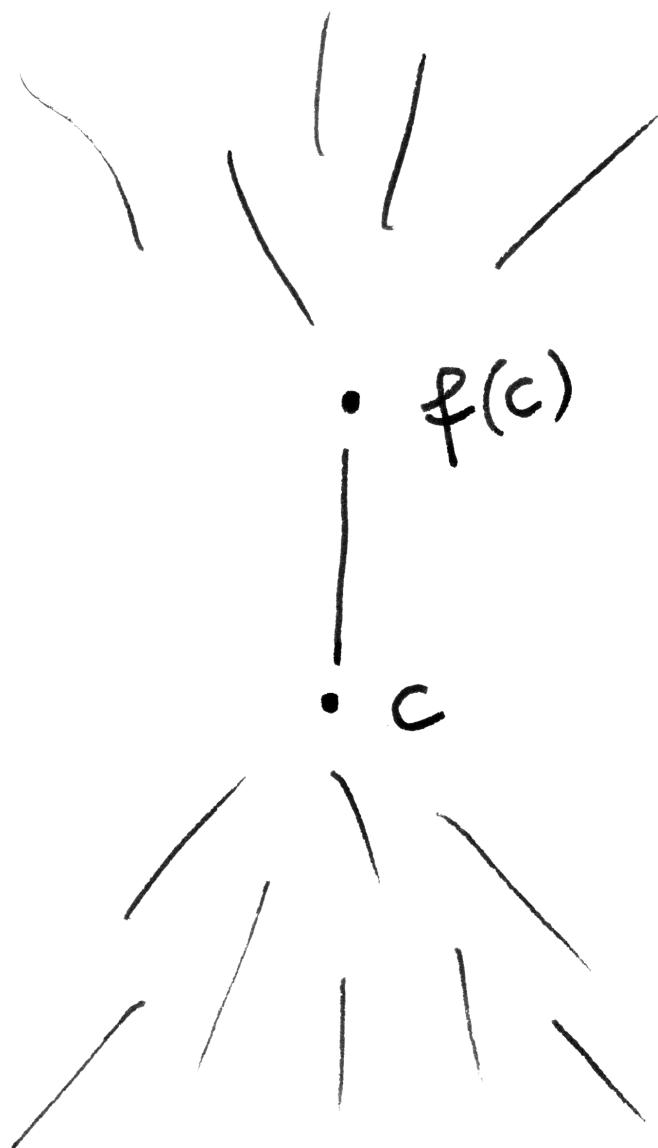


Illustration im Fall, daß unsere Engstelle des kleinsten Turms  $c \in R$  kein Fixpunkt von  $f$  ist. Die Teilordnung wird hier vage durch Striche angedeutet, die von kleineren zu größeren Elementen aufsteigen.

wie  $f(t), f^2(t), f^3(t) \dots$  Na ja, und dann geht es irgendwie immer so weiter und wird recht unübersichtlich, weshalb diese Überlegungen beim Nachweis, daß der kleinste Turm eine Kette sein muß, auch nicht direkt zum Ziel führen und wir den obigen etwas komplizierterem Weg gegangen sind.

**Lemma 3.1.9.9 (Auswahlaxiom).** *Für jede surjektive Abbildung  $f : X \rightarrow Y$  von Mengen existiert eine Abbildung  $g : Y \rightarrow X$  mit  $f \circ g = \text{id}_Y$ .*

3.1.9.10. So eine Abbildung  $g$  heißt ein **Rechtsinverses** oder auch ein **Schnitt**. Vom Standpunkt der naiven Mengenlehre aus, den wir bisher stets eingenommen haben und den wir auch weiterhin einnehmen werden, kann man dieses Lemma mühelos beweisen: Man wählt halt zu jedem Element  $y \in Y$  ein Element  $x \in X$  aus mit  $f(x) = y$  und nennt dies Element  $g(y)$ . Wenn man jedoch die Mengenlehre wie bei Zermelo und Fraenkel in einer Formelsprache formalisiert, so läßt sich die Aussage dieses Lemmas nicht formal aus den nach Zermelo und Fraenkel üblicherweise zugrundegelegten anderen Axiomen herleiten, die wir zwar ihrerseits auch nie formalisiert haben, die wir aber ständig in intuitiver Weise benutzen. Daher röhrt die Bezeichnung unseres Lemmas als „Axiom“. Wir werden das Auswahlaxiom hier für die Herleitung des „Zorn’schen Lemmas“ 3.1.9.15 benötigen, von dem man sogar zeigen kann, daß es zum Auswahlaxiom äquivalent ist.

**Lemma 3.1.9.11 (Auswahlaxiom, Variante).** *Gegeben eine Menge  $X$  gibt es stets eine Abbildung  $a : \mathcal{P}(X) \setminus \emptyset \rightarrow X$  mit  $a(T) \in T \forall T \in \mathcal{P}(X)$ .*

3.1.9.12. In Worten wählt die Abbildung  $a$  also in jeder nichtleeren Teilmenge  $T \subset X, T \neq \emptyset$  von  $X$  ein Element aus. Man nennt solch eine Abbildung deshalb auch eine **Auswahlfunktion**.

3.1.9.13. Vom Standpunkt der naiven Mengenlehre aus, den wir bisher stets eingenommen haben und den wir auch weiterhin einnehmen werden, kann man diese Variante genauso mühelos beweisen: Man wählt halt in jeder nichtleeren Teilmenge  $T \subset X$  ein Element aus und nennt es  $a(T)$ . Die etwas schwächere Forderung, daß es für jede Folge  $X_0, X_1, \dots$  nichtleerer Teilmengen einer Menge  $X$  eine Folge von Elementen  $x_0, x_1, \dots$  gibt mit  $x_i \in X_i \forall i$ , mag man das „Folgenauswahlaxiom“ nennen. Es wird häufig bereits zu Beginn der ersten Grundvorlesung der Analysis verwendet, zum Beispiel beim Nachweis, daß jede folgenstetige Funktion das  $\varepsilon$ - $\delta$ -Kriterium erfüllt.

3.1.9.14. Man sieht leicht, daß die beiden hier vorgestellten Varianten des Auswahlaxioms äquivalent sind. Um die Erste aus der Zweiten herzuleiten, betrachtet man schlicht die Familie der Fasern von  $f$ . Um die Zweite aus der Ersten herzuleiten, betrachtet man für eine beliebige Menge  $X$  im Produkt  $X \times \mathcal{P}(X)$  die Teilmenge  $Y = \{(x, T) \mid x \in T\}$  und die durch die Projektion auf die zweite Koordinate  $(x, T) \mapsto T$  gegebene Abbildung  $Y \rightarrow \mathcal{P}(X)$ . Sie induziert eine

Surjektion  $Y \rightarrow \mathcal{P}(X) \setminus \emptyset$ , und verknüpfen wir einen Schnitt dieser Surjektion mit der Projektion auf die erste Koordinate  $(x, T) \mapsto x$ , so erhalten wir eine Auswahlfunktion  $\mathcal{P}(X) \setminus \emptyset \rightarrow X$ .

**Lemma 3.1.9.15 (Zorn'sches Lemma).** *Sei  $(X, \leq)$  eine teilgeordnete Menge. Besitzt jede total geordnete Teilmenge  $Y \subset X$  eine obere Schranke in  $X$ , so gibt es in unserer teilgeordneten Menge  $X$  mindestens ein maximales Element.*

*Ergänzung 3.1.9.16.* Es reicht nicht aus, im Zorn'schen Lemma nur die Existenz einer oberen Schranke für jede monoton wachsende Folge zu fordern, vergleiche 3.1.9.19.

*Beweis.* Das Zorn'sche Lemma besagt in unserer Terminologie, daß jede induktiv teilgeordnete Menge ein maximales Element besitzt. Wir zeigen das zunächst nur für eine streng induktiv teilgeordnete Menge  $(S, \leq)$ . In der Tat finden wir mit dem Auswahlaxiom 3.1.9.11 eine Abbildung  $f : S \rightarrow S$  mit  $f(s) \geq s \forall s \in S$  und  $f(s) = s$  nur für  $s$  maximal. Diese Abbildung muß nach dem Fixpunktsatz von Bourbaki 3.1.9.6 einen Fixpunkt haben und dieser Fixpunkt ist notwendig ein maximales Element von  $S$ . Ist  $(X, \leq)$  eine beliebige induktiv teilgeordnete Menge, so betrachten wir die bezüglich Inklusion teilgeordnete Menge  $\mathcal{S} \subset \mathcal{P}(X)$  der Ketten von  $X$ . Diese Menge  $\mathcal{S}$  ist dann sogar streng induktiv teilgeordnet, das Supremum über ein total geordnetes System  $\mathcal{K} \subset \mathcal{S}$  alias eine Kette von Ketten ist einfach ihre Vereinigung  $\sup \mathcal{K} = \bigcup_{C \in \mathcal{K}} C$ . Nach der bereits bewiesenen Aussage gibt es also ein maximales Element von  $\mathcal{S}$  alias eine maximale Kette  $C_{\max}$  in  $X$ . Eine obere Schranke einer solchen maximalen Kette  $C_{\max}$  alias ihr größtes Element ist dann notwendig ein maximales Element von  $X$ .  $\square$

3.1.9.17. Gegeben eine Menge  $X$  bezeichne wie üblich  $\mathcal{P}(X)$  ihre Potenzmenge, als da heißt die Menge aller Teilmengen von  $X$ . Teilmengen von  $\mathcal{P}(X)$  werde ich oft als **Systeme von Teilmengen von  $X$**  ansprechen. Besonders häufig benutzt man das Zorn'sche Lemma in der folgenden Gestalt:

**Korollar 3.1.9.18.** *Ist  $M$  eine Menge und  $\mathcal{X} \subset \mathcal{P}(M)$  ein System von Teilmengen von  $M$ , das mit jedem bezüglich Inklusion total geordneten Teilsystem auch die Vereinigungsmenge des besagten Teilsystems enthält, so besitzt  $\mathcal{X}$  ein bezüglich Inklusion maximales Element.*

3.1.9.19. Hier verwenden wir die Konvention 3.1.5.13, nach der die Vereinigung über überhaupt keine Teilmenge einer Menge die leere Menge ist. Insbesondere folgt aus unseren Annahmen, daß die leere Menge zu  $\mathcal{X}$  gehört. Es reicht hier nicht, nur die Stabilität unter Vereinigungen von aufsteigenden Folgen in unserem Mengensystem zu fordern: So bilden etwa alle abzählbaren Teilmengen einer

überabzählbaren Menge ein Mengensystem, das zwar stabil ist unter Vereinigungen von aufsteigenden Folgen, das aber keine maximalen Elemente besitzt. Wir nennen ein System  $\mathcal{M} \subset \mathcal{P}(X)$  von Teilmengen einer gegebenen Menge  $X$  **stabil unter aufsteigenden Vereinigungen**, wenn es mit jedem total geordneten Teilsystem auch die Vereinigungsmenge des besagten Teilsystems enthält. In dieser Terminologie kann unser Korollar dann dahingehend formuliert werden, daß jedes System von Teilmengen einer gegebenen Menge, das stabil ist unter aufsteigenden Vereinigungen, mindestens ein maximales Element besitzt.

*Beweis.* Wir können das Zorn'sche Lemma auf die teilgeordnete Menge  $\mathcal{X}$  anwenden, denn für jede Kette in  $\mathcal{X}$  gehört nach Annahme die Vereinigung ihrer Mitglieder auch zu  $\mathcal{X}$ , und diese Vereinigung ist offensichtlich eine obere Schranke unserer Kette. Sie ist sogar eine kleinste obere Schranke, so daß wir nur die erste Hälfte von unserem Beweis des Zorn'schen Lemmas wirklich brauchen.  $\square$

**Satz 3.1.9.20 (Basisexistenzsatz und Basisergänzungssatz).** *Jeder Vektorraum besitzt eine Basis. Ist allgemeiner  $M \subset E$  eine linear unabhängige Teilmenge in einem Erzeugendensystem eines Vektorraums, so gibt es stets eine Basis  $B$  unseres Vektorraums mit  $M \subset B \subset E$ .*

3.1.9.21. Bereits der Basisexistenzsatz ist hochgradig nichtkonstruktiv. Ich bin etwa außerstande, Ihnen für irgendeinen Körper  $K$ , und sei es der Körper  $K = \mathbb{F}_2$  mit zwei Elementen, eine Basis des  $K$ -Vektorraums  $\text{Ens}(\mathbb{N}, K)$  hinzuschreiben. Geeignet verstanden ist das sogar prinzipiell unmöglich. Mehr dazu mögen Sie in der Logik lernen.

*Beweis.* Sei  $V$  unser Vektorraum und  $\mathcal{X} \subset \mathcal{P}(V)$  das System aller linear unabhängigen Teilmengen  $A$  mit  $M \subset A \subset E$ , teilgeordnet durch Inklusion. Wir zeigen zunächst, daß  $\mathcal{X}$  stabil ist unter aufsteigenden Vereinigungen. Ist in der Tat  $\mathcal{Y}$  ein total geordnetes System von linear unabhängigen Teilmengen von  $V$ , so ist auch  $\bigcup_{A \in \mathcal{Y}} A$  linear unabhängig, denn sind  $v_1, \dots, v_r \in \bigcup_{A \in \mathcal{Y}} A$  paarweise verschieden, so gibt es ein  $A \in \mathcal{Y}$  mit  $v_1, \dots, v_r \in A$  und folglich verschwindet keine nichttriviale Linearkombination der  $v_i$ . Also ist  $\mathcal{X}$  stabil unter aufsteigenden Vereinigungen und nach dem vorhergehenden Korollar 3.1.9.18 gibt es damit ein maximales Element von  $\mathcal{X}$  alias eine linear unabhängige Teilmenge  $A_{\max} \subset V$ , die  $M$  umfaßt und maximal ist unter allen linear unabhängigen Teilmengen  $A$  mit  $A \subset E$ . Diese Teilmenge muß dann aber nach der Maximalcharakterisierung 3.1.6.17 eine Basis von  $V$  sein.  $\square$

## Übungen

*Übung 3.1.9.22.* Gegeben eine teilgeordnete Menge besitzt jede nichtleere Teilmenge ein maximales Element genau dann, wenn jede monoton wachsende Folge

stagniert.

*Übung 3.1.9.23.* Man zeige, daß es auf jeder Menge eine Anordnung gibt.

## 3.2 Lineare Abbildungen

### 3.2.1 Homomorphismen und Isomorphismen

**Definition 3.2.1.1.** Seien  $V, W$  Vektorräume über einem Körper  $K$ . Eine Abbildung  $f : V \rightarrow W$  heißt **linear** und genauer  **$K$ -linear**, wenn für alle  $\vec{v}, \vec{w} \in V$  und  $\lambda \in K$  gilt

$$\begin{aligned} f(\vec{v} + \vec{w}) &= f(\vec{v}) + f(\vec{w}) \\ f(\lambda \vec{v}) &= \lambda f(\vec{v}) \end{aligned}$$

Lineare Abbildungen heißen auch **Homomorphismen von  $K$ -Vektorräumen**.

**Definition 3.2.1.2.** Eine lineare Abbildung  $\phi$  heißt ein **Isomorphismus von Vektorräumen**, wenn es eine lineare Abbildung  $\psi$  in die Gegenrichtung gibt derart, daß beide Kompositionen  $\psi \circ \phi$  und  $\phi \circ \psi$  die Identität sind. Gibt es zwischen zwei Vektorräumen einen Isomorphismus, so heißen sie **isomorph**. Ein Homomorphismus von einem Vektorraum in sich selber heißt ein **Endomorphismus** unseres Vektorraums. Ein Isomorphismus von einem Vektorraum in sich selber heißt ein **Automorphismus** unseres Vektorraums.

3.2.1.3. Die Automorphismen eines Vektorraums  $V$  bilden mit der Hintereinanderausführung als Verknüpfung eine Gruppe. Sie heißt die **allgemeine lineare Gruppe** oder auch die **Automorphismengruppe** unseres Vektorraums  $V$  und wird notiert

$$\mathrm{GL}(V) = \mathrm{Aut}(V)$$

nach der englischen Bezeichnung **general linear group**. Wenn wir betonen wollen, daß wir  $K$ -lineare Automorphismen meinen, schreiben wir auch  $\mathrm{Aut}_K(V)$ .

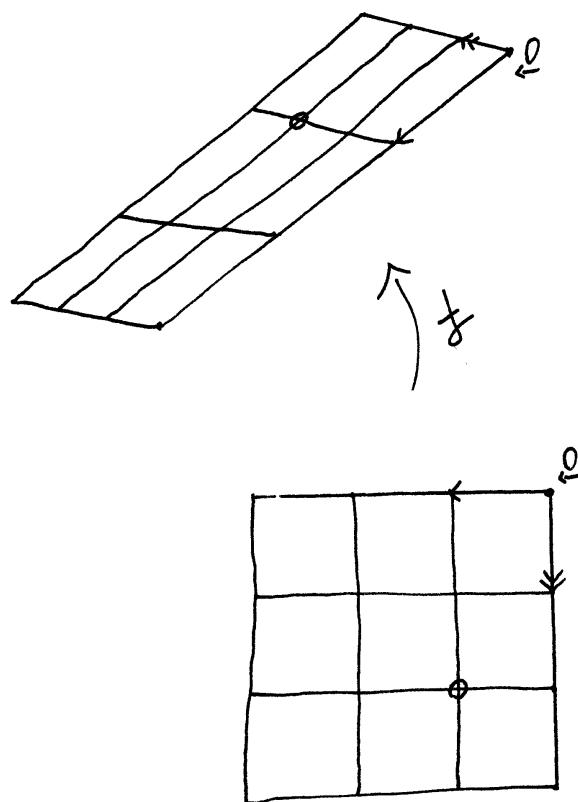
3.2.1.4. Jede lineare Abbildung bildet den Nullvektor auf den Nullvektor ab, denn für  $f : V \rightarrow W$  linear gilt  $f(\vec{0}) = f(\vec{0} + \vec{0}) = f(\vec{0}) + f(\vec{0})$  und Addition des Negativen von  $f(\vec{0})$  auf beiden Seiten liefert die Behauptung. Man zeigt auch leicht per Induktion über  $n$ , daß gegeben  $f : V \rightarrow W$  linear gilt

$$f(\lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n) = \lambda_1 f(\vec{v}_1) + \dots + \lambda_n f(\vec{v}_n)$$

für beliebige  $\lambda_i \in K$  und  $\vec{v}_i \in V$ .

*Didaktische Anmerkung* 3.2.1.5. Ich denke, an dieser Stelle mag auch der Abschnitt 2.2.3 über Homomorphismen von Magmas und Monoiden und Gruppen besprochen werden, ergänzt um Homomorphismen von Körpern. Besser wäre es aber, diesen Abschnitt schon früher zu besprechen. Dann kann man hier an 2.2.3.7 erinnern, wonach sogar überhaupt jeder Gruppenhomomorphismus das neutrale Element auf das neutrale Element werfen muß.

Übung



Eine lineare Abbildung des Richtungsraums der Papierebene auf sich selbst. Sie ist sogar ein Automorphismus.

**3.2.1.6 (Herkunft der Terminologie).** Die Herkunft eines Teils dieser Terminologie haben wir bereits in 2.2.3.9 diskutiert. „Linear“ heißen unsere Abbildungen vermutlich, weil im Fall  $\mathbb{R}$ -linearer Abbildungen  $f : \mathbb{R} \rightarrow \mathbb{R}$  ihre Graphen Geraden alias gerade Linien sind. Allerdings sind auch allgemeiner die Graphen der Funktionen  $f : \mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto ax + b$  gerade Linien, und diese Abbildungen sind in unserem Sinne nur linear im Fall  $b = 0$ . Auf der Schule haben Sie möglicherweise diese Funktionen auch im Fall  $b \neq 0$  „linear“ genannt, aber in der mathematischen Fachsprache heißen besagte Funktionen nur im Fall  $b = 0$  linear und sonst „affin“. Das Wort „Endomorphismus“ kommt von griechisch „ενδον“ für deutsch „drinnen“, und das Wort „Automorphismus“ von „αυτός“ für deutsch „selbst“.

**Beispiele 3.2.1.7.** Die Projektionen auf die Faktoren  $\text{pr}_i : K^n \rightarrow K$  sind linear. Die Abbildung  $K^2 \rightarrow K$  gegeben durch  $(x, y) \mapsto ax + by$  ist linear für beliebige aber feste  $a, b \in K$ . Gegeben ein Vektorraum  $V$  und ein Vektor  $\vec{v} \in V$  ist die Abbildung  $K \rightarrow V$  gegeben durch  $\lambda \mapsto \lambda\vec{v}$  linear. Jede lineare Abbildung von  $K$  in einen  $K$ -Vektorraum ist von dieser Gestalt. Das Quadrieren  $K \rightarrow K$  ist nicht linear, es sei denn,  $K$  ist ein Körper mit zwei Elementen, so daß das Quadrieren mit der Identität zusammenfällt.

**Beispiele 3.2.1.8.** Gegeben Vektorräume  $V, W$  sind die Projektionsabbildungen  $\text{pr}_V : (V \oplus W) \rightarrow V$  und  $\text{pr}_W : (V \oplus W) \rightarrow W$  linear. Dasselbe gilt allgemeiner für die Projektionen  $\text{pr}_i : V_1 \oplus \dots \oplus V_n \rightarrow V_i$ . Ebenso sind die **kanonischen Injektionen**  $\text{in}_V : V \rightarrow (V \oplus W)$ ,  $v \mapsto (v, 0)$  und  $\text{in}_W : W \rightarrow (V \oplus W)$ ,  $w \mapsto (0, w)$  linear und dasselbe gilt allgemeiner für die analog definierten Injektionen  $\text{in}_i : V_i \rightarrow V_1 \oplus \dots \oplus V_n$ .

**3.2.1.9.** Das Bild eines Erzeugendensystems unter einer surjektiven linearen Abbildung ist ein Erzeugendensystem. Das Bild einer linear unabhängigen Teilmenge unter einer injektiven linearen Abbildung ist eine linear unabhängige Teilmenge.

**Satz 3.2.1.10 (Klassifikation von Vektorräumen durch ihre Dimension).** *Gegeben eine natürliche Zahl  $n$  ist ein Vektorraum über einem Körper  $K$  genau dann isomorph zu  $K^n$ , wenn er die Dimension  $n$  hat.*

**Beweis.** Natürlich gehen unter einem Vektorraumisomorphismus Erzeugendensysteme in Erzeugendensysteme, linear unabhängige Teilmengen in linear unabhängige Teilmengen und Basen in Basen über. Sind also zwei Vektorräume isomorph, so haben sie auch dieselbe Dimension. Hat umgekehrt ein Vektorraum  $V$  eine angeordnete Basis  $B = (\vec{v}_1, \dots, \vec{v}_n)$  aus  $n$  Vektoren, so liefert die Vorschrift  $(\lambda_1, \dots, \lambda_n) \mapsto \lambda_1\vec{v}_1 + \dots + \lambda_n\vec{v}_n$  etwa nach 3.1.6.12 einen Vektorraumisomorphismus  $K^n \xrightarrow{\sim} V$ .  $\square$

**3.2.1.11 (Stufenzahl nach Durchführen des Gauß-Algorithmus).** Nun können wir auch unsere Ausgangsfrage 3.1.1.15 lösen, ob die „Zahl der freien Parameter“ bei unserer Darstellung der Lösungsmenge eines linearen Gleichungssystems eigentlich wohlbestimmt ist oder präziser, ob beim Anwenden des Gauß-Algorithmus dieselbe Zahl von Stufen entsteht, wenn wir zuvor die Variablen umnummerieren alias die Spalten vertauschen. Wenn wir das für homogene Systeme zeigen können, so folgt es offensichtlich für beliebige Systeme. Bei homogenen Systemen ist jedoch die Lösungsmenge  $L \subset K^m$  ein Untervektorraum und wir erhalten einen Vektorraumisomorphismus  $L \xrightarrow{\sim} K^{m-r}$  durch „Streichen aller Einträge, bei denen eine neue Stufe beginnt“, also durch Weglassen von  $x_{s(1)}, x_{s(2)}, \dots, x_{s(r)}$  aus einem  $m$ -Tupel  $(x_1, \dots, x_m) \in L$ . Damit erhalten wir für die Zahl  $r$  der Stufen die von allen Wahlen unabhängige Beschreibung als Zahl der Variablen abzüglich der Dimension des Lösungsraums, in Formeln  $r = m - \dim_K L$ .

## Übungen

*Übung 3.2.1.12.* Ein Punkt, der unter einer Abbildung auf sich selbst abgebildet wird, heißt ein **Fixpunkt** besagter Abbildung. Gegeben eine Abbildung  $f : X \rightarrow X$  notiert man die Menge ihrer Fixpunkte auch

$$X^f := \{x \in X \mid f(x) = x\}$$

Man zeige: Gegeben ein Vektorraum  $V$  und ein Endomorphismus  $f \in \text{End } V$  bildet die Menge der von  $f$  festgehaltenen Vektoren alias aller **Fixvektoren von  $f$**  stets einen Untervektorraum  $V^f \subset V$ .

*Übung 3.2.1.13.* Jede Verknüpfung von Vektorraumhomomorphismen ist wieder ein Vektorraumhomomorphismus. Sind also in Formeln  $g : U \rightarrow V$  und  $f : V \rightarrow W$  Vektorraumhomomorphismen, so ist auch  $f \circ g : U \rightarrow W$  ein Vektorraumhomomorphismus.

*Übung 3.2.1.14.* Gegeben ein surjektiver Vektorraumhomomorphismus  $g : U \twoheadrightarrow V$  und eine Abbildung  $f : V \rightarrow W$  in einen weiteren Vektorraum ist  $f$  genau dann linear, wenn die Verknüpfung  $f \circ g : U \rightarrow W$  linear ist. Gegeben ein injektiver Vektorraumhomomorphismus  $f : V \hookrightarrow W$  und eine Abbildung  $g : U \twoheadrightarrow V$  von einem weiteren Vektorraum nach  $V$  ist  $g$  genau dann linear, wenn die Verknüpfung  $f \circ g : U \rightarrow W$  linear ist. Hinweis: 2.2.3.37.

*Übung 3.2.1.15.* Ist  $f : V \rightarrow W$  ein bijektiver Vektorraumisomorphismus, so ist auch die Umkehrabbildung  $f^{-1} : W \rightarrow V$  ein Vektorraumhomomorphismus und  $f$  ist folglich ein Isomorphismus.

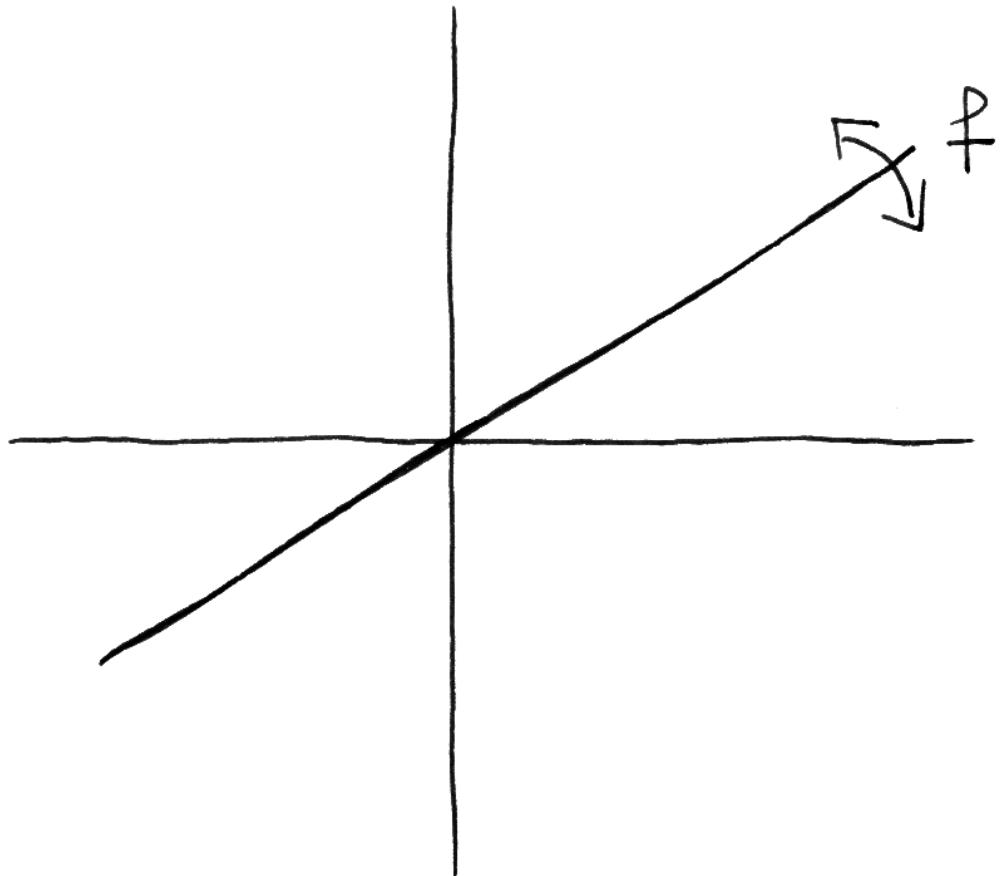


Illustration zu Übung 3.2.1.12, nach der die Fixpunktmenge jedes Endomorphismus eines Vektorraums ein Untervektorraum ist. Zum Beispiel ist die Spiegelung an einer Ursprungsgerade eine lineare Abbildung und ihre Fixpunktmenge ist in der Tat ein Untervektorraum, nämlich besagte Ursprungsgerade.

*Übung 3.2.1.16.* Wieviele Untervektorräume besitzt der  $\mathbb{R}^2$ , die unter der Spiegelung  $(x, y) \mapsto (x, -y)$  in sich selber überführt werden? Welche Untervektorräume des  $\mathbb{R}^3$  werden unter der Spiegelung  $(x, y, z) \mapsto (x, y, -z)$  in sich selber überführt?

*Ergänzende Übung 3.2.1.17.* Eine Gruppe, in der jedes Element sein eigenes Inverses ist, kann nach 3.1.2.18 auf genau eine Weise mit der Struktur eines Vektorraums über dem Körper mit zwei Elementen versehen werden. Ein Beispiel ist unsere Gruppe aus 2.2.2.19 mit den Teilmengen einer Menge  $Z$  als Elementen. Man zeige, daß dieser Vektorraum isomorph ist zum Vektorraum aller Abbildungen der Menge  $Z$  in der Körper mit zwei Elementen.

*Übung 3.2.1.18.* Eine Abbildung  $f : V \rightarrow W$  von Vektorräumen ist genau dann linear, wenn ihr Graph  $\Gamma(f) \subset V \times W$  ein Untervektorraum des Produkts ist.

### 3.2.2 Dimensionsformel für lineare Abbildungen

**Lemma 3.2.2.1.** *Das Bild eines Untervektorräums unter einer linearen Abbildung ist ein Untervektorraum. Das Urbild eines Untervektorräums unter einer linearen Abbildung ist ein Untervektorraum.*

*Beweis.* 1. Sei  $f : V \rightarrow W$  unsere lineare Abbildung. Sei  $U \subset V$  ein Untervektorraum. Wir müssen zeigen, daß auch  $f(U) \subset W$  ein Untervektorraum ist. Da  $f$  ein Homomorphismus der zugrundeliegenden additiven Gruppen ist, ist  $f(U)$  schon mal eine additive Untergruppe von  $W$  nach 2.2.3.24. Da  $U$  ein Untervektorraum ist, gilt weiter  $\lambda \vec{u} \in U$ . Dann folgt mit der Linearität  $\lambda \vec{w} = \lambda f(\vec{u}) = f(\lambda \vec{u}) \in f(U)$ . Also hat  $f(U)$  alle von einem Untervektorraum geforderten Eigenschaften.

2. Sei  $f : V \rightarrow W$  unsere lineare Abbildung. Sei  $Z \subset W$  ein Untervektorraum. Da  $f$  ein Homomorphismus der zugrundeliegenden additiven Gruppen ist, ist  $f^{-1}(Z) := \{\vec{v} \in V \mid f(\vec{v}) \in Z\}$  schon mal eine additive Untergruppe von  $V$  nach 2.2.3.24. Gegeben  $\vec{v} \in f^{-1}(Z)$  und  $\lambda \in K$  gilt weiter  $f(\lambda \vec{v}) = \lambda f(\vec{v}) \in Z$  wegen der Linearität und da  $Z$  ein Untervektorraum ist. Aus der Definition des Urbilds folgt  $\lambda \vec{v} \in f^{-1}(Z)$ . Also hat  $f^{-1}(Z)$  alle von einem Untervektorraum geforderten Eigenschaften.  $\square$

3.2.2.2. Das **Bild** einer linearen Abbildung  $f : V \rightarrow W$  alias die Teilmenge  $(\text{im } f) := f(V) \subset W$  ist nach 3.2.2.1 ein Untervektorraum von  $W$ .

3.2.2.3. Das Urbild des Nullvektors unter einer linearen Abbildung  $f : V \rightarrow W$  notiert man auch

$$(\ker f) := f^{-1}(0) = \{v \in V \mid f(v) = 0\}$$

und nennt es den **Kern** der linearen Abbildung  $f$ . Der Kern ist nach 3.2.2.1 ein Untervektorraum von  $V$ . Wir hatten ihn in 2.2.3.21 sogar bereits für beliebige Gruppenhomomorphismen eingeführt.

**Lemma 3.2.2.4 (Verschwindender Kern bedeutet Injektivität).** *Eine lineare Abbildung  $f : V \rightarrow W$  ist injektiv genau dann, wenn ihr Kern Null ist.*

*Beweis.* Das sollten sie in Übung 2.2.3.21 bereits für beliebige Gruppenhomomorphismen zeigen. Hier geben wir das Argument noch einmal in unserem Spezialfall. Liegen im Kern außer dem Nullvektor von  $V$  noch andere Vektoren, so werden verschiedene Vektoren aus  $V$  unter  $f$  auf den Nullvektor von  $W$  abgebildet und unsere Abbildung ist nicht injektiv. Ist umgekehrt unsere Abbildung nicht injektiv, so gibt es  $v \neq v_1$  in  $V$  mit  $f(v) = f(v_1)$  und es folgt  $f(v - v_1) = 0$  aber  $v - v_1 \neq 0$ . Mit  $v - v_1$  liegt also ein von Null verschiedener Vektor im Kern, der folglich nicht der Nullraum sein kann.  $\square$

**Satz 3.2.2.5.** *Für jede lineare Abbildung  $f : V \rightarrow W$  von Vektorräumen gilt die Dimensionsformel*

$$\dim V = \dim(\ker f) + \dim(\operatorname{im} f)$$

*Beweis.* Ist  $V$  endlich erzeugt, so ist auch  $(\operatorname{im} f)$  endlich erzeugt, da ja für jedes Erzeugendensystems  $E \subset V$  sein Bild  $f(E)$  ein Erzeugendensystem von  $f(V) = \operatorname{im} f$  ist. Ebenso ist mit  $V$  auch  $(\ker f)$  endlich erzeugt, nach 3.1.7.11 ist ja sogar jeder Untervektorraum eines endlich erzeugten Vektorraums endlich erzeugt. Gilt also umgekehrt  $\dim(\ker f) = \infty$  oder  $\dim(\operatorname{im} f) = \infty$ , so folgt  $\dim V = \infty$  und unser Satz gilt in diesen beiden Fällen. Wir brauchen ihn also nur noch in dem Fall zu zeigen, daß  $(\ker f)$  und  $(\operatorname{im} f)$  beide endlichdimensional sind. In diesem Fall folgt er aus dem anschließenden präziseren Lemma 3.2.2.6. Alternativ kann man auch mit Übung 3.2.2.12 argumentieren.  $\square$

**Lemma 3.2.2.6.** *Sei  $f : V \rightarrow W$  eine lineare Abbildung. Ist  $A$  eine Basis ihres Kerns,  $B$  eine Basis ihres Bildes und  $g : B \rightarrow V$  eine Wahl von Urbildern unserer Basis des Bildes, so ist  $g(B) \cup A$  eine Basis von  $V$ .*

3.2.2.7. Wir zeigen sogar stärker: Erzeugt  $A$  den Kern und  $B$  das Bild, so erzeugt  $g(B) \cup A$  ganz  $V$ . Sind  $A$  und  $B$  linear unabhängig, so auch  $g(B) \cup A$ .

*Beweis.* Gegeben  $\vec{v} \in V$  haben wir  $f(\vec{v}) = \lambda_1 \vec{w}_1 + \dots + \lambda_r \vec{w}_r$  mit  $\vec{w}_i \in B$ . Offensichtlich liegt dann  $\vec{v} - \lambda_1 g(\vec{w}_1) - \dots - \lambda_r g(\vec{w}_r)$  im Kern von  $f$  und so folgt, daß  $g(B) \cup A$  ganz  $V$  erzeugt. Um die lineare Unabhängigkeit zu zeigen nehmen wir an, es gelte

$$\lambda_1 g(\vec{w}_1) + \dots + \lambda_r g(\vec{w}_r) + \mu_1 \vec{v}_1 + \dots + \mu_s \vec{v}_s = 0$$

mit den  $\vec{v}_i \in A$  und  $\vec{w}_j \in B$  paarweise verschieden. Wenden wir  $f$  an, so folgt  $\lambda_1 \vec{w}_1 + \dots + \lambda_r \vec{w}_r = 0$  und damit  $\lambda_1 = \dots = \lambda_r = 0$  wegen der linearen Unabhängigkeit der  $\vec{w}_i$ . Setzen wir diese Erkenntnis in die ursprüngliche Gleichung ein, so folgt weiter  $\mu_1 = \dots = \mu_s = 0$  wegen der linearen Unabhängigkeit der Vektoren  $\vec{v}_j$ .  $\square$

**Korollar 3.2.2.8 (Isomorphismus durch Dimensionsvergleich).** *Jede injektive lineare Abbildung zwischen Vektorräumen derselben endlichen Dimension ist ein Isomorphismus. Jede surjektive lineare Abbildung zwischen Vektorräumen derselben endlichen Dimension ist ein Isomorphismus.*

*Beweis.* Sei  $f : V \rightarrow W$  unsere lineare Abbildung. Ist  $f$  injektiv, so folgt  $\ker f = 0$  und dann  $\dim(\text{im } f) = \dim V = \dim W$  aus der Dimensionsformel und so  $\text{im } f = W$  mit 3.1.7.11. Ist  $f$  surjektiv, so folgt erst  $\ker f = 0$  aus der Dimensionsformel und dann die Injektivität aus 3.2.2.4.  $\square$

**Korollar 3.2.2.9 (Dimensionssatz).** *Gegeben ein Vektorraum  $V$  mit Teilräumen  $U, W \subset V$  gilt*

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$$

*Beweis.* Wir haben diesen Satz bereits in 3.1.7.12 sozusagen zu Fuß bewiesen. Mit unserer Dimensionsformel 3.2.2.5 können wir nun noch einen alternativen Beweis geben. Betrachtet man nämlich die lineare Abbildung

$$f : U \oplus W \rightarrow V$$

gegeben durch  $f(u, w) = u + w$ , so gilt  $(\text{im } f) = U + W$  und die Abbildung  $d \mapsto (d, -d)$  definiert einen Isomorphismus  $(U \cap W) \xrightarrow{\sim} \ker f$ . Die Formel 3.1.7.16 für die Dimension der direkten Summe in Verbindung mit der Dimensionsformel liefert so

$$\dim U + \dim W = \dim(U \oplus W) = \dim(U \cap W) + \dim(U + W) \quad \square$$

**Definition 3.2.2.10.** Zwei Untervektorräume  $U, W$  eines Vektorraums  $V$  heißen **komplementär**, wenn die Addition eine Bijektion

$$U \times W \xrightarrow{\sim} V$$

liefert. Als lineare Abbildung ist das unter Verwendung der in 3.1.3.10 eingeführten Notation dann sogar ein Vektorraumisomorphismus  $+ : U \oplus W \xrightarrow{\sim} V$ . Des Weiteren sagt man in dieser Situation,  $W$  sei ein **Vektorraumkomplement** oder kurz **Komplement von  $U$  in  $V$** .

**3.2.2.11 (Vektorraumkomplement und Komplementmenge).** Man unterscheidet sorgfältig zwischen Vektorraumkomplement und Komplementmenge: Komplementäre Untervektorräume sind keineswegs disjunkt, sondern schneiden sich im Nullvektor, und die Vereinigung komplementärer echter Untervektorräume ist auch nie der ganze Ausgangsraum, sondern nur ein Erzeugendensystem desselben. Auf französisch spricht man von einem „sousespace supplémentaire“, das ist noch deutlicher. Allerdings werden sich beide Begriffe in 4.7.7.16 als Ausprägungen von „Koprodukten“ erweisen, und das ist zumindest eine gewisse Rechtfertigung für diese möglicherweise verwirrende Terminologie.

### Übungen

*Übung 3.2.2.12.* Sei  $f : V \rightarrow W$  eine lineare Abbildung. Man zeige: Ist  $\vec{v}_1, \dots, \vec{v}_s$  eine Basis des Kerns  $\ker f$  und  $\vec{v}_{s+1}, \dots, \vec{v}_n$  eine Erweiterung zu einer linear unabhängigen Teilmenge  $\vec{v}_1, \dots, \vec{v}_n$  von  $V$ , so ist die Familie  $f(\vec{v}_{s+1}), \dots, f(\vec{v}_n)$  linear unabhängig in  $W$ . Ist unsere Erweiterung sogar eine Basis von  $V$ , so ist unsere Familie eine Basis des Bildes von  $f$ .

*Übung 3.2.2.13.* Man zeige: Zwei Untervektorräume  $U, W$  eines Vektorraums  $V$  sind komplementär genau dann, wenn gilt  $V = U + W$  und  $U \cap W = 0$ .

*Ergänzende Übung 3.2.2.14.* Die Menge aller Untervektorräume eines gegebenen Vektorraums bildet mit den Verknüpfungen  $+$  und  $\cap$  als  $\vee$  und  $\wedge$  einen Verband im Sinne von 2.2.6.3 und in diesem Verband gilt zusätzlich

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

für alle  $a, b, c$ . Ein Verband mit dieser Eigenschaft heißt **modular**. Gleichbedeutend ist die Forderung  $(a \vee b) \wedge c = a \vee (b \wedge c)$  für alle  $a, b, c$  mit  $a \vee c = c$ . Mit demselben Beweis wird in einer später eingeführten Terminologie folgen, daß die Untermoduln eines gegebenen Moduls einen modularen Verband bilden, und daher röhrt auch die Terminologie. Mit einem Verband ist auch der duale Verband modular, wie man durch Einsetzen von  $a \wedge c$  für  $a$  erkennt.

*Ergänzende Übung 3.2.2.15.* Ein Verband  $(B, \wedge, \vee)$  ist genau dann modular, wenn wir für je zwei Elemente  $a, b \in B$  in Bezug auf die in ?? beschriebene Ordnungsrelation zueinander inverse Bijektionen zwischen den Intervallen  $[a \wedge b, b]$  und  $[a, a \vee b]$  erhalten durch die Regeln  $w \mapsto a \vee w$  und  $v \mapsto v \wedge b$ . Hinweis: Man setze ein Element  $w \in [a, a \vee b]$  an als  $w = (a \vee c) \wedge (a \vee b)$  und transportiere es hin und zurück. Dualitätsbetrachtungen liefern den Rest der Behauptung.

*Übung 3.2.2.16.* Man zeige: Zwei Untervektorräume  $U, W$  eines endlichdimensionalen Vektorraums  $V$  sind komplementär genau dann, wenn gilt  $V = U + W$  und  $\dim U + \dim W \leq \dim V$ . Hinweis: 3.1.7.16.

*Übung 3.2.2.17.* Der Kern einer von Null verschiedenen linearen Abbildung in den Grundkörper ist stets eine Hyperebene im Sinne von 3.1.5.16.

*Ergänzende Übung 3.2.2.18.* Sei  $\varphi : V \rightarrow V$  ein Endomorphismus eines endlich-dimensionalen Vektorraums. Man zeige, daß  $\ker(\varphi^2) = \ker \varphi$  gleichbedeutend ist zu  $+ : \ker \varphi \oplus \text{im } \varphi \xrightarrow{\sim} V$ .

*Ergänzende Übung 3.2.2.19.* Ein Element  $f$  einer Menge mit Verknüpfung heißt **idempotent** genau dann, wenn in multiplikativer Notation gilt  $f^2 = f$ . Die idempotenten Endomorphismen eines Vektorraums entsprechen eineindeutig seinen Zerlegungen in eine direkte Summe von zwei komplementären Teilmengen. Gegeben ein Vektorraum  $V$  liefert genauer die Abbildung  $f \mapsto (\text{im } f, \ker f)$  eine Bijektion

$$\{f \in \text{End } V \mid f^2 = f\} \rightsquigarrow \left\{ (I, J) \in \mathcal{P}(V)^2 \mid \begin{array}{l} I, J \subset V \text{ sind Teilmengen} \\ \text{und als solche komplementär} \end{array} \right\}$$

Für die Umkehrabbildung unserer Bijektion sagt man, sie ordne unserem Paar  $(I, J)$  komplementärer Teilmengen die **Projektion von  $V$  auf  $I$  längs  $J$**  zu.

*Übung 3.2.2.20.* Sei  $p : V \twoheadrightarrow W$  eine surjektive lineare Abbildung. Man zeige: Genau dann ist ein Teilraum  $U \subset V$  komplementär zu  $\ker p$ , wenn  $p$  einen Isomorphismus  $p : U \xrightarrow{\sim} W$  induziert.

### 3.2.3 Räume von linearen Abbildungen

3.2.3.1. Seien  $V, W$  Vektorräume über einem Körper  $K$ . Die Menge aller Homomorphismen von  $V$  nach  $W$  notieren wir

$$\text{Hom}_K(V, W) = \text{Hom}(V, W) \subset \text{Ens}(V, W)$$

**Lemma 3.2.3.2 (Lineare Abbildungen und Basen).** *Seien  $V, W$  Vektorräume über einem Körper  $K$  und sei  $B \subset V$  eine Basis. So liefert das Einschränken von Abbildungen eine Bijektion*

$$\text{Hom}_K(V, W) \xrightarrow{\sim} \text{Ens}(B, W)$$

*Jede lineare Abbildung ist also in Worten festgelegt und festlegbar durch ihre Werte auf einer Basis.*

*Beweis im Fall einer endlichen Basis.* Seien  $f, g : V \rightarrow W$  linear. Gilt  $f(\vec{v}) = g(\vec{v})$  für alle  $\vec{v} \in B$ , so folgt  $f(\lambda_1 \vec{v}_1 + \dots + \lambda_r \vec{v}_r) = g(\lambda_1 \vec{v}_1 + \dots + \lambda_r \vec{v}_r)$  für alle  $\lambda_1, \dots, \lambda_r \in K$  und  $\vec{v}_1, \dots, \vec{v}_r \in B$  und damit  $f(\vec{v}) = g(\vec{v})$  für alle  $\vec{v}$  im Erzeugnis von  $B$  alias für alle  $\vec{v} \in V$ . Das zeigt die Injektivität der im Lemma betrachteten Einschränkungsabbildung sogar allgemeiner für jedes Erzeugendensystem  $B$  von

V. Ist  $B$  zusätzlich eine Basis und ist umgekehrt eine Abbildung von Mengen  $g : B \rightarrow W$  gegeben, so können wir sie zu einer linearen Abbildung  $\tilde{g} : V \rightarrow W$  ausdehnen wie folgt: Jeder Vektor  $\vec{v} \in V$  lässt sich ja nach 3.1.6.12 eindeutig als Linearkombination der Basisvektoren schreiben, etwa  $\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_r \vec{v}_r$  mit paarweise verschiedenen  $\vec{v}_i \in B$ . Wir können nun schlicht  $\tilde{g}$  definieren durch die Vorschrift

$$\tilde{g}(\vec{v}) := \lambda_1 g(\vec{v}_1) + \dots + \lambda_r g(\vec{v}_r)$$

Man sieht leicht, daß dann  $\tilde{g}$  linear ist und auf der Basis zu  $g$  einschränkt.  $\square$

3.2.3.3. Im Fall einer unendlichen Basis funktioniert derselbe Beweis, nur sollten wir noch genauer sagen, was wir meinen mit der Aussage, jeder Vektor  $\vec{v} \in V$  lasse sich eindeutig als Linearkombination der Basisvektoren schreiben. Dazu entwickeln wir die Terminologie des „freien Vektorraums über einer Menge“.

3.2.3.4 (**Freie Vektorräume und ihre universelle Eigenschaft**). Seien  $X$  eine Menge und  $K$  ein Körper. Die Menge  $\text{Ens}(X, K)$  aller Abbildungen  $f : X \rightarrow K$  mit der punktweisen Addition und Multiplikation mit Skalaren ist offensichtlich ein  $K$ -Vektorraum. Darin bilden alle Abbildungen, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen, einen Untervektorraum

$$K\langle X \rangle \subset \text{Ens}(X, K)$$

Dieser Vektorraum  $K\langle X \rangle$  heißt der **freie Vektorraum über der Menge  $X$** . Gegeben  $x \in X$  bezeichne  $\delta_x : X \rightarrow K$  die Abbildung mit  $\delta_x(x) = 1$  und  $\delta_x(y) = 0$  für  $y \neq x$ . So ist die sogenannte **kanonische Einbettung**  $\text{can} : X \rightarrow K\langle X \rangle$  gegeben durch  $x \mapsto \delta_x$  offensichtlich eine Basis im Sinne einer Familie von  $K\langle X \rangle$ . Weiter liefert für jeden  $K$ -Vektorraum  $V$  das Vorschalten der kanonischen Einbettung  $\text{can}$  eine Bijektion

$$(\circ \text{can}) : \text{Hom}_K(K\langle X \rangle, V) \xrightarrow{\sim} \text{Ens}(X, V)$$

In der Tat kann man in diesem Fall eine Umkehrabbildung leicht angeben durch die Vorschrift  $\phi \mapsto \Phi$  mit

$$\Phi : a \mapsto \sum_{\{x | a(x) \neq 0\}} a(x) \phi(x)$$

Wir sagen dann auch, die lineare Abbildung  $\Phi : K\langle X \rangle \rightarrow V$  entstehe aus der Abbildung  $\phi : X \rightarrow V$  durch **lineare Fortsetzung**.

3.2.3.5 (**Notationen im Zusammenhang mit freien Vektorräumen**). Ein Element  $a \in K\langle X \rangle$  des freien Vektorraums über einer Menge  $X$  fassen wir am liebsten als „formale Linearkombination von Elementen von  $X$ “ auf und notieren

es statt  $\sum_{\{x|a(x) \neq 0\}} a(x)\delta_x$  lieber  $\sum_{x \in X} a_x x$  mit der Indexnotation  $a(x) = a_x$  für Abbildungen, der Abkürzung  $\delta_x = x$  und der Konvention, daß bei unendlichen Summen mit nur endlich vielen von Null verschiedenen Summanden eben nur die Summe der von Null verschiedenen Summanden gemeint sein soll. In dieser Notation wirkt dann die kanonische Einbettung wie die Einbettung einer Teilmenge. Weiter wird in dieser Notation die lineare Fortsetzung  $\Phi$  einer Abbildung  $\phi : X \rightarrow V$  beschrieben durch die hoffentlich suggestivere Formel

$$\Phi : \sum_{x \in X} a_x x \mapsto \sum_{x \in X} a_x \phi(x)$$

Im Fall der Menge  $X = \{\sharp, \flat, \natural\}$  wäre ein typisches Element von  $\mathbb{Q}\langle X \rangle$  etwa der Ausdruck

$$\frac{1}{2} \sharp - \frac{7}{5} \flat + 3 \natural$$

Im Fall einer endlichen Menge  $X = \{x_1, \dots, x_n\}$  schreiben wir statt dem etwas umständlichen  $K\langle\{x_1, \dots, x_n\}\rangle$  auch abkürzend  $K\langle x_1, \dots, x_n \rangle$ . Unseren Vektorraum von eben hätten wir also auch mit  $\mathbb{Q}\langle \sharp, \flat, \natural \rangle$  bezeichnen können. Wenn wir betonen wollen, daß  $X$  für eine Menge von Erzeugern und nicht etwa einen einzigen Erzeuger steht, schreiben wir statt  $K\langle X \rangle$  genauer  $K\langle !X \rangle$ . Manchmal lassen wir auch die eckigen Klammern weg und schreiben statt  $K\langle X \rangle$  einfach  $KX$ .

**Satz 3.2.3.6 (Linearkombinationen von Basiselementen, Variante).** *Seien  $K$  ein Körper,  $V$  ein  $K$ -Vektorraum und  $(\vec{v}_i)_{i \in I}$  eine Familie von Vektoren aus  $V$ . So sind gleichbedeutend:*

1. *Die Familie  $(\vec{v}_i)_{i \in I}$  ist eine Basis von  $V$ ;*
2. *Die durch lineare Fortsetzung von  $\phi : I \rightarrow V$ ,  $i \mapsto \vec{v}_i$  nach 3.2.3.4 entstehende lineare Abbildung ist ein Isomorphismus  $\Phi : K\langle I \rangle \xrightarrow{\sim} V$ .*

*Beweis.* Ausführlicher gilt sogar:

$$\begin{aligned} (\vec{v}_i)_{i \in I} \text{ ist Erzeugendensystem} &\Leftrightarrow \Phi \text{ ist eine Surjektion } K\langle I \rangle \twoheadrightarrow V \\ (\vec{v}_i)_{i \in I} \text{ ist linear unabhängig} &\Leftrightarrow \Phi \text{ ist eine Injektion } K\langle I \rangle \hookrightarrow V \\ (\vec{v}_i)_{i \in I} \text{ ist eine Basis} &\Leftrightarrow \Phi \text{ ist eine Bijektion } K\langle I \rangle \xrightarrow{\sim} V \end{aligned}$$

Der Beweis ist mutatis mutandis derselbe wie im in 3.1.6.12 behandelten Fall einer endlichen Familie, mit einigen Vereinfachungen, die die bereits entwickelte Theorie ermöglicht. Das Bild von  $\Phi$  ist offensichtlich der von unserer Familie erzeugte Untervektorraum. Andererseits ist  $\Phi$  nach 3.2.2.4 genau dann injektiv, wenn gilt  $\ker(\Phi) = 0$ . Diese Bedingung bedeutet aber nach unseren Definitionen genau die lineare Unabhängigkeit unserer Familie.  $\square$

*Beweis von Lemma 3.2.3.2 im allgemeinen.* Ist  $V$  ein  $K$ -Vektorraum und  $B \subset V$  eine Basis, so liefert die lineare Ausdehnung der Einbettung  $\phi : B \hookrightarrow V$  nach 3.2.3.6 einen Isomorphismus  $\Phi : K\langle B \rangle \xrightarrow{\sim} V$ . Wir erhalten so für jeden weiteren  $K$ -Vektorraum Bijektionen

$$\text{Hom}_K(V, W) \xrightarrow{\sim} \text{Hom}_K(K\langle B \rangle, W) \xrightarrow{\sim} \text{Ens}(B, W)$$

durch Vorschalten von  $\Phi$  und  $\text{can}$ . Deren Verknüpfung alias das Vorschalten der Einbettung  $B \hookrightarrow V$  ist also auch eine Bijektion, und das war genau die Behauptung.  $\square$

3.2.3.7. Die folgende Definition mit den zugehörigen Übungen ist dazu gedacht, die Diskussion der Determinante und allgemeinerer multilinearer Abbildungen vorzubereiten. An dieser Stelle ist es wesentlich, daß wir über einem Körper und nicht etwa über einem Schiefkörper arbeiten.

**Definition 3.2.3.8.** Seien  $U, V, W$  Vektorräume über einem Körper  $K$ . Eine Abbildung  $F : U \times V \rightarrow W$  alias 2-Multiabbildung  $F : U \curlyvee V \rightarrow W$  heißt **bilinear**, wenn sie für jedes feste  $v \in V$  linear ist in  $u \in U$  und für jedes feste  $u \in U$  linear in  $v \in V$ . In Formeln bedeutet das

$$\begin{aligned} F(u + a, v) &= F(u, v) + F(a, v) \\ F(\lambda u, v) &= \lambda F(u, v) \\ F(u, v + b) &= F(u, v) + F(u, b) \\ F(u, \mu v) &= \mu F(u, v) \end{aligned}$$

für alle  $\lambda, \mu \in K$  und  $u, a \in U$  und  $v, b \in V$ . Die Menge aller solchen bilinearen Abbildungen notieren wir

$$\text{Mod}_K(U \curlyvee V, W) = \text{Hom}_K^{(2)}(U \times V, W) \subset \text{Ens}(U \times V, W)$$

Mir gefällt die erste Notation besser, in der  $\curlyvee$  ein neues Trennsymbol ist und  $\text{Mod}_K$  die „Schmelzkategorie der  $K$ -Moduln“ meint, die wir später einführen werden. Diese Notation ist jedoch unüblich. Eine bilineare Abbildung  $V \times V \rightarrow K$  in den Grundkörper heißt eine **Bilinearform auf  $V$** . Die Menge, ja den Vektorraum aller Bilinearformen auf  $V$  notieren wir  $\text{Bil}(V)$ .

## Übungen

*Übung 3.2.3.9.* Seien  $U, V, W$  Vektorräume und  $A \subset U$  sowie  $B \subset V$  jeweils Basen. So liefert die Einschränkung eine Bijektion

$$\text{Mod}_K(U \curlyvee V, W) \xrightarrow{\sim} \text{Ens}(A \times B, W)$$

In Worten ist also eine bilineare Abbildung festgelegt und festlegbar durch ihre Werte auf Paaren von Basisvektoren. Hinweis: Man orientiere sich am Beweis von 3.2.3.2.

*Ergänzende Übung 3.2.3.10.* Seien  $(X, \leq)$  eine teilgeordnete Menge und  $K$  ein Körper. Seien für alle  $x \in X$  Abbildungen  $f_x : X \rightarrow K$  gegeben mit  $f_x(x) \neq 0$  und  $f_x(y) \neq 0 \Rightarrow y \geq x$ . Man zeige, daß dann die Familie  $(f_x)_{x \in X}$  linear unabhängig ist im Vektorraum  $\text{Ens}(X, K)$  aller Abbildungen von  $X$  nach  $K$ .

*Weiterführende Übung 3.2.3.11.* Man zeige, daß für eine unendliche Menge  $X$  weder der Vektorraum  $\text{Ens}(X, K)$  noch der freie Vektorraum  $K\langle X \rangle$  über  $X$  endlich erzeugt sind.

*Übung 3.2.3.12 (Homomorphismen aus direkten Summen).* Gegeben Vektorräume  $V_1, \dots, V_n, W$  liefert die Vorschrift  $f \mapsto (f \circ \text{in}_i)_i$  einen Isomorphismus

$$\text{Hom}(V_1 \oplus \dots \oplus V_n, W) \xrightarrow{\sim} \text{Hom}(V_1, W) \oplus \dots \oplus \text{Hom}(V_n, W)$$

Die Umkehrabbildung ordnet einem Tupel linearer Abbildungen  $f_i : V_i \rightarrow W$  die lineare Abbildung  $f : V_1 \oplus \dots \oplus V_n \rightarrow W$  zu mit

$$f(\vec{v}_1, \dots, \vec{v}_n) := f_1(\vec{v}_1) + \dots + f_n(\vec{v}_n)$$

Wir notieren diese Abbildung auch  $f = (f_1, \dots, f_n)$  und denken sie uns als eine ‘‘Zeilenmatrix von linearen Abbildungen‘‘, die auf die ‘‘Spaltenmatrix von Vektoren‘‘  $(\vec{v}_1, \dots, \vec{v}_n)^\top$  angewandt wird. Es erweist sich in diesem und ähnlichen Kontexten als bequem, Elemente von direkten Summen als Spaltenvektoren zu denken.

*Übung 3.2.3.13 (Homomorphismen in direkte Summen).* Gegeben Vektorräume  $V, W_1, \dots, W_n$  liefert die Vorschrift  $g \mapsto (\text{pr}_i \circ g)_i$  einen Isomorphismus

$$\text{Hom}(V, W_1 \oplus \dots \oplus W_n) \xrightarrow{\sim} \text{Hom}(V, W_1) \oplus \dots \oplus \text{Hom}(V, W_n)$$

Die Umkehrabbildung ordnet einem Tupel linearer Abbildungen  $g_i : V \rightarrow W_i$  die lineare Abbildung  $g : V \rightarrow W_1 \oplus \dots \oplus W_n$  zu mit  $g(\vec{v}) = (g_1(\vec{v}), \dots, g_n(\vec{v}))$ . Wir notieren diese Abbildung auch  $g = (g_1, \dots, g_n)^\top$  und denken sie uns als eine ‘‘Spaltenmatrix von linearen Abbildungen‘‘, die aus einem Vektor  $\vec{v}$  eine Spalte von Vektoren macht, die wir dann als Elemente der direkten Summe auffassen.

*Übung 3.2.3.14 (Der Hom-Raum und seine Dimension).* Seien  $V, W$  Vektorräume über einem Körper  $K$ . Man zeige, daß  $\text{Hom}_K(V, W)$  ein Untervektorraum der Menge  $\text{Ens}(V, W)$  aller Abbildungen von  $V$  nach  $W$  mit ihrer Vektorraumstruktur aus 3.2.3.4 ist. Man zeige für die Dimension von  $\text{Hom}_K(V, W)$  die Formel

$$\dim \text{Hom}_K(V, W) = (\dim V)(\dim W)$$

unter der Konvention  $0 \cdot \infty = \infty \cdot 0 = 0$ . Diese Formel ist insofern mit Vorsicht zu genießen, als sie bei einer feineren Interpretation der Dimension als Kardinalität im Fall unendlichdimensionaler Räume ihre Gültigkeit verliert. Hinweis: 3.2.3.2.

*Übung 3.2.3.15.* Man zeige, daß für je drei Vektorräume  $U, V, W$  über einem Körper die Verknüpfung  $\text{Hom}(U, V) \times \text{Hom}(V, W) \rightarrow \text{Hom}(U, W)$  von linearen Abbildungen bilinear ist. Hier sind unsere Homomorphismenräume zu verstehen mit ihrer in 3.2.3.14 erklärten Vektorraumstruktur.

*Übung 3.2.3.16 (Exponentialgesetz für lineare Abbildungen).* Gegeben Vektorräume  $U, V, W$  über einem Körper induziert die Identifikation  $\text{Ens}(U \times V, W) \xrightarrow{\sim} \text{Ens}(U, \text{Ens}(V, W))$  aus dem Exponentialgesetz 2.1.6.5 einen Isomorphismus

$$\text{Hom}^{(2)}(U \times V, W) \xrightarrow{\sim} \text{Hom}(U, \text{Hom}(V, W))$$

zwischen dem Raum der bilinearen Abbildungen  $U \times V \rightarrow W$  und dem Raum der linearen Abbildungen  $U \rightarrow \text{Hom}(V, W)$ .

### 3.2.4 Lineare Abbildungen $K^n \rightarrow K^m$ und Matrizen

**Satz 3.2.4.1 (Lineare Abbildungen und Matrizen).** *Gegeben ein Körper  $K$  und natürliche Zahlen  $n, m \in \mathbb{N}$  erhalten wir eine Bijektion zwischen der Menge der linearen Abbildungen  $K^n \rightarrow K^m$  und der Menge der  $K$ -wertigen Matrizen mit  $m$  Zeilen und  $n$  Spalten*

$$\begin{aligned} M : \quad \text{Hom}_K(K^n, K^m) &\xrightarrow{\sim} \text{Mat}(m \times n; K) \\ f &\mapsto [f] \end{aligned}$$

durch die Vorschrift, die jeder linearen Abbildung  $f$  ihre **darstellende Matrix**  $M(f) := [f]$  zuordnet. Die darstellende Matrix wird dabei ihrerseits dadurch erklärt, daß in ihren Spalten die Bilder unter  $f$  der Vektoren der Standardbasis des  $K^n$  stehen, in Formeln

$$[f] := (f(e_1) | f(e_2) | \dots | f(e_n))$$

*Beweis.* Das folgt unmittelbar aus unserer Erkenntnis 3.2.3.2, daß eine lineare Abbildung festgelegt wird durch ihre Werte auf den Vektoren einer Basis, die ihrerseits beliebig vorgegeben werden können.  $\square$

*Beispiel 3.2.4.2.* Die Matrix der Identität auf  $K^n$  ist die **Einheitsmatrix**

$$I = I_n := [\text{id}] = \begin{pmatrix} 1 & & 0 & & \\ & 1 & & & \\ & & \ddots & & \\ & 0 & & & 1 \end{pmatrix}$$

mit Einträgen  $I_{i,j} = \delta_{i,j}$  in der unter der Bezeichnung **Kroneckerdelta** bekannten und allgemein gebräuchlichen Konvention

$$\delta_{i,j} = \begin{cases} 1 & i = j; \\ 0 & \text{sonst.} \end{cases}$$

Ist allgemeiner  $n \geq m$ , so ist die Matrix des „Weglassens der überzähligen Koordinaten“  $f : (x_1, \dots, x_n) \mapsto (x_1, \dots, x_m)$  gerade

$$[f] = \begin{pmatrix} 1 & & 0 & & 0 \dots 0 \\ & \ddots & & & \\ & & \ddots & & \\ 0 & & & 1 & 0 \dots 0 \end{pmatrix}$$

Die Matrix des „Vertauschens der Koordinaten“  $g : K^2 \rightarrow K^2$ ,  $(x, y) \mapsto (y, x)$  schließlich ist

$$[g] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

**Definition 3.2.4.3.** Gegeben natürliche Zahlen  $m, n, l \in \mathbb{N}$  und ein Körper  $K$  und Matrizen  $A \in \text{Mat}(n \times m; K)$ ,  $B \in \text{Mat}(m \times l; K)$  definieren wir ihr **Produkt**  $A \circ B = AB \in \text{Mat}(n \times l; K)$  durch die Formel

$$(AB)_{ik} = \sum_{j=1}^m A_{ij} B_{jk}$$

Diese Formel drückt den Eintrag der Produktmatrix  $AB$  in der  $i$ -ten Zeile und  $k$ -ten Spalte durch die Einträge der Matrizen  $A$  und  $B$  aus. In Worten gilt es, jeweils den  $j$ -ten Eintrag der  $i$ -ten Zeile von  $A$  mit dem  $j$ -ten Eintrag der  $k$ -ten Spalte von  $B$  zu multiplizieren, und die Summe dieser  $m$  Produkte ist dann der Eintrag der Produktmatrix  $AB$  in der  $i$ -ten Zeile und  $k$ -ten Spalte. Manchmal schreiben wir die Produktmatrix auch ausführlicher  $AB = A \circ B$ . Die **Matrixmultiplikation** liefert eine Abbildung

$$\begin{aligned} \text{Mat}(n \times m; K) \times \text{Mat}(m \times l; K) &\rightarrow \text{Mat}(n \times l; K) \\ (A, B) &\mapsto AB \end{aligned}$$

3.2.4.4. In der Terminologie aus 3.2.3.8 ist unsere Matrixmultiplikation eine bilineare Abbildung, wie man unschwer einsieht. Den Ursprung dieser auf den ersten Blick vielleicht absonderlich anmutenden Definition des Produkts zweier Matrizen und unserer leicht mit dem Verknüpfen von Abbildungen zu verwechselnden alternativen Notation  $AB = A \circ B$  erklärt der folgende Satz.

$$\begin{pmatrix} 1 & 2 \\ \cancel{2} & 0 \\ 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 0 & 2 & \cancel{2} & 0 \\ 1 & 7 & \cancel{6} & 6 \end{pmatrix} = \begin{pmatrix} 2 & 16 & 14 & 12 \\ 0 & 4 & \cancel{4} & 0 \\ 3 & 29 & 26 & 18 \end{pmatrix}$$

Produkt zweier Matrizen. Der gestrichelt eingekringelte Eintrag 4 in der zweiten Zeile und dritten Spalte auf der rechten Seite etwa ergibt sich aus der gestrichelt eingekringelten zweiten Zeile des ersten Faktors und der gestrichelt eingekringelten dritten Spalte des zweiten Faktors mittels der Rechnung

$$4 = 2 \cdot 2 + 0 \cdot 6.$$

**Satz 3.2.4.5 (Verknüpfen von Abbildungen und Matrixprodukt).** *Gegeben lineare Abbildungen  $g : K^l \rightarrow K^m$  und  $f : K^m \rightarrow K^n$  ist die Matrix ihrer Verknüpfung das Produkt der zugehörigen Matrizen, in Formeln*

$$[f \circ g] = [f] \circ [g]$$

*Beweis.* Sei  $(a_{ij})$  die Matrix  $[f]$  und  $(b_{jk})$  die Matrix  $[g]$ . Wir notieren die Standardbasen von  $K^n$ ,  $K^m$  und  $K^l$  als  $\vec{u}_i, \vec{v}_j$  und  $\vec{w}_k$  in der Hoffnung, daß die folgende Rechnung dadurch transparenter wird, daß wir nicht für die Standardbasis in allen drei Räumen die sonst eigentlich übliche Notation  $\vec{e}_r$  verwenden. Weiter schreiben wir die Skalare hinter die Vektoren, was wir bei konsequenter Arbeit mit einem Schiefkörper eh hätten tun müssen und was in jedem Fall die Formeln transparenter macht. In dieser Notation haben wir also

$$\begin{aligned} g(\vec{w}_k) &= (b_{*k}) = \vec{v}_1 b_{1k} + \dots + \vec{v}_m b_{mk} \\ f(\vec{v}_j) &= (a_{*j}) = \vec{u}_1 a_{1j} + \dots + \vec{u}_n a_{nj} \end{aligned}$$

und folgern

$$\begin{aligned} (f \circ g)(\vec{w}_k) &= f(\vec{v}_1 b_{1k} + \dots + \vec{v}_m b_{mk}) \\ &= f(\vec{v}_1) b_{1k} + \dots + f(\vec{v}_m) b_{mk} \\ &= \sum_{j=1}^m f(\vec{v}_j) b_{jk} \\ &= \sum_{j=1}^m \left( \sum_{i=1}^n \vec{u}_i a_{ij} \right) b_{jk} \\ &= \sum_{i=1}^n \vec{u}_i \left( \sum_{j=1}^m a_{ij} b_{jk} \right) \end{aligned}$$

Andererseits sind ja die Einträge  $(c_{ik})$  der Matrix  $[f \circ g]$  gerade definiert durch die Identität  $(f \circ g)(\vec{w}_k) = \vec{u}_1 c_{1k} + \dots + \vec{u}_n c_{nk}$ , und durch einen Koeffizientenvergleich folgt für die Einträge  $c_{ik}$  von  $[f \circ g]$  wie gewünscht  $c_{ik} = \sum_{j=1}^m a_{ij} b_{jk}$ .  $\square$

**Proposition 3.2.4.6 (Rechnen mit Matrizen).** *Für die Matrixmultiplikation gelten die folgenden Rechenregeln:*

$$\begin{aligned} (A + A')B &= AB + A'B \\ A(B + B') &= AB + AB' \\ IB &= B \\ AI &= A \\ (AB)C &= A(BC) \end{aligned}$$

für beliebige  $k, l, m, n \in \mathbb{N}$  und  $A, A' \in \text{Mat}(n \times m; K)$ ,  $B, B' \in \text{Mat}(m \times l; K)$ ,  $C \in \text{Mat}(l \times k; K)$  und  $I = I_m$  die  $(m \times m)$ -Einheitsmatrix.

*Erster Beweis.* Stures Rechnen, ich führe nur zwei Teile beispielhaft aus. Wir haben  $(AI)_{ij} = \sum_k A_{ik}I_{kj} = \sum_k A_{ik}\delta_{kj} = A_{ij}$  und das zeigt  $AI = A$ . Für die nächste Rechnung verwende ich einmal andere Notationen und nehme  $\kappa, \lambda, \mu, \nu$  als Laufindizes. Dann haben wir

$$\begin{aligned} ((AB)C)_{\nu\kappa} &= \sum_{\lambda=1}^l (AB)_{\nu\lambda} C_{\lambda\kappa} \\ &= \sum_{\lambda=1}^l \left( \sum_{\mu=1}^m A_{\nu\mu} B_{\mu\lambda} \right) C_{\lambda\kappa} \\ &= \sum_{\lambda,\mu=1}^{l,m} A_{\nu\mu} B_{\mu\lambda} C_{\lambda\kappa} \\ (A(BC))_{\nu\kappa} &= \sum_{\mu=1}^m A_{\nu\mu} (BC)_{\mu\kappa} \\ &= \sum_{\mu=1}^m A_{\nu\mu} \left( \sum_{\lambda=1}^l B_{\mu\lambda} C_{\lambda\kappa} \right) \\ &= \sum_{\mu,\lambda=1}^{m,l} A_{\nu\mu} B_{\mu\lambda} C_{\lambda\kappa} \end{aligned}$$

und das zeigt  $(AB)C = A(BC)$ .  $\square$

*Zweiter Beweis.* Wir können unsere Rechenregeln für Matrizen auch mit 3.2.4.1 und 3.2.4.5 auf die entsprechenden Regeln für lineare Abbildungen zurückführen. Um zum Beispiel  $(AB)C = A(BC)$  zu zeigen, betrachten wir die linearen Abbildungen  $a, b, c$  mit den entsprechenden Matrizen im Sinne von 3.2.4.1, finden mit 3.2.4.5 sofort

$$\begin{aligned} (AB)C &= ([a] \circ [b]) \circ [c] = [a \circ b] \circ [c] = [(a \circ b) \circ c] \\ A(BC) &= [a] \circ ([b] \circ [c]) = [a] \circ [b \circ c] = [a \circ (b \circ c)] \end{aligned}$$

und die Behauptung ergibt sich aus der für die Verknüpfung von Abbildungen offensichtlichen Identität  $(a \circ b) \circ c = a \circ (b \circ c)$ .  $\square$

**3.2.4.7 (Lineare Abbildungen  $K^m \rightarrow K^n$  als Matrixmultiplikationen).** Mit dem Formalismus der Matrixmultiplikation können wir auch die Umkehrung unserer Bijektion  $\text{Hom}_K(K^m, K^n) \xrightarrow{\sim} \text{Mat}(n \times m; K)$ ,  $f \mapsto [f]$  aus 3.2.4.1, bei der jeder linearen Abbildung ihre darstellende Matrix zugeordnet wird, elegant beschreiben. Dazu müssen wir nur die Elemente von  $K^m$  beziehungsweise  $K^n$  als Spaltenvektoren auffassen und einer Matrix  $A \in \text{Mat}(n \times m; K)$  die durch Matrixmultiplikation gegebene Abbildung  $(A \circ) : \text{Mat}(m \times 1; K) \rightarrow \text{Mat}(n \times 1; K)$  alias

$$(A \circ) : K^m \rightarrow K^n$$

zuordnen. Das folgt unmittelbar aus den Definitionen. Statt  $A \circ x$  schreibt man dann auch einfacher schlicht  $Ax$ . Die Umkehrabbildung zu  $f \mapsto [f]$  kann mit diesen Konventionen also in der Form  $A \mapsto (x \mapsto Ax)$  für  $x \in K^m$  dargestellt werden, oder noch knapper in der Form  $A \mapsto (A \circ)$ . Auf die Dauer sollte einem diese Identifikation von linearen Abbildungen  $K^m \rightarrow K^n$  und Matrizen eh so

in Fleisch und Blut übergehen, daß man unterschiedslos  $A$  schreiben und damit beides gleichzeitig meinen kann.

**3.2.4.8 (Lineare Abbildungen als Matrixmultiplikationen, Variante).** Gegeben ein Körper  $K$  liefert für jeden  $K$ -Vektorraum  $V$  das Auswerten auf dem Element  $1 \in K$  eine Bijektion  $\text{Hom}(K, V) \xrightarrow{\sim} V$ . Deren Umkehrabbildung kann explizit beschrieben werden als die Abbildung

$$V \xrightarrow{\sim} \text{Hom}(K, V)$$

gegeben durch  $\vec{v} \mapsto (\cdot\vec{v})$  mit  $(\cdot\vec{v}) : \lambda \mapsto \lambda\vec{v}$ . Im Spezialfall  $V = K^m$  ist für  $\vec{v} \in K^m$  die darstellende Matrix  $[\vec{v}]$  von  $(\cdot\vec{v}) : K \rightarrow K^m$  offensichtlich gerade  $\vec{v}$  selber, aufgefaßt als Spaltenmatrix. Wir notieren diese Spaltenmatrix abkürzend

$$[\vec{v}]$$

oder später auch einfach nur noch  $\vec{v}$ . Ist nun  $f : V \rightarrow W$  linear, so gilt auch ganz allgemein sicher  $f \circ (\cdot\vec{v}) = (\cdot f(\vec{v}))$ , denn diese beiden linearen Abbildungen  $K \rightarrow W$  nehmen auf dem Erzeuger  $1 \in K$  denselben Wert  $f(\vec{v})$  an. Im Spezialfall  $W = K^n$  folgern wir für das Produkt der darstellenden Matrizen aus der vorhergehenden Bemerkung 3.2.4.7 nocheinmal die Identität

$$[f] \circ [\vec{v}] = [f(\vec{v})]$$

von Spaltenvektoren, diesmal aber als Konsequenz unseres Satzes 3.2.4.5 über die Matrix einer Verknüpfung.

*Ergänzung 3.2.4.9.* Gegeben eine Matrix  $A \in \text{Mat}(n \times m; K)$  definiert man die **transponierte Matrix**  $A^\top \in \text{Mat}(m \times n; K)$  durch die Vorschrift  $(A^\top)_{ij} = A_{ji}$ . Anschaulich gesprochen entsteht also  $A^\top$  aus  $A$  durch „Spiegeln an der Hauptdiagonalen“. Zum Beispiel ist die Transponierte eines Spaltenvektors alias einer  $(n \times 1)$ -Matrix ein **Zeilenvektor** alias eine  $(1 \times n)$ -Matrix. Natürlich gilt  $(A^\top)^\top = A$ . Viele Autoren verwenden für die transponierte Matrix auch die alternative Notation  ${}^t A$ .

**3.2.4.10 (Zeilenvektoren versus Spaltenvektoren).** An dieser Stelle will ich kurz auf die Frage eingehen, „ob denn Elemente eines  $K^n$  nun eigentlich Zeilenvektoren oder Spaltenvektoren sein sollen“. A priori sind Elemente eines  $K^n$  halt  $n$ -Tupel und wie wir sie schreiben ist egal. Wenn wir jedoch eine Matrix darvormultiplizieren wollen, ist es wichtig, unsere  $n$ -Tupel als Spaltenvektoren alias Spaltenmatrizen aufzufassen. Da das oft vorkommt, plädiere ich dafür, sich  $n$ -Tupel grundsätzlich als Spalten zu denken. Allerdings ist es in einem durchlaufenden Text ungeschickt, Spaltenvektoren auch als solche zu schreiben. Da fügen

$$\begin{pmatrix} 1 & 4 & 7 & 3 \\ 2 & 2 & 0 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 2 \\ 4 & 2 \\ 7 & 0 \\ 3 & 0 \end{pmatrix}$$

Die transponierte Matrix erhält man durch eine „Spiegelung an der Hauptdiagonalen“.

sich Zeilenvektoren einfach viel besser ein. Wenn ich dennoch auf Spaltenvektoren bestehen will, schreibe ich sie im Text als „zu transponierende Zeilenvektoren“, als da heißt, in der Form  $(x_1, \dots, x_n)^\top$ . Oft schreibe ich aber auch einfach  $(x_1, \dots, x_n)$  und der Leser muß aus dem Kontext erschließen, was genau gemeint ist, wenn es denn darauf überhaupt ankommen sollte.

3.2.4.11. Eine alternative Notation mag besser sein, in der  $(x_1, \dots, x_n)$  im Zweifelsfall einen Spaltenvektor meint und  $(x_1 | \dots | x_n)$  stets einen Zeilenvektor. Im vorliegenden Text wird diese Konvention jedoch nicht durchgehalten.

*Ergänzung 3.2.4.12 (Homomorphismen zwischen direkten Summen).* Gegeben Vektorräume  $V_1, \dots, V_m$  und  $W_1, \dots, W_n$  über einem Körper  $k$  liefern die Identifikationen 3.2.3.12 und 3.2.3.13 zusammen eine natürliche Identifikation

$$\begin{aligned} \text{Hom}(V_1 \oplus \dots \oplus V_m, W_1 \oplus \dots \oplus W_n) &\xrightarrow{\sim} \prod_{i,j} \text{Hom}(V_j, W_i) \\ f &\mapsto (\text{pr}_i \circ f \circ \text{in}_j)_{ij} \end{aligned}$$

Wir werden die Elemente einer endlichen direkten Summe oft als Spaltenvektoren auffassen und die Homomorphismen zwischen direkten Summen als Matrizen von Homomorphismen zwischen den Summanden. So fassen wir ein Element  $(f_{ij})$  des rechten Produkts oben auf als eine Matrix von Homomorphismen, mit  $f_{11}, f_{21}, \dots, f_{n1}$  als erster Spalte,  $f_{12}, f_{22}, \dots, f_{n2}$  als zweiter Spalte und so weiter. Diese Darstellung als Matrix erlaubt es dann, die Komposition solcher Homomorphismen mit dem Formalismus der Matrixmultiplikation zu berechnen: Entspricht genauer einer weiteren linearen Abbildung  $g : U_1 \oplus \dots \oplus U_l \rightarrow V_1 \oplus \dots \oplus V_m$  die Matrix der  $g_{jk} = \text{pr}_j \circ g \circ \text{in}_k : U_k \rightarrow V_j$ , so entspricht der Verknüpfung  $f \circ g$  die Matrix mit Einträgen

$$\left( \sum_j f_{ij} \circ g_{jk} \right) : U_k \rightarrow W_i$$

Sind speziell alle unsere Vektorräume irgendwelche  $k^a$ , so erhalten wir insbesondere, daß das Produkt zweier multiplizierbarer Matrizen auch berechnet werden kann, indem man sie „in verträglicher Weise“ als Blockmatrizen auffaßt und dann diese Blockmatrizen nach den Regeln der Matrixmultiplikation „multipliziert, als ob die Blöcke Zahlen wären“.

## Übungen

*Übung 3.2.4.13.* Man zeige, daß die Abbildung  $M$  aus 3.2.4.1 sogar ein Vektorraumisomorphismus ist für die Vektorraumstruktur 3.2.3.14 auf dem Raum der Homomorphismen und die Vektorraumstruktur 3.1.2.19 auf der Menge der Matrizen.

*Übung 3.2.4.14.* Sei  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  die Spiegelung  $(x, y) \mapsto (x, -y)$ . Man zeige, daß die linearen Abbildungen  $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  mit der Eigenschaft  $fg = gf$  einen Untervektorraum des Homomorphismenraums  $\text{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2)$  bilden und gebe eine Basis dieses Untervektorraums des Homomorphismenraums an.

*Übung 3.2.4.15.* Man zeige für das Produkt transponierter Matrizen die Formel

$$(AB)^\top = B^\top A^\top$$

### 3.2.5 Eigenschaften von Matrizen

3.2.5.1. Eine Matrix mit gleichviel Zeilen wie Spalten heißt **quadratisch**. Für jedes  $n \in \mathbb{N}$  bilden die zugehörigen quadratischen Matrizen mit der Matrixmultiplikation als Verknüpfung ein Monoid, das wir abkürzend

$$\text{Mat}(n; K) := \text{Mat}(n \times n; K)$$

notieren. Die invertierbaren Elemente dieses Monoids heißen die **invertierbaren** oder gleichbedeutend auch die **regulären**  $(n \times n)$ -**Matrizen**. In Formeln heißt eine quadratische Matrix  $A \in \text{Mat}(n; K)$  also invertierbar, wenn es eine Matrix  $B \in \text{Mat}(n; K)$  gibt mit  $AB = I = BA$ . Diese Matrix  $B$  heißt dann auch ihre **Inverse**. Im Einklang mit unseren allgemeinen Konventionen für multiplikativ notierte Monoide notieren wir diese Matrix  $A^{-1}$  und nennen sie die **inverse Matrix zu A**. Die invertierbaren  $(n \times n)$ -Matrizen mit Einträgen in einem Körper  $K$  bilden mit der Matrixmultiplikation eine Gruppe, die **allgemeine lineare Gruppe der  $(n \times n)$ -Matrizen**, die man notiert als

$$\text{GL}(n; K) := \text{Mat}(n; K)^\times$$

in Anlehnung an die englische Bezeichnung **general linear group**.

**Lemma 3.2.5.2 (Invertierbarkeit a priori nicht quadratischer Matrizen).** *Sei  $K$  ein Körper und  $A \in \text{Mat}(m \times n; K)$  eine nicht notwendig quadratische Matrix.*

1. *Gilt  $n \geq m$  und gibt es  $B \in \text{Mat}(n \times m; K)$  mit  $BA = I$ , so gilt  $n = m$  und  $A$  ist invertierbar;*
2. *Gilt  $n \leq m$  und gibt es  $B \in \text{Mat}(n \times m; K)$  mit  $AB = I$ , so gilt  $n = m$  und  $A$  ist invertierbar.*

*Beweis.* Gibt es  $B$  mit  $BA = I$ , so ist die durch  $BA$  gegebene lineare Abbildung injektiv, also ist die durch  $A$  gegebene lineare Abbildung injektiv, also ist sie unter der Annahme  $n \geq m$  nach Dimensionsvergleich ein Isomorphismus. Gibt es  $B$  mit  $AB = I$ , so ist die durch  $AB$  gegebene lineare Abbildung surjektiv, also ist die durch  $A$  gegebene lineare Abbildung surjektiv, also ist sie unter der Annahme  $n \leq m$  nach Dimensionsvergleich ein Isomorphismus.  $\square$

3.2.5.3 (Lineare Gleichungssysteme und Matrixalgebra). Ein lineares Gleichungssystem

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m &= b_2 \\ \vdots &\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m &= b_n \end{aligned}$$

können wir in unseren neuen Notationen zur Gleichung von Spaltenvektoren

$$Ax = b$$

abkürzen, wobei links das Produkt der Koeffizientenmatrix  $A$  mit dem Spaltenvektor  $x$  gemeint ist. Gesucht ist das Urbild von  $b \in K^n$  unter der linearen Abbildung  $(A \circ) : K^m \rightarrow K^n$ . Die Lösung des homogenisierten Systems ist genau der Kern dieser linearen Abbildung, und die Erkenntnis 3.1.1.13, nach der die allgemeine Lösung eines inhomogenen Systems die Summe einer speziellen Lösung des inhomogenen Systems mit einer allgemeinen Lösung des homogenisierten Systems ist, erweist sich als ein Spezialfall der Beschreibung 3.3.2.14 der Fasern linearer Abbildungen. Die Operationen des Gauß-Algorithmus können wir in diesem Rahmen wie folgt interpretieren: Bezeichnet

$$E_{ij}$$

die **Basismatrix** mit dem Eintrag Eins in der  $i$ -ten Zeile und  $j$ -ten Spalte und Nullen sonst, so kann für  $i \neq j$  das Gleichungssystem, das durch Addition des  $\lambda$ -fachen der  $j$ -ten Zeile zur  $i$ -ten Zeile entsteht, in Matrixschreibweise dargestellt werden als

$$(I + \lambda E_{ij})Ax = (I + \lambda E_{ij})b$$

Wegen  $(I - \lambda E_{ij})(I + \lambda E_{ij}) = I$  hat es offensichtlich dieselbe Lösungsmenge wie das ursprüngliche System. Bezeichnet weiter  $P_{ij}$  für  $i \neq j$  die Matrix zu der linearen Abbildung  $K^m \xrightarrow{\sim} K^m$ , die die  $i$ -te Koordinate mit der  $j$ -ten Koordinate vertauscht und sonst alles so lässt wie es ist, so kann das Gleichungssystem, das durch Vertauschen der  $i$ -ten Zeile mit der  $j$ -ten Zeile entsteht, in Matrixschreibweise dargestellt werden als

$$P_{ij}Ax = P_{ij}b$$

Wegen  $P_{ij}P_{ij} = I$  hat es offensichtlich dieselbe Lösungsmenge wie das ursprüngliche System.

3.2.5.4. Man lasse sich durch die terminologische Inkohärenz nicht verwirren:  $E_{ij}$  und  $P_{ij}$  sind an dieser Stelle Matrizen, nicht wie vorher Einträge von Matrizen.

3.2.5.5. Unter einer **Elementarmatrix** verstehen wir eine quadratische Matrix, die sich in höchstens einem Eintrag von der Einheitsmatrix unterscheidet. Mit Ausnahme der Matrizen, die entstehen, wenn man in der Einheitsmatrix eine Eins durch eine Null ersetzt, sind alle Elementarmatrizen mit Einträgen in einem Körper invertierbar.

*Ergänzung 3.2.5.6 (Diskussion der Terminologie).* Es herrscht in der Literatur keine Einigkeit in der Frage, was man genau unter einer Elementarmatrix zu verstehen hat. Manche Quellen bezeichnen zusätzlich zu unseren Elementarmatrizen auch noch die Permutationsmatrizen  $P_{ij}$  als Elementarmatrizen, andere Quellen insbesondere im Zusammenhang mit der sogenannten „K-Theorie“ hinwiederum lassen nur solche Matrizen zu, die sich von der Einheitsmatrix in höchstens einem Eintrag außerhalb der Diagonale unterscheiden. Ich schlage vor, diese letzteren Matrizen **spezielle Elementarmatrizen** zu nennen, da sie genau die Elementarmatrizen sind, die zur speziellen linearen Gruppe 4.1.4.5 gehören.

3.2.5.7. Eine Matrix, die nur auf der Diagonalen von Null verschiedene Einträge hat, und zwar erst einige Einsen und danach nur noch Nullen, nennen wir eine Matrix in **Smith-Normalform**.

**Satz 3.2.5.8 (Transformation auf Smith-Normalform).** *Gegeben ein Körper  $K$  und eine Matrix  $A \in \text{Mat}(n \times m; K)$  gibt es invertierbare Matrizen  $P, Q$  derart, daß  $PAQ$  eine Matrix in Smith-Normalform ist.*

*Beweis.* Das folgt unmittelbar aus der anschließenden technischen Variante 3.2.5.9. In 3.2.6.11 geben wir einen noch alternativen eigenständigen Beweis.  $\square$

**Proposition 3.2.5.9 (Transformation auf Smith-Normalform, Variante).** *Gegeben ein Körper  $K$  und eine Matrix  $A \in \text{Mat}(n \times m; K)$  gibt es invertierbare Elementarmatrizen  $S_1, \dots, S_n, T_1, \dots, T_m$  derart, daß  $S_n \dots S_1 A$  Zeilenstufenform hat und  $S_n \dots S_1 A T_1 \dots T_m$  Smith-Normalform.*

*Beweis.* Zunächst einmal beachten wir, daß die Permutationsmatrizen  $P_{ij}$  mit  $i \neq j$  sich als Produkte von Elementarmatrizen schreiben lassen, wir haben etwa

$$P_{ij} = \text{diag}(1, \dots, 1, -1, 1, \dots, 1)(I + E_{ij})(I - E_{ji})(I + E_{ij})$$

Hier soll die  $(-1)$  an der  $j$ -ten Stelle stehen und  $\text{diag}(\lambda_1, \dots, \lambda_n)$  meint die **Diagonalmatrix** mit Einträgen  $a_{ij} = 0$  für  $i \neq j$  und  $a_{ii} = \lambda_i$ . Dann beachte man, daß die Rechtsoperation von Elementarmatrizen das Ausführen von Spaltenoperationen bedeutet. Damit folgt unsere Proposition aus dem Gauß-Algorithmus.  $\square$

**Korollar 3.2.5.10.** *Jede quadratische Matrix mit Einträgen in einem Körper läßt sich als ein Produkt von Elementarmatrizen darstellen.*

$$\left( \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Eine Matrix in Smith-Normalform

*Ergänzung 3.2.5.11.* Der Beweis zeigt sogar, daß es für jedes  $n$  ein  $N$  gibt derart, daß sich jede  $(n \times n)$ -Matrix als ein Produkt von höchstens  $N$  Elementarmatrizen darstellen läßt.

*Beweis.* Nach 3.2.5.9 können wir invertierbare Elementarmatrizen  $S_i, T_j$  finden derart, daß  $S_n \dots S_1 A T_1 \dots T_m$  die Gestalt  $\text{diag}(1, \dots, 1, 0, \dots, 0)$  hat. Die letztere Matrix schreiben wir leicht als Produkt von nun nicht mehr invertierbaren diagonalen Elementarmatrizen, in Formeln etwa  $S_n \dots S_1 A T_1 \dots T_m = D_1 \dots D_r$  und folgern

$$A = S_1^{-1} \dots S_n^{-1} D_1 \dots D_r T_m^{-1} \dots T_1^{-1}$$

□

**3.2.5.12 (Invertieren von Matrizen).** Um die Inverse einer  $(n \times n)$ -Matrix  $A$  zu berechnen, kann man wie folgt vorgehen: Man schreibt die Einheitsmatrix  $I$  daneben und wendet dann auf die  $(n \times 2n)$ -Matrix  $(A|I)$  Zeilenoperationen an, einschließlich des Multiplizierens einer Zeile mit einem von Null verschiedenen Skalar, bis man  $A$  erst in Zeilenstufenform gebracht und dann sogar zur Einheitsmatrix gemacht hat. Dann steht in der rechten Hälfte unserer  $(n \times 2n)$ -Matrix die Inverse zu  $A$ . In der Tat, sind unsere Zeilenumformungen etwa gegeben durch das Davormultiplizieren der Matrizen  $S_1, S_2, \dots, S_t$ , so steht nach diesen Umformungen da

$$(S_t \dots S_2 S_1 A | S_t \dots S_2 S_1 I)$$

und wenn dann gilt  $S_t \dots S_2 S_1 A = I$ , so folgt  $S_t \dots S_2 S_1 I = S_t \dots S_2 S_1 = A^{-1}$ . Dasselbe Verfahren funktioniert auch, wenn wir statt mit Zeilen- mit Spaltenumformungen arbeiten. Es ist nur nicht erlaubt, diese zu mischen, denn aus  $S_t \dots S_1 A T_1 \dots T_r = I$  folgt keineswegs  $S_t \dots S_1 T_1 \dots T_r = A^{-1}$ .

**Definition 3.2.5.13.** Gegeben eine Matrix  $A \in \text{Mat}(n \times m; K)$  heißt die Dimension des von ihren Spaltenvektoren aufgespannten Untervektorraums von  $K^n$  der **Spaltenrang** unserer Matrix. Analog heißt die Dimension des von ihren Zeilenvektoren aufgespannten Untervektorraums von  $K^m$  der **Zeilenrang** unserer Matrix.

**Satz 3.2.5.14.** Für jede Matrix stimmen Zeilenrang und Spaltenrang überein, in Formeln gilt also  $\text{rg}(A) = \text{rg}(A^\top)$ .

**3.2.5.15.** Diese gemeinsame Zahl heißt dann der **Rang** oder auf englisch **rank** unserer Matrix und wird  $\text{rg } A$  notiert. Ist der Rang einer Matrix so groß wie für Matrizen derselben Gestalt möglich, sind also entweder die Spalten oder die Zeilen linear unabhängig, so sagt man, unsere Matrix habe **vollen Rang**.

*Beweis.* Der Spaltenrang einer Matrix  $A \in \text{Mat}(n \times m; K)$  kann interpretiert werden als die Dimension des Bildes von

$$(A \circ) : K^m \rightarrow K^n$$

Diese Interpretation zeigt sofort, daß  $PAQ$  denselben Spaltenrang hat wie  $A$  für beliebige invertierbare Matrizen  $P, Q$ . Durch Transponieren erkennen wir, daß  $PAQ$  auch denselben Zeilenrang hat wie  $A$  für beliebige invertierbare Matrizen  $P, Q$ . Nun finden wir jedoch nach 3.2.5.8 invertierbare Matrizen  $P, Q$  mit  $PAQ$  in Smith-Normalform. Dann stimmen natürlich Zeilenrang und Spaltenrang von  $PAQ$  überein, und dasselbe folgt für unsere ursprüngliche Matrix  $A$ .  $\square$

**Definition 3.2.5.16.** Ganz allgemein nennt man die Dimension des Bildes einer linearen Abbildung auch den **Rang** unserer linearen Abbildung. Dieser Rang kann unendlich sein, es gibt aber auch zwischen unendlichdimensionalen Vektorräumen durchaus Null verschiedene Abbildungen endlichen Ranges.

### Übungen

*Übung 3.2.5.17.* Gegeben lineare Abbildungen  $f : U \rightarrow V$  und  $g : V \rightarrow W$  zeige man, daß der Rang ihrer Verknüpfung  $g \circ f$  sowohl beschränkt ist durch den Rang von  $f$  als auch durch den Rang von  $g$ .

*Übung 3.2.5.18.* Man gebe eine ganzzahlige  $(3 \times 3)$ -Matrix vom Rang Zwei ohne Eintrag Null an, bei der je zwei Spalten linear unabhängig sind.

*Übung 3.2.5.19.* Eine quadratische Block-obere Dreiecksmatrix ist invertierbar genau dann, wenn alle Blöcke auf der Diagonalen invertierbar sind. Hinweis: 3.2.4.12.

*Ergänzende Übung 3.2.5.20.* Die Automorphismengruppe eines zweidimensionalen Vektorraums über einem zweielementigen Körper ist isomorph zur Gruppe der Permutationen von drei Elementen, in Formeln  $\mathrm{GL}(2; \mathbb{F}_2) \cong \mathcal{S}_3$ .

*Ergänzende Übung 3.2.5.21.* Eine quadratische Blockmatrix

$$\begin{pmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{pmatrix}$$

ist invertierbar, wenn  $W_{22}$  und  $W_{11} - W_{12}W_{22}^{-1}W_{21}$  invertierbar sind. Hinweis: Multipliziere von rechts erst mit  $\begin{pmatrix} I & 0 \\ 0 & W_{22}^{-1} \end{pmatrix}$  und dann mit  $\begin{pmatrix} I & 0 \\ -W_{21} & I \end{pmatrix}$ .

*Übung 3.2.5.22.* Sei  $K$  ein Körper und sei  $n$  fest vorgegeben. Gegeben  $i, j \leq n$  mit  $i \neq j$  bilden die speziellen Elementarmatrizen mit von Null verschiedenen Eintrag höchstens in der  $i$ -ten Zeile und  $j$ -ten Spalte eine Untergruppe  $U_{ij} \subset \mathrm{GL}(n; K)$  eine Untergruppe und wir erhalten einen Gruppenisomorphismus  $U_{ij} \xrightarrow{\sim} K$  in die additive Gruppe durch die Vorschrift  $A \mapsto A_{ij}$ .

*Übung 3.2.5.23.* Gegeben ein Körper  $K$  erhält man einen injektiven Monoidhomomorphismus  $\mathcal{S}_n \hookrightarrow \mathrm{Mat}(n; K)$  durch die Vorschrift  $\sigma \mapsto \sum E_{\sigma(i), i}$ . Die Matrizen im Bild dieses Monoidhomomorphismus heißen die **Permutationsmatrizen** und wir notieren sie gerne abkürzend auch  $\sigma$ .

### 3.2.6 Lineare Abbildungen und Matrizen

3.2.6.1. Die im folgenden verwendeten Notationen  ${}_{\mathcal{B}}[v]$  und  ${}_{\mathcal{A}}[f]_{\mathcal{B}}$  habe ich Urs Hartl abgeschaut. Ähnlich wie die geschickt gewählten Steckverbindungen, die man bei Computerzubehör gewohnt ist, sorgen sie dafür, daß man fast nichts mehr falsch machen kann.

**Satz 3.2.6.2 (Abstrakte lineare Abbildungen und Matrizen).** *Seien  $K$  ein Körper und  $V, W$  Vektorräume über  $K$  mit angeordneten Basen  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_m)$  und  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$ . Ordnen wir jeder linearen Abbildung  $f : V \rightarrow W$  die **darstellende Matrix**  ${}_{\mathcal{B}}[f]_{\mathcal{A}}$  zu mit Einträgen  $a_{ij}$ , die durch die Identitäten  $f(\vec{v}_j) = a_{1j}\vec{w}_1 + \dots + a_{nj}\vec{w}_n$  gegeben werden, so erhalten wir eine Bijektion, ja sogar einen Vektorraumisomorphismus*

$$\begin{aligned} M_{\mathcal{B}}^{\mathcal{A}} : \text{Hom}_K(V, W) &\xrightarrow{\sim} \text{Mat}(n \times m; K) \\ f &\mapsto {}_{\mathcal{B}}[f]_{\mathcal{A}} \end{aligned}$$

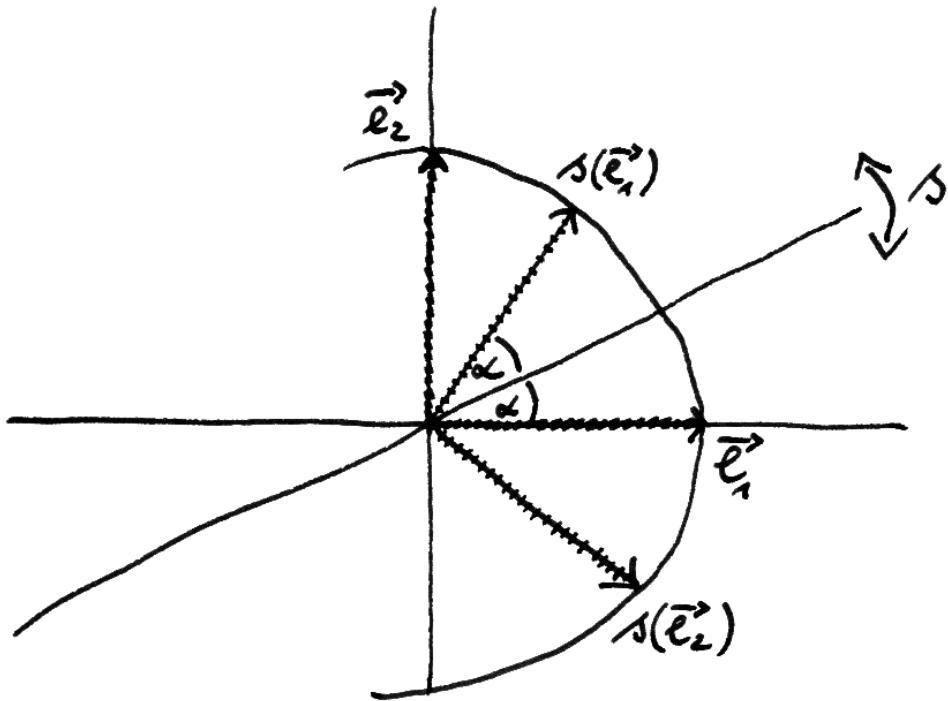
3.2.6.3. Wir nennen  $M_{\mathcal{B}}^{\mathcal{A}}(f) = {}_{\mathcal{B}}[f]_{\mathcal{A}}$  die **darstellende Matrix der Abbildung  $f$  in Bezug auf die Basen  $\mathcal{A}$  und  $\mathcal{B}$** . In Worten ausgedrückt stehen in ihren Spalten die Koordinaten der Bilder der Vektoren der Basis  $\mathcal{A}$  des Ausgangsraums in Bezug auf die Basis  $\mathcal{B}$  des Zielraums. Beliebt ist statt  ${}_{\mathcal{B}}[f]_{\mathcal{A}}$  und  $M_{\mathcal{B}}^{\mathcal{A}}(f)$  auch die ausführlichere Notation  $\text{Mat}_{\mathcal{B}}^{\mathcal{A}}(f)$ . Die Matrix einer linearen Abbildung  $f : K^m \rightarrow K^n$  in Bezug auf die jeweiligen Standardbasen  $\mathcal{S}(m), \mathcal{S}(n)$  nach 3.1.6.11 ist genau unsere darstellende Matrix  $[f]$  aus 3.2.4.1, in Formeln gilt also

$$[f] = {}_{\mathcal{S}(n)}[f]_{\mathcal{S}(m)}$$

Wir vereinbaren allgemeiner, daß wir bei unserer Notation Standardbasen hinfert auch weglassen dürfen. Für eine lineare Abbildung  $f : K^m \rightarrow W$  schreiben wir also abkürzend  ${}_{\mathcal{B}}[f]_{\mathcal{S}(m)} = {}_{\mathcal{B}}[f]$  und für eine lineare Abbildung  $f : V \rightarrow K^n$  entsprechend  ${}_{\mathcal{S}(n)}[f]_{\mathcal{A}} = [f]_{\mathcal{A}}$ .

*Ergänzung 3.2.6.4.* Wenn wir die Matrixmultiplikation in der offensichtlichen Weise erweitern zur Definition des Produkts einer Matrix mit einer Spaltenmatrix von Vektoren, so können wir die definierende Gleichung der darstellenden Matrix  $M = {}_{\mathcal{B}}[f]_{\mathcal{A}}$  auch schreiben in der Form

$$\begin{pmatrix} f(\vec{v}_1) \\ \vdots \\ f(\vec{v}_m) \end{pmatrix} = M^{\top} \begin{pmatrix} \vec{w}_1 \\ \vdots \\ \vec{w}_n \end{pmatrix}$$



Die Matrix der anschaulichen Spiegelung  $s : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  an einer Gerade mit dem Winkel  $\alpha$  zur  $x$ -Achse hat die Gestalt

$$[s] = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

mit den Bildern der Vektoren der Standardbasis in den Spalten. Zum Beispiel hat  $s(\vec{e}_1)$  die  $x$ -Koordinate  $\cos 2\alpha$  und die  $y$ -Koordinate  $\sin 2\alpha$  und das erklärt bereits die erste Spalte unserer Matrix. Bei  $s(\vec{e}_2)$  scheint mir einsichtig, daß die  $x$ -Koordinate von  $s(\vec{e}_2)$  die  $y$ -Koordinate von  $s(\vec{e}_1)$  ist und die  $y$ -Koordinate von  $s(\vec{e}_2)$  das Negative der  $x$ -Koordinate von  $s(\vec{e}_1)$ . Das erklärt dann auch die zweite Spalte unserer Matrix.

*Beweis.* Wir könnten hier eine Variation unseres Beweises von 3.2.4.5 ein weiteres Mal ausschreiben, aber stattdessen erinnern wir einfacher unsere Isomorphismen  $\Phi_{\mathcal{A}} : K^m \xrightarrow{\sim} V$  und  $\Phi_{\mathcal{B}} : K^n \xrightarrow{\sim} W$  aus 3.1.6.13 und beachten, daß unsere Definition der darstellenden Matrix gleichbedeutend ist zur Identität

$${}_{\mathcal{B}}[f]_{\mathcal{A}} = [\Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}}]$$

Damit können wir unsere Abbildung dann schreiben als die Komposition von Bijektionen

$$\begin{aligned} \text{Hom}_K(V, W) &\xrightarrow{\sim} \text{Hom}_K(K^m, K^n) \xrightarrow{\sim} \text{Mat}(n \times m; K) \\ f &\mapsto \Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}} \end{aligned}$$

mit unserer Abbildung :  $g \mapsto [g]$  aus 3.2.4.1 rechts, die eben jeder Abbildung  $g : K^m \rightarrow K^n$  ihre darstellende Matrix zuordnet.  $\square$

**Satz 3.2.6.5 (Darstellende Matrix einer Verknüpfung).** *Gegeben ein Körper  $K$  und  $K$ -Vektorräume  $U, V, W$  endlicher Dimension mit angeordneten Basen  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  und lineare Abbildungen  $f : U \rightarrow V$  und  $g : V \rightarrow W$  ist die darstellende Matrix der Verknüpfung das Produkt der darstellenden Matrizen, in Formeln*

$$c[g \circ f]_{\mathcal{A}} = c[g]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}}$$

*Erster Beweis.* Wir können die Behauptung nach Erinnern aller Notationen umschreiben zu  $[\Phi_{\mathcal{C}}^{-1} g f \Phi_{\mathcal{A}}] = [\Phi_{\mathcal{C}}^{-1} g \Phi_{\mathcal{B}}] \circ [\Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}}]$ , und in dieser Form folgt sie offensichtlich aus dem in 3.2.4.5 behandelten Spezialfall.  $\square$

*Zweiter Beweis.* Wir könnten auch expliziter vorgehen und den Beweis von 3.2.4.5 nocheinmal wiederholen mit der alternativen Interpretation von  $\vec{u}_i, \vec{v}_j$  und  $\vec{w}_k$  als den Vektoren unserer angeordneten Basen  $\mathcal{A}, \mathcal{B}, \mathcal{C}$ .  $\square$

**Definition 3.2.6.6.** Gegeben ein endlichdimensionaler Vektorraum  $V$  mit einer angeordneten Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  notieren wir die Inverse unserer Bijektion  $\Phi_{\mathcal{A}} : K^n \xrightarrow{\sim} V$ ,  $(\lambda_1, \dots, \lambda_n)^{\top} \mapsto \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$  in der Form

$$\vec{v} \mapsto {}_{\mathcal{A}}[\vec{v}]$$

Der Spaltenvektor  ${}_{\mathcal{A}}[\vec{v}]$  heißt die **Darstellung des Vektors  $\vec{v}$  in der Basis  $\mathcal{A}$** .

**Satz 3.2.6.7 (Darstellung des Bildes eines Vektors).** *Gegeben endlichdimensionale Räume  $V, W$  mit angeordneten Basen  $\mathcal{A}, \mathcal{B}$  und eine lineare Abbildung  $f : V \rightarrow W$  gilt für jeden Vektor  $v \in V$  die Identität*

$${}_{\mathcal{B}}[f(v)] = {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[v]$$

*Beweis.* Hier wird bei genauerer Betrachtung nur die Gleichheit von Spaltenvektoren  $[\Phi_B^{-1}(f(v))] = [(\Phi_B^{-1} f \Phi_A)] \circ [\Phi_A^{-1} v]$  behauptet, die aus 3.2.4.7 folgt.  $\square$

*Ergänzung 3.2.6.8.* Betrachtet man zu einem beliebigen Vektor  $v \in V$  die lineare Abbildung  $(\cdot v) : K \rightarrow V$ ,  $\lambda \mapsto \lambda v$ , und bezeichnet mit  $\mathcal{S}(1)$  die Standardbasis  $(1) = (e_1)$  des  $K$ -Vektorraums  $K$ , die wir ja eh aus der Notation weglassen wollten, so ergibt sich die Identität  ${}_{\mathcal{A}}[v] = {}_{\mathcal{A}}[\cdot v]_{\mathcal{S}(1)}$ . Wegen  $(\cdot f(v)) = f \circ (\cdot v)$  können wir damit den vorhergehenden Satz 3.2.6.7 auch auffassen als den Spezialfall  ${}_{\mathcal{B}}[\cdot f(v)]_{\mathcal{S}(1)} = {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\cdot v]_{\mathcal{S}(1)}$  von Satz 3.2.6.5 über die darstellende Matrix einer Verknüpfung.

**Definition 3.2.6.9.** Gegeben zwei angeordnete Basen  $\mathcal{A} = (v_1, \dots, v_n)$  und  $\mathcal{B} = (w_1, \dots, w_n)$  eines Vektorraums  $V$  nennt man die darstellende Matrix der Identität

$${}_{\mathcal{B}}[\text{id}_V]_{\mathcal{A}}$$

in diesen Basen die **Basiswechselmatrix**. Ihre Einträge  $a_{ij}$  werden per Definition gegeben durch die Gleichungen  $v_j = \sum_{i=1}^n a_{ij} w_i$ .

**3.2.6.10 (Änderung der darstellenden Matrix bei Basiswechsel).** Offensichtlich ist  ${}_{\mathcal{A}}[\text{id}]_{\mathcal{A}} = I$  die Einheitsmatrix. Nach 3.2.6.5 ist damit die Basiswechselmatrix  ${}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}$  invers zur Basiswechselmatrix in der Gegenrichtung  ${}_{\mathcal{B}}[\text{id}]_{\mathcal{A}}$ , in Formeln  ${}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}^{-1} = {}_{\mathcal{B}}[\text{id}]_{\mathcal{A}}$ . Haben wir nun eine lineare Abbildung  $f : V \rightarrow W$  und angeordnete Basen  $\mathcal{A}, \mathcal{B}$  von  $V$  und angeordnete Basen  $\mathcal{C}, \mathcal{D}$  von  $W$ , so folgt aus 3.2.6.5 die Identität  ${}_{\mathcal{D}}[f]_{\mathcal{B}} = {}_{\mathcal{D}}[\text{id}_W]_{\mathcal{C}} \circ {}_{\mathcal{C}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\text{id}_V]_{\mathcal{B}}$ . Sind noch spezieller  $\mathcal{A}, \mathcal{B}$  zwei angeordnete Basen ein- und desselben Vektorraums  $V$  und ist  $f : V \rightarrow V$  ein Endomorphismus von  $V$ , so erhalten wir unmittelbar die Identität  ${}_{\mathcal{B}}[f]_{\mathcal{B}} = {}_{\mathcal{B}}[\text{id}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}$  alias

$$N = T^{-1}MT$$

für  $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}$  und  $M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$  die darstellenden Matrizen bezüglich unserer beiden Basen und  $T = {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}$  die Basiswechselmatrix.

**Satz 3.2.6.11 (Smith-Normalform).** *Gegeben eine lineare Abbildung zwischen endlichdimensionalen Vektorräumen  $f : V \rightarrow W$  existieren stets angeordnete Basen  $\mathcal{A}$  von  $V$  und  $\mathcal{B}$  von  $W$  derart, daß die darstellende Matrix  ${}_{\mathcal{B}}[f]_{\mathcal{A}}$  nur auf der Diagonale von Null verschiedene Einträge hat, und zwar erst einige Einsen und danach nur noch Nullen.*

*Beweis.* Das folgt sofort aus 3.2.2.6: Wir wählen zunächst eine angeordnete Basis  $(w_1, \dots, w_r)$  des Bildes von  $f$ , dazu Urbilder  $v_1, \dots, v_r$  in  $V$ , ergänzen diese durch eine angeordnete Basis des Kerns von  $f$  zu einer angeordneten Basis  $\mathcal{A} = (v_1, \dots, v_n)$  von  $V$ , und ergänzen unsere angeordnete Basis des Bildes zu einer angeordneten Basis  $\mathcal{B} = (w_1, \dots, w_m)$  von  $W$ . In diesen Basen hat dann die Matrix von  $f$  offensichtlich die behauptete Gestalt.  $\square$

**Definition 3.2.6.12.** Die **Spur** einer endlichen quadratischen Matrix ist definiert als die Summe ihrer Diagonaleinträge. Auf englisch und französisch sagt man **trace**, und ich werde die Spur einer Matrix  $A$  notieren als

$$\mathrm{tr}(A)$$

*Vorschau 3.2.6.13.* Eine vielleicht natürlichere Definition der Spur wird in 4.6.1.46 erklärt. Im Rahmen der Analysis werden wir die Spur in ?? als das Differential der Determinante an der Einheitsmatrix wiedersehen.

## Übungen

*Übung 3.2.6.14.* Gegeben ein  $K$ -Vektorraum  $V$  mit einer angeordneten Basis  $\mathcal{A} = (v_1, \dots, v_n)$  liefert die Zuordnung, die jeder weiteren angeordneten Basis  $\mathcal{B}$  die Basiswechselmatrix von  $\mathcal{A}$  nach  $\mathcal{B}$  zuordnet, eine Bijektion

$$\begin{aligned} \{\text{angeordnete Basen von } V\} &\xrightarrow{\sim} \mathrm{GL}(n; K) \\ \mathcal{B} &\mapsto {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \end{aligned}$$

*Ergänzende Übung 3.2.6.15.* Ein Endomorphismus  $f : V \rightarrow V$  eines Vektorraums heißt **nilpotent**, wenn es  $d \in \mathbb{N}$  gibt mit  $f^d = 0$ . Sei  $f : V \rightarrow V$  ein nilpotenter Endomorphismus eines endlichdimensionalen Vektorraums. Man zeige, daß unser Vektorraum eine angeordnete Basis  $\mathcal{B}$  besitzt derart, daß die Matrix  ${}_{\mathcal{B}}[f]_{\mathcal{B}}$  von  $f$  in Bezug auf diese Basis eine obere Dreiecksmatrix ist mit Nullen auf der Diagonalen. Man zeige umgekehrt auch, daß für jede derartige  $(n \times n)$ -Matrix  $D$  gilt  $D^{n-1} = 0$ . Hinweis: Man betrachte die Teilräume  $\ker(f) \subset \dots \subset \ker(f^{d-1}) \subset \ker(f^d) = V$ , beginne mit einer Basis von  $\ker(f)$  und ergänze sie sukzessive zu einer Basis von  $V$ . Eine stärkere Aussage in dieser Richtung werden wir als 4.3.4.2 zeigen.

*Übung 3.2.6.16.* Man zeige  $\mathrm{tr}(AB) = \mathrm{tr}(BA)$  wann immer  $A$  eine  $(m \times n)$ -Matrix ist und  $B$  eine  $(n \times m)$ -Matrix. Man folgere daraus weiter die Identität  $\mathrm{tr}(BAB^{-1}) = \mathrm{tr}(A)$  wann immer  $A$  eine  $(n \times n)$ -Matrix ist und  $B$  eine invertierbare  $(n \times n)$ -Matrix. Insbesondere kann man jedem Endomorphismus  $f$  eines endlichdimensionalen Vektorraums  $V$  über einem Körper  $K$  seine **Spur**

$$\mathrm{tr}(f) = \mathrm{tr}(f|V) = \mathrm{tr}_K(f|V)$$

zuordnen als die Spur seiner Matrix in Bezug auf eine und jede Basis. Gegeben endlichdimensionale Vektorräume  $V, W$  und lineare Abbildungen  $f : V \rightarrow W$  und  $g : W \rightarrow V$  zeige man auch  $\mathrm{tr}(fg) = \mathrm{tr}(gf)$ .

*Ergänzende Übung 3.2.6.17.* Leser, die schon mit dem Inhalt des Abschnitts 3.2.7 über komplexe Zahlen vertraut sind, mögen zeigen: Ist  $f : V \rightarrow V$  ein Endomorphismus eines endlichdimensionalen  $\mathbb{C}$ -Vektorraums, so gilt für seine Spur auf dem zugrundeliegenden reellen Vektorraum  $\text{tr}_{\mathbb{R}}(f|V) = 2 \operatorname{Re} \text{tr}_{\mathbb{C}}(f|V)$ .

*Ergänzende Übung 3.2.6.18.* Ist  $L$  ein endlichdimensionaler  $K$ -Vektorraum und  $A : L \rightarrow L$  eine  $K$ -lineare Abbildung, so gilt

$$\text{tr}((A \circ)| \operatorname{End}_K L) = (\dim_K L) \text{tr}(A|L)$$

*Ergänzung 3.2.6.19.* Gegeben ein Endomorphismus  $f$  von endlichem Rang eines Vektorraums  $V$  erklärt man die **Spur**

$$\text{tr } f = \text{tr}(f|V)$$

von  $f$  als die Spur der Verknüpfung  $\imath : f \hookrightarrow V \rightarrow \operatorname{im} f$  im Sinne unserer Definition 3.2.6.16 für die Spur eines Endomorphismus eines endlichdimensionalen Vektorraums. Aus 3.2.6.16 folgt unmittelbar, daß diese Definition im Fall eines endlichdimensionalen Raums  $V$  dieselbe Spur liefert wie unsere ursprüngliche auf den endlichdimensionalen Fall beschränkte Definition 3.2.6.12.

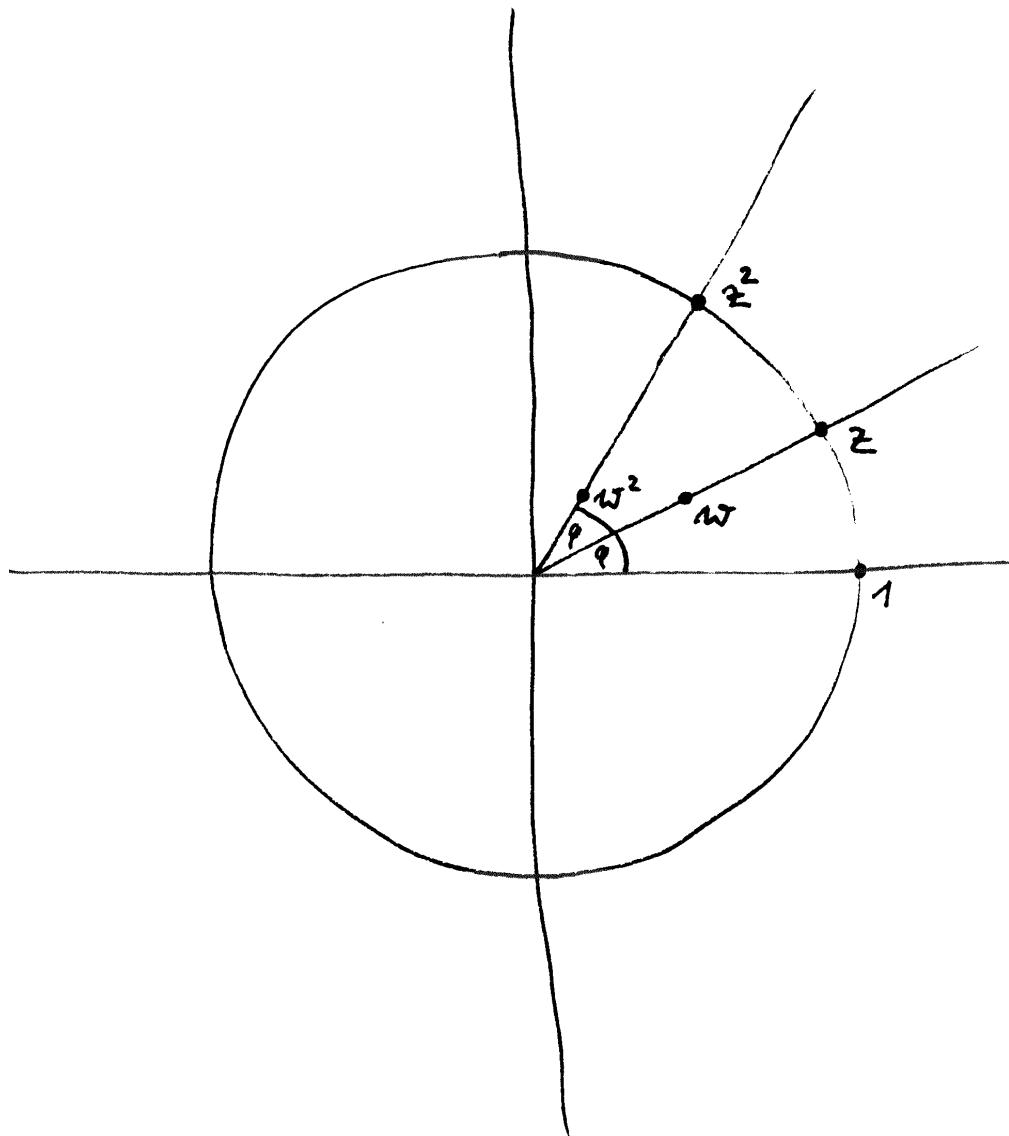
*Ergänzende Übung 3.2.6.20.* Sind  $V, W$  Vektorräume und  $f : V \rightarrow W$  sowie  $g : W \rightarrow V$  lineare Abbildungen und ist eine unserer Abbildungen von endlichem Rang, so gilt  $\text{tr}(fg) = \text{tr}(gf)$ . Hinweis: Der endlichdimensionale Fall kann nach 3.2.6.16 vorausgesetzt werden.

*Ergänzende Übung 3.2.6.21.* Gegeben ein Endomorphismus  $f$  von endlichem Rang eines Vektorraums mit der Eigenschaft  $f^2 = af$  für ein Element  $a$  des Grundkörpers gilt stets  $\text{tr}(f) = a \dim(\operatorname{im} f)$ . Hinweis: 3.2.2.19.

*Übung 3.2.6.22.* Man finde alle Matrizen  $A \in \operatorname{Mat}(2; \mathbb{R})$  mit  $A \circ A = I$  der Einheitsmatrix und beschreibe geometrisch die linearen Abbildungen, die durch diese Matrizen  $A$  beschrieben werden.

### 3.2.7 Komplexe Zahlen

3.2.7.1. Viele mathematische Zusammenhänge werden bei einer Behandlung im Rahmen der sogenannten „komplexen Zahlen“ besonders transparent. Ich denke hier etwa an die Integration rationaler Funktionen ??, die Normalform orthogonaler Matrizen 4.1.11.3 oder die Lösung der Schwingungsgleichung ???. Die abschreckenden Bezeichnungen „komplexe Zahlen“ oder auch „imaginäre Zahlen“ für diesen ebenso einfachen wie konkreten Körper haben historische Gründe: Als Mathematiker in Italien bemerkten, daß man polynomiale Gleichungen der Grade Drei und Vier lösen kann, wenn man so tut, als ob man aus  $(-1)$  eine Quadratwurzel ziehen könnte, gab es noch keine Mengenlehre und erst recht nicht



Anschauung für das Quadrieren komplexer Zahlen in ihrer anschaulichen  
Interpretation als Punkte der komplexen Zahlenebene

den abstrakten Begriff eines Körpers 2.2.4.2. Das Rechnen mit Zahlen, die keine konkreten Interpretationen als Länge oder Guthaben oder zumindest als Schulden haben, schien eine „imaginäre“ Angelegenheit, ein bloßer Trick, um zu reellen Lösungen reeller Gleichungen zu kommen.

3.2.7.2. In diesem Abschnitt werden die komplexen Zahlen nur als algebraische Struktur diskutiert. Für die Diskussion der analytischen Aspekte, insbesondere die komplexe Exponentialfunktion und ihre Beziehung zu den trigonometrischen Funktionen, verweise ich auf die Analysis, insbesondere auf ?? . Die hier gegebene Konstruktion der komplexen Zahlen als Menge aller Matrizen zu Drehstreckungen der Ebene paßt unter didaktischen Aspekten gut hierher, weil gleichzeitig der Zusammenhang zwischen Matrizen und linearen Abbildungen angewandt und eingeübt werden kann.

**Satz 3.2.7.3 (Charakterisierung der komplexen Zahlen).** 1. Es gibt Tripel

$$(\mathbb{C}, i, \kappa)$$

bestehend aus einem Körper  $\mathbb{C}$ , einem Element  $i \in \mathbb{C}$  und einem Körperhomomorphismus  $\kappa : \mathbb{R} \rightarrow \mathbb{C}$  derart, daß gilt  $i^2 = -1$  und daß  $i$  und  $1$  eine  $\mathbb{R}$ -Basis von  $\mathbb{C}$  bilden in Bezug auf die durch  $\mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}$ ,  $(a, z) \mapsto \kappa(a)z$  auf  $\mathbb{C}$  gegebene Struktur als  $\mathbb{R}$ -Vektorraum;

2. Derartige Tripel sind eindeutig bis auf eindeutigen Isomorphismus. Ist genauer  $(\mathbb{C}', i', \kappa')$  ein weiteres derartiges Tripel, so gibt es genau einen Körperhomomorphismus  $\varphi : \mathbb{C} \xrightarrow{\sim} \mathbb{C}'$  mit  $\varphi : i \mapsto i'$  und  $\varphi \circ \kappa = \kappa'$  und der ist stets ein Isomorphismus.

**Definition 3.2.7.4.** Wir wählen für den weiteren Verlauf der Vorlesung ein festes Tripel  $(\mathbb{C}, i, \kappa)$  der im Satz beschriebenen Art. Wegen der im zweiten Teil des Satzes formulierten „Eindeutigkeit bis auf eindeutigen Isomorphismus“ erlauben wir uns den bestimmten Artikel und nennen  $\mathbb{C}$  den **Körper der komplexen Zahlen**. Weiter kürzen wir für reelle Zahlen  $a \in \mathbb{R}$  stets  $\kappa(a) = a$  ab und gehen sogar so weit, die reellen Zahlen mittels  $\kappa$  als Teilmenge von  $\mathbb{C}$  aufzufassen.

**Ergänzung 3.2.7.5 (Zur Eindeutigkeit der komplexen Zahlen).** Man beachte, daß  $\mathbb{C}$  als Körper ohne weitere Daten im Gegensatz zum Körper der reellen Zahlen ?? keineswegs eindeutig ist bis auf eindeutigen Isomorphismus. Genauer gibt es überabzählbar viele Körperisomorphismen  $\mathbb{C} \xrightarrow{\sim} \mathbb{C}$ , überabzählbar viele nicht-bijektive Körperhomomorphismen  $\mathbb{C} \rightarrow \mathbb{C}$  und auch überabzählbar viele Körperhomomorphismen  $\mathbb{R} \rightarrow \mathbb{C}$ , wie etwa in ?? ausgeführt wird. Zeichnet man jedoch einen Körperhomomorphismus  $\kappa : \mathbb{R} \rightarrow \mathbb{C}$  aus derart, daß  $\mathbb{C}$  darunter zu einem endlichdimensionalem  $\mathbb{R}$ -Vektorraum wird, und versieht  $\mathbb{C}$  mit der dazugehörigen

„natürlichen Topologie“ im Sinne von ??, so wird  $\kappa$  seinerseits durch diese Topologie festgelegt als der einzige im Sinne von ?? „stetige“ Körperhomomorphismen  $\mathbb{R} \rightarrow \mathbb{C}$ , und es gibt in Bezug auf unsere Topologie nur genau zwei „stetige“ Körperhomomorphismen  $\mathbb{C} \rightarrow \mathbb{C}$ , die Identität und die sogenannte „komplexe Konjugation“, die wir demnächst kennenlernen werden.

3.2.7.6. Ich hoffe, Sie werden schnell merken, daß sich viele Fragestellungen bei Verwendung dieser sogenannten komplexen Zahlen sehr viel leichter lösen lassen und daß die komplexen Zahlen auch der Anschauung ebenso zugänglich sind wie die reellen Zahlen. Früher schrieb man „complex“, deshalb die Bezeichnung  $\mathbb{C}$ . Unser  $i$  ist eine „Wurzel aus  $(-1)$ “, und weil es so eine Wurzel in den reellen Zahlen nicht geben kann, notiert man sie  $i$  wie „imaginär“.

*Ergänzung 3.2.7.7.* Für feinere Untersuchungen finde ich es praktisch, auch Paare  $(K, \kappa)$  zu betrachten, die aus einem Körper  $K$  nebst einem Körperhomomorphismus  $\kappa : \mathbb{R} \rightarrow K$  bestehen derart, daß es einen Körperisomorphismus  $a : K \xrightarrow{\sim} \mathbb{C}$  gibt, der mit den vorgegebenen Einbettungen von  $\mathbb{R}$  verträglich ist. Auch bei solch einem Paar notiere ich den Körper  $K$  gerne  $\mathbb{C}$  und fasse die Einbettung von  $\mathbb{R}$  als Einbettung einer Teilmenge auf und notiere sie nicht. Ich rede dann von einem Körper von **vergeblichen komplexen Zahlen**, da es sich dabei salopp gesprochen um eine „Kopie von  $\mathbb{C}$ “ handelt, die vergessen hat, welche ihrer beiden Wurzeln von  $(-1)$  sie als  $i$  auszeichnen wollte“.

*Beweis.* Wir beginnen mit der Eindeutigkeit. Jedes Element  $z \in \mathbb{C}$  läßt sich ja nach Annahme und mit der Abkürzung  $\kappa(x) = x$  eindeutig schreiben in der Form  $z = a + bi$  mit  $a, b \in \mathbb{R}$ . Die Addition und Multiplikation in  $\mathbb{C}$  haben in dieser Notation die Gestalt

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i\end{aligned}$$

Damit ist auch bereits die im zweiten Teil formulierte Eindeutigkeitsaussage gezeigt. Natürlich kann man auch die Existenz direkt anhand dieser Rechenregeln prüfen. So gewinnt man an Unabhängigkeit von der linearen Algebra, verliert aber an Anschauung und muß die Körperaxiome ohne Einsicht nachrechnen. Das sollten Sie bereits als Übung 2.2.4.14 durchgeführt haben. Alternativ kann man die im ersten Teil behauptete Existenz mit mehr Kenntnissen in linearer Algebra und weniger Rechnung auch einsehen, wie es im folgenden ausgeführt werden soll. Man betrachtet dazu die Menge  $\mathbb{C}$  aller reellen  $(2 \times 2)$ -Matrizen der Gestalt

$$\mathbb{C} := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subset \text{Mat}(2; \mathbb{R})$$

Anschaulich gesagt sind das genau die Matrizen zu Drehstreckungen der Ebene, die den Ursprung festhalten. Die Addition und Multiplikation von Matrizen induzieren offensichtlich eine Addition und Multiplikation auf  $\mathbb{C}$ , man prüft mühelos die Körperaxiome 2.2.4.2 und erhält so einen Körper  $\mathbb{C}$ . Die Drehung um einen rechten Winkel oder vielmehr ihre Matrix

$$i := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

hat natürlich die Eigenschaft  $i^2 = -1$ , und die Abbildung  $\kappa : \mathbb{R} \rightarrow \mathbb{C}$  gegeben durch  $\kappa : a \mapsto \text{diag}(a, a)$  ist ein Körperhomomorphismus derart, daß das Tripel  $(\mathbb{C}, i, \kappa)$  die geforderten Eigenschaften besitzt.  $\square$

3.2.7.8. Es ist allgemein üblich, komplexe Zahlen mit  $z$  zu bezeichnen und als  $z = x + y i$  zu schreiben mit  $x, y \in \mathbb{R}$ . Man mag sich die komplexe Zahl  $z = x + y i$  vorstellen als den Punkt  $(x, y)$  der Koordinatenebene  $\mathbb{R}^2$ . Wenn wir diese Vorstellung evozieren wollen, reden wir von der **komplexen Zahlenebene**. Unter dieser Identifikation von  $\mathbb{C}$  mit  $\mathbb{R}^2$  bedeutet für  $w \in \mathbb{C}$  die Additionsabbildung  $(w+) : \mathbb{C} \rightarrow \mathbb{C}$ ,  $z \mapsto w + z$  anschaulich die Verschiebung um den Vektor  $w$ . Die Multiplikationsabbildung  $(w \cdot) : \mathbb{C} \rightarrow \mathbb{C}$ ,  $z \mapsto wz$  dahingegen bedeutet anschaulich diejenige Drehstreckung, die  $(1, 0)$  in  $w$  überführt.

3.2.7.9. Gegeben eine komplexe Zahl  $z = x + y i$  nennt man  $x$  ihren **Realteil**  $\text{Re } z := x$  und  $y$  ihren **Imaginärteil**  $\text{Im } z := y$ . Wir haben damit zwei Funktionen

$$\text{Re}, \text{Im} : \mathbb{C} \rightarrow \mathbb{R}$$

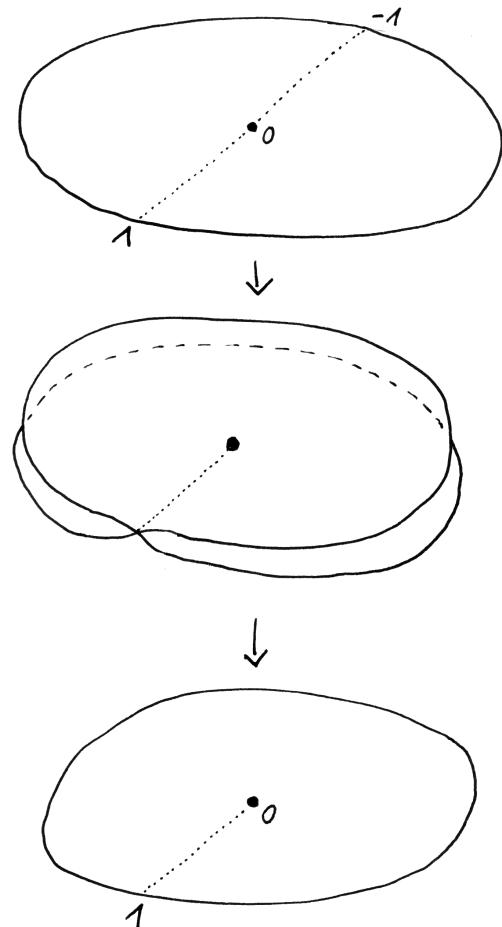
definiert und es gilt  $z = \text{Re } z + i \text{Im } z$  für alle  $z \in \mathbb{C}$ . Man definiert weiter die **Norm**  $|z|$  einer komplexen Zahl  $z = x + y i \in \mathbb{C}$  durch  $|z| := \sqrt{x^2 + y^2} \in \mathbb{R}_{\geq 0}$ . Im Fall einer reellen Zahl  $x \in \mathbb{R}$  ist diese Norm genau unser Absolutbetrag aus ??, in Formeln  $|x| = |x|$ . In der Anschauung der komplexen Zahlenebene bedeutet die Norm einer komplexen Zahl ihren Abstand vom Ursprung.

3.2.7.10 (**Diskussion der Terminologie**). Bei rechtem Lichte besehen scheint mir an dieser Terminologie absonderlich, daß der Imaginärteil einer komplexen Zahl darin eine reelle Zahl ist, aber so hat es sich nun einmal eingebürgert.

3.2.7.11. Stellen wir uns  $|z|$  vor als den Streckfaktor der Drehstreckung  $(z \cdot)$ , so wird anschaulich klar, daß für alle  $z, w \in \mathbb{C}$  gelten muß

$$|zw| = |z||w|$$

Besonders bequem rechnet man diese Formel nach, indem man zunächst für  $z = x + y i \in \mathbb{C}$  die **konjugierte komplexe Zahl**  $\bar{z} = x - y i \in \mathbb{C}$  einführt. Im



Dies Bild soll zusätzliche Anschauung für die Abbildung  $z \mapsto z^2$  der komplexen Zahlenebene auf sich selbst vermitteln. Es stellt diese Abbildung dar als die Komposition einer Abbildung der Einheitskreisscheibe auf eine räumliche sich selbst durchdringende Fläche, gegeben in etwa durch eine Formel der Gestalt  $z \mapsto (z^2, \varepsilon(\operatorname{Im} z))$  in  $\mathbb{C} \times \mathbb{R} \cong \mathbb{R}^3$  für geeignetes monotones und in einer Umgebung von Null streng monotones  $\varepsilon$ , gefolgt von einer senkrechten Projektion auf die ersten beiden Koordinaten. Das hat den Vorteil, daß im ersten Schritt nur Punkte der reellen Achse identifiziert werden, was man sich leicht wegdenken kann, und daß der zweite Schritt eine sehr anschauliche Bedeutung hat, eben die senkrechte Projektion.

Bild der komplexen Zahlenebene bedeutet das komplexe Konjugieren anschaulich die Spiegelung an der reellen Achse. Nun prüft man durch explizite Rechnung unschwer die Formeln

$$\begin{aligned}\overline{z+w} &= \bar{z} + \bar{w} \\ \overline{z \cdot w} &= \bar{z} \cdot \bar{w} \\ |z|^2 &= z\bar{z}\end{aligned}$$

Dann rechnet man einfach

$$|zw|^2 = zw\bar{z}\bar{w} = z\bar{z}w\bar{w} = |z|^2|w|^2$$

In der Terminologie aus 2.2.4.13 ist  $z \mapsto \bar{z}$  ein Körperisomorphismus  $\mathbb{C} \rightarrow \mathbb{C}$ . Offensichtlich gilt auch  $\bar{\bar{z}} = z$  und ebenso offensichtlich  $|z| = |\bar{z}|$ .

3.2.7.12. Die Formel  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$  kann man auch prüfen, indem man davon ausgeht, daß beide Seiten offensichtlich  $\mathbb{R}$ -bilineare Abbildungen  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  definieren. Deren Gleichheit kann nach 3.2.3.9 auf Basen geprüft werden. Es reicht also, sie für  $z, w \in \{1, i\}$  nachzuweisen, und das ist schnell getan.

3.2.7.13. Wir können den Realteil und den Imaginärteil von  $z \in \mathbb{C}$  mithilfe der konjugierten komplexen Zahl ausdrücken als

$$\operatorname{Re} z = \frac{z + \bar{z}}{2} \quad \operatorname{Im} z = \frac{z - \bar{z}}{2i}$$

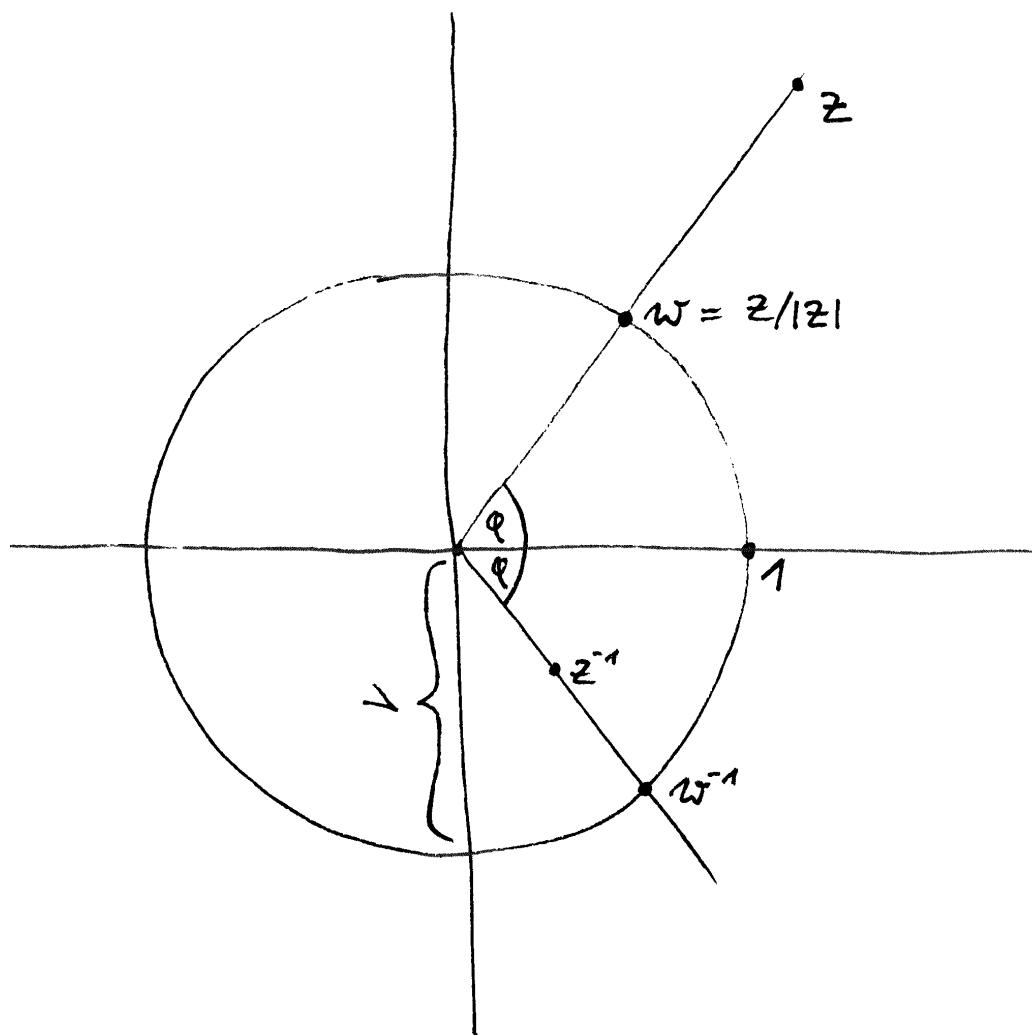
Weiter gilt offensichtlich  $z = \bar{z} \Leftrightarrow z \in \mathbb{R}$ , und für komplexe Zahlen  $z$  der Norm  $|z| = 1$  ist die konjugierte komplexe Zahl genau das Inverse, in Formeln  $|z| = 1 \Rightarrow \bar{z} = z^{-1}$ . Im Bild der komplexen Zahlenebene kann man das Bilden des Inversen einer von Null verschiedenen komplexen Zahl anschaulich interpretieren als die „Spiegelung“ oder präziser **Inversion** am Einheitskreis  $z \mapsto z/|z|^2$  gefolgt von der Spiegelung an der reellen Achse  $z \mapsto \bar{z}$ . Der Einheitskreis  $S^1 := \{z \in \mathbb{C}^\times \mid |z| = 1\}$  ist insbesondere eine Untergruppe der multiplikativen Gruppe des Körpers der komplexen Zahlen und die Multiplikation liefert einen Gruppenisomorphismus  $\mathbb{R}_{>0} \times S^1 \xrightarrow{\sim} \mathbb{C}^\times$ . Wir nennen  $S^1$  die **Kreisgruppe**. Im Fall eines vergeblichen Körpers von komplexen Zahlen notiere ich die Untergruppe der Elemente der Norm Eins  $U(1)$ , da uns in diesem Fall keine ausgezeichnete Bijektion mit  $S^1 \subset \mathbb{R}^2$  mehr zur Verfügung steht.

3.2.7.14. Für unsere Norm komplexer Zahlen aus 3.2.7.9 gilt offensichtlich

$$|z| = 0 \Leftrightarrow z = 0$$

Da in einem Dreieck eine einzelne Seite nicht länger sein kann als die beiden anderen zusammengenommen, erwarten wir weiter die **Dreiecksungleichung**

$$|z + w| \leq |z| + |w|$$



Anschauung für das Invertieren komplexer Zahlen

Formal mag man sie prüfen, indem man beide Seiten quadriert, wodurch die äquivalente Behauptung  $(z + w)(\bar{z} + \bar{w}) \leq z\bar{z} + 2|z||w| + w\bar{w}$  entsteht, und dann vereinfacht zu immer noch äquivalenten Behauptung  $2 \operatorname{Re}(z\bar{w}) \leq 2|z\bar{w}|$ . Die Abschätzungen  $\operatorname{Re}(u) \leq |u|$  und  $\operatorname{Im}(u) \leq |u|$  sind aber für jede komplexe Zahl  $u$  auch formal offensichtlich.

*Ergänzung 3.2.7.15.* Für eine Diskussion der analytischen Aspekte der komplexen Zahlen, insbesondere die komplexe Exponentialfunktion und ihre Beziehung zu den trigonometrischen Funktionen, verweise ich auf die Analysis ??.

### Übungen

*Übung 3.2.7.16.* Man bestimme Real- und Imaginärteil einer Quadratwurzel von i. Man bestimme Real- und Imaginärteil einer Quadratwurzel von  $1 + i$ .

*Übung 3.2.7.17.* Gegeben eine von Null verschiedene komplexe Zahl  $z = x + iy$  zeige man für Real- und Imaginärteil ihrer Inversen die Formeln  $\operatorname{Re}(z^{-1}) = x/(x^2 + y^2)$  und  $\operatorname{Im}(z^{-1}) = -y/(x^2 + y^2)$ .

*Übung 3.2.7.18.* Eine Teilmenge von  $\mathbb{C} \sqcup \{\infty\}$  heißt ein **verallgemeinerter Kreis**, wenn sie entweder ein Kreis

$$K(a; r) := \{z \in \mathbb{C} \mid |z - a|^2 = r^2\}$$

ist für  $a \in \mathbb{C}$  und  $r > 0$  oder aber eine reelle affine Gerade vereinigt mit dem Punkt  $\infty$ . Man prüfe, daß die Selbstabbildung von  $\mathbb{C} \sqcup \{\infty\}$  mit  $z \mapsto z^{-1}$  für  $z \in \mathbb{C}^\times$  und  $0 \mapsto \infty$  und  $\infty \mapsto 0$  verallgemeinerte Kreise in verallgemeinerte Kreise überführt.

### 3.2.8 Möbiusfunktion\*

3.2.8.1. Gegeben  $(X, \leq)$  eine endliche teilgeordnete Menge betrachten wir die  $(X \times X)$ -Matrix  $A$  mit Einträgen  $a_{x,y} = 1$  falls  $x \leq y$  und Null sonst. Zählen wir die Elemente von  $X$  auf als  $x_1, x_2, \dots, x_n$  derart, daß gilt  $x_i \leq x_j \Rightarrow i \leq j$ , so wird  $A$  eine obere Dreiecksmatrix mit ganzzahligen Einträgen und Einsen auf der Diagonalen. Diese Matrix ist also invertierbar und ihre Inverse  $A^{-1}$  ist ebenfalls ein obere Dreiecksmatrix mit Einsen auf der Diagonalen. Besitzt  $X$  ein kleinstes Element  $x_1 = k$ , so nennt man die oberste Zeile von  $A^{-1}$  die **Möbiusfunktion** unserer teilgeordneten Menge

$$\begin{aligned} \mu : X &\rightarrow \mathbb{Z} \\ y &\mapsto (A^{-1})_{k,y} \end{aligned}$$

Sie wird demnach charakterisiert durch die Formeln

$$\mu(k) = 1 \quad \text{und} \quad \sum_{y \leq z} \mu(y) = 0 \text{ falls } z > k.$$

Analoges gilt allgemeiner für jede teilgeordnete Menge  $X$ , die man aufzählen kann als  $x_1, x_2, \dots$  mit  $x_i \leq x_j \Rightarrow i \leq j$ .

3.2.8.2. Ist  $X = \mathbb{N} = \{0, 1, 2, \dots\}$  mit der üblichen Ordnung, so haben wir  $\mu(0) = 1, \mu(1) = -1$  und  $\mu(n) = 0$  für  $n \geq 2$ . Ist  $X = \mathbb{N}_{\geq 1} = \{1, 2, \dots\}$  mit der durch das Teilen gegebenen Ordnung  $a \leq b \Leftrightarrow a|b$ , so erhalten wir die **Möbiusfunktion der Zahlentheorie**

$$\mu(n) = \begin{cases} 0 & n \text{ enthält einen Primfaktor mindestens zweimal;} \\ 1 & n \text{ ist quadratfrei mit gerade vielen Primfaktoren;} \\ -1 & n \text{ ist quadratfrei mit ungerade vielen Primfaktoren.} \end{cases}$$

Dieser Fall kann im übrigen auch als das Produkt von abzählbar vielen Kopien des zuvor behandelten Falls verstanden werden. Speziell haben wir in diesem Fall also

$$\mu(1) = 1 \quad \text{und} \quad \sum_{d|n} \mu(d) = 0 \text{ falls } n > 1.$$

### Übungen

*Ergänzende Übung 3.2.8.3 (Kehrwerte der Riemann'schen  $\zeta$ -Funktion).* Mit  $\mu$  der Möbiusfunktion der Zahlentheorie zeige man, daß für  $s \in \mathbb{C}$  mit  $\operatorname{Re} s > 1$  die Inversen der Werte der Riemann'schen  $\zeta$ -Funktion geschrieben werden können als

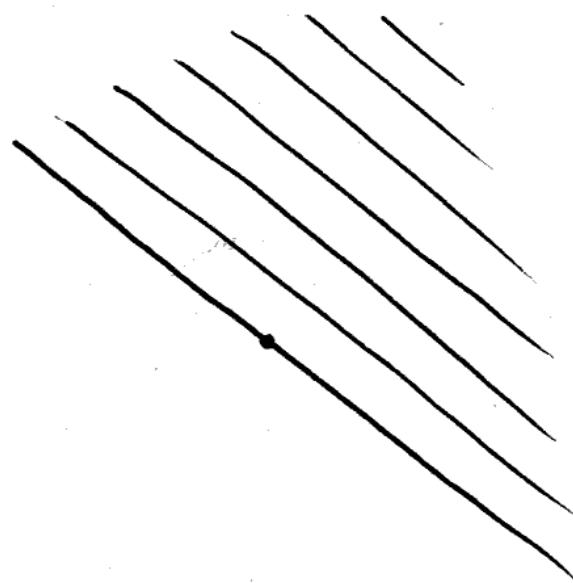
$$\frac{1}{\zeta(s)} = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$$

*Übung 3.2.8.4.* Man bestimme die Inverse der  $(n \times n)$ -Matrix gegeben durch  $a_{ij} = 1$  für  $i \leq j$  und  $a_{ij} = 0$  für  $i > j$ .

### 3.2.9 Dualräume und transponierte Abbildungen

**Definition 3.2.9.1.** Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  nennt man eine lineare Abbildung  $V \rightarrow K$  eine **Linearform auf  $V$**  oder einen **Kovektor**. Die Menge aller solchen Linearformen bildet nach 3.2.3.14 einen Untervektorraum  $\operatorname{Hom}_K(V, K) \subset \operatorname{Ens}(V, K)$  im Vektorraum aller Abbildungen von  $V$  nach  $K$ . Man nennt diesen Vektorraum aller Linearformen den **Dualraum von  $V$** . Wir verwenden dafür die beiden Notationen

$$V^* = V^\top := \operatorname{Hom}_K(V, K)$$



Versuch der graphischen Darstellung eines Kovektors in der Ebene. Sei Wert auf einem Vektor wäre zu verstehen als die Zahl der von unserem Vektorpfeil gekreuzten Linien, beziehungsweise das Negative der Zahl der von seinem Negativen gekreuzten Linien, wenn er in die falsche Richtung geht. Natürlich ist der Wert nicht immer ganzzahlig, das Bild ist deshalb nur mäßig brauchbar. Man sieht aber gut, welche Vektorraumautomorphismen unseren Kovektor festhalten.

3.2.9.2 (**Diskussion der Notation**). Üblich für den Dualraum ist die Notation  $V^*$ . Im Zusammenhang mir darstellenden Matrizen und dergleichen schien mir jedoch die Notation  $V^\top$  suggestivere Formeln zu liefern, weshalb ich diese sonst eher unübliche Notation in diesem Zusammenhang vorziehe.

3.2.9.3. Die Bezeichnung als **Form** für Abbildungen mit Werten im Grundkörper ist allgemein üblich: Wir kennen bis jetzt nur Linearformen, später werden aber noch Bilinearformen und quadratische Formen und Multilinearformen hinzukommen. Über die Herkunft dieser Bezeichnungsweise weiß ich wenig. Vermutlich steckt derselbe Wortstamm wie bei dem Wort „Formel“ dahinter.

*Beispiel 3.2.9.4 (Frequenzraum als Dualraum des Raums der Zeitspannen).* Denken wir uns die Menge aller Zeitspannen als reellen Vektorraum, so können wir uns den Dualraum dieses Vektorraums denken als die Gesamtheit aller „Frequenzen“ oder vielleicht besser, weil man ja eigentlich nicht von negativen Frequenzen reden kann, als den Raum aller möglichen „Drehgeschwindigkeiten von Drehungen um eine feste Achse mit vorgegebenem positiven Drehsinn“. Dann entspräche eine Drehgeschwindigkeit der Linearform, die jeder Zeitspanne die Zahl der in dieser Zeitspanne erfolgten Umdrehungen zuordnet. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist.

3.2.9.5 (**Koordinatenfunktionen zu einer Basis als Kovektoren**). Gegeben ein Vektorraum  $V$  und eine Basis  $B \subset V$  erhalten wir im Dualraum  $V^\top$  eine linear unabhängige Familie von Linearformen  $(b^\top)_{b \in B}$ , indem wir  $b^\top = b_B^\top : V \rightarrow K$  erklären durch

$$b^\top(c) = \delta_{bc} \quad \forall c \in B$$

Die Linearformen  $b^\top$  heißen die **Koordinatenfunktionen** oder kurz **Koordinaten** zu unserer Basis  $B$ . Vielfach werden sie auch  $b^*$  notiert. Ist etwa  $V = \mathbb{R}^n$  und  $B = \mathcal{S}(n) = (\vec{e}_1, \dots, \vec{e}_n)$  die Standardbasis, so wird  $\vec{e}_i^\top : \mathbb{R}^n \rightarrow \mathbb{R}$  die „Projektion auf die  $i$ -te Koordinate“  $\vec{e}_i^\top = \text{pr}_i : (x_1, \dots, x_n) \mapsto x_i$ , die man oft auch einfach  $x_i : \mathbb{R}^n \rightarrow \mathbb{R}$  notiert und die „ $i$ -te Koordinatenfunktion“ nennt. Man beachte, daß solch eine Koordinatenfunktion  $b^\top$  keineswegs nur vom Basisvektor  $b$  abhängt, auch wenn die Notation das suggerieren mag, sondern vielmehr von der ganzen Basis  $B$ . Wenn man es ganz genau nehmen will, sollte man also  $b^\top = (b; B)^\top$  schreiben.

*Beispiel 3.2.9.6 (Dualraum eines  $K^n$ ).* In der Literatur findet man oft die Aussage, daß der Dualraum des Raums der Spaltenvektoren der Länge  $n$  der Raum der Zeilenvektoren der Länge  $n$  sei. Das kann man so sehen, wenn man den kanonischen Isomorphismus  $\text{Mat}(1 \times n; K) \xrightarrow{\sim} \text{Hom}(K^n, K)$  aus 3.2.4.7 soweit verinnerlicht hat, daß man beide Seiten schlicht als gleich ansieht.

*Beispiel 3.2.9.7 (Dualraum des Richtungsraums zum Raum der Anschauung).* Denken wir uns wie in 3.1.5.6 den Raum der Anschauung mit einem ausgezeichneten festen Punkt als reellen Vektorraum, so liefert jeder von Null verschiedene Vektor eine Linearform auf unserem Vektorraum mittels der anschaulich zu verstehenden Vorschrift „projiziere jeden weiteren Vektor orthogonal auf die Gerade durch den gegebenen Vektor und nimm die Zahl, mit der man den den gegebenen Vektor multiplizieren muß, um die Projektion zu erhalten“. Diese Entsprechung hat nur den Nachteil, daß der doppelte Vektor die halbe Linearform liefert und daß überhaupt die Addition von Vektoren keineswegs der Addition von Linearformen entspricht. Wählt man eine feste anschaulich zu verstehende Längeneinheit, so kann man den Raum der Linearformen auf dem Raum der Vektoren in unserem Bild identifizieren mit dem Raum der Vektoren selber, indem man jedem Vektor als Linearform dieselbe Linearform wie oben zuordnet, nur noch zusätzlich geteilt durch das Quadrat seiner Länge. In anderen Worten kann diese Linearform auch beschrieben werden als „beliebigem Vektor ordne zu Länge der Projektion mal Länge des gegebenen Vektors“. Diese Identifikation entspräche dann einem Vektorraumisomorphismus. Es ist vielleicht die Möglichkeit dieser Identifikation, die es uns so schwer macht, eine Anschauung für den Dualraum zu entwickeln. Sie benutzt jedoch die „euklidische Struktur“ des Raums der Anschauung, die das Reden über orthogonale Projektionen eigentlich erst ermöglicht und die wir in erst in 4.1.3 oder noch besser in 4.1.6 mathematisch modellieren werden. Formal diskutieren wir obige Identifikation dann in 4.6.4.11. Auf allgemeinen Vektorräumen stehen uns keine orthogonalen Projektionen zur Verfügung und der Dualraum kann dann nicht mehr so leicht mit dem Ausgangsraum identifiziert werden.

3.2.9.8. Gegeben ein  $k$ -Vektorraum  $V$  haben wir stets eine kanonische bilineare Abbildung  $V \times V^\top \rightarrow k$ , die **Auswertungsabbildung**, auch genannt die **kanonische Paarung** von Vektoren mit Kovektoren.

3.2.9.9 (**Dimension des Dualraums**). Ist  $V$  ein Vektorraum und  $B \subset V$  eine Basis, so liefert nach 3.2.3.2 das Einschränken von Abbildungen eine Bijektion  $V^\top \xrightarrow{\sim} \text{Ens}(B, K)$ , der man leicht ansieht, daß sie sogar ein Vektorraumisomorphismus sein muß. Gegeben ein endlichdimensionaler Vektorraum stimmt insbesondere seine Dimension mit der Dimension seines Dualraums überein, in Formeln

$$\dim V^\top = \dim V$$

3.2.9.10. Ist  $B$  eine Basis eines endlichdimensionalen Vektorraums  $V$ , so muß unsere linear unabhängige Familie  $B^\top := (b^\top)_{b \in B}$  der zugehörigen Koordinatenfunktionen aus 3.2.9.5 nach 3.1.7.10 eine Basis des Dualraums  $V^\top$  sein, da die Zahl ihrer Elemente mit der Dimension des Dualraums übereinstimmt. Man nennt dann  $B^\top$  die **duale Basis** zur Basis  $B$ . Insbesondere besteht die duale Basis zur

Standardbasis des  $\mathbb{R}^n$  genau aus den üblichen Koordinatenfunktionen, in Formeln  $\mathcal{S}(n)^\top = (\text{pr}_i)_{i=1}^n$ .

*Beispiel 3.2.9.11.* Wir kehren noch einmal zu unserem Beispiel 3.2.9.4 zurück. Dort hatten wir besprochen, inwiefern man sich den Dualraum der Gesamtheit aller Zeitspannen als den Raum aller Drehgeschwindigkeiten denken mag. Die zur Basis „Minute“ der Gesamtheit aller Zeitspannen „duale Basis“, die wir gleich in allgemeinen Dualräumen einführen werden, bestünde dann aus dem Vektor „eine Umdrehung pro Minute in positivem Drehsinn“, den man üblicherweise **Umin** notiert.

*Vorschau 3.2.9.12 (Dualräume unendlichdimensionaler Vektorräume).* Im Fall eines unendlichdimensionalen Vektorraums ist wieder nach 3.2.3.14 auch sein Dualraum unendlichdimensional, aber dessen Dimension ist „noch unendlicher“ als die Dimension des Ausgangsraums in einem Sinne, der in ?? präzisiert wird.

**Definition 3.2.9.13.** Gegeben eine  $K$ -lineare Abbildung  $f : V \rightarrow W$  erklären wir die **duale** oder auch **transponierte Abbildung**

$$f^\top : W^\top \rightarrow V^\top$$

als das „Vorschalten von  $f$ “, in Formeln  $f^\top(\lambda) := \lambda \circ f : V \rightarrow K$  für jede Linearform  $\lambda : W \rightarrow K$ .

3.2.9.14. Man beachte, daß die duale Abbildung „in die umgekehrte Richtung“ geht. Oft wird die duale Abbildung auch  $f^* : W^* \rightarrow V^*$  notiert. Nicht selten schreibt man auch ein kleines  $t$  als Index oben links und notiert die duale alias transponierte Abbildung  ${}^t f$ .

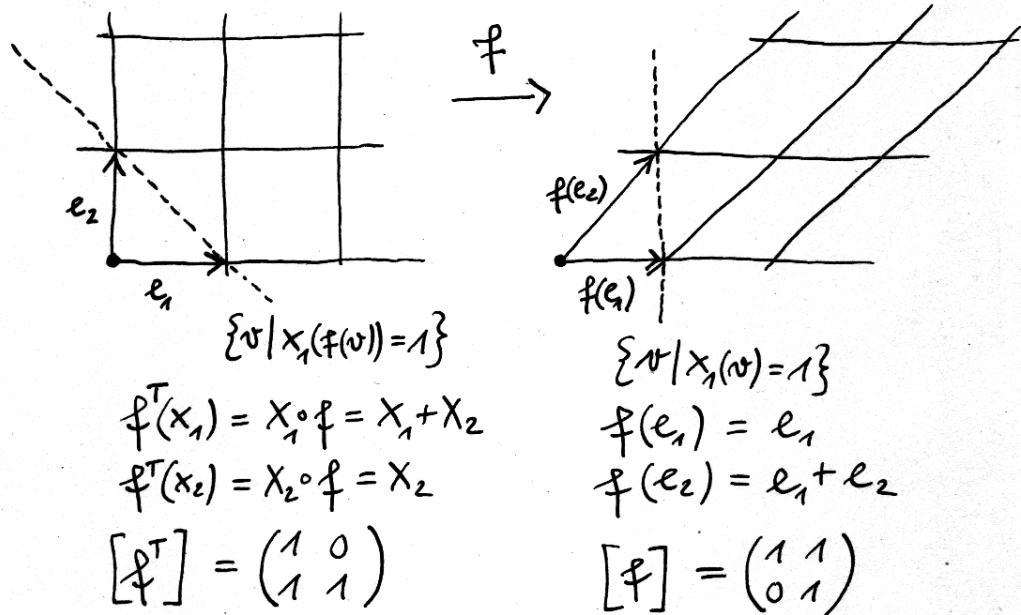
3.2.9.15 (**Verknüpfung und Transponieren**). Sicher gilt stets  $\text{id}_V^\top = \text{id}_{V^\top} : V^\top \rightarrow V^\top$ . Man prüft auch leicht für eine Verknüpfung  $f \circ g$  von linearen Abbildungen die Identität

$$(f \circ g)^\top = g^\top \circ f^\top$$

In der Tat bedeutet das Vorschalten von  $f \circ g$  nichts anderes, als erst  $f$  und dann  $g$  vorzuschalten.

**Proposition 3.2.9.16 (Matrix der dualen Abbildung).** *Gegeben eine lineare Abbildung  $f : V \rightarrow W$  von endlichdimensionalen Vektorräumen mit angeordneten Basen  $\mathcal{A}, \mathcal{B}$  ist die darstellende Matrix der dualen Abbildung  $f^\top : W^\top \rightarrow V^\top$  bezüglich der dualen Basen  $\mathcal{B}^\top, \mathcal{A}^\top$  gerade Transponierte der Matrix von  $f$ , in Formeln*

$${}_{\mathcal{A}^\top} [f^\top]_{\mathcal{B}^\top} = ({}_{\mathcal{B}} [f]_{\mathcal{A}})^\top$$



Eine lineare Abbildung  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ , deren Matrix in einer Basis  $e_1, e_2$ , und die Matrix der dualen Abbildung auf der dualen Basis alias der Effekt des Vorschaltens unserer Abbildung auf den Koordinatenfunktionen

$$x_1, x_2 : \mathbb{R}^2 \rightarrow \mathbb{R}.$$

3.2.9.17. Diese Identität ist der Grund dafür, daß ich für den Dualraum vorzugsweise die Notation mit einem hochgestellten  $\top$  verwenden will. Die dualen Basen sind dabei mit der offensichtlichen Anordnung zu verstehen.

*Beweis.* Seien  $\mathcal{A} = (v_1, \dots, v_n)$  und  $\mathcal{B} = (w_1, \dots, w_n)$  unsere angeordneten Basen. Die Matrixeinträge  $a_{ij}$  der darstellenden Matrix  ${}_{\mathcal{B}}[f]_{\mathcal{A}}$  sind festgelegt durch die Identität von Vektoren  $f(v_j) = \sum_i a_{ij} w_i$ . Die Matrixeinträge  $b_{ji}$  der darstellenden Matrix  ${}_{\mathcal{A}^{\top}}[f^{\top}]_{\mathcal{B}^{\top}}$  sind festgelegt durch die Identität von Linearformen  $f^{\top}(w_i^{\top}) = \sum_j b_{ji} v_j^{\top}$ . Es gilt zu zeigen  $b_{ji} = a_{ij}$ . Um das zu sehen, werten wir diese Identität von Linearformen auf den Vektoren  $v_k$  aus und erhalten

$$b_{ki} = \sum_j b_{ji} v_j^{\top} (v_k) = (f^{\top}(w_i^{\top}))(v_k) = w_i^{\top} (f(v_k)) = w_i^{\top} \left( \sum_l a_{lk} w_l \right) = a_{ik}$$

Das aber war gerade zu zeigen.  $\square$

3.2.9.18 (**Auswerten als Matrixmultiplikation**). Sei  $V$  ein endlichdimensionaler Vektorraum mit einer angeordneten Basis  $\mathcal{A}$ . Eine Linearform  $\lambda \in V^{\top}$  wird als lineare Abbildung  $\lambda : V \rightarrow k$  beschrieben durch eine Zeilenmatrix  $[\lambda]_{\mathcal{A}} = {}_{\mathcal{S}(1)}[\lambda]_{\mathcal{A}}$ . Für das Auswerten unserer Linearform  $\lambda$  auf einem Vektor  $v \in V$  erhalten wir dann

$$\lambda(v) = [\lambda]_{\mathcal{A}} \circ {}_{\mathcal{A}}[v]$$

unter der offensichtlichen Identifikation von Elementen unseres Grundkörpers mit  $(1 \times 1)$ -Matrizen. Erinnern wir dann noch für  $v \in V$  an die lineare Abbildung  $(\cdot v) : K \rightarrow V$  mit  $\alpha \mapsto \alpha v$  und an unsere Identität  ${}_{\mathcal{A}}[\cdot v]_{\mathcal{S}(1)} = {}_{\mathcal{A}}[v]$ , so kann auch obige Formel interpretiert werden als der Spezialfall

$${}_{\mathcal{S}(1)}[\lambda \circ (\cdot v)]_{\mathcal{S}(1)} = {}_{\mathcal{S}(1)}[\lambda]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\cdot v]_{\mathcal{S}(1)}$$

der allgemeinen Formel 3.2.6.5 für die Matrix der Verknüpfung zweier linearer Abbildungen.

3.2.9.19 (**Darstellung einer Linearform in der dualen Basis**). Sei  $V$  ein endlichdimensionaler Vektorraum mit einer angeordneten Basis  $\mathcal{A}$ . Eine Linearform  $\lambda \in V^{\top}$  kann auch als Element des Dualraums in Bezug auf die duale Basis dargestellt werden durch die Spaltenmatrix  ${}_{\mathcal{A}^{\top}}[\lambda]$ . Es ist nun nicht schwer, die Formel

$${}_{\mathcal{A}^{\top}}[\lambda] = ([\lambda]_{\mathcal{A}})^{\top}$$

zu prüfen. Ich bin bei dieser Formel noch etwas unglücklich, daß  $\lambda$  auf der linken Seite nicht transponiert zu sehen. Dieser Anschein von Inkonsistenz kommt dadurch zustande, daß wir in unserer Formel links  $\lambda$  als Vektor auffassen und rechts als lineare Abbildung. Erinnern wir, daß die Spaltenmatrix eines Vektors  $v$

ja auch die Matrix der vom Grundkörper mit seiner Standardbasis ausgehenden linearen Abbildung  $(\cdot v)$  ist, und beachten, daß die Abbildung  $(\cdot \lambda) : k \rightarrow V^\top$  bis auf die offensichtliche Identifikation  $k \xrightarrow{\sim} k^\top$  genau die transponierte Abbildung zu  $\lambda : V \rightarrow k$  ist, so erhalten wir

$${}_{\mathcal{A}^\top}[\lambda] = {}_{\mathcal{A}^\top}[\cdot \lambda]_{\mathcal{S}(1)} = {}_{\mathcal{A}^\top}[\lambda^\top]_{\mathcal{S}(1)^\top}$$

Wir erkennen die Übereinstimmung mit unserer allgemeinen Formel 3.2.9.16 für die Matrix der dualen Abbildung, indem wir die linke Seite obiger Formel in dieser Weise umformen und ihre rechte Seite ausschreiben zu  $({}_{\mathcal{S}(1)}[\lambda]_{\mathcal{A}})^\top$ .

**Beispiel 3.2.9.20 (Transport von Linearformen unter Isomorphismen).** Gegeben ein Vektorraumisomorphismus  $f : V \xrightarrow{\sim} W$  ist die duale Abbildung ein Vektorraumisomorphismus  $f^\top : W^\top \xrightarrow{\sim} V^\top$  und ihre Inverse ist ein Vektorraumisomorphismus  $(f^\top)^{-1} : V^\top \xrightarrow{\sim} W^\top$ . Dieser Isomorphismus leistet, was man sich anschaulich vielleicht am ehesten unter dem „Transport einer Linearform“ vorstellt: Gegeben  $v \in V$  und  $\lambda \in V^\top$  nimmt  $(f^\top)^{-1}(\lambda)$  auf  $f(v)$  denselben Wert an wie  $\lambda$  auf  $v$ . Betrachten wir etwa die Scherung  $f : \mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$ ,  $(x, y) \mapsto (x + y, y)$  mit der Matrix  $[f] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  und  $f(\vec{e}_1) = \vec{e}_1$ ,  $f(\vec{e}_2) = \vec{e}_1 + \vec{e}_2$ . Offensichtlich bleibt die  $y$ -Koordinate eines Punktes unter solch einer Scherung unverändert,  $(f^\top)^{-1}(\vec{e}_2^\top) = \vec{e}_2^\top$ , und die  $x$ -Koordinate des Urbildpunkts entspricht der Differenz zwischen  $x$ -Koordinate und  $y$ -Koordinate des Bildpunkts,  $(f^\top)^{-1}(\vec{e}_1^\top) = \vec{e}_1^\top - \vec{e}_2^\top$ . Das entspricht auch unseren Formeln, nach denen  $f^\top$  bezüglich der Basis  $(\vec{e}_1^\top, \vec{e}_2^\top)$  dargestellt wird durch die transponierte Matrix  $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ , was genau die Formel  $(f^\top)^{-1} : \vec{e}_1^\top \mapsto \vec{e}_1^\top - \vec{e}_2^\top$  und  $(f^\top)^{-1} : \vec{e}_2^\top \mapsto \vec{e}_2^\top$  beinhaltet.

**3.2.9.21 (Anschauung für den Transport von Linearformen).** Eine von Null verschiedene Linearform  $\lambda : V \rightarrow K$  mag man sich veranschaulichen, indem man sich den affinen Teilraum  $\lambda^{-1}(1)$  vorstellt, auf dem sie den Wert Eins annimmt. In dieser Anschauung ist die Multiplikation von Linearformen mit von Null verschiedenen Skalaren noch einigermaßen sichtbar, für die Addition von Linearformen oder die Nullform versagt sie jedoch grandios. Dahingegen ist in dieser Anschauung für einen Automorphismus  $f : \mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$  der Effekt des Inversen  $(f^\top)^{-1}$  der transponierten Abbildung auf Linearformen gut verständlich.

**Definition 3.2.9.22.** Seien  $K$  ein Körper und  $V$  ein  $K$ -Vektorraum. Der Dualraum des Dualraums von  $V$  heißt sein **Bidualraum** und wird  $(V^\top)^\top =: V^{\top\top}$  notiert oder in der Literatur meist  $V^{**}$ . Wir erklären die **kanonische Einbettung in den Bidualraum alias Evaluationsabbildung**

$$\text{ev} = \text{ev}_V : V \hookrightarrow V^{\top\top}$$

als die Vorschrift, die jedem Vektor  $v \in V$  das „Evaluieren auf  $v$ “ zuordnet. In Formeln ist  $\text{ev}(v) \in V^{\top\top}$  also definiert als die lineare Abbildung  $\text{ev}(v) : V^\top \rightarrow K$  mit  $\lambda \mapsto \lambda(v)$ .

**3.2.9.23 (Injektivität der Evaluationsabbildung).** Die Injektivität der kanonischen Abbildung  $V \rightarrow V^{\top\top}$  ergibt sich aus der Erkenntnis, daß es für jeden von Null verschiedenen Vektor  $v \neq 0$  eine Linearform  $\lambda \in V^\top$  gibt mit  $\lambda(v) \neq 0$ . Man kann das etwa zeigen, indem man den Satz 3.2.10.3 über die Fortsetzbarkeit linearer Abbildungen bemüht oder auch, indem man  $v$  zu einer Basis  $B$  von  $V$  ergänzt und dann  $\lambda = v^\top$  wählt. Im Fall unendlichdimensionaler Räume brauchen wir jedoch in jedem Fall den Basiserweiterungssatz in seiner vollen Allgemeinheit 3.1.9.20. Man kann ohne die ihm zugrundeliegenden raffinierteren Methoden der Mengenlehre noch nicht einmal zeigen, daß es auf einem beliebigen von Null verschiedenen Vektorraum überhaupt irgendeine von Null verschiedene Linearform gibt.

**3.2.9.24 (Bidualraum im endlichdimensionalen Fall).** Im Fall eines endlichdimensionalen Vektorraums  $V$  zeigt ein Dimensionsvergleich unmittelbar, daß die Evaluationsabbildung einen Isomorphismus  $V \xrightarrow{\sim} V^{\top\top}$  liefern muß. Manchmal wird diese Erkenntnis als Gleichung  $V = V^{\top\top}$  geschrieben, aber das ist dann mit einigen Hintergedanken zu lesen, denn gleich sind diese beiden Mengen ja keineswegs. Den Hauptbestandteil dieser Hintergedanken macht die folgende Bemerkung explizit.

**3.2.9.25.** Gegeben Mengen  $X, Y, Z, W$  und Abbildungen  $f : X \rightarrow Y$  und  $g : X \rightarrow Z$  und  $h : Y \rightarrow W$  und  $l : Z \rightarrow W$  mit  $h \circ f = l \circ g$  sagt man auch, man habe ein **kommutatives Rechteck**

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ g \downarrow & & \downarrow h \\ Z & \xrightarrow{l} & W \end{array}$$

Ich finde diese Darstellung sehr viel übersichtlicher.

**3.2.9.26 (Kanonische Einbettung und bitransponierte Abbildung).** Gegeben eine lineare Abbildung  $f : V \rightarrow W$  kommutiert das Rechteck

$$\begin{array}{ccc} V & \xrightarrow{\text{ev}_V} & V^{\top\top} \\ f \downarrow & & \downarrow f^{\top\top} \\ W & \xrightarrow{\text{ev}_W} & W^{\top\top} \end{array}$$

In Worten ausgedrückt gilt mithin die Identität  $\text{ev}_W \circ f = f^{\top\top} \circ \text{ev}_V$  von Abbildungen  $V \rightarrow W^{\top\top}$ . Um das zu sehen, muß man nur für alle  $v \in V$  die Identität  $f^{\top\top}(\text{ev}_V(v)) = \text{ev}_W(f(v))$  in  $W^{\top\top}$  prüfen. Dazu gilt es zu zeigen, daß beide Seiten auf allen  $\lambda \in W^\top$  denselben Wert annehmen, daß also gilt

$$(f^{\top\top}(\text{ev}_V(v)))(\lambda) = (\text{ev}_W(f(v)))(\lambda)$$

alias  $((\text{ev}_V v) \circ f^\top)(\lambda) = \lambda(f(v))$  alias  $(\text{ev}_V v)(\lambda \circ f) = \lambda(f(v))$ . Das ist jedoch klar.

**3.2.9.27 (Diskussion der Terminologie).** Meines Erachtens ist es diese letzte Erkenntnis 3.2.9.26, die die Bezeichnung von  $V^\top$  als „Dualraum von  $V$ “ eigentlich erst verständlich macht. „Dual“ kommt ja vom selben Wortstamm wie „Zwei“, und die letzte Erkenntnis formalisiert die Intuition, daß der Bidualraum im Fall endlichdimensionaler Vektorräume „im wesentlichen dasselbe“ ist wie der Ausgangsraum. Etwas formaler werden wir in 4.7.4.9 mit der dort eingeführten Begrifflichkeit die obige Erkenntnis dahingehend aussprechen können, daß für jeden Körper  $K$  die Evaluationsabbildungen eine „Isotransformation des Identitätsfaktors auf der Kategorie der endlichdimensionalen  $K$ -Vektorräume zum Bidualraumfunktor“ bilden.

**3.2.9.28.** Oft verwende ich für das Auswerten einer Linearform  $\lambda \in V^\top$  auf einem Vektor  $v \in V$  auch die symmetrischeren Notationen  $\langle \lambda, v \rangle$  oder sogar  $\langle v, \lambda \rangle$ .

## Übungen

*Ergänzende Übung 3.2.9.29.* Seien  $K$  ein Körper und  $V$  ein  $K$ -Vektorraum. Eine endliche Familie von Linearformen  $f_1, \dots, f_n \in V^\top$  ist linear unabhängig genau dann, wenn sie eine Surjektion  $(f_1, \dots, f_n) : V \twoheadrightarrow K^n$  liefert.

*Übung 3.2.9.30.* Gegeben Vektorräume  $V, W$  liefern die transponierten Abbildungen zu den kanonischen Injektionen nach 3.2.1.8 auf den Dualräumen einen Isomorphismus  $(\text{in}_V^\top, \text{in}_W^\top) : (V \oplus W)^\top \xrightarrow{\sim} V^\top \oplus W^\top$ . Analoges gilt für allgemeinere endliche Summen.

*Übung 3.2.9.31.* Für endlichdimensionale Vektorräume  $V$  ist die kanonische Einbettung aus Dimensionsgründen stets ein Isomorphismus  $V \xrightarrow{\sim} V^{\top\top}$ . Gegeben ein endlichdimensionaler Vektorraum  $V$  zeige man, daß unter der kanonischen Identifikation  $\text{ev}_V : V \xrightarrow{\sim} V^{\top\top}$  jede Basis  $B$  ihrer Dualen entspricht, in Formeln

$$\text{ev}_V(b) = (b^\top)^\top \quad \forall b \in B$$

*Ergänzende Übung 3.2.9.32.* Man zeige: Gegeben ein Vektorraum  $V$  ist die Verknüpfung

$$V^\top \xrightarrow{\text{ev}_{V^\top}} V^{\top\top\top} \xrightarrow{\text{ev}_V^\top} V^\top$$

der Auswertungsabbildung zum Dualraum von  $V$  mit der Transponierten der Auswertungsabbildung von  $V$  die Identität auf dem Dualraum von  $V$ . Hinweis: 2.1.6.13 mag helfen. Vom höheren Standpunkt ?? hängt das damit zusammen, daß „der Dualraumfunktor sein eigener Adjungierter ist“.

*Übung 3.2.9.33.* Sei  $K$  ein Körper. Wir erhalten Isomorphismen  $\text{Mat}(n \times m; K) \xrightarrow{\sim} \text{Mat}(m \times n; K)^\top$  durch die Vorschrift  $A \mapsto (B \mapsto \text{tr}(AB))$ .

*Übung 3.2.9.34 (Spur einer transponierten Abbildung).* Genau dann hat eine lineare Abbildung endlichen Rang, wenn ihre transponierte Abbildung endlichen Rang hat. Ein Endomorphismus endlichen Ranges eines Vektorraums hat stets dieselbe Spur wie der transponierte Endomorphismus des Dualraums.

### 3.2.10 Ergänzungen zu linearen Abbildungen\*

**Satz 3.2.10.1.** *In einem Vektorraum besitzt jeder Untervektorraum ein Komplement.*

*Beweis.* Der Beweis benötigt im unendlichdimensionalen Fall das Zorn'sche Lemma. Seien  $V \supset U$  unser Raum mit seinem Untervektorraum. Ist unser Raum  $V$  endlich erzeugt, so ist auch  $U$  endlich erzeugt nach 3.1.7.11. Wir finden nach 3.1.6.16 eine Basis  $L$  von  $U$  und können sie nach 3.1.7.3 zu einer Basis  $B$  von  $V$  ergänzen. Das Erzeugnis des Komplements  $B \setminus L$  ist dann der gesuchte komplementäre Teilraum. Ist unser Raum  $V$  beliebig, so funktioniert derselbe Beweis, wenn wir die beiden letzten beiden Verweise durch Verweise auf den allgemeinen Basisexistenz- und Ergänzungssatz 3.1.9.20 ersetzen.  $\square$

**Proposition 3.2.10.2.** 1. *Für jede injektive lineare Abbildung  $f : V \hookrightarrow W$  existiert ein **Linksinverses**, als da heißt, eine lineare Abbildung  $g : W \rightarrow V$  mit  $g \circ f = \text{id}_V$ ;*  
 2. *Für jede surjektive lineare Abbildung  $f : V \twoheadrightarrow W$  existiert ein **Rechtsinverses**, als da heißt, eine lineare Abbildung  $g : W \rightarrow V$  mit  $f \circ g = \text{id}_W$ .*

*Beweis.* Der Beweis beider Aussagen benötigt im unendlichdimensionalen Fall das Zorn'sche Lemma. Um Teil 1 zu zeigen, wählen wir mit 3.2.10.1 ein Komplement  $U \subset W$  von  $f(V)$  und definieren  $g : W \rightarrow V$  durch die Vorschrift  $g(u + f(v)) = v \quad \forall u \in U, v \in V$ . Das ist erlaubt, da nach unsren Annahmen die Abbildung  $(u, v) \mapsto u + f(v)$  eine Bijektion  $U \times V \xrightarrow{\sim} W$  induziert. Um Teil 2 zu zeigen, wählen wir ein Komplement  $U \subset V$  von  $\ker f$  und prüfen, daß  $f$  einen einen Isomorphismus  $U \xrightarrow{\sim} W$  induziert. Dessen Inverses liefert unmittelbar das gesuchte Rechtsinverse von  $f$ .  $\square$

### Übungen

*Übung 3.2.10.3.* Jede lineare Abbildung von einem Untervektorraum  $U$  eines Vektorraums  $V$  in einen weiteren Vektorraum  $f : U \rightarrow W$  läßt sich zu einer linearen Abbildung  $\tilde{f} : V \rightarrow W$  auf den ganzen Raum  $V$  fortsetzen. Hinweis: 3.2.10.2.

## 3.3 Affine Räume

### 3.3.1 Affine Räume und affine Abbildungen

**Definition 3.3.1.1.** Ein **affiner Raum** oder kurz **Raum** über einem Körper  $K$  ist ein Tripel

$$E = (E, \vec{E}, a)$$

bestehend aus einer Menge  $E$ , einer abelschen Untergruppe  $\vec{E} \subset \text{Ens}^{\times} E$  der Gruppe der Permutationen von  $E$  sowie einer Abbildung  $a : K \times \vec{E} \rightarrow \vec{E}$  derart, daß gilt:

1. Die Menge  $E$  ist nicht leer und das Auswerten liefert für alle  $p \in E$  eine Bijektion  $\vec{E} \xrightarrow{\sim} E, \vec{v} \mapsto \vec{v}(p)$ ;
2. Mit der Abbildung  $a : K \times \vec{E} \rightarrow \vec{E}$  als der Multiplikation mit Skalaren wird  $\vec{E}$  ein  $K$ -Vektorraum.

Die Elemente von  $E$  heißen die **Punkte** unseres affinen Raums. Die Elemente von  $\vec{E}$  heißen **Translationen** oder **Richtungsvektoren** unseres affinen Raums. Den Vektorraum  $\vec{E}$  nennen wir den **Richtungsraum** unseres affinen Raums und notieren ihn auch  $\vec{E} = \text{Richt}(E)$ . Das Resultat der Operation einer Translation  $\vec{v} \in \vec{E}$  auf einem Punkt  $p \in E$  notieren wir  $\vec{v} + p := \vec{v}(p)$  oder auch  $p + \vec{v}$ .

**3.3.1.2 (Diskussion der Notation und Terminologie).** Die leere Menge kann in unseren Konventionen nie ein affiner Raum sein. Unser Richtungsraum wird in manchen Quellen der **Differenzraum** genannt. Vielfach findet man auch die begriffliche Variante eines **affinen Raums über einem vorgegebenen Vektorraum**. Darunter versteht man dann eine Menge  $E$  mit einer „freien transitiven Wirkung“ des vorgegebenen Vektorraums. Ich ziehe die oben gegebene Definition vor, da sie jeden Bezug auf einen bereits vorgegebenen Vektorraum vermeidet und den Raum unserer Anschauung dadurch meines Erachtens überzeugender modellieren kann.

*Ergänzung 3.3.1.3.* Die Notation des Richtungsraums mit einem Pfeil steht in Konflikt zu unserer Notation aus ??, nach der das Versehen mit einem Pfeil bei Mannigfaltigkeiten die Wahl einer Orientierung andeutet. Was im Einzelfall jeweils gemeint ist, muß der Leser aus dem Kontext erschließen.

**3.3.1.4.** Unter der **Dimension** eines affinen Raums verstehen wir die Dimension seines Richtungsraums. Ein affiner Raum über dem Körper  $\mathbb{R}$  der reellen Zahlen heißt auch ein **reeller affiner Raum** oder kurz **reeller Raum**.

**3.3.1.5.** Ein affiner Raum hat die Dimension Null genau dann, wenn er aus einem einzigen Punkt besteht. Affine Räume der Dimension Eins heißen **affine Geraden**. Affine Räume der Dimension Zwei heißen **affine Ebenen**.

**3.3.1.6 (Einige Formeln für affine Räume).** Ist  $E$  ein affiner Raum, so liefert nach Annahme für jedes  $p \in E$  das Anwenden der Richtungsvektoren auf besagten Punkt eine Bijektion  $\vec{E} \xrightarrow{\sim} E$ ,  $\vec{v} \mapsto \vec{v} + p$  und es gilt  $\vec{0} + p = p$  sowie  $\vec{u} + (\vec{v} + p) = (\vec{u} + \vec{v}) + p$  für alle  $\vec{u}, \vec{v} \in \vec{E}$  und  $p \in E$ . Flapsig gesprochen ist also ein affiner Raum ein „Vektorraum, bei dem man den Ursprung vergessen hat“. Gegeben  $p, q \in E$  erklären wir

$$p - q \in \vec{E}$$

als denjenigen Richtungsvektor  $\vec{u} \in \vec{E}$  mit  $p = \vec{u} + q$ . Das erklärt auch die alternative Bezeichnung des Richtungsraums als „Differenzraum“.

*Ergänzung 3.3.1.7.* In Schulbüchern verwendet man für die Punkte eines affinen Raums meist Großbuchstaben  $A, B, C, \dots$  und schreibt

$$\overrightarrow{AB}$$

für den Richtungsvektor, der  $A$  nach  $B$  schiebt und den wir hier  $B - A$  notieren. In einem didaktischen Kontext mag man statt  $p - q$  auch  $p \leftarrow q$  schreiben wollen.

**3.3.1.8 (Vektorräume als affine Räume).** Jeder Vektorraum  $V$  kann als affiner Raum aufgefaßt werden, indem wir als Translationen die durch die Addition von festen Vektoren gegebenen Abbildungen nehmen, so daß unsere Gruppe von Translationen das Bild des injektiven Gruppenhomomorphismus  $V \hookrightarrow \text{Ens}^\times(V)$ ,  $v \mapsto (v+)$  wird. Die Vektorraumstruktur auf der Gruppe der Translationen erklären wir dabei dadurch, daß dieser Gruppenhomomorphismus einen Vektorraumisomorphismus auf sein Bild liefern soll. Insbesondere erhalten wir damit eine kanonische Identifikation

$$\text{trans} : V \xrightarrow{\sim} \vec{V} = \text{Richt}(V)$$

zwischen unserem Vektorraum und dem Richtungsraum des dazu gebildeten affinen Raums. Diese Identifikation scheint mir derart kanonisch, daß ich sie in Sprache und Notation oft so behandeln werde, als seien diese beiden Vektorräume schlicht gleich.

**Beispiel 3.3.1.9 (Der Raum unserer Anschauung als affiner Raum).** Es scheint mir besonders sinnfällig, den schmutzigen „Raum unserer Anschauung“ mathematisch als einen dreidimensionalen reellen affinen Raum

$$\mathbb{E}$$

zu modellieren. Dieses Modell werden wir in 4.1.6.2 folgende noch um die Vorgabe einer ausgezeichneten „Bewegungsgruppe“ und je nach Kontext einer ausgezeichneten „Orientierung“ erweitern und so den „Anschauungsraum“ formal als

ein Gebilde der Mengenlehre definieren. Die endgültige Definition muß aber noch auf die Einführung dieser Begriffe warten. Der Buchstabe  $\mathbb{E}$  soll an das französische Wort „espace“ für „Raum“ erinnern. Unser „Raum unserer Anschauung“ ist der „Raum der klassischen Mechanik“. Manche Punkte dieses Raums können wir uns direkt als Kirchturmspitzen, Zimmerecken und dergleichen denken, die Übrigengilt es sich vorzustellen. Die „affinen Geraden“ entsprechen unseren Sichtlinien. Wir ignorieren dabei, daß die Erde sich um sich selber dreht und dabei gleichzeitig um die Sonne rast, die sich hinwiederum mit unvorstellbarer Geschwindigkeit um das Zentrum der Milchstraße bewegt, und ich könnte noch eine Weile so weitermachen. Den zum Raum unserer Anschauung gehörigen Richtungsraum denke ich mir als die Gesamtheit aller „Parallelverschiebungen des Raums der Anschauung“. In 3.3.3 werden Sie lernen, in welchem Sinne die Bedingung, daß unsere Sichtlinien gerade den „affinen Geraden“ entsprechen sollen, die Struktur als reeller affiner Raum bereits eindeutig festlegt. Daß wir als Grundkörper für die Modellierung des Raums der Anschauung den Körper der reellen Zahlen nehmen, hat analytische Gründe: Im Kern liegen sie darin, daß für diesen Körper der Zwischenwertsatz ?? gilt. Deshalb modellieren reelle Vektorräume, insbesondere wenn es später auch um Drehungen, Winkel im Bogenmaß und dergleichen gehen wird, unsere geometrische Anschauung besser als etwa Vektorräume über den rationalen Zahlen. Überspitzt könnte man sagen, daß im Gegensatz zu früher, als die mathematische Modellierung der Ebene mithilfe der euklidischen Axiome an den Anfang gestellt wurde, die Mathematik seit dem Anfang des 20.-ten Jahrhunderts mit der Modellierung der Gerade beginnt, genauer mit der Axiomatik des Körpers der reellen Zahlen ??.

*Beispiel 3.3.1.10.* Man mag sich die Schreibfläche einer in jeder Richtung unbegrenzten Tafel als einen zweidimensionalen reellen affinen Raum denken. Daß dieses Beispiel schmutzig ist, versteht sich von selbst.

*Beispiel 3.3.1.11.* Die schmutzige Menge aller **Zeitpunkte der klassischen Mechanik** mag man mathematisch als einen eindimensionalen reellen affinen Raum

 $\mathbb{T}$ 

modellieren. Dieses Modell für die „Zeit“ werden wir in 3.6.5.11 noch durch die Vorgabe einer ausgezeichneten „Orientierung“ erweitern. Der Buchstabe  $\mathbb{T}$  soll an das lateinische Wort „tempus“ für „Zeit“ erinnern. Ein Richtungsvektor dieses affinen Raums wäre etwa die Vorschrift: Man warte von einem vorgegebenen Zeitpunkt sieben Ausschläge eines bestimmten Pendels ab, dann erreicht man den um besagte Translation verschobenen Zeitpunkt. Die Elemente des Richtungsraums  $\vec{\mathbb{T}}$  dieses affinen Raums mag man sich als **Zeitspannen** denken, wobei jedoch auch „negative Zeitspannen“ zugelassen sind. Die Flugbahn einer Fliege etwa würden wir durch eine Abbildung  $\mathbb{T} \rightarrow \mathbb{E}$  oder genauer, da Fliegen ja sterblich sind, durch die Abbildung von einer geeigneten Teilmenge  $I \subset \mathbb{T}$  nach  $\mathbb{E}$  beschreiben.

*Beispiel 3.3.1.12.* Ein Vektor des Homomorphismenraums  $\text{Hom}(\vec{\mathbb{T}}, \vec{\mathbb{E}})$  vom Vektorraum der Zeitspannen in den Richtungsraum des Anschauungsraums modelliert, was man in der Physik eine **vektorielle Geschwindigkeit** nennt.

**Definition 3.3.1.13.** Eine Abbildung  $\varphi : E \rightarrow F$  zwischen affinen Räumen über demselben Körper heißt eine **affine Abbildung**, wenn es eine lineare Abbildung zwischen den zugehörigen Richtungsräumen  $\vec{\varphi} : \vec{E} \rightarrow \vec{F}$  gibt mit

$$\varphi(p) - \varphi(q) = \vec{\varphi}(p - q) \quad \forall p, q \in E$$

Diese lineare Abbildung  $\vec{\varphi}$  ist dann durch  $\varphi$  eindeutig bestimmt und heißt der **lineare Anteil** oder **Richtungsanteil**  $\text{Richt}(\varphi) := \vec{\varphi}$  unserer affinen Abbildung. Die Menge aller affinen Abbildungen von einem affinen Raum  $E$  in einen weiteren affinen Raum  $F$  über demselben Grundkörper  $K$  notieren wir

$$\text{Aff}(E, F) = \text{Aff}_K(E, F)$$

Eine bijektive affine Abbildung heißt ein **Isomorphismus von affinen Räumen**. Die Menge aller Isomorphismen von  $E$  nach  $F$  notieren wir  $\text{Aff}^\times(E, F)$ . Ein Isomorphismus von einem affinen Raum auf sich selbst heißt ein **Automorphismus** oder auch eine **Affinität** des besagten affinen Raums. Die Gruppe aller Affinitäten eines affinen Raums  $E$  notieren wir  $\text{Aff}^\times(E) := \text{Aff}^\times(E, E)$ .

*Beispiel 3.3.1.14 (Affine Abbildungen zwischen Vektorräumen).* Eine Abbildung  $\varphi : V \rightarrow W$  zwischen Vektorräumen ist affin als Abbildung zwischen den dazu gebildeten affinen Räumen genau dann, wenn es eine lineare Abbildung  $\vec{\varphi} : V \rightarrow W$  und einen Punkt  $w \in W$  gibt mit

$$\varphi(v) = w + \vec{\varphi}(v)$$

für alle  $v \in V$ . Jede affine Abbildung  $\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^m$  hat also die Gestalt  $v \mapsto Av + b$  für  $A \in \text{Mat}(m \times n; \mathbb{R})$  und  $b \in \mathbb{R}^m$ . Dabei ist  $A = [\vec{\varphi}]$  die Matrix des Richtungsanteils und  $b = \varphi(0)$  das Bild des Ursprungs.

*Beispiel 3.3.1.15 (Affine Selbstabbildungen einer Gerade).* Die affinen Abbildungen einer Gerade auf sich selber sind anschaulich gesprochen alle Streckungen von einem gegebenem Fixpunkt aus, alle Verschiebungen und alle konstanten Abbildungen, die man auch als Streckungen mit Streckfaktor Null auffassen kann. Im reellen Fall sind im Graphenbild aus der Schule die affinen Abbildungen  $\mathbb{R} \rightarrow \mathbb{R}$  genau diejenigen Abbildungen, deren Graph eine Gerade ist und die auf der Schule meist als „lineare Abbildungen“ bezeichnet werden.

### Übungen

*Übung 3.3.1.16.* Die Verknüpfung affiner Abbildungen ist affin und der lineare Anteil einer Verknüpfung affiner Abbildungen ist die Verknüpfung ihrer linearen Anteile, in Formeln  $\vec{\varphi} \circ \vec{\rho} = \overrightarrow{\varphi \circ \rho}$ .

*Übung 3.3.1.17.* Eine Abbildung  $\varphi : E \rightarrow F$  zwischen affinen Räumen ist genau dann affin, wenn es einen Punkt  $p \in E$  und eine lineare Abbildung  $\vec{\varphi} : \vec{E} \rightarrow \vec{F}$  zwischen den zugehörigen Richtungsräumen gibt mit

$$\varphi(p + \vec{v}) = \varphi(p) + \vec{\varphi}(\vec{v}) \quad \forall \vec{v} \in \vec{E}$$

*Übung 3.3.1.18 (Affine Abbildungen mit der Identität als linearem Anteil).* Die Richtungsvektoren eines affinen Raums sind genau alle seine affinen Selbstabbildungen, deren linearer Anteil die Identität ist. In Formeln gilt für einen affinen Raum  $E$  also

$$\vec{E} = \{\varphi \in \text{Aff}(E, E) \mid \vec{\varphi} = \text{id}_{\vec{E}}\}$$

*Übung 3.3.1.19 (Affine Abbildungen mit Null als linearem Anteil).* Die affinen Abbildungen mit verschwindendem linearen Anteil sind genau die konstanten Abbildungen. Gegeben affine Räume  $E, F$  über demselben Körper gilt also in Formeln

$$\{\varphi \in \text{Aff}(E, F) \mid \vec{\varphi} = 0\} = \{\varphi \in \text{Ens}(E, F) \mid \varphi \text{ ist konstant}\}$$

*Übung 3.3.1.20.* Gegeben ein affiner Raum  $E$  und ein Punkt  $p \in E$  zeige man, daß die Abbildung  $E \rightarrow E$  gegeben durch  $p + \vec{v} \mapsto p - \vec{v} \quad \forall \vec{v} \in \vec{E}$  affin ist. Sie heißt die **Punktspiegelung an  $p$** . Allgemeiner zeige man, daß für alle Skalare  $\lambda$  aus dem Grundkörper die Abbildung  $E \rightarrow E$  gegeben durch  $p + \vec{v} \mapsto p + \lambda \vec{v}$  affin ist. Sie heißt die **Streckung** oder auch **Homothetie mit Zentrum  $p$  und Streckfaktor  $\lambda$** .

*Übung 3.3.1.21.* Beschreiben Sie in schmutzigen Worten affine Abbildungen  $\mathbb{T} \rightarrow \mathbb{E}$  des affinen Raums der Zeiten in den Anschauungsraum. Natürlich ist das keine mathematische Übung im eigentlichen Sinne!

*Übung 3.3.1.22 (Produkt affiner Räume).* Gegeben affine Räume  $X_1, \dots, X_n$  gibt es auf ihrem kartesischen Produkt  $X_1 \times \dots \times X_n$  genau eine Struktur als affiner Raum derart, daß alle Projektionen  $\text{pr}_i$  affin sind. Des weiteren liefern dann die linearen Anteile der Projektionen einen Isomorphismus

$$(\text{pr}_1, \dots, \text{pr}_n) : \text{Richt}(X_1 \times \dots \times X_n) \xrightarrow{\sim} \vec{X}_1 \times \dots \times \vec{X}_n$$

zwischen dem Richtungsraum des Produkts und dem Produkt der Richtungsräume der Faktoren.

*Beispiel 3.3.1.23.* Bezeichnet  $\mathbb{E}$  den Raum unserer Anschauung, mutig gedacht für einen fest auf der Sonne stehenden Beobachter, so mag man jede mögliche Konstellation von Erde und Mond als einen Punkt von  $\mathbb{E} \times \mathbb{E}$  modellieren.

*Übung 3.3.1.24 (Vorübung für affine Teileräume).* Gegeben ein injektiver Homomorphismus von affinen Räumen  $\varphi : F \hookrightarrow E$  zeige man, daß sein linearer Anteil  $\vec{\varphi}$  einen Vektorraumisomorphismus  $\vec{\varphi} : \vec{F} \xrightarrow{\sim} \{\vec{v} \in \vec{E} \mid \vec{v} + \varphi(F) = \varphi(F)\}$  induziert.

### 3.3.2 Affine Teileräume

**Definition 3.3.2.1.** Sei  $E$  ein affiner Raum. Eine Teilmenge  $F \subset E$  heißt ein **affiner Teilraum**, wenn  $F$  so mit der Struktur eines affinen Raums  $(F, \vec{F}, b)$  versehen werden kann, daß die Einbettung eine affine Abbildung ist. Übung 3.3.1.24 zeigt, daß diese Struktur als affiner Raum auf unserer Teilmenge  $F$  dann eindeutig bestimmt ist und daß die Richtungsvektoren von  $F$  genau die Einschränkungen derjenigen Richtungsvektoren von  $E$  sind, die  $F$  stabilisieren.

3.3.2.2. Gegeben  $F \subset E$  ein affiner Teilraum eines affinen Raums bezeichnen wir mit  $\vec{F}$  sowohl den Richtungsraum von  $F$  als auch sein Bild in  $\vec{F} \subset \vec{E}$  unter dem Richtungsanteil der Einbettung und nennen auch dieses Bild den **Richtungsraum von  $F$** . Offensichtlich gilt dann  $F = p + \vec{F}$  für jeden Punkt  $p \in F$ . Umgekehrt ist auch für jeden Punkt  $p \in E$  und jeden Untervektorraum  $W \subset \vec{E}$  die Teilmenge  $p + W$  ein affiner Teilraum von  $E$ .

*Beispiel 3.3.2.3.* Die affinen Teileräume des  $\mathbb{R}^3$  sind genau: Alle einelementigen Teilmengen, alle Geraden  $G = p + \mathbb{R}\vec{v}$  mit  $\vec{v} \neq \vec{0}$ , alle Ebenen  $P = p + \mathbb{R}\vec{v} + \mathbb{R}\vec{w}$  mit  $\vec{v}, \vec{w}$  linear unabhängig, sowie der ganze  $\mathbb{R}^3$ .

3.3.2.4. Eine Teilmenge eines affinen Raums heißt eine **Gerade** oder genauer eine **affine Gerade**, wenn sie ein affiner Teilraum der Dimension Eins ist. Eine Teilmenge eines affinen Raums heißt eine **Ebene** oder genauer eine **affine Ebene**, wenn sie ein affiner Teilraum der Dimension Zwei ist. Eine Teilmenge eines affinen Raums heißt **kollinear**, wenn sie in einer Geraden enthalten ist.

3.3.2.5. Ein nichtleerer Schnitt von affinen Teileräumen eines affinen Raums ist stets wieder ein affiner Teilraum. Weiter ist der Richtungsraum des Schnitts der Schnitt der Richtungsräume, wenn wir alle diese Richtungsräume wie in 3.3.2.2 als Teilmengen des Richtungsraums unseres ursprünglichen Raums betrachten. Sie mögen den Beweis als Übung 3.3.2.19 ausschreiben.

**Definition 3.3.2.6.** Gegeben eine nichtleere Teilmenge  $T \neq \emptyset$  eines affinen Raums gibt es nach 3.3.2.5 einen kleinsten affinen Teilraum  $\langle T \rangle_{\text{aff}}$ , der sie umfaßt. Wir bezeichnen ihn als den **von unserer Teilmenge erzeugten** affinen Teilraum. Ein

**Erzeugendensystem eines affinen Raums** ist eine nichtleere Teilmenge, die ihn erzeugt.

3.3.2.7. Man beachte, daß in unserer Terminologie insbesondere auch in einem einpunktigen affinen Raum die leere Teilmenge kein Erzeugendensystem ist.

3.3.2.8 (**Explizite Beschreibung affiner Erzeugnisse**). Man mag den von einer nichtleeren Teilmenge  $T \neq \emptyset$  eines affinen Raums  $E$  erzeugten affinen Teilraum  $\langle T \rangle_{\text{aff}}$  auch beschreiben als

$$\langle T \rangle_{\text{aff}} = T + \langle p - q \mid p, q \in T \rangle_{\text{lin}}$$

In Worten nehme man also den Untervektorraum des Richtungsraums von  $\vec{E}$ , der von allen zwei Punkten unserer Teilmenge ineinander überführenden Vektoren erzeugt wird, und lasse seine Vektoren auf Punkte unserer Teilmenge los: Alle Punkte, die man so erhalten kann, bilden einen affinen Teilraum, da ja offensichtlich gilt  $T + \langle p - q \mid p, q \in T \rangle_{\text{lin}} = t + \langle p - q \mid p, q \in T \rangle_{\text{lin}}$  für alle  $t \in T$ .

3.3.2.9 (**Anschauliche Interpretation linearer Gleichungssysteme**). Wählen wir im Anschauungsraum  $\mathbb{E}$  einen festen Punkt  $p$  als **Ursprung** und eine angeordnete Basis  $\vec{v}_1, \vec{v}_2, \vec{v}_3$  seines Richtungsraums, so erhalten wir eine Bijektion

$$\mathbb{R}^3 \xrightarrow{\sim} \mathbb{E}$$

vermittels der Abbildungsvorschrift  $(x, y, z) \mapsto p + x\vec{v}_1 + y\vec{v}_2 + z\vec{v}_3$ . Die Abbildungen  $\mathbb{E} \rightarrow \mathbb{R}^3$ , die jedem Punkt die Komponenten seines Urbilds unter dieser Identifikation zuordnen, heißen auch **Koordinaten** und in ihrer Gesamtheit ein **Koordinatensystem auf  $\mathbb{E}$** . Unter jeder derartigen Identifikation des  $\mathbb{R}^3$  mit dem Raum unserer Anschauung kann man sich die Lösungsmenge einer homogenen linearen Gleichung in drei Unbekannten als eine Ebene durch den Ursprung denken, wenn man einmal von der „Nullgleichungen“ absieht, und die Lösungsmenge einer nicht notwendig homogenen linearen Gleichung in drei Unbekannten als eine affine Ebene, wenn man wieder von dem Fall der „Nullgleichung“ absieht, bei denen die Koeffizienten von  $x, y, z$  alle drei verschwinden. Die Lösungsmenge eines linearen Gleichungssystems ohne Nullgleichung kann man sich demnach anschaulichen als den Schnitt einiger affiner Ebenen, eben der Lösungsmengen seiner einzelnen Gleichungen. So sieht man auch anschaulich ein, daß die Lösungsmenge eines linearen Gleichungssystems ohne Nullgleichung mit zwei Gleichungen in drei Veränderlichen im Allgemeinen einen eindimensionalen Lösungsraum haben wird, da sich eben zwei Ebenen im Raum im Allgemeinen in einer Geraden schneiden, daß aber als Lösungsraum auch die leere Menge in Frage kommt, als Schnitt zweier paralleler Ebenen, und eine Ebene, wenn nämlich die Lösungsräume unserer beiden Gleichungen übereinstimmen.

3.3.2.10. Eine Teilmenge eines affinen Raums heißt eine **Hyperebene** oder genauer eine **affine Hyperebene**, wenn sie ein echter affiner Teilraum ist, der zusammen mit einem einzigen weiteren Punkt unseren ganzen affinen Raum affin erzeugt.

**Definition 3.3.2.11.** Zwei affine Teilräume  $T, S \subset E$  eines affinen Raums  $E$  heißen **parallel**, wenn sie disjunkt sind und im Richtungsraum  $\vec{E}$  gilt  $\vec{T} \subset \vec{S}$  oder  $\vec{S} \subset \vec{T}$ .

3.3.2.12 (**Diskussion der Terminologie**). Die Konventionen scheinen in der Literatur nicht ganz eindeutig zu sein. Die hier gegebene Definition von Parallelität hat den Vorteil, die üblichen Definitionen für die Parallelität von Geraden oder Ebenen im zweidimensionalen wie im dreidimensionalen Raum zu liefern. Allerdings hat sie den Nachteil, daß ein Punkt zu jedem Teilraum parallel ist, der ihn nicht enthält, was meinem Sprachempfinden eigentlich zuwiderläuft.

*Ergänzung 3.3.2.13.* Der Begriff „parallel“ kommt aus dem Griechischen und heißt „nebeneinander“.

## Übungen

*Übung 3.3.2.14 (Fasern linearer Abbildungen).* Gegeben eine lineare Abbildung  $f : V \rightarrow W$  gilt für alle  $v \in V$  die Identität  $f^{-1}(f(v)) = v + \ker f$  von Teilmengen von  $V$ . Für alle  $w \in W$  ist mithin die Faser  $f^{-1}(w)$  entweder leer oder aber ein affiner Teilraum von  $V$ .

*Übung 3.3.2.15 (Urbilder affiner Teilräume).* Ist  $f : V \rightarrow W$  eine affine Abbildung, so ist für jeden affinen Teilraum  $A \subset W$  sein Urbild  $f^{-1}(A)$  entweder leer oder aber ein affiner Teilraum von  $V$ . Das verallgemeinert die vorhergehende Übung 3.3.2.14.

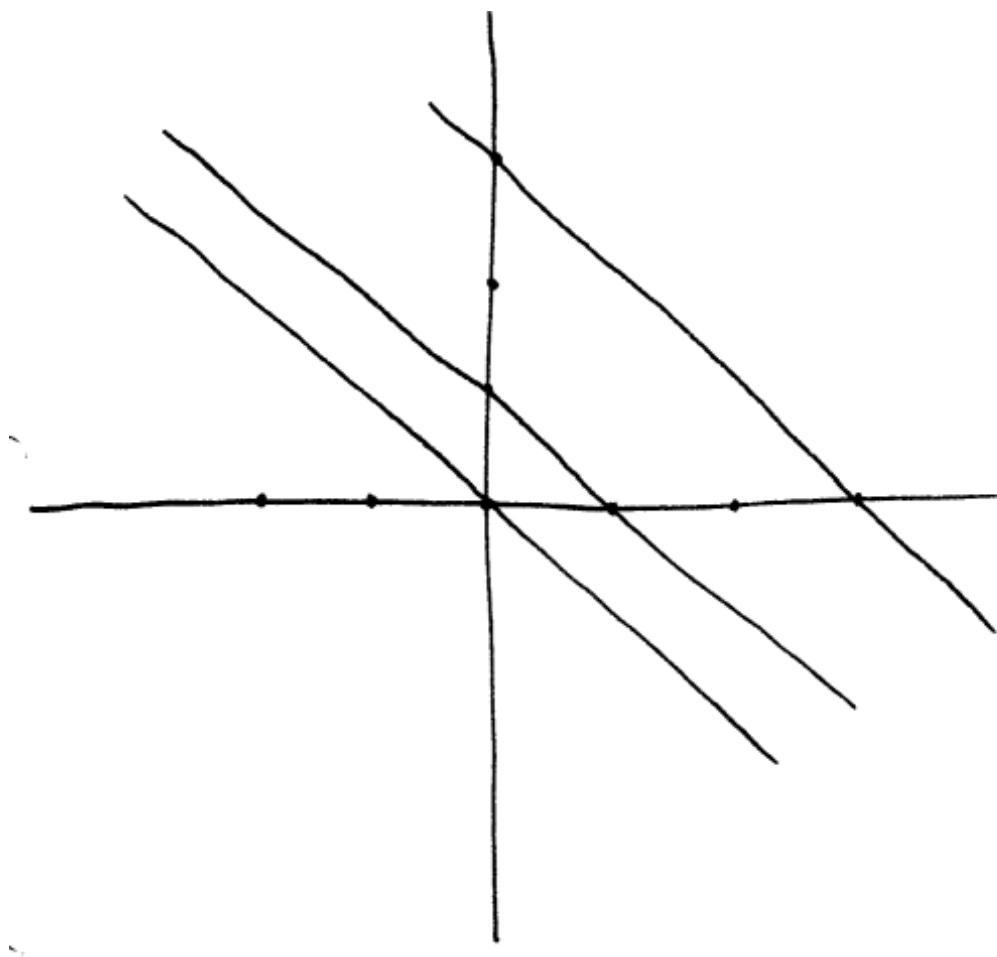
*Übung 3.3.2.16.* Durch je zwei verschiedene Punkte eines affinen Raums geht genau eine Gerade, als da heißt, es gibt genau einen affinen Teilraum der Dimension Eins, der unsere beiden Punkte enthält. Bringt man also Kimme und Korn in eine Sichtlinie mit dem Ziel, so ist das Gewehr bereits auf das Ziel ausgerichtet.

*Übung 3.3.2.17.* Durch je drei Punkte eines affinen Raums, die nicht auf einer gemeinsamen Geraden liegen, geht genau eine Ebene. Insbesondere wird also ein dreibeiniger Hocker nie kippeln.

*Übung 3.3.2.18.* Der von einer nichtleeren endlichen Teilmenge  $T$  eines affinen Raums erzeugte Teilraum hat höchstens die Dimension  $|T| - 1$ .

*Übung 3.3.2.19 (Richtungsraum eines Schnitts).* Gegeben ein affiner Raum  $E$  und affine Teilräume  $F, G \subset E$  mit nichtleerem Schnitt  $F \cap G \neq \emptyset$  ist der Richtungsraum ihres Schnitts der Schnitt ihrer Richtungsräume, in Formeln

$$\text{Richt}(F \cap G) = \text{Richt}(F) \cap \text{Richt}(G)$$



Die Fasern der durch  $(x, y) \mapsto x + y$  gegebenen linearen Abbildung  $\mathbb{R}^2 \rightarrow \mathbb{R}$  zu den Werten 0, 1 und 3.

Man zeige immer unter der Annahme, daß besagter Schnitt nicht leer ist, dasselbe auch allgemeiner für den Schnitt eines beliebigen Systems affiner Teilräume.

*Übung 3.3.2.20 (Erzwungene Schnitte).* Gegeben ein affiner Raum  $E$  und affine Teilräume  $F, G \subset E$  gilt

$$\vec{F} + \vec{G} = \vec{E} \Rightarrow F \cap G \neq \emptyset$$

*Übung 3.3.2.21 (Dimension eines affinen Erzeugnisses).* Gegeben zwei endlich-dimensionale affine Teileräume  $A, B$  eines affinen Raums  $E$  gilt für die Dimension des affinen Erzeugnisses  $C$  ihrer Vereinigung die Formel

$$\dim C = \begin{cases} \dim A + \dim B - \dim(A \cap B) & \text{falls } A \cap B \neq \emptyset; \\ \dim A + \dim B - \dim(\vec{A} \cap \vec{B}) + 1 & \text{falls } A \cap B = \emptyset. \end{cases}$$

*Übung 3.3.2.22 (Kodimension eines Schnitts).* Ist  $E$  ein endlichdimensionaler affiner Raum und vereinbaren wir die Notation  $\text{codim}(A \subset E) := \dim E - \dim A$  für die Dimensionsdifferenz, die sogenannte **Kodimension von  $A$  in  $E$** , so gilt unter der Annahme  $A \cap B \neq \emptyset$  die Abschätzung

$$\text{codim}((A \cap B) \subset E) \leq \text{codim}(A \subset E) + \text{codim}(B \subset E)$$

Die Kodimension des Schnitts ist also höchstens die Summe der Kodimensionen der sich schneidenden Teileräume.

*Vorschau 3.3.2.23.* In der kommutativen Algebra ?? können Sie lernen, wie man diese Abschätzung für die Kodimension eines Schnitts auf Nullstellenmengen polynomialer Gleichungssysteme verallgemeinern kann, wenn der Grundkörper algebraisch abgeschlossen ist. So etwas wie zwei Sphären im Raum, die sich in einem Punkt berühren, kann es also im Komplexen nicht geben: Da kann der Schnitt der Nullstellenmengen zweier Polynome in drei Variablen  $f, g \in \mathbb{C}[X, Y, Z]$  nie isolierte Punkte haben.

*Übung 3.3.2.24.* Eine Abbildung  $f : E \rightarrow F$  von affinen Räumen ist genau dann affin, wenn ihr Graph  $\Gamma(f) \subset E \times F$  ein affiner Teilraum des Produkts unserer beiden Räume ist.

### 3.3.3 Affine Räume und ihre Geraden

**Satz 3.3.3.1 (Charakterisierung affiner Abbildungen im Reellen).** Eine injektive Abbildung von einem mindestens zweidimensionalen reellen affinen Raum in einen weiteren reellen affinen Raum ist affin genau dann, wenn das Bild jeder Geraden wieder eine Gerade ist.

3.3.3.2. Dieselbe Charakterisierung gilt allgemeiner über jedem Grundkörper, dessen einziger Körperautomorphismus die Identität ist. Wir diskutieren mehr dazu in 3.3.3.5.

**3.3.3.3 (Bezug zum schmutzigen Raum unserer Anschauung).** Die affinen Geraden des Raums unserer Anschauung denke ich mir als Sichtlinien: Drei Punkte liegen auf einer Geraden genau dann, wenn man sich so hinstellen kann, daß man sie hintereinander sieht. Der vorhergehende Satz 3.3.3.1 zeigt, daß im Fall reeller affiner Räume ab der Dimension Zwei die Kenntnis aller Geraden auch umgekehrt bereits die Struktur als reeller affiner Raum festlegt: Haben nämlich zwei Strukturen als affiner reeller Raum auf derselben Menge dieselben Geraden, und gibt es in besagtem Raum mehr als nur eine Gerade, so ist nach 3.3.3.1 die Identität auf unserer Menge ein Morphismus von affinen Räumen zwischen unserer Menge einmal mit der einen Struktur als affiner Raum und ein andermal mit der anderen Struktur als affiner Raum. Dann aber müssen diese beiden Strukturen bereits übereinstimmen. Anschaulich gesprochen legt also im Raum unserer Anschauung „die Kenntnis der Sichtlinien bereits fest, welche Abbildungen als Parallelverschiebungen anzusehen sind“. Explizit kann man das wie folgt einsehen: Zunächst legt die Kenntnis der Sichtlinien alias Geraden fest, welche Teilmengen die Bezeichnung als „Ebene“ verdienen; Dann vereinbart man, zwei Geraden „parallel“ zu nennen, wenn sie in einer Ebene liegen und sich nicht schneiden; Und schließlich kann man dann Parallelverschiebungen charakterisieren als diejenigen bijektiven Abbildungen, die jede Gerade bijektiv auf sich selbst oder aber bijektiv in eine parallele Gerade überführen. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist.

*Beweis.* Wir zeigen den Satz zunächst unter der Annahme, daß sowohl unser Ausgangsraum als auch der Raum, in den abgebildet wird, beide die Dimension Zwei haben. Ohne Beschränkung der Allgemeinheit dürfen wir dann annehmen, daß es sich bei beiden Räumen um den  $\mathbb{R}^2$  handelt, und indem wir unsere Abbildung noch mit einer geeigneten Verschiebung verknüpfen, dürfen wir sogar annehmen, daß sie den Ursprung festhält. Diesen Fall behandeln wir als eigenständiges Lemma.

**Lemma 3.3.3.4.** *Eine injektive Abbildung  $\Phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  mit  $\Phi(0) = 0$ , unter der das Bild jeder affinen Geraden wieder eine affine Gerade ist, muß linear sein.*

*Beweis.* Indem wir eine geeignete lineare Abbildung dahinterhalten, dürfen daß wir ohne Beschränkung der Allgemeinheit annehmen, daß unser  $\Phi$  die Vektoren  $e_1$  und  $e_2$  der Standardbasis festhält. Unter dieser Zusatzannahme zeigen wir nun, daß  $\Phi$  sogar die Identität ist. Zunächst gibt es sicher Abbildungen  $\psi_1, \psi_2 : \mathbb{R} \rightarrow \mathbb{R}$  mit  $\Phi(ae_i) = \psi_i(a)e_i$ . Da wir  $\Phi$  injektiv angenommen haben, müssen unter  $\Phi$  parallele alias sich nicht schneidende Geraden parallel bleiben. Die Gerade durch

$a\mathbf{e}_1$  und  $a\mathbf{e}_2$  für  $a \neq 0, 1$  ist parallel zu der durch  $\mathbf{e}_1$  und  $\mathbf{e}_2$ , also ist für  $a \neq 0, 1$  auch die Gerade durch  $\Phi(a\mathbf{e}_1) = \psi_1(a)\mathbf{e}_1$  und  $\Phi(a\mathbf{e}_2) = \psi_2(a)\mathbf{e}_2$  parallel zu der durch  $\Phi(\mathbf{e}_1) = \mathbf{e}_1$  und  $\Phi(\mathbf{e}_2) = \mathbf{e}_2$ . Es folgt  $\psi_1(a) = \psi_2(a)$  für  $a \neq 0, 1$ . Für  $a = 0, 1$  ist das eh klar und wir notieren diese Abbildung nun  $\psi := \psi_1 = \psi_2$ . Natürlich gilt  $\psi(0) = 0$  und  $\psi(1) = 1$ . Da man die Addition von linear unabhängigen Vektoren durch Parallelogramme darstellen kann, gilt  $\Phi(v + w) = \Phi(v) + \Phi(w)$  falls  $v$  und  $w$  linear unabhängig sind. Wir erhalten für  $a \in \mathbb{R}$  damit

$$\Phi(\mathbf{e}_1 + a\mathbf{e}_2) = \mathbf{e}_1 + \psi(a)\mathbf{e}_2$$

wegen der linearen Unabhängigkeit im Fall  $a \neq 0$  und im Fall  $a = 0$  wegen  $\psi(0) = 0$ . Daraus folgt sofort die Erste der beiden Gleichungen

$$\begin{aligned}\Phi(\mathbf{e}_1 + (a+b)\mathbf{e}_2) &= \mathbf{e}_1 + \psi(a+b)\mathbf{e}_2 \\ \Phi(\mathbf{e}_1 + a\mathbf{e}_2 + b\mathbf{e}_2) &= \mathbf{e}_1 + \psi(a)\mathbf{e}_2 + \psi(b)\mathbf{e}_2\end{aligned}$$

Die Zweite folgt hier, indem wir ohne Beschränkung der Allgemeinheit  $b \neq 0$  annehmen und erst den letzten Summanden abspalten. Es folgt sofort  $\psi(a+b) = \psi(a) + \psi(b)$ . Da für  $a, b \in \mathbb{R}$  mit  $a \neq 0$  und  $b \neq 0, 1$  die Gerade durch  $\mathbf{e}_1$  und  $a\mathbf{e}_2$  parallel ist zu der durch  $b\mathbf{e}_1$  und  $ba\mathbf{e}_2$  folgt auch  $\psi(ba) = \psi(b)\psi(a)$  erst für alle  $a, b \neq 0, 1$ , dann aber wegen  $\psi(0) = 0$  und  $\psi(1) = 1$  sogar für alle  $a, b \in \mathbb{R}$ . Da nach ?? oder besser ?? die Identität der einzige Körperhomomorphismus  $\psi : \mathbb{R} \rightarrow \mathbb{R}$  ist, folgt  $\psi = \text{id}$ . Da wie bereits erwähnt gilt  $\Phi(v + w) = \Phi(v) + \Phi(w)$  falls  $v$  und  $w$  linear unabhängig sind, folgt sofort  $\Phi = \text{id}$ .  $\square$

Um nun Satz 3.3.3.1 zu zeigen, sei  $\Phi : E \hookrightarrow F$  unsere injektive Abbildung von reellen affinen Räumen, unter der das Bild jeder Geraden eine Gerade ist. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß  $E$  und  $F$  reelle Vektorräume sind und daß gilt  $\Phi(\vec{0}) = \vec{0}$ . Unter diesen stärkeren Annahmen zusammen mit der Annahme  $\dim E \geq 2$  folgern wir nun sogar die Linearität von  $\Phi$ . Gegeben  $v, w \in E$  linear unabhängig kann offensichtlich die von  $v$  und  $w$  aufgespannte Ursprungsebene dargestellt werden als die Vereinigung des Ursprungs mit allen affinen Geraden, die durch einen Punkt von  $\mathbb{R}v$  und einen Punkt von  $\mathbb{R}w$  laufen, so daß also in Formeln ausgedrückt gilt

$$\langle v, w \rangle = \bigcup_{u \in \mathbb{R}v, x \in \mathbb{R}w} \langle u, x \rangle_{\text{aff}}$$

Gegeben  $v, w \in E$  linear unabhängig müssen auch  $\Phi(v)$  und  $\Phi(w)$  linear unabhängig sein, da sonst die zwei verschiedenen Geraden  $\mathbb{R}v$  und  $\mathbb{R}w$  bijektiv auf dieselbe Gerade abgebildet würden im Widerspruch zur Injektivität von  $\Phi$ . Da  $\Phi$

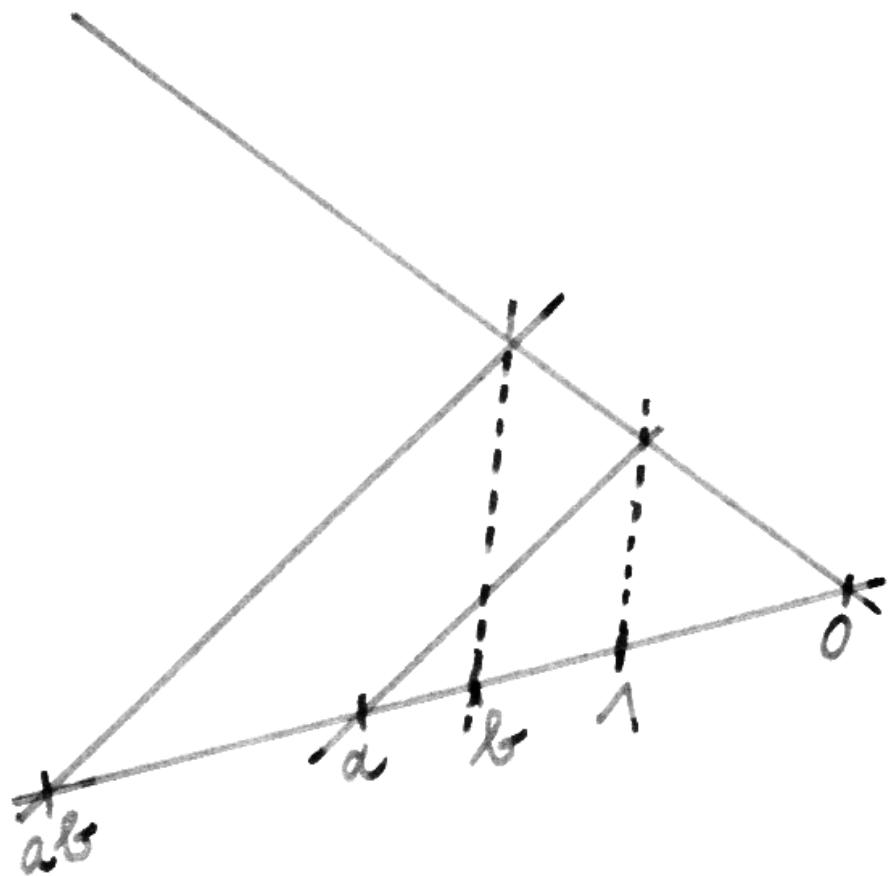
Geraden auf Geraden abbildet, folgt  $\Phi(\langle v, w \rangle) = \langle \Phi(v), \Phi(w) \rangle$ . Von der mithin von  $\Phi$  induzierten Bijektion

$$\Phi : \langle v, w \rangle \xrightarrow{\sim} \langle \Phi(v), \Phi(w) \rangle$$

wissen wir aber nun bereits, daß sie linear sein muß, daß also in Formeln ausgedrückt gilt  $\Phi(u + x) = \Phi(u) + \Phi(x)$  und  $\Phi(\lambda u) = \lambda\Phi(u)$  für alle  $u, x \in \langle v, w \rangle$  und  $\lambda \in \mathbb{R}$ . Da aber in einem Vektorraum der Dimension mindestens Zwei je zwei Vektoren  $u, x$  in einem gemeinsamen zweidimensionalen Teilraum liegen, zeigt das bereits die Linearität von  $\Phi$  selbst.  $\square$

*Ergänzung 3.3.3.5.* Geht man den Beweis von Lemma 3.3.3.4 nocheinmal durch, so erkennt man, daß er auch die folgende feinere Aussage zeigt: Sind  $K, L$  Körper und ist  $\Phi : K^2 \hookrightarrow L^2$  eine Injektion mit  $\Phi(0) = 0$ , unter der das Bild jeder affinen Geraden wieder eine affine Gerade ist, so ist  $\Phi$  ein Gruppenhomomorphismus und es gibt einen Körperisomorphismus  $\psi : K \xrightarrow{\sim} L$  mit  $\Phi(\lambda\vec{v}) = \psi(\lambda)\Phi(\vec{v})$  für alle  $\lambda \in K$  und  $\vec{v} \in K^2$ . Salopp gesprochen ist also unsere Abbildung  $\Phi$  „linear bis auf einen Körperisomorphismus“. Geht man den Beweis von Lemma 3.3.3.4 ein drittes Mal durch, so erkennt man, daß er dasselbe sogar zeigt für Schiefkörper  $K, L$  mit der Maßgabe, daß wir unter Geraden in  $K^2$  Teilmengen der Gestalt  $p + vK$  verstehen für  $p, v \in K^2$  mit  $v \neq 0$ .

*Ergänzung 3.3.3.6 (Von der Geometrie zur Algebra).* Geht man den Beweis von Satz 3.3.3.1 im Lichte von 3.3.3.5 nocheinmal durch, so erkennt man, daß er auch die folgende feinere Aussage zeigt: Haben zwei Strukturen  $(E, \vec{E}, a)$  und  $(E, \vec{E}', a')$  auf ein- und derselben Menge  $E$  als zweidimensionaler affiner Raum über Körpern  $K$  beziehungsweise  $K'$  dieselben Geraden, so gilt  $\vec{E} = \vec{E}'$  und es gibt genau einen Körperisomorphismus  $\varphi : K \xrightarrow{\sim} K'$  mit  $a(\lambda, \vec{v}) = a'(\varphi(\lambda), \vec{v})$  für alle  $\lambda \in K$  und  $\vec{v} \in \vec{E}$ . Flapsig gesagt kennt also ein weißes Blatt Papier zusammen mit einem Lineal bereits den Körper  $\mathbb{R}$  der reellen Zahlen! Gegeben eine Menge  $E$  von „Punkten“ und eine Teilmenge  $\mathcal{G} \subset \mathcal{P}(E)$  ihrer Potenzmenge, deren Elemente  $G \in \mathcal{G}$  „Geraden“ heißen, kann man auch eine Liste von geometrisch sinnvollen Forderungen angeben, die genau dann erfüllt sind, wenn unsere Menge  $E$  so mit der Struktur eines zweidimensionalen affinen Raums über einem Körper versehen werden kann, daß  $\mathcal{G}$  aus allen zugehörigen affinen Geraden besteht. Die einfachsten dieser Forderungen sind, daß durch je zwei verschiedene Punkte genau eine Gerade gehen soll und daß sich je zwei Geraden in höchstens einem Punkt schneiden. Die zusätzlichen Forderungen werden in ?? besprochen. In dieser Weise lassen sich die Körperaxiome 2.2.4.2 sogar geometrisch rechtferigen.



Wie man auf einer Gerade der Papierebene mit zwei verschiedenen als Null und Eins ausgezeichneten Punkten zwei beliebige Punkte multipliziert, wenn man nur ein Lineal zur Verfügung hat, das aber „unendlich lang“ ist in dem Sinne, daß man durch einen gegebenen Punkt die zu einer gegebenen Gerade parallele Gerade zeichnen kann.

### 3.3.4 Baryzentrische Koordinaten\*

3.3.4.1. Gegeben ein affiner Raum  $E$  über einem Körper  $K$  der Charakteristik Null  $\text{char } K = 0$  und eine nichtleere endliche Teilmenge  $\emptyset \neq T \subset E$  erklärt man den **Schwerpunkt**  $\text{Bar}(T)$  von  $T$  als den eindeutig bestimmten Punkt  $\text{Bar}(T) = s \in E$  mit

$$\sum_{e \in T} (e - s) = \vec{0}$$

Das ist gleichbedeutend dazu, daß für einen und jeden Punkt  $p \in E$  gilt

$$\sum_{e \in T} (e - p) = \sum_{e \in T} (e - p) - \sum_{e \in T} (e - s)$$

und mit offensichtlichen weiteren Umformungen sehen wir, daß es auch äquivalent ist zur Identität

$$\sum_{e \in T} (e - p) = |T|(s - p)$$

Daß zeigt einerseits die Eindeutigkeit des Schwerpunkts und andererseits auch dessen Existenz, da wir ja einen Schwerpunkt  $s$  von  $T$  finden können, indem wir von einem beliebigen Punkt  $p \in E$  ausgehen und  $s := p + |T|^{-1} \sum_{e \in T} (e - p)$  nehmen. Nach griechisch „βαρύς“ für „schwer“ heißt der Schwerpunkt auch das **Baryzentrum**.

3.3.4.2. Gegeben ein Körper  $K$ , ein affiner Raum  $E$  über  $K$ , Punkte  $e_0, \dots, e_n \in E$  und Skalare  $\lambda_0, \dots, \lambda_n \in K$  mit  $\lambda_0 + \dots + \lambda_n \neq 0$  erklärt man allgemeiner den **Schwerpunkt**

$$s = \text{Bar}((e_0, \lambda_0), \dots, (e_n, \lambda_n))$$

**der Punkte  $e_i$  mit den Gewichten  $\lambda_i$**  durch die Bedingung  $\sum_{i=0}^n \lambda_i(e_i - s) = \vec{0}$ . Ich lasse hier die Indize bei Null beginnen, um besonders deutlich zu machen, daß der Fall einer leeren Familie ausgeschlossen ist, auch wenn das unsere Bedingung  $\sum \lambda_i \neq 0$  bereits impliziert. Um die Existenz und Eindeutigkeit des Schwerpunkts mit Gewichten zu zeigen, prüft man wie zuvor für jeden Punkt  $p \in E$ , daß die Schwerpunkteigenschaft von  $s \in E$  gleichbedeutend ist zur Identität

$$\sum_{i=0}^n \lambda_i(e_i - p) = \left( \sum_{i=0}^n \lambda_i \right) (s - p)$$

Daraus folgt analog wie im Fall ohne Gewichte die Existenz und Eindeutigkeit.

3.3.4.3 (**Affines Erzeugnis als Menge von Schwerpunkten**). Gegeben eine nichtleere Teilmenge  $T \subset E$  eines affinen Raums kann ihr affines Erzeugnis offensichtlich beschrieben werden als die Menge aller Schwerpunkte zu gewichteten endlichen Teilmengen. Man erkennt das besonders leicht, indem man bei der zuvor gegebenen Beschreibung des Schwerpunkts  $p \in T$  wählt.

3.3.4.4 (**Eigenschaften des Schwerpunkts**). Offensichtlich bleibt der Schwerpunkt derselbe, wenn man alle Gewichte mit demselben von Null verschiedenen Körperelement  $\alpha \in K^\times$  multipliziert, in Formeln

$$\text{Bar}((e_0, \lambda_0), \dots, (e_n, \lambda_n)) = \text{Bar}((e_0, \alpha\lambda_0), \dots, (e_n, \alpha\lambda_n))$$

Offensichtlich bleibt der Schwerpunkt derselbe, wenn man Punkte mit Gewicht Null wegläßt. Offensichtlich hängt der Schwerpunkt auch im Fall einer nichtleeren gewichteten Punktfamilie nicht von der Reihenfolge ab. Wir können also sinnvoll

$$\text{Bar}((e_i, \lambda_i)_{i \in I})$$

erklären, wann immer  $(e_i, \lambda_i)_{i \in I}$  eine nichtleere Familie von gewichteten Punkten ist und nur für endlich viele  $i \in I$  gilt  $\lambda_i \neq 0$  und zusätzlich  $\sum_{i \in I} \lambda_i \neq 0$ .

**Definition 3.3.4.5.** Eine Teilmenge eines affinen Raums heißt **affin unabhängig**, wenn sie nicht leer ist und sich keiner ihrer Punkte als gewichteter Schwerpunkt von endlich vielen anderen ihrer Punkte schreiben läßt.

**Definition 3.3.4.6.** Eine Familie von Punkten eines affinen Raums heißt **affin unabhängig** oder ganz pedantisch **affin unabhängig als Familie**, wenn sie nicht leer ist und wenn sich für keinen Index der zugehörige Punkt als gewichteter Schwerpunkt der Punkte zu endlich vielen anderen Indizes schreiben läßt.

**Lemma 3.3.4.7 (Affine und lineare Unabhängigkeit).** *Gegeben eine nichtleere Teilmenge  $T$  eines affinen Raums  $E$  sind gleichbedeutend:*

1. *Die Menge  $T$  ist affin unabhängig;*
2. *Es gibt ein  $p \in T$  derart, daß die Menge der Vektoren  $\{t - p \mid t \in T \setminus p\}$  in  $\vec{E}$  linear unabhängig ist;*
3. *Für alle  $p \in T$  ist die Menge  $\{t - p \mid t \in T \setminus p\}$  in  $\vec{E}$  linear unabhängig.*

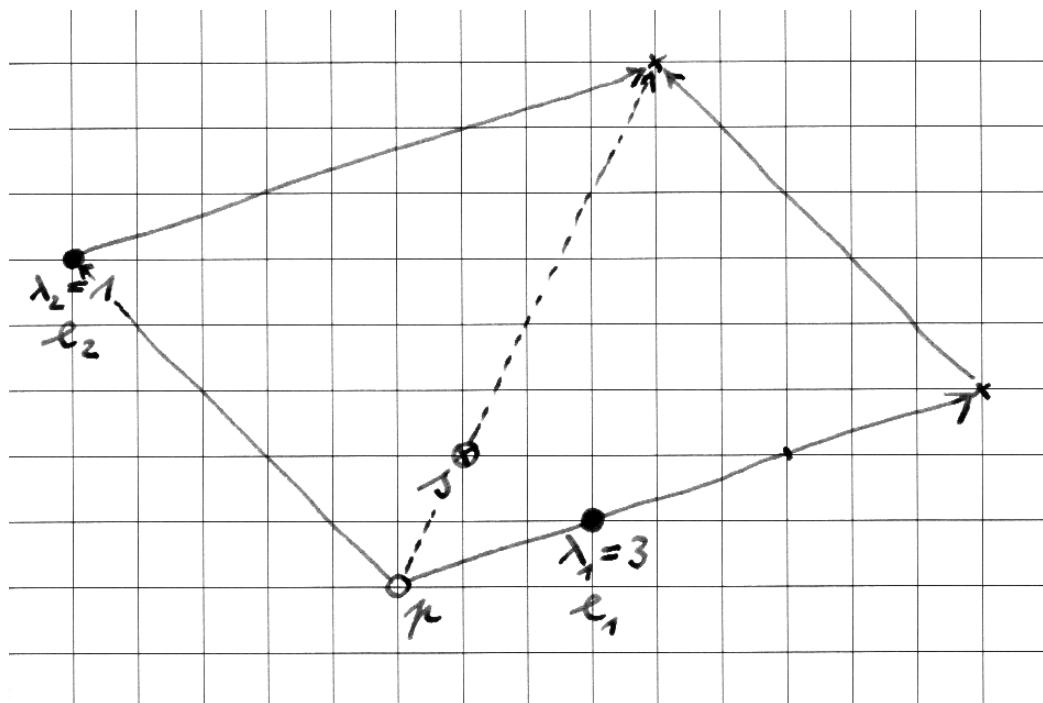
Analoges gilt für Familien.

*Beweis.* Übung. □

3.3.4.8. Sind  $e_0, \dots, e_n$  paarweise verschiedene Elemente einer endlichen affin unabhängigen Teilmenge eines affinen Raums  $E$ , so folgt aus

$$\text{Bar}((e_0, \lambda_0), \dots, (e_n, \lambda_n)) = \text{Bar}((e_0, \mu_0), \dots, (e_n, \mu_n))$$

bereits, daß es  $\alpha \in K^\times$  gibt mit  $\mu_i = \alpha\lambda_i \forall i$ . Läßt sich ein Punkt als gewichteter Schwerpunkt zu geeigneten Gewichten auf einer affin unabhängigen Teilmenge



Zwei fette Punkte der Gewichte 3 und 1 und ihr Schwerpunkt  $s$  nebst seiner Bestimmung mithilfe eines beliebigen weiteren Punktes  $p$ .

darstellen, so ist diese Darstellung mithin eindeutig, wenn wir zusätzlich Gesamtgewicht Eins fordern. Ist also in Formeln  $E$  ein affiner Raum und  $T \subset E$  ein affin unabhängiges Erzeugendensystem von  $E$ , so liefert das Bilden der gewichteten Schwerpunkte eine Bijektion

$$\begin{aligned} \{\sum a_t t \in KT \mid \sum a_t = 1\} &\xrightarrow{\sim} E \\ \sum a_t t &\mapsto \text{Bar}((t, a_t)_{t \in T}) \end{aligned}$$

Für  $p = \text{Bar}((t, a_t))$  heißen die  $a_t$  dann die **baryzentrischen Koordinaten von  $p$**  in Bezug auf unser affin unabhängiges Erzeugendensystem  $T$ .

### Übungen

*Übung 3.3.4.9.* Zeigen Sie, daß sich die drei Seitenhalbierenden eines Dreiecks in einem Punkt schneiden, dessen baryzentrische Koordinaten in Bezug auf die drei Ecken des Dreiecks jeweils  $(1/3)$  sind, und daß dieser Punkt alle drei Seitenhalbierenden in zwei Stücke teilt, von denen eines doppelt so lang ist wie das Andere. Kür: Rechnen Sie nach, daß dieser Punkt auch der Schwerpunkt des Dreiecks ist, wenn sie es aus Papier ausschneiden. Das braucht aber eher analytische Fertigkeiten.

*Übung 3.3.4.10.* Bestimmen Sie in  $\mathbb{R}^3$  die baryzenrischen Koordinaten des Punktes  $(1, 1, 1)$  in Bezug auf die drei Vektoren der Standardbasis und den Ursprung.

### 3.3.5 Lineare und affine Ungleichungen\*

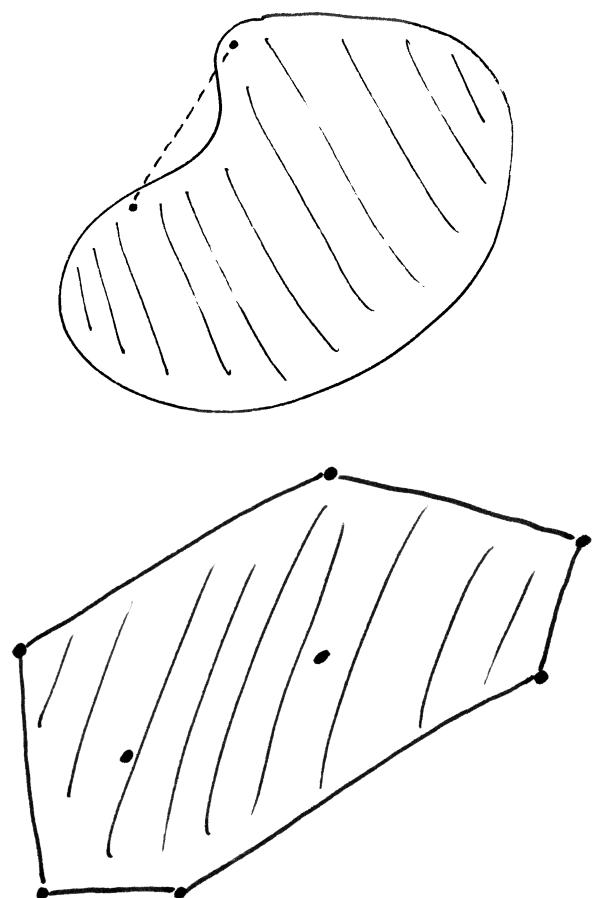
**Definition 3.3.5.1.** Gegeben Punkte  $p, q$  in einem affinen Raum  $E$  über einem angeordneten Körper schreiben wir

$$[p, q] := \{p + \lambda(q - p) \mid 0 \leq \lambda \leq 1\}$$

und nennen diese Menge im Fall  $p \neq q$  das die Punkte  $p$  und  $q$  verbindende **Geradensegment**.

**Definition 3.3.5.2.** Eine Teilmenge eines affinen Raums über einem angeordneten Körper heißt **konvex**, wenn sie mit je zwei Punkten auch das ganze diese verbindende Geradensegment enthält.

**Definition 3.3.5.3.** Sei  $E$  ein affiner Raum über einem angeordneten Körper. Offensichtlich ist der Schnitt einer beliebigen Familie konvexer Teilmengen von  $E$  wieder konvex. Gegeben eine Teilmenge  $T \subset E$  bezeichnet man die kleinste konvexe Teilmenge des fraglichen affinen Raums, die  $T$  umfaßt, auch als die **konvexe Hülle von  $T$** . Natürlich existiert solch eine kleinste konvexe Teilmenge, wir



Eine nicht konvexe Teilmenge der Ebene und eine endliche Teilmenge der Ebene, dargestellt durch fette Punkte, mit ihrer konvexen Hülle, dargestellt als schraffierter Bereich.

können sie etwa konstruieren als den Schnitt aller konvexen Teilmengen, die  $T$  umfassen. Wir verwenden für die konvexe Hülle von  $T$  die Notation

$$\text{konv}(T)$$

*Beispiel 3.3.5.4.* Gegeben zwei Punkte in einem affinen Raum über einem angeordneten Körper ist ihre konvexe Hülle genau das verbindende Geradensegment, in Formeln  $[p, q] = \text{konv}(p, q)$ .

**Definition 3.3.5.5.** Seien  $V$  ein Vektorraum über einem angeordneten Körper und  $T \subset V$  eine Teilmenge. Wir sagen, ein Vektor  $v \in V$  **lässt sich aus  $T$  positiv linear kombinieren**, wenn er eine Darstellung

$$v = \lambda_1 t_1 + \dots + \lambda_n t_n$$

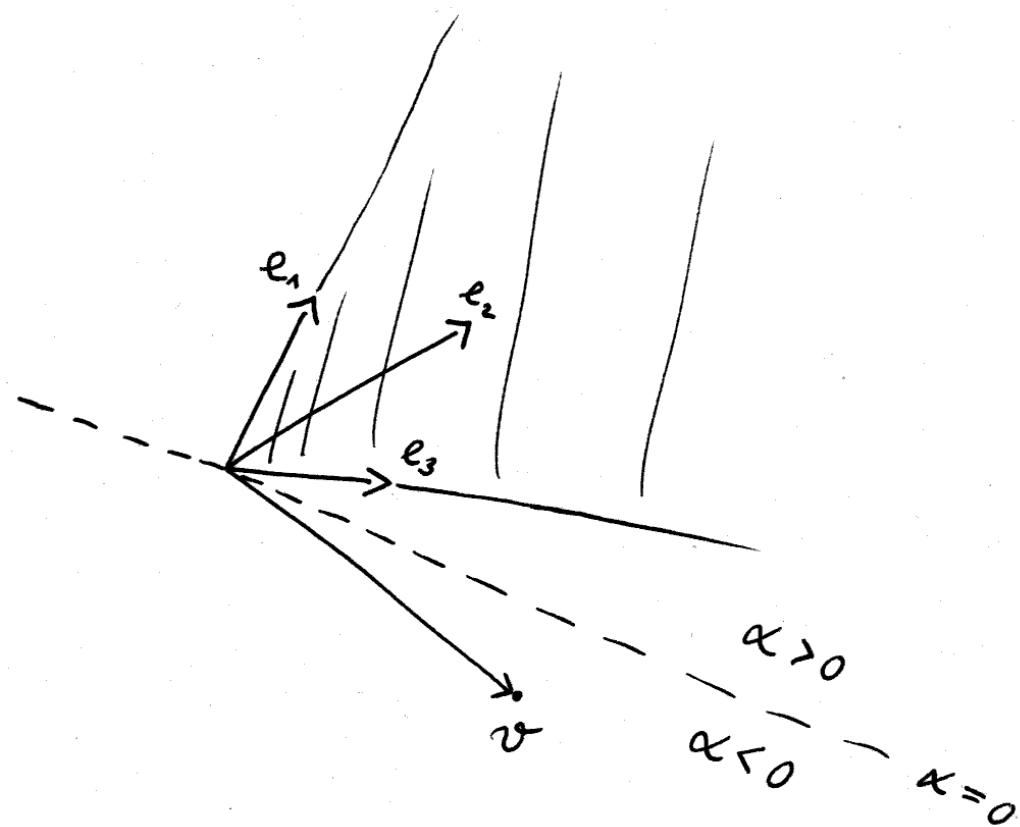
besitzt mit  $\lambda_i > 0$  und  $t_i \in T$  und  $n \geq 0$ . Die leere Linearkombination mit  $n = 0$  verstehen wir hier wie immer als den Nullvektor, der sich also in unseren Konventionen aus jeder Teilmenge positiv linear kombinieren lässt. Die Menge aller positiven Linearkombinationen aus Vektoren von  $T$  notieren wir  $\langle T \rangle_{>0}$ .

3.3.5.6. Zum Beispiel ist die Menge der aus der Standardbasis des  $\mathbb{R}^2$  positiv linear kombinierbaren Vektoren der abgeschlossene positive Quadrant: Die Punkte im Inneren erhalten wir mit  $n = 2$ , die vom Ursprung verschiedenen Punkte auf den Rändern mit  $n = 1$  und den Ursprung mit  $n = 0$ . Statt  $\alpha_i > 0$  hätten wir in der Definition also gleichbedeutend auch  $\lambda_i \geq 0$  schreiben können. Wenn wir aber im folgenden von einer **positiven Linearkombination** reden, so meinen wir stets positive und nicht etwa nur nichtnegative Koeffizienten.

**Proposition 3.3.5.7 (Satz von Caratheodory).** *Seien  $V \supset T$  ein Vektorraum über einem angeordneten Körper mit einer ausgezeichneten Teilmenge. Läßt sich ein Vektor  $v \in V$  aus  $T$  positiv linear kombinieren, so läßt er sich bereits aus einer linear unabhängigen Teilmenge von  $T$  positiv linear kombinieren.*

*Beweis.* Sei  $v = \lambda_1 v_1 + \dots + \lambda_n v_n$  eine Darstellung von  $v$  als positive Linearkombination von Elementen von  $T$ . Sie die  $v_i$  linear abhängig, so ist  $(\lambda_1, \dots, \lambda_n) \in k^n$  ein Punkt aus dem positiven Quadranten einer ganzen affinen Gerade von Lösungen. Der Punkt, an dem diese affine Gerade den positiven Quadranten verläßt, ist dann eine kürzere Darstellung von  $v$  als positive Linearkombination von Elementen von  $T$ .  $\square$

**Satz 3.3.5.8 (Hauptsatz über lineare Ungleichungen).** *Ist  $V$  ein Vektorraum über einem angeordneten Körper und  $T \subset V$  ein endliches Erzeugendensystem, so gilt für jeden Vektor  $v \in V$  genau eine der beiden folgenden Aussagen:*



Eine Menge  $T = \{e_1, e_2, e_3\}$  von drei Vektoren des Richtungsraums der Papierebene, die bis auf ihre Bezeichnung nichts mit der Standardbasis des  $\mathbb{R}^3$  zu tun haben, sowie ein Vektor  $v$  außerhalb der Menge ihrer positiven Linearkombinationen, der sich nach unserem Satz durch eine Hyperebene  $\ker \alpha$ , in diesem Fall die gestrichelt eingezeichnete Gerade, von unserer Menge aller positiven Linearkombinationen trennen lässt.

1. Der Vektor  $v$  läßt sich aus  $T$  positiv linear kombinieren;
2. Es gibt eine Linearform  $\alpha \in V^\top$  mit  $\alpha(t) \geq 0 \ \forall t \in T$  und  $\alpha(v) < 0$  und der Eigenschaft, daß  $\ker \alpha$  von seinem Schnitt mit  $T$  erzeugt wird.

3.3.5.9. Lassen wir in unserem Satz die Forderung fallen, daß die endliche Teilmenge  $T$  den Vektorraum  $V$  erzeugt, so können wir ihn immer noch auf das Erzeugnis von  $T$  anwenden und ein so gefundenes  $\alpha$  dann irgendwie linear auf ganz  $V$  fortsetzen. Wir können wir dann nur nicht mehr sicherstellen, daß  $\ker \alpha$  von seinem Schnitt mit  $T$  erzeugt wird.

3.3.5.10. Der Satz und der hier gegebene Beweis stammen von Weyl [Wey35]. Im Fall des Grundkörpers  $\mathbb{R}$  geht er bereits auf Farkas zurück und heißt mancherorts das **Lemma von Farkas**. Eine algorithmische Darstellung des Beweises und mehr zur praktischen Bedeutung unseres Satzes in der linearen Optimierung findet man in [Sch86].

3.3.5.11 (**Der Hauptsatz über lineare Ungleichungen in Koordinaten**). Spezialisieren wir den Satz oder genauer 3.3.5.9 zu  $V = \mathbb{R}^n$ , dessen Elemente wir als Spaltenvektoren auffassen, und besteht unsere endliche Menge  $T$  aus den  $m$  Spaltenvektoren einer Matrix  $A \in \text{Mat}(n \times m; \mathbb{R})$ , so folgt, daß für einen Spaltenvektor  $v = b = (b_1, \dots, b_n)^\top \in \mathbb{R}^n$  genau eine der folgenden Aussagen gilt:

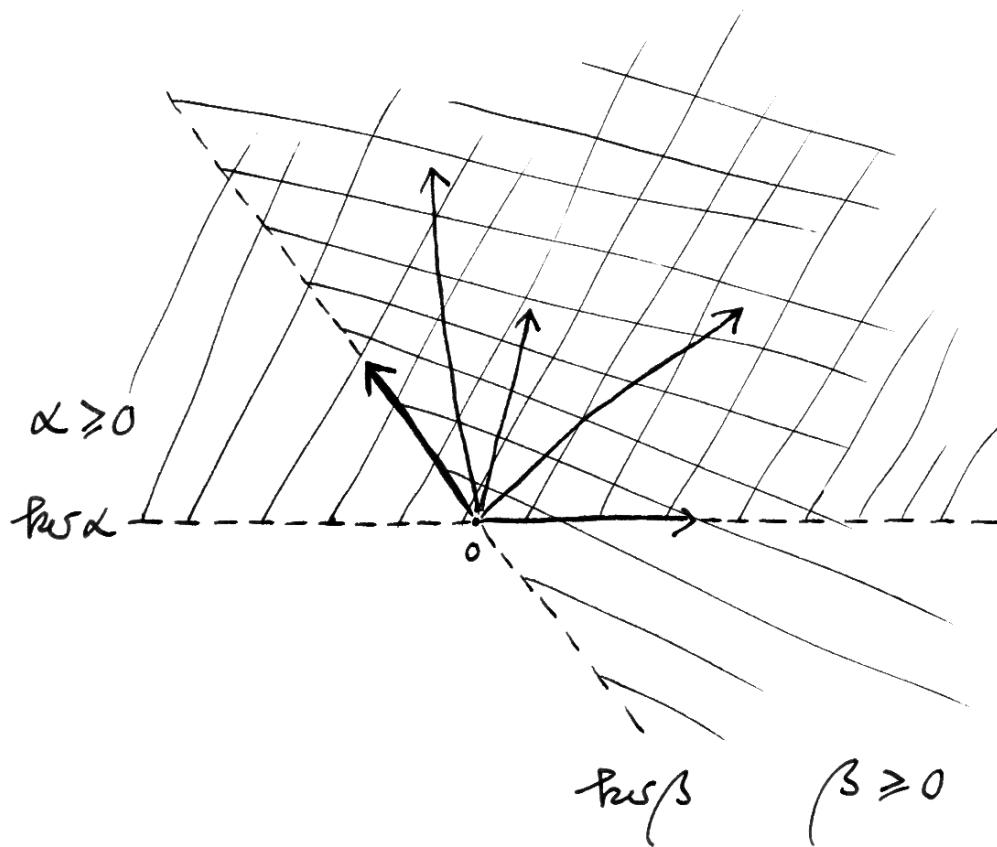
1. Es gibt einen Spaltenvektor  $x \in (\mathbb{R}_{\geq 0})^m$  mit  $b = Ax$ ;
2. Es gibt  $y = (y_1, \dots, y_n)^\top \in \mathbb{R}^n$  mit  $y^\top A \in (\mathbb{R}_{\geq 0})^m$  und  $y^\top b < 0$ .

Unser  $\alpha$  ist in diesem Fall der Zeilenvektor  $y^\top = (y_1, \dots, y_n)$ .

3.3.5.12 (**Variante zum Hauptsatz über lineare Ungleichungen**). Besteht unsere endliche Menge  $T$  aus den  $m$  Spaltenvektoren einer Matrix  $C \in \text{Mat}(n \times m; \mathbb{R})$  und ihren Negativen sowie den Vektoren der Standardbasis, so erhalten wir aus 3.3.5.8, daß für einen Spaltenvektor  $b = (b_1, \dots, b_n)^\top \in \mathbb{R}^n$  genau eine der folgenden Aussagen gilt:

1. Es gibt einen Spaltenvektor  $x \in \mathbb{R}^m$  mit  $Cx \leq b$  in dem Sinne, daß diese Ungleichung koordinatenweise richtig ist;
2. Es gibt  $y = (y_1, \dots, y_n)^\top \in (\mathbb{R}_{\geq 0})^n$  mit  $y^\top C = 0$  und  $y^\top b < 0$ .

*Beispiel* 3.3.5.13. Man denke sich einen Ikosaeder mit einer Ecke im Ursprung, und denke sich  $E$  als seine Eckenmenge. In diesem Fall hätte die Menge der positiven Linearkombinationen von Vektoren aus  $T$  die Gestalt eines eckigen Kegels mit fünf Flächen, die übrigends genau die Kerne der „extremen Stützen von  $T$ “ aus dem gleich folgenden Beweis sind.



Eine Menge von fünf Vektoren der Ebene, eingezeichnet als Pfeile, nebst der Menge aller positiven Linearkombinationen von Teilmengen unserer fünf Vektoren, eingezeichnet als der kreuzweise schraffierte Bereich, zu dem auch der gestrichelt eingezeichnete Rand hinzuzurechnen ist. Die beiden gestrichelt eingezeichneten Geraden sind die Kerne extremer Stützen, in diesem Fall gibt es bis auf Multiplikation mit positiven Skalaren genau zwei extreme Stützen. Einfach schraffiert die Bereiche, auf denen jeweils eine dieser extremen Stützen nichtnegativ ist.

**3.3.5.14 (Der Fall positiver Linearkombinationen unendlicher Mengen).** Gegeben eine Gerade in der Ebene  $\mathbb{R}^2$ , die die Menge der Punkte mit rationalen Koordinaten  $\mathbb{Q}^2$  nur im Nullpunkt trifft, betrachte man in  $\mathbb{Q}^2$  einen der beiden zugehörigen Halbraume mitsamt der Null. Dieser durch den Ursprung ergänzte Halbraum ist eine konvexe Teilmenge  $T$  von  $\mathbb{Q}^2$ , die von überhaupt keinem Punkt aus ihrem Komplement durch eine Gerade des  $\mathbb{Q}$ -Vektorraums  $\mathbb{Q}^2$  getrennt werden kann. Unser Hauptsatz über lineare Ungleichungen ist also für unendliches  $T$  im allgemeinen nicht mehr richtig. Betrachten wir jedoch abgeschlossene konvexe Kegel  $T$  im Sinne von 3.3.6.1 in reellen Banach-Räumen, so gibt es für jeden Vektor  $v$  im Komplement eine stetige Linearform, die auf besagtem Kegel nichtnegativ ist, auf dem Vektor aber negativ: Dieser Satz ist eine Variante der grundlegenden Trennungssätze aus der Funktionalanalysis, der sogenannten „Trennungssätze von Hahn-Banach“.

*Beweis.* Eine Linearform  $\alpha \in V^\top \setminus 0$  mit  $\alpha(t) \geq 0 \ \forall t \in T$  nennen wir eine **Stütze** von  $T$ . Wird zusätzlich  $\ker \alpha$  erzeugt von  $(\ker \alpha) \cap T$ , so nennen wir  $\alpha$  eine **extreme Stütze** von  $T$ . Wir notieren  $\text{Ex}(T) = \text{Ex}_V(T)$  die Menge der extremen Stützen von  $T$ . Der Satz behauptet in diesen Notationen

$$\langle T \rangle_{>0} = \{v \in V \mid \alpha(v) \geq 0 \ \forall \alpha \in \text{Ex}(T)\}$$

Die Inklusion  $\subset$  ist offensichtlich. Um auch  $\supset$  zu zeigen, argumentieren wir mit vollständiger Induktion über die Dimension. Im Fall  $\dim V = 0$  bestehen beide Seiten nur aus dem Nullvektor und unsere Aussage gilt. Im allgemeinen betrachten wir einen festen Vektor  $v \in V$  und zeigen

$$(\alpha(v) \geq 0 \ \forall \alpha \in \text{Ex}(T)) \Rightarrow v \in \langle T \rangle_{>0}$$

durch eine Fallunterscheidung mit der Induktionsannahme.

Erster Fall: Es gibt eine extreme Stütze  $\alpha \in \text{Ex}(T)$  mit  $\alpha(v) = 0$ . In diesem Fall wenden wir die Induktionsannahme auf  $(T \cap \ker \alpha) \subset \ker \alpha$  an. Dazu zeigen wir zunächst, daß jede extreme Stütze  $\beta \in \text{Ex}_{\ker \alpha}(T \cap \ker \alpha)$  Restriktion einer extremen Stütze  $\hat{\beta} \in \text{Ex}(T)$  ist. Sicher läßt sich ja  $\beta \in (\ker \alpha)^\top$  ausdehnen zu einer Linearform  $\tilde{\beta} \in V^\top$ . Dann muß  $\tilde{\beta} + \mu\alpha$  für hinreichend großes  $\mu$  eine Stütze von  $T$  sein und eine extreme Stütze von  $T$ , wenn wir  $\mu$  dabei kleinstmöglich wählen. Für dieses  $\mu$  ist  $\hat{\beta} = \tilde{\beta} + \mu\alpha$  die gesuchte Ausdehnung von  $\beta$  zu einer extremen Stütze von  $T$ . Insgesamt folgt mit der Induktionsannahme nun sogar  $v \in \langle T \cap \ker \alpha \rangle_{>0}$ .

Zweiter Fall: Es gibt keine extreme Stütze  $\alpha \in \text{Ex}(T)$  mit  $\alpha(v) = 0$ , aber es gibt zumindest überhaupt eine extreme Stütze  $\beta \in \text{Ex}(T)$ . In diesem Fall finden wir  $t \in T$  mit  $\beta(t) > 0$  und betrachten das größte  $\lambda \in k$  mit  $\alpha(v - \lambda t) \geq 0 \ \forall \alpha \in \text{Ex}(T)$ . Nach unseren Annahmen gibt es solch ein  $\lambda$  und es gilt  $\lambda > 0$

und  $v - \lambda t$  liegt im Kern einer extremen Stütze. Der bereits behandelte Fall liefert  $v - \lambda t \in \langle T \rangle_{>0}$  und es folgt sofort  $v \in \langle T \rangle_{>0}$ .

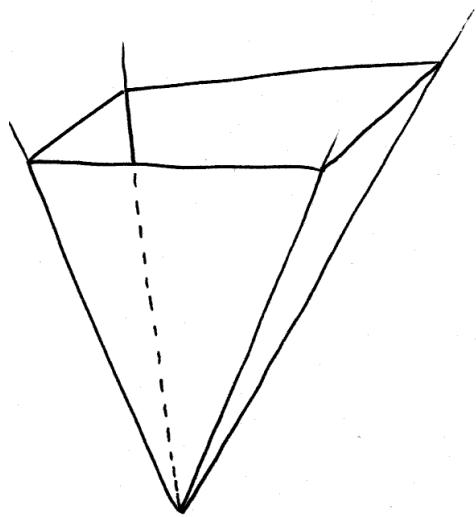
Dritter Fall: Unsere Menge  $T$  hat überhaupt keine extremen Stützen  $\text{Ex}(T) = \emptyset$ . In diesem Fall müssen wir  $\langle T \rangle_{>0} = V$  zeigen. Wir dürfen  $V \neq 0$  annehmen und wählen unter allen  $\alpha \in V^\top \setminus 0$  mit  $\ker \alpha = \langle T \cap \ker \alpha \rangle$  ein  $\alpha$  aus, für das die Kardinalität von  $T^+ = T^+(\alpha) := \{t \in T \mid \alpha(t) \geq 0\}$  größtmöglich wird. Nach Annahme finden wir dennoch ein  $t^- \in T$  mit  $\alpha(t^-) < 0$  und dürfen ohne Beschränkung der Allgemeinheit  $\alpha(t^-) = -1$  annehmen. Dann betrachten wir die Projektion  $\pi : v \mapsto v + \alpha(v)t^-$  von  $V$  auf  $\ker \alpha$  längs  $t^-$ . Hätte  $\pi(T^+)$  eine extreme Stütze  $\beta \in \text{Ex}_{\ker \alpha}(\pi(T^+))$ , so könnten wir diese durch die Vorschrift  $\hat{\beta}(t^-) = 0$  fortsetzen zu einer Linearform  $\hat{\beta} \in V^\top$  mit  $\hat{\beta}|T^+ \geq 0$  und  $\hat{\beta}(t^-) = 0$ . Dann wäre auch  $\ker \hat{\beta}$  erzeugt von seinem Schnitt mit  $T$ , im Widerspruch zur Wahl von  $\alpha$ . Also hat  $\pi(T^+)$  keine extreme Stütze und nach Induktionsvoraussetzung lässt sich jeder Vektor aus  $\ker \alpha$  positiv linear aus  $\pi(T^+)$  kombinieren. Also lässt sich jedes  $v \in V$  schon mal aus  $T$  linear kombinieren unter der Einschränkung, daß nur der Koeffizient vor  $t^-$  negativ sein darf. Weiter gibt es aber auch mindestens ein  $t^+ \in T$  mit  $\alpha(t^+) > 0$ , sonst wäre ja  $-\alpha$  eine extreme Stütze von  $T$ . Schreiben wir  $-t^+$  in unserer eingeschränkten Weise und wenden  $\alpha$  an, so erkennen wir, daß der Koeffizient von  $t^-$  positiv sein muß. Nach geeigneter Umformung stellen wir  $-t^-$  dar als positive Linearkombination von Elementen von  $T^+$ . Damit lässt sich nun offensichtlich jeder Vektor aus  $V$  positiv linear aus  $T$ , ja sogar aus  $T^+ \cup \{t^-\}$  kombinieren.  $\square$

**Proposition 3.3.5.15 (Satz von Caratheodory im Affinen).** *Ist  $E \supset T$  ein affiner Raum über einem angeordneten Körper  $k$  mit einer ausgezeichneten Teilmenge, so liegt jeder Punkt aus der konvexen Hülle von  $T$  bereits in der konvexen Hülle einer endlichen affin unabhängigen Teilmenge von  $T$ .*

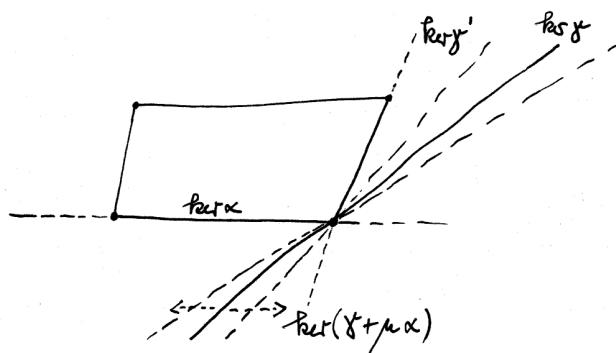
*Beweis.* Jeder Punkt  $p \in \text{konv}(T)$  der konvexen Hülle von  $T$  lässt sich schreiben als Schwerpunkt einer nichtleeren endlichen Teilmenge  $p_0, \dots, p_n$  mit positiven Gewichten  $\lambda_0, \dots, \lambda_n$  und  $\lambda_0 + \dots + \lambda_n = 1$ . Sind unsere Punkte affin abhängig, so gehört diese Lösung sogar zu einer ganzen affinen Gerade von Lösungen  $(\lambda_0, \dots, \lambda_n) \in k^{n+1}$ , also von Tupeln mit der Summe Eins und mit

$$p = \text{Bar}((p_i, \lambda_i))$$

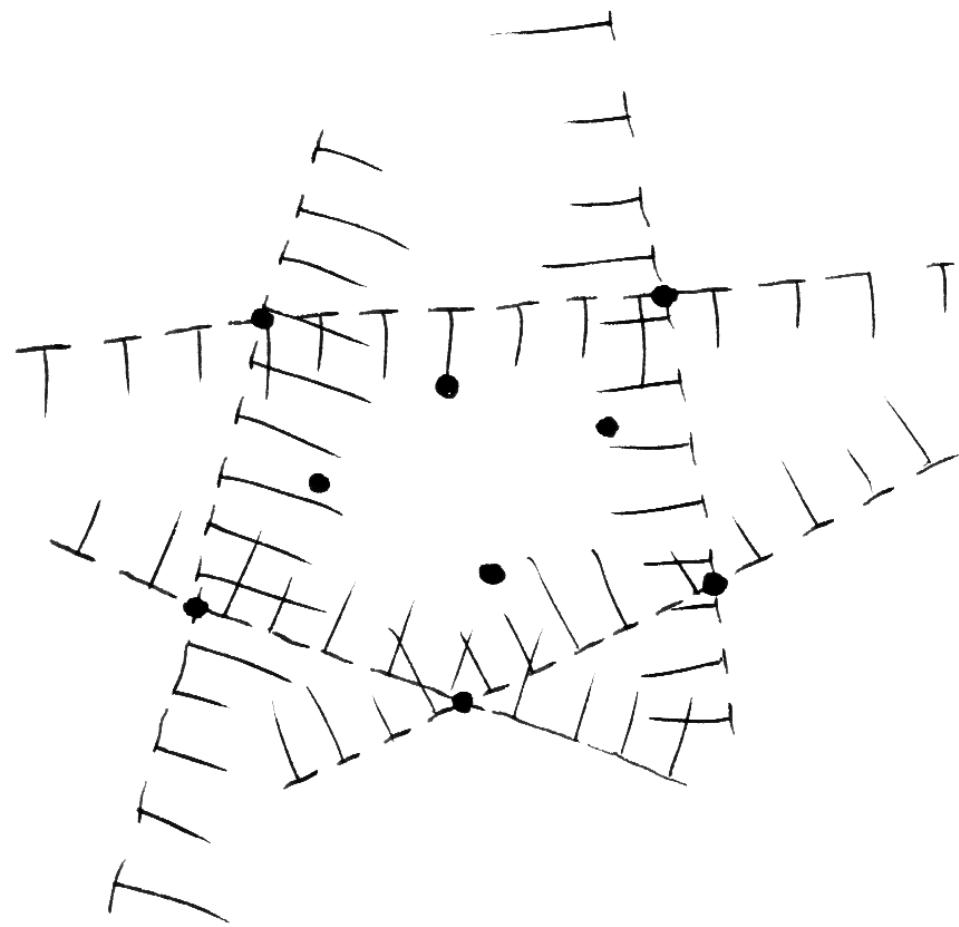
Die Stelle, an der unsere affine Gerade den positiven Quadranten  $(k_{>0})^{n+1}$  verläßt, ist dann eine Darstellung von  $p$  als Schwerpunkt einer kleineren endlichen Teilmenge mit positiven Gewichten.  $\square$



Ein Kegel im Raum mit vier  $\mathbb{R}_{>0}$ -Bahnen von extremen Stützen, deren Kerne von den vier Flächen unseres Kegels erzeugt werden. Die obere viereckige Fläche habe ich nur eingezeichnet, um das Bild plastischer aussehen zu lassen.  
Unser  $\ker \alpha$  aus dem Beweis ist die Vorderfläche.



Ein Schnitt durch obige Figur, der zeigen soll, wie man im Beweis die fortgesetzte extreme Stütze  $\gamma$  in  $\ker \alpha$  zu einer extremen Stütze  $\gamma'$  verwackelt.



Eine Menge von neun Punkten der affinen Ebene, eingezeichnet als fette Punkte, nebst ihrer konvexen Hülle, einem unregelmäßigen Fünfeck, zu dem auch der gestrichelt eingezeichnete Rand hinzuzurechnen ist. Man erkennt, daß dieses Fünfeck wie in 3.3.5.17 besprochen in der Tat genau der Schnitt derjenigen „abgeschlossenen Halbebenen“ ist, die unsere neun Punkte umfassen und deren „begrenzende Hyperebene“, in unserem Fall jeweils eine der gestrichelt eingezeichneten Geraden, von ihrem Schnitt mit  $T$  affin erzeugt wird.

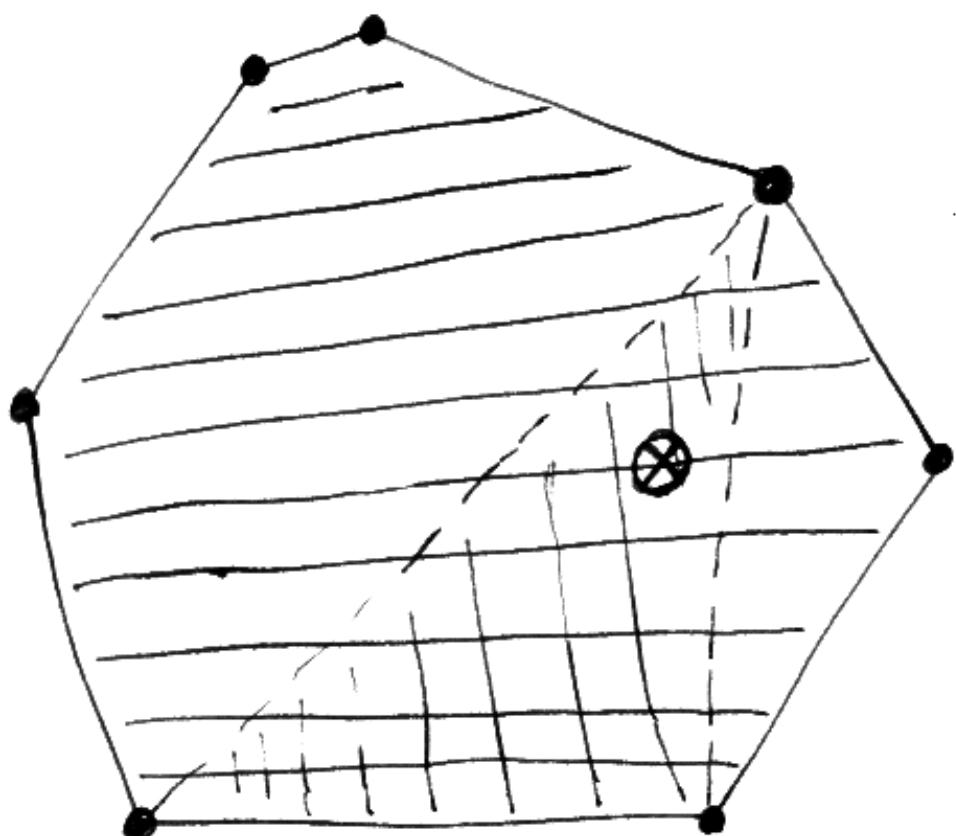


Illustration zum Satz von Caratheodory. Die konvexe Hülle der sieben fetten Punkte  $T$  ist das schraffierte Siebeneck, und jeder Punkt aus diesem Siebeneck liegt in der Tat auf einem Dreieck, dessen drei Ecken Ecken unseres Siebenecks sind.

**Korollar 3.3.5.16 (Hauptsatz über affine Ungleichungen).** Ist  $T$  ein endliches Erzeugendensystem eines affinen Raums  $E$  über einem angeordneten Körper  $k$ , so gilt für jedes  $p \in E$  genau eine der beiden folgenden Aussagen:

1. Der Punkt  $p$  liegt in der konvexen Hülle von  $T$ ;
2. Es gibt eine affine Abbildung  $\alpha : E \rightarrow k$  mit  $\alpha(e) \geq 0 \forall e \in T$  und  $\alpha(p) < 0$  und der Eigenschaft, daß die Nullstellenmenge von  $\alpha$  von ihrem Schnitt mit  $T$  erzeugt wird.

3.3.5.17. Ist also  $E$  ein affiner Raum über einem angeordneten Körper und  $T \subset E$  eine endliche Teilmenge, die unseren affinen Raum erzeugt, so ist die konvexe Hülle von  $T$  anschaulich gesprochen genau der Schnitt aller abgeschlossenen Halbräume, die  $T$  umfassen und deren begrenzende Hyperebene von ihrem Schnitt mit  $T$  erzeugt wird. Diese Formulierung ist meiner Anschauung besonders gut zugänglich.

3.3.5.18. Eine Teilmenge eines affinen Raums über einem angeordneten Körper, die die konvexe Hülle einer endlichen Teilmenge ist, heißt ein **Polytop** oder genauer ein **konvexes Polytop**. Eine Teilmenge eines affinen Raums über einem angeordneten Körper, die man als Schnitt einer endlichen Familie abgeschlossener Halbräume schreiben kann, heißt ein **Polyeder** oder genauer ein **konvexer Polyeder**. In einem endlichdimensionalen affinen Raum über einem angeordneten Körper ist in dieser Terminologie nach unserem Hauptsatz über affine Ungleichungen jedes Polytop ein Polyeder.

3.3.5.19. Die Terminologie, die bei Wikipedia angegeben wird, ist etwas anders. Insbesondere wird dort von Polytopen oder Polyedern nicht a priori die Konvexität gefordert.

*Beweis.* Wir identifizieren unseren affinen Raum mit einer affinen nichtlinearen Hyperebene in einem Vektorraum. Das Korollar folgt dann unmittelbar aus dem Hauptsatz über lineare Ungleichungen 3.3.5.8.  $\square$

### 3.3.6 Endlich erzeugte Kegel\*

**Definition 3.3.6.1.** Ein **Kegel** in einem Vektorraum  $V$  über einem angeordneten Körper  $k$  ist eine Teilmenge  $C \subset V$ , die den Ursprung enthält und stabil ist unter der Multiplikation mit nichtnegativen Skalaren. Einen konvexen Kegel nennen wir einen **Konvexkegel**. Ein Kegel, der keine Gerade umfaßt, heißt ein **spitzer Kegel**.

3.3.6.2. Auf Englisch sagt man **cone** für „Kegel“ und **strongly convex cone** für „spitzer Konvexkegel“.

3.3.6.3. Ein Teilmenge  $C$  in einem Vektorraum  $V$  über einem angeordneten Körper  $k$  ist genau dann ein Konvexkegel, wenn sie den Ursprung enthält und stabil ist unter Addition und unter der Multiplikation mit nichtnegativen Skalaren. In Formeln ausgedrückt kann ein Konvexkegel also charakterisiert werden als eine Teilmenge  $C \subset V$  mit den Eigenschaften  $0 \in C$  und  $v, w \in C \Rightarrow v + w \in C$  und  $v \in C \Rightarrow \lambda v \in C \forall \lambda \in k_{\geq 0}$ .

3.3.6.4. Natürlich ist jeder Schnitt von Kegeln wieder ein Kegel und jeder Schnitt von Konvexkegeln wieder ein Konvexkegel. Der kleinste Konvexkegel, der eine gegebene Menge von Vektoren umfaßt, heißt der von dieser Menge **erzeugte Konvexkegel**. Er besteht genau aus allen Vektoren, die sich aus unserer Menge positiv linear kombinieren lassen.

3.3.6.5. Man beachte den Unterschied zwischen dem von einer Menge erzeugten Kegel und dem von derselben Menge erzeugten Konvexkegel.

**Definition 3.3.6.6.** Gegeben eine Teilmenge  $T \subset V$  eines Vektorraums über einem angeordneten Körper definieren wir im Dualraum  $V^\top$  unseres Vektorraums ihre **Polarenmenge**  $T^\circ \subset V^\top$  durch die Vorschrift

$$T^\circ := \{\lambda \in V^\top \mid \lambda(e) \leq 1 \quad \forall e \in T\}$$

3.3.6.7. Die Polarenmenge eines Kegels  $C$  ist offensichtlich ein Konvexkegel und kann beschrieben werden durch die Formel

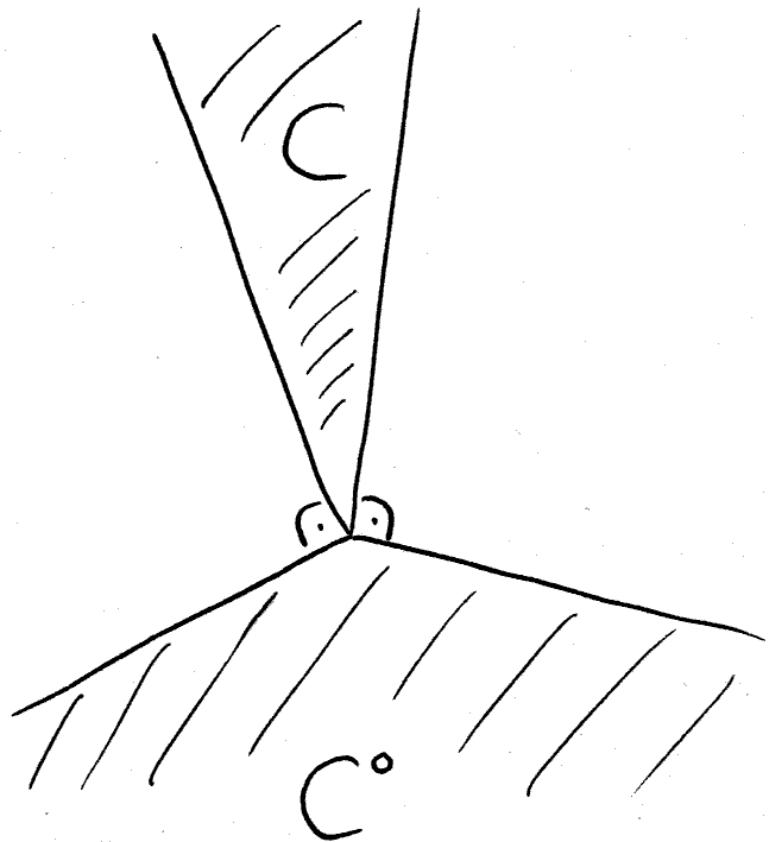
$$C^\circ = \{\lambda \in V^\top \mid \lambda(c) \leq 0 \quad \forall c \in C\}$$

Die Polarenmenge eines Kegels nennt man auch den **dualen Kegel**. Daß diese Terminologie sinnvoll ist, zeigt der folgende Satz.

**Satz 3.3.6.8 (von Farkas über duale Kegel).** *Ist  $C$  ein endlich erzeugter Konvexkegel in einem endlichdimensionalen Vektorraum  $V$  über einem angeordneten Körper, so ist auch seine Polarenmenge  $C^\circ \subset V^\top$  ein endlich erzeugter Konvexkegel und der kanonische Isomorphismus  $V \xrightarrow{\sim} V^{\top\top}$  induziert eine Bijektion*

$$C \xrightarrow{\sim} C^{\circ\circ}$$

3.3.6.9. Ein Konvexkegel in einem Vektorraum über einem angeordneten Körper heißt ein **polyedrischer Konvexkegel**, wenn er ein Polyeder ist, wenn er also als Schnitt endlich vieler abgeschlossener Halbräume geschrieben werden kann. In einem endlichdimensionalen Vektorraum über einem angeordneten Körper sind nach dem Satz von Farkas die endlich erzeugten Konvexkegel genau die polyedrischen Konvexkegel.



Ein Konvexkegel und sein dualer Kegel im Richtungsraum  $\vec{P}$  der Papierebene  $P$ , den wir dazu vermittels eines unter allen Kongruenzbewegungen invarianten Skalarprodukts  $\langle \cdot, \cdot \rangle$  durch  $\text{can} : \vec{P} \xrightarrow{\sim} \vec{P}^\top, v \mapsto \langle v, \cdot \rangle$  mit seinem Dualraum identifiziert haben, so daß wir erhalten

$$\text{can}^{-1}(C^\circ) = \{v \mid \langle v, c \rangle \leq 0 \ \forall c \in C\}$$

Ein Punkt der Papierebene stellt dabei denjenigen Richtungsvektor dar, der vom „Zentrum“ unseres Bildes zum entsprechenden Punkt schiebt.

*Beweis.* Wir identifizieren im folgenden  $V^{\top\top}$  und  $V$  mittels des kanonischen Isomorphismus. Für jede Teilmenge  $T \subset V$  gilt  $T \subset T^{\circ\circ}$  und für einen endlich erzeugten Konvexkegel  $C$  haben wir nach dem Hauptsatz über lineare Ungleichungen 3.3.5.8 auch  $C \supset C^{\circ\circ}$ , mithin  $C = C^{\circ\circ}$ . Es bleibt nur zu zeigen, daß auch  $C^\circ$  ein endlich erzeugter Konvexkegel ist. Wir zeigen dazu erst einmal, daß wir endlich viele Gleichungen  $\lambda_1, \dots, \lambda_r \in V^\top$  finden können mit

$$C = \{v \in V \mid \lambda_i(v) \geq 0 \quad \forall i\}$$

Sei in der Tat  $T \subset C$  ein endliches Erzeugendensystem unseres Konvexkegels  $C$ . Erzeugt  $T$  schon ganz  $V$  als Vektorraum, so folgt unsere Behauptung aus dem Hauptsatz über lineare Ungleichungen 3.3.5.8, genauer seiner allerletzten Aussage. Andernfalls gilt es eben, geeignete Linearformen,  $\lambda_1, \dots, \lambda_s$  auf dem von  $C$  erzeugten Untervektorraum  $W$  zu wählen, diese auf  $V$  fortzusetzen, und noch genügend auf  $W$  verschwindende Linearformen hinzuzunehmen. Die Linearformen  $-\lambda_1, \dots, -\lambda_r \in V^\top$  erzeugen nun per definitionem einen Konvexkegel  $K \subset V^\top$  mit  $K^\circ = C$ , und wegen  $K = K^{\circ\circ} = C^\circ$  folgt, daß auch  $C^\circ$  endlich erzeugt ist.  $\square$

**Korollar 3.3.6.10 (Charakterisierungen spitzer Konvexkegel).** *Für einen endlich erzeugten Konvexkegel in einem endlichdimensionalen Vektorraum über einem angeordneten Körper sind gleichbedeutend:*

1. *Unser Konvexkegel ist spitz;*
2. *Es gibt eine Linearform auf unserem Vektorraum, die auf dem Konvexkegel mit Ausnahme des Ursprungs echt positiv ist;*
3. *Die Polarenmenge unseres Konvexkegels erzeugt den Dualraum unseres Vektorraums.*

3.3.6.11. Die Bedingung „endlich erzeugt“ ist hier wesentlich. Zum Beispiel wäre die Menge aller Punkte in  $\mathbb{Q}^2$  echt unterhalb der  $x$ -Achse mitsamt dem Ursprung ein spitzer Konvexkegel, dessen Polarenmenge nicht den ganzen Dualraum erzeugt.

*Beweis.* Für einen beliebigen Kegel  $C$  umfaßt  $C^\circ$  eine Gerade genau dann, wenn  $C$  nicht den ganzen Raum erzeugt. Mit 3.3.6.8 folgt  $(1) \Leftrightarrow (3)$ . Die Implikation  $(2) \Rightarrow (1)$  ist offensichtlich. Um schließlich  $(3) \Rightarrow (2)$  zu zeigen wählen wir nach 3.3.6.8 ein endliches Erzeugendensystem der Polarenmenge unseres Konvexkegels und betrachten die Summe seiner Elemente. Verschwindet diese Summe an einem Punkt des Kegels, so verschwinden dort überhaupt alle Linearformen auf unserem Vektorraum und damit ist besagter Punkt der Ursprung.  $\square$

### Übungen

*Übung 3.3.6.12 (Konvexe Hülle und Baryzentrum).* Gegeben ein affiner Raum  $E$  über einem angeordneten Körper und eine Teilmenge  $T \subset E$  ist die konvexe Hülle von  $T$  genau die Menge aller Schwerpunkte zu nichtleeren endlichen mit positiven Gewichten versehenen Teilmengen von  $T$ .

*Übung 3.3.6.13.* Man schreibe in Formeln und beweise: Ein System von endlich vielen homogenen linearen Ungleichungen über einem angeordneten Körper hat genau dann eine nichttriviale Lösung, wenn es keine nichttriviale lineare Abhängigkeit mit nichtnegativen Koeffizienten zwischen unseren Linearformen gibt.

*Übung 3.3.6.14 (Lineare Fortsetzung positivlinearer Abbildungen).* Gegeben ein Konvexkegel in einem Vektorraum über einem angeordneten Körper  $C \subset V$ , der den ganzen Vektorraum erzeugt, in Formeln  $V = \langle C \rangle$ , lässt sich jede Abbildung  $\varphi : C \rightarrow W$  in einen weiteren Vektorraum mit  $\varphi(v + w) = \varphi(v) + \varphi(w)$  sowie  $\varphi(\alpha v) = \alpha\varphi(v)$  für alle  $v, w \in C$  und  $\alpha > 0$  auf genau eine Weise zu einer linearen Abbildung  $V \rightarrow W$  fortsetzen. Wir nennen eine Abbildung  $\varphi : C \rightarrow W$  mit diesen Eigenschaften **positivlinear**.

*Ergänzende Übung 3.3.6.15 (Duale Kegel unter Körpererweiterung).* Seien  $K \supset k$  ein angeordneter Körper mit einem Teilkörper, den wir mit der induzierten Anordnung versehen. Sei  $V$  ein endlichdimensionaler  $k$ -Vektorraum,  $C \subset V$  ein endlich erzeugter Konvexkegel, und  $C_K \subset V_K$  der davon erzeugte Konvexkegel im zu Skalaren  $K$  erweiterten Vektorraum  $V_K = V \otimes_k K$ . So stimmt der duale Kegel zum Kegel  $C_K$  unter der kanonischen Identifikation  $(V_K)^\top \xrightarrow{\sim} (V^\top)_K$  überein mit dem Erzeugnis in  $(V^\top)_K$  des dualen Kegels  $C^\circ \subset V^\top$  von  $C$ . In Formeln gilt also

$$(C_K)^\circ = (C^\circ)_K$$

*Übung 3.3.6.16.* Gegeben eine Teilmenge  $T$  eines affinen Raums über einem angeordneten Körper  $k$  bezeichne  $\text{konv}(T)$  ihre konvexe Hülle. Ist  $T$  die Standardbasis des  $k^n$  und  $W \subset k^n$  ein affiner Teilraum, so zeige man, daß ein Punkt  $p$  extrem ist im Schnitt  $W \cap \text{konv}(T)$  genau dann, wenn er für mindestens eine Teilmenge  $T' \subset T$  der einzige Punkt von  $W \cap \text{konv}(T')$  ist.

*Übung 3.3.6.17.* Sei  $k$  ein angeordneter Körper. Gegeben Kegel  $C, D$  in einem  $k$ -Vektorraum gilt für die dualen Kegel offensichtlich  $(C + D)^\circ = C^\circ \cap D^\circ$ . Für endlich erzeugte Konvexkegel  $C, D$  in einem endlichdimensionalen  $k$ -Vektorraum  $V$  folgere man mit dem Satz 3.3.6.8 über duale Kegel

$$(C \cap D)^\circ = C^\circ + D^\circ$$

Gegeben endlich viele Linearformen  $\alpha_1, \dots, \alpha_n \in V^*$  hat insbesondere der Konvexkegel  $C := \{v \mid \alpha_i(v) \geq 0 \forall i\}$  als dualen Kegel  $C^\circ$  den Kegel aller negativen

Linearkombinationen der  $\alpha_i$ , in Formeln

$$C^\circ = \{\sum_i x_i \alpha_i \mid x_i \leq 0 \ \forall i\}$$

*Übung 3.3.6.18 (Starker Dualitätssatz der linearen Optimierung).* Ungleichungen zwischen Vektoren des  $\mathbb{R}^n$  oder  $\mathbb{R}^m$  sind im folgenden stets komponentenweise zu verstehen. Seien  $A \in \text{Mat}(n \times m; \mathbb{R})$  und  $b \in \mathbb{R}^n$  und  $c \in \mathbb{R}^m$  gegeben. Man zeige, daß für  $d \in \mathbb{R}$  gleichbedeutend sind:

1. Unser  $d$  ist das Maximum der linearen Funktion  $x \mapsto c^\top x$  auf der Menge  $\{x \in \mathbb{R}^m \mid Ax \leq b\}$ ;
2. Unser  $d$  ist das Kleinste aller  $\delta \in \mathbb{R}$  mit  $\{x \in \mathbb{R}^m \mid c^\top x \leq \delta\} \supset \{x \in \mathbb{R}^m \mid Ax \leq b\}$ ;
3. Unser  $d$  ist das Kleinste aller  $\delta \in \mathbb{R}$  mit  $\{(x, t) \in \mathbb{R}^{m+1} \mid (c^\top | -\delta)(\begin{smallmatrix} x \\ t \end{smallmatrix}) \leq 0\} \supset \{(x, t) \in \mathbb{R}^{m+1} \mid (\begin{smallmatrix} A & -b \\ 0 & -1 \end{smallmatrix})(\begin{smallmatrix} x \\ t \end{smallmatrix}) \leq 0\}$ ;
4. Unser  $d$  ist das Kleinste aller  $\delta \in \mathbb{R}$  mit  $\mathbb{R}_{\geq 0}(-c^\top | \delta) \subset \{(y^\top | \gamma)(\begin{smallmatrix} A & -b \\ 0 & -1 \end{smallmatrix}) \mid (y, \gamma) \in \mathbb{R}^{n+1}, (y, \gamma) \leq 0\}$ ;
5. Unser  $d$  ist das Kleinste aller  $\delta \in \mathbb{R}$ , für das  $y \geq 0$  und  $\gamma \geq 0$  existieren mit  $(-c^\top | \delta) = (-y^\top A | y^\top b + \gamma)$ ;
6. Unser  $d$  ist das Minimum der linearen Funktion  $y \mapsto y^\top b$  auf der Menge  $\{y \in \mathbb{R}^n \mid y \geq 0 \text{ und } c^\top = y^\top A\}$ .

Beim Übergang zwischen 3 und 4 benötigt man Übung 3.3.6.17, die anderen Übergänge sind elementar. Die Äquivalenz von 1 und 6 heißt der **starke Dualitätssatz**.

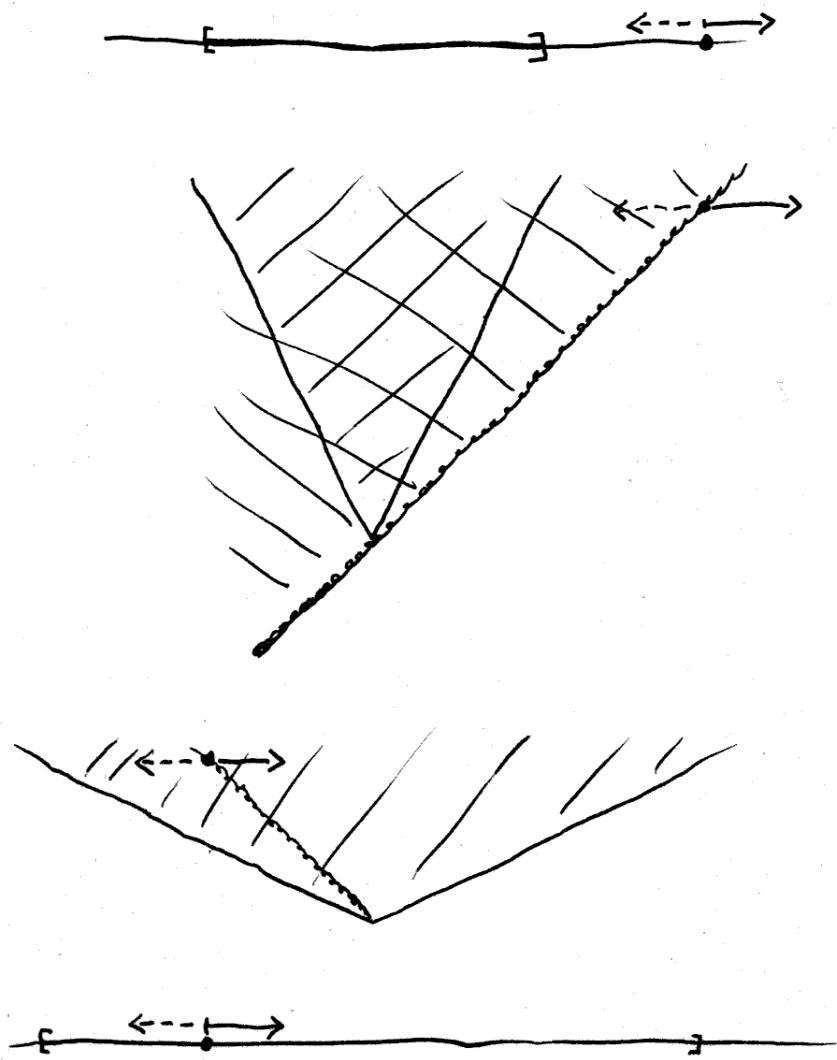


Illustration zum starken Dualitätssatz. Die Frage des Maximums wird übersetzt in eine Frage nach dem Enthaltensein von Kegeln und dualisiert durch Übergang zu den dualen Kegeln. Der duale Kegel zu einem Halbraum ist dabei ein Strahl.

## 3.4 Zahlen

### 3.4.1 Konstruktion der natürlichen Zahlen\*

3.4.1.1. Im folgenden diskutiere ich die Beschreibung der natürlichen Zahlen im Rahmen der naiven Mengenlehre. Eine vollständig überzeugende Diskussion dieser Struktur ist meines Erachtens nur im Rahmen der Logik möglich.

3.4.1.2. Führt man die Mengenlehre axiomatisch ein, so definiert man eine Menge als **unendlich**, wenn es eine injektive aber nicht bijektive Abbildung von unserer Menge in sich selbst gibt. Eine Menge heißt **endlich**, wenn sie nicht unendlich ist. Die Existenz einer unendlichen Menge ist eines der Axiome der Zermelo-Fraenkel-Mengenlehre, wir nennen es das **Unendlichkeitsaxiom**. Bei Zermelo und Fraenkel ist diese Axiomatik noch formaler und präziser, aber so weit gehen wir hier nicht.

3.4.1.3. Es ist klar, daß jede Menge mit einer unendlichen Teilmenge auch selbst unendlich sein muß. Es folgt, daß jede Teilmenge einer endlichen Menge wieder endlich ist. Es ist klar, daß eine unendliche Menge unendlich bleibt, wenn wir ihr ein Element wegnehmen: Wir können ja unsere injektive aber nicht bijektive Abbildung leicht so abändern, daß ein vorgegebenes Element auf sich selber abgebildet wird. Es folgt, daß die Vereinigung einer endlichen Menge mit einer einteiligen Menge wieder endlich ist.

*Ergänzung 3.4.1.4 (Maximale Elemente endlicher teilgeordneter Mengen).* Jede nichtleere endliche teilgeordnete Menge  $(E, \leq)$  besitzt mindestens ein maximales Element. Diese Erkenntnis haben wir bereits mehrfach als intuitiv klar verwendet, etwa im Beweis ?? der Tatsache, daß zwischen je zwei verschiedenen reellen Zahlen immer noch eine rationale Zahl liegt, oder beim Beweis des Basisexistenzsatzes für endlich erzeugte Vektorräume 3.1.6.16, aber das war noch vor der Formalisierung des Begriffs einer endlichen Menge. Etwas formaler können wir durch Widerspruch argumentieren. In der Tat könnten wir andernfalls eine Abbildung  $f : E \rightarrow E$  finden, die jedem Element ein echter größeres Element zuordnet. Halten wir dann  $a \in E$  fest, so erhalten wir eine injektive aber nicht surjektive Abbildung von  $\{x \in E \mid x \geq a\}$  zu sich selbst, und dieser Widerspruch zeigt die Behauptung.

- Satz 3.4.1.5 (Die natürlichen Zahlen).**
1. *Es gibt Paare  $(N, s)$  aus einer Menge  $N$  und einer injektiven Abbildung  $s : N \hookrightarrow N$  derart, daß  $N \setminus s(N)$  aus einem einzigen Element  $o$  besteht und daß jede  $s$ -stabile Teilmenge von  $N$ , die  $o$  enthält, bereits ganz  $N$  sein muß;*
  2. *Sei  $(N, s)$  solch ein Paar. Ist dann  $(X, x, f)$  ein Tripel bestehend aus einer Menge  $X$ , einem Element  $x \in X$  und einer Abbildung  $f : X \rightarrow X$ , so gibt es genau eine Abbildung  $\psi : N \rightarrow X$  mit  $\psi(o) = x$  und  $\psi s = f\psi$ ;*

3. Ein Paar  $(N, s)$  wie im ersten Teil ist im wesentlichen eindeutig bestimmt. Ist genauer  $(N', s')$  ein weiteres derartiges Paar und  $\{o'\} = N' \setminus s'(N')$ , so ist die eindeutig bestimmte Abbildung  $\psi : N \rightarrow N'$  mit  $s'\psi = \psi s$  und  $\psi(o) = o'$  eine Bijektion.

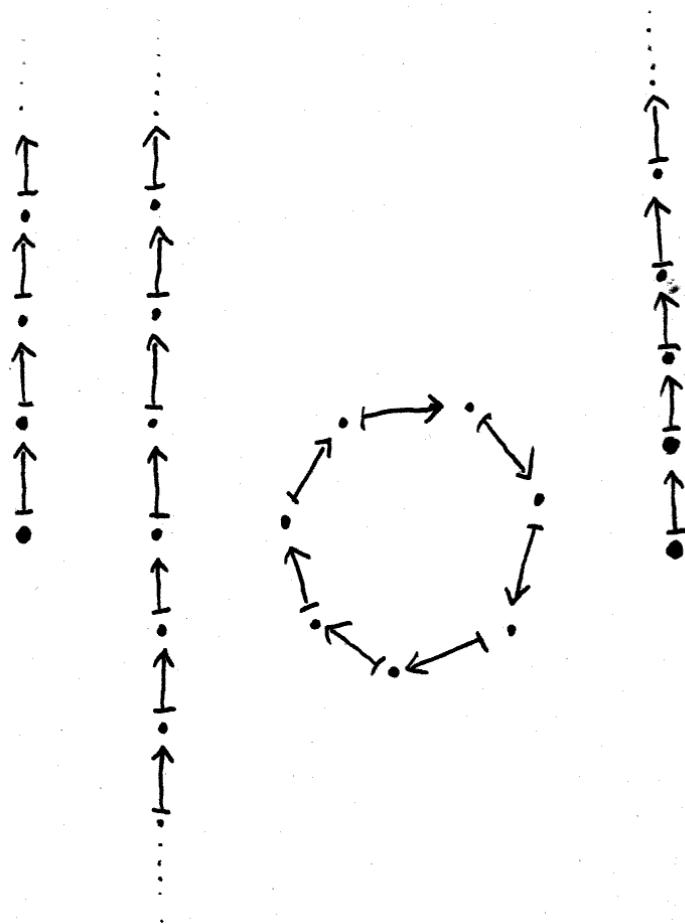
3.4.1.6. Sobald der Satz bewiesen ist, halten wir ein derartiges Paar ein für allemal fest, verwenden dafür die Notation  $(\mathbb{N}, s)$ , erlauben uns aufgrund der Eindeutigkeit den bestimmten Artikel und nennen  $\mathbb{N}$  die Menge der **natürlichen Zahlen**. Gegeben  $a \in \mathbb{N}$  heißt  $s(a)$  der **Nachfolger** oder genauer der **unmittelbare Nachfolger** von  $a$ . Die Notation  $s$  steht für „successor“. Wir vereinbaren für das eindeutig bestimmte Element von  $\mathbb{N}$ , das kein Nachfolger ist und daß oben  $o$  hieß, die Notation  $0 \in \mathbb{N}$  und die Bezeichnung **Null**.

3.4.1.7. Gegeben eine Menge  $X$  und zwei Abbildungen  $\psi, \phi : \mathbb{N} \rightarrow X$  mit  $\psi(0) = \phi(0)$  und  $(\psi(b) = \phi(b)) \Rightarrow (\psi(s(b)) = \phi(s(b)))$  folgt  $\psi = \phi$ . In der Tat bedeuten unsere Annahmen, daß die Teilmenge  $\{b \in \mathbb{N} \mid \psi(b) = \phi(b)\}$  das Element  $0 \in \mathbb{N}$  enthält und stabil ist unter  $s$  und also aufgrund der charakterisierenden Eigenschaft der natürlichen Zahlen ganz  $\mathbb{N}$  sein muß. Diese Umformulierung der Definition 3.4.1.6 heißt das **Prinzip der vollständigen Induktion**.

3.4.1.8. Die in diesem Satz gegebene Charakterisierung und im folgenden Beweis durchgeführte Konstruktion der natürlichen Zahlen gehen auf einen berühmten Artikel von Richard Dedekind zurück mit dem Titel „Was sind und was sollen die Zahlen?“. Eine alternative Charakterisierung besprechen wir in ??.

*Beweis.* 1. Nach dem Unendlichkeitsaxiom 3.4.1.2 finden wir eine Menge  $A$  nebst einer injektiven Abbildung  $s : A \hookrightarrow A$  und einem Element  $o \in A \setminus s(A)$ . Unter allen Teilmengen  $M \subset A$  mit  $o \in M$  und  $s(M) \subset M$  gibt es sicher eine kleinste, nämlich den Schnitt  $N$  aller derartigen Teilmengen. Für diese gilt dann notwendig  $N \subset \{o\} \cup s(N)$ , da die rechte Seite auch eine mögliche Teilmenge  $M$  mit unseren Eigenschaften ist. Da die andere Inklusion eh klar ist, folgt  $N = \{o\} \cup s(N)$ . So haben wir bereits ein mögliches Paar  $(N, s)$  gefunden.

2. Gegeben  $(X, x, f)$  wie oben betrachten wir die Gesamtheit aller Teilmengen  $G \subset N \times X$  mit  $(o, x) \in G$  und  $(n, y) \in G \Rightarrow (s(n), f(y)) \in G$ . Sicher gibt es eine kleinste derartige Teilmenge  $G_{\min} = \Gamma$ , nämlich den Schnitt aller möglichen derartigen Teilmengen  $G$ . Wir zeigen nun, daß  $\Gamma$  der Graph einer Funktion ist. Dazu betrachten wir die Teilmenge  $M$  aller  $m \in N$  derart, daß es genau ein  $y \in X$  gibt mit  $(m, y) \in \Gamma$ . Sicher gilt  $o \in M$ , denn gäbe es  $y \in X$  mit  $x \neq y$  und  $(o, y) \in \Gamma$ , so könnten wir  $(o, y)$  ohne Schaden aus  $\Gamma$  entfernen im Widerspruch zur Minimalität von  $\Gamma$ . Ist ähnlich  $m \in M$ , so zeigen wir in derselben Weise  $s(m) \in M$ . Also gilt  $M = N$  und  $\Gamma$  ist der Graph einer Funktion  $f : N \rightarrow X$  mit den gewünschten Eigenschaften. Finden wir eine weitere Funktion mit den



Versuch der graphischen Darstellung einer Menge mit einer injektiven aber nicht surjektiven Abbildung in sich selbst.

gewünschten Eigenschaften, so ist deren Graph auch ein mögliches  $G$  und wir folgern erst  $G \supset \Gamma$  und dann  $G = \Gamma$ .

3. Nach Teil 2 gibt es auch genau eine Abbildung  $\varphi : N' \xrightarrow{\sim} N$  mit  $s\varphi = \varphi s'$  und  $\varphi : o' \mapsto o$ . Nach Teil 2, diesmal der Eindeutigkeitsaussage, gilt dann  $\psi\varphi = \text{id}$  und  $\varphi\psi = \text{id}$ . Also ist unser  $\psi$  in der Tat eine Bijektion.  $\square$

3.4.1.9. In unseren natürlichen Zahlen  $(\mathbb{N}, s)$  erklären wir die **Eins** als den Nachfolger der Null und setzen in Formeln

$$1 := s(0)$$

3.4.1.10 (**Potenzen von Abbildungen**). Sei  $(X, x, f)$  ein Tripel bestehend aus einer Menge  $X$ , einem Element  $x \in X$  und einer Abbildung  $f : X \rightarrow X$ . Für die Werte der Abbildung  $\psi : \mathbb{N} \rightarrow X$  aus Teil 2 vereinbaren wir die Notation

$$f^n(x) := \psi(n)$$

Unser  $f^n(x)$  wird also in Formeln charakterisiert durch  $f^0(x) = x$  und  $f^{s(n)}(x) = f(f^n(x))$ . Indem wir es für alle  $x \in X$  betrachten, erhalten wir für alle  $n \in \mathbb{N}$  eine Abbildung

$$f^n : X \rightarrow X$$

Wir nennen  $f^n$  die  **$n$ -te Potenz von  $f$** . Per definitionem gilt  $f^0 = \text{id}$  und  $f^1 = f$ . Vollständige Induktion zeigt  $\text{id}^n = \text{id}$  für alle  $n$ .

**Lemma 3.4.1.11.** *Für alle  $n \in \mathbb{N}$  gilt  $n = s^n(0)$ .*

*Beweis.* Wir argumentieren mit vollständiger Induktion über  $n$ . Für  $n = 0$  sind beide Seiten 0 und die Behauptung stimmt. Gilt die Formel für ein  $n$ , so folgt  $s(n) = s(s^n(0)) = s^{s(n)}(0)$  mit der ersten Gleichung durch Anwenden von  $s$  und der zweiten nach der definitorischen Gleichung  $f(f^n(x)) = f^{s(n)}(x)$  für Potenzen 3.4.1.10. Damit ist unsere Behauptung bewiesen.  $\square$

3.4.1.12 (**Funktionalität von Potenzen**). Gegeben eine Abbildung  $h : X \rightarrow Y$  und Abbildungen  $f : X \rightarrow X$  sowie  $g : Y \rightarrow Y$  mit  $hf = gh$  gilt

$$hf^n = g^n h$$

für alle  $n \in \mathbb{N}$ . In der Tat reicht es, für alle  $x \in X$  die Identität  $hf^n(x) = g^n h(x)$  zeigen. Beide Seiten sind aber als Funktionen von  $n$  Abbildungen  $\psi : \mathbb{N} \rightarrow Y$  mit demselben Wert  $\psi(0) = h(x)$  für  $n = 0$  und derselben charakterisierenden Eigenschaft  $\psi s = g\psi$ . Für je zwei Selbstabbildungen  $f, g : X \rightarrow X$  einer Menge mit  $fg = gf$  folgern wir  $gf^a = f^a g$  und  $g^b f^a = f^a g^b$  für alle  $a, b \in \mathbb{N}$ .

**Definition 3.4.1.13.** Für die Menge der natürlichen Zahlen mit Nachfolgerabbildung  $(\mathbb{N}, s)$  aus 3.4.1.6 erklären wir die **Addition**  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ,  $(a, b) \mapsto a + b$  durch die Vorschrift

$$a + b := s^a(b)$$

3.4.1.14. Wir finden  $0 + b = s^0(b) = \text{id}(b) = b$  und  $1 + b = s^1(b) = s(b)$  für alle  $b \in \mathbb{N}$ . Andererseits finden wir  $b + 0 = s^b(0) = b$  nach 3.4.1.11.

**Lemma 3.4.1.15.** Die Addition natürlicher Zahlen ist eine kommutative Verknüpfung mit der Null als neutralem Element.

*Beweis.* Aus der Funktionalität von Potenzen 3.4.1.12 folgt  $s^a s^b = s^b s^a$  für alle  $a, b \in \mathbb{N}$ . Werten wir beide Seiten auf 0 aus, so erhalten wir mit 3.4.1.11 die Kommutativität  $s^a(b) = s^b(a)$ . Daß 0 ein neutrales Element ist alias die Identitäten  $0 + b = b = b + 0$  kennen wir bereits aus 3.4.1.14.  $\square$

**Lemma 3.4.1.16 (Produkt von Potenzen und Addition).** Gegeben eine Menge  $X$  und eine Abbildung  $f : X \rightarrow X$  und  $a, b \in \mathbb{N}$  gilt  $f^{a+b} = f^a f^b$ .

3.4.1.17. Es folgt, daß die Addition natürlicher Zahlen assoziativ ist, denn gegeben  $a, b, c \in \mathbb{N}$  finden wir  $s^{(a+b)+c} = (s^a s^b) s^c = s^a s^b s^c = s^a (s^b s^c) = s^{a+(b+c)}$  und Auswerten bei 0 liefert die Behauptung.

*Beweis.* Wir zeigen das durch vollständige Induktion über  $a$ . Im Fall  $a = 0$  ist es klar. Für den Induktionsschritt wenden wir  $f$  an und finden von der Mitte ausgehend

$$f^{s(a)+b} = f^{s(a+b)} = f f^{a+b} = f(f^a f^b) = (f f^a) f^b = f^{s(a)} f^b$$

Hier nutzen wir nach rechts die Assoziativität der Verknüpfung von Abbildungen und nach links die Identität  $s(a) + b = s^{s(a)}(b) = s(s^a(b)) = s(a + b)$ .  $\square$

**Satz 3.4.1.18 (Eigenschaften der Addition natürlicher Zahlen).** Die Menge der natürlichen Zahlen wird mit der Verknüpfung  $+$  ein kommutatives Monoid, in dem die **Kürzungsregel**  $(a + b = c + b) \Rightarrow (a = c)$  gilt sowie die Regel  $(a + b = 0) \Rightarrow (a = b = 0)$ .

*Beweis.* Kommutativität, neutrales Element und Assoziativität haben wir bereits in 3.4.1.15 und 3.4.1.17 erledigt. Was unsere Kürzungsregel angeht, enthält für  $a \neq c$  die Menge aller  $b$  mit  $a + b \neq c + b$  sicher  $b = 0$  und ist stabil unter  $s$ , enthält also alle  $b \in \mathbb{N}$ . Aus  $a + b = 0$  folgt zu guter Letzt  $a = 0$ , weil ja sonst die Null gar nicht im Bild der Abbildung  $(a+) : \mathbb{N} \rightarrow \mathbb{N}$  liegt, und dann folgt auch  $b = 0$  nach der Kürzungsregel.  $\square$

**Satz 3.4.1.19 (Anordnung auf den natürlichen Zahlen).** Sei  $(\mathbb{N}, s)$  die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus 3.4.1.6 und Addition aus 3.4.1.18. Die Relation  $\leq$  auf  $\mathbb{N}$  gegeben durch die Vorschrift

$$(a \leq b) \Leftrightarrow (\exists c \in \mathbb{N} \text{ mit } a + c = b)$$

ist eine Anordnung auf  $\mathbb{N}$ . Für diese Anordnung ist  $0 \in \mathbb{N}$  das kleinste Element und jede nichtleere Teilmenge von  $\mathbb{N}$  besitzt ein kleinstes Element.

*Beweis.* Bis auf die allerletzte Aussage folgt das alles leicht aus den in 3.4.1.18 gezeigten Eigenschaften der Addition. Ist nun  $A \subset \mathbb{N}$  eine Teilmenge ohne kleinstes Element, so ist  $\{n \in \mathbb{N} \mid n \leq a \ \forall a \in A\}$  stabil unter  $s$  und enthält die Null, ist also ganz  $\mathbb{N}$ , und es folgt  $A = \emptyset$ .  $\square$

**Satz 3.4.1.20 (Zählen endlicher Mengen).** Eine Menge  $X$  ist genau dann endlich, wenn es ein  $n \in \mathbb{N}$  und eine Bijektion  $\mathbb{N}_{<n} \xrightarrow{\sim} X$  gibt. Dies  $n$  ist dann wohlbestimmt und heißt die **Kardinalität** von  $X$  und wird  $n = |X|$  notiert.

*Beweis.* Daß es eine Injektion  $\mathbb{N}_{<a} \xrightarrow{\sim} \mathbb{N}_{<b}$  nur für  $a \leq b$  geben kann, zeigt man leicht durch Induktion. Das zeigt die Eindeutigkeit von  $n$ . Umgekehrt liefert das Zorn'sche Lemma ein maximales Paar bestehend aus einem  $a \in \mathbb{N} \sqcup \{\infty\}$  und einer injektiven Abbildung  $\mathbb{N}_{<a} \hookrightarrow X$ . Ist  $X$  endlich, so haben wir notwendig  $a \neq \infty$  und unsere maximale injektive Abbildung muß eine Bijektion  $\mathbb{N}_{<a} \xrightarrow{\sim} X$  gewesen sein.  $\square$

**Lemma 3.4.1.21 (Potenzen einer Verknüpfung kommutierender Abbildungen).** Gegeben Abbildungen  $f, g : X \rightarrow X$  mit  $fg = gf$  gilt für alle  $a \in \mathbb{N}$  die Identität  $(fg)^a = f^a g^a$ .

*Beweis.* Durch vollständige Induktion. Der Fall  $a = 0$  ist offensichtlich. Für den Induktionsschritt verwenden wir die Assoziativität der Verknüpfung von Abbildungen implizit, schalten wir  $fg$  auf beiden Seiten nach und entwickeln mit der Funktionalität von Potenzen 3.4.1.12 von der Mitte ausgehend

$$(fg)^{s(a)} = (fg)(fg)^a = fgf^a g^a = f f^a gg^a = f^{s(a)} g^{s(a)}$$

$\square$

**Lemma 3.4.1.22 (Iterierte Potenzen).** Gegeben eine Abbildung  $f : X \rightarrow X$  gilt für alle  $a, b \in \mathbb{N}$  die Identität

$$(f^a)^b = (f^b)^a$$

*Beweis.* Induktion über  $a$ . Der Fall  $a = 0$  ist offensichtlich. Für den Induktions-schritt schalten wir auf beiden Seiten  $f^b$  nach und finden von der Mitte ausgehend

$$(f^{s(a)})^b = (ff^a)^b = f^b(f^a)^b = f^b(f^b)^a = (f^b)^{s(a)}$$

Nach links haben wir dabei die Regel 3.4.1.21 für Potenzen einer Verknüpfung kommutierender Abbildungen verwendet. Das Kommutieren von  $f$  und  $f^a$  folgt aus der Funktionalität 3.4.1.12 von Potenzen.  $\square$

**Satz 3.4.1.23 (Multiplikation natürlicher Zahlen).** *Sei  $(\mathbb{N}, s)$  die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus 3.4.1.6 und bezeichne  $+$  ihre Addition aus 3.4.1.18. Die Verknüpfung*

$$(a, b) \mapsto ab = a \cdot b := (b+)^a(0)$$

*ist kommutativ mit neutralem Element dem Nachfolger  $1 = s(0)$  der Null. Weiter folgt aus  $a \neq 0$  und  $b \neq 0$  bereits  $ab \neq 0$ .*

**3.4.1.24 (Produkt mit Null).** Wir folgern  $a \cdot 0 = (0+)^a(0) = \text{id}^a(0) = \text{id}(0) = 0$  wegen der Neutralität von Null für die Addition und unseren Erkenntnissen 3.4.1.10 zu Potenzen der Identität.

*Beweis.* Per definitionem gilt  $(b+) = s^b$ , also  $ab = (b+)^a(0) = (s^b)^a(0)$ . Sind weder  $a$  noch  $b$  Null, so ist das ein echter Nachfolger der Null und folglich nicht Null. Die Kommutativität der Multiplikation erhalten wir, indem wir die Identität  $(s^a)^b = (s^b)^a$  aus 3.4.1.22 auf 0 anwenden. Um die Eins als neutral zu erkennen, erinnern wir  $(1+) = s$  aus 3.4.1.14 und rechnen  $a \cdot 1 = (1+)^a(0) = s^a(0) = a$ . Mit der Kommutativität der Multiplikation folgt, daß 1 in der Tat neutral ist für die Multiplikation.  $\square$

**Lemma 3.4.1.25 (Iterierte Potenzen und Multiplikation).** *Gegeben eine Abbildung  $f : X \rightarrow X$  und  $a, b \in \mathbb{N}$  gilt  $(f^a)^b = f^{ab}$ .*

*Beweis.* Induktion über  $a$ . Im Fall  $a = 0$  ist die Aussage klar wegen unseren Erkenntnissen  $f^0 = \text{id}$  und  $\text{id}^b = \text{id}$  aus 3.4.1.10 und dem Verschwinden des Produkts mit Null 3.4.1.24. Für den Induktionsschritt rechnen wir  $b+ab = (b+)((b+)^a(0)) = (b+)^{s(a)}(0) = s(a)b$  und damit

$$(f^{s(a)})^b = (f f^a)^b = f^b (f^a)^b = f^b f^{ab} = f^{b+ab} = f^{s(a)b}$$

nach Definition, der Regel für Potenzen von Verknüpfungen 3.4.1.21, der Induktionsannahme und der Regel für Produkte von Potenzen 3.4.1.16. Wir verwenden dabei implizit unsere stehende Vereinbarung „Punkt vor Strich“.  $\square$

**3.4.1.26 (Assoziativität der Multiplikation).** Gegeben  $a, b, c \in \mathbb{N}$  finden wir mit unserer Formel für iterierte Potenzen 3.4.1.25 von der Mitte ausgehend die Identität

$$s^{a(bc)} = (s^a)^{bc} = ((s^a)^b)^c = (s^{ab})^c = s^{(ab)c}$$

Wenden wir beide Seiten auf  $0 \in \mathbb{N}$  an, ergibt sich mit 3.4.1.11 wie gewünscht die Assoziativität der Multiplikation  $a(bc) = (ab)c$ . Unter der Multiplikation ist  $\mathbb{N}$  also ein kommutatives Monoid mit der Eins als neutralem Element.

3.4.1.27 (**Distributivgesetz**). Wir finden mit unseren Regeln zum Produkt von Potenzen 3.4.1.16 beziehungsweise zu iterierten Potenzen 3.4.1.25 die Identitäten

$$s^{ab+ac} = s^{ab}s^{ac} = (s^a)^b(s^a)^c = (s^a)^{b+c} = s^{a(b+c)}$$

Das Distributivgesetz  $ab + ac = a(b + c)$  ergibt sich, indem wir beide Seiten auf die Null anwenden und 3.4.1.11 beachten.

3.4.1.28. Zusammenfassend haben wir so auf unserer Menge mit Nachfolgerabbildung  $(\mathbb{N}, s)$  ein Element Null ausgezeichnet als das einzige Element, das kein Nachfolger ist, und ein Element Eins als dessen Nachfolger. Wir haben weiter auf  $\mathbb{N}$  eine Addition und Multiplikation eingeführt und gezeigt, daß beide assoziative und kommutative Verknüpfungen sind mit neutralen Elementen Null beziehungsweise Eins und daß das Distributivgesetz gilt.

3.4.1.29 (**Potenzgesetze**). Gegeben ein multiplikativ notiertes Monoid  $M$  und  $a \in \mathbb{N}$  erklären wir für jedes  $m \in M$  seine  **$a$ -te Potenz**

$$m^a := (m \cdot)^a(1_M)$$

als den Wert der  $a$ -ten Potenz der Linksmultiplikation mit  $m$  auf dem neutralen Element. Sie dürfen als Übung zeigen, daß es am Ergebnis nichts ändert, wenn wir stattdessen mit der Rechtsmultiplikation arbeiten. Im Spezialfall des Monoids  $\text{Ens}(X)$  aller Selbstabbildungen einer Menge erhalten wir unsere Potenzen von Selbstabbildungen aus 3.4.1.6 zurück. Gegeben ein multiplikativ notiertes Monoid  $M$  übersetzen sich unsere Regeln für das Potenzieren von Selbstabbildungen in die Regeln  $m^0 = 1_M$ ,  $m^1 = m$ ,  $m^{a+b} = m^a m^b$ ,  $(m^a)^b = m^{ab}$  und, im Fall von kommutierenden  $m, n \in M$ , die Zusatzregel  $(mn)^a = m^a n^a$  in unserem Monoid. Im Fall eines additiv notierten Monoids, das nach unseren Konventionen stets als kommutativ angenommen wird, erhalten wir dahingegen die Regeln  $0m = 0_M$ ,  $1m = m$ ,  $(a + b)m = am + bm$ ,  $b(am) = (ab)m$  und  $a(m + n) = am + an$ . All diese Regeln gelten insbesondere auch für  $\mathbb{N}$  selbst, auf dem wir ja sogar zwei Strukturen als kommutatives Monoid erklärt hatten, die additive und die multiplikative Struktur. Letztere Formeln hatten wir in diesem Fall auch bereits zuvor bereits gezeigt.

**Satz 3.4.1.30 (Teilen mit Rest).** Sei  $(\mathbb{N}, s)$  die Menge der natürlichen Zahlen mit Nachfolgerabbildung und Addition, Multiplikation und Anordnung wie in 3.4.1.23 und 3.4.1.19. Gegeben  $a, b \in \mathbb{N}$  mit  $b \neq 0$  gibt es eindeutig bestimmte  $c, d \in \mathbb{N}$  mit  $a = bc + d$  und  $d < b$ .

*Beweis.* Übung. □

3.4.1.31. Die Nachfolger von 0 notieren wir der Reihe nach 1, 2, 3, 4, 5, 6, 7, 8, 9 und nennen sie der Reihe nach **Eins, Zwei, Drei, Vier, Fünf, Sechs, Sieben,**

**Acht, Neun.** Den Nachfolger von Neun nennen wir **Zehn** und notieren ihn vorerst  $Z \in \mathbb{N}$ . Dann vereinbaren wir für  $a_0, a_1, \dots, a_r \in \{0, 1, \dots, 9\}$  die **Dezimaldarstellung**

$$a_r \dots a_1 a_0 := a_r Z^r + \dots + a_1 Z^1 + a_0 Z^0$$

So erhalten wir insbesondere für unsere natürliche Zahl Zehn die Dezimaldarstellung  $Z = 10 = 1Z^1 + 0Z^0$ . Wenn ganz allgemein eine endliche Folge der Symbole  $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$  ohne Punkt und Komma nebeneinandersteht und nichts anderes gesagt wird, ist davon auszugehen, daß eine natürliche Zahl in Dezimaldarstellung gemeint ist. In diesem Kontext dürfen Multiplikationssymbole natürlich nicht, wie sonst üblich, einfach weggelassen werden. Schließlich gilt es zu zeigen, daß jede natürliche Zahl eine eindeutig bestimmte Dezimaldarstellung hat mit  $r > 0 \Rightarrow a_r \neq 0$ , was wieder dem Leser zur Übung überlassen sei.

3.4.1.32 (**Zahldarstellungen**). Gegeben eine beliebige natürliche Zahl  $b > 1$  hat jede natürliche Zahl  $n$  genau eine Darstellung der Form

$$n = a_r b^r + \dots + a_1 b^1 + a_0 b^0$$

mit  $a_0, a_1, \dots, a_r \in \{0, 1, \dots, b - 1\}$  und  $r > 0 \Rightarrow a_r \neq 0$ . Wenn wir Symbole alias Ziffern für die Elemente dieser Menge vereinbaren, so können wir die Sequenz von Ziffern  $a_r \dots a_0$  als Darstellung der Zahl  $n$  interpretieren. Wir sagen dann auch, sie **stelle  $n$  im  $b$ -adischen System dar** und schreiben

$$a_r \dots a_0 = [a_r, \dots, a_0]_b = n$$

Wenn aber ganz links nicht eine Darstellung zur Basis zehn gemeint sein sollte, muß man das deutlich dazusagen. Das zehn-adische System heißt das **Dezimalsystem** und man spricht dann auch von der **Dezimaldarstellung** einer natürlichen Zahl und wir haben etwa

$$[2, 5, 5]_{10} = 255$$

Bei  $b \leq 10$  wählt man als Ziffern meist die ersten  $b$  üblichen Ziffern des Dezimalsystems. Das 2-adische System heißt das **Dualsystem** und man spricht dann auch von der **Binärdarstellung** einer natürlichen Zahl. So wäre

$$1010 = [1, 0, 1, 0]_2 = 2^3 + 2^1 = 10$$

die Darstellung der Zahl Zehn im Dualsystem, wo ganz links dazugesagt werden muß, daß 1010 als Binärdarstellung gemeint ist. Gebräuchlich sind auch Darstellungen im 16-adischen System alias **Hexadezimalsystem** mit den üblicherweise verwendeten Ziffern 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. So hätten wir zum Beispiel

$$\text{FF} = [\text{F}, \text{F}]_{16} = 15 \cdot 16 + 15 = 255$$

und müssen ganz links dazusagen, daß FF als Hexadesimaldarstellung gemeint ist. Wenn aber in so einer Ziffernfolge die ersten sechs Buchstaben des Alphabets als Großbuchstaben auftauchen, liegt der Verdacht einer Zahl in Hexadesimaldarstellung nahe.

### Übungen

*Übung 3.4.1.33.* Man zeige, daß gilt  $s(a) \neq a$  für alle  $a \in \mathbb{N}$ .

*Übung 3.4.1.34.* Man führe den Beweis für das Teilen mit Rest 3.4.1.30 aus.

*Übung 3.4.1.35.* Man zeige, daß die Vereinigung einer endlichen Menge mit einer einelementigen Menge wieder endlich ist. Man zeige durch vollständige Induktion über  $a$ , daß für alle  $a \in \mathbb{N}$  die Menge  $\mathbb{N}_{< a} := \{n \in \mathbb{N} \mid n < a\}$  endlich ist. Daß umgekehrt jede endliche Menge in Bijektion zu genau einer dieser Mengen ist, zeigen wir formal erst in ??, obwohl wir es natürlich schon oft verwendet haben und weiter verwenden müssen. Der Beweis ist nicht schwer, aber alles zu seiner Zeit.

*Übung 3.4.1.36.* Gegeben eine endliche Menge  $X$  und eine Abbildung  $f : X \rightarrow X$  und  $x \in X$  zeige man, daß es natürliche Zahlen  $n \neq m$  gibt mit  $f^n(x) = f^m(x)$ . Ist also  $X$  eine nichtleere endliche Menge und  $f : X \rightarrow X$  eine Abbildung, so gibt es  $y \in X$  und  $r \geq 1$  mit  $f^r(y) = y$ .

*Übung 3.4.1.37.* Gegeben eine Menge  $X$  und eine Abbildung  $f : \mathbb{N} \times X \rightarrow X$  und ein Element  $a \in X$  gibt es genau eine Folge  $\mathbb{N} \rightarrow X$ ,  $n \mapsto x_n$  mit  $x_0 = a$  und  $x_{n+1} = f(n, x_n) \forall n \in \mathbb{N}$ .

*Übung 3.4.1.38.* Gegeben ein multiplikativ notiertes Monoid  $M$  und  $a \in \mathbb{N}$  zeige man  $(m \cdot)^a(1_M) = (\cdot m)^a(1_M)$ .

*Übung 3.4.1.39.* Man zeige die Iterationsregeln 2.2.1.17 für Mengen mit einer assoziativen Verknüpfung.

## 3.4.2 Äquivalenzrelationen und ganze Zahlen

3.4.2.1. Unter einer **Relation**  $R$  auf einer Menge  $X$  verstehen wir wie in 3.1.4.2 eine Teilmenge  $R \subset X \times X$  des kartesischen Produkts von  $X$  mit sich selbst, also eine Menge von Paaren von Elementen von  $X$ . Statt  $(x, y) \in R$  schreiben wir in diesem Zusammenhang meist  $xRy$ .

**Definition 3.4.2.2.** Eine Relation  $R \subset X \times X$  auf einer Menge  $X$  heißt eine **Äquivalenzrelation**, wenn für alle Elemente  $x, y, z \in X$  gilt:

1. **Transitivität:**  $(xRy \text{ und } yRz) \Rightarrow xRz$ ;

2. **Symmetrie:**  $xRy \Leftrightarrow yRx$ ;

3. **Reflexivität:**  $xRx$ .

3.4.2.3. Ist eine Relation symmetrisch und transitiv und ist jedes Element in Relation zu mindestens einem weiteren Element, so ist unsere Relation bereits reflexiv. Ein Beispiel für eine Relation, die symmetrisch und transitiv ist, aber nicht reflexiv, wäre etwa die „leere Relation“  $R = \emptyset$  auf einer nichtleeren Menge  $X \neq \emptyset$ .

*Beispiel 3.4.2.4.* Gegeben eine Abbildung  $f : X \rightarrow Z$  erhalten wir eine Äquivalenzrelation auf  $X$  durch die Vorschrift  $(x \sim y) \Leftrightarrow (f(x) = f(y))$ . Die Äquivalenzklassen sind dann genau die nichtleeren Fasern von  $f$ . Wir werden demnächst zeigen, daß jede Äquivalenzrelation auf diese Weise beschrieben werden kann.

3.4.2.5. Gegeben eine Äquivalenzrelation  $\sim$  auf einer Menge  $X$  betrachtet man für  $x \in X$  die Menge  $A(x) := \{z \in X \mid z \sim x\}$  und nennt sie die **Äquivalenzklasse von  $x$** . Eine Teilmenge  $A \subset X$  heißt eine **Äquivalenzklasse** für unsere Äquivalenzrelation genau dann, wenn es ein  $x \in X$  gibt derart, daß  $A = A(x)$  die Äquivalenzklasse von  $x$  ist. Ein Element einer Äquivalenzklasse nennt man auch einen **Repräsentanten** der Klasse. Eine Teilmenge  $Z \subset X$ , die aus jeder Äquivalenzklasse genau ein Element enthält, heißt ein **Repräsentantensystem**. Aufgrund der Reflexivität gilt  $x \in A(x)$ , und man sieht leicht, daß für  $x, y \in X$  die folgenden drei Aussagen gleichbedeutend sind:

1.  $x \sim y$ ;
2.  $A(x) = A(y)$ ;
3.  $A(x) \cap A(y) \neq \emptyset$ .

3.4.2.6. Gegeben eine Äquivalenzrelation  $\sim$  auf einer Menge  $X$  bezeichnen wir die Menge aller Äquivalenzklassen, eine Teilmenge der Potenzmenge  $\mathcal{P}(X)$ , mit

$$(X/\sim) := \{A(x) \mid x \in X\}$$

und haben eine kanonische Abbildung  $\text{can} : X \rightarrow (X/\sim)$ ,  $x \mapsto A(x)$ . Diese kanonische Abbildung ist eine Surjektion und ihre Fasern sind genau die Äquivalenzklassen unserer Äquivalenzrelation.

3.4.2.7. Ist  $f : X \rightarrow Z$  eine Abbildung mit  $x \sim y \Rightarrow f(x) = f(y)$ , so gibt es nach der universellen Eigenschaft von Surjektionen 2.1.5.11 genau eine Abbildung  $\bar{f} : (X/\sim) \rightarrow Z$  mit  $f = \bar{f} \circ \text{can}$ . Wir zitieren diese Eigenschaft manchmal als die **universelle Eigenschaft des Raums der Äquivalenzklassen**. Sagt man, eine Abbildung  $g : (X/\sim) \rightarrow Z$  sei **wohldefiniert** durch eine Abbildung  $f : X \rightarrow Z$ , so ist gemeint, daß  $f$  die Eigenschaft  $x \sim y \Rightarrow f(x) = f(y)$  hat und daß man  $g = \bar{f}$  setzt.

3.4.2.8. Gegeben auf einer Menge  $X$  eine Relation  $R \subset X \times X$  gibt es eine kleinste Äquivalenzrelation  $T \subset X \times X$ , die  $R$  umfaßt. Man kann diese Äquivalenzrelation entweder beschreiben als den Schnitt aller Äquivalenzrelationen, die  $R$  umfassen, oder auch als die Menge  $T$  aller Paare  $(x, y)$  derart, daß es ein  $n \geq 0$  gibt und Elemente  $x = x_0, x_1, \dots, x_n = y$  von  $X$  mit  $x_\nu Rx_{\nu-1}$  oder  $x_{\nu-1}Rx_\nu$  für alle  $\nu$  mit  $1 \leq \nu \leq n$ . Wir nennen  $T$  auch die **von der Relation  $R$  erzeugte Äquivalenzrelation auf  $X$** .

*Beispiel 3.4.2.9.* Denken wir uns die Menge  $X$  als die „Menge aller Tiere“ und  $R$  als die Relation „können im Prinzip miteinander fruchtbaren Nachwuchs zeugen“, so wären die Äquivalenzklassen unter der von dieser Relation erzeugten Äquivalenzrelation eine mathematische Fassung dessen, was Biologen unter einer „Tierart“ verstehen würden.

*Beispiel 3.4.2.10.* Gegeben eine Menge  $X$  und eine Abbildung  $f : X \rightarrow X$  betrachten wir die von der Relation  $f(x) \sim x$  erzeugte Äquivalenzrelation. Man zeigt unschwer, daß sie explizit beschrieben werden kann durch

$$(x \sim y) \Leftrightarrow (\exists m, n \in \mathbb{N} \text{ mit } f^n(x) = f^m(y)).$$

*Beispiel 3.4.2.11.* Gegeben  $M \supset N$  ein kommutatives Monoid mit einem Untermonoid erhält man eine Äquivalenzrelation auf der Menge  $M \times N$  durch die Vorschrift

$$(a, s) \sim (b, t) \Leftrightarrow (\exists x \in N \text{ mit } atx = bsx)$$

Hier sind Symmetrie und Reflexivität offensichtlich. Um die Transitivität zu prüfen, müssen wir etwas rechnen: Gilt außerdem  $(b, t) \sim (c, r)$ , also  $bry = cty$  für ein  $y \in N$ , so folgt  $atxry = bsxry = ctysx$  und damit in der Tat  $(a, s) \sim (c, r)$ . Die Menge der Äquivalenzklassen notieren wir

$$N^{-1}M := (M \times N)/\sim$$

und notieren  $s \setminus a$  die Äquivalenzklasse von  $(a, s)$ . Man prüft, daß es auf  $N^{-1}M$  eine Verknüpfung gibt mit  $(s \setminus a)(t \setminus b) = (st \setminus ab)$  und daß  $N^{-1}M$  mit dieser Verknüpfung ein kommutatives Monoid wird und  $\text{can} : M \rightarrow N^{-1}M$  gegeben durch  $a \mapsto 1 \setminus a$  ein Monoidhomomorphismus, unter dem jedes  $s \in N$  auf ein invertierbares Element von  $N^{-1}M$  abgebildet wird. Offensichtlich ist  $\text{can}$  genau dann ein Injektion  $M \hookrightarrow N^{-1}M$ , wenn  $N$  aus kürzbaren Elementen von  $M$  besteht. Schließlich induziert das Vorschalten von  $\text{can}$  für jedes weitere Monoid  $L$  eine Bijektion

$$\text{Mon}(N^{-1}M, L) \xrightarrow{\sim} \{\varphi \in \text{Mon}(M, L) \mid \varphi(N) \subset L^\times\}$$

wir sagen, das Monoid  $N^{-1}M$  „gehe aus  $M$  durch formales Invertieren der Elemente von  $N$  hervor“. Im Spezialfall  $N = M$  ist insbesondere  $M^{-1}M$  stets eine Gruppe. Sie heißt die **einhüllende Gruppe** des kommutativen Monoids  $M$ .

3.4.2.12 (**Konstruktion des Rings der ganzen Zahlen**). Die einhüllende Gruppe unseres Monoids  $(\mathbb{N}, +)$  der natürlichen Zahlen aus 3.4.1.18 heißt die additive Gruppe

$$\mathbb{Z}$$

der **ganzen Zahlen**. Aufgrund der Kürzungsregel 3.4.1.18 ist die kanonische Abbildung in diesem Fall eine Injektion  $\mathbb{N} \hookrightarrow \mathbb{Z}$ . Man prüft leicht, daß wir auf  $\mathbb{Z}$  eine Anordnung erhalten durch die Vorschrift  $(a \leq b) \Leftrightarrow (\text{Es gibt } c \in \mathbb{N} \text{ mit } a+c = b)$ . Diese Anordnung hat die Eigenschaft  $(a \leq b) \Rightarrow (a+x \leq b+x)$  und  $\mathbb{N} = \mathbb{Z}_{\geq 0}$ . Nach 3.4.1.23 induziert unsere Multiplikation auf  $\mathbb{Z}_{\geq 0}$  eine Multiplikation auf  $\mathbb{Z}_{>0}$  und diese ist nach 3.4.1.27 distributiv über der Addition. Aus ?? folgt dann schließlich, daß sich unsere Multiplikation auf  $\mathbb{Z}_{>0}$  aus 3.4.1.23 auf eine und nur eine Weise zu einer kommutativen und über  $+$  distributiven Multiplikation auf  $\mathbb{Z}$  fortsetzen läßt. Von dieser Multiplikation ist a posteriori dann auch klar, daß sie unsere Multiplikation auf  $\mathbb{N} \supset \mathbb{Z}_{>0}$  fortsetzt. Wenn wir in 3.5.1.1 lernen, was ein „Ring“ ist, werden sich unsere ganzen Zahlen mit dieser Addition und Multiplikation als eines der ersten Beispiele für einen Ring erweisen.

*Ergänzung 3.4.2.13.* Gegeben Relationen  $R \subset X \times X$  und  $S \subset Y \times Y$  ist auch das Bild von  $(R \times S) \subset (X \times X) \times (Y \times Y)$  unter der durch Vertauschen der mittleren Einträge gegebenen Identifikation  $(X \times X) \times (Y \times Y) \xrightarrow{\sim} (X \times Y) \times (X \times Y)$  eine Relation. Wir notieren diese Relation auf dem Produkt kurz  $R \times S$ . Sind  $R$  und  $S$  Äquivalenzerelationen, so auch  $R \times S$ .

### Übungen

*Ergänzende Übung 3.4.2.14.* Ist  $G$  eine Gruppe und  $H \subset G \times G$  eine Untergruppe, die die Diagonale umfaßt, so ist  $H$  eine Äquivalenzrelation.

### 3.4.3 Untergruppen der Gruppe der ganzen Zahlen

**Definition 3.4.3.1.** Eine Teilmenge einer Gruppe heißt eine **Untergruppe**, wenn sie abgeschlossen ist unter der Verknüpfung und der Inversenbildung und zusätzlich das neutrale Element enthält. Ist  $G$  eine multiplikativ geschriebene Gruppe, so ist eine Teilmenge  $U \subset G$  also eine Untergruppe, wenn in Formeln gilt:  $a, b \in U \Rightarrow ab \in U, a \in U \Rightarrow a^{-1} \in U$  sowie  $1 \in U$ .

*Ergänzung 3.4.3.2.* Nach der reinen Lehre sollte eine Teilmenge einer Gruppe eine „Untergruppe“ heißen, wenn sie so mit der Struktur einer Gruppe versehen werden kann, daß die Einbettung ein Gruppenhomomorphismus wird. Da diese Definition jedoch für Anwendungen erst aufgeschlüsselt werden muß, haben wir gleich die aufgeschlüsselte Fassung als Definition genommen und überlassen den

Nachweis der Äquivalenz zur Definition nach der reinen Lehre dem Leser zur Übung.

*Beispiele 3.4.3.3.* In jeder Gruppe ist die einelementige Teilmenge, die nur aus dem neutralen Element besteht, eine Untergruppe. Wir nennen sie die **triviale Untergruppe**. Ebenso ist natürlich die ganze Gruppe stets eine Untergruppe von sich selber. Gegeben ein Vektorraum  $V$  ist die Menge aller Automorphismen eine Untergruppe  $\text{Aut}(V) \subset \text{Ens}^\times(V)$  der Gruppe aller Permutationen der zugrundeliegenden Menge.

**Satz 3.4.3.4 (Untergruppen der additiven Gruppe  $\mathbb{Z}$  der ganzen Zahlen).** *Jede Untergruppe  $H \subset \mathbb{Z}$  ist von der Form  $H = m\mathbb{Z}$  für genau ein  $m \in \mathbb{N}$ . Die Abbildungsvorschrift  $m \mapsto m\mathbb{Z}$  liefert mithin eine Bijektion*

$$\mathbb{N} \xrightarrow{\sim} \{H \subset \mathbb{Z} \mid H \text{ ist Untergruppe von } \mathbb{Z}\}$$

*Beweis.* Im Fall  $H = \{0\}$  ist  $m = 0$  die einzige natürliche Zahl mit  $H = m\mathbb{Z}$ . Gilt  $H \neq \{0\}$ , so enthält  $H$  echt positive Elemente. Sei dann  $m \in H$  das kleinste echt positive Element von  $H$ . Wir behaupten  $H = m\mathbb{Z}$ . Die Inklusion  $H \supset m\mathbb{Z}$  ist hier offensichtlich. Aber gäbe es  $n \in H \setminus m\mathbb{Z}$ , so könnten wir  $n$  mit Rest teilen durch  $m$  und also schreiben  $n = ms + r$  für geeignete  $s, r \in \mathbb{Z}$  mit  $0 < r < m$ . Es folgte  $r = n - ms \in H$  im Widerspruch zur Minimalität von  $m$ . Das zeigt die Surjektivität unserer Abbildung. Die Injektivität ist offensichtlich.  $\square$

3.4.3.5. Der Schnitt über eine beliebige Familie von Untergruppen einer gegebenen Gruppe ist selbst wieder eine Untergruppe. Für eine Teilmenge  $T$  einer Gruppe  $G$  definieren wir die **von  $T$  erzeugte Untergruppe**

$$\langle T \rangle \subset G$$

als die kleinste Untergruppe von  $G$ , die  $T$  umfaßt. Natürlich gibt es so eine kleinste Untergruppe, nämlich den Schnitt über alle Untergruppen von  $G$ , die  $T$  umfassen. Für  $T \neq \emptyset$  können wir  $\langle T \rangle$  konkret beschreiben als die Menge aller endlichen Produkte von Elementen aus  $T$  und deren Inversen. Für  $T = \emptyset$  besteht  $\langle T \rangle$  dahingegen nur aus dem neutralen Element. Ist  $T$  durch einen Ausdruck in Mengenklammern gegeben, so lassen wir diese meist weg und schreiben also zum Beispiel kürzer  $\langle a_1, \dots, a_n \rangle$  statt  $\langle \{a_1, \dots, a_n\} \rangle$ . Ob der Ausdruck  $\langle T \rangle$  in einem speziellen Fall die von einer Menge  $T$  erzeugte Untergruppe oder vielmehr die von der einelementigen Menge mit einzigm Element  $T$  erzeugte Untergruppe meint, muß der Leser meist selbst aus dem Kontext erschließen. Schreiben wir jedoch  $\langle !T \rangle$ , so ist stets zu verstehen, daß  $T$  eine Menge von Erzeugern und nicht einen einzelnen Erzeuger meint.

3.4.3.6. Ist  $V$  ein  $k$ -Vektorraum und  $T \subset V$  eine Teilmenge, so muß der Leser von nun an aus dem Kontext erschließen, ob mit  $\langle T \rangle$  die von  $T$  erzeugte Untergruppe oder der von  $T$  erzeugte Untervektorraum gemeint ist. Zur Unterscheidung schreiben wir manchmal  $\langle T \rangle_{\mathbb{Z}}$  für die von  $T$  erzeugte Untergruppe und  $\langle T \rangle_k$  für den von  $T$  erzeugten Untervektorraum.

### Übungen

*Ergänzende Übung 3.4.3.7.* Eine endliche nichtleere Teilmenge einer Gruppe, die mit je zwei Elementen auch die Verknüpfung der beiden enthält, ist notwendig bereits eine Untergruppe.

*Übung 3.4.3.8.* Sind  $H, K \subset G$  zwei Untergruppen einer Gruppe mit  $H \cap K = 1$ , so induziert die Verknüpfung eine Injektion  $H \times K \hookrightarrow G$ .

*Übung 3.4.3.9.* Wieviele Untergruppen hat die additive Gruppe eines zweidimensionalen Vektorraums über dem Körper mit zwei Elementen? Wieviele Untergruppen hat die additive Gruppe eines  $n$ -dimensionalen Vektorraums über dem Körper mit zwei Elementen?

*Ergänzende Übung 3.4.3.10.* Sei  $G$  eine Gruppe und  $\varphi : G \rightarrow G$  ein Gruppenhomomorphismus. Man zeige: Gilt für ein  $n \in \mathbb{N}$  die Gleichheit  $\ker \varphi^n = \ker \varphi^{n+1}$ , so folgt  $\ker \varphi^n = \ker \varphi^{n+1} = \ker \varphi^{n+2} = \dots$

*Übung 3.4.3.11.* Ist  $\varphi : G \rightarrow H$  ein Gruppenhomomorphismus, so gilt die Formel  $|G| = |\text{im } \varphi| \cdot |\ker \varphi|$ . Man bemerke, daß diese Formel im Fall linearer Abbildungen von Vektorräumen über endlichen Körpern äquivalent ist zur Dimensionsformel.

### 3.4.4 Primfaktorzerlegung

**Definition 3.4.4.1.** Eine **Primzahl** ist eine natürliche Zahl  $\geq 2$ , die sich nicht als das Produkt von zwei echt kleineren natürlichen Zahlen erhalten läßt.

*Beispiel 3.4.4.2.* Die Primzahlen unterhalb von 50 sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

3.4.4.3. Eine Möglichkeit, alle Primzahlen zu finden, ist das sogenannte **Sieb des Eratosthenes**: Man beginnt mit der kleinsten Primzahl, der Zwei. Streicht man alle Vielfachen der Zwei, als da heißtt, alle geraden Zahlen, so ist die erste Zahl unter den Übrigen die nächste Primzahl, die Drei. Streicht man nun auch noch alle Vielfachen der Drei, so ist die erste Zahl unter den Übrigen die nächste Primzahl, die Fünf, und so weiter. „Der Erste“ heißtt auf lateinisch „Primus“ und auf griechisch ähnlich und es könnte sein, daß die Bezeichnung „Primzahl“ daher röhrt.

**Satz 3.4.4.4 (Existenz einer Primfaktorzerlegung).** *Jede natürliche Zahl  $n \geq 2$  kann als ein Produkt von Primzahlen  $n = p_1 p_2 \dots p_r$  dargestellt werden.*

3.4.4.5. Der Satz gilt in unserer Terminologie auch für die Zahl  $n = 1$ , wenn wir auch Produkte der Länge  $r = 0$  erlauben und erinnern, daß nach unseren Konventionen die Eins durch das „leere Produkt“ mit  $r = 0$  dargestellt wird. Eine Primzahl  $p$  ist darin als das Produkt  $p = p_1$  mit nur einem Faktor zu verstehen.

*Beweis.* Das ist klar mit vollständiger Induktion: Ist eine Zahl nicht bereits selbst prim, so kann sie als Produkt echt kleinerer Faktoren geschrieben werden, von denen nach Induktionsannahme bereits bekannt ist, daß sie Primfaktorzerlegungen besitzen.  $\square$

**Satz 3.4.4.6.** *Es gibt unendlich viele Primzahlen.*

*Beweis.* Durch Widerspruch. Gäbe es nur endlich viele Primzahlen, so könnten wir deren Produkt betrachten und dazu Eins hinzuzählen. Die so neu entstehende Zahl müßte dann wie jede von Null verschiedene natürliche Zahl nach 3.4.4.4 eine Primfaktorzerlegung besitzen, aber keine unserer endlich vielen Primzahlen käme als Primfaktor in Frage.  $\square$

*Ergänzung 3.4.4.7.* Noch offen (2019) ist die Frage, ob es auch unendlich viele **Primzahlzwillinge** gibt, als da heißt, Paare von Primzahlen mit der Differenz Zwei, wie zum Beispiel 5, 7 oder 11, 13 oder 17, 19. Ebenso offen ist die Frage, ob jede gerade Zahl  $n > 2$  die Summe von zwei Primzahlen ist. Die Vermutung, daß das richtig sein sollte, ist bekannt als **Goldbach-Vermutung**. Bekannt ist, daß es unendlich viele Paare von Primzahlen mit einem Abstand  $\leq 246$  gibt.

**Satz 3.4.4.8 (Eindeutigkeit der Primfaktorzerlegung).** *Die Darstellung einer natürlichen Zahl  $n \geq 1$  als ein Produkt von Primzahlen  $n = p_1 p_2 \dots p_r$  ist eindeutig bis auf die Reihenfolge der Faktoren. Nehmen wir zusätzlich  $p_1 \leq p_2 \leq \dots \leq p_r$  an, so ist unsere Darstellung mithin eindeutig.*

3.4.4.9. Dieser Satz ist einer von vielen Gründen, aus denen man bei der Definition des Begriffs einer Primzahl die Eins ausschließt, obwohl das die Definition verlängert: Hätten wir der Eins erlaubt, zu unseren Primzahlen dazugehören, so wäre der vorhergehende Satz in dieser Formulierung falsch. In obigem Satz ist  $r \geq 0$  gemeint, genauer ist die Eins das leere Produkt und Primzahlen werden durch ein Produkt mit nur einem Faktor dargestellt.

*Beweis.* Der Beweis dieses Satzes braucht einige Vorbereitungen. Ich bitte Sie, gut aufzupassen, daß wir bei diesen Vorbereitungen den Satz über die Eindeutigkeit der Primfaktorzerlegung nirgends verwenden, bis er dann im Anschluß an Lemma 3.4.4.15 endlich bewiesen werden kann.  $\square$

**Definition 3.4.4.10.** Seien  $a, b \in \mathbb{Z}$  ganze Zahlen. Wir sagen  $a$  teilt  $b$  oder  $a$  ist ein Teiler von  $b$  und schreiben  $a|b$ , wenn es  $c \in \mathbb{Z}$  gibt mit  $ac = b$ .

**Definition 3.4.4.11.** Sind ganze Zahlen  $a, b \in \mathbb{Z}$  nicht beide Null, so gibt es eine größte ganze Zahl  $c \in \mathbb{Z}$ , die sie beide teilt. Diese Zahl heißt der **größte gemeinsame Teiler** von  $a$  und  $b$ . Ganze Zahlen  $a$  und  $b$  heißen **teilerfremd**, wenn sie außer  $\pm 1$  keine gemeinsamen Teiler besitzen. Insbesondere sind also  $a = 0$  und  $b = 0$  nicht teilerfremd.

**Satz 3.4.4.12 (über den größten gemeinsamen Teiler).** Gegeben zwei ganze Zahlen  $a, b \in \mathbb{Z}$ , die nicht beide Null sind, kann ihr größter gemeinsamer Teiler  $c$  als eine ganzzahlige Linearkombination unserer beiden Zahlen dargestellt werden. Es gibt also in Formeln  $r, s \in \mathbb{Z}$  mit

$$c = ra + sb$$

Teilt weiter  $d \in \mathbb{Z}$  sowohl  $a$  als auch  $b$ , so teilt  $d$  auch den größten gemeinsamen Teiler von  $a$  und  $b$ .

3.4.4.13. Der letzte Teil dieses Satzes ist einigermaßen offensichtlich, wenn man die Eindeutigkeit der Primfaktorzerlegung als bekannt voraussetzt. Da wir besagte Eindeutigkeit der Primfaktorzerlegung jedoch erst aus besagtem zweiten Teil ableiten werden, ist es wichtig, auch für den zweiten Teil dieses Satzes einen eigenständigen Beweis zu geben.

*Beweis.* Man betrachte die Teilmenge  $a\mathbb{Z} + b\mathbb{Z} = \{ar + bs \mid r, s \in \mathbb{Z}\} \subset \mathbb{Z}$ . Sie ist offensichtlich eine von Null verschiedene Untergruppe von  $\mathbb{Z}$ . Also ist sie nach unserer Klassifikation 3.4.3.4 der Untergruppen von  $\mathbb{Z}$  von der Form  $a\mathbb{Z} + b\mathbb{Z} = \hat{c}\mathbb{Z}$  für genau ein  $\hat{c} > 0$  und es gilt:

- i.  $\hat{c}$  teilt  $a$  und  $b$ . In der Tat haben wir ja  $a, b \in \hat{c}\mathbb{Z}$ ;
- ii.  $\hat{c} = ra + sb$  für geeignete  $r, s \in \mathbb{Z}$ . In der Tat haben wir ja  $\hat{c} \in a\mathbb{Z} + b\mathbb{Z}$ ;
- iii.  $(d \text{ teilt } a \text{ und } b) \Rightarrow (d \text{ teilt } \hat{c})$ .

Daraus folgt sofort, daß  $\hat{c}$  der größte gemeinsame Teiler von  $a$  und  $b$  ist, und damit folgt dann der Satz.  $\square$

3.4.4.14 (**Notation für größte gemeinsame Teiler**). Gegeben  $a_1, \dots, a_n \in \mathbb{Z}$  können wir mit der Notation 3.4.3.5 kürzer schreiben

$$a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = \langle a_1, \dots, a_n \rangle$$

Üblich ist hier auch die Notation  $(a_1, \dots, a_n)$ , die jedoch oft auch  $n$ -Tupel von ganzen Zahlen bezeichnet, also Elemente von  $\mathbb{Z}^n$ , und in der Analysis im Fall  $n =$

$\mathbb{Z}$  meist ein offenes Intervall. Es gilt dann aus dem Kontext zu erschließen, was jeweils gemeint ist. Sind  $a$  und  $b$  nicht beide Null und ist  $c$  ihr größter gemeinsamer Teiler, so haben wir nach dem Vorhergehenden  $\langle a, b \rangle = \langle c \rangle$ . Wir benutzen von nun an diese Notation. Über die Tintenersparnis hinaus hat sie den Vorteil, auch im Fall  $a = b = 0$  sinnvoll zu bleiben.

**Lemma 3.4.4.15 (von Euklid).** *Teilt eine Primzahl ein Produkt von zwei ganzen Zahlen, so teilt sie einen der Faktoren.*

3.4.4.16 (**Diskussion der Terminologie**). Dies Lemma findet sich bereits in Euklid's Elementen in Buch VII als Proposition 30.

3.4.4.17. Wenn wir die Eindeutigkeit der Primfaktorzerlegung als bekannt voraussetzen, so ist dies Lemma offensichtlich. Diese Argumentation hilft aber hier nicht weiter, da sie voraussetzt, was wir gerade erst beweisen wollen. Sicher ist Ihnen die Eindeutigkeit der Primfaktorzerlegung aus der Schule und ihrer Rechenerfahrung wohlvertraut. Um die Schwierigkeit zu sehen, sollten Sie vielleicht selbst einmal versuchen, einen Beweis dafür anzugeben. Im übrigen werden wir in ?? sehen, daß etwa im Ring  $\mathbb{Z}[\sqrt{-5}]$  das Analogon zur Eindeutigkeit der Primfaktorzerlegung nicht mehr richtig ist.

*Beweis.* Sei  $p$  unsere Primzahl und seien  $a, b \in \mathbb{Z}$  gegeben mit  $p|ab$ . Teilt  $p$  nicht  $a$ , so folgt für den größten gemeinsamen Teiler  $\langle p, a \rangle = \langle 1 \rangle$ , denn die Primzahl  $p$  hat nur die Teiler  $\pm 1$  und  $\pm p$ . Der größte gemeinsame Teiler von  $p$  und  $a$  kann aber nicht  $p$  sein und muß folglich 1 sein. Nach 3.4.4.12 gibt es also  $r, s \in \mathbb{Z}$  mit  $1 = rp + sa$ . Es folgt  $b = rpb + sab$  und damit  $p|b$ , denn  $p$  teilt natürlich  $rpb$  und teilt nach Annahme auch  $sab$ .  $\square$

*Beweis der Eindeutigkeit der Primfaktorzerlegung 3.4.4.8.* Zunächst bemerken wir, daß aus Lemma 3.4.4.15 per Induktion dieselbe Aussage auch für Produkte beliebiger Länge folgt: Teilt eine Primzahl ein Produkt, so teilt sie einen der Faktoren. Seien  $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$  zwei Primfaktorzerlegungen derselben Zahl  $n \geq 1$ . Da  $p_1$  unser  $n$  teilt, muß es damit eines der  $q_i$  teilen. Da auch dies  $q_i$  prim ist, folgt  $p_1 = q_i$ . Wir kürzen den gemeinsamen Primfaktor und sind fertig per Induktion.  $\square$

3.4.4.18. Ich erkläre am Beispiel  $a = 160, b = 625$  den sogenannten **euklidischen Algorithmus**, mit dem man den größten gemeinsamen Teiler  $c$  zweier positiver natürlicher Zahlen  $a, b$  bestimmen kann nebst einer Darstellung  $c = ra + rb$ . In unseren Gleichungen wird jeweils geteilt mit Rest.

$$\begin{aligned} 160 &= 1 \cdot 145 + 15 \\ 145 &= 9 \cdot 15 + 10 \\ 15 &= 1 \cdot 10 + 5 \\ 10 &= 2 \cdot 5 + 0 \end{aligned}$$

Daraus folgt für den größten gemeinsamen Teiler  $\langle 625, 160 \rangle = \langle 160, 145 \rangle = \langle 145, 15 \rangle = \langle 15, 10 \rangle = \langle 10, 5 \rangle = \langle 5, 0 \rangle = \langle 5 \rangle$ . Die vorletzte Zeile liefert eine Darstellung  $5 = x \cdot 10 + y \cdot 15$  unseres größten gemeinsamen Teilers  $5 = \text{ggT}(10, 15)$  als ganzzahlige Linearkombination von 10 und 15. Die vorvorletzte Zeile eine Darstellung  $10 = x' \cdot 15 + y' \cdot 145$  und nach Einsetzen in die vorherige Gleichung eine Darstellung  $5 = x(x' \cdot 15 + y' \cdot 145) + y \cdot 15$  unseres größten gemeinsamen Teilers  $5 = \text{ggT}(15, 145)$  als ganzzahlige Linearkombination von 15 und 145. Indem wir so induktiv hochsteigen, erhalten wir schließlich für den größten gemeinsamen Teiler die Darstellung  $5 = -11 \cdot 625 + 43 \cdot 160$ .

*Ergänzung 3.4.4.19.* Gegeben eine positive natürliche Zahl  $n$  bezeichne  $\text{rad}(n)$  das Produkt ohne Vielfachheiten aller Primzahlen, die  $n$  teilen. Die **ABC-Vermutung** besagt, daß es für jedes  $\varepsilon > 0$  nur endlich viele Tripel von paarweise teilerfremden positiven natürlichen Zahlen  $a, b, c$  geben soll mit  $a + b = c$  und

$$c > (\text{rad}(abc))^{1+\varepsilon}$$

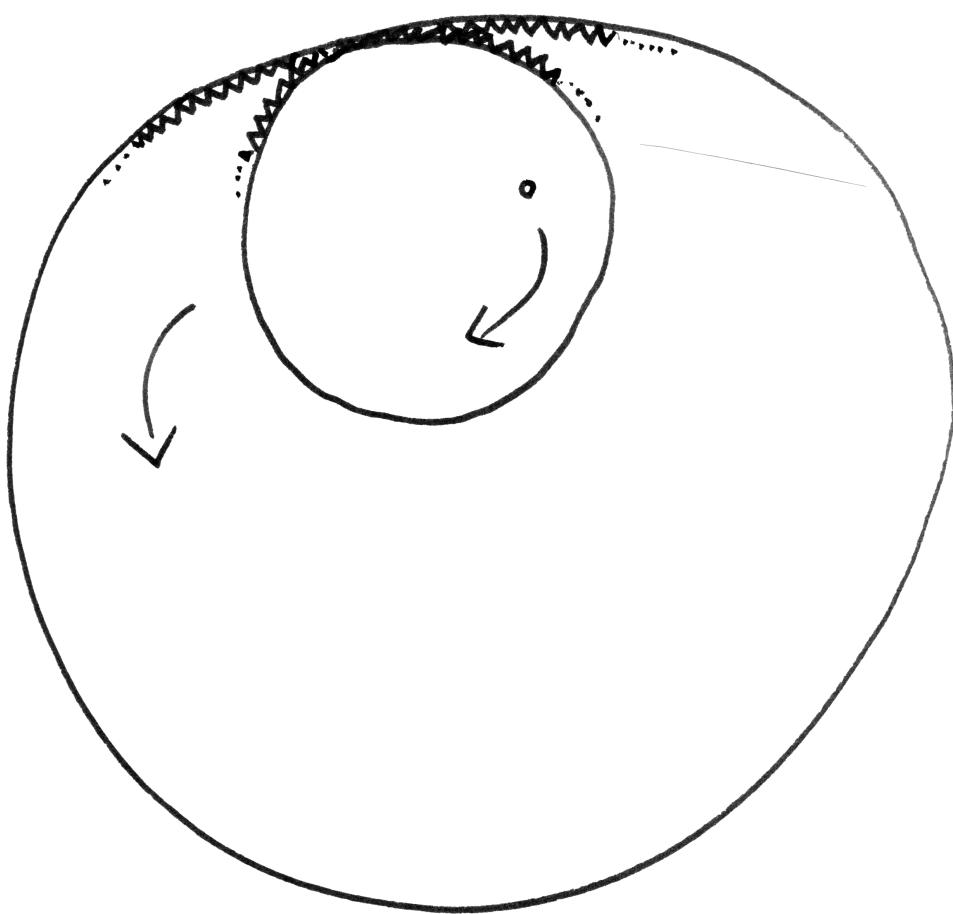
Es soll also salopp gesprochen sehr selten sein, daß für teilerfremde positive natürliche Zahlen  $a, b$  mit vergleichsweise kleinen Primfaktoren ihre Summe auch nur kleine Primfaktoren hat. Der Status der Vermutung ist zur Zeit (2019) noch ungeklärt. Man kann zeigen, daß es unendlich viele Tripel von paarweise teilerfremden positiven natürlichen Zahlen  $a < b < c$  gibt mit  $a + b = c$  und  $c \geq \text{rad}(abc)$ . Diese sind jedoch bereits vergleichsweise selten, so gibt es etwa nur 120 mögliche Tripel mit  $c < 10000$ .

## Übungen

*Übung 3.4.4.20.* Man berechne den größten gemeinsamen Teiler von 3456 und 436 und eine Darstellung desselben als ganzzahlige Linearkombination unserer beiden Zahlen.

*Übung 3.4.4.21.* Gegeben zwei von Null verschiedene natürliche Zahlen  $a, b$  nennt man die kleinste von Null verschiedene natürliche Zahl, die sowohl ein Vielfaches von  $a$  als auch ein Vielfaches von  $b$  ist, das **kleinste gemeinsame Vielfache** von  $a$  und  $b$  und notiert sie  $\text{kgV}(a, b)$ . Man zeige in dieser Notation die Formel  $\text{kgV}(a, b) \text{ggT}(a, b) = ab$ .

*Ergänzende Übung 3.4.4.22.* Beim sogenannten „Spirographen“, einem Zeichenspiel für Kinder, kann man an einem innen mit 105 Zähnen versehenen Ring ein Zahnrad mit 24 Zähnen entlanglaufen lassen. Steckt man dabei einen Stift durch ein Loch außerhalb des Zentrums des Zahnrads, so entstehen dabei die köstlichsten Figuren. Wie oft muß das Zahnrad auf dem inneren Zahnkranz umlaufen, bevor solch eine Figur fertig gemalt ist?



Der Spirograph aus Übung 3.4.4.22

*Ergänzende Übung 3.4.4.23.* Berechnen Sie, wieviele verschiedene Strophen das schöne Lied hat, dessen erste Strophe lautet:

Tomatensalat Tomatensalat Tooood  
-matensalat Tomatensaaaaaaa-  
-lat Tomatensalat Tomatensalat  
Tomatensalat Tomatensaaaaaaa-

## 3.5 Ringe und Polynome

### 3.5.1 Ringe

**Definition 3.5.1.1.** Ein **Ring**, französisch **anneau**, ist eine Menge mit zwei Verknüpfungen  $(R, +, \cdot)$  derart, daß gilt:

1.  $(R, +)$  ist eine kommutative Gruppe;
2.  $(R, \cdot)$  ist ein Monoid; ausgeschrieben heißt das nach 2.2.1.20, daß auch die Verknüpfung  $\cdot$  assoziativ ist und daß es ein Element  $1 = 1_R \in R$  mit der Eigenschaft  $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$  gibt, das **Eins-Element** oder kurz die **Eins** unseres Rings;
3. Es gelten die Distributivgesetze, als da heißtt, für alle  $a, b, c \in R$  gilt

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \end{aligned}$$

Die beiden Verknüpfungen heißen die **Addition** und die **Multiplikation** in unserem Ring. Das Element  $1 \in R$  aus unserer Definition ist wohlbestimmt als das neutrale Element des Monoids  $(R, \cdot)$ , vergleiche 2.2.1.19. Ein Ring, dessen Multiplikation kommutativ ist, heißt ein **kommutativer Ring** und bei uns in unüblicher Verkürzung ein **Kring**.

3.5.1.2. Wir schreiben meist kürzer  $a \cdot b = ab$  und vereinbaren die Regel „Punkt vor Strich“, so daß zum Beispiel das erste Distributivgesetz auch übersichtlicher in der Form  $a(b + c) = ab + ac$  geschrieben werden kann.

*Beispiel 3.5.1.3.* Die ganzen Zahlen  $\mathbb{Z}$  bilden mit der üblichen Multiplikation und Addition nach 3.4.2.12 einen kommutativen Ring.

3.5.1.4 (**Ursprung der Terminologie**). Der Begriff „Ring“ soll zum Ausdruck bringen, daß diese Struktur nicht in demselben Maße „geschlossen“ ist wie ein Körper, da wir nämlich nicht die Existenz von multiplikativen Inversen fordern. Er wird auch im juristischen Sinne für gewisse Arten weniger geschlossener Körperschaften verwendet. So gibt es etwa den „Ring deutscher Makler“ oder den „Ring deutscher Bergingenieure“.

3.5.1.5 (**Diskussion der Terminologie**). Eine Struktur wie in der vorhergehenden Definition, bei der nur die Existenz eines Einselementes nicht gefordert wird, bezeichnen wir im Vorgriff auf ?? als eine **assoziative  $\mathbb{Z}$ -Algebra**. In der Literatur wird jedoch auch diese Struktur oft als „Ring“ bezeichnet, sogar bei der von mir hochgeschätzten Quelle Bourbaki. Die Ringe, die eine Eins besitzen, heißen in dieser Terminologie „unitäre Ringe“.

*Ergänzung 3.5.1.6.* Allgemeiner als in 3.2.6.15 erklärt ein Element  $a$  eines beliebigen Ringes, ja einer beliebigen assoziativen  $\mathbb{Z}$ -Algebra **nilpotent**, wenn es  $d \in \mathbb{N}$  gibt mit  $a^d = 0$ .

*Beispiele 3.5.1.7.* Die einelementige Menge mit der offensichtlichen Addition und Multiplikation ist ein Ring, der **Nullring**. Jeder Körper ist ein Ring. Die ganzen Zahlen  $\mathbb{Z}$  bilden einen Ring. Ist  $R$  ein Ring und  $X$  eine Menge, so ist die Menge  $\text{Ens}(X, R)$  aller Abbildungen von  $X$  nach  $R$  ein Ring unter punktweiser Multiplikation und Addition. Ist  $R$  ein Ring und  $n \in \mathbb{N}$ , so bilden die  $(n \times n)$ -Matrizen mit Einträgen in  $R$  einen Ring  $\text{Mat}(n; R)$  unter der üblichen Addition und Multiplikation von Matrizen; im Fall  $n = 0$  erhalten wir den Nullring, im Fall  $n = 1$  ergibt sich  $R$  selbst. Ist  $A$  eine abelsche Gruppe, so bilden die Gruppenhomomorphismen von  $A$  in sich selbst, die sogenannten **Endomorphismen** von  $A$ , einen Ring mit der Verknüpfung von Abbildungen als Multiplikation und der punktweisen Summe als Addition. Man notiert diesen Ring

$$\text{End}A$$

und nennt ihn den **Endomorphismenring der abelschen Gruppe**  $A$ . Ähnlich bilden auch die Endomorphismen eines Vektorraums  $V$  über einem Körper  $k$  einen Ring  $\text{End}_k V$ , den sogenannten **Endomorphismenring von**  $V$ . Oft notiert man auch den Endomorphismenring eines Vektorraums abkürzend  $\text{End}V$  in der Hoffnung, daß aus dem Kontext klar wird, daß die Endomorphismen von  $V$  als Vektorraum gemeint sind und nicht die Endomorphismen der  $V$  zugrundeliegenden abelschen Gruppe. Will man besonders betonen, daß die Endomorphismen als Gruppe gemeint sind, so schreibt man manchmal auch  $\text{End}_{\mathbb{Z}} A$  aus Gründen, die erst in ?? erklärt werden. Ich verwende für diesen Ring zur Vermeidung von Indizes lieber die Notation  $\text{End}_{\mathbb{Z}} A = \text{Ab}A$ , die sich aus den allgemeinen kategorientheoretischen Konventionen 4.7.1.6 ergibt.

**Definition 3.5.1.8.** Eine Abbildung  $\varphi : R \rightarrow S$  von einem Ring in einen weiteren Ring heißt ein **Ringhomomorphismus**, wenn gilt  $\varphi(1) = 1$  und  $\varphi(a + b) = \varphi(a) + \varphi(b)$  sowie  $\varphi(ab) = \varphi(a)\varphi(b)$  für alle  $a, b \in R$ . In anderen Worten ist ein Ringhomomorphismus also eine Abbildung, die sowohl für die Addition als auch für die Multiplikation ein Monoidhomomorphismus ist. Die Menge aller Ringhomomorphismen von einem Ring  $R$  in einen Ring  $S$  notieren wir

$$\text{Ring}(R, S)$$

*Ergänzung 3.5.1.9.* Von Homomorphismen zwischen  $\mathbb{Z}$ -Algebren können wir natürlich nicht fordern, daß sie das Einselement auf das Einselement abbilden. Wir sprechen dann von **Algebrenhomomorphismen**. In der Terminologie, in der unsere assoziativen  $\mathbb{Z}$ -Algebren als Ringe bezeichnet werden, werden unsere Ringhomomorphismen „unitäre Ringhomomorphismen“ genannt.

**Proposition 3.5.1.10.** Für jeden Ring  $R$  gibt es genau einen Ringhomomorphismus  $\mathbb{Z} \rightarrow R$ , in Formeln  $|\text{Ring}(\mathbb{Z}, R)| = 1$ .

*Beweis.* Nach 2.2.3.31 gibt es genau einen Gruppenhomomorphismus von additiven Gruppen  $\varphi : \mathbb{Z} \rightarrow R$ , der die  $1 \in \mathbb{Z}$  auf  $1_R \in R$  abbildet. Wir müssen nur noch zeigen, daß er mit der Multiplikation verträglich ist, in Formeln  $\varphi(nm) = \varphi(n)\varphi(m)$  für alle  $n, m \in \mathbb{Z}$ . Mit 3.5.1.15 zieht man sich leicht auf den Fall  $n, m > 0$  zurück. In diesem Fall beginnt man mit der Erkenntnis  $\varphi(1 \cdot 1) = \varphi(1) = 1_R = 1_R \cdot 1_R = \varphi(1)\varphi(1)$  und argumentiert von da aus mit vollständiger Induktion und dem Distributivgesetz.  $\square$

**3.5.1.11 (Ganze Zahlen und allgemeine Ringe).** Gegeben ein Ring  $R$  notieren wir den Ringhomomorphismus  $\mathbb{Z} \rightarrow R$  aus 3.5.1.10 manchmal  $n \mapsto n_R$  und meist  $n \mapsto n$ . Ich will kurz diskutieren, warum das ungefährlich ist. Gegeben  $r \in R$  und  $n \in \mathbb{Z}$  gilt nämlich stets  $nr = n_Rr = rn_R$ , wobei  $nr$  in Bezug auf die Struktur von  $R$  als additive abelsche Gruppe verstehen, also  $nr = n^+r = r+r+\dots+r$  mit  $n$  Summanden falls  $n \geq 1$  und so weiter, wie in der Tabelle 2.2.2.13 und in 2.2.2.11 ausgeführt wird. Unsere Gleichung  $nr = n_Rr = rn_R$  bedeutet dann hinwiederum, daß es auf den Unterschied zwischen  $n_R$  und  $n$  meist gar nicht ankommt. Deshalb führt es auch selten zu Mißverständnissen, wenn wir statt  $n_R$  nur kurz  $n$  schreiben.

**3.5.1.12.** Eine Teilmenge eines Rings heißt ein **Teilring**, wenn sie eine additive Untergruppe und ein multiplikatives Untermonoid ist. Ist also  $R$  unser Ring, so ist eine Teilmenge  $T \subset R$  genau dann ein Teilring, wenn gilt  $0_R, 1_R \in T$ ,  $a \in T \Rightarrow (-a) \in T$  sowie  $a, b \in T \Rightarrow a+b, ab \in T$ . Wir diskutieren diesen Begriff hier nur im Vorbeigehen, da er in dieser Vorlesung nur eine Nebenrolle spielt.

## Übungen

*Übung 3.5.1.13 (Quotientenring).* Gegeben ein Ring  $R$  und eine Surjektion  $R \twoheadrightarrow Q$  von  $R$  auf eine Menge  $Q$ , die an die Multiplikation und Addition von  $R$  angepaßt ist im Sinne von 2.2.3.28, ist  $Q$  mit der koinduzierten Addition und Multiplikation auch wieder ein Ring.

*Ergänzende Übung 3.5.1.14.* Auf der abelschen Gruppe  $\mathbb{Z}$  gibt es genau zwei Verknüpfungen, die als Multiplikation genommen die Addition zu einer Ringstruktur ergänzen.

*Übung 3.5.1.15.* Man zeige, daß in jedem Ring  $R$  gilt  $0a = 0 \ \forall a \in R$ ;  $-a = (-1)a \ \forall a \in R$ ;  $(-1)(-1) = 1$ ;  $(-a)(-b) = ab \ \forall a, b \in R$ .

*Übung 3.5.1.16.* Gegeben eine Überdeckung einer endlichen Menge  $X$  durch Teilmengen  $X = X_1 \cup \dots \cup X_n$  zeige man die **Einschluß-Ausschluß-Formel**

$$0 = \sum_{I \subset \{1, \dots, n\}} (-1)^{|I|} |\bigcap_{i \in I} X_i|$$

mit der Interpretation des leeren Schnitts als  $X$ . Im Fall  $n = 3$  etwa können wir das ausschreiben zu

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cup Y| - |X \cup Z| - |Y \cup Z| + |X \cup Y \cup Z|$$

Hinweis: Sogar im Fall einer beliebigen Menge  $X$  mit beliebigen Teilmengen  $X_i$  mag man deren charakteristische Funktionen mit  $\chi_i$  bezeichnen und im Ring der  $\mathbb{Z}$ -wertigen Funktionen auf  $X$  das Produkt  $(1 - \chi_1) \dots (1 - \chi_n)$  ausmultiplizieren.

*Übung 3.5.1.17.* Für jeden Ring  $R$  gibt es höchstens einen Ringhomomorphismus  $\mathbb{Q} \rightarrow R$ , in Formeln  $|\text{Ring}(\mathbb{Q}, R)| \leq 1$ .

### 3.5.2 Restklassenringe des Rings der ganzen Zahlen

**Definition 3.5.2.1.** Gegeben  $G \supset H$  eine Gruppe mit einer Untergruppe definieren wir den **Quotienten**  $G/H$ , eine Teilmenge  $G/H \subset \mathcal{P}(G)$ , durch die Vorschrift

$$G/H := \{L \subset G \mid \exists g \in G \text{ mit } L = gH\}$$

Die Teilmenge  $gH \subset G$  heißt die  **$H$ -Linksnebenklasse von  $g$  in  $G$** . Unser Quotient ist also die Menge aller  $H$ -Linksnebenklassen in  $G$ . Jedes Element einer Linksnebenklasse heißt auch ein **Repräsentant** besagter Linksnebenklasse. Eine Teilmenge  $R \subset G$  derart, daß die Vorschrift  $g \mapsto gH$  eine Bijektion  $R \xrightarrow{\sim} G/H$  induziert, heißt ein **Repräsentantsystem** für die Menge der Linksnebenklassen.

*Vorschau 3.5.2.2.* Diese Konstruktion wird in 4.4.1.2 noch sehr viel ausführlicher diskutiert werden.

*Beispiel 3.5.2.3.* Im Fall der additiven Gruppe  $\mathbb{Z}$  mit der Untergruppe  $m\mathbb{Z}$  haben wir speziell  $\mathbb{Z}/m\mathbb{Z} = \{L \subset \mathbb{Z} \mid \exists a \in \mathbb{Z} \text{ mit } L = a + m\mathbb{Z}\}$ . Die Linksnebenklasse von  $a$  heißt in diesem Fall auch die **Restklasse von  $a$  modulo  $m$** , da zumindest im Fall  $a \geq 0$  und  $m > 0$  ihre nichtnegativen Elemente genau alle natürlichen Zahlen sind, die beim Teilen durch  $m$  denselben Rest lassen wie  $a$ . Wir notieren diese Restklasse auch  $\bar{a}$ . Natürlich ist  $\bar{a} = \bar{b}$  gleichbedeutend zu  $a - b \in m\mathbb{Z}$ . Gehören  $a$  und  $b$  zur selben Restklasse, in Formeln  $a + m\mathbb{Z} = b + m\mathbb{Z}$ , so nennen wir sie **kongruent modulo  $m$**  und schreiben

$$a \equiv b \pmod{m}$$

Offensichtlich gibt es für  $m > 0$  genau  $m$  Restklassen modulo  $m$ , in Formeln  $|\mathbb{Z}/m\mathbb{Z}| = m$ , und wir haben genauer

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{m-1}\}$$

Da in dieser Aufzählung keine Nebenklassen mehrfach genannt werden, ist die Teilmenge  $\{0, 1, \dots, m - 1\}$  also ein Repräsentantensystem für die Menge von Nebenklassen  $\mathbb{Z}/m\mathbb{Z}$ . Ein anderes Repräsentantensystem wäre  $\{1, \dots, m\}$ , ein Drittes  $\{1, \dots, m - 1, 7m\}$ .

**Satz 3.5.2.4 (Restklassenring).** *Für alle  $m \in \mathbb{Z}$  gibt es auf der Menge  $\mathbb{Z}/m\mathbb{Z}$  genau eine Struktur als Ring derart, daß die Abbildung  $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  mit  $a \mapsto \bar{a}$  ein Ringhomomorphismus ist.*

3.5.2.5. Das ist dann natürlich die Struktur als Quotientenring im Sinne unserer Übung 3.5.1.13.

*Beweis.* Daß es höchstens eine derartige Ringstruktur gibt, es eh klar. Zu zeigen bleibt nur deren Existenz. Nach 2.2.1.3 induziert jede Verknüpfung auf einer Menge  $A$  eine Verknüpfung auf ihrer Potenzmenge  $\mathcal{P}(A)$ . Für die so von der Verknüpfung  $+$  auf  $\mathbb{Z}$  induzierte Verknüpfung  $+$  auf  $\mathcal{P}(\mathbb{Z})$  gilt offensichtlich

$$\bar{a} + \bar{b} = (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z} = \overline{a + b} \quad \forall a, b \in \mathbb{Z}$$

Insbesondere induziert unsere Verknüpfung  $+$  auf  $\mathcal{P}(\mathbb{Z})$  eine Verknüpfung  $+$  auf  $\mathbb{Z}/m\mathbb{Z}$  und  $a \mapsto \bar{a}$  ist für diese Verknüpfungen ein Morphismus von Magmas alias Mengen mit Verknüpfung. Ebenso können wir auf  $\mathcal{P}(\mathbb{Z})$  eine Verknüpfung  $\odot = \odot_m$  einführen durch die Vorschrift

$$T \odot S := T \cdot S + m\mathbb{Z} := \{ab + mr \mid a \in T, b \in S, r \in \mathbb{Z}\}$$

Wieder prüft man für die so erklärte Multiplikation mühelos die Formel

$$\bar{a} \odot \bar{b} = \overline{ab}$$

Daß  $\mathbb{Z}/m\mathbb{Z}$  mit unseren beiden Verknüpfungen ein Ring wird und  $a \mapsto \bar{a}$  ein Ringhomomorphismus, folgt ohne weitere Schwierigkeiten aus der Surjektivität der natürlichen Abbildung  $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$  alias Übung 3.5.1.13.  $\square$

3.5.2.6. Wir geben wir die komische Notation  $\odot$  nun auch gleich wieder auf und schreiben stattdessen  $\bar{a} \cdot \bar{b}$  oder noch kürzer  $\bar{a}\bar{b}$ . Auch die Notation  $\bar{a}$  werden wir meist zu  $a$  vereinfachen, wie wir es ja in 3.5.1.11 eh schon vereinbart hatten.

*Beispiel 3.5.2.7.* Modulo  $m = 2$  gibt es genau zwei Restklassen: Die Elemente der Restklasse von 0 bezeichnet man üblicherweise als **gerade Zahlen**, die Elemente der Restklasse von 1 als **ungerade Zahlen**. Der Ring  $\mathbb{Z}/2\mathbb{Z}$  mit diesen beiden Elementen  $\bar{0}$  und  $\bar{1}$  ist offensichtlich sogar ein Körper.

**Beispiel 3.5.2.8 (Der Ring  $\mathbb{Z}/12\mathbb{Z}$  der Uhrzeiten).** Den Ring  $\mathbb{Z}/12\mathbb{Z}$  könnte man als „Ring von Uhrzeiten“ ansehen. Er hat die zwölf Elemente  $\{\bar{0}, \bar{1}, \dots, \bar{11}\}$  und wir haben  $\bar{11} + \bar{5} = \bar{16} = \bar{4}$  alias „5 Stunden nach 11 Uhr ist es 4 Uhr“. Weiter haben wir in  $\mathbb{Z}/12\mathbb{Z}$  etwa auch  $\bar{3} \cdot \bar{8} = \bar{24} = \bar{0}$ . In einem Ring kann es also durchaus passieren, daß ein Produkt von zwei von Null verschiedenen Faktoren Null ist.

**Vorschau 3.5.2.9.** Sei  $m \geq 1$  eine natürliche Zahl. Eine Restklasse modulo  $m$  heißt eine **prime Restklasse**, wenn sie aus zu  $m$  teilerfremden Zahlen besteht. Wir zeigen in ??, daß es in jeder primen Restklasse unendlich viele Primzahlen gibt. Im Fall  $m = 10$  bedeutet das zum Beispiel, daß es jeweils unendlich viele Primzahlen gibt, deren Dezimaldarstellung mit einer der Ziffern 1, 3, 7 und 9 endet.

**Proposition 3.5.2.10 (Teilbarkeitskriterien über Quersummen).** Eine natürliche Zahl ist genau dann durch Drei beziehungsweise durch Neun teilbar, wenn ihre Quersumme durch Drei beziehungsweise durch Neun teilbar ist.

*Beweis.* Wir erklären das Argument nur an einem Beispiel. Das ist natürlich im Sinne der Logik kein Beweis. Dies Vorgehen schien mir aber in diesem Fall besonders gut geeignet, dem Leser den Grund dafür klarzumachen, aus dem unsere Aussage im Allgemeinen gilt. Und das ist es ja genau, was ein Beweis in unserem mehr umgangssprachlichen Sinne leisten soll! Also frisch ans Werk. Per definitio-nem gilt

$$1258 = 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 8$$

Offensichtlich folgt

$$1258 \equiv 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 8 \pmod{3}$$

Da 10 kongruent ist zu 1 modulo 3 erhalten wir daraus

$$1258 \equiv 1 + 2 + 5 + 8 \pmod{3}$$

Insbesondere ist die rechte Seite durch Drei teilbar genau dann, wenn die linke Seite durch Drei teilbar ist. Das Argument für Neun statt Drei geht genauso.  $\square$

3.5.2.11. In  $\mathbb{Z}/12\mathbb{Z}$  gilt zum Beispiel  $\bar{3} \cdot \bar{5} = \bar{3} \cdot \bar{1}$ . In allgemeinen Ringen dürfen wir also nicht kürzen. Dies Phänomen werden wir nun begrifflich fassen. Dazu vereinbaren wir, daß bei Ringen unsere allgemeinen Konventionen 2.2.1.4 zu Kürzbarkeit und Teilen stets in Bezug auf die Multiplikation zu verstehen sein sollen. Wir schreiben das auch noch aus.

**Definition 3.5.2.12.** 1. Gegeben ein Ring  $R$  und Elemente  $a, b \in R$  sagen wir,  $a$  **teilt**  $b$  oder auch  $a$  ist ein **Teiler von  $b$**  und schreiben  $a|b$ , wenn es  $d \in R$  gibt mit  $ad = b$ . Ist unser Ring nicht kommutativ, so nennen wir  $a$  genauer einen **Linksteiler** von  $b$  und erklären analog **Rechtsteiler**;

2. Ein Element  $a \in R$  eines Rings heißt **linkskürzbar**, wenn die Multiplikation mit  $a$  eine Injektion  $(a \cdot) : R \hookrightarrow R$  liefert. Analog erklären wir die Eigenschaft **rechtskürzbar**. Ein Element, das linkskürzbar und rechtskürzbar ist, nennen wir **kürzbar**. Ein nicht kürzbares Element nennen wir **nichtkürzbar**;
3. Ein Ring heißt ein **Integritätsring** oder **Integritätsbereich**, wenn er nicht der Nullring ist und das Produkt von je zwei von Null verschiedenen Elementen von Null verschieden ist. Einen kommutativen Integritätsring nennen wir auch einen **Integritätskring**.

*Beispiel 3.5.2.13.* Die nichtkürzbaren Elemente in  $\mathbb{Z}/12\mathbb{Z}$  sind  $0, 2, 3, 4, 6, 8, 9, 10$ .

3.5.2.14 (**Diskussion der Terminologie**). In der Literatur heißen die nichtkürzbaren Elemente eines Rings meist die „Nullteiler“. Mir gefiel diese Terminologie nicht, da ja nach unseren sonstigen Definitionen alle Elemente eines Rings Teiler der Null sind.

3.5.2.15 (**Kürzen in Ringen**). Sei  $R$  ein Ring. Natürlich ist der Gruppenhomomorphismus  $(a \cdot) : R \rightarrow R$  genau dann injektiv, wenn sein Kern Null ist, wenn also gilt  $ax = 0 \Rightarrow x = 0$ .

**Definition 3.5.2.16.** Ein Element  $a$  eines Rings  $R$  heißt **invertierbar** oder genauer **invertierbar in  $R$**  oder auch eine **Einheit von  $R$** , wenn es bezüglich der Multiplikation invertierbar ist im Sinne von 2.2.2.2, wenn es also  $b \in R$  gibt mit  $ab = ba = 1$ . Die Menge der invertierbaren Elemente eines Rings bildet unter der Multiplikation eine Gruppe, die man die **Gruppe der Einheiten von  $R$**  nennt und gemäß unserer allgemeinen Konventionen 2.2.2.13 mit  $R^\times$  bezeichnet.

*Beispiel 3.5.2.17.* Der Ring  $\mathbb{Z}$  der ganzen Zahlen hat genau zwei Einheiten, nämlich  $1$  und  $(-1)$ . In Formeln haben wir also  $\mathbb{Z}^\times = \{1, -1\}$ . Dahingegen sind die Einheiten im Ring  $\mathbb{Q}$  der rationalen Zahlen genau alle von Null verschiedenen Elemente, in Formeln  $\mathbb{Q}^\times = \mathbb{Q} \setminus 0$ .

3.5.2.18. Eine Einheit eines Krings teilt alle Elemente unseres Krings und ist sogar dasselbe wie ein Teiler der Eins.

**Definition 3.5.2.19.** Zwei Elemente eines Krings heißen **teilerfremd**, wenn sie außer Einheiten keine gemeinsamen Teiler haben.

3.5.2.20. Allgemeiner mag man eine Teilmenge eines Krings **teilerfremd** nennen, wenn es keine Nichteinheit unseres Krings gibt, die alle Elemente unserer Teilmenge teilt.

3.5.2.21 (**Kürzbare Elemente endlicher Kringe**). In einem endlichen Kring  $R$  sind die Einheiten genau die kürzbaren Elemente. In der Tat ist in diesem Fall die Multiplikation  $(a \cdot) : R \rightarrow R$  genau dann injektiv, wenn sie bijektiv ist.

*Beispiel 3.5.2.22.* Die Einheiten von  $\mathbb{Z}/12\mathbb{Z}$  sind mithin genau 1, 5, 7, 11. Man prüft unschwer, daß sogar jedes dieser Elemente sein eigenes Inverses ist. Mithin ist die Einheitengruppe  $(\mathbb{Z}/12\mathbb{Z})^\times$  des Uhrzeitenrings gerade unsere Klein'sche Vierergruppe. Im allgemeinen ein Inverses zu  $a$  in  $\mathbb{Z}/m\mathbb{Z}$  zu finden, läuft auf die Lösung der Gleichung  $ax = 1 + my$  hinaus, von der wir bereits gesehen hatten, daß der euklidische Algorithmus das leisten kann.

**3.5.2.23 (Ursprung der Terminologie).** A priori meint eine Einheit in der Physik das, was ein Mathematiker eine Basis eines eindimensionalen Vektorraums nennt würde. So wäre etwa die Sekunde  $s$  eine Basis des reellen Vektorraums  $\vec{\mathbb{T}}$  aller Zeitspannen aus 3.3.1.11. In Formeln ausgedrückt bedeutet das gerade, daß das Daranmultiplizieren von  $s$  eine Bijektion  $\mathbb{R} \xrightarrow{\sim} \vec{\mathbb{T}}$  liefert. Mit den Einheiten eines kommutativen Ringes  $R$  verhält es sich nun genauso: Genau dann ist  $u \in R$  eine Einheit, wenn das Daranmultiplizieren von  $u$  eine Bijektion  $R \xrightarrow{\sim} R$  liefert. Daher röhrt dann wohl auch die Terminologie.

*Ergänzung 3.5.2.24.* In der Chemie rechnet man oft mit **mol** und versteht darunter seit 2019 genau  $6,02214076 \cdot 10^{23}$  und verwendet das als eine Einheit. Mathematisch gesehen sollte man das eigentlich eine Zahl nennen, aber natürlich ist  $\mathbb{R}$  auch ein eindimensionaler reeller Vektorraum und in diesem Sinne mag man auch alle von Null verschiedenen Elemente von  $\mathbb{R}$  Einheiten. Diese Konvention war früher noch sinnvoller, als man ein Mol als die Zahl der Kohlenstoffatome in einem Gramm des Standardisotops von Kohlenstoff erklärte und nicht so genau sagen konnte, wie viele Atome das nun genau sind.

**3.5.2.25.** Ein Körper kann in dieser Begrifflichkeit definiert werden als ein Integritätsring, in dem jedes von Null verschiedenen Element eine Einheit ist.

**Proposition 3.5.2.26 (Endliche Primkörper).** Sei  $m \in \mathbb{N}$ . Genau dann ist der Restklassenring  $\mathbb{Z}/m\mathbb{Z}$  ein Körper, wenn  $m$  eine Primzahl ist.

*Beweis.* Sei ohne Beschränkung der Allgemeinheit  $m \geq 2$ . Ist  $m$  keine Primzahl, so gibt es  $a, b \in \mathbb{N}$  mit  $a < m$  und  $b < m$  aber  $ab = m$ . Dann gilt in  $\mathbb{Z}/m\mathbb{Z}$  offensichtlich  $\bar{a} \neq 0$  und  $\bar{b} \neq 0$ , aber ebenso offensichtlich gilt  $\bar{a}\bar{b} = 0$  und  $\mathbb{Z}/m\mathbb{Z}$  hat von Null verschiedenen nicht invertierbare Elemente. Damit kann  $\mathbb{Z}/m\mathbb{Z}$  kein Körper sein. Ist dagegen  $m = p$  eine Primzahl, so folgt aus dem Satz von Euklid 3.4.4.15, daß  $\mathbb{Z}/p\mathbb{Z}$  ein Integritätsring ist. Dann aber sind nach 3.5.2.21 alle seine von Null verschiedenen Elemente Einheiten und  $\mathbb{Z}/p\mathbb{Z}$  ist folglich ein Körper.  $\square$

**3.5.2.27 (Terminologie und Notation).** Die Körper  $\mathbb{Z}/p\mathbb{Z}$  für Primzahlen  $p$  sowie der Körper  $\mathbb{Q}$  sind die „kleinstmöglichen Körper“ in einem Sinne, der in ?? präzisiert wird. Man nennt diese Körper deshalb auch **Primkörper**. Die endlichen Primkörper werden meist

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

notiert, mit einem  $\mathbb{F}$  für „field“ oder „finite“. Die Notation  $\mathbb{F}_q$  verwendet man allerdings auch allgemeiner mit einer echten Primzahlpotenz  $q$  im Index als Bezeichnung für „den endlichen Körper mit  $q$  Elementen“, den wir erst in ?? kennenlernen werden, und der weder als Ring noch als abelsche Gruppe isomorph ist zu  $\mathbb{Z}/q\mathbb{Z}$ .

*Ergänzung 3.5.2.28.* Ich bespreche kurz das **Verfahren von Diffie-Hellman** zum öffentlichen Vereinbaren geheimer Schlüssel. Wir betrachten dazu das folgende Schema:

| Geheimbereich Alice   | Öffentlicher Bereich  | Geheimbereich Bob   |
|---|---|---|
|   | Bekanntgemacht wird eine Gruppe $G$ und ein Element $g \in G$ . |   |
| Alice wählt $a \in \mathbb{N}$ , berechnet $g^a$ und macht es öffentlich.     |   | Bob wählt $b \in \mathbb{N}$ , berechnet $g^b$ und macht es öffentlich.     |
|   | $g^a, g^b$  |   |
| Nach dem öffentlichen Austausch berechnet Alice $(g^b)^a = g^{ba} = g^{ab}$ . |   | Nach dem öffentlichen Austausch berechnet Bob $(g^a)^b = g^{ab} = g^{ba}$ . |

Das Gruppenelement  $g^{ba} = g^{ab}$  ist der gemeinsame hoffentlich geheime Schlüssel. Der Trick hierbei besteht darin, geeignete Paare  $(G, g)$  und eine geeignete Zahl  $a$  so zu finden, daß die Berechnung von  $g^a$  unproblematisch ist, daß jedoch kein schneller Algorithmus bekannt ist, der aus der Kenntnis von  $G, g$  und  $g^a$  ein mögliches  $a$  bestimmt, der also, wie man auch sagt, einen **diskreten Logarithmus von  $g^a$  zur Basis  $g$**  findet. Dann kann Alice  $g^a$  veröffentlichen und dennoch  $a$  geheim halten und ebenso kann Bob  $g^b$  veröffentlichen und dennoch  $b$  geheim halten. Zum Beispiel kann man für  $G$  die Einheitengruppe  $G = (\mathbb{Z}/p\mathbb{Z})^\times$  des Primkörpers zu einer großen Primzahl  $p$  nehmen. Nun ist es natürlich denkbar, daß man aus der Kenntnis von  $g^a$  und  $g^b$  direkt  $g^{ab}$  berechnen kann, ohne zuvor  $a$  zu bestimmen, aber auch für die Lösung dieses sogenannten **Diffie-Hellman-Problems** ist in diesem Fall kein schneller Algorithmus bekannt. Mit den derzeitig verfügbaren Rechenmaschinen können also Alice und Bob mit einer Rechenzeit von unter einer Minute einen geheimen Schlüssel vereinbaren, dessen Entschlüsselung auf derselben Maschine beim gegenwärtigen Stand der veröffentlichten Forschung Millionen von Jahren bräuchte. Allerdings ist auch wieder nicht bewiesen, daß es etwa Fall der Einheitengruppe eines großen Primkörpers nicht doch einen effizienten Algorithmus zur Lösung des Diffie-Hellman-Problems geben könnte. Wenn wir Pech haben, sind die mathematischen Abteilungen irgendwelcher Geheimdienste

schon längst so weit.

*Vorschau 3.5.2.29.* Statt mit der Einheitengruppe endlicher Körper arbeitet man in der Praxis auch oft mit sogenannten „elliptischen Kurven“ alias Lösungsmengen kubischer Gleichungen, deren Gruppengesetz Sie in einer Vorlesung über algebraische Geometrie kennenlernen können.

**Definition 3.5.2.30.** Gegeben ein Ring  $R$  gibt es nach 3.5.1.10 genau einen Ringhomomorphismus  $\mathbb{Z} \rightarrow R$ . Dessen Kern alias das Urbild der Null ist nach 2.2.3.24 eine Untergruppe von  $\mathbb{Z}$  und hat nach 3.4.3.4 folglich die Gestalt  $m\mathbb{Z}$  für genau ein  $m \in \mathbb{N}$ . Diese natürliche Zahl  $m$  nennt man die **Charakteristik des Rings  $R$**  und notiert sie  $m = \text{char } R$ .

**3.5.2.31 (Bestimmung der Charakteristik eines Rings).** Um die Charakteristik eines Rings  $R$  zu bestimmen, müssen wir anders gesagt sein Einselement  $1 \in R$  nehmen und bestimmen, wieviele Summanden wir mindestens brauchen, damit gilt  $1 + 1 + \dots + 1 = 0$  mit einer positiven Zahl von Summanden links. Kriegen wir da überhaupt nie Null heraus, so ist die Charakteristik Null, wir haben also etwa  $\text{char } \mathbb{Z} = \text{char } \mathbb{Q} = \text{char } \mathbb{R} = \text{char } \mathbb{C} = 0$ . Gilt bereits  $1 = 0$ , so ist die Charakteristik 1 und wir haben den Nullring vor uns. Für  $p \in \mathbb{N}$  gilt allgemein  $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$ .

**3.5.2.32 (Die Charakteristik eines Körpers ist stets prim).** Es ist leicht zu sehen, daß die Charakteristik eines Körpers, wenn sie nicht Null ist, stets eine Primzahl sein muß: Da der Nullring kein Körper ist, kann die Charakteristik nicht 1 sein. Hätten wir aber einen Körper der Charakteristik  $m = ab > 0$  mit natürlichen Zahlen  $a < m$  und  $b < m$ , so wären die Bilder von  $a$  und  $b$  in unserem Körper von Null verschiedene Elemente mit Produkt Null. Widerspruch!

*Ergänzung 3.5.2.33.* Im Körper  $\mathbb{F}_7$  ist  $(-1)$  kein Quadrat, wie man durch Ausprobieren schnell prüft. Einen Körper mit 49 Elementen kann man deshalb nach 2.2.4.15 zum Beispiel erhalten, indem man analog wie bei der Konstruktion der komplexen Zahlen aus den reellen Zahlen formal eine Wurzel aus  $(-1)$  adjungiert.

## Übungen

*Ergänzende Übung 3.5.2.34.* Gegeben eine abelsche Gruppe  $V$  und ein Körper  $K$  induziert die kanonische Identifikation  $\text{Ens}(K \times V, V) \xrightarrow{\sim} \text{Ens}(K, \text{Ens}(V, V))$  aus 2.1.6.5 eine Bijektion

$$\left\{ \begin{array}{l} \text{Strukturen als } K\text{-Vektorraum} \\ \text{auf der abelschen Gruppe } V \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Ringhomomorphismen} \\ K \rightarrow \text{Ab } V \end{array} \right\}$$

Wir verwenden hier unsere alternative Notation  $\text{Ab } V$  für den Endomorphismenring der abelschen Gruppe  $V$ , um jede Verwechslung mit dem Endomorphismenring als Vektorraum auszuschließen.

*Übung 3.5.2.35.* Man finde das multiplikative Inverse der Nebenklasse von 22 im Körper  $\mathbb{F}_{31}$ . Hinweis: Euklidischer Algorithmus.

*Ergänzende Übung 3.5.2.36.* Man konstruiere einen Körper mit 49 Elementen und einen Körper mit 25 Elementen. Hinweis: 2.2.4.14 und 2.2.4.15.

*Ergänzende Übung 3.5.2.37.* Sei  $R$  ein Kring, dessen Charakteristik eine Primzahl  $p$  ist, für den es also einen Ringhomomorphismus  $\mathbb{Z}/p\mathbb{Z} \rightarrow R$  gibt. Man zeige, daß dann der sogenannte **Frobenius-Homomorphismus**  $F : R \rightarrow R$ ,  $a \mapsto a^p$  ein Ringhomomorphismus von  $R$  in sich selber ist. Hinweis: Man verwende, daß die binomische Formel 2.2.4.9 offensichtlich in jedem Kring gilt, ja sogar für je zwei Elemente  $a, b$  eines beliebigen Rings mit  $ab = ba$ .

*Ergänzende Übung 3.5.2.38.* Wieviele Untergruppen hat die abelsche Gruppe  $\mathbb{Z}/4\mathbb{Z}$ ? Wieviele Untergruppen hat die abelsche Gruppe  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ?

*Ergänzende Übung 3.5.2.39.* Eine natürliche Zahl ist durch 11 teilbar genau dann, wenn ihre „alternierende Quersumme“ durch 11 teilbar ist.

*Ergänzende Übung 3.5.2.40.* Eine natürliche Zahl, die kongruent zu sieben ist modulo acht, kann nicht eine Summe von drei Quadraten sein.

*Ergänzende Übung 3.5.2.41.* Eine Zahl mit einer Dezimaldarstellung der Gestalt  $abcabc$  wie zum Beispiel 349349 ist stets durch 7 teilbar.

*Ergänzende Übung 3.5.2.42.* Es kann in Ringen durchaus Elemente  $a$  geben, für die es zwar ein  $b$  gibt mit  $ba = 1$  aber kein  $c$  mit  $ac = 1$ : Man denke etwa an Endomorphismenringe unendlichdimensionaler Vektorräume. Wenn es jedoch  $b$  und  $c$  gibt mit  $ba = 1$  und  $ac = 1$ , so folgt bereits  $b = c$  und  $a$  ist eine Einheit.

*Übung 3.5.2.43.* Jeder Ringhomomorphismus macht Einheiten zu Einheiten. Jeder Ringhomomorphismus von einem Körper in einen vom Nullring verschiedenen Ring ist injektiv.

*Übung 3.5.2.44.* Sei  $p$  eine Primzahl. Eine abelsche Gruppe  $G$  kann genau dann mit der Struktur eines  $\mathbb{F}_p$ -Vektorraums versehen werden, wenn in additiver Notation gilt  $pg = 0$  für alle  $g \in G$ , und die fragliche Vektorraumstruktur ist dann durch die Gruppenstruktur eindeutig bestimmt.

*Ergänzende Übung 3.5.2.45.* Wieviele Untervektorräume hat ein zweidimensionaler Vektorraum über einem Körper mit fünf Elementen? Wieviele angeordnete Basen?

*Ergänzende Übung 3.5.2.46.* Gegeben ein Vektorraum über einem endlichen Primkörper sind seine Untervektorräume genau die Untergruppen der zugrundeliegenden abelschen Gruppe.

*Ergänzende Übung 3.5.2.47.* Man zeige: In jedem endlichen Körper ist das Produkt aller von Null verschiedenen Elemente  $(-1)$ . Hinweis: Man zeige zunächst,

daß nur die Elemente  $\pm 1$  ihre eigenen Inversen sind. Als Spezialfall erhält man die Kongruenz  $(p - 1)! \equiv -1 \pmod{p}$  für jede Primzahl  $p$ . Diese Aussage wird manchmal auch als **Satz von Wilson** zitiert. Ist  $n \in \mathbb{N}_{\geq 1}$  keine Primzahl, so zeigt man im übrigen leicht  $(n - 1)! \equiv 0 \pmod{n}$ .

*Übung 3.5.2.48.* Gegeben  $m \geq 1$  sind die Einheiten des Restklassenrings  $\mathbb{Z}/m\mathbb{Z}$  genau die Restklassen derjenigen Zahlen  $a$  mit  $0 \leq a < m$ , die zu  $m$  teilerfremd sind, in anderen Worten die primen Restklassen. In Formeln haben wir also  $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \mid 0 \leq a < m, \langle m, a \rangle = \langle 1 \rangle\}$ . Hinweis: 3.4.4.12.

*Übung 3.5.2.49.* Man zeige für Binomialkoeffizienten im Körper  $\mathbb{F}_p$  die Identität  $\binom{p-1}{i} = (-1)^i$ .

### 3.5.3 Polynome

3.5.3.1. Ist  $R$  ein Ring, so bildet die Menge  $R[X]$  aller „formalen Ausdrücke“ der Gestalt  $a_nX^n + \dots + a_1X + a_0$  mit  $a_i \in R$  unter der offensichtlichen Addition und Multiplikation einen Ring, den **Polynomring über  $R$  in einer Variablen  $X$** , und wir haben eine offensichtliche Einbettung  $\text{can} : R \hookrightarrow R[X]$ . Die Herkunft der Bezeichnung diskutieren wir in **??**. Die  $a_\nu$  heißen in diesem Zusammenhang die **Koeffizienten** unseres Polynoms, genauer heißt  $a_\nu$  der **Koeffizient von  $X^\nu$** . Das  $X$  heißt die **Variable** unseres Polynoms und kann auch schon mal mit einem anderen Buchstaben bezeichnet werden. Besonders gebräuchlich sind hierbei Großbuchstaben vom Ende des Alphabets. Diese Beschreibung des Polynomrings ist hoffentlich verständlich, sie ist aber nicht so exakt, wie eine Definition es sein sollte. Deshalb geben wir auch noch eine exakte Variante.

**Definition 3.5.3.2.** Sei  $R$  ein Ring. Wir bezeichnen mit  $R[X]$  die Menge aller Abbildungen  $\varphi : \mathbb{N} \rightarrow R$ , die nur an endlich vielen Stellen von Null verschiedene Werte annehmen, und definieren auf  $R[X]$  eine Addition und eine Multiplikation durch die Regeln

$$\begin{aligned} (\varphi + \psi)(n) &:= \varphi(n) + \psi(n) \\ (\varphi \cdot \psi)(n) &:= \sum_{i+j=n} \varphi(i)\psi(j) \end{aligned}$$

Mit diesen Verknüpfungen wird  $R[X]$  ein Ring, der **Polynomring über  $R$** . Ordnen wir jedem  $a \in R$  die Abbildung  $\mathbb{N} \rightarrow R$  zu, die bei 0 den Wert  $a$  annimmt und sonst den Wert Null, so erhalten wir eine Einbettung, ja einen injektiven Ringhomomorphismus

$$\text{can} : R \hookrightarrow R[X]$$

Wir notieren ihn schlicht  $a \mapsto a$  und nennen die Polynome im Bild dieser Einbettung **konstante Polynome**. Bezeichnen wir weiter mit  $X$  die Abbildung  $\mathbb{N} \rightarrow R$ , die bei 1 den Wert 1 annimmt und sonst nur den Wert Null, so können wir jede

Abbildung  $\varphi \in R[X]$  eindeutig schreiben in der Form  $\varphi = \sum_{\nu} \varphi(\nu)X^{\nu}$  und sind auf einem etwas formaleren Weg wieder am selben Punkt angelangt.

*Ergänzung 3.5.3.3.* Im Fall eines Körpers  $K$  ist insbesondere  $K[X]$  als Gruppe per definitionem der freie  $K$ -Vektorraum  $K[X] := K\langle \mathbb{N} \rangle$  über der Menge  $\mathbb{N}$  der natürlichen Zahlen.

3.5.3.4. Die wichtigste Eigenschaft eines Polynomrings ist, daß man „für die Variable etwas einsetzen darf“. Das wollen wir nun formal aufschreiben.

**Proposition 3.5.3.5 (Einsetzen in Polynome).** *Seien  $R$  ein Kring und  $b \in R$  ein Element. So gibt es genau einen Ringhomomorphismus*

$$E_b : R[X] \rightarrow R$$

mit  $E_b(X) = b$  und  $E_b \circ \text{can} = \text{id}_R$ . Wir nennen  $E_b$  den **Einsetzungshomomorphismus zu  $b$** .

*Beweis.* Dieser eindeutig bestimmte Ringhomomorphismus  $E_b$  ist eben gegeben durch die Vorschrift  $E_b(a_nX^n + \dots + a_1X + a_0) = a_nb^n + \dots + a_1b + a_0$ .  $\square$

3.5.3.6. Es ist üblich, das Bild unter dem Einsetzungshomomorphismus  $E_b$  eines Polynoms  $P \in R[X]$  abzukürzen als

$$P(b) := E_b(P)$$

Ich verwende später meist die Notation  $E_b = \delta_b$ , die die Interpretation als „Dirac-Maß“ anklingen läßt.

3.5.3.7. Unsere übliche Darstellung einer Zahl in Zifferschreibweise läuft darauf hinaus, die Koeffizienten eines Polynoms anzugeben, das an der Stelle 10 die besagte Zahl als Wert ausgibt, also etwa  $7258 = P(10)$  für  $P(X)$  das Polynom  $7X^3 + 2X^2 + 5X + 8$ .

3.5.3.8. Es geht auch noch allgemeiner, man darf etwa über einem Körper auch quadratische Matrizen in Polynome einsetzen. Um das zu präzisieren, vereinbaren wir die Sprechweise, daß zwei Elemente  $b$  und  $c$  eines Rings **kommutieren**, wenn gilt  $bc = cb$ . Das bedeutet also, daß sie in Bezug auf die Multiplikation kommutieren im Sinne von 2.2.1.7.

**Proposition 3.5.3.9 (Einsetzen in Polynome, Variante).** *Seien  $\varphi : R \rightarrow S$  ein Ringhomomorphismus und  $b \in S$  ein Element derart, daß  $b$  für alle  $a \in R$  mit  $\varphi(a)$  **kommutiert**. So gibt es genau einen Ringhomomorphismus*

$$E_{\varphi,b} = E_b : R[X] \rightarrow S$$

mit  $E_b(X) = b$  und  $E_b \circ \text{can} = \varphi$ . Wir nennen  $E_{\varphi,b}$  den **Einsetzungshomomorphismus zu  $b$  über  $\varphi$** .

*Beweis.* Dieser eindeutig bestimmte Ringhomomorphismus  $E_b$  ist gegeben durch die Vorschrift  $E_b(a_nX^n + \dots + a_1X + a_0) := \varphi(a_n)b^n + \dots + \varphi(a_1)b + \varphi(a_0)$ .  $\square$

3.5.3.10. Es ist auch in dieser Allgemeinheit üblich, das Bild unter dem Einsetzungshomomorphismus  $E_{\varphi,b}$  eines Polynoms  $P \in R[X]$  abzukürzen als

$$P(b) := E_{\varphi,b}(P)$$

So schreiben wir im Fall eines Krings  $R$  zum Beispiel  $P(A)$  für die Matrix, die beim Einsetzen einer quadratischen Matrix  $A \in \text{Mat}(n; R)$  in das Polynom  $P$  entsteht. In diesem Fall hätten wir  $S = \text{Mat}(n; R)$  und  $\varphi$  wäre der Ringhomomorphismus, der jedem  $a \in R$  das  $a$ -fache der Einheitsmatrix zuordnet.

3.5.3.11 (**Wechsel der Koeffizienten**). Ist  $\varphi : R \rightarrow S$  ein Ringhomomorphismus, so erhalten wir einen Ringhomomorphismus  $\varphi = \varphi_{[X]} : R[X] \rightarrow S[X]$  der zugehörigen Polynomringe durch das „Anwenden von  $\varphi$  auf die Koeffizienten“. Formal können wir ihn als das „Einsetzen von  $X$  für  $X$  über  $\varphi$ “ beschreiben, also als den Ringhomomorphismus  $\varphi_{[X]} = E_{\varphi,X}$ .

**Definition 3.5.3.12.** Seien  $R$  ein Kring und  $P \in R[X]$  ein Polynom. Ein Element  $a \in R$  heißt eine **Nullstelle** oder auch eine **Wurzel** von  $P$ , wenn gilt  $P(a) = 0$ .

**Definition 3.5.3.13.** Sei  $R$  ein Ring. Jedem Polynom  $P \in R[X]$  ordnen wir seinen **Grad**  $\text{grad } P \in \mathbb{N} \sqcup \{-\infty\}$  (englisch **degree**, französisch **degré**) durch die Vorschrift

$$\begin{aligned} \text{grad } P = n &\quad \text{für } P = a_nX^n + \dots + a_1X + a_0 \text{ mit } a_n \neq 0; \\ \text{grad } P = -\infty &\quad \text{für } P \text{ das Nullpolynom.} \end{aligned}$$

Für ein von Null verschiedenes Polynom  $P = a_nX^n + \dots + a_1X + a_0$  mit  $n = \text{grad } P$  nennt man  $a_n \in R \setminus 0$  seinen **Leitkoeffizienten**. Den Leitkoeffizienten des Nullpolynoms erklären wir als die Null von  $R$ . Ein Polynom heißt **normiert**, wenn sein Leitkoeffizient 1 ist. Das Nullpolynom ist demnach nur über dem Nullring normiert, hat aber auch dort den Grad  $-\infty$ . Auf Englisch heißen unsere normierten Polynome **monic polynomials**. Ein Polynom vom Grad Eins heißt **linear**, ein Polynom vom Grad Zwei **quadratisch**, ein Polynom vom Grad Drei **kubisch**.

**Lemma 3.5.3.14 (Grad eines Produkts).** *Ist  $R$  ein Integritätsring, so ist auch der Polynomring  $R[X]$  ein Integritätsring und der Grad eines Produkts ist die Summe der Grade der Faktoren, in Formeln*

$$\text{grad}(PQ) = \text{grad } P + \text{grad } Q$$

*Beweis.* Ist  $R$  ein Integritätsring, so ist offensichtlich der Leitkoeffizient von  $PQ$  das Produkt der Leitkoeffizienten von  $P$  und von  $Q$ .  $\square$

**Lemma 3.5.3.15 (Polynomdivision mit Rest).** Sei  $R$  ein Ring. Gegeben Polynome  $P, Q \in R[X]$  mit  $Q$  normiert gibt es eindeutig bestimmte Polynome  $A, B$  mit  $P = AQ + B$  und  $\text{grad } B \leq (\text{grad } Q) - 1$ .

*Beispiel 3.5.3.16.* Die Polynomdivision mit Rest des Polynoms  $X^4 + 2X^2$  durch  $X^2 + 2X + 1$  liefert

$$\begin{aligned} X^4 + 2X^2 &= X^2(X^2 + 2X + 1) - 2X^3 + X^2 \\ &= X^2(X^2 + 2X + 1) - 2X(X^2 + 2X + 1) + 5X^2 + 2X \\ &= (X^2 - 2X + 5)(X^2 + 2X + 1) - 8X - 5 \end{aligned}$$

*Beweis.* Ich habe mir bei der Formulierung des Lemmas Mühe gegeben, daß es auch im Fall des Nullrings  $R = 0$  richtig ist, wenn wir  $-\infty - 1 = -\infty$  verstehen. Für den Beweis dürfen wir damit annehmen, daß  $R$  nicht der Nullring ist. Wir suchen ein Polynom  $A$  mit  $\text{grad}(P - AQ)$  kleinstmöglich. Gälte dennoch  $\text{grad}(P - AQ) \geq (\text{grad}(Q))$ , sagen wir  $B := P - AQ = aX^r + \dots + c$  mit  $a \neq 0$  und  $r > d = \text{grad}(Q)$ , so hätte  $P - (A + aX^{r-d})Q$  echt kleineren Grad als  $B$ , im Widerspruch zur Wahl von  $A$ . Das zeigt die Existenz. Für den Nachweis der Eindeutigkeit gehen wir aus von einer weiteren Gleichung  $P = A'Q + B'$  mit  $\text{grad } B' < d$ . Es folgt zunächst  $(A - A')Q = B' - B$  und wegen der offensichtlichen Formel für den Grad des Produkts eines beliebigen Polynoms mit einem normierten Polynom weiter  $A - A' = 0$  und dann auch  $B' - B = 0$ .  $\square$

**Korollar 3.5.3.17 (Abspalten von Linearfaktoren bei Nullstellen).** Sei  $R$  ein Ring und  $P \in R[X]$  ein Polynom. Genau dann ist  $\lambda \in R$  eine Nullstelle von  $P$ , wenn das Polynom  $(X - \lambda)$  das Polynom  $P$  teilt, in Formeln

$$P(\lambda) = 0 \Leftrightarrow (X - \lambda)|P$$

*Beweis.* Nach Lemma 3.5.3.15 über die Division mit Rest finden wir ein Polynom  $A \in R[X]$  und eine Konstante  $b \in R$  mit  $P = A(X - \lambda) + b$ . Einsetzen von  $\lambda$  für  $X$  liefert dann  $b = 0$ .  $\square$

3.5.3.18. Der im Sinne von 3.5.3.13 lineare Faktor  $(X - \lambda)$  unseres Polynoms heißt auch ein **Linearfaktor**, daher der Name des Korollars.

**Satz 3.5.3.19 (Zahl der Nullstellen eines Polynoms).** Ist  $K$  ein Körper oder allgemeiner ein kommutativer Integritätsring, so hat ein von Null verschiedenes Polynom  $P \in K[X]$  höchstens  $\text{grad } P$  Nullstellen in  $K$ .

*Beweis.* Ist  $\lambda \in K$  eine Nullstelle, so finden wir nach 3.5.3.17 eine Darstellung  $P = A(X - \lambda)$  mit  $\text{grad } A = \text{grad } P - 1$ . Eine von  $\lambda$  verschiedene Nullstelle von  $P$  ist für  $K$  ein Integritätsring notwendig eine Nullstelle von  $A$  und der Satz folgt mit Induktion.  $\square$

*Beispiel 3.5.3.20.* In einem Körper  $K$  oder allgemeiner einem kommutativen Integritätsring gibt es zu jedem Element  $b \in K$  höchstens zwei Elemente  $a \in K$  mit  $a^2 = b$ . Ist nämlich  $a$  eine Lösung dieser Gleichung, so gilt  $X^2 - b = (X - a)(X + a)$ , und wenn wir da für  $X$  etwas von  $\pm a$  Verschiedenes einsetzen, kommt sicher nicht Null heraus.

*Ergänzung 3.5.3.21.* Die Kommutativität ist hierbei wesentlich. In 3.5.6.4 werden wir den sogenannten „Schiefkörper der Quaternionen“ einführen, einen Ring, der außer der Kommutativität der Multiplikation alle unsere Körperaxiome erfüllt. In diesem Ring hat die Gleichung  $X^2 = -1$  dann offensichtlich die sechs Lösungen  $\pm i, \pm j, \pm k$  und nicht ganz so offensichtlich ?? sogar unendlich viele Lösungen.

3.5.3.22. Ist  $K$  ein Körper oder allgemeiner ein Kring,  $P \in K[X]$  ein Polynom und  $\lambda \in K$  eine Nullstelle von  $P$ , so nennen wir das Supremum über alle  $n \in \mathbb{N}$  mit  $(X - \lambda)^n | P$  die **Vielfachheit der Nullstelle**  $\lambda$  oder auch ihre **Ordnung**. Das Nullpolynom hat insbesondere an jeder Stelle eine Nullstelle der Vielfachheit  $\infty$  und gar keine Nullstelle bei  $\lambda$  ist dasselbe wie eine „Nullstelle der Vielfachheit Null“. Durch Abspalten von Nullstellen wie in 3.5.3.17 zeigt man, daß im Fall eines Körpers oder allgemeiner eines kommutativen Integritätsrings auch die Zahl der mit ihren Vielfachheiten gezählten Nullstellen eines von Null verschiedenen Polynoms beschränkt ist durch seinen Grad.

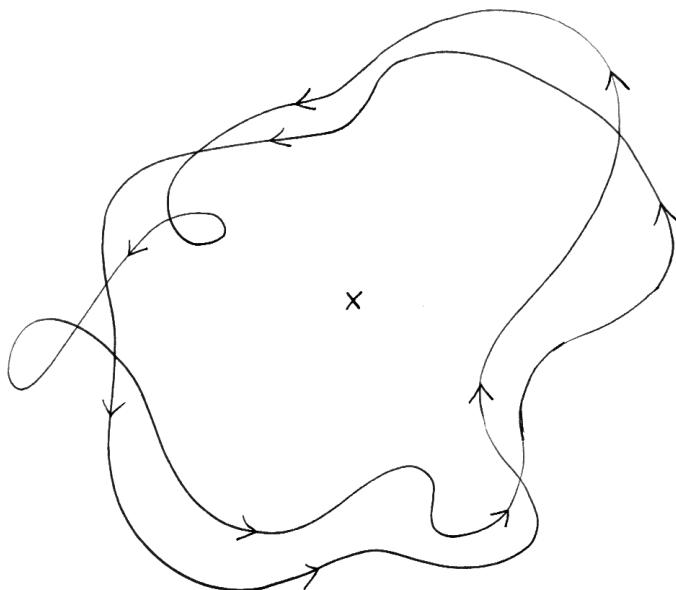
**Definition 3.5.3.23.** Ein Körper  $K$  heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom  $P \in K[X] \setminus K$  mit Koeffizienten in unserem Körper  $K$  eine Nullstelle in unserem Körper  $K$  hat.

*Beispiel 3.5.3.24.* Der Körper  $K = \mathbb{R}$  ist nicht algebraisch abgeschlossen, denn das Polynom  $X^2 + 1$  hat keine reelle Nullstelle.

*Vorschau 3.5.3.25.* Der Körper  $\mathbb{C}$  der komplexen Zahlen ist algebraisch abgeschlossen. Das ist die Aussage des sogenannten **Fundamentalsatzes der Algebra**, für den wir mehrere Beweise geben werden: Einen besonders elementaren Beweis nach Argand in der Analysis in ??, einen sehr eleganten mit den Methoden der Funktionentheorie in ??, und einen mehr algebraischen Beweis, bei dem die Analysis nur über den Zwischenwertsatz eingeht, in ?. Mir selbst gefällt der noch wieder andere Beweis mit den Mitteln der Topologie ?? am besten, da er meine Anschauung am meisten anspricht. Er wird in analytischer Verkleidung bereits in ?? vorgeführt. Eine heuristische Begründung wird in nebenstehendem Bild gegeben.

**Satz 3.5.3.26.** Ist  $K$  ein algebraisch abgeschlossener Körper, so hat jedes von Null verschiedene Polynom  $P \in K[X] \setminus 0$  eine **Zerlegung in Linearfaktoren der Gestalt**

$$P = c(X - \lambda_1) \dots (X - \lambda_n)$$



Heuristische Begründung für den Fundamentalsatz der Algebra. Ein Polynom  $n$ -ten Grades wird eine sehr große Kreislinie in der komplexen Zahlenebene mit Zentrum im Ursprung abbilden auf einen Weg in der komplexen Zahlenebene, der „den Ursprung  $n$ -mal umläuft“. Angedeutet ist etwa das Bild einer sehr großen Kreislinie unter einem Polynom vom Grad Zwei. Schrumpfen wir nun unsere sehr große Kreislinie zu immer kleineren Kreislinien bis auf einen Punkt, so schrumpfen auch diese Wege zu einem konstanten Weg zusammen. Unsere  $n$ -fach um einen etwa am Ursprung aufgestellten Pfahl laufende Seilschlinge kann jedoch offensichtlich nicht auf einen Punkt zusammengezogen werden, ohne daß wir sie über den Pfahl heben, anders gesagt: Mindestens eines der Bilder dieser kleineren Kreislinien muß durch den Ursprung laufen, als da heißt, unser Polynom muß auf mindestens einer dieser kleineren Kreislinien eine Nullstelle habe. In ?? oder besser ?? werden wir diese Heuristik zu einem formalen Beweis ausbauen.

mit  $n \geq 0$ ,  $c \in K^\times$  und  $\lambda_1, \dots, \lambda_n \in K$ . Darauf hinaus ist diese Zerlegung eindeutig bis auf die Reihenfolge der Faktoren.

3.5.3.27. Gegeben eine Nullstelle  $\mu$  von  $P$  ist in diesem Fall die Zahl der Indizes  $i$  mit  $\lambda_i = \mu$  die Vielfachheit der Nullstelle  $\mu$ . In der Sprache der Multimengen aus 2.1.6.8 erhalten wir für jeden algebraisch abgeschlossenen Körper  $K$  eine Bijektion zwischen der Menge aller „endlichen Multimengen von Elementen von  $K$ “ und der Menge aller normierten Polynome mit Koeffizienten in  $K$ , indem wir einer Multimenge  ${}_\mu\{\lambda_1, \dots, \lambda_n\}$  das Polynom  $(X - \lambda_1) \dots (X - \lambda_n)$  zuordnen.

*Beweis.* Ist  $P$  ein konstantes Polynom, so ist nichts zu zeigen. Ist  $P$  nicht konstant, so gibt es nach Annahme eine Nullstelle  $\lambda \in K$  von  $P$  und wir finden genau ein Polynom  $\tilde{P}$  mit  $P = (X - \lambda)\tilde{P}$ . Der Satz folgt durch vollständige Induktion über den Grad von  $P$ .  $\square$

**Korollar 3.5.3.28 (Faktorisierung reeller Polynome).** *Jedes von Null verschiedene Polynom  $P$  mit reellen Koeffizienten besitzt eine Zerlegung in Faktoren der Gestalt*

$$P = c(X - \lambda_1) \dots (X - \lambda_r)(X^2 + \mu_1 X + \nu_1) \dots (X^2 + \mu_s X + \nu_s)$$

mit  $c, \lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_s, \nu_1, \dots, \nu_s \in \mathbb{R}$  derart, daß die quadratischen Faktoren keine reellen Nullstellen haben. Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.

*Beweis.* Da unser Polynom invariant ist unter der komplexen Konjugation, müssen sich seine mit ihren Vielfachheiten genommenen komplexen Nullstellen so durchnummernieren lassen, daß  $\lambda_1, \dots, \lambda_r$  reell sind und daß eine gerade Zahl nicht reeller Nullstellen übrigbleibt mit  $\lambda_{r+2t-1} = \bar{\lambda}_{r+2t}$  für  $1 \leq t \leq s$  und  $r, s \geq 0$ . Die Produkte  $(X - \lambda_{r+2t-1})(X - \lambda_{r+2t})$  haben dann reelle Koeffizienten, da sie ja invariant sind unter der komplexen Konjugation, haben jedoch keine reellen Nullstellen.  $\square$

*Vorschau 3.5.3.29.* In der Algebra ?? können Sie lernen, inwiefern sowohl die vorhergehenden Aussagen über die Faktorisierung von Polynomen als auch die Primfaktorzerlegung natürlicher Zahlen Spezialfälle eines allgemeinen Satzes über die „Faktorialität euklidischer Ringe“ sind.

3.5.3.30 (**Polynomringe in mehreren Variablen**). Ähnlich wie den Polynomring in einer Variablen 3.5.3.2 konstruiert man auch Polynomringe in mehr Variablen über einem gegebenen Grundring  $R$ . Ist die Zahl der Variablen endlich, so kann man induktiv definieren

$$R[X_1, \dots, X_n] = (R[X_1, \dots, X_{n-1}])[X_n]$$

Man kann aber auch für eine beliebige Menge  $I$  den Polynomring  $R[X_i]_{i \in I}$  bilden als die Menge aller „endlichen formalen Linearkombinationen mit Koeffizienten aus  $R$  von endlichen Monomen in den  $X_i$ “. Ich verzichte an dieser Stelle auf eine formale Definition.

*Ergänzung 3.5.3.31.* Bei Hochster kann man ein Beispiel für nichtisomorphe kommutative Ringe  $A \not\cong B$  finden, deren Polynomringe in einer Variablen doch isomorph sind,  $A[T] \cong B[T]$ . Die Konstruktion eines derartigen Beispiels ist aber bereits höhere Mathematik und für uns an dieser Stelle nicht relevant.

## Übungen

*Übung 3.5.3.32.* Welche Matrix entsteht beim Einsetzen der quadratischen Matrix  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  in das Polynom  $X^2 + 1$ ?

*Ergänzende Übung 3.5.3.33.* Man zeige, daß jede Nullstelle  $\alpha \in \mathbb{C}$  eines normierten Polynoms mit komplexen Koeffizienten  $X^n + a_{n-1}X^{n-1} + \dots + a_0$  die Abschätzung  $|\alpha| \leq 1 + |a_{n-1}| + \dots + |a_0|$  erfüllt. Hinweis: Sonst gilt erst  $|\alpha| > 1$  und dann  $|\alpha|^n > |a_{n-1}\alpha^{n-1}| + \dots + |a_0|$ . Umgekehrt zeige man auch, daß aus der Abschätzung  $|\alpha| \leq C$  für alle komplexen Wurzeln die Abschätzung  $|a_k| \leq \binom{n}{k}C^{n-k}$  für die Koeffizienten folgt.

*Übung 3.5.3.34.* Ist  $P \in \mathbb{R}[X]$  ein Polynom mit reellen Koeffizienten und  $\mu \in \mathbb{C}$  eine komplexe Zahl, so gilt  $P(\mu) = 0 \Rightarrow P(\bar{\mu}) = 0$ . Ist also eine komplexe Zahl Nullstelle eines Polynoms mit reellen Koeffizienten, so ist auch die konjugiert komplexe Zahl eine Nullstelle desselben Polynoms.

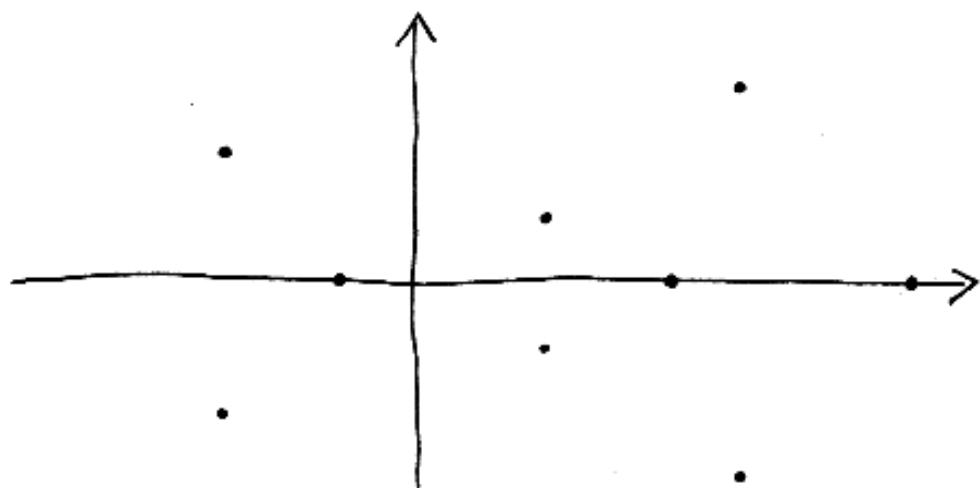
*Ergänzende Übung 3.5.3.35.* Seien  $k, K$  kommutative Ringe,  $i : k \rightarrow K$  ein Ringhomomorphismus und  $i : k[X] \rightarrow K[X]$  der induzierten Ringhomomorphismus zwischen den zugehörigen Polynomringen. Man zeige: Ist  $\lambda \in k$  eine Nullstelle eines Polynoms  $P \in k[X]$ , so ist  $i(\lambda) \in K$  eine Nullstelle des Polynoms  $i(P)$ .

*Ergänzende Übung 3.5.3.36.* Ist  $K$  ein Integritätsbereich, so induziert die kanonische Einbettung  $K \hookrightarrow K[X]$  auf den Einheitengruppen eine Bijektion  $K^\times \xrightarrow{\sim} K[X]^\times$ . Im Ring  $(\mathbb{Z}/4\mathbb{Z})[X]$  aber ist etwa auch  $\bar{1} + \bar{2}X$  eine Einheit.

*Übung 3.5.3.37.* Man zeige, daß es in einem endlichen Körper  $\mathbb{F}$  einer von 2 verschiedenen Charakteristik genau  $(|\mathbb{F}| + 1)/2$  Quadrate gibt, wohingegen in einem endlichen Körper der Charakteristik 2 jedes Element das Quadrat eines weiteren Elements ist.

*Übung 3.5.3.38.* Man zerlege das Polynom  $X^4 + 2$  in  $\mathbb{R}[X]$  in der in 3.5.3.28 beschriebenen Weise in ein Produkt quadratischer Faktoren ohne Nullstelle.

*Ergänzende Übung 3.5.3.39.* Ein reelles Polynom hat bei  $\lambda \in \mathbb{R}$  eine mehrfache Nullstelle genau dann, wenn auch seine Ableitung bei  $\lambda$  verschwindet.



Die komplexen Nullstellen eines Polynoms mit reellen Koeffizienten, die nicht reell sind, tauchen immer in Paaren aus einer Wurzel und ihrer komplex Konjugierten auf, vergleiche auch Übung 3.5.3.34.

*Ergänzende Übung 3.5.3.40.* Gegeben ein reelles Polynom, dessen komplexe Nullstellen bereits sämtlich reell sind, ist jede Nullstelle seiner Ableitung reell und wenn sie keine Nullstelle der Funktion selbst ist, eine einfache Nullstelle der Ableitung. Hinweis: Zwischen je zwei Nullstellen unserer Funktion muß mindestens eine Nullstelle ihrer Ableitung liegen.

*Ergänzende Übung 3.5.3.41.* Man zeige: Die rationalen Nullstellen eines normierten Polynoms mit ganzzahligen Koeffizienten  $P \in \mathbb{Z}[X]$  sind bereits alle ganz. In Formeln folgt aus  $P(\lambda) = 0$  für  $\lambda \in \mathbb{Q}$  also bereits  $\lambda \in \mathbb{Z}$ .

*Ergänzende Übung 3.5.3.42.* Gegeben ein Ring  $R$  bilden auch die **formalen Potenzreihen mit Koeffizienten in  $R$**  der Gestalt  $\sum_{n \geq 0} a_n X^n$  mit  $a_n \in R$  einen Ring, der meist  $R[[X]]$  notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß seine Einheiten genau diejenigen Potenzreihen sind, deren konstanter Term eine Einheit in  $R$  ist, in Formeln

$$R[[X]]^\times = R^\times + X R[[X]]$$

Man verallgemeinere die Definition und Beschreibung der Einheiten auf Potenzreihenringe  $R[[X_1, \dots, X_n]]$  in mehreren Variablen und konstruiere einen Ringisomorphismus

$$(R[[X_1, \dots, X_n]])[X_{n+1}] \xrightarrow{\sim} R[[X_1, \dots, X_n, X_{n+1}]]$$

*Ergänzende Übung 3.5.3.43.* Gegeben ein Ring  $R$  bilden auch die **formalen Laurentreihen mit Koeffizienten in  $R$**  der Gestalt  $\sum_{n \geq -N} a_n X^n$  mit  $a_n \in R$  und  $N \in \mathbb{N}$  einen Ring, der meist  $R((X))$  notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß im Fall  $R \neq 0$  seine Einheiten genau diejenigen von Null verschiedenen Reihen sind, bei denen der Koeffizient der kleinsten mit von Null verschiedenem Koeffizienten auftauchenden Potenz von  $X$  eine Einheit in  $R$  ist, in Formeln

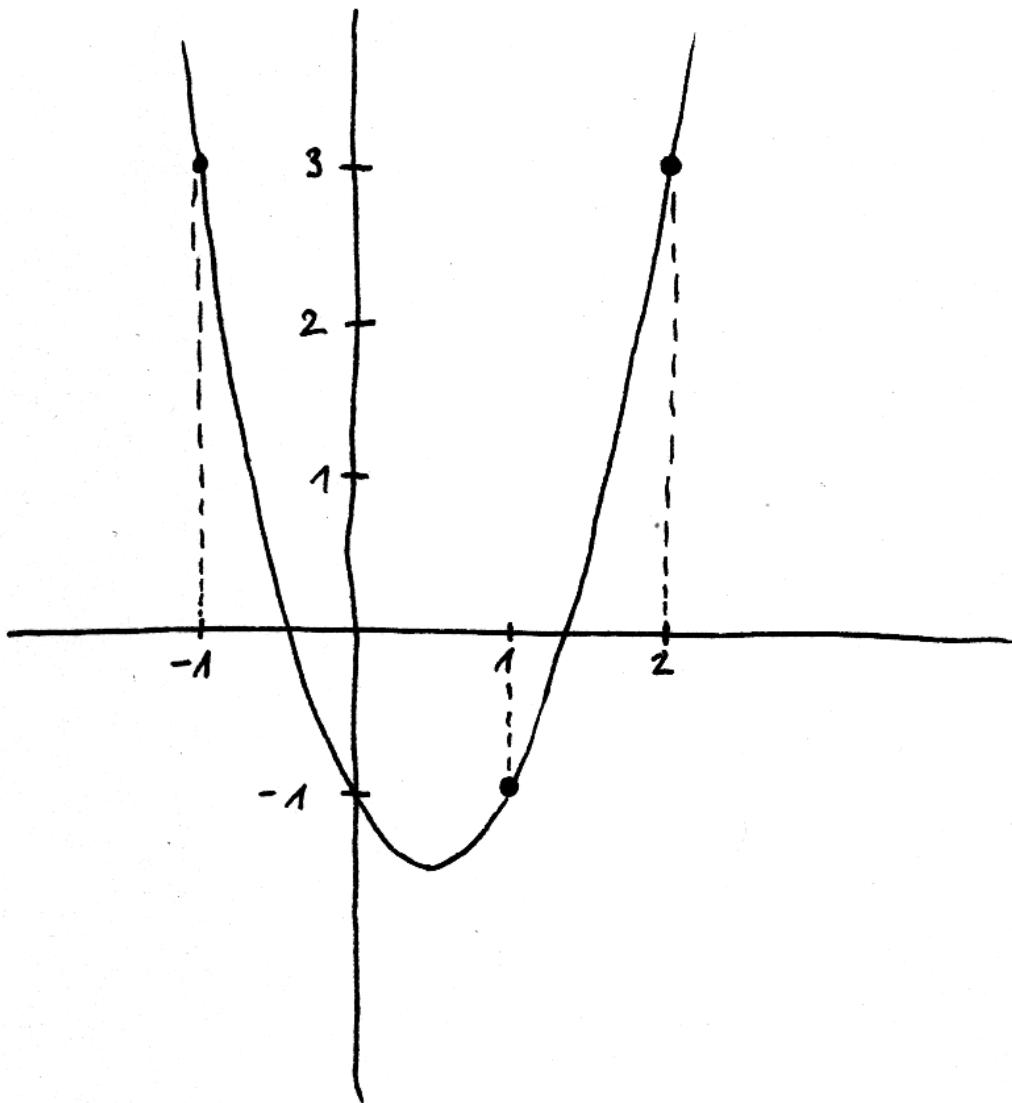
$$R((X))^\times = \bigcup_{n \in \mathbb{Z}} X^n R[[X]]^\times$$

Insbesondere ist im Fall eines Körpers  $K$  auch  $K((X))$  ein Körper.

*Ergänzung 3.5.3.44.* Wir verwenden hier die Terminologie, nach der bei **formalen Laurentreihen** im Gegensatz zu den Laurentreihen der Funktionentheorie nur endlich viele Terme mit negativen Exponenten erlaubt sind.

### 3.5.4 Polynome als Funktionen\*

**Lemma 3.5.4.1 (Interpolation durch Polynome).** *Seien  $K$  ein Körper und  $x_0, \dots, x_n \in K$  paarweise verschiedene **Stützstellen** und  $y_0, \dots, y_n \in K$  beliebig vorgegebene Werte. So gibt es genau ein Polynom  $P \in K[X]$  vom Grad  $\leq n$  mit  $P(x_0) = y_0, \dots, P(x_n) = y_n$ .*



Das Polynom  $P(X) = 2X^2 - 2X - 1$  mit reellen Koeffizienten, das die an den Stützstellen  $-1, 1, 2$  vorgegebenen Werte  $3, -1, 3$  interpoliert.

*Beweis.* Zunächst ist sicher  $(X - x_1) \dots (X - x_n) =: A_0(X)$  ein Polynom vom Grad  $n$ , das bei  $x_1, \dots, x_n$  verschwindet und an allen anderen Stellen von Null verschieden ist, insbesondere auch bei  $x_0$ . Dann ist  $L_0(X) := A_0(X)/A_0(x_0)$  ein Polynom vom Grad  $n$ , das bei  $x_0$  den Wert Eins annimmt und bei  $x_1, \dots, x_n$  verschwindet. In derselben Weise konstruieren wir auch Polynome  $L_1(X), \dots, L_n(X)$  und erhalten ein mögliches Interpolationspolynom als

$$P(X) = y_0 L_0(X) + \dots + y_n L_n(X) = \sum_{i=0}^n y_i \frac{\prod_{j \neq i} (X - x_j)}{\prod_{j \neq i} (x_i - x_j)}$$

Das zeigt die Existenz. Ist  $Q$  eine weitere Lösung derselben Interpolationsaufgabe vom Grad  $\leq n$ , so ist  $P - Q$  ein Polynom vom Grad  $\leq n$  mit  $n+1$  Nullstellen, eben bei den Stützstellen  $x_0, \dots, x_n$ . Wegen 3.5.3.19 muß dann aber  $P - Q$  das Nullpolynom sein, und das zeigt die Eindeutigkeit.  $\square$

3.5.4.2. Um die bisher eingeführten algebraischen Konzepte anschaulicher zu machen, will ich sie in Bezug setzen zu geometrischen Konzepten. Ist  $K$  ein Kring, so können wir jedem Polynom  $f \in K[X_1, \dots, X_n]$  die Funktion  $\tilde{f} : K^n \rightarrow K$ ,  $(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$  zuordnen. Wir erhalten so einen Ringhomomorphismus

$$K[X_1, \dots, X_n] \rightarrow \text{Ens}(K^n, K)$$

Dieser Homomorphismus ist im Allgemeinen weder injektiv noch surjektiv. Schon für  $n = 1$ ,  $K = \mathbb{R}$  lässt sich ja keineswegs jede Abbildung  $\mathbb{R} \rightarrow \mathbb{R}$  durch ein Polynom beschreiben, also ist sie in diesem Fall nicht surjektiv. Im Fall eines endlichen Körpers  $K$  kann weiter für  $n \geq 1$  unsere  $K$ -lineare Auswertungsabbildung vom unendlichdimensionalen  $K$ -Vektorraum  $K[X_1, \dots, X_n]$  in den endlichdimensionalen  $K$ -Vektorraum  $\text{Ens}(K^n, K)$  unmöglich injektiv sein. Wir haben jedoch den folgenden Satz.

**Satz 3.5.4.3 (Polynome als Funktionen).** 1. Ist  $K$  ein unendlicher Körper, ja allgemeiner ein unendlicher Integritätsring, so ist für alle  $n \in \mathbb{N}$  die Auswertungsabbildung eine Injektion  $K[X_1, \dots, X_n] \hookrightarrow \text{Ens}(K^n, K)$ ;  
2. Ist  $K$  ein endlicher Körper, so ist für alle  $n \in \mathbb{N}$  die Auswertungsabbildung eine Surjektion  $K[X_1, \dots, X_n] \twoheadrightarrow \text{Ens}(K^n, K)$ . Den Kern dieser Surjektion beschreibt Übung 4.4.3.19.

*Beweis.* 1. Durch Induktion über  $n$ . Der Fall  $n = 0$  ist eh klar. Für  $n = 1$  folgt die Behauptung aus der Erkenntnis, dass jedes von Null verschiedene Polynom in  $K[X]$  nur endlich viele Nullstellen in  $K$  haben kann. Der Kern der Abbildung

$$K[X] \rightarrow \text{Ens}(K, K)$$

besteht also nur aus dem Nullpolynom. Für den Induktionsschritt setzen wir  $X_n = Y$  und schreiben unser Polynom in der Gestalt

$$P = a_d Y^d + \dots + a_1 Y + a_0$$

mit  $a_i \in K[X_1, \dots, X_{n-1}]$ . Halten wir  $(x_1, \dots, x_{n-1}) = x \in K^{n-1}$  fest, so ist  $a_d(x)Y^d + \dots + a_1(x)Y + a_0(x) \in K[Y]$  das Nullpolynom nach dem Fall  $n = 1$ . Also verschwinden  $a_d(x), \dots, a_1(x), a_0(x)$  für alle  $x \in K^{n-1}$ , mit Induktion sind somit alle  $a_i$  schon das Nullpolynom und wir haben  $P = 0$ .

2. Das bleibt dem Leser überlassen. Man mag sich beim Beweis an 3.5.4.1 orientieren. Wir folgern in ?? eine allgemeinere Aussage aus dem abstrakten chinesischen Restsatz.  $\square$

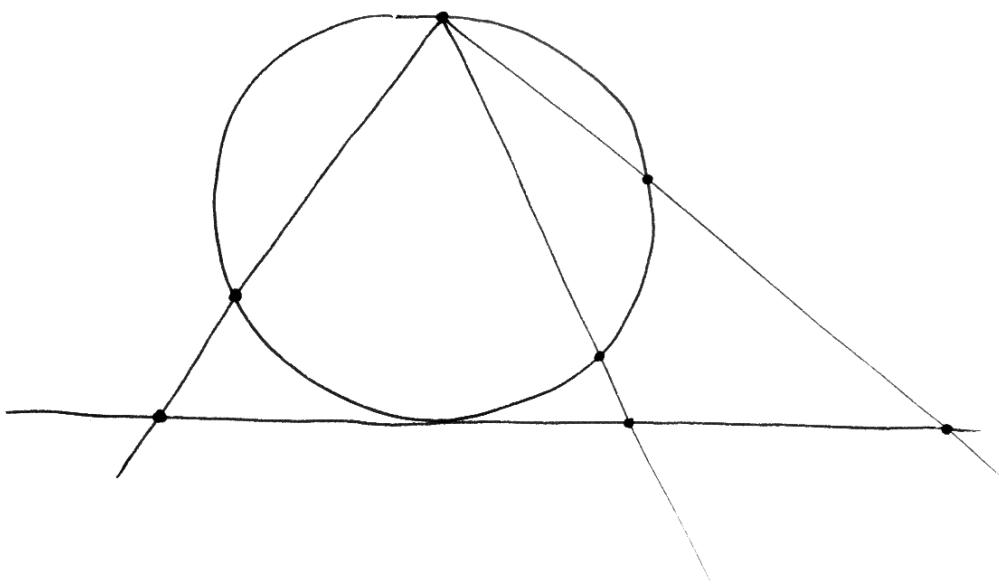
## Übungen

*Ergänzende Übung 3.5.4.4.* Man zeige, daß jeder algebraisch abgeschlossene Körper unendlich ist. Hinweis: Im Fall  $1 \neq -1$  reicht es, Quadratwurzeln zu suchen. Man zeige, daß jedes nichtkonstante Polynom  $P \in K[X, Y]$  in zwei Veränderlichen über einem algebraisch abgeschlossenen Körper unendlich viele Nullstellen in  $K^2$  hat.

*Ergänzende Übung 3.5.4.5 (Nullstellensatz für Hyperebenen).* Sei  $K$  ein unendlicher Körper. Verschwindet ein Polynom im Polynomring in  $d$  Variablen über  $K$  auf einer affinen Hyperebene in  $K^d$ , so wird es von jeder linearen Gleichung besagter Hyperebene geteilt. Hinweis: Ohne Beschränkung der Allgemeinheit mag man unsere Hyperebene als eine der Koordinatenhyperebenen annehmen. Man zeige auch allgemeiner: Verschwindet ein Polynom in  $d$  Veränderlichen über einem unendlichen Körper auf der Vereinigung der paarweise verschiedenen affinen Hyperebenen  $H_1, \dots, H_n \subset K^d$ , so wird es vom Produkt der linearen Gleichungen unserer Hyperebenen geteilt.

*Ergänzende Übung 3.5.4.6 (Pythagoreische Zahlen).* Man zeige: Stellen wir eine Lampe oben auf den Einheitskreis und bilden jeden von  $(0, 1)$  verschiedenen Punkt des Einheitskreises ab auf denjenigen Punkt der Parallelen zur  $x$ -Achse durch  $(0, -1)$ , auf den sein Schatten fällt, so entsprechen die Punkte mit rationalen Koordinaten auf dem Einheitskreis genau den Punkten mit rationalen Koordinaten auf unserer Parallelen. Hinweis: Hat ein Polynom in  $\mathbb{Q}[X]$  vom Grad drei zwei rationale Nullstellen, so ist auch seine dritte Nullstelle rational. Geben wir das Bild vom Schattenwurf auf und nehmen den Schnitt des Lichtstrahls mit der  $x$ -Achse, so steht eine explizite Formel für die Umkehrabbildung in ??.

*Ergänzung 3.5.4.7.* Unter einem **pythagoreischen Zahlentripel** versteht man ein Tripel  $(a, b, c)$  von positiven natürlichen Zahlen mit  $a^2 + b^2 = c^2$ , die also als



Wir stellen eine Lampe oben auf den Einheitskreis und bilden jeden von  $(0, 1)$  verschiedenen Punkt des Einheitskreises ab auf denjenigen Punkt der Parallelen zur  $x$ -Achse durch  $(0, -1)$ , auf den sein Schatten fällt. So entsprechen nach Übung 3.5.4.6 die Punkte mit rationalen Koordinaten auf dem Einheitskreis genau den Punkten mit rationalen Koordinaten auf unserer Parallelen. Ein Tripel  $a, b, c \in \mathbb{Z}$  mit  $a^2 + b^2 = c^2$  heißt ein **pythagoreisches Zahlentripel**. Die pythagoreischen Zahlentripel mit größtem gemeinsamen Teiler  $\langle a, b, c \rangle = \langle 1 \rangle$  und  $c > 0$  entsprechen nun offensichtlich eineindeutig den Punkten mit rationalen Koordinaten auf dem Einheitskreis vermittels der Vorschrift  $(a, b, c) \mapsto (a/c, b/c)$ . In dieser Weise liefert unser Bild also einen geometrischen Zugang zur Klassifikation der pythagoreischen Zahlentripel.

Seitenlängen eines rechtwinkligen Dreiecks auftreten können. Es scheint mir offensichtlich, daß die Bestimmung aller pythagoreischen Zahlentripel im wesentlichen äquivalent ist zur Bestimmung aller Punkte mit rationalen Koordinaten auf dem Einheitskreis, also aller Punkte  $(x, y) \in \mathbb{Q}^2$  mit  $x^2 + y^2 = 1$ .

*Übung 3.5.4.8.* Man zeige, daß die Menge der Polynome in  $\mathbb{Q}[X]$ , die an allen Punkten aus  $\mathbb{N}$  ganzzahlige Werte annehmen, übereinstimmt mit der Menge aller Linearkombinationen mit ganzzahligen Koeffizienten der mithilfe der Binomialkoeffizienten gebildeten Polynome

$$\binom{X}{k} := \frac{X(X-1)\dots(X-k+1)}{k(k-1)\dots 1} \quad \text{falls } k \geq 1 \text{ und } \binom{X}{0} := 1.$$

Hinweis: Man berechne die Werte unserer Polynome bei  $X = 0, 1, 2, \dots$ . Die Übung zeigt, daß diejenigen Polynome in  $\mathbb{Q}[X]$ , die an allen Punkten aus  $\mathbb{N}$  ganzzahlige Werte annehmen, sogar an allen Punkten aus  $\mathbb{Z}$  ganzzahlige Werte annehmen müssen. Sie heißen **ganzwertige** oder **numerische Polynome**. Man zeige weiter für jedes Polynom in  $\mathbb{Q}[X]$  vom Grad  $d \geq 0$ , das an fast allen Punkten aus  $\mathbb{N}$  ganzzahlige Werte annimmt, daß es ein ganzwertiges Polynom sein muß und daß das  $(d!)$ -fache seines Leitkoeffizienten mithin eine ganze Zahl sein muß.

*Ergänzende Übung 3.5.4.9.* Man zeige, daß die Menge aller Polynome mit rationalen Koeffizienten in  $\mathbb{Q}[X_1, \dots, X_r]$ , die an allen Punkten aus  $\mathbb{N}^r$  ganzzahlige Werte annehmen, übereinstimmt mit der Menge aller Linearkombinationen mit ganzzahligen Koeffizienten von Produkten der Gestalt

$$\binom{X_1}{k_1} \dots \binom{X_r}{k_r}$$

mit  $k_1, \dots, k_r \geq 0$ . Hinweis: Man argumentiere wie in 3.5.4.8.

### 3.5.5 Quotientenkörper und Partialbruchzerlegung

3.5.5.1. Die Konstruktion des Körpers  $\mathbb{Q}$  der Bruchzahlen aus dem Integritätsbereich  $\mathbb{Z}$  der ganzen Zahlen hatten wir bisher noch nicht formal besprochen. Hier holen wir das gleich in größerer Allgemeinheit nach und zeigen, wie man zu jedem Integritätsbereich seinen „Quotientenkörper“ konstruieren kann.

**Definition 3.5.5.2.** Gegeben ein kommutativer Integritätsbereich  $R$  konstruieren wir seinen **Quotientenkörper**

$$\text{Quot}(R)$$

wie folgt: Wir betrachten die Menge  $R \times (R \setminus 0)$  und definieren darauf eine Relation  $\sim$  durch die Vorschrift

$$(a, s) \sim (b, t) \text{ genau dann, wenn gilt } at = bs.$$

Diese Relation ist eine Äquivalenzrelation, wie man leicht prüft. Wir bezeichnen die Menge der Äquivalenzklassen mit  $\text{Quot}(R)$  und die Äquivalenzklasse von  $(a, s)$  mit  $\frac{a}{s}$  oder  $a/s$ . Dann definieren wir auf  $\text{Quot}(R)$  Verknüpfungen  $+$  und  $\cdot$  durch die Regeln

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{und} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

und überlassen dem Leser den Nachweis, daß diese Verknüpfungen wohldefiniert sind und  $\text{Quot}(R)$  zu einem Körper machen und daß die Abbildung  $\text{can} : R \rightarrow \text{Quot}(R)$ ,  $r \mapsto r/1$  ein injektiver Ringhomomorphismus ist. Er heißt die **kanonische Einbettung** unseres Integritätsbereichs in seinen Quotientenkörper.

*Ergänzung 3.5.5.3.* Auf Englisch bezeichnet man den Quotientenkörper als **fraction field** und auf Französisch als **corps de fractions**. Dort verwendet man folgerichtig statt unserer Notation  $\text{Quot}(R)$  die Notation  $\text{Frac}(R)$ . Die noch allgemeinere Konstruktion der „Lokalisierung“ lernen wir erst in ?? kennen.

*Beispiel 3.5.5.4.* Der Körper der rationalen Zahlen  $\mathbb{Q}$  wird formal definiert als der Quotientenkörper des Rings der ganzen Zahlen, in Formeln

$$\mathbb{Q} := \text{Quot } \mathbb{Z}$$

Sicher wäre es unter formalen Aspekten betrachtet eigentlich richtig gewesen, diese Definition schon viel früher zu geben. Es schien mir jedoch didaktisch ungeschickt, gleich am Anfang derart viel Zeit und Formeln auf die exakte Konstruktion einer Struktur zu verwenden, die Ihnen bereits zu Beginn ihres Studiums hinreichend vertraut sein sollte. Wie bereits bei rationalen Zahlen nennt man auch im allgemeinen bei einem Bruch  $g/h$  das  $g$  den **Zähler** und das  $h$  den **Nenner** des Bruchs.

**Satz 3.5.5.5 (Universelle Eigenschaft des Quotientenkörpers).** *Sei  $R$  ein kommutativer Integritätsbereich. Ist  $\varphi : R \rightarrow A$  ein Ringhomomorphismus, unter dem jedes von Null verschiedene Element von  $R$  auf eine Einheit von  $A$  abgebildet wird, so faktorisiert  $\varphi$  eindeutig über  $\text{Quot } R$ , es gibt also in Formeln genau einen Ringhomomorphismus  $\tilde{\varphi} : \text{Quot } R \rightarrow A$  mit  $\varphi(r) = \tilde{\varphi}(r/1) \forall r \in R$ .*

*Beweis.* Für jedes mögliche  $\tilde{\varphi}$  muß gelten  $\tilde{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$ . Das zeigt bereits die Eindeutigkeit von  $\tilde{\varphi}$ . Um auch seine Existenz zu zeigen, betrachten wir die Abbildung  $\hat{\varphi} : R \times (R \setminus 0) \rightarrow A$  gegeben durch  $\hat{\varphi}(r, s) = \varphi(r)\varphi(s)^{-1}$  und prüfen, daß sie konstant ist auf Äquivalenzklassen. Dann muß sie nach 3.4.2.6 eine wohlbestimmte Abbildung  $\text{Quot } R \rightarrow A$  induzieren, von der der Leser leicht selbst prüfen wird, daß sie ein Ringhomomorphismus ist.  $\square$

**3.5.5.6 (Brüche mit kontrollierten Nennern).** Gegeben ein kommutativer Integritätsbereich  $R$  und eine Teilmenge  $S \subset R \setminus 0$  betrachten wir im Quotientenkörper von  $R$  den Teilring

$$S^{-1}R := \{(r/s) \in \text{Quot } R \mid s \text{ ist ein Produkt von Elementen von } S\}$$

Hierbei ist die Eins auch als Produkt von Elementen von  $S$  zu verstehen, eben als das leere Produkt. Insbesondere erhalten wir eine Einbettung  $R \hookrightarrow S^{-1}R$  durch  $r \mapsto (r/1)$ . Ist nun  $\varphi : R \rightarrow A$  ein Ringhomomorphismus, unter dem jedes Element von  $S$  auf eine Einheit von  $A$  abgebildet wird, so faktorisiert  $\varphi$  mit demselben Beweis wie zuvor eindeutig über  $S^{-1}R$ , es gibt also in Formeln genau einen Ringhomomorphismus  $\tilde{\varphi} : S^{-1}R \rightarrow A$  mit  $\varphi(r) = \tilde{\varphi}(r/1) \forall r \in R$ .

**Beispiel 3.5.5.7 (Auswerten rationaler Funktionen).** Ist  $K$  ein Körper, so bezeichnet man den Quotientenkörper des Polynomrings mit  $K(X) := \text{Quot } K[X]$  und nennt ihn den **Funktionenkörper zu  $K$**  und seine Elemente **rationale Funktionen**. Man lasse sich durch die Terminologie nicht verwirren, Elemente dieses Körpers sind per definitionem formale Ausdrücke und eben gerade keine Funktionen. Inwiefern man sie zumindest für unendliches  $K$  doch als Funktionen versteht darf, soll nun ausgeführt werden. Gegeben  $\lambda \in K$  betrachten wir dazu die Menge  $S_\lambda := \{P \mid P(\lambda) \neq 0\}$  aller Polynome, die bei  $\lambda$  keine Nullstelle haben, und bezeichnen mit

$$K[X]_\lambda := S_\lambda^{-1}K[X] \subset K(X)$$

der Teilring aller Quotienten von Polynomen, die sich darstellen lassen als ein Bruch, dessen Nenner bei  $\lambda$  keine Nullstelle hat. Auf diesem Teilring ist das Auswerten bei  $\lambda$  nach 3.5.5.6 ein wohlbestimmter Ringhomomorphismus  $K[X]_\lambda \rightarrow K$ , den wir notieren als  $f \mapsto f(\lambda)$ . Er ist der einzige derartige Ringhomomorphismus mit  $X \mapsto \lambda$ . Gegeben  $f \in K(X)$  heißen die Punkte  $\lambda \in K$  mit  $f \notin K[X]_\lambda$  die **Polstellen von  $f$**  und das kleinste  $n$  mit  $(X - \lambda)^n f \in K[X]_\lambda$  heißt die **Polstellenordnung von  $f$  bei  $\lambda$** . Natürlich hat jedes Element  $f \in K(X)$  höchstens endlich viele Polstellen. Für jede rationale Funktion  $f \in K(X)$  erklärt man ihren **Definitionsbereich**  $D(f) \subset K$  als die Menge aller Punkte  $a \in K$ , die keine Polstellen von  $f$  sind. Durch „Kürzen von Nullstellen“ überzeugt man sich leicht, daß jede rationale Funktion so als Quotient  $f = g/h$  geschrieben werden kann, daß Zähler und Nenner keine gemeinsamen Nullstellen in  $K$  haben, und daß dann die Polstellen gerade die Nullstellen des Nenners sind. Vereinbart man, daß  $f$  diesen Stellen als Wert ein neues Symbol  $\infty$  zuweisen soll, so erhält man für jeden unendlichen Körper  $K$  sogar eine wohlbestimmte Injektion  $K(X) \hookrightarrow \text{Ens}(K, K \sqcup \{\infty\})$ .

**3.5.5.8.** In der Schule mögen Sie gelernt haben, daß etwa die Funktion  $x/x$  bei  $x = 0$  nicht definiert ist. Von unserem Standpunkt aus ist das nicht so klar. Es

gibt einerseits den Begriff einer Funktion als einer Abbildung, und um eine Abbildung anzugeben müssen bei uns im Prinzip Definitionsbereich, Wertebereich und Abbildungsvorschrift gleich mit angegeben werden, und die Abbildungsvorschrift  $x \mapsto x/x$  kann in der Tat bei  $x = 0$  nicht sinnvoll in der Art „setze erst  $x = 0$  für die Variable ein und führe dann die vorgeschriebenen Operationen im Körper  $\mathbb{R}$  aus“ ausgewertet werden. Im Sinne unserer obigen Definition gilt im Funktionenkörper  $\mathbb{R}(X)$  dahingegen  $1 = X/X$  und die Null gehört durchaus zum Definitionsbereich dieser rationalen Funktion im in 3.5.5.7 erklärten Sinne.

*Ergänzung 3.5.5.9.* Es ist sogar richtig, daß jede rationale Funktion eine eindeutige maximal gekürzte Darstellung mit normiertem Nenner hat. Um das einzusehen, benötigt man ein Analogon der eindeutigen Primfaktorzerlegung für Polynomringe, das wir für allgemeines  $K$  erst in ?? zeigen.

3.5.5.10. Wir erinnern aus 3.5.3.42 und 3.5.3.43 die Ringe der Potenzreihen und der Laurentreihen. Gegeben ein Körper  $K$  liefert die Verknüpfung von Einbettungen  $K[X] \hookrightarrow K[[X]] \hookrightarrow K((X))$  offensichtlich einen Ringhomomorphismus und nach der universellen Eigenschaft 3.5.5.5 mithin eine Einbettung  $K(X) \hookrightarrow K((X))$ . Das Bild von  $(1 - X)^{-1}$  unter dieser Einbettung wäre etwa die „formale geometrische Reihe“  $1 + X + X^2 + X^3 + \dots$

*Ergänzung 3.5.5.11.* Sei  $K$  ein Körper. Ist  $p \in K$  fest gewählt und  $K(T) \xrightarrow{\sim} K(X)$  der durch  $T \mapsto (X + p)$  gegebene Isomorphismus, so bezeichnet man das Bild von  $f \in K(T)$  unter der Komposition  $K(T) \xrightarrow{\sim} K(X) \hookrightarrow K((X))$  auch als die **Laurententwicklung von  $f$  um den Entwicklungspunkt  $p$** . Meist schreibt man in einer Laurententwicklung statt  $X$  auch  $(T - p)$ . So wäre die Laurententwicklung von  $f = T^2/(T - 1)$  um den Entwicklungspunkt  $T = 1$  etwa die endliche Laurentreihe  $(T - 1)^{-1} + 2 + (T - 1)$ .

**Satz 3.5.5.12 (Partialbruchzerlegung).** *Gegeben ein algebraisch abgeschlossener Körper  $K$  wird eine  $K$ -Basis des Funktionenkörpers  $K(X)$  gebildet von erstens den Potenzen der Variablen  $(X^n)_{n \geq 1}$  mitsamt zweitens den Potenzen der Inversen der Linearfaktoren  $((X - a)^{-n})_{n \geq 1, a \in K}$  zuzüglich drittens der Eins  $1 \in K(X)$ .*

3.5.5.13. Eine Darstellung einer rationalen Funktion als Linearkombination der Elemente dieser Basis nennt man eine **Partialbruchzerlegung** unserer rationalen Funktion. Anschaulich scheint mir zumindest die lineare Unabhängigkeit der behaupteten Basis recht einsichtig: Polstellen an verschiedenen Punkten können sich ebensowenig gegenseitig aufheben wie Polstellen verschiedener Ordnung an einem vorgegebenen Punkt. Alle rationalen Funktionen mag man auffassen als Funktionen auf der projektiven Gerade  $\mathbb{P}^1 K$  aus ?? und die  $(X^n)_{n \geq 1}$  als Funktionen, die „eine Polstelle der Ordnung  $n$  im Unendlichen haben“. Das ist auch der

Grund dafür, daß ich die 1 im Satz oben extra aufgeführt habe und nicht stattdessen einfach kürzer  $(X^n)_{n \geq 0}$  schreibe.

**3.5.5.14.** Ist  $K$  ein algebraisch abgeschlossener Körper, so sind die Polstellen eines Elements  $f \in K(X)$  im Sinne von 3.5.5.7 genau die Elemente  $a \in K$  mit der Eigenschaft, daß für ein  $n \geq 1$  der Term  $(X - a)^{-n}$  mit von Null verschiedenem Koeffizienten in der Partialbruchzerlegung von  $f$  auftritt.

*Ergänzung 3.5.5.15.* In Büchern zur Analysis findet man oft eine Variante dieses Satzes für den Körper  $K = \mathbb{R}$ : In diesem Fall werden die im Satz beschriebenen Elemente ergänzt zu einer Basis durch die Elemente  $1/((X - \lambda)(X - \bar{\lambda}))^n$  und die Elemente  $X/((X - \lambda)(X - \bar{\lambda}))^n$  für  $\lambda \in \mathbb{C}$  mit positivem Imaginärteil und  $n \geq 1$  beliebig, wie der Leser zur Übung selbst zeigen mag. Eine Verallgemeinerung auf den Fall eines beliebigen Körpers  $K$  wird in ?? diskutiert.

*Beweis.* Wir zeigen zunächst, daß unsere Familie den Funktionenkörper als  $K$ -Vektorraum erzeugt. Sei also  $f \in K(X)$  dargestellt als Quotient von zwei Polynomen  $f = P/Q$  mit  $Q \neq 0$ . Wir argumentieren mit Induktion über den Grad von  $Q$ . Ist  $Q$  konstant, so haben wir schon gewonnen. Sonst besitzt  $Q$  eine Nullstelle  $\mu \in K$  und wir können schreiben  $Q(x) = (X - \mu)^m \tilde{Q}(x)$  mit  $m \geq 1$  und  $\tilde{Q}(\mu) \neq 0$ . Dann nehmen wir  $c = P(\mu)/\tilde{Q}(\mu)$  und betrachten die Funktion

$$\frac{P}{Q} - \frac{c}{(X - \mu)^m} = \frac{P - c\tilde{Q}}{(X - \mu)^m \tilde{Q}}$$

Aufgrund unserer Wahl von  $c$  hat der Zähler auf der rechten Seite eine Nullstelle bei  $X = \mu$ , wir können im Bruch also  $(X - \mu)$  kürzen, und eine offensichtliche Induktion über dem Grad des Polynoms  $Q$  beendet den Beweis. Zum Beweis der linearen Unabhängigkeit betrachten wir eine Linearkombination unserer Basis inspe, die die Nullfunktion darstellt. Sei  $c(X - a)^{-n}$  ein Summand darin mit  $n \geq 1$  größtmöglich für die gewählte Polstelle  $a$ . So multiplizieren wir mit  $(X - a)^n$  und werten aus bei  $a$  im Sinne von 3.5.5.6 und finden, daß schon  $c = 0$  gegolten haben muß. So argumentieren wir alle Polstellen weg, und daß die nichtnegativen Potenzen von  $X$  linear unabhängig sind folgt ja schon aus der Definition des Polynomrings.  $\square$

**3.5.5.16 (Berechnung einer Partialbruchzerlegung).** Will man konkret eine Partialbruchzerlegung bestimmen, so rate ich dazu, mit einer Polynomdivision zu beginnen und  $P = AQ + R$  zu schreiben mit Polynomen  $A$  und  $R$  derart, daß der Grad von  $R$  echt kleiner ist als der Grad von  $Q$ . Wir erhalten  $P/Q = A + R/Q$ , und in der Partialbruchzerlegung von  $R/Q$  tritt dann kein polynomialer Summand mehr auf. Die Polstellen-Summanden gehören dann alle zu Nullstellen von  $Q$  und ihr Grad ist beschränkt durch die Vielfachheit der entsprechenden Nullstelle von

*Q.* Nun setzen wir die Koeffizienten unserer Linearkombination als Unbestimmte an, für die wir dann ein lineares Gleichungssystem erhalten, das wir mit den üblichen Verfahren lösen.

*Beispiel 3.5.5.17.* Wir bestimmen von  $(X^4 + 2X^2)/(X^2 + 2X + 1)$  die Partialbruchzerlegung. Die Polynomdivision haben wir bereits in 3.5.3.16 durchgeführt und  $X^4 + 2X^2 = (X^2 - 2X + 5)(X^2 + 2X + 1) - 8X - 5$  erhalten, so daß sich unser Bruch vereinfacht zu

$$\frac{X^4 + 2X^2}{X^2 + 2X + 1} = X^2 - 2X + 5 - \frac{8X + 5}{X^2 + 2X + 1}$$

Jetzt zerlegen wir den Nenner in Linearfaktoren  $X^2 + 2X + 1 = (X + 1)^2$  und dürfen nach unserem Satz über die Partialbruchzerlegung

$$\frac{8X + 5}{(X + 1)^2} = \frac{a}{X + 1} + \frac{b}{(X + 1)^2}$$

ansetzen, woraus sich ergibt  $8X + 5 = aX + a + b$  und damit  $a = 8$  und  $b = -3$ . Die Partialbruchzerlegung unserer ursprünglichen Funktion hat also die Gestalt

$$\frac{X^4 + 2X^2}{X^2 + 2X + 1} = X^2 - 2X + 5 - \frac{8}{X + 1} + \frac{3}{(X + 1)^2}$$

**3.5.5.18 (Geschlossene Darstellung der Fibonacci-Zahlen).** Wir bilden die sogenannte **erzeugende Funktion** der Fibonacci-Folge alias die formale Potenzreihe  $f(x) = \sum_{n \geq 0} f_n x^n$  mit den Fibonacci-Zahlen aus 1.1.2.2 als Koeffizienten. Die Rekursionsformel für Fibonacci-Zahlen  $f_{n+2} = f_{n+1} + f_n$  liefert unmittelbar  $xf(x) + x^2 f(x) = f(x) - x$ . Wir folgern  $(1 - x - x^2)f(x) = x$ . Umgekehrt hat jede formale Potenzreihe, die diese Identität erfüllt, die Fibonacci-Zahlen als Koeffizienten. Es gilt also, die Funktion  $x/(1 - x - x^2)$  in eine Potenzreihe zu entwickeln. Dazu erinnern wir Satz 3.5.5.12 über die Partialbruchzerlegung, schreiben  $x^2 + x - 1 = (x + \alpha)(x + \beta)$  mit  $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}$  und  $\beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}$  und dürfen  $x/(1 - x - x^2) = a/(x + \alpha) + b/(x + \beta)$  ansetzen. Zur Vereinfachung der weiteren Rechnungen erinnern wir  $\alpha\beta = -1$  und variieren unseren Ansatz zu  $x/(1 - x - x^2) = c/(1 - x\alpha) + d/(1 - x\beta)$ . Das führt zu  $c + d = 0$  alias  $c = -d$  und  $\alpha c + \beta d = -1$  alias  $c = 1/(\beta - \alpha) = 1/\sqrt{5}$ . Die Entwicklung unserer Brüche in eine geometrische Reihe nach 3.5.5.10 liefert damit im Ring der formalen Potenzreihen die Identität

$$\frac{x}{1 - x - x^2} = \sum_{i \geq 0} \frac{(x\alpha)^i}{\sqrt{5}} - \frac{(x\beta)^i}{\sqrt{5}}$$

und für den Koeffizienten von  $x^i$  alias die  $i$ -te Fibonacci-Zahl  $f_i$  ergibt sich wie in 1.1.2.2 die Darstellung

$$f_i = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^i - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^i$$

## Übungen

*Übung 3.5.5.19.* Man zeige: Besitzt ein kommutativer Integritätsbereich  $R$  eine Anordnung  $\leq$ , unter der er im Sinne von ?? ein angeordneter Ring wird, so besitzt sein Quotientenkörper  $\text{Quot } R$  genau eine Struktur als angeordneter Körper, für die die kanonische Einbettung  $R \hookrightarrow \text{Quot } R$  mit der Anordnung verträglich alias monoton wachsend ist. Speziell erhalten wir so die übliche Anordnung auf  $\mathbb{Q} = \text{Quot } \mathbb{Z}$ .

*Ergänzende Übung 3.5.5.20.* Gegeben ein unendlicher Körper  $K$  und eine von Null verschiedene rationale Funktion  $f \in K(X)^\times$  sind die Polstellen von  $f$  genau die Nullstellen von  $(1/f)$ , als da heißt, die Stellen aus dem Definitionsbereich von  $(1/f)$ , an denen diese Funktion den Wert Null annimmt. Fassen wir genauer  $f$  als Abbildung  $f : K \rightarrow K \sqcup \{\infty\}$  auf, so entspricht  $(1/f)$  der Abbildung  $a \mapsto f(a)^{-1}$ , wenn wir  $0^{-1} = \infty$  und  $\infty^{-1} = 0$  vereinbaren.

*Übung 3.5.5.21.* Ist  $K$  ein algebraisch abgeschlossener Körper, so nimmt eine von Null verschiedene rationale Funktion  $f \in K(X)^\times$  auf ihrem Definitionsbereich fast jeden Wert an gleichviel Stellen an, genauer an  $n = \max(\text{grad } g, \text{grad } h)$  Stellen für  $f = g/h$  eine unkürzbare Darstellung als Quotient zweier Polynome. In anderen Worten haben unter  $f : D(f) \rightarrow K$  fast alle Punkte  $a \in K$  genau  $n$  Urbilder.

*Übung 3.5.5.22.* Sei  $P \in \mathbb{Q}(X)$  gegeben. Man zeige: Gibt es eine Folge ganzer Zahlen aus dem Definitionsbereich unserer rationalen Funktion  $a_n \in \mathbb{Z} \cap D(P)$  mit  $a_n \rightarrow \infty$  und  $P(a_n) \in \mathbb{Z}$  für alle  $n$ , so ist  $P$  bereits ein Polynom  $P \in \mathbb{Q}[X]$ .

*Übung 3.5.5.23.* Sei  $K$  ein Körper und seien  $f, g \in K(X)$  gegeben. Man zeige: Gibt es unendlich viele Punkte aus dem gemeinsamen Definitionsbereich  $D(f) \cap D(g)$ , an denen  $f$  und  $g$  denselben Wert annehmen, so gilt bereits  $f = g$  in  $K(X)$ .

*Ergänzende Übung 3.5.5.24.* Man zeige, daß im Körper  $\mathbb{Q}((X))$  jede formale Potenzreihe mit konstantem Koeffizienten Eins eine Quadratwurzel besitzt. Die Quadratwurzel von  $(1 + X)$  kann sogar durch die binomische Reihe ?? explizit angegeben werden, aber das sieht man leichter mit den Methoden der Analysis.

*Übung 3.5.5.25.* Man bestimme die Partialbruchzerlegung von  $1/(1 + X^4)$  in  $\mathbb{C}(X)$ .

*Übung 3.5.5.26.* Man zeige, daß bei einem Bruch  $P(T)/(T^n(T-1)^m)$  mit Zähler  $P(T) \in \mathbb{Z}[T]$  auch alle Koeffizienten bei der Partialbruchzerlegung ganze Zahlen sind.

*Übung 3.5.5.27.* Man bearbeite noch einmal die Übungen 1.1.2.10 und 1.1.2.11.

*Übung 3.5.5.28 (Verknüpfung rationaler Funktionen).* Ist  $K$  ein Körper und  $P \in K[X]$  ein von Null verschiedenes Polynom, so liegt jede Nullstelle von  $P$  im größeren Körper  $K(Y) \supset K$  bereits im Teilkörper  $K$ . Gegeben  $f \in K(X)$  gehört mithin jedes  $g \in K(Y) \setminus K$  zum Definitionsbereich von  $f$  und wir können mithin setzen

$$f \circ g := f(g) \in K(Y)$$

Man zeige, daß die  $K$ -linearen Körperhomomorphismen  $\varphi : K(X) \rightarrow K(Y)$  alle die Gestalt  $\varphi : f \mapsto f \circ g$  haben für  $g = \varphi(X) \in K(Y) \setminus K$ . Sind  $f$  und  $g$  beide nicht konstant, so ist auch  $f \circ g$  nicht konstant. Gegeben  $f, g, h \in K(X) \setminus K$  zeige man die Assoziativität  $(f \circ g) \circ h = f \circ (g \circ h)$ . Unsere Abbildung  $K(X) \rightarrow \text{Ens}(K, K \sqcup \{\infty\})$  kann zu einer Abbildung  $K(X) \rightarrow \text{Ens}(K \sqcup \{\infty\})$  fortgesetzt werden, indem wir für  $f = P/Q$  den Wert  $f(\infty)$  erklären als den Quotienten  $a_n/b_n$  der Leitkoeffizienten, falls  $P$  und  $Q$  denselben Grad  $n$  haben, und  $\infty$  falls der Grad von  $P$  größer ist als der von  $Q$ , und  $0$  falls er kleiner ist. So erhalten wir einen Monoidhomomorphismus  $(K(X), \circ) \rightarrow (\text{Ens}(K \sqcup \{\infty\}), \circ)$ , der im Fall eines unendlichen Körpers  $K$  injektiv ist.

*Übung 3.5.5.29 (Quotientenkörper von Ringen formaler Potenzreihen).* Gegeben ein kommutativer Integritätsbereich  $R$  zeige man, daß die universelle Eigenschaft des Quotientenkörpers einen Körperisomorphismus

$$\text{Quot}(R[[X]]) \xrightarrow{\sim} (\text{Quot } R)((X))$$

induziert. Induktiv erhalten wir so etwa für jeden Körper  $K$  einen Körperisomorphismus

$$(K((X)))((Y)) \xrightarrow{\sim} (K((Y)))((X))$$

Zum Beispiel ist  $(X - Y)^{-1} = X^{-1}(1 - Y/X)^{-1} = \sum_{n \geq 0} X^{-n-1}Y^n$  die Darstellung eines Elements auf der linken Seite, das auf der rechten Seite auf den Ausdruck  $\sum_{n \geq 0} -Y^{-n-1}X^n$  abgebildet wird.

### 3.5.6 Quaternionen\*

3.5.6.1. Dieser Abschnitt ist für den Rest der Vorlesung unerheblich. Allerdings gehören die Quaternionen zur mathematischen Allgemeinbildung.

**Definition 3.5.6.2.** Ein **Schiefkörper** ist ein Ring  $R$ , der nicht der Nullring ist und in dem alle von Null verschiedenen Elemente Einheiten sind. Auf englisch

sagt man **skew field**, auf französisch **corps gauche**. Gleichbedeutend spricht man auch von einem **Divisionsring**.

**Satz 3.5.6.3 (Quaternionen).** *Es gibt Fünftupel  $(\mathbb{H}, i, j, k, \kappa)$  bestehend aus einem Ring  $\mathbb{H}$ , Elementen  $i, j, k \in \mathbb{H}$  und einem Ringhomomorphismus  $\kappa : \mathbb{R} \rightarrow \mathbb{H}$  derart, daß gilt*

$$i^2 = j^2 = k^2 = ijk = -1$$

*und  $\kappa(a)q = q\kappa(a) \forall a \in \mathbb{R}, q \in \mathbb{H}$  und daß  $1, i, j, k$  eine Basis von  $\mathbb{H}$  bilden für die durch die Vorschrift  $\mathbb{R} \times \mathbb{H} \rightarrow \mathbb{H}, (a, q) \mapsto \kappa(a)q$  auf  $\mathbb{H}$  gegebene Struktur als  $\mathbb{R}$ -Vektorraum. Des weiteren ist in einem derartigem Fünftupel der Ring  $\mathbb{H}$  ein Schiefkörper.*

3.5.6.4. Ein derartiges Fünftupel ist im wesentlichen eindeutig bestimmt in der offensichtlichen Weise. Um das zu sehen beachten wir, daß durch Multiplikation der letzten Gleichung von rechts mit  $k$  folgt  $ijk = k$  und durch Invertieren beider Seiten weiter  $ji = -k$ . Von da ausgehend erhalten wir unmittelbar die Formeln

$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik,$$

und so die Eindeutigkeit. Wegen dieser Eindeutigkeit erlauben wir uns den bestimmten Artikel und nennen  $\mathbb{H}$  den Schiefkörper der **Quaternionen**, da er nämlich als Vektorraum über den reellen Zahlen die Dimension Vier hat, oder auch den Schiefkörper der **Hamilton'schen Zahlen** nach seinem Erfinder Hamilton. Weiter kürzen wir für reelle Zahlen  $a \in \mathbb{R}$  meist  $\kappa(a) = a$  ab. Jedes Element  $q \in \mathbb{H}$  hat also die Gestalt

$$q = a + bi + cj + dk$$

mit wohlbestimmten  $a, b, c, d \in \mathbb{R}$ . Die Abbildung  $\mathbb{C} \hookrightarrow \mathbb{H}$  mit  $a + bi_{\mathbb{C}} \mapsto a + bi$  ist ein Ringhomomorphismus und wir machen auch für komplexe Zahlen meist in der Notation keinen Unterschied zwischen unserer Zahl und ihrem Bild in  $\mathbb{H}$  unter obiger Einbettung. In ?? diskutieren wir, warum und in welcher Weise  $\mathbb{R}, \mathbb{C}$  und  $\mathbb{H}$  bis auf Isomorphismus die einzigen Schiefkörper endlicher Dimension „über dem Körper  $\mathbb{R}$ “ sind.

3.5.6.5. Auch die Abbildungen  $\mathbb{C} \rightarrow \mathbb{H}$  mit  $a + bi_{\mathbb{C}} \mapsto a + bj$  oder mit  $a + bi_{\mathbb{C}} \mapsto a + bk$  sind Ringhomomorphismen, und wir werden bald sehen, daß es sogar unendlich viele  $\mathbb{R}$ -lineare Ringhomomorphismen, ja eine ganze 3-Sphäre von  $\mathbb{R}$ -linearen Ringhomomorphismen  $\mathbb{C} \rightarrow \mathbb{H}$  gibt.

3.5.6.6. Hamilton war von seiner Entdeckung so begeistert, daß er eine Gedenktafel an der Dubliner Broom Bridge anbringen ließ, auf der zu lesen ist: „Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication  $i^2 = j^2 = k^2 = ijk = -1$  & cut it on a stone of this bridge“.

*Beweis.* Bezeichne  $\mathbb{H}$  die Menge aller komplexen  $(2 \times 2)$ -Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -y \\ \bar{y} & \bar{z} \end{pmatrix} \mid z, y \in \mathbb{C} \right\} \subset \text{Mat}(2; \mathbb{C})$$

Die Addition und Multiplikation von Matrizen induziert offensichtlich eine Addition und Multiplikation auf  $\mathbb{H}$  und wir erhalten eine Einbettung  $\mathbb{C} \hookrightarrow \mathbb{H}$  vermittels  $z \mapsto \text{diag}(z, \bar{z})$ . Das Bilden der konjugierten transponierten Matrix definiert einen Antiautomorphismus  $q \mapsto \bar{q}$  von  $\mathbb{H}$ , in Formeln  $\bar{qw} = \bar{w}\bar{q}$ , und  $q\bar{q}$  ist für  $q \neq 0$  stets positiv und reell. Folglich ist  $\mathbb{H}$  ein Schiefkörper. Wir fassen  $\mathbb{C}$  meist als Teilmenge von  $\mathbb{H}$  auf vermittels der eben erklärten Einbettung, aber vorerst unterscheiden wir noch zwischen den komplexen Zahlen  $1_{\mathbb{C}}, i_{\mathbb{C}}$  und den Matrizen  $1 = \text{diag}(1_{\mathbb{C}}, 1_{\mathbb{C}}), i = \text{diag}(i_{\mathbb{C}}, -i_{\mathbb{C}})$ . Unser  $\mathbb{H}$  hat dann über  $\mathbb{R}$  die Basis  $1, i, j, k$  mit  $i := \text{diag}(i_{\mathbb{C}}, -i_{\mathbb{C}})$  und

$$j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } k := \begin{pmatrix} 0 & i_{\mathbb{C}} \\ i_{\mathbb{C}} & 0 \end{pmatrix}$$

und es gilt

$$i^2 = j^2 = k^2 = ijk = -1$$

□

3.5.6.7. Jede zyklische Vertauschung von  $i, j, k$  liefert einen Automorphismus der Quaternionen. Die Konjugation  $q \mapsto \bar{q}$  aus der im Beweis gegebenen Konstruktion hat in der Basis  $1, i, j, k$  die Gestalt

$$\overline{a + bi + cj + dk} = a - bi - cj - dk$$

und hat wie bereits erwähnt die Eigenschaft  $\bar{qw} = \bar{w}\bar{q}$ . Gegeben ein Quaternion  $q = a + bi + cj + dk$  nennt man  $a = (q + \bar{q})/2$  seinen **Realteil** und schreibt  $a = \text{Re}(q)$ . Für  $q = a + bi + cj + dk$  ist  $q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2$  und man setzt  $|q| = \sqrt{q\bar{q}}$  und nennt diese reelle Zahl den **Betrag** unseres Quaternions. Offensichtlich kann für  $q \neq 0$  sein Inverses durch die Formel  $q^{-1} = \bar{q}/|q|^2$  angegeben werden. Offensichtlich gilt dann  $|qw| = |q||w|$  für alle  $q, w \in \mathbb{H}$  und die Gruppe aller Quaternionen der Länge Eins besteht genau aus allen unitären  $(2 \times 2)$ -Matrizen mit Determinante Eins. Darin enthalten ist die Untergruppe der acht Quaternionen  $\{\pm 1, \pm i, \pm j, \pm k\}$ , die sogenannte **Quaternionengruppe**, von deren Multiplikationstabelle Hamilton bei seiner Konstruktion ausgegangen war.

Vorschau 3.5.6.8. Gegeben ein Kring  $R$  mitsamt einem selbstinversen Ringhomomorphismus  $R \rightarrow R$ ,  $r \mapsto \bar{r}$  und einem Element  $v \in R$  mit  $\bar{v} = v$  bildet allgemeiner die Menge aller  $(2 \times 2)$ -Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & vy \\ \bar{y} & \bar{z} \end{pmatrix} \mid z, y \in R \right\} \subset \text{Mat}(2; R)$$

einen Teilring des Matrizenrings. Derartige Ringe heißen **Quaternionenringe**.

3.5.6.9. Es gibt außer der Identität nur einen  $\mathbb{R}$ -linearen Körperhomomorphismus  $\mathbb{C} \rightarrow \mathbb{C}$ , nämlich die komplexe Konjugation. Im Fall der Quaternionen liefert da hingegen jede von Null verschiedene Quaternion  $q \in \mathbb{H}^\times$  einen  $\mathbb{R}$ -linearen Ringhomomorphismus  $\text{int } q : \mathbb{H} \rightarrow \mathbb{H}$ ,  $w \mapsto qwq^{-1}$ , und  $\text{int } q = \text{int } q'$  impliziert bereits  $\mathbb{R}q = \mathbb{R}q'$ .

### Übungen

*Übung 3.5.6.10.* Man zeige, daß es für jedes Quaternion  $q$  mit Realteil  $\text{Re } q = 0$  und Betrag  $|q| = 1$  einen  $\mathbb{R}$ -linearen Ringhomomorphismus  $\mathbb{C} \rightarrow \mathbb{H}$  gibt mit  $i_{\mathbb{C}} \mapsto q$ .

*Ergänzende Übung 3.5.6.11.* Man zeige: Sind zwei natürliche Zahlen jeweils eine Summe von vier Quadraten, so auch ihr Produkt. Diese Erkenntnis ist ein wichtiger Schritt bei einem Beweis des sogenannten **Vier-Quadrat-Satzes** von Lagrange, nach dem jede natürliche Zahl eine Summe von vier Quadratzahlen ist, etwa  $3 = 1^2 + 1^2 + 1^2 + 0^2$  oder  $23 = 3^2 + 3^2 + 2^2 + 1^2$ .

## 3.6 Determinanten und Eigenwerte

### 3.6.1 Das Signum einer Permutation

3.6.1.1. Wir beginnen hier mit dem Studium der sogenannten „symmetrischen Gruppen“. Mehr dazu können Sie später in ?? lernen.

**Definition 3.6.1.2.** Die Gruppe aller Permutationen alias bijektiven Selbstabbildungen der Menge  $\{1, 2, \dots, n\}$  notieren wir

$$\mathcal{S}_n := \text{Ens}^\times \{1, 2, \dots, n\}$$

Sie heißt auch die  **$n$ -te symmetrische Gruppe**. Nach 2.1.5.15 hat diese Gruppe  $|\mathcal{S}_n| = n!$  Elemente. Viele Autoren verwenden statt  $\mathcal{S}_n$  auch die alternative Notation  $\Sigma_n$ . Eine Permutation, die zwei Elemente unserer Menge vertauscht und alle anderen Elemente festhält, heißt eine **Transposition**.

**Definition 3.6.1.3.** Ein **Fehlstand** einer Permutation  $\sigma \in \mathcal{S}_n$  ist ein Paar  $(i, j)$  mit  $1 \leq i < j \leq n$  aber  $\sigma(i) > \sigma(j)$ . Die Zahl der Fehlstände heißt die **Länge**  $l(\sigma)$  unserer Permutation, in Formeln

$$l(\sigma) := |\{(i, j) \mid i < j \text{ aber } \sigma(i) > \sigma(j)\}|$$

Das **Signum** einer Permutation ist definiert als die Parität der Zahl ihrer Fehlstände, in Formeln

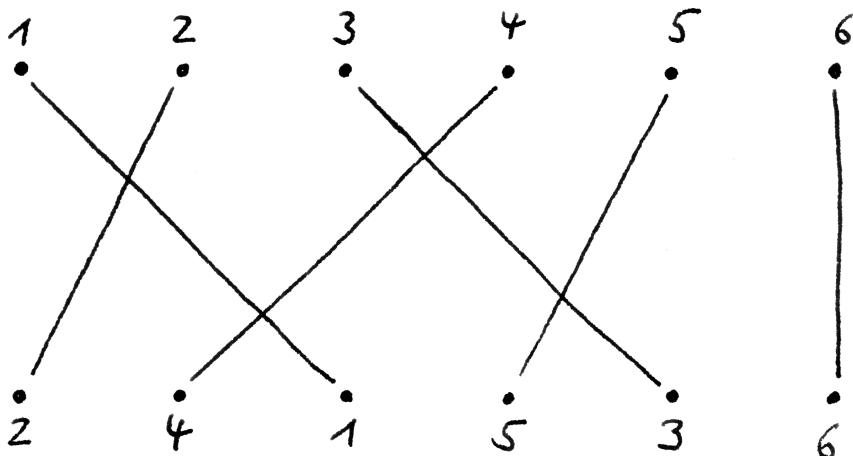
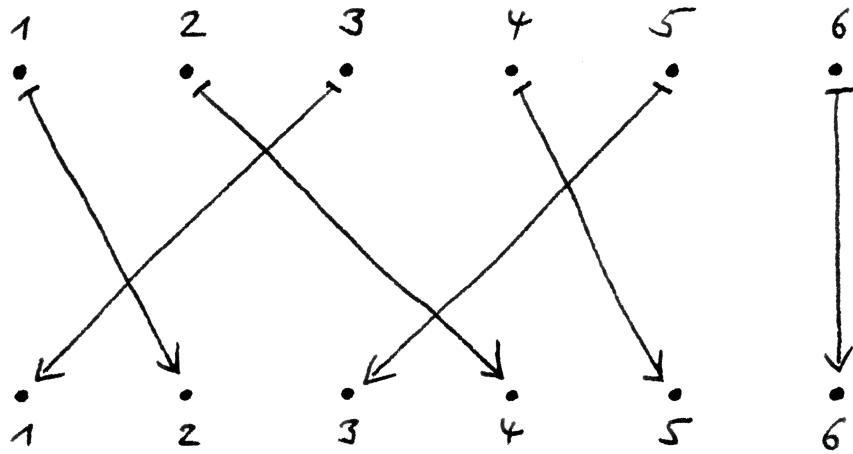
$$\text{sgn}(\sigma) = (-1)^{l(\sigma)}$$

Eine Permutation mit Signum +1 alias gerader Länge heißt eine **gerade Permutation**, eine Permutation mit Signum -1 alias ungerader Länge eine **ungerade Permutation**.

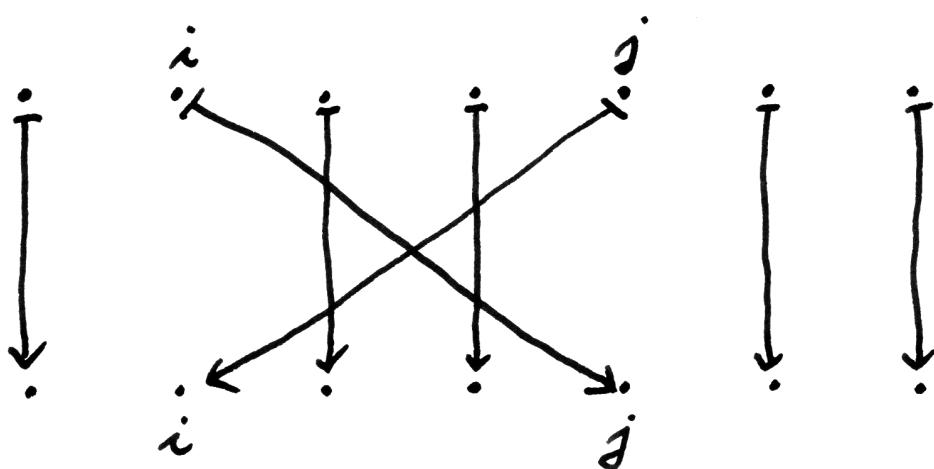
*Beispiel 3.6.1.4.* Die Identität von  $\mathcal{S}_n$  ist jeweils die einzige Permutation der Menge  $\{1, \dots, n\}$  der Länge Null. Die Transposition, die die Zahlen  $i$  und  $j$  vertauscht, hat die Länge  $2|i - j| - 1$ , wie auch nebenstehendes Bild zeigt, und ist insbesondere stets ungerade.

**Lemma 3.6.1.5 (Multiplikativität des Signums).** Für jede natürliche Zahl  $n$  ist unser Signum ein Gruppenhomomorphismus  $\text{sgn} : \mathcal{S}_n \rightarrow \{1, -1\}$  von der symmetrischen Gruppe  $\mathcal{S}_n$  in die zweielementige Gruppe der Vorzeichen, in Formeln gilt also

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \text{sgn}(\tau) \quad \forall \sigma, \tau \in \mathcal{S}_n$$



Diese Bilder illustrieren zwei mögliche Anschauungen für die Länge einer Permutation, in diesem Fall der Permutation  $\sigma \in S_6$  mit  $1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 5, 5 \mapsto 3$  und  $6 \mapsto 6$ : Im oberen Bild ist die Länge ganz offensichtlich die „Zahl der Kreuzungen von Abbildungspfeilen“, in unserem Fall haben wir also  $l(\sigma) = 4$ . Im unteren Bild habe ich unter jede Zahl  $n$  jeweils  $\sigma(n)$  geschrieben und dann gleiche Zahlen verbunden, und hier ist ähnlich  $l(\sigma) = 4$  gerade die „Zahl der Kreuzungen solcher Verbindungslien“. Der Leser sei ermutigt, sich auch die Produktformel für das Signum 3.6.1.5 mithilfe dieser Bilder anschaulich zu machen.



Die Transposition, die  $i$  und  $j$  vertauscht, hat genau  $2|i - j| - 1$  Fehlstände.  
Insbesondere ist jede Transposition ungerade.

*Gar kein Beweis.* Wir interpretieren Fehlstände als „Kreuzungspunkte“. Hängen wir zwei unserer Bilder aneinander, so ist anschaulich klar, daß sich die Zahl der Fehlstände der Komposition alias die „Zahl Kreuzungspunkte nach dem Glattziehen“ von der Summe der Zahlen der Fehlstände der Faktoren alias der „Zahl Kreuzungspunkte vor dem Glattziehen“ nur um eine gerade Zahl unterscheiden kann.  $\square$

*Erster Beweis.* Wir vereinbaren speziell für diesen Beweis für das Vorzeichen einer von Null verschiedenen ganzen Zahl  $a \in \mathbb{Z} \setminus 0$  die Notation  $[a] := a/|a| \in \{1, -1\}$ . Damit können wir das Signum einer Permutation  $\sigma$  dann auch schreiben als

$$\operatorname{sgn}(\sigma) = \prod_{i < j} [\sigma(j) - \sigma(i)]$$

Für eine beliebige weitere Permutation  $\tau$  finden wir dann

$$\prod_{i < j} [\sigma\tau(j) - \sigma\tau(i)] = \prod_{i < j} \frac{[\sigma(\tau(j)) - \sigma(\tau(i))]}{[\tau(j) - \tau(i)]} \prod_{i < j} [\tau(j) - \tau(i)]$$

Da nun aber für eine beliebige weitere Permutation  $\tau$  auch die  $\{\tau(j), \tau(i)\}$  für  $i < j$  genau die zweielementigen Teilmengen von  $\{1, \dots, n\}$  durchlaufen, gilt für eine beliebige weitere Permutation  $\tau$  auch die Formel

$$\operatorname{sgn}(\sigma) = \prod_{i < j} \frac{[\sigma(\tau(j)) - \sigma(\tau(i))]}{[\tau(j) - \tau(i)]}$$

Das zeigt die Behauptung.  $\square$

*Zweiter Beweis.* Wir betrachten den Polynomring  $\mathbb{Z}[X_1, \dots, X_n]$  aus 3.5.3.30. Für jede Permutation  $\sigma \in \mathcal{S}_n$  erklären wir für diesen Ring einen Ringhomomorphismus  $\sigma : \mathbb{Z}[X_1, \dots, X_n] \rightarrow \mathbb{Z}[X_1, \dots, X_n]$  zu sich selber vermittels der Vertauschung der Variablen, in Formeln  $\sigma : X_i \mapsto X_{\sigma(i)}$ . Dann gilt für jedes Polynom  $P$  sicher  $\tau(\sigma P) = (\tau\sigma)P$ . Betrachten wir nun speziell das Polynom

$$P = \prod_{i < j} (X_i - X_j)$$

Offensichtlich gilt  $\sigma P = \operatorname{sgn}(\sigma)P$ . Damit folgt aber unmittelbar die von der Mitte aus zu entwickelnde Gleichungskette

$$\operatorname{sgn}(\tau) \operatorname{sgn}(\sigma) P = \tau(\sigma P) = (\tau\sigma)P = \operatorname{sgn}(\tau\sigma)P$$

Daraus folgt dann die Behauptung.  $\square$

*Ergänzung 3.6.1.6.* Für jedes  $n$  bilden die geraden Permutationen als Kern eines Gruppenhomomorphismus nach 2.2.3.21 eine Untergruppe von  $\mathcal{S}_n$ . Diese Gruppe heißt die **alternierende Gruppe** und wird  $A_n$  notiert.

## Übungen

*Übung 3.6.1.7.* Die Permutation  $\sigma \in S_n$ , die  $i$  ganz nach vorne schiebt ohne die Reihenfolge der übrigen Elemente zu ändern, hat  $(i - 1)$  Fehlstände und folglich das Signum  $\text{sgn}(\sigma) = (-1)^{i-1}$ .

*Übung 3.6.1.8.* Jede Permutation einer endlichen angeordneten Menge lässt sich darstellen als eine Verknüpfung von Transpositionen benachbarter Elemente.

*Ergänzende Übung 3.6.1.9.* Ist  $T$  eine endliche Menge, so gibt es genau einen Gruppenhomomorphismus

$$\text{sign} : \text{Ens}^\times(T) \rightarrow \{1, -1\}$$

derart, von der Gruppe der Permutationen von  $T$  in die zweielementige Gruppe der Vorzeichen derart, daß jede Transposition auf  $(-1)$  abgebildet wird. Im Fall  $|T| \geq 2$  ist das sogar der einzige surjektive Gruppenhomomorphismus zwischen besagten Gruppen. Wir nennen unseren Gruppenhomomorphismus auch in dieser Allgemeinheit das **Signum** und kürzen ihn wieder mit  $\text{sign} = \text{sgn}$  ab. Auch in dieser Allgemeinheit nennen wir eine Permutation mit Signum  $+1$  **gerade**, und eine Permutation mit Signum  $-1$  **ungerade**. Es ist allerdings nicht mehr sinnvoll, in dieser Allgemeinheit von der „Länge“ einer Permutation zu reden.

*Übung 3.6.1.10.* Die symmetrische Gruppe  $S_n$  wird erzeugt von der Transposition  $\tau$  der Elemente 1 und 2 zusammen mit der „zyklischen Vertauschung“  $\sigma : i \mapsto i + 1$  für  $1 \leq i < n$  und  $n \mapsto 1$ . Die symmetrische Gruppe  $S_5$  wird sogar erzeugt von der „zyklischen Vertauschung“ und einer beliebigen weiteren Transposition  $\tau$ . Mutige zeigen stärker: Die symmetrische Gruppe  $S_p$  für eine beliebige Primzahl  $p$  wird erzeugt von der „zyklischen Vertauschung“ und einer beliebigen weiteren Transposition  $\tau$ .

*Übung 3.6.1.11.* Man gebe einen Gruppenisomorphismus  $S_3 \xrightarrow{\sim} \text{GL}(2; \mathbb{F}_2)$  an.

*Übung 3.6.1.12.* Eine Permutation einer Menge, die „von vier Elementen unserer Menge erst Zwei vertauscht und dann auch noch die anderen beiden vertauscht“, heißt eine **Doppeltranspositionen**. Man zeige, daß in der symmetrischen Gruppe  $S_4$  die drei Doppeltranspositionen zusammen mit dem neutralen Element eine Untergruppe bilden, die isomorph ist zur Klein'schen Vierergruppe  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

## 3.6.2 Determinante und ihre Bedeutung

**Definition 3.6.2.1.** Seien  $K$  ein Kring und  $n \in \mathbb{N}$ . Die **Determinante** ist die Abbildung  $\det : \text{Mat}(n; K) \rightarrow K$  von den quadratischen Matrizen mit Einträgen

in unserem Kring in besagten Kring selbst, die gegeben wird durch die Vorschrift

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \quad \mapsto \quad \det A := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

Summiert wird über alle Permutationen von  $n$  und der Vorfaktor  $\operatorname{sgn}(\sigma)$  meint das Signum der Permutation  $\sigma$  nach 3.6.1.3. Unsere Formel heißt die **Leibniz-Formel**. Für den Extremfall  $n = 0$  der „leeren Matrix“ ist zu verstehen, daß ihr die Determinante 1 zugeordnet wird: Formal gibt es genau eine Permutation der leeren Menge, deren Signum ist Eins, und dies Signum wird multipliziert mit dem leeren Produkt, das nach unseren Konventionen auch den Wert Eins hat.

**3.6.2.2 (Herkunft der Terminologie).** Wie wir in 3.6.4.2 sehen werden, bestimmt alias determiniert die Determinante, ob ein quadratisches lineares Gleichungssystem eindeutig lösbar ist. Daher röhrt die Terminologie.

*Beispiele 3.6.2.3.* Wir erhalten etwa

$$\begin{aligned} \det(a) &= a \\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= ad - cb \\ \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\quad - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12} \end{aligned}$$

Im Fall der  $(3 \times 3)$ -Matrizen heißt das manchmal die **Jägerzaunformel** aus einem Grund, den die nebenstehende Abbildung illustriert. Für  $n \geq 4$  macht die Berechnung der Determinante anhand der Leibniz-Formel als Summe von  $n! \geq 24$  Termen keinen Spaß mehr. Wir besprechen in 3.6.3.9, wie man in diesen Fällen geschickter vorgehen kann.

*Beispiel 3.6.2.4 (Determinanten von Dreiecksmatrizen).* Die Determinante einer oberen Dreiecksmatrix ist das Produkt ihrer Diagonaleinträge. In der Tat ist die Identität die einzige Permutation  $\sigma$  mit  $\sigma(i) \leq i$  für alle  $i$ , folglich trägt im Fall einer oberen Dreiecksmatrix in der Leibniz-Formel nur der Summand mit  $\sigma = \text{id}$  zur Determinante bei. Dasselbe gilt für untere Dreiecksmatrizen.

**Lemma 3.6.2.5.** *Die Determinante einer Matrix ändert sich nicht beim Transponieren, in Formeln*

$$\det A^\top = \det A$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Um die Determinante einer  $(3 \times 3)$ -Matrix zu berechnen mag man die erste und zweite Spalte danebenschreiben und dann die Produkte der drei Dreierdiagonalen nach rechts unten addieren und davon die Produkte der drei Dreierdiagonalen nach rechts oben abziehen. Diese Eselsbrücke heißt auch die „Jägerzaunformel“. Für  $(4 \times 4)$ -Matrizen liefert aber die analoge Regel nicht mehr die Determinante!

*Beweis.* Per definitionem gilt  $\det A^\top = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$ . Ist nun  $\tau = \sigma^{-1}$  die inverse Permutation, so haben wir  $\text{sgn}(\tau) = \text{sgn}(\sigma)$  und darüber hinaus  $a_{1\tau(1)} \dots a_{n\tau(n)} = a_{\sigma(1)1} \dots a_{\sigma(n)n}$ , denn diese Produkte unterscheiden sich nur in der Reihenfolge ihrer Faktoren. Damit ergibt sich dann wie behauptet

$$\det A^\top = \sum_{\tau \in S_n} \text{sgn}(\tau) a_{1\tau(1)} \dots a_{n\tau(n)}$$

□

**3.6.2.6 (Schmutzige Anschauung: Betrag der Determinante und Volumen).** Vor der weiteren Entwicklung der Theorie will ich nun zunächst die anschauliche Bedeutung der Determinante einer Matrix mit reellen Einträgen diskutieren. Ich beginne mit der anschaulichen Bedeutung des Betrags der Determinante und beschränke mich dazu erst einmal auf den Fall  $n = 2$ . Hoffentlich ist anschaulich klar, daß jede lineare Abbildung  $L : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  einen „Flächenveränderungsfaktor“  $c(L)$  haben sollte, daß es also dazu eine reelle Konstante  $c(L) \geq 0$  geben sollte derart, daß „das Bild unter  $L$  eines Flächenstücks  $U$  der Fläche  $\text{vol}(U)$  die Fläche  $\text{vol}(LU) = c(L) \text{vol}(U)$  hat“. Formal zeigt das die Transformationsformel ??, die für besagte Konstante auch gleich die Formel

$$c(L) = |\det L|$$

liefert. Ich will diese Formel im folgenden heuristisch begründen. Anschaulich ist hoffentlich klar, daß unsere durch die Vorschrift  $L \mapsto c(L)$  gegebene „Flächenveränderungsfaktorabbildung“  $c : \text{Mat}(2; \mathbb{R}) \rightarrow \mathbb{R}_{\geq 0}$  die folgenden Eigenschaften haben sollte:

1. Sie sollte „multiplikativ“ sein, in Formeln  $c(LM) = c(L)c(M)$ ;
2. Die Streckung einer Achse sollte die Fläche eines Flächenstücks genau durch Multiplikation mit dem Betrag des Streckfaktors ändern, in Formeln  $c(\text{diag}(a, 1)) = c(\text{diag}(1, a)) = |a|$ ;
3. Scherungen sollten Flächen unverändert lassen, in Formeln  $c(D) = 1$  für  $D$  eine obere oder untere Dreiecksmatrix mit Einsen auf der Diagonale.

Da sich nun nach 3.2.5.10 jede Matrix als Produkt von Elementarmatrizen darstellen läßt, kann es höchstens eine Abbildung  $c : \text{Mat}(2; \mathbb{R}) \rightarrow \mathbb{R}_{\geq 0}$  geben, die diese drei Eigenschaften hat. In 3.6.4.1 werden wir für unsere Determinante die „Multiplikationsformel“  $\det(LM) = \det(L)\det(M)$  zeigen, und zusammen mit unserer Formel 3.6.2.4 für die Determinante einer oberen oder unteren Dreiecksmatrix wird dann auch umgekehrt klar, daß  $M \mapsto |\det M|$  eine Abbildung mit unseren drei Eigenschaften ist. Das beendet unsere heuristische Argumentation für die Stichhaltigkeit der Anschauung als Flächenveränderungsfaktor für den

$$\det \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} = (\det A)(\det B)$$

Die Determinante einer block-oberen Dreiecksmatrix ist, wie Sie in Übung 3.6.2.9 zeigen, das Produkt der Determinanten ihrer Blöcke auf der Diagonalen. Dieses Bild illustriert den Fall von nur zwei Blöcken auf der Diagonalen. Das Symbol unten links ist eine Null, das Symbol \* deutet an, daß unerheblich ist, was da steht.

Betrag der Determinante von reellen  $(2 \times 2)$ -Matrizen. In höheren Dimensionen liefert dieselbe Argumentation analoge Resultate, insbesondere kann der Betrag der Determinante einer  $(3 \times 3)$ -Matrix aufgefaßt werden als der Faktor, um den die zugehörige lineare Abbildung Volumina ändert. Damit sollte auch anschaulich klar werden, warum  $\det L \neq 0$  gleichbedeutend ist zur Invertierbarkeit von  $L$ , was wir im allgemeinen als 3.6.4.2 zeigen.

**3.6.2.7 (Schmutzige Anschauung: Determinantenvorzeichen und Drehsinn).** Das Vorzeichen der Determinante einer invertierbaren reellen  $(2 \times 2)$ -Matrix zeigt anschaulich gesprochen an, „ob die dadurch gegebene lineare Selbstabbildung der Ebene  $\mathbb{R}^2$  den Drehsinn erhält oder umkehrt“. Formal prüft man leicht, daß  $GL(2; \mathbb{R})$  genau zwei „Wegzusammenhangskomponenten“ hat, nämlich die Matrizen mit positiver Determinante und die mit negativer Determinante. Dasselbe gilt für  $GL(n; \mathbb{R})$  und  $n \geq 1$  beliebig, vergleiche ???. Im Fall allgemeiner angeordneter Körper wird diese anschauliche Erkenntnis ihrerseits unsere Definition 3.6.5.2 einer „Orientierung“ auf einem Vektorraum über einem angeordneten Körper motivieren. Um die Beziehung zwischen Drehsinn und Determinante heuristisch zu begründen, können wir ähnlich argumentieren wie zuvor: Zunächst einmal führen wir ganz heuristisch eine angepaßte Notation ein und erklären für eine invertierbare lineare Abbildung  $L : \mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$  ein Vorzeichen  $\varepsilon(L)$  durch die Vorschrift

$$\varepsilon(L) = \begin{cases} 1 & L \text{ erhält den Drehsinn;} \\ -1 & L \text{ kehrt den Drehsinn um.} \end{cases}$$

In Formeln ausgedrückt behaupten wir dann also

$$\varepsilon(L) = \det L / |\det L|$$

Diese Formel will ich im folgenden heuristisch begründen. Anschaulich ist hoffentlich klar, daß unser  $\varepsilon : GL(2; \mathbb{R}) \rightarrow \{1, -1\}$  die folgenden Eigenschaften haben sollte:

1. Es sollte „multiplikativ“ sein, in Formeln  $\varepsilon(LM) = \varepsilon(L)\varepsilon(M)$ ;
2. Die Streckung einer Achse sollte den Drehsinn genau durch die Multiplikation mit dem Vorzeichen des Streckfaktors ändern, in Formeln sollte für  $a \in \mathbb{R}^\times$  also gelten  $\varepsilon(\text{diag}(a, 1)) = \varepsilon(\text{diag}(1, a)) = a / |a|$ ;
3. Scherungen sollten den Drehsinn nicht ändern, in Formeln sollte also gelten  $\varepsilon(D) = 1$  für  $D$  eine obere oder untere Dreiecksmatrix mit Einsen auf der Diagonale.

Da sich nun nach 3.2.5.10 jede invertierbare Matrix als Produkt von invertierbaren Elementarmatrizen darstellen läßt, kann es höchstens eine Abbildung  $\varepsilon :$

$\mathrm{GL}(2; \mathbb{R}) \rightarrow \{1, -1\}$  geben, die diese drei Eigenschaften hat. In 3.6.4.1 werden wir die „Multiplikationsformel“  $\det(LM) = \det(L)\det(M)$  für unsere Determinante zeigen, und zusammen mit unserer Formel 3.6.2.4 für die Determinante einer oberen oder unteren Dreiecksmatrix wird dann umgekehrt auch klar, daß  $M \mapsto \det M / |\det M|$  eine Abbildung mit unseren drei Eigenschaften ist. Das bedeutet unsere heuristische Argumentation für die Stichhaltigkeit der Anschauung  $\det M / |\det M| = \varepsilon(L)$  für das Vorzeichen der Determinante von invertierbaren  $(2 \times 2)$ -Matrizen. In höheren Dimensionen liefert eine analoge Argumentation analoge Resultate. So zeigt etwa das Vorzeichen der Determinante einer invertierbaren Abbildung  $L : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  an, ob sie die „Händigkeit“ erhält oder vielmehr „Rechtsgewinde und Linksgewinde vertauscht“.

*Ergänzung 3.6.2.8 (Händigkeit und Spiegel).* Amüsant ist in diesem Zusammenhang die naive Frage, warum ein Spiegel „rechts und links vertauscht, aber nicht oben und unten“. Die Antwort lautet, daß ein Spiegel ebensowenig rechts und links vertauscht wie oben und unten, sondern vielmehr vorne und hinten. Wir versuchen nur unbewußt, uns so gut wie möglich mit unserem Spiegelbild zu identifizieren, indem wir hinter den Spiegel treten, in Formeln also durch eine  $180^\circ$ -Drehung im Raum um eine geeignete vertikale Achse im Spiegel. Dann stellen wir fest, daß das zwar fast gelingt aber nicht ganz, und daß genauer die Verknüpfung der Spiegelung am Spiegel mit dieser Drehung gerade eine Spiegelung ist, die rechts und links vertauscht.

## Übungen

*Übung 3.6.2.9.* Die Determinante einer block-oberen Dreiecksmatrix ist das Produkt der Determinanten ihrer Blöcke auf der Diagonalen. Hinweis: Man variiere das Argument für 3.6.2.4.

*Übung 3.6.2.10.* Man betrachte die  $(n \times n)$ -Matrix mit Einträgen  $(-1)$  oberhalb der Diagonalen und  $1$  auf und unterhalb der Diagonalen und zeige, daß ihre Determinante  $n!$  ist.

## 3.6.3 Charakterisierung der Determinante

**Definition 3.6.3.1.** Seien  $V, U$  Vektorräume über einem Körper  $K$ . Eine bilineare Abbildung  $F : V \times V \rightarrow U$  heißt **symmetrisch**, wenn gilt

$$F(v, w) = F(w, v) \quad \forall v, w \in V$$

Eine bilineare Abbildung  $F : V \times V \rightarrow U$  heißt **alternierend**, wenn gilt

$$F(v, v) = 0 \quad \forall v \in V$$

3.6.3.2 (**Herkunft der Bezeichnung „alternierend“**). Gegeben eine bilineare Abbildung  $F : V \times V \rightarrow U$  mit der Eigenschaft  $F(v, v) = 0 \quad \forall v \in V$ , die also im Sinne unserer Definition 3.6.3.1 alternierend ist, gilt stets

$$F(v, w) = -F(w, v) \quad \forall v, w \in V$$

In der Tat haben wir

$$\begin{aligned} 0 &= F(v + w, v + w) \\ &= F(v, v + w) + F(w, v + w) \\ &= F(v, v) + F(v, w) + F(w, v) + F(w, w) \\ &= F(v, w) + F(w, v) \end{aligned}$$

Gilt umgekehrt  $F(v, w) = -F(w, v) \quad \forall v, w \in V$ , so folgt  $F(v, v) = -F(v, v)$  alias  $(1_K + 1_K)F(v, v) = 0_K$  für alle  $v \in V$ , und haben wir  $1_K + 1_K \neq 0_K$  alias  $\text{char } K \neq 2$ , so folgt daraus auch wieder  $F(v, v) = 0$ .

3.6.3.3. Man mag eine bilineare Abbildung  $F : V \times V \rightarrow U$  **antisymmetrisch** nennen, wenn gilt  $F(v, w) = -F(w, v)$  für alle  $v, w$ . Damit sind allerdings in Charakteristik Zwei symmetrische Bilinearformen dasselbe wie antisymmetrische Bilinearformen.

**Definition 3.6.3.4.** Seien  $V_1, \dots, V_n, W$  Vektorräume über einem Körper  $K$ . Eine Abbildung  $F : V_1 \times \dots \times V_n \rightarrow W$  alias Multiabbildung  $F : V_1 \curlyvee \dots \curlyvee V_n \rightarrow W$  heißt **multilinear**, wenn für alle  $j$  und alle für  $i \neq j$  beliebig aber fest gewählten  $v_i \in V_i$  die Abbildung  $V_j \rightarrow W$ ,  $v_j \mapsto F(v_1, \dots, v_j, \dots, v_n)$  linear ist. Für die Menge aller derartigen multilinearen Abbildungen verwenden wir analog zum Fall bilinearer Abbildungen die beiden Notationen

$$\text{Hom}_K(V_1 \curlyvee V_2 \curlyvee \dots \curlyvee V_n, W) = \text{Hom}^{(n)}(V_1 \times V_2 \times \dots \times V_n, W)$$

Im Fall  $n = 2$  erhalten wir unsere bilinearen Abbildungen aus 3.2.3.8. Im Fall  $n = 1$  erhalten wir unsere linearen Abbildungen. Im Fall  $n = 0$  verwenden wir die Notationen  $\text{Hom}_K(\emptyset, W) = \text{Hom}_K^{(0)}(\{\}\}, W)$  für die Menge aller 0-multilinearen Abbildungen vom leeren Produkt nach  $W$  alias aller beliebigen Abbildungen von der einelementigen Menge  $\{\}\}$  nach  $W$ . Das Auswerten bei  $*$  liefert damit eine Bijektion  $\text{Hom}_K(\emptyset, W) \xrightarrow{\sim} W$ . Wir werden sie in der Notation oft so behandeln, als seien diese Mengen schlicht gleich.

**Definition 3.6.3.5.** Seien  $V, W$  Vektorräume über einem Körper  $K$ . Eine multilineare Abbildung  $F : V \times \dots \times V \rightarrow W$  heißt **alternierend**, wenn sie auf jedem  $n$ -Tupel verschwindet, in dem zwei Einträge übereinstimmen, wenn also in Formeln gilt

$$(\exists i \neq j \text{ mit } v_i = v_j) \Rightarrow F(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = 0$$

Wir verwenden für den Raum aller derartigen alternierenden multilinear Abbildungen die Notation  $\text{Alt}^n(V, W)$ . Ist  $W = K$  der Grundkörper, so sprechen wir von **Multilinearformen** und verwenden die abkürzende Notation  $\text{Alt}^n(V) := \text{Alt}^n(V, K)$ .

**3.6.3.6.** Sei  $F : V \times \dots \times V \rightarrow W$  eine alternierende multilineare Abbildung. Mit 3.6.3.2 folgt, daß sich das Vorzeichen von  $F$  ändert, wenn immer man zwei Einträge vertauscht, in Formeln

$$F(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -F(v_1, \dots, v_j, v_i, \dots, v_n)$$

Im Fall eines Grundkörpers einer von Zwei verschiedenen Charakteristik erhält man wieder mit 3.6.3.2 auch die umgekehrte Implikation.

**Satz 3.6.3.7 (Charakterisierung der Determinante).** *Ist  $K$  ein Körper, so ist die Determinante die einzige Abbildung  $\det : \text{Mat}(n; K) \rightarrow K$ , die multilinear und alternierend ist als Funktion der  $n$  Spaltenvektoren und die der Einheitsmatrix die Eins zuordnet.*

*Beweis.* Daß unsere in 3.6.2.1 durch die Leibniz-Formel definierte Determinante multilinear ist und der Einheitsmatrix die Eins zuordnet, scheint mir offensichtlich. Stimmen weiter zwei Spalten einer Matrix überein, so verschwindet ihre Determinante, denn für  $\tau \in \mathcal{S}_n$  die Transposition der entsprechenden Indizes gilt  $a_{1\sigma(1)} \dots a_{n\sigma(n)} = a_{1\tau\sigma(1)} \dots a_{n\tau\sigma(n)}$  und  $\text{sgn}(\sigma) = -\text{sgn}(\tau\sigma)$ , so daß sich in der Leibniz-Formel die entsprechenden Terme gerade wegheben. Unsere durch die Leibniz-Formel gegebene Abbildung hat also die geforderten Eigenschaften, und es gilt nur noch zu zeigen, daß es keine weiteren Abbildungen  $d : \text{Mat}(n; K) \rightarrow K$  mit den besagten Eigenschaften gibt. Nach 3.6.3.10 ist nun eine multilinear Abbildung festgelegt und festlegbar durch ihre Werte auf Tupeln von Basisvektoren. Insbesondere kennen wir aber unsere multilinear Abbildung  $d$  bereits, wenn wir ihre Werte

$$d(e_{\sigma(1)} | \dots | e_{\sigma(n)})$$

kennen für alle Abbildungen  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ . Ist  $d$  zusätzlich alternierend, so gilt  $d(e_{\sigma(1)} | \dots | e_{\sigma(n)}) = 0$ , falls  $\sigma$  nicht injektiv ist, und für jede Transposition  $\tau$  haben wir  $d(e_{\sigma\tau(1)} | \dots | e_{\sigma\tau(n)}) = -d(e_{\sigma(1)} | \dots | e_{\sigma(n)})$ . Da nach 3.6.1.8 die Transpositionen die symmetrische Gruppe erzeugen, folgt daraus

$$d(e_{\sigma(1)} | \dots | e_{\sigma(n)}) = \begin{cases} \text{sgn}(\sigma)d(e_1 | \dots | e_n) & \sigma \in \mathcal{S}_n; \\ 0 & \text{sonst.} \end{cases}$$

Erfüllt  $d$  dann auch noch unsere Bedingung  $d(e_1 | \dots | e_n) = 1$  für die Determinante der Einheitsmatrix, so folgt sofort  $d = \det$ .  $\square$

**3.6.3.8 (Multilineare alternierende Funktionen auf Matrizen).** Im allgemeinen folgt über einem beliebigen Körper  $K$  mit den Argumenten des vorhergehenden Beweises für jede Abbildung  $d : \text{Mat}(n; K) \rightarrow K$ , die multilinear und alternierend ist als Funktion der  $n$  Spaltenvektoren, die Formel

$$d = d(\mathbf{e}_1 | \dots | \mathbf{e}_n) \det$$

Das brauchen wir für den vorhergehenden Beweis zwar schon gar nicht mehr zu wissen, es wird sich aber beim Beweis der Multiplikativität der Determinante als hilfreich erweisen.

**3.6.3.9 (Berechnung der Determinante).** Will man die Determinante einer Matrix explizit ausrechnen, so empfiehlt es sich bei größeren Matrizen, sie zunächst mit dem Gauß-Algorithmus in Zeilenstufenform zu bringen: Addieren wir ein Vielfaches einer Zeile zu einer anderen, ändert sich die Determinante nach 3.6.3.7 ja nicht, und vertauschen wir zwei Zeilen, so ändert sich nur ihr Vorzeichen. Bei einer Matrix in Zeilenstufenform ist dann nach 3.6.2.4 die Determinante schlicht das Produkt der Diagonaleinträge.

## Übungen

*Übung 3.6.3.10.* Gegeben Vektorräume  $V_1, V_2, \dots, V_n, W$  über einem festen Körper und  $B_i \subset V_i$  jeweils eine Basis liefert die Restriktion eine Bijektion

$$\text{Hom}_K^{(n)}(V_1 \times \dots \times V_n, W) \xrightarrow{\sim} \text{Ens}(B_1 \times \dots \times B_n, W)$$

oder in unseren Notationen für multilinear Abbildungen und Multiabbildungen gleichbedeutend

$$\text{Hom}_K(V_1 \curlyvee \dots \curlyvee V_n, W) \xrightarrow{\sim} \text{Ens}(B_1 \curlyvee \dots \curlyvee B_n, W)$$

Jede multilinear Abbildung ist also festgelegt und festlegbar durch die Bilder von Tupeln von Basisvektoren. Den Spezialfall  $n = 1$  kennen wir bereits aus 3.2.3.2, den Spezialfall  $n = 2$  aus 3.2.3.9, im Fall  $n = 0$  ist die Aussage eh tautologisch.

*Übung 3.6.3.11.* Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum der endlichen Dimension  $\dim V = n \geq 0$  ist der Raum der alternierenden multilinear Abbildungen  $V^n \rightarrow K$  eindimensional.

*Übung 3.6.3.12 (Multiverknüpfung multilinearer Abbildungen).* Man zeige: Gegeben ein Körper  $K$  und natürliche Zahlen  $n \geq 0$  und  $m(1), \dots, m(n) \geq 0$  und  $K$ -Vektorräume  $W, V_1, \dots, V_n, U_{1,1}, \dots, U_{1,m(1)}, \dots, U_{n,m(n)}$  und multilinear Abbildungen  $f : V_1 \times \dots \times V_n \rightarrow W$  sowie  $g_i : U_{i,1} \times \dots \times U_{i,m(i)} \rightarrow V_i$  ist auch die Abbildung  $f \circ (g_1 \times \dots \times g_n)$  vom Produkt der  $U_{i,j}$  nach  $W$  multilinear. Oder nein, das ist scheußlich auszuschreiben: Man behandle nur den Fall  $n = 3$ ,  $m(1) = m(2) = 2, m(3) = 0$ .

### 3.6.4 Rechenregeln für Determinanten

**Satz 3.6.4.1 (Multiplikativität der Determinante).** Sei  $K$  ein Kring. Gegeben quadratische Matrizen  $A, B \in \text{Mat}(n; K)$  gilt

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

*Erster Beweis.* Wir notieren  $\mathcal{T}_n := \text{Ens}(\{1, \dots, n\})$  die Menge aller Abbildungen  $\kappa : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  und rechnen

$$\begin{aligned} \det(AB) &= \sum_{\sigma} \text{sgn}(\sigma) \prod_i (AB)_{i\sigma(i)} \\ &= \sum_{\sigma} \text{sgn}(\sigma) \prod_i \sum_j a_{ij} b_{j\sigma(i)} \\ &= \sum_{\sigma \in \mathcal{S}_n, \kappa \in \mathcal{T}_n} \text{sgn}(\sigma) a_{1\kappa(1)} b_{\kappa(1)\sigma(1)} \dots a_{n\kappa(n)} b_{\kappa(n)\sigma(n)} \\ &= \sum_{\kappa \in \mathcal{T}_n} a_{1\kappa(1)} \dots a_{n\kappa(n)} \sum_{\sigma \in \mathcal{S}_n} \text{sgn}(\sigma) b_{\kappa(1)\sigma(1)} \dots b_{\kappa(n)\sigma(n)} \\ &= \sum_{\kappa \in \mathcal{T}_n} a_{1\kappa(1)} \dots a_{n\kappa(n)} \det(B_{\kappa}) \end{aligned}$$

mit der Vereinbarung, daß  $B_{\kappa}$  diejenige Matrix bezeichnet, deren Zeilen der Reihe nach die Zeilen mit den Indizes  $\kappa(1), \dots, \kappa(n)$  der Matrix  $B$  sind. Aus 3.6.3.7 folgt aber  $\det B_{\kappa} = 0$  falls  $\kappa \notin \mathcal{S}_n$  und  $(\det B_{\kappa}) = \text{sgn}(\kappa)(\det B)$  falls  $\kappa \in \mathcal{S}_n$ . Damit erhalten wir dann  $\det(AB) = (\det A)(\det B)$  wie gewünscht.  $\square$

*Zweiter Beweis im Körperfall.* Die Formel ist klar, wenn die Zweite der beiden Matrizen eine Elementarmatrix ist, also eine Matrix, die sich von der Einheitsmatrix in höchstens einem Eintrag unterscheidet. In der Tat entspricht in diesem Fall die Rechtsmultiplikation mit besagter Matrix einer Spaltenoperation. Unsere Formel folgt im allgemeinen, da nach 3.2.5.10 jede Matrix ein Produkt von Elementarmatrizen ist.  $\square$

*Dritter Beweis im Körperfall.* Man hält die Matrix  $A$  fest und betrachtet die beiden Abbildungen  $\text{Mat}(n; K) \rightarrow K$  gegeben durch  $B \mapsto \det(A) \det(B)$  und  $B \mapsto \det(AB)$ . Beide sind multilinear und alternierend als Funktion der Spalten von  $B$ , und beide ordnen der Einheitsmatrix  $B = I$  den Wert  $\det(A)$  zu. Aus 3.6.3.8 folgt damit unmittelbar, daß unsere beiden Abbildungen übereinstimmen. Dieser Beweis funktioniert auch für beliebige Kringe, sobald wir die Theorie linearer und multilinearer Abbildungen entsprechend verallgemeinert haben.  $\square$

*Vierter Beweis im Körperfall.* Im Rahmen der allgemeinen Theorie der Multilinearformen geben wir einen alternativen Beweis in ?? sowie ähnlich aber in einem noch größeren Rahmen in 4.6.5.16.  $\square$

*Ableitung des Falls beliebiger Kringe aus dem Fall eines Körpers.* Man betrachte die  $(n \times n)$ -Matrizen mit Einträgen  $X_{ij}$  und  $Y_{ij}$  im Polynomring  $\mathbb{Z}[X_{ij}, Y_{ij}]$

über  $\mathbb{Z}$  in  $2n^2$  Veränderlichen. Als kommutativer Integritätsbereich liegt dieser Polynomring in einem Körper, eben in seinem Quotientenkörper, weshalb man aus dem Körperfall folgern kann, daß die Multiplikationsformel auch für Matrizen mit Einträgen in diesem Ring gelten muß, und insbesondere für die eben beschriebenen Matrizen. Dann aber gilt sie auch, wenn wir für die Variablen irgendwelche Elemente irgendeines Krings einsetzen.  $\square$

**Satz 3.6.4.2 (Determinantenkriterium für Invertierbarkeit).** *Die Determinante einer quadratischen Matrix mit Einträgen in einem Körper ist von Null verschieden genau dann, wenn unsere Matrix invertierbar ist.*

*Beweis.* In Formeln behaupten wir für einen Körper  $K$  und eine beliebige quadratische Matrix  $A \in \text{Mat}(n; K)$  also

$$\det A \neq 0 \Leftrightarrow A \text{ invertierbar}$$

Ist  $A$  invertierbar, so gibt es eine Matrix  $B = A^{-1}$  mit  $AB = I$ . Mit der Multiplikationsformel folgt  $(\det A)(\det B) = \det I = 1$  und folglich  $\det A \neq 0$ . Das zeigt die Implikation  $\Leftarrow$ . Ist  $A$  nicht invertierbar, so hat  $A$  nicht vollen Rang, die Familie der Spaltenvektoren von  $A$  ist demnach linear abhängig. Wir können also einen Spaltenvektor, ohne Beschränkung der Allgemeinheit den Ersten, durch die Anderen ausdrücken, etwa  $a_{*1} = \lambda_2 a_{*2} + \dots + \lambda_n a_{*n}$ . Dann folgt mit den Eigenschaften multilinear und alternierend jedoch

$$\begin{aligned} \det A &= \det(\lambda_2 a_{*2} + \dots + \lambda_n a_{*n} | a_{*2} | \dots | a_{*n}) \\ &= \lambda_2 \det(a_{*2} | a_{*2} | \dots | a_{*n}) + \dots + \lambda_n \det(a_{*n} | a_{*2} | \dots | a_{*n}) \\ &= \lambda_2 0 + \dots + \lambda_n 0 \\ &= 0 \end{aligned}$$

Damit ist auch die andere Implikation  $\Rightarrow$  gezeigt.  $\square$

**3.6.4.3 (Determinante eines Endomorphismus).** Aus der Multiplikationsformel folgt sofort  $\det(T^{-1}) = (\det T)^{-1}$  für jede invertierbare Matrix  $T$  und damit ergibt sich für jede weitere quadratische Matrix  $M$  die Identität  $\det(T^{-1}MT) = \det M$ . Nach 3.2.6.10 gilt für einen Endomorphismus  $f : V \rightarrow V$  eines endlichdimensionalen Vektorraums über einem Körper  $K$  und  $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}$  und  $M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$  die darstellenden Matrizen bezüglich zwei angeordneten Basen und  $T = {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}$  die Basiswechselmatrix nun

$$N = T^{-1}MT$$

Folglich hängt die Determinante einer darstellenden Matrix von  $f$  nicht von der Wahl der zur Darstellung gewählten angeordneten Basis ab, in Formeln gilt also

$\det(\mathcal{B}[f]_{\mathcal{B}}) = \det(\mathcal{A}[f]_{\mathcal{A}})$  für je zwei angeordnete Basen  $\mathcal{A}$  und  $\mathcal{B}$  von  $V$ . Diesen Skalar notieren wir von nun an

$$\det f = \det(f|V) = \det_K(f|V)$$

und nennen ihn die **Determinante des Endomorphismus**  $f$ . Dem einzigen Automorphismus des Nullraums ist insbesondere die Determinante 1 zuzuordnen.

**Satz 3.6.4.4 (Laplace'scher Entwicklungssatz).** *Gegeben eine  $(n \times n)$ -Matrix  $A = (a_{ij})$  und feste  $k, l$  bezeichne  $A\langle k, l \rangle$  die **Streichmatrix**, die aus  $A$  durch Streichen der  $k$ -ten Zeile und  $l$ -ten Spalte entsteht. So gilt für jedes feste  $i$  die **Entwicklung der Determinante nach der  $i$ -ten Zeile***

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

und für jedes feste  $j$  die **Entwicklung nach der  $j$ -ten Spalte**

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

3.6.4.5. Der folgende Beweis verwendet zwar die Sprache der Vektorräume, das Argument funktioniert jedoch ganz genauso statt für Matrizen mit Einträgen in einem Körper auch für Matrizen mit Einträgen in einem Kring.

*Beweis.* Wegen  $\det A = \det A^\top$  reicht es, die erste unserer beiden Formeln zu zeigen. Wir wissen bereits, daß sich die Determinante einer quadratischen Matrix nur um den Faktor  $(-1)^{j-1}$  ändert, wenn wir die  $j$ -te Spalte ganz nach vorne schieben, ohne die Reihenfolge der übrigen Spalten zu ändern. Es reicht also, unsere Formel für die Entwicklung nach der ersten Spalte zu zeigen, was im folgenden Beweis insbesondere die Notation vereinfacht. Wir schreiben unsere Matrix als Tupel von Spaltenvektoren  $A = (a_{*1}|a_{*2}| \dots |a_{*n})$  und schreiben den ersten Spaltenvektor als Linearkombination der Standardbasisvektoren

$$a_{*1} = a_{11}\mathbf{e}_1 + \dots + a_{n1}\mathbf{e}_n$$

Die Multilinearität der Determinante liefert sofort die erste Gleichung der Gleichungskette

$$\det A = \sum_{i=1}^n a_{i1} \det(\mathbf{e}_i|a_{*2}| \dots |a_{*n}) = \sum_{i=1}^n a_{i1} (-1)^{i-1} \det A\langle i, 1 \rangle$$

Die zweite Gleichung sehen wir ein, indem wir in der Matrix  $(\mathbf{e}_i|a_{*2}| \dots |a_{*n})$  die  $i$ -te Zeile ganz nach oben schieben, ohne die Reihenfolge der übrigen Zeilen zu ändern, um dann die Formel 3.6.2.9 für die Determinante von Block-oberen-Dreiecksmatrizen anzuwenden.  $\square$

**Satz 3.6.4.6 (Cramer'sche Regel).** Bildet man zu einer quadratischen Matrix  $A$  mit Einträgen in einem Kring die sogenannte **adjunkte Matrix**  $A^\sharp$  mit den Einträgen  $A_{ij}^\sharp = (-1)^{i+j} \det A\langle j, i \rangle$  für  $A\langle j, i \rangle$  die entsprechende Streichmatrix nach 3.6.4.4, so gilt

$$A \circ A^\sharp = (\det A) \cdot I$$

**3.6.4.7 (Diskussion der Terminologie).** Diese adjunkte Matrix ist nicht zu verwechseln mit der adjungierten Abbildung aus 4.1.12.5, mit der sie außer der Bezeichnung rein gar nichts zu tun hat. Man beachte auch die Indexvertauschung: In der  $i$ -ten Zeile und  $j$ -ten Spalte der adjungierten Matrix steht bis auf ein „schachbrettartig verteiltes Vorzeichen“ die Determinante der Matrix, die entsteht, wenn man die  $j$ -te Zeile und  $i$ -te Spalte der ursprünglichen Matrix streicht.

**3.6.4.8.** Meist versteht man unter der **Cramer'schen Regel** die Formel

$$x_i = \frac{\det(a_{*1} | \dots | b_* | \dots | a_{*n})}{\det(a_{*1} | \dots | a_{*i} | \dots | a_{*n})}$$

für die Lösung des Gleichungssystems  $x_1 a_{*1} + \dots + x_i a_{*i} \dots + x_n a_{*n} = b_*$ , wenn es denn eindeutig lösbar ist. Hier ist im Zähler wie angedeutet die  $i$ -te Spalte  $a_{*i}$  der Koeffizientenmatrix durch den Vektor  $b_*$  zu ersetzen. Besagte Formel ergibt sich unmittelbar durch Einsetzen der alternativen Darstellung von  $b_*$  als Linearkombination der Spalten in die Determinante im Zähler. Setzen wir in dieser Formel für  $b_*$  die Vektoren der Standardbasis ein, so erhalten wir die Einträge der inversen Matrix in der Form, in der sie auch im Satz beschrieben werden. Diese Formel wirkt zwar explizit, ist jedoch in der Praxis völlig unbrauchbar.

*Beweis.* Es gilt zu zeigen

$$\sum_i (-1)^{i+j} a_{ki} \det A\langle j, i \rangle = \delta_{kj}(\det A)$$

Im Fall  $k = j$  folgt das direkt aus unserer Entwicklung der Determinante nach der  $j$ -ten Zeile 3.6.4.4. Im Fall  $k \neq j$  steht die Formel für die Entwicklung nach der  $j$ -ten Zeile der Determinante der Matrix  $\tilde{A}$  da, die aus  $A$  entsteht beim Ersetzen der  $j$ -ten Zeile durch die  $k$ -te Zeile. Da diese Matrix jedoch zwei gleiche Zeilen hat und damit Determinante Null, gilt unsere Formel auch in diesem Fall.  $\square$

**Korollar 3.6.4.9 (Invertierbarkeit ganzzahliger Matrizen).** Eine quadratische Matrix mit Einträgen in einem Kring besitzt genau dann eine Inverse mit Einträgen in besagtem Kring, wenn ihre Determinante eine Einheit ist.

**3.6.4.10.** Eine quadratische Matrix mit ganzzahligen Einträgen besitzt insbesondere genau dann eine Inverse mit ganzzahligen Einträgen, wenn ihre Determinante

1 oder  $-1$  ist, und eine quadratische Matrix mit Einträgen im Polynomring über einem Körper besitzt genau dann eine Inverse mit polynomialem Einträgen, wenn ihre Determinante ein von Null verschiedenes konstantes Polynom ist.

*Beweis.* Sei  $K$  unser Kring. Gegeben Matrizen  $A, B \in \text{Mat}(n; K)$  mit  $AB = I$  gilt natürlich  $(\det A)(\det B) = \det I = 1$  und damit ist  $\det A$  eine Einheit in  $K$ . Ist umgekehrt  $\det A$  eine Einheit in  $K$ , so liefert nach der Cramer'schen Regel 3.6.4.6 die Formel  $B = (\det A)^{-1}A^\sharp$  eine Matrix  $B \in \text{Mat}(n; K)$  mit  $AB = I$ . Indem wir dies Argument auf die transponierte Matrix anwenden und das Resultat wieder transponieren, finden wir auch  $C \in \text{Mat}(n; K)$  mit  $CA = I$ . Durch Multiplizieren der zweiten Gleichung mit  $B$  von rechts folgt sofort  $B = C$ , folglich ist  $A$  in der Tat invertierbar in  $\text{Mat}(n; K)$  im Sinne von 2.2.2.  $\square$

## Übungen

*Übung 3.6.4.11.* Gegeben Endomorphismen  $f, g$  eines endlichdimensionalen Vektorraums gilt  $\det(fg) = (\det f)(\det g)$ .

*Ergänzende Übung 3.6.4.12.* Man zeige die Formel für die **Vandermonde-Determinante**

$$\det \begin{pmatrix} 1 & X_0 & X_0^2 & \dots & X_0^n \\ \vdots & & & & \vdots \\ 1 & X_n & X_n^2 & \dots & X_n^n \end{pmatrix} = \prod_{0 \leq j < i \leq n} (X_i - X_j)$$

Hinweis: Ich empfehle, vom Nullstellensatz für Hyperebenen 3.5.4.5 und dem Fall des Grundkörpers  $\mathbb{Q}$  auszugehen.

*Übung 3.6.4.13.* Sei  $K$  ein Körper. Für jedes  $r$  versteht man unter den  **$r$ -Minoren** unserer Matrix die Determinanten aller derjenigen  $(r \times r)$ -Matrizen, die wir aus unserer Matrix durch das Streichen von Zeilen und Spalten erhalten können. Man zeige: Die Matrizen vom Rang  $< r$  in  $\text{Mat}(m \times n; K)$  sind genau diejenigen Matrizen, bei denen alle  $r$ -Minoren verschwinden.

*Ergänzende Übung 3.6.4.14.* Jeder komplexe Vektorraum  $V$  kann auch als reeller Vektorraum aufgefaßt werden. Man zeige im endlichdimensionalen Fall die Formel  $\det_{\mathbb{R}}(f|V) = |\det_{\mathbb{C}}(f|V)|^2$ . Eine Verallgemeinerung auf allgemeinere Körpererweiterungen wird in ?? diskutiert.

*Ergänzende Übung 3.6.4.15 (Determinante geeignet geblockter Matrizen).* Es seien  $n^2$  paarweise kommutierende Matrizen  $A_{11}, \dots, A_{nn}$  mit  $m$  Zeilen und Spalten und Einträgen in einem Kring  $R$  gegeben. Wir bilden die  $(mn \times mn)$ -Matrix

$$B = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \dots & A_{nn} \end{pmatrix}$$

Man zeige, daß gilt

$$\det B = \det \left( \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) A_{1\sigma(1)} \dots A_{n\sigma(n)} \right)$$

Hinweis: Ist  $A_{11}$  die Einheitsmatrix, so folgt die Behauptung durch Nullen der ersten Blockspalte und Induktion. Ist  $\det(A_{11})$  kürzbar, so folgt die Aussage durch Multiplizieren mit  $\operatorname{diag}(A_{11}^\sharp, I, \dots, I)$  für  $A_{11}^\sharp$  die adjunkte Matrix zu  $A_{11}$ . Im allgemeinen kann man eine weitere Variable  $X$  einführen und  $A_{11}$  durch die Matrix  $A_{11} + XI$  ersetzen, deren Determinante ein normiertes Polynom in  $R[X]$  und deshalb kürzbar ist. Nachher setze man dann  $X = 0$ .

*Übung 3.6.4.16 (Determinante geeignet geblockter Matrizen, Variante).* Man zeige dieselbe Formel wie in 3.6.4.15 auch für den Fall, daß die Matrizen  $A_{ij}$  alle obere Dreiecksmatrizen sind. Hinweis: Wir betrachten diejenige Abbildung

$$f : \{1, \dots, mn\} \rightarrow \{1, \dots, m\}$$

die verträglich ist mit der Restklassenabbildung beider Mengen auf  $\mathbb{Z}/m\mathbb{Z}$ , und beachten, daß für eine Permutation  $\sigma \in S_{mn}$  mit  $f(\sigma(i)) \leq f(i) \forall i$  notwendig Gleichheit gilt für alle  $i$ .

*Ergänzende Übung 3.6.4.17 (Satz von Hensel).* Seien ein Körper  $K$  und ein Gruppenhomomorphismus  $\varphi : \operatorname{GL}(n; K) \rightarrow K^\times$  gegeben. Man zeige, daß es einen Gruppenhomomorphismus  $\alpha : K^\times \rightarrow K^\times$  gibt mit  $\varphi = \alpha \circ \det$ . Hinweis: Je zwei Elementarmatrizen  $A, B$  mit genau einem von Null verschiedenen Eintrag an derselben Stelle außerhalb der Diagonalen sind zueinander konjugiert, als da heißt, es gibt eine invertierbare Matrix  $C$  mit  $CAC^{-1} = B$ .

### 3.6.5 Orientierung

3.6.5.1. Wir verwandeln nun unsere anschauliche Interpretation 3.6.2.7 des Vorzeichens der Determinante in eine formale Definition. Gegeben ein Element  $a \neq 0$  eines angeordneten Körpers  $K$  bezeichne  $\operatorname{sign}(a) \in \{1, -1\}$  das Vorzeichen von  $a$ , also  $\operatorname{sign}(a) = 1$  für  $a > 0$  und  $\operatorname{sign}(a) = -1$  für  $a < 0$ .

**Definition 3.6.5.2.** Eine **Orientierung** eines endlichdimensionalen Vektorraums  $V$  über einem angeordneten Körper ist eine Vorschrift  $\varepsilon$ , die jeder angeordneten Basis  $\mathcal{A}$  unseres Vektorraums ein Vorzeichen  $\varepsilon(\mathcal{A}) \in \{+1, -1\}$  zuordnet und zwar so, daß für je zwei angeordnete Basen  $\mathcal{A}, \mathcal{B}$  die Determinante der Basiswechselmatrix das Vorzeichen  $\varepsilon(\mathcal{A})\varepsilon(\mathcal{B})$  hat, in Formeln

$$\varepsilon(\mathcal{A})\varepsilon(\mathcal{B}) = \operatorname{sign}(\det_{\mathcal{A}}[\operatorname{id}]_{\mathcal{B}})$$

Das Vorzeichen  $\varepsilon(\mathcal{A})$  nennen wir die **Orientierung der angeordneten Basis  $\mathcal{A}$**  unseres orientierten Vektorraums. Eine angeordnete Basis der Orientierung  $+1$  in einem orientierten Vektorraum nennen wir eine **verträglich orientierte Basis**, eine angeordnete Basis der Orientierung  $-1$  eine **unverträglich orientierte Basis**. Sprechen wir von der **durch eine angeordnete Basis gegebenen Orientierung**, so meinen wir diejenige Orientierung, die besagter Basis das Vorzeichen  $+1$  zuordnet. Gegeben ein angeordneter Körper  $K$  bezeichnen wir diejenige Orientierung des  $K^n$  als die **Standardorientierung**, die der Standardbasis mit ihrer Standardanordnung das Vorzeichen  $+1$  zuordnet. Unter der **Standardorientierung des Nullraums** verstehen wir diejenige Orientierung, die der einzigen angeordneten Basis  $\emptyset$  das Vorzeichen  $+1$  zuordnet.

3.6.5.3. Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem angeordneten Körper erklären wir seine **Orientierungsmenge**

$$\text{or}(V)$$

als die zweielementige Menge seiner beiden Orientierungen nach 3.6.5.2. Jeder Vektorraumisomorphismus  $f : V \xrightarrow{\sim} W$  liefert eine Bijektion  $\text{or}(f) : \text{or}(V) \xrightarrow{\sim} \text{or}(W)$  vermittels der von  $f$  zwischen den Mengen der angeordneten Basen beider Räume induzierten Bijektion. Es gilt dann  $\text{or}(f \circ g) = \text{or}(f) \circ \text{or}(g)$  und  $\text{or}(\text{id}) = \text{id}$ . Weiter gilt für jeden Automorphismus  $f : V \xrightarrow{\sim} V$  offensichtlich

$$\text{or}(f) = \text{id}_{\text{or}(V)} \Leftrightarrow (\det f) > 0$$

In Worten sind also die orientierungserhaltenden Automorphismen genau die mit positiver Determinante und entsprechend die orientierungsumkehrenden Automorphismen genau die mit negativer Determinante.

3.6.5.4. Unter einer **Orientierung eines endlichdimensionalen affinen Raums  $E$**  über einem angeordneten Körper verstehen wir eine Orientierung seines Richtungsraums und setzen  $\text{or}(E) := \text{or}(\vec{E})$  sowie  $\text{or}(\varphi) := \text{or}(\vec{\varphi})$  für jeden Isomorphismus  $\varphi : E \xrightarrow{\sim} F$  endlichdimensionaler affiner Räume über unserem angeordneten Körper.

*Vorschau* 3.6.5.5. In der Topologie werden wir jedem endlichdimensionalen reellen Vektorraum  $V$  auch seine „topologische Orientierungsmenge“ zuordnen als die Menge  $\text{or}^{\text{top}}(V)$  der beiden Erzeuger der relativen Homologie  $H(V, V \setminus 0)$ . Ähnlich werden wir auch jedem endlichdimensionalen reellen affinen Raum seine „topologische Orientierungsmenge“ zuordnen. In diesem Kontext nennen wir die hier eingeführten Begriffe präziser die **algebraischen Orientierungsmengen** und verwenden dafür die Notation  $\text{or}^{\text{alg}}$ .

*Bemerkung* 3.6.5.6 (**Diskussion der Terminologie**). In der Literatur findet man vielfach eine Definition, bei der eine Orientierung eines reellen Vektorraums als

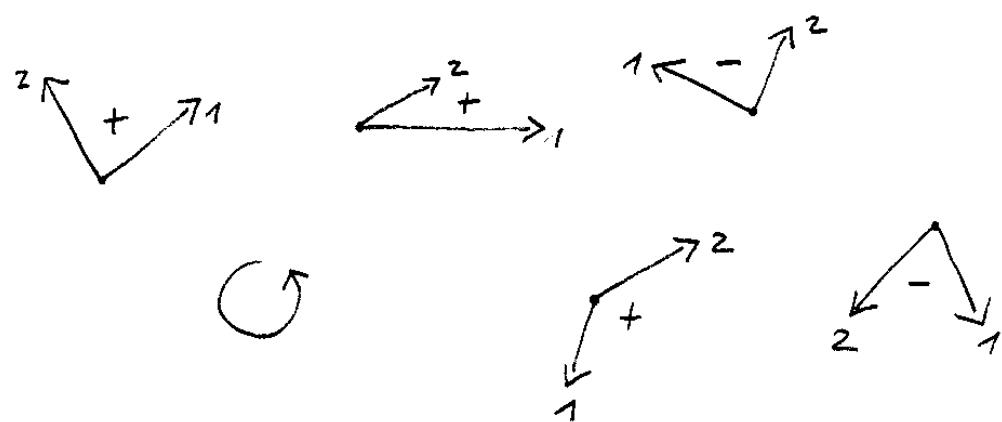
eine Äquivalenzklasse von Basen unter einer geeigneten Äquivalenzrelation erklärt wird. Diese Definition liefert dasselbe außer im Fall des Nullraums. In diesem Fall scheint mir die hier gegebene Definition, die auch dem Nullraum zwei verschiedene Orientierungen erlaubt, das sinnvollere Konzept.

*Beispiel 3.6.5.7.* Eine Orientierung einer reellen Gerade anzugeben bedeutet anschaulich, auf dieser Gerade eine „Richtung“ auszuwählen, eben die Richtung, in die diejenigen Vektoren zeigen, die verträglich orientierte Basen ihres Richtungsraums bilden. Wir nennen diese Vektoren dann kurzerhand **positive Vektoren** und denken uns unsere Gerade mit derjenigen Anordnung versehen, für die die Addition positiver Vektoren Elemente vergrößert. Mit diesen Konventionen können wir für einen orientierten eindimensionalen Vektorraum  $L$  die Menge der positiven Vektoren mit  $L_{>0}$  bezeichnen. Analog vereinbaren wir für die Elemente von  $L_{<0}$  die Bezeichnung **negative Vektoren** und nennen die Elemente von  $L_{\geq 0}$  die **nicht-negativen Vektoren**.

*Beispiel 3.6.5.8.* Der schmutzige Raum unserer Anschauung aus 3.3.1.9 besitzt die **Rechte-Hand-Orientierung**, in der Daumen, Zeigefinger und Mittelfinger der entspannten rechten Hand als schmutzige angeordnete Basis des Richtungsraums aufgefaßt eine verträgliche angeordnete Basis bilden. Mit der linken Hand erhalten wir in derselben Weise die andere Orientierung, die **Linke-Hand-Orientierung**. Daß diese Orientierungen sich nicht ändern, egal wie wir uns drehen und wenden und auf den Kopf stellen, mag man als Illustration oder Konsequenz unserer Erkenntnis 3.6.5.16 sehen, daß zwei angeordnete Basen eines endlichdimensionalen reellen Vektorraums dieselbe Orientierung liefern genau dann, wenn sie sich „im Raum der Basen stetig ineinander deformieren lassen“.

*Beispiel 3.6.5.9.* Denken wir uns die Tafel ebene als einen schmutzigen zweidimensionalen reellen affinen Raum, so dürfen wir uns eine Orientierung der Tafel ebene anschaulich als die Auszeichnung eines **Drehsinns** denken, nämlich den Drehsinn mit der Eigenschaft, daß bei Drehung in diesem Drehsinn der erste Vektor einer positiv orientierten angeordneten Basis ihres Richtungsraums zuerst in ein positives Vielfaches des zweiten Vektors gedreht wird und erst dann in ein negatives Vielfaches. Wenn, wie etwa bei der Tafel ebene oder bei einem vor uns liegenden Blatt Papier, zusätzlich klar ist, „von welcher Seite man auf die Ebene gucken soll“, so mag man diese beiden Orientierungen als **im Uhrzeigersinn** und **im Gegenuhrzeigersinn** ansprechen. Ist unsere Ebene dahingegen eine Glasscheibe und die Betrachter stehen auf beiden Seiten, so legt man eine Orientierung besser fest, indem man einen Drehsinn als Kreispfeil mit einem Wachsstift einzeichnet.

*Vorschau 3.6.5.10.* In ?? werden wir einen Drehsinn formal definieren als die „Auswahl eines Erzeugers der Fundamentalgruppe vom Komplement des Ursprungs“.



Angeordnete Basen des Raums der Richtungsvektoren der Papierebene mit den Vorzeichen, die der Orientierung „im Gegenuhrzeigersinn“ entsprechen

Man kann dann trefflich darüber streiten, wie natürlich die hier skizzierte Identifikation zwischen Drehsinn und Orientierung ist und ob nicht die entgegengesetzte Identifikation genauso natürlich wäre, aber alles zu seiner Zeit.

**Definition 3.6.5.11.** Wir fixieren von nun an ein für allemal einen eindimensionalen orientierten reellen affinen Raum

$$\mathbb{T}$$

und nennen ihn die **mathematische Zeit** oder kurz **Zeit**.

3.6.5.12 (**Die schmutzige Anschauung**). Ich denke mir  $\mathbb{T}$  als die Menge aller Zeitpunkte und denke mir die ausgezeichnete Orientierung in der Weise, daß jeder Richtungsvektor, der einen Zeitpunkt auf einen „späteren“ Zeitpunkt schiebt, eine positiv orientierte Basis bildet. Das mag aber jeder halten wie er will, Sie dürfen etwa bei den Elementen von  $\mathbb{T}$  etwa auch an unendlich viele verschiedene Gemüse denken, oder an was auch immer. Den Richtungsraum  $\vec{\mathbb{T}}$  bezeichnen wir als den Raum aller **Zeitspannen**, seine positiv orientierten Vektoren nennen wir **Zeiteinheiten**. Sie modellieren die Zeiteinheiten der Physik wie etwa die **Sekunde**  $s \in \vec{\mathbb{T}}$ .

3.6.5.13 (**Herkunft der Zeiteinheiten**). Die Einteilung eines Tages in vierundzwanzig Stunden und die Einteilung dieser Stunden in je sechzig Minuten geht wohl auf die Babylonier zurück, die angeblich mit ihren Händen bis 60 zählten, indem sie mit jedem der 5 Finger der rechten Hand der Reihe nach die 12 Fingerglieder der linken Hand an den Fingern mit Ausnahme des Daumens berührten. Die Einteilung jeder Minute in wiederum 60 Sekunden bot sich dann als natürliche Verfeinerung an.

3.6.5.14 (**Orientierung des Dualraums**). Jede Orientierung auf einem Vektorraum induziert eine Orientierung auf seinem Dualraum mittels der Vorschrift, daß die Duale einer orientierten angeordneten Basis eine orientierte angeordnete Basis des Dualraums sein soll. Die Elemente des positiven Teils  $\vec{\mathbb{T}}_{>0}^\top$  des Dualraums des Raums  $\vec{\mathbb{T}}$  der Zeitspannen nennt man **Frequenzen**. Eine solche Frequenz ist etwa der einzige Vektor  $s^\top$  der dualen Basis zur orientierten Basis der Sekunde  $s \in \vec{\mathbb{T}}$ . Statt  $s^\top$  schreibt man meist  $s^{-1}$  oder Hz und nennt diese Frequenz ein **Hertz** nach dem Physiker Heinrich Rudolf Hertz.

*Ergänzung 3.6.5.15.* Die hier getroffene Wahl für die Orientierung des Dualraums ist im Fall höherer Dimension nicht vollständig kanonisch, aber ich sehe keine andere Möglichkeit, als sich auf eine Wahl festzulegen. Es ist jedoch wichtig, diese Wahl passend zu gewissen weiteren ebenso unkanonischen Wahlen im Zusammenhang mit den sogenannten „äußeren Potenzen“ zu treffen, die Sie später kennen lernen werden. Wir diskutieren das in 4.6.5.18 noch ausführlich. Unsere

Wahl wird im eindimensionalen Fall durch die in 4.6.1.15 für die Orientierung von Tensorpotenzen orientierter eindimensionaler Räume getroffenen Wahlen verallgemeinert.

*Vorschau 3.6.5.16 (Orientierung und Stetigkeit).* Zwei angeordnete Basen eines endlichdimensionalen reellen Vektorraums liefern dieselbe Orientierung genau dann, wenn sie sich „stetig ineinander deformieren lassen“ alias in derselben „Wegzusammenhangskomponente“ im Sinne von ?? des Raums aller angeordneten Basen liegen. Man kann sich davon etwa mithilfe der Iwasawa-Zerlegung 4.1.11.9 überzeugen. Auch die präzise Formulierung und der formale Beweis wird Ihnen davon ausgehend leicht gelingen, sobald Sie in der Analysis die Grundtatsachen über Stetigkeit in mehreren Veränderlichen kennengelernt haben. Eine äquivalente Aussage dürfen Sie in der Analysis als Übung ?? zeigen. Der in meinen Augen natürlichste Zugang zu diesem Resultat verwendet Methoden der Topologie und wird in ?? diskutiert.

**3.6.5.17 (Zusammengesetzte Orientierung).** Sei  $f : V \twoheadrightarrow W$  eine surjektive lineare Abbildung endlichdimensionaler Vektorräume über einem angeordneten Körper und sei  $U := \ker f \subset V$  ihr Kern. So gibt es genau eine Abbildung  $\text{or}(U) \times \text{or}(W) \rightarrow \text{or}(V)$ ,  $(\varepsilon, \eta) \mapsto \varepsilon\eta$  mit der Eigenschaft, daß gegeben eine angeordnete Basis  $\mathcal{A}$  des Kerns  $U$  und eine angeordnete Basis  $\mathcal{B}$  des Bildes  $W$  und eine Wahl  $\tilde{\mathcal{B}}$  von Urbildern letzterer Basisvektoren in  $V$  für die durch Hintereinanderschreiben erhaltene angeordnete Basis  $(\mathcal{A}, \tilde{\mathcal{B}})$  von  $V$  gilt

$$(\varepsilon\eta)(\mathcal{A}, \tilde{\mathcal{B}}) = \varepsilon(\mathcal{A})\eta(\mathcal{B})$$

Diese 2-Multiabbildung alias „Funktion in zwei Variablen“ ist **antikonstant** in dem Sinne, daß sich der Wert ändert, wann immer wir einen Eintrag in einem der beiden Faktoren ihres Definitionsbereichs ändern. Wir nennen Orientierungen  $\varepsilon, \eta, \theta$  auf  $U, W, V$  **verträglich**, wenn gilt  $\varepsilon\eta = \theta$ , und nennen  $\theta$  die **zusammengesetzte Orientierung**. Wenn wir hier von unseren drei Orientierungen beliebige Zwei festlegen, gibt es mithin stets genau eine Möglichkeit, die Dritte verträglich zu wählen. Die so durch Orientierungen auf  $U$  und  $V$  festgelegte Orientierung auf  $W$  nennen wir die **Quotientenorientierung**. Gegeben Orientierungen auf zwei endlichdimensionalen Vektorräumen  $U, W$  erhalten wir auch auf  $U \oplus W$  eine Orientierung als die zusammengesetzte Orientierung für die offensichtliche kurze exakte Sequenz  $U \hookrightarrow U \oplus W \twoheadrightarrow W$ . Wir nennen sie die **Produktorientierung**.

*Beispiel 3.6.5.18 (Orientierungsverträglichkeiten im Anschauungsraum).* Wir denken uns im schmutzigen Raum der Anschauung von einer schmutzigen Tafel und betrachten die orthogonale Projektion des Raums auf unsere Tafel. Der Kern ihres linearen Anteils ist der eindimensionale Raum aller Richtungsvektoren, die auf der Tafel senkrecht stehen. Geben wir ihm die **Nach-vorne-Orientierung**,

in der die uns entgegenkommenden Richtungsvektoren positiv sind, so sind diese Nach-vorne-Orientierung, die Rechte-Hand-Orientierung des Raums und die Gegenuhrzeigersinn-Orientierung der Tafeloberfläche verträglich im Sinne von 3.6.5.17.

*Vorschau* 3.6.5.19. In ?? vereinbaren wir auch eine Konvention für die „Schnittorientierung“ auf dem Schnitt eines angeordneten Paares zweier orientierter Teilräume eines orientierten Raums unter der Voraussetzung, daß die Summe unserer Teilräume der ganze Raum ist.

3.6.5.20. Unsere Definition der zusammengesetzten Orientierung ist in der Weise willkürlich, als es nicht mehr und nicht weniger natürlich gewesen wäre, die Abbildung  $\text{or}(W) \times \text{or}(U) \rightarrow \text{or}(V)$ ,  $(\eta, \varepsilon) \mapsto \eta\varepsilon$  zu betrachten mit der Eigenschaft  $(\eta\varepsilon)(\mathcal{B}, \mathcal{A}) = \eta(\mathcal{B})\varepsilon(\mathcal{A})$  und sie zu benutzen, um die Verträglichkeit zu definieren. Ich sehe an dieser Stelle keine andere Möglichkeit, als einmal willkürlich eine Wahl zu treffen. Unsere Wahl mag man salopp „Kern vorne“ nennen. Es ist jedoch wichtig, diese Wahl passend zu gewissen ebenso unkanonischen Wahlen im Zusammenhang mit den sogenannten „äußereren Potenzen“ zu treffen, die Sie später kennen lernen werden. Das wird in 4.6.5.18 diskutiert.

## Übungen

*Übung* 3.6.5.21 (**Orientierung affiner Räume durch Erzeugendensysteme**). Gegeben ein endlichdimensionaler affiner Raum  $E$  über einem angeordneten Körper und ein minimales affines Erzeugendensystem  $p_1, \dots, p_n$  von  $E$  vereinbaren wir, daß wir unter der **zu**  $p_1, \dots, p_n$  **gehörigen Orientierung von**  $E$  die durch die angeordnete Basis  $p_2 - p_1, \dots, p_n - p_1$  des Richtungsraums gegebene Orientierung verstehen wollen. Man zeige, daß sich für jede Permutation  $\sigma \in \mathcal{S}_n$  die zu  $p_{\sigma(1)}, \dots, p_{\sigma(n)}$  gehörigen Orientierung von  $E$  nur um das Vorzeichen  $\text{sgn}(\sigma)$  von der zu  $p_1, \dots, p_n$  gehörigen Orientierung unterscheidet.

## 3.6.6 Eigenwerte und Eigenvektoren

**Definition 3.6.6.1.** Sei  $f : V \rightarrow V$  ein Endomorphismus eines Vektorraums über einem Körper  $K$ . Ein Skalar  $\lambda \in K$  heißt ein **Eigenwert von**  $f$ , wenn es einen von Null verschiedenen Vektor  $v \neq 0$  aus  $V$  gibt mit

$$f(v) = \lambda v$$

Jeder derartige von Null verschiedene Vektor heißt ein **Eigenvektor von**  $f$  **zum Eigenwert**  $\lambda$ . Die Menge aller Eigenvektoren zum Eigenwert  $\lambda$  bildet zusammen mit dem Nullvektor einen Untervektorraum von  $V$ , den **Eigenraum**  $\text{Eig}(f; \lambda)$  **von**  $f$  **zum Eigenwert**  $\lambda$ .

**Beispiel 3.6.6.2 (Eigenvektoren zu den Eigenwerten Null und Eins).** Ein Eigenvektor zum Eigenwert Eins einer linearen Abbildung ist dasselbe wie ein vom Nullvektor verschiedener Fixvektor unserer Abbildung. Ein Eigenvektor zum Eigenwert Null einer linearen Abbildung ist dasselbe wie ein vom Nullvektor verschiedenes Element des Kerns unserer Abbildung.

**Beispiel 3.6.6.3 (Die schmutzige Anschauung).** Zunächst zwei nicht ganz mathematisch ausformulierte Beispiele: Die Drehung des Richtungsraums der Papierebene um den rechten Winkel im Uhrzeigersinn besitzt keinen reellen Eigenwert. Eine Spiegelung des Richtungsraums der Papierebene an einer Geraden besitzt stets Eigenvektoren zum Eigenwert Eins, nämlich alle Richtungsvektoren der Spiegelachse, und Eigenvektoren zum Eigenwert  $(-1)$ , die der Leser selbst finden mag. Für das Ableiten, aufgefaßt als Endomorphismus des Raums aller reellen polynomiauen Funktionen, ist der einzige Eigenwert die Null und die zugehörigen Eigenvektoren sind genau die von Null verschiedenen konstanten Polynome.

**Satz 3.6.6.4 (Existenz von Eigenwerten).** *Jeder Endomorphismus eines von Null verschiedenen endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper besitzt einen Eigenwert.*

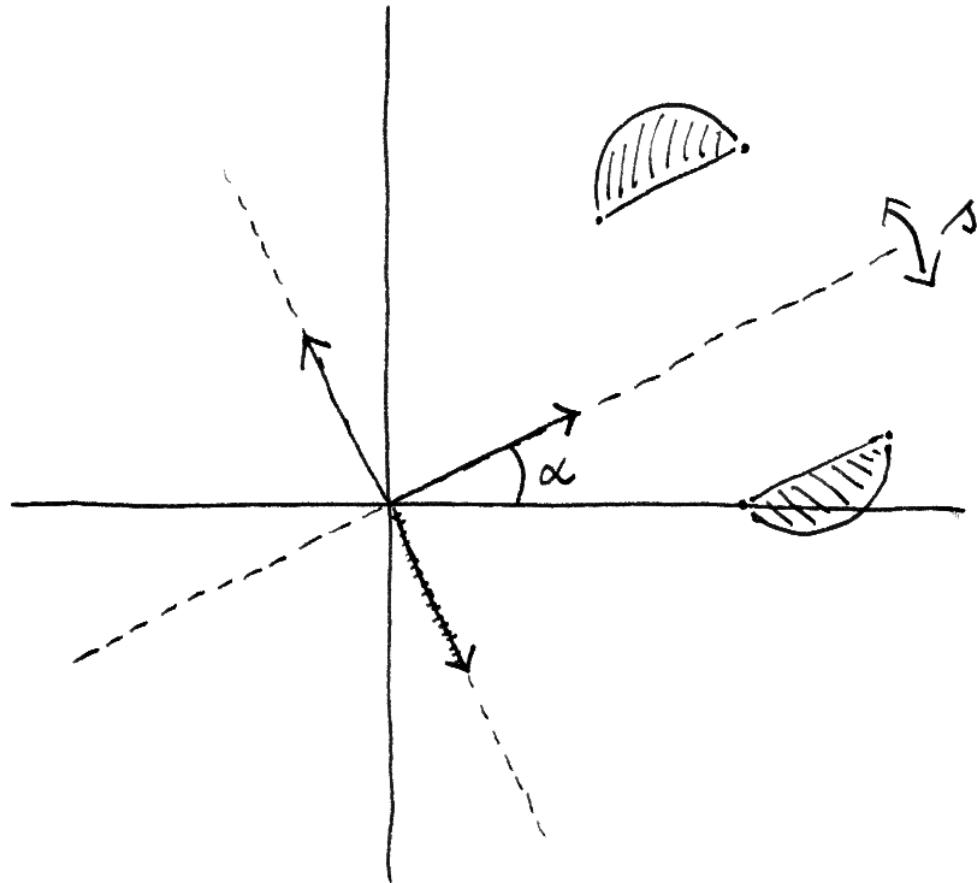
3.6.6.5. Auf dem  $\mathbb{C}$ -Vektorraum  $\mathbb{C}[T]$  der Polynome besitzt der Endomorphismus „Multipliziere mit  $T$ “ keine Eigenwerte. Die Annahme endlicher Dimension ist also wesentlich für die Gültigkeit unseres Satzes. Die Drehung des Richtungsraums der Papierebene um einen von  $0^\circ$  und  $180^\circ$  verschiedenen Winkel – hier noch nicht formal eingeführt aber doch wohl anschaulich klar gesagt – besitzt auch keinen reellen Eigenwert. Die Annahme eines algebraisch abgeschlossenen Grundkörpers ist also auch wesentlich. Für den Beweis entwickeln wir zunächst unsere Theorie etwas weiter und geben dann den Beweis im Anschluß an 3.6.6.9.

**Definition 3.6.6.6.** Seien  $K$  ein Körper und  $A \in \text{Mat}(n; K)$  eine quadratische Matrix mit Koeffizienten in  $K$ . Bezeichne  $I \in \text{Mat}(n; K)$  die Einheitsmatrix. Das Polynom  $\det(A - TI)$  aus dem Polynomring  $K[T]$  heißt das **charakteristische Polynom der Matrix**  $A$ . Es wird mit einem griechischen  $\chi$  notiert in der Form

$$\chi_A(T) := \det(A - TI)$$

**Satz 3.6.6.7 (Eigenwerte und charakteristisches Polynom).** *Seien  $K$  ein Körper und  $A \in \text{Mat}(n; K)$  eine quadratische Matrix mit Koeffizienten in  $K$ . So sind die Eigenwerte des durch unsere Matrix gegebenen Homomorphismus  $A : K^n \rightarrow K^n$  genau die Nullstellen ihres charakteristischen Polynoms  $\chi_A$ .*

*Beweis.* Bezeichnet  $I \in \text{Mat}(n; K)$  die Einheitsmatrix, so haben wir für  $\lambda \in K$



Die anschauliche Spiegelung  $s$  an der gestrichelt eingezeichneten Achse ist eine lineare Abbildung  $s : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  mit den Eigenwerten  $\pm 1$ . Eigenvektoren zum Eigenwert  $1$  sind alle von Null verschiedenen Vektoren der Spiegelachse, Eigenvektoren zum Eigenwert  $-1$  sind alle von Null verschiedenen Vektoren, die auf der Spiegelachse senkrecht stehen. Die Matrix unserer Abbildung in Standardbasis ist nach dem Bild bei 3.2.6.4 die Matrix

$$A = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

mit charakteristischem Polynom  
 $\chi_A(T) = (T - \cos 2\alpha)(T + \cos 2\alpha) - \sin^2 2\alpha = T^2 - 1.$

die Äquivalenzen

$$\begin{aligned}
 (\lambda \text{ ist Eigenwert von } A) &\Leftrightarrow \exists v \neq 0 \text{ mit } Av = \lambda v \\
 &\Leftrightarrow \exists v \neq 0 \text{ mit } (A - \lambda I)v = 0 \\
 &\Leftrightarrow \ker(A - \lambda I) \neq 0 \\
 &\Leftrightarrow \det(A - \lambda I) = 0 \\
 &\Leftrightarrow \chi_A(\lambda) = 0
 \end{aligned} \quad \square$$

3.6.6.8. Es ist üblich, bei charakteristischen Polynomen die Variable mit  $\lambda$  zu bezeichnen. Ich werde dieser Konvention von hier an meist folgen.

3.6.6.9. Sei  $K$  ein Körper und  $f : V \rightarrow V$  ein Endomorphismus eines endlichdimensionalen  $K$ -Vektorraums. Mit demselben Argument wie in 3.6.4.3 sehen wir, daß bezüglich jeder angeordneten Basis von  $V$  die darstellende Matrix von  $f$  dasselbe charakteristische Polynom hat, in Formeln  $\det(\mathcal{B}[f]_{\mathcal{B}} - \lambda \text{id}) = \det(\mathcal{A}[f]_{\mathcal{A}} - \lambda \text{id})$  für je zwei angeordnete Basen  $\mathcal{A}$  und  $\mathcal{B}$  von  $V$ . Dies Polynom notieren wir dann

$$\chi_f = \chi_f(\lambda) = \text{char}(f|V)$$

und nennen es das **charakteristische Polynom des Endomorphismus  $f$** . Die Eigenwerte von  $f$  sind nach 3.6.6.6 genau die Nullstellen des charakteristischen Polynoms  $\chi_f$  von  $f$ .

*Beweis von Satz 3.6.6.4.* Satz 3.6.6.4 besagt, daß jeder Endomorphismus eines endlichdimensionalen von Null verschiedenen Vektorraums über einem algebraisch abgeschlossenen Körper einen Eigenwert besitzt. Um das zu zeigen, müssen wir nur bemerken, daß das charakteristische Polynom unseres Endomorphismus nicht konstant ist, da unser Raum nämlich nach Annahme nicht der Nullraum ist. Im Fall eines algebraisch abgeschlossenen Körpers besitzt es also stets eine Nullstelle, und die ist dann nach 3.6.6.9 auch bereits der gesuchte Eigenwert.  $\square$

3.6.6.10. Das charakteristische Polynom einer Block-oberen-Dreiecksmatrix ist nach 3.6.2.9 das Produkt der charakteristischen Polynome ihrer Blöcke auf der Diagonalen.

**Proposition 3.6.6.11 (Trigonaisierbarkeit).** *Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums  $f : V \rightarrow V$  über einem Körper  $K$  sind gleichbedeutend:*

1. *Der Vektorraum  $V$  besitzt eine angeordnete Basis  $\mathcal{B}$ , bezüglich derer die Matrix  $\mathcal{B}[f]_{\mathcal{B}}$  von  $f$  obere Dreiecksgestalt hat. Man sagt dann auch,  $f$  sei **trigonaisierbar**;*
2. *Das charakteristische Polynom  $\chi_f$  von  $f$  zerfällt bereits im Polynomring  $K[\lambda]$  vollständig in Linearfaktoren.*

*Beweis.*  $1 \Rightarrow 2$  ist klar nach unserer Formel 3.6.2.4 für die Determinante einer oberen Dreiecksmatrix: Hat  ${}_{\mathcal{B}}[f]_{\mathcal{B}}$  obere Dreiecksgestalt mit Diagonaleinträgen  $\lambda_1, \dots, \lambda_n$ , so haben wir ja  $\chi_f(\lambda) = (\lambda_1 - \lambda) \dots (\lambda_n - \lambda)$ . Um  $2 \Rightarrow 1$  zu zeigen, dürfen wir ohne Beschränkung der Allgemeinheit  $V = K^n$  annehmen, so daß  $f$  durch die Multiplikation mit einer Matrix  $A$  gegeben ist. Zu zeigen ist dann die Existenz von  $B \in \mathrm{GL}(n; K)$  mit  $B^{-1}AB = D$  von oberer Dreiecksgestalt: Die Spaltenvektoren der Matrix  $B$  bilden dann nämlich die gesuchte Basis  $\mathcal{B}$ . Wir argumentieren mit vollständiger Induktion über  $n$ . Für  $n \geq 1$  gibt es nach Voraussetzung eine Nullstelle  $\lambda_1$  von  $\chi_A$  und dann nach 3.6.6.7 ein  $c_1 \in K^n \setminus 0$  mit  $Ac_1 = \lambda_1 c_1$ . Ergänzen wir  $c_1$  durch  $c_2, \dots, c_n$  zu einer Basis von  $K^n$  und betrachten die Matrix  $C = (c_1 | \dots | c_n)$ , so gilt

$$AC = C \left( \begin{array}{c|c} \lambda_1 & * \\ \hline 0 & H \end{array} \right)$$

mit  $H \in \mathrm{Mat}((n-1) \times (n-1); K)$ . Nach unseren Erkenntnissen 3.6.2.9 zur Determinante von Block-oberen-Dreiecksmatrizen haben wir dann  $\chi_H = (\lambda_2 - \lambda) \dots (\lambda_n - \lambda)$  und per Induktion finden wir  $F \in \mathrm{GL}(n-1; K)$  mit  $F^{-1}HF$  von oberer Dreiecksgestalt. Bilden wir nun  $\tilde{F} = \mathrm{diag}(1, F)$ , so ist offensichtlich auch  $\tilde{F}^{-1}(C^{-1}AC)\tilde{F}$  von oberer Dreiecksgestalt und die Matrix  $B = C\tilde{F}$  löst unser Problem.  $\square$

**Proposition 3.6.6.12 (Charakterisierung nilpotenter Matrizen).** *Eine Matrix mit Koeffizienten in einem Körper ist nilpotent genau dann, wenn ihr charakteristisches Polynom nur aus dem Leitterm besteht. In Formeln ist also  $A \in \mathrm{Mat}(n; K)$  nilpotent genau dann, wenn gilt  $\chi_A(\lambda) = (-\lambda)^n$ .*

*Beweis.* Ist unsere Matrix nilpotent, so ist sie nach 3.2.6.15 konjugiert zu einer oberen Dreiecksmatrix mit Nullen auf der Diagonalen und unsere Behauptung folgt aus 3.6.6.10. Besteht umgekehrt das charakteristische Polynom nur aus dem Leitterm, so existiert nach 3.6.6.11 oder zumindest seinem Beweis eine invertierbare Matrix  $B \in \mathrm{GL}(n; K)$  mit  $B^{-1}AB$  von oberer Dreiecksgestalt mit Nullen auf der Diagonale. Daraus folgt jedoch unmittelbar erst  $(B^{-1}AB)^n = 0$  und dann  $A^n = 0$ .  $\square$

*Ergänzung 3.6.6.13.* Alternative Argumente für die Rückrichtung beim Beweis der Proposition liefern der Satz von Cayley-Hamilton 3.6.6.20 und der Satz über die Hauptraumzerlegung 4.3.2.13.

**Definition 3.6.6.14.** Seien  $K$  ein Körper und  $n \in \mathbb{N}$ . Eine quadratische Matrix  $A \in \mathrm{Mat}(n; K)$  heißt **diagonalisierbar**, wenn es eine invertierbare Matrix  $S \in \mathrm{GL}(n; K)$  gibt mit  $S^{-1}AS = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$  diagonal.

**Definition 3.6.6.15.** Ein Endomorphismus eines Vektorraums heißt **diagonalisierbar**, wenn unser Vektorraum von den Eigenvektoren des besagten Endomorphismus erzeugt wird. Im Fall eines endlichdimensionalen Vektorraums ist das gleichbedeutend dazu, daß unser Vektorraum  $V$  eine angeordnete Basis  $\mathcal{B} = (v_1, \dots, v_n)$  besitzt, für die die Matrix unserer Abbildung Diagonalgestalt hat, in Formeln  ${}_{\mathcal{B}}[f]_{\mathcal{B}} = \text{diag}(\lambda_1, \dots, \lambda_n)$ . In der Tat bedeutet das ja gerade  $f(v_i) = \lambda_i v_i$ .

**3.6.6.16 (Diagonalisierbare Endomorphismen und ihre Matrizen).** Sei  $K$  ein Körper und  $n \in \mathbb{N}$ . Der durch Multiplikation mit einer Matrix  $A \in \text{Mat}(n; K)$  gegebene Endomorphismus des  $K^n$  ist genau dann diagonalisierbar, wenn die Matrix  $A$  diagonalisierbar ist. In der Tat, genau dann ist  $v_1, \dots, v_n$  eine Basis des  $K^n$  aus Eigenvektoren  $Av_i = \lambda_i v_i$ , wenn die Matrix  $S = (v_1 | \dots | v_n)$  mit den  $v_i$  in den Spalten invertierbar ist mit  $S^{-1}AS = \text{diag}(\lambda_1, \dots, \lambda_n)$  diagonal.

**Beispiel 3.6.6.17.** Eine nilpotente Matrix ist genau dann diagonalisierbar, wenn sie die Nullmatrix ist. Die folgende Proposition zeigt unter anderem, daß jede  $(n \times n)$ -Matrix, deren charakteristisches Polynom  $n$  paarweise verschiedene Nullstellen hat, diagonalisierbar sein muß. Salopp gesprochen sind also „komplexe quadratische Matrizen für gewöhnlich diagonalisierbar“.

**Proposition 3.6.6.18 (Lineare Unabhängigkeit von Eigenvektoren).** Sei  $f$  ein Endomorphismus eines Vektorraums und seien  $v_1, \dots, v_n$  Eigenvektoren von  $f$  zu paarweise verschiedenen Eigenwerten  $\lambda_1, \dots, \lambda_n$ . So sind unsere Eigenvektoren linear unabhängig.

*Beweis.* Der Endomorphismus  $(f - \lambda_1 \text{id}) \dots (f - \lambda_n \text{id})$  macht  $v_2, \dots, v_n$  zu Null, nicht aber  $v_1$ . Gegeben  $x_1, \dots, x_n \in K$  mit  $x_1 v_1 + \dots + x_n v_n = 0$  folgt demnach durch Anwenden unseres Endomorphismus  $x_1 = 0$ . Ebenso zeigt man  $x_2 = \dots = x_n = 0$ .  $\square$

*Variante des Beweises.* Durch Widerspruch. Sei sonst  $v_1, v_2, \dots, v_n$  ein Gegenbeispiel mit der kleinstmöglichen Anzahl von Vektoren. So gilt sicher  $n \geq 2$  und gegeben eine lineare Abhängigkeit  $x_1 v_1 + \dots + x_n v_n = 0$  müssen alle  $x_i$  verschieden von Null sein. Dann aber folgte durch Anwenden von  $(f - \lambda_1 \text{id})$  die lineare Abhängigkeit der Vektoren  $v_2, \dots, v_n$  im Widerspruch zu unserer Annahme.  $\square$

**Lemma 3.6.6.19 (Restriktion diagonalisierbarer Endomorphismen).** Die Restriktion eines diagonalisierbaren Endomorphismus auf einen unter besagtem Endomorphismus stabilen Teilraum ist stets wieder diagonalisierbar.

*Beweis.* Sei  $f : V \rightarrow V$  unser Endomorphismus und  $W \subset V$  ein unter  $f$  stabiler Teilraum. Gegeben  $v \in W$  haben wir nach Annahme eine Darstellung

$v = v_1 + \dots + v_n$  mit  $v_i \in V$  Eigenvektoren zu paarweise verschiedenen Eigenwerten  $\lambda_1, \dots, \lambda_n \in K$ . Dann gilt wegen  $(f - \lambda_i \text{id})v_i = 0$  aber

$$(f - \lambda_2 \text{id}) \dots (f - \lambda_n \text{id})v = (\lambda_1 - \lambda_2) \dots (\lambda_1 - \lambda_n)v_1 \in W$$

und folglich  $v_1 \in W$ . Ebenso zeigt man auch  $v_2, \dots, v_n \in W$ . Mithin wird auch  $W$  von Eigenvektoren erzeugt.  $\square$

**Satz 3.6.6.20 (Cayley-Hamilton).** *Setzt man eine quadratische Matrix in ihr eigenes charakteristisches Polynom ein, so erhält man die Nullmatrix.*

3.6.6.21. Ich gebe zwei Beweise. Der Erste baut auf der algebraischen Abgeschlossenheit des Körpers der komplexen Zahlen auf und damit auf noch unbewiesenen Tatsachen. Der Zweite ist in gewisser Weise elementarer, scheint mir aber wenig transparent. Ein alternativer Beweis, der in meinen Augen mehr Einsicht vermittelt, wird in ?? angedeutet.

*Beweis mit dem Fundamentalsatz der Algebra.* Wir beginnen mit dem Fall einer komplexen Matrix  $E$ . Nach 3.6.6.11 ist sie trigonalisierbar. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß sie bereits obere Dreiecksgestalt hat. Sind dann  $\lambda_1, \dots, \lambda_n$  ihre Diagonaleinträge und betrachten wir die von den ersten  $k$  Vektoren der Standardbasis aufgespannten Untervektorräume  $\mathbb{C}^k \times 0 \subset \mathbb{C}^n$ , so gilt  $(E - \lambda_k)(\mathbb{C}^k \times 0) \subset \mathbb{C}^{k-1} \times 0$  für alle  $k$ . Damit ist klar, daß das Produkt aller  $(E - \lambda_k)$  alias  $\chi_E(E)$  den ganzen Vektorraum  $\mathbb{C}^n$  annulliert. Jetzt betrachten wir den Fall der Matrix  $E$  über dem Polynomring  $\mathbb{Z}[X_{ij}]$  in  $n^2$  Variablen mit Einträgen den Variablen, in Formeln  $E_{ij} = X_{ij}$ . Setzen wir diese Matrix in ihr eigenes charakteristisches Polynom ein, so erhalten wir ein Polynom aus  $\mathbb{Z}[X_{ij}]$ , das nach dem vorhergehenden die Nullfunktion auf  $\mathbb{C}^{n^2}$  liefert. Nach 3.5.4.3 ist es also schon selbst das Nullpolynom und der Satz folgt.  $\square$

*Beweis ohne den Fundamentalsatz der Algebra.* Gegeben eine quadratische Matrix  $A$  mit Koeffizienten in einem Kring gibt es nach 3.6.4.6 eine weitere Matrix  $A^\sharp$  mit Koeffizienten in demselben Kring derart, daß im Ring der quadratischen Matrizen mit Einträgen in unserem Kring gilt

$$A^\sharp A = (\det A) \cdot I$$

für  $I$  die Einheitsmatrix. Nehmen wir speziell den Kring  $K[t]$  und die Matrix  $A = F - tI$  für eine vorgegebene Matrix  $F \in \text{Mat}(n; K)$ , so erhalten wir in  $\text{Mat}(n; K[t])$  die Gleichung

$$A^\sharp(F - tI) = \chi_F(t) \cdot I$$

$$\left( \begin{array}{|ccc|c|} \hline & 1 & 2 & 3 \\ \hline 1 & & 1 & 2 & 2 \\ & 1 & & 2 & 3 \\ \hline 0 & 0 & 5 & 4 & 4 \\ 0 & 0 & 5 & 4 & 4 \\ \hline 0 & 0 & 5 & 4 & 4 \\ 7 & 7 & 8 & 6 & 6 \\ 7 & 7 & 8 & 6 & 6 \\ \hline \end{array} \right) - \left( \begin{array}{|ccc|c|} \hline & 1 & 0 & 7 \\ \hline 2 & 2 & 5 & 8 \\ & 3 & 4 & 6 \\ \hline 1 & 1 & 0 & 7 \\ 2 & 2 & 5 & 8 \\ 3 & 3 & 4 & 6 \\ \hline 1 & 1 & 0 & 7 \\ 2 & 2 & 5 & 8 \\ 3 & 3 & 4 & 6 \\ \hline \end{array} \right) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$(F - fE)(e_1^\top, \dots, e_n^\top)^\top = 0$  am Beispiel einer Matrix  $F$  mit drei Zeilen und Spalten. Alle nicht ausgeschriebenen Einträge der obigen Matrizen sind als Null zu verstehen.

Bezeichne nun  $f : K^n \rightarrow K^n$  die durch Multiplikation von Spaltenvektoren mit der zu  $F$  transponierten Matrix  $F^\top$  gegebene lineare Abbildung. Wenden wir auf beide Seiten unserer Gleichung von Matrizen den Ringhomomorphismus  $K[t] \rightarrow \text{End}_K K^n$  mit  $t \mapsto f$  an, so erhalten wir in  $\text{Mat}(n; \text{End}_K K^n)$  alias  $\text{Mat}(n^2; K)$  die Gleichung

$$A^\sharp(F - f\mathbf{I}) = \chi_F(f) \cdot \mathbf{I}$$

Betrachten wir nun die Standardbasis  $e_1, \dots, e_n$  aus Spaltenvektoren des  $K^n$  und wenden beide Seiten dieser Gleichung an auf den Vektor  $(e_1^\top, \dots, e_n^\top)^\top$ , aufgefaßt als Spaltenvektor in  $K^{n^2}$ , so ergibt auf der linken Seite schon die Multiplikation mit  $(F - f\mathbf{I})$  den Nullvektor, denn bei

$$(F - f\mathbf{I})(e_1^\top, \dots, e_n^\top)^\top$$

steht im  $i$ -ten Block von  $K^{n^2}$  genau  $F_{i1}e_1 + \dots + F_{in}e_n - f(e_i) = 0$ . Also wird die rechte Seite auch Null und es folgt  $\chi_F(f)e_1 = \dots = \chi_F(f)e_n = 0$ . Hier ist zwar  $\chi_F$  a priori das charakteristische Polynom der zu einer Matrix von  $f$  transponierten Matrix, aber das stimmt nach 3.6.2.5 mit dem charakteristischen Polynom von  $f$  überein.  $\square$

**Proposition\* 3.6.6.22.** *Seien  $f$  ein Endomorphismus eines Vektorraums  $V$  über einem Körper  $K$  und  $P \in K[X]$  ein normiertes Polynom ohne mehrfache Nullstellen, das in  $K$  vollständig in Linearfaktoren zerfällt und  $f$  annulliert, in Formeln  $P(f) = 0$ . So ist  $f$  diagonalisierbar und seine Eigenwerte sind Nullstellen von  $P$ .*

*Beweis.* Man wähle einen festen Vektor  $v \in V$  und suche dazu einen normierten Teiler  $Q = (X - \lambda_1)\dots(X - \lambda_r)$  von  $P$  kleinstmöglichen Grades  $r$  mit  $Q(f) : v \mapsto 0$ . Dann ist  $E := \langle v, f(v), f^2(v), \dots, f^{r-1}(v) \rangle$  ein unter  $f$  stabiler Untervektorraum von  $V$ . Andererseits ist  $(f - \lambda_2)\dots(f - \lambda_r)v$  nach Annahme nicht Null und folglich ein Eigenvektor von  $f$  zum Eigenwert  $\lambda_1$  in  $E$ . In derselben Weise finden wir auch Eigenvektoren zu den Eigenwerten  $\lambda_2, \dots, \lambda_r$ . Da Eigenvektoren zu paarweise verschiedenen Eigenwerten linear unabhängig sind nach 3.6.6.18, ist damit  $f|_E$  diagonalisierbar und  $v$  eine Summe von Eigenvektoren von  $f$ . Die Proposition folgt.  $\square$

## Übungen

*Übung 3.6.6.23.* Seien  $K$  ein Körper und  $A \in \text{Mat}(n; K)$  eine quadratische Matrix mit Koeffizienten in  $K$ . Man zeige, daß das charakteristische Polynom von  $A$  die Gestalt

$$\chi_A(T) = (-T)^n + \text{tr}(A)(-T)^{n-1} + \dots + \det(A)$$

hat, in Worten also den Leitkoeffizienten  $(-1)^n$ , als nächsten Koeffizienten bis auf ein Vorzeichen die Spur von  $A$ , und als konstanten Term die Determinante von  $A$ .

*Übung 3.6.6.24.* Jeder Endomorphismus eines endlichdimensionalen reellen Vektorraums mit negativer Determinante besitzt einen negativen reellen Eigenwert. Hinweis: Zwischenwertsatz. Man zeige weiter, daß er im zweidimensionalen Fall zusätzlich auch noch einen positiven reellen Eigenwert besitzt.

*Ergänzende Übung 3.6.6.25.* Jeder Endomorphismus eines endlichdimensionalen reellen Vektorraums ungerader Dimension besitzt einen reellen Eigenwert. Ist die Determinante unseres Endomorphismus positiv, so besitzt er sogar einen positiven reellen Eigenwert.

*Ergänzende Übung 3.6.6.26.* Sind  $k \subset K$  Körper und ist  $k$  algebraisch abgeschlossen und gilt  $\dim_k K < \infty$ , so folgt  $K = k$ . Hinweis: Man betrachte für alle  $a \in K$  die durch Multiplikation mit  $a$  gegebene  $k$ -lineare Abbildung  $(a \cdot) : K \rightarrow K$  und deren Eigenwerte.

*Ergänzende Übung 3.6.6.27.* Gegeben ein Endomorphismus eines endlichdimensionalen reellen Vektorraums gibt es stets eine Basis derart, daß die zugehörige Matrix Block-obere Dreiecksgestalt hat mit höchstens Zweierblöcken auf der Diagonalen.

*Übung 3.6.6.28.* Sei ein diagonalisierbarer Endomorphismus eines vierdimensionalen Vektorraums gegeben, dessen Eigenwerte paarweise verschieden sind. Wieviele unter unserem Endomorphismus stabile Untervektorräume besitzt unser Vektorraum?

*Übung 3.6.6.29 (Endomorphismen, deren Quadrat die Identität ist).* Sei  $V$  ein Vektorraum über einem Körper einer von Zwei verschiedenen Charakteristik und  $r : V \rightarrow V$  eine lineare Abbildung mit  $r^2 = \text{id}_V$ . So ist  $r$  diagonalisierbar und alle seine Eigenwerte sind  $\pm 1$ . Fordern wir zusätzlich  $\dim V = 2$  und  $r \neq \text{id}_V$ , so hat  $r$  die Eigenwerte  $1$  und  $(-1)$  und die Determinante  $\det(r) = -1$ . Hinweis:  $v = (v + r(v))/2 + (v - r(v))/2$ .

*Ergänzende Übung 3.6.6.30 (Jordanform für  $(2 \times 2)$ -Matrizen).* Sei  $K$  ein algebraisch abgeschlossener Körper. Man zeige, daß es für jede quadratische Matrix  $A \in \text{Mat}(2; K)$  eine invertierbare Matrix  $P \in \text{GL}(2; K)$  gibt derart, daß  $P^{-1}AP$  eine der beiden Gestalten

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad \text{hat.}$$

*Übung 3.6.6.31.* Gegeben zwei quadratische Matrizen  $A, B$  derselben Größe gilt  $\chi_{AB} = \chi_{BA}$ . Hinweis: Man erinnere beim Beweis der Multiplikativität der Determinante 3.6.4.1 das Argument zur Herleitung des Falls eines beliebigen Krings aus dem Körperfall.

### **3.7 Danksagung**

Für Korrekturen und Verbesserungen danke ich Judith Bender, Anna Staron, Markus Junker, Olaf Schnürer, Bernhard Krötz, Pascal Soergel. Besonders danke ich Veronika Thierfelder, deren fundamentale allgemeine Ratschläge zur Darstellung mir sehr geholfen haben.

## 3.8 Die Vorlesung LA1 im Wintersemester 14/15

Es handelte sich um eine vierstündige Vorlesung, also  $4 \times 45$  Minuten Vorlesung, mit 2 Stunden Übungen. Für die Darstellung der Grundlagen fand keine Abstimmung mit anderen Grundvorlesungen statt.

- 20.10 Fibonacci-Folge und Vektorraumbegriff; Mengen; Keine Diskussion von Binomial-Koeffizienten; Keine Diskussion der vollständigen Induktion.
- 23.10 Abbildungen, Beginn der Diskussion von Verknüpfungen, Beispiele für Verknüpfungen;
- 27.10 Assoziativität macht Klammern überflüssig. Monoide, Gruppen. Körper begonnen. Keine Diskussion von Homomorphismen.
- 30.10 Körper fertig. Lineare Gleichungssysteme, Lösungsmenge, Gauß-Algorithmus; Definition abstrakter Vektorräume, Beispiele; Endliche kartesische Produkte, der Vektorraum der Tupel.
- 3.11 Untervektorräume, Erzeugung, Linearkombinationen, lineare Unabhängigkeit; Basis, Extremalcharakterisierung von Basen, noch ohne Beweis.
- 6.11 Extremalcharakterisierung von Basen, Beweis, dauerte etwa eine Stunde. Dann Hauptabschätzung der linearen Algebra, Korollare, Dimension, Dimensionssatz noch ohne Beweis.
- 10.11 Beweis Dimensionssatz, Steinitz weggelassen, freier Vektorraum über Menge, freier Vektorraum über Basis in Bijektion zu Vektorraum, Zorn für Mengensysteme 3.1.9.18, Basisexistenzsatz mit Variante, Homomorphismen von Magmas, Monoiden, Gruppen, Körpern, Vektorräumen, Beispiele für lineare Abbildungen, Endo, Iso, Auto, isomorphe Vektorräume haben dieselbe Dimension noch ohne Beweis;
- 13.11 Beweis isomorphe Vektorräume haben dieselbe Dimension; Stufenzahl nach Gauß-Algorithmus als Dimension des Lösungsraums. Kern, Bild, Injektiv bedeutet Kern Null. Dimensionsformel, zweiter Beweis des Dimensionssatzes. Komplemente.
- 17.11 Lineare Abbildung festgelegt und festlegbar durch Werte auf Basis. Existenz komplementärer Unterräume, Halbinverser zu linearen Surjektionen und Injektionen. Affine Räume, affine Abbildungen, affine Teilräume.
- 20.11 Schnitt affiner Teilräume, Bezug zu Lösungsmengen linearer Gleichungssysteme. Erzeugen affiner Teilräume, affine Abbildungen im Fall reeller affiner Räume charakterisiert durch Erhaltung von Geraden. Matrizen linearer

Abbildungen  $K^n \rightarrow K^m$ , Produkt von Matrizen, Zusammenhang mit Verknüpfung linearer Abbildungen noch ohne Beweis.

- 24.11 Produkt von Matrizen, Zusammenhang mit Verknüpfung linearer Abbildungen, Rechenregeln für Matrizen, Zusammenhang mit linearen Gleichungssystemen, invertierbare Matrizen, Elementarmatrizen, Darstellung jeder Matrix als Produkt von solchen noch ohne Beweis.
- 27.11 Darstellung jeder Matrix als Produkt von Elementarmatrizen mit Beweis, Smith-Normalform, Rang einer Matrix, Zeilenrang ist Spaltenrang, Berechnung der inversen Matrix. Matrizen beliebiger linearer Abbildungen in Bezug auf Basen, Basiswechsel. Nicht Spur, das soll in die Übungen. Noch nicht: Notation für Darstellung eines Vektors in Basis.
- 1.12 Anwenden einer linearen Abbildung auf Darstellung eines Vektors in entsprechender Basis. Alternativer Beweis für die Smith-Normalform. Dualraum, transponierte Abbildung und duale Basis. Matrix der transponierten Abbildung noch ohne Beweis.
- 4.12 Matrix der transponierten Abbildung: Beweis. Bidualraum und bitransponierte Abbildung. Kovektoren als Zeilenmatrizen. Realisierung der komplexen Zahlen als Drehstreckungen; Konjugation, Inverse, geometrische Interpretation des Quadrierens.
- 8.12 Äquivalenzrelationen. Primzahlen, Eindeutigkeit der Primfaktorzerlegung noch ohne Beweis. Auch Satz über den größten gemeinsamen Teiler noch ohne Beweis.
- 11.12 Eindeutigkeit der Primfaktorzerlegung mit Beweis. Satz über den größten gemeinsamen Teiler mit Beweis. Euklidischer Algorithmus. Restklassenringe. Ringhomomorphismen. Quersummenkriterien.
- 15.12 Integritätsbereiche. Kürzen, Einheiten. Primkörper. Verschlüsselung. Polynomringe, Einsetzen, Wurzeln, Grad. Grad Schranke für Zahl der Wurzeln ohne Beweis. Teilen mit Rest ohne Beweis.
- 18.12 Teilen mit Rest für Polynome. Grad Schranke für Zahl der Wurzeln mit Beweis. Polynome als Funktionen, über endlichen und unendlichen Körpern. Algebraisch abgeschlossene Körper, Faktorisierung im Komplexen und im Reellen, anschauliche Begründung für den Fundamentalsatz der Algebra. Quotientenkörper, rationale Funktionen, Partialbruchzerlegung.
- 22.12 Projektive Räume, Hamilton'sche Zahlen, Inzidenzgeometrie, Pappus-Eigenschaft und Koordinatisierbarkeit.

- 8.1 Signum einer Permutation, Leibnizformel, Charakterisierung der Determinante, noch ohne Beweis der Einzigkeit.
- 12.1 Beweis der Einzigkeit. Determinantenmultiplikationssatz, Invertierbarkeitskriterium, Laplace'scher Entwicklungssatz, Cramer'sche Regel, Invertierbarkeitskriterium über kommutativen Ringen.
- 15.1 Orientierung endlichdimensionaler Räume über angeordneten Körpern. Begründung der Evaluation der Vorlesung. Eigenwerte, Eigenvektoren, charakteristisches Polynom von quadratischer Matrix und Endomorphismus, Nullstellen des charakteristischen Polynoms und Eigenwerte. Trigonalisierbarkeit gleichbedeutend zur Zerfällung des charakteristischen Polynoms formuliert, nur einfache Richtung gezeigt.
- 19.1 Trigonalisierbarkeit gleichbedeutend zur Zerfällung des charakteristischen Polynoms, schwierige Richtung gezeigt. Charakteristisches Polynom nilpotenter Endomorphismen. Diagonalisierbarkeit. Lineare Unabhängigkeit der Eigenvektoren zu paarweise verschiedenen Eigenwerten. Theorem von Cayley-Hamilton mit Beweis.
- 22.1 Bemerkungen zum Theorem von Cayley-Hamilton und zur Evaluation von Polynomen. Beispiel. Einfacherer Beweis des Theorems von Cayley-Hamilton über die komplexen Zahlen. Beispiel: Diagonalisierung einer Matrix.
- 26.1 Kongruenzebenen, Beweis der Existenz invariante Skalarprodukte noch nicht ganz fertig, Eindeutigkeit noch nicht gemacht.
- 29.1 Beweis der Existenz und Eindeutigkeit invariante Skalarprodukte für Kongruenzebenen. Tensorprodukt mit eindimensionalem Raum, Längengrade, kanonisches Skalarprodukt. Bewegungsräume werden in der Vorlesung nicht behandelt werden.
- 2.2 Reelle und komplexe Skalarprodukträume. Orthonormalsysteme und Orthonormalbasen. Deren Existenz. Orthogonale Projektion und orthogonales Komplement. Cauchy-Schwarz'sche Ungleichung mit Beweis. Dreiecksungleichung noch ohne Beweis.
- 5.2 Beweis Dreiecksungleichung und Bessel'sche Ungleichung. Orthogonale und unitäre Abbildungen und deren Matrizen, Determinanten, Eigenwerte. Vorgezogen: Charakterisierung orthogonaler Abbildungen als nicht notwendig lineare Abbildungen, die den Nullvektor festhalten und alle Abstände zwischen Vektoren erhalten. Satz vom Fußball.
- 9.2 Sartori rechnet Beispiele.

- 12.2 Besprechung des Formats der Klausur, Wiederholung der groben Struktur der Vorlesung. Spektralsatz für unitäre Automorphismen, Normalform für orthogonale Automorphismen.

Große Themen:

1. Mengen, Abbildungen, Verknüpfungen, Monoide, Gruppen, Körper.
2. Lineare Gleichungssysteme, Gauß-Algorithmus, Vektorräume, Untervektorräume, Erzeugung, lineare Unabhängigkeit, Basis, Dimension, Hauptabschätzung.
3. Homomorphismen, lineare Abbildungen, Injektivität, Kern, Bild, Dimensionsformel.
4. Affine Räume, affine Teilmengen, affine Abbildungen.
5. Lineare Abbildungen und Matrizen, Rechnen mit Matrizen, Inverse, Transponierte, Basiswechsel, Smith-Normalform.
6. Dualraum, Bidualraum, Zusammenhang mit dem Transponieren.
7. Rechnen mit komplexen Zahlen.
8. Primzahlen, Primfaktorzerlegung, euklidischer Algorithmus, Ringe, Restklassenringe.
9. Polynomringe, Auffaktorisieren von Wurzeln, Quotientenkörper, Partialbruchzerlegung.
10. Signum, Determinante, Multiplikationsformel, Entwicklungssatz, Cramer'sche Regel.
11. Eigenwerte, Eigenvektoren, charakteristisches Polynom, Trigonalisierbarkeit, Diagonalisierbarkeit, Cayley-Hamilton.

# **Kapitel 4**

## **Lineare Algebra 2**

## 4.1 Skalarprodukt und Geometrie

### 4.1.1 Skalarprodukt und die Ebene von Euklid

4.1.1.1. Sei  $V$  ein Vektorraum über einem Körper  $K$ . Ich erinnere daran, daß man unter einer **Bilinearform auf  $V$**  eine bilineare Abbildung  $s : V \times V \rightarrow K$  versteht. Ich erinnere weiter daran, daß eine Bilinearform **symmetrisch** heißt, wenn gilt

$$s(v, w) = s(w, v) \quad \forall v, w \in V$$

**Definition 4.1.1.2.** Eine symmetrische Bilinearform  $s$  auf einem reellen Vektorraum  $V$  heißt **positiv definit**, wenn gilt

$$v \neq 0 \Rightarrow s(v, v) > 0$$

Ein **Skalarprodukt** auf einem reellen Vektorraum ist eine positiv definite symmetrische Bilinearform. Ein reeller Vektorraum mit einem ausgezeichneten Skalarprodukt heißt ein **Skalarproduktraum**. Die **Norm** eines Vektors  $v$  in einem Skalarproduktraum  $(V, s)$  erklärt man als die nichtnegative reelle Zahl

$$\|v\| = \|v\|_s := \sqrt{s(v, v)}$$

4.1.1.3 (**Diskussion der Terminologie**). Das Skalarprodukt trägt seinen Namen, da es aus zwei Vektoren einen Skalar macht. Es darf nicht verwechselt werden mit der „Multiplikation mit Skalaren“ aus der Axiomatik eines Vektorraums, die aus einem Skalar und einem Vektor einen Vektor macht. Für Skalarprodukte sind auch die Notationen  $s(v, w) = \langle v, w \rangle = v \cdot w = vw$  gebräuchlich.

*Beispiel 4.1.1.4.* Auf  $V = \mathbb{R}^n$  erklärt man das **Standard-Skalarprodukt** durch die Vorschrift

$$\langle \vec{v}, \vec{w} \rangle := v_1 w_1 + \dots + v_n w_n$$

für  $\vec{v} = (v_1, \dots, v_n)$  und  $\vec{w} = (w_1, \dots, w_n)$ . Im Formalismus der Matrixmultiplikation und mit unserer Interpretation von Elementen des  $\mathbb{R}^n$  als Spaltenvektoren und Elementen von  $\mathbb{R}$  als  $(1 \times 1)$ -Matrizen können wir das Standardskalarprodukt auch schreiben als das Produkt  $\langle \vec{v}, \vec{w} \rangle = \vec{v}^\top \circ \vec{w}$  eines Zeilenvektors mit einem Spaltenvektor.

4.1.1.5. Sei  $V$  ein reeller Vektorraum. Gegeben eine Bilinearform  $s$  auf  $V$  und ein Automorphismus  $g \in \mathrm{GL}(V)$  von  $V$  sagen wir, unsere Bilinearform  $s$  sei **invariant unter  $g$**  und unser Automorphismus  $g$  **erhalte  $s$** , wenn gilt

$$s(gv, gw) = s(v, w) \quad \forall v, w \in V$$

Ist  $G \subset \mathrm{GL}(V)$  eine Untergruppe, so heißt eine Bilinearform  **$G$ -invariant**, wenn sie unter allen Elementen  $g \in G$  invariant ist. Die Gruppe aller Automorphismen eines reellen Vektorraums  $V$ , die die Bilinearform  $s$  erhalten, notieren wir

$$\mathrm{O}(V, s) := \{g \in \mathrm{GL}(V) \mid s(gv, gw) = s(v, w) \forall v, w \in V\}$$

Ist  $s$  ein Skalarprodukt, so heißen die  $s$  erhaltenden Automorphismen **orthogonal** und  $\mathrm{O}(V, s)$  heißt die **orthogonale Gruppe** von  $(V, s)$ . Im Fall des  $\mathbb{R}^n$  mit seinem Standardskalarprodukt  $s$  bezeichnet  $\mathrm{O}(n) := \{[g] \mid g \in \mathrm{O}(\mathbb{R}^n, s)\}$  für die Menge aller Matrizen orthogonaler Automorphismen alias aller **orthogonalen Matrizen**.

*Beispiel 4.1.1.6.* Die einzigen orthogonalen Automorphismen von  $\mathbb{R}$  mit seinem Standardskalarprodukt sind die Identität und die Multiplikation mit  $(-1)$ . In Formeln haben wir also  $\mathrm{O}(1) = \{1, -1\}$ . Wir verzichten hier darauf, in der Notation einen Unterschied zwischen Zahlen und  $(1 \times 1)$ -Matrizen zu machen.

*Beispiel 4.1.1.7.* Wir zeigen

$$\mathrm{O}(2) = \left\{ \begin{pmatrix} c & -d \\ d & c \end{pmatrix}, \begin{pmatrix} c & d \\ d & -c \end{pmatrix} \middle| c^2 + d^2 = 1 \right\}$$

Man kann das ohne alle Theorie mühevlos nachrechnen. Etwas konzeptueller mag man bemerken, daß für  $g \in \mathrm{O}(\mathbb{R}^2)$  ja gelten muß  $\langle g(e_1), g(e_1) \rangle = \langle e_1, e_1 \rangle = 1$  und folglich  $g(e_1) = (c, d)^\top$  mit  $c^2 + d^2 = 1$  in der ersten Spalte unserer Matrix  $[g]$ . Ebenso muß gelten  $g(e_2) = (a, b)^\top$  mit  $a^2 + b^2 = 1$ . Und da schließlich auch gelten muß  $\langle g(e_1), g(e_2) \rangle = \langle e_1, e_2 \rangle = 0$ , folgt zusätzlich  $ca + db = 0$ . Das läßt für die zweite Spalte unserer Matrix  $[g]$  nur noch die beiden Möglichkeiten  $\pm(-d, c)^\top$  offen. Da es umgekehrt ausreicht, die Bedingung  $\langle \vec{v}, \vec{w} \rangle = \langle g\vec{v}, g\vec{w} \rangle$  für  $\vec{v}, \vec{w}$  aus einem Erzeugendensystem zu prüfen, sagen wir dem Erzeugendensystem der beiden Vektoren der Standardbasis, folgt die Behauptung. Anschaulich mag man sich die Elemente der orthogonalen Gruppe  $\mathrm{O}(2) \cong \mathrm{O}(\mathbb{R}^2)$  als „Drehungen“ und „Spiegelungen“ der Ebene  $\mathbb{R}^2$  vorstellen, die den Ursprung festhalten. Wir diskutieren das später noch ausführlich.

**4.1.1.8 (Geometrie durch Symmetrie).** Ich erwarte, daß Sie aus der Schule eine gewisse Vertrautheit mit dem Standardskalarprodukt mitbringen und wissen, daß salopp gesprochen „Senkrechtstehen Skalarprodukt Null bedeutet“ und daß „die Norm eines Vektors seine Länge bedeutet“. Das kann man sich, wenn man auf der Papierebene eine Längeneinheit und ein Paar von aufeinander senkrecht stehenden und orientierten Geraden wählt und die Papierebene darüber mit dem  $\mathbb{R}^2$  identifiziert, auch mit Hilfe des Satzes von Pythagoras leicht klarmachen. Mir scheint jedoch eine andere Modellierung der Papierebene sinnvoller und unserer Anschauung besser zugänglich, bei der man stattdessen von der Vorgabe einer ausgezeichneten Gruppe von „Kongruenzen“ ausgeht und die Begriffe Senkrechtstehen, Skalarprodukt und Länge sowie ihre Beziehungen untereinander daraus entwickelt. Das mag auch gleich als eine erste Illustration für die Bedeutung

von „Symmetrien“ alias „strukturerhaltenden Selbstabbildungen“ in der Geometrie dienen. Wir werden im folgenden, von diesen Symmetrien oder in unserem Fall Kongruenzen ausgehend, sogar den Satz des Pythagoras selbst noch einmal in der Sprache der Mengenlehre herleiten.

**Definition 4.1.1.9.** Eine Teilmenge  $A$  eines reellen affinen Raums  $E$  heißt eine **Halbgerade**, wenn es einen Punkt  $p \in E$  und einen von Null verschiedenen Richtungsvektor  $\vec{v} \in \vec{E} \setminus 0$  gibt mit

$$A = p + \mathbb{R}_{\geq 0} \vec{v}$$

**Definition 4.1.1.10.** Eine Untergruppe  $K \subset \text{Aff}^\times(E)$  der Automorphismengruppe einer reellen affinen Ebene  $E$  heißt eine **Kongruenzgruppe**, wenn sie alle Translationen enthält, in Formeln  $\vec{E} \subset K$ , und wenn es für je zwei Halbgeraden  $A, B \subset E$  genau zwei Elemente  $k, h \in K$  gibt mit

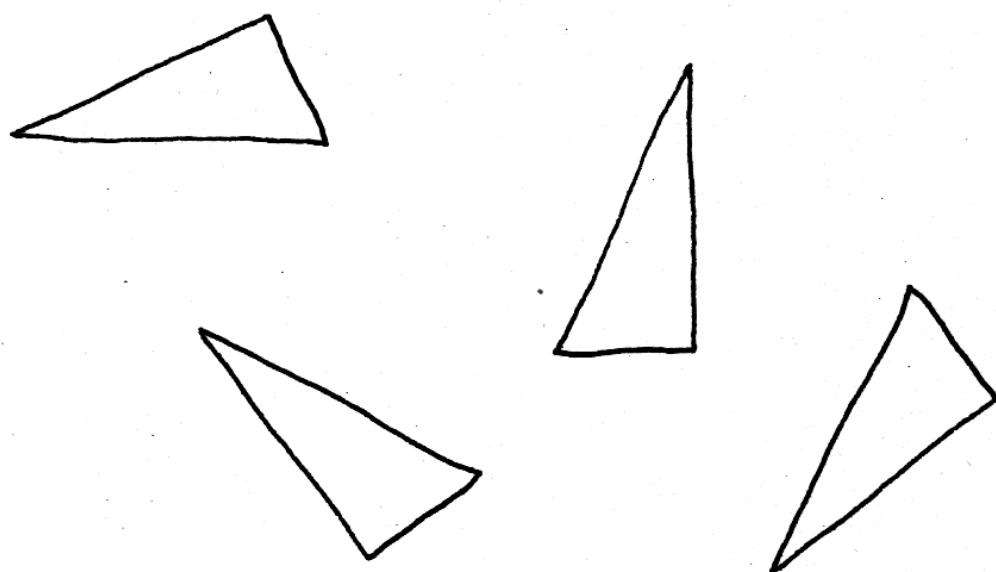
$$k(A) = B = h(A)$$

Eine **Kongruenzebene**  $(E, K)$  ist ein zweidimensionaler reeller affiner Raum  $E$  mit einer ausgezeichneten Kongruenzgruppe  $K$ . Die Elemente unserer Kongruenzgruppe nennen wir die **Kongruenzen** unserer Kongruenzebene.

4.1.1.11. Unter einem **invarianten Skalarprodukt** einer Kongruenzebene  $(E, K)$  verstehen wir ein unter der Gruppe  $\vec{K}$  der linearen Anteile aller Kongruenzen invariantes Skalarprodukt auf ihrem Richtungsraum  $\vec{E}$ .

4.1.1.12 (**Diskussion der Terminologie**). Unsere Kongruenzebenen sind unsere erste axiomatische Beschreibung der schmutzigen Papierebene. Wir werden noch zwei weitere äquivalente axiomatische Beschreibungen dieser Struktur einführen, die eher algebraischen „euklidischen Ebenen“ alias „zweidimensionalen euklidischen Räume“ aus 4.1.5.1 und besonders nah an der geometrischen Anschauung und der Axiomatik von Euklid selbst die „fasteuklidischen Ebenen mit Paralellaxiom“ aus ??.

*Vorschau* 4.1.1.13. In 4.1.2.9 zeigen wir, daß es zu jeder Kongruenzebene  $(E, K)$  ein invariantes Skalarprodukt  $s$  gibt und daß sich je zwei invarianten Skalarprodukte zu ein- und derselben Kongruenzebene höchstens um eine positive multiplikative Konstante unterscheiden. In 4.1.2.11 zeigen wir, daß die Kongruenzen sich dann umgekehrt charakterisieren lassen als alle Affinitäten, deren linearer Anteil in Bezug auf dieses Skalarprodukt  $s$  orthogonal ist. Daraus mögen Sie in Übung 4.1.2.13 folgern, daß je zwei Kongruenzebenen in einer dort genauer präzisierten Weise isomorph sind.



Einige Dreiecke in der Papierebene, die durch Kongruenzen ineinander überführt werden können. Man nennt sie deshalb auch **kongruente Dreiecke**.

4.1.1.14. Orientierungserhaltende Kongruenzen einer beliebig vorgegebenen Kongruenzebene heißen **gleichsinnige Kongruenzen** und orientierungsumkehrende Kongruenzen **gegensinnige Kongruenzen**. Sie werden in 4.1.2.14 zeigen, daß jede gleichsinnige Kongruenz entweder eine Translation ist oder genau einen Fixpunkt hat. Sie weden dort auch zeigen, inwiefern man sie sich im letzteren Fall als eine „Drehung“ vorstellen darf. Andererseits werden sie in 4.1.2.15 zeigen, daß jede gegensinnige Kongruenz genau eine affine Gerade stabilisiert, und werden erklären, inwiefern man sie sich als eine „Gleitspiegelung“ vorstellen darf. Spiegelungen fassen wir dabei als spezielle Gleitspiegelungen auf.

4.1.1.15 (**Die schmutzige Anschauung**). Man mag bei einer Kongruenzebene an eine unendlich ausgedehnte Pappe denken und bei einer Kongruenz an eine anschauliche Bewegung im Raum, die diese Pappe in sich selber überführt. Gleichsinnige Kongruenzen erhält man, indem man sich die Pappe als auf einem Tisch liegend denkt und sie auf dem Tisch verschiebt oder dreht, ohne sie dabei vom Tisch hochzuheben. Gegensinnige Kongruenzen erhält man, indem man die Pappe auf irgendeine Weise umdreht. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist.

4.1.1.16 (**Norm als Länge**). Gegeben eine Kongruenzebene  $(E, K)$  mit invariantem Skalarprodukt  $\langle \cdot, \cdot \rangle$  gilt für die zugehörige Norm  $\|v\| := \sqrt{\langle v, v \rangle}$  offensichtlich

$$\|p - q\| = \|k(p) - k(q)\| \quad \forall p, q \in E, k \in K$$

sowie  $\|\lambda v\| = |\lambda| \|v\|$  für jeden reellen Skalar  $\lambda$ . In der schmutzigen Papierebene entspricht folglich  $\|p - q\|$  der Zahl, die wir als Abstand zwischen den Punkten  $p$  und  $q$  messen, wenn wir ein Lineal anlegen alias mit einer Kongruenzabbildung entsprechend bewegen, und wenn wir zusätzlich unser Lineal dadurch eichen, daß wir damit für einen fest vorgegebenen Richtungsvektor  $m \neq 0$  die Länge  $\|m\| = 1$  messen.

**Satz 4.1.1.17 (Senkrechtstehen und Skalarprodukt).** *Gegeben eine Kongruenzebene  $(E, K)$  mit invariantem Skalarprodukt  $\langle \cdot, \cdot \rangle$  und Richtungsvektoren  $v, w \in \vec{E}$  sind gleichbedeutend:*

1. *Es gibt eine Kongruenz  $\varphi \in K$  mit  $\varphi(v) = -v$  und  $\varphi(w) = w$ ;*
2. *Es gilt  $\langle v, w \rangle = 0$ .*

4.1.1.18. Die erste dieser Bedingungen knüpft an unsere geometrische Anschauung an. Wir nennen im folgenden zwei Richtungsvektoren **geometrisch senkrecht**, wenn sie diese Bedingung erfüllen. Die zweite dieser Bedingungen ist Ihnen vermutlich bereits aus der Schule vertraut. Wir formulieren sie gleich als Definition und nennen Vektoren  $v, w$  in einem Skalarproduktraum **algebraisch**

**senkrecht** oder gleichbedeutend **orthogonal**, wenn ihr Skalarprodukt verschwindet.

**4.1.1.19 (Ursprung der Terminologie).** Das Wort „senkrecht“ kommt her von „senken“, speziell dem Hinablassen eines Gewichts oder „Senkbleis“ an einem Faden, um die Vertikale zu bestimmen. Vom Begriff des „senkrecht Stehens einer Säule auf dem Boden“ zum „senkrecht Stehen eines Vektors auf einem anderen“ ist es dann nur noch ein kleiner Schritt. Das Wort „orthogonal“ ist griechisch für „rechtwinklig“, und zwar ist „gon“ derselbe Wortstamm wie „Knie“ und meint hier „Winkel“, wohingegen „ortho“ für „recht, richtig“ steht wie etwa in „Orthographie“ für „Rechtschreibung“.

*Beweis.* Gibt es eine Kongruenz  $\varphi$  mit  $\vec{\varphi}(v) = -v$  und  $\vec{\varphi}(w) = w$ , so folgt für unser invariantes Skalarprodukt

$$\langle v, w \rangle = \langle \vec{\varphi}(v), \vec{\varphi}(w) \rangle = \langle -v, w \rangle$$

und damit  $\langle v, w \rangle = 0$ . Im Fall  $w \neq 0$  gibt es umgekehrt für alle  $p \in E$  genau eine nichttriviale Kongruenz  $\varphi \in K \setminus \text{id}$ , die die Halbgerade  $p + \mathbb{R}_{\geq 0}w$  festhält. Aus  $\varphi(p) = p$  folgt  $\vec{\varphi} \neq \text{id}$ . Andererseits gilt notwendig  $\varphi^2 = \text{id}$  und folglich  $(\vec{\varphi})^2 = \text{id}$ . Nach 3.6.6.29 hat  $\vec{\varphi}$  also die Eigenwerte 1 und  $(-1)$  und beide Eigenräume sind eindimensional. Nach der bereits bewiesenen Implikation umfaßt der  $(-1)$ -Eigenraum den Untervektorraum  $\{v \in \vec{E} \mid \langle v, w \rangle = 0\}$ . Aus Dimensionsgründen muß er dann bereit mit diesem Untervektorraum zusammenfallen und wir haben für alle  $v, w \in \vec{E}$  mit  $\langle v, w \rangle = 0$  und  $w \neq 0$  eine Kongruenz  $\varphi$  gefunden mit  $\vec{\varphi}(v) = -v$  und  $\vec{\varphi}(w) = w$ . Im Fall  $w = 0$  können wir dasselbe Argument für irgendeinen Vektor  $w_1 \in \vec{E} \setminus \{0\}$  mit  $\langle v, w_1 \rangle = 0$  anwenden und das so konstruierte  $\varphi$  erfüllt dann natürlich auch  $\vec{\varphi}(w) = 0 = w$ .  $\square$

**Satz 4.1.1.20 (Pythagoras).** Zwei Vektoren  $v, w$  des Richtungsraums einer Kongruenzebene mit invariantem Skalarprodukt  $\langle \cdot, \cdot \rangle$  stehen genau dann aufeinander geometrisch senkrecht, wenn für die zugehörige Norm  $\| \cdot \|$  gilt

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2$$

*Beweis.* Per definitionem gilt  $\|v\|^2 = \langle v, v \rangle$ . Aus der Bilinearität und Symmetrie des Skalarprodukts folgern wir für beliebige Richtungsvektoren  $v, w$  die Identität

$$\|v + w\|^2 = \|v\|^2 + 2\langle v, w \rangle + \|w\|^2$$

Aus 4.1.1.17 wissen wir bereits, daß das geometrische Senkrechtstehen gleichbedeutend ist zum algebraischen Senkrechtstehen alias dem Verschwinden des Skalarprodukts. Der Satz folgt.  $\square$

*Ergänzung 4.1.1.21 (Bezug zum geometrischen Beweis).* Der auf der Schule übliche geometrische Zugang zum Satz von Pythagoras durch Flächenvergleich ist uns dadurch verbaut, daß in unserem formalen Aufbau das Konzept einer Fläche noch gar nicht zur Verfügung steht. In der schmutzigen Anschauung mag man jedoch  $\langle v, w \rangle$  verstehen als die „orientierte Fläche  $\langle v, w \rangle = \text{vol}(v, w')$  des Parallelogramms mit den Kantenvektoren  $v, w'$  für  $w'$  den Vektor, der aus  $w$  durch Drehung um einen rechten Winkel gegen den Uhrzeigersinn entsteht“. In dieser Anschauung bedeutet die Bilinearität des Skalarprodukts dann insbesondere die „Invarianz von Flächen unter Scherungen“. So erweist sich unsere algebraische Rechnung als eine Übersetzung der in der Schule üblichen und adäquaten anschaulichen Argumentation in den hier entwickelten Formalismus.

*Ergänzung 4.1.1.22.* Ich will kurz auf die naheliegende Frage eingehen, warum man nicht anstelle des Skalarprodukts einfacher die Zuordnung betrachtet, die je zwei Vektoren einer euklidischen Ebene die Fläche des von ihnen aufgespannten Parallelogramms zuordnet. Die Schwierigkeit dabei ist, daß diese Zuordnung nicht bilinear wäre, man kann also nur schöne algebraische Formeln erwarten für die Zuordnung, die je zwei Vektoren einer euklidischen Ebene die „orientierte Fläche“ des von ihnen aufgespannten Parallelogramms zuordnet. Diese Zuordnung kann durchaus durch einen einfachen algebraischen Ausdruck beschrieben werden, sie hängt aber von der Wahl einer Orientierung ab und ist nicht symmetrisch, sondern vielmehr schiefsymmetrisch. Bei der zuvor beschriebenen geometrischen Bedeutung des Skalarprodukts geht dagegen die Wahl einer Orientierung zweimal ein und kürzt sich weg, so daß es im Endeffekt von dieser Wahl doch nicht abhängt.

*Ergänzung 4.1.1.23 (Allgemeinere Grundkörper als die reellen Zahlen).* Bei den hier und im folgenden ausgeführten Überlegungen mag man ein tieferes Verständnis aus der Frage gewinnen, inwieweit sie sich auch über allgemeineren angeordneten Körpern durchführen lassen. Für die meisten Resultate müssen wir nur fordern, daß alle nichtnegativen Elemente des fraglichen angeordneten Körpers Quadrate sind. Sobald es aber um Winkelmaße gehen wird, benötigen wir analytische Hilfsmittel und müssen mit dem Körper der reellen Zahlen arbeiten oder eine große Künstlichkeit der Konstruktionen und Argumente in Kauf nehmen.

## Übungen

*Übung 4.1.1.24 (Die komplexe Zahlenebene als Kongruenzebene).* Man zeige, daß die komplexen Zahlen  $\mathbb{C}$  zu einer Kongruenzebene werden, wenn wir als Kongruenzen diejenigen Abbildungen auszeichnen, die eine der beiden Gestalten  $z \mapsto az + b$  oder  $z \mapsto a\bar{z} + b$  haben mit  $a, b \in \mathbb{C}$  und  $|a| = 1$ . Man zeige, daß die Formel  $\langle z, w \rangle := \text{Re } \bar{z}w$  ein invariantes Skalarprodukt auf  $\vec{\mathbb{C}} = \mathbb{C}$

liefert, für dessen Norm gilt  $\|z\| = |z|$ . Man mag mit mehr Mut weiter zeigen, daß unsere Kongruenzen genau alle Abbildungen  $k : \mathbb{C} \rightarrow \mathbb{C}$  sind mit  $|k(p) - k(q)| = |p - q| \forall p, q \in \mathbb{C}$ .

*Übung 4.1.1.25.* Gegeben ein reeller Skalarproduktraum  $V$  mit Skalarprodukt  $\langle \cdot, \cdot \rangle$  verwendet man üblicherweise die Notation  $\|v\| := \sqrt{\langle v, v \rangle}$ . Man zeige in einem reellen Skalarproduktraum die Äquivalenz

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2 \Leftrightarrow \langle v, w \rangle = 0$$

Man zeige weiter in einem reellen Skalarproduktraum die **Parallelogrammregel**, nach der die Summe der Quadrate der vier Seiten eines Parallelogramms gleich der Summe der Quadrate der beiden Diagonalen ist, in Formeln

$$2\|v\|^2 + 2\|w\|^2 = \|v - w\|^2 + \|v + w\|^2$$

*Übung 4.1.1.26 (Rechtfertigung der Konstruktion der Mittelsenkrechte).* Seien  $E$  eine reelle affine Ebene und  $\langle \cdot, \cdot \rangle$  ein Skalarprodukt auf ihrem Richtungsraum. Gegeben paarweise verschiedene Punkte  $a, b, c, d \in E$  mit  $\|a - c\| = \|a - d\|$  und  $\|b - c\| = \|b - d\|$  zeige man, daß  $(a - b)$  senkrecht steht auf  $(c - d)$ . Gilt hier sogar  $\|a - c\| = \|a - d\| = \|b - c\| = \|b - d\|$ , so zeige man, daß der Schnittpunkt  $p$  der Geraden  $\overline{ab}$  und  $\overline{cd}$  durch  $a$  und  $b$  beziehungsweise  $c$  und  $d$  denselben Abstand zu allen unseren vier Punkten  $a, b, c, d$  hat, in Formeln  $\|a - p\| = \|b - p\| = \|c - p\| = \|d - p\|$ .

## 4.1.2 Invariante Skalarprodukte zu Drehspiegelgruppen

**Definition 4.1.2.1.** Sei  $V$  ein reeller Vektorraum. Eine Teilmenge  $A \subset V$  heißt ein **Strahl**, wenn es einen Vektor  $v \in V \setminus 0$  gibt mit  $A = \mathbb{R}_{\geq 0}v$ .

**Definition 4.1.2.2.** Gegeben ein zweidimensionaler reeller Vektorraum  $Z$  heiße eine Untergruppe  $O \subset \mathrm{GL}(Z)$  eine **Drehspiegelgruppe**, wenn es für je zwei Strahlen  $A, B \subset Z$  genau zwei Elemente  $k, h \in O$  gibt mit  $k(A) = B = h(A)$ . Die Elemente einer ausgezeichneten Drehspiegelgruppe nennen wir im folgenden **Drehspiegelungen**.

*Beispiel 4.1.2.3.* Gegeben ein zweidimensionaler reeller Vektorraum  $Z$  mit Skalarprodukt  $s$  ist die orthogonale Gruppe  $O(Z, s)$  eine Drehspiegelgruppe. Ich überlasse es dem Leser, dafür einen Beweis auszuschreiben.

4.1.2.4. Sei  $(Z, O)$  ein zweidimensionaler reeller Vektorraum mit ausgezeichneter Drehspiegelgruppe. Für alle  $v \in Z \setminus 0$  gibt es dann nach Annahme genau ein nichttriviales Element  $r_v \in O \setminus \mathrm{id}$  mit  $r_v(\mathbb{R}_{\geq 0}v) = \mathbb{R}_{\geq 0}v$ . Es folgt erst  $r_v^2 = \mathrm{id}$  und dann  $r_v(v) = v$ . Aus  $r_v^2 = \mathrm{id}$  folgt andererseits, daß  $r_v$  die Eigenwerte 1 und  $(-1)$  hat. Wir nennen  $r_v$  die **Spiegelung zu  $v$** . Die Notation mag an „Reflektion“ erinnern, der Buchstabe  $s$  ist schon für Skalarprodukte vergeben.

**Lemma 4.1.2.5 (Drehspiegelungen mit negativer Determinante).** Sei  $(Z, O)$  ein zweidimensionaler reeller Vektorraum mit ausgezeichneter Drehspiegelgruppe. So sind die Drehspiegelungen mit negativer Determinante genau die Spiegelungen, in Formeln

$$\{k \in O \mid \det(k) < 0\} = \{r_v \mid v \in Z \setminus \{0\}\}$$

*Beweis.* Ein Automorphismus  $r$  eines zweidimensionalen reellen Vektorraums mit negativer Determinante muß nach 3.6.6.24 einen positiven und einen negativen Eigenwert haben. Ist  $r$  unsere Drehspiegelung und  $v$  ein Eigenvektor von  $r$  zum positiven Eigenwert, so muß  $r$  die einzige nichttriviale Drehspiegelung sein, die den Strahl  $\mathbb{R}_{\geq 0}v$  festhält.  $\square$

**Lemma 4.1.2.6.** Sei  $(Z, O)$  ein zweidimensionaler reeller Vektorraum mit ausgezeichneter Drehspiegelgruppe. So werden je zwei Strahlen  $A, B \subset Z$  durch genau eine Spiegelung aus  $O$  miteinander vertauscht.

*Beweis.* Sicher gibt es stets eine Drehspiegelung  $k$ , die  $A$  in  $B$  überführt, und eine Spiegelung  $r$ , die  $A$  festhält. Dann hat von den beiden Drehspiegelungen  $r$  und  $kr$ , die  $A$  in  $B$  überführen, genau eine negative Determinante, und diese ist nach 4.1.2.5 die gesuchte Spiegelung.  $\square$

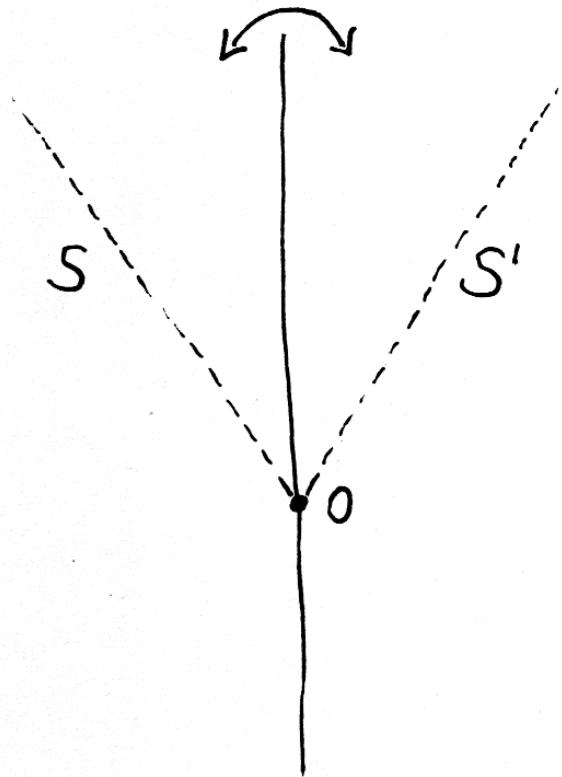
**4.1.2.7 (Einführen einer Norm).** Sei  $(Z, O)$  ein zweidimensionaler reeller Vektorraum mit ausgezeichneter Drehspiegelgruppe. Sei  $m \in Z \setminus \{0\}$  ein fest gewählter von Null verschiedener Vektor. Für jeden weiteren von Null verschiedenen Vektor  $v \in Z \setminus \{0\}$  gibt es offensichtlich genau eine Drehspiegelung  $d \in O$  mit positiver Determinante, die den Strahl  $\mathbb{R}_{\geq 0}v$  auf den Strahl  $\mathbb{R}_{\geq 0}m$  abbildet. Wir können also eine positive reelle Zahl  $\|v\|_m = \|v\|$  definieren durch die Forderung

$$d(v) = \|v\|_m$$

Wir nennen diese positive reelle Zahl die **durch  $m$  bestimmte Norm** oder kurz die  **$m$ -Norm von  $v$** . Vereinbaren wir zusätzlich  $\|0\| = 0$ , so gilt offensichtlich  $\|\mu v\| = \mu\|v\|$  für alle Vektoren  $v \in Z$  und alle nichtnegativen reellen Zahlen  $\mu \in \mathbb{R}_{\geq 0}$ . Offensichtlich gilt auch  $\|kv\| = \|v\|$  für alle Drehspiegelungen  $k \in O$  und wir haben für  $v, w \in Z$  sogar

$$\|v\| = \|w\| \Leftrightarrow \exists k \in O \text{ mit } k(v) = w.$$

**Satz 4.1.2.8 (Invariante Skalarprodukte zu Drehspiegelgruppen).** Sei  $(Z, O)$  ein zweidimensionaler reeller Vektorraum mit ausgezeichneter Drehspiegelgruppe. So gibt es auf  $Z$  ein  $O$ -invariantes Skalarprodukt und jede  $O$ -invariante Bilinearform auf  $Z$  ist ein Vielfaches dieses Skalarprodukts.



Je zwei Strahlen in einem zweidimensionalen reellen Vektorraum mit ausgezeichneter Drehspiegelgruppe werden durch eine Spiegelung vertauscht.  
Der ausgezeichnete Punkt stellt den Ursprung dar.

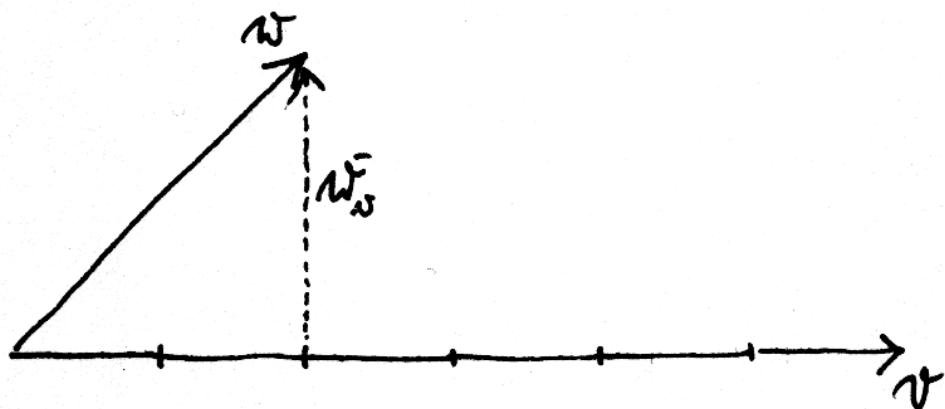


Illustration der Definition von  $\alpha_v(w)$ . Im Bild hätten wir etwa  $\alpha_v(w) = 1/3$ .

*Beweis.* Gegeben Vektoren  $v, w \in Z$  mit  $v \neq 0$  erklären wir einen Skalar  $\alpha_v(w) \in \mathbb{R}$  durch die Vorschrift

$$\alpha_v(w)v = (w + r_v w)/2$$

Das ist sinnvoll, da die rechte Seite offensichtlich ein Fixpunkt der Spiegelung  $r_v$  ist und folglich ein Vielfaches von  $v$  sein muß. Die rechte Seite ist genauer der Fixpunktanteil von  $w$  bei seiner Zerlegung  $w = w_v^+ + w_v^-$  in Eigenvektoren von  $r_v$  zu den Eigenwerten  $\pm 1$ . Mit dieser Notation gilt also

$$\alpha_v(w)v = w_v^+$$

In der schmutzigen Anschauung mag man sich  $w_v^+$  als das Bild von  $w$  unter der „orthogonalen Projektion auf die Gerade  $\mathbb{R}v$ “ vorstellen, wie Sie sie möglicherweise in der Schule bereits kennengelernt haben. Jetzt halten wir einen Vektor  $m \in Z \setminus 0$  fest und erklären eine Abbildung  $Z \times Z \rightarrow \mathbb{R}$ ,  $(v, w) \mapsto \langle v, w \rangle$  durch die Vorschrift

$$\langle v, w \rangle := \begin{cases} \|v\|^2 \alpha_v(w) & v \neq 0; \\ 0 & v = 0. \end{cases}$$

Wir zeigen im folgenden, daß das ein invariantes Skalarprodukt ist. Offensichtlich gilt  $\langle v, v \rangle = \|v\|^2$  und  $w \mapsto \langle v, w \rangle$  ist linear für alle  $v$ . Ist weiter  $k \in O$  eine Drehspiegelung, so gilt  $kr_v = r_{kv}k$ , denn beide Abbildungen haben dieselbe Determinante und bilden  $v$  auf  $kv$  ab. Daraus folgt  $\alpha_v(w) = \alpha_{kv}(kw)$  mittels der Umformungen

$$\alpha_v(w)kv = (kw + kr_v w)/2 = (kw + r_{kv} kw)/2 = \alpha_{kv}(kw)kv$$

Es folgt die Invarianz  $\langle v, w \rangle = \langle kv, kw \rangle$  für alle  $k \in O$ . Um schließlich zu zeigen, daß auch  $v \mapsto \langle v, w \rangle$  linear ist für alle  $w$ , reicht es, die Symmetrie  $\langle v, w \rangle = \langle w, v \rangle$  zu prüfen. Es reicht, das für  $v \neq 0 \neq w$  zu prüfen. Es reicht sogar, das unter der zusätzlichen Voraussetzung  $\|v\| = \|w\|$  zu prüfen, denn offensichtlich gilt stets  $\langle \lambda v, w \rangle = \lambda \langle v, w \rangle = \langle v, \lambda w \rangle$ . Damit dürfen wir nach 4.1.2.6 annehmen, daß es eine Spiegelung  $r \in O$  gibt mit  $rv = w$  und  $r^2 = \text{id}$ . Es folgt  $rw = v$  und so die gewünschte Symmetrie  $\langle v, w \rangle = \langle rv, rw \rangle = \langle w, v \rangle$ . Damit liefert unsere Konstruktion in der Tat das gesuchte invariante Skalarprodukt. Um die Eindeutigkeit bis auf Skalar zu zeigen, wählen wir  $v \in Z \setminus 0$  und einen Eigenvektor  $w$  von  $r_v$  zum Eigenwert  $-1$  derart, daß es eine Drehspiegelung  $d \in O$  gibt mit  $dv = w$ . Für jede invariante Bilinearform  $\langle , \rangle$  gilt dann

$$\langle v, w \rangle = \langle r_v v, r_v w \rangle = \langle v, -w \rangle = -\langle v, w \rangle$$

und damit  $\langle v, w \rangle = 0$ . Weiter gilt  $\langle v, v \rangle = \langle dv, dv \rangle = \langle w, w \rangle$  und so

$$\langle av + bw, xv + yw \rangle = (ax + by)\langle v, v \rangle$$

Das zeigt die behauptete Eindeutigkeit bis auf Skalar.  $\square$

**Korollar 4.1.2.9 (Invariante Skalarprodukte zu Kongruenzebenen).** *Zu jeder Kongruenzebene gibt es ein invariantes Skalarprodukt und jede invariante Bilinearform ist ein Vielfaches dieses Skalarprodukts.*

*Beweis.* Gegeben eine Kongruenzebene  $(E, K)$  ist offensichtlich  $\vec{K} \subset \mathrm{GL}(\vec{E})$  eine Drehspiegelgruppe. Damit folgt die Behauptung aus Satz 4.1.2.8 über invariante Skalarprodukte zu Drehspiegelgruppen.  $\square$

**Proposition 4.1.2.10 (Drehspiegelgruppe als orthogonale Gruppe).** *Sei  $(Z, O)$  ein zweidimensionaler reeller Vektorraum mit ausgezeichneter Drehspiegelgruppe und  $s$  ein  $O$ -invariantes Skalarprodukt. So ist unsere Drehspiegelgruppe die orthogonale Gruppe zu  $s$ , in Formeln*

$$O = O(Z, s)$$

*Beweis.* Per definitionem haben wir  $O \subset O(Z, s)$  und nach 4.1.2.3 ist auch  $O(Z, s)$  eine Drehspiegelgruppe. Beide Gruppen haben also dieselben Elemente mit negativer Determinante, nämlich unsere Spiegelungen  $r_v$  mit  $v \in Z \setminus 0$ . Sie mögen als Übung 4.1.2.12 zeigen, daß jede Drehspiegelgruppe von ihren Spiegelungen erzeugt wird. Das beendet dann den Beweis.  $\square$

**Korollar 4.1.2.11 (Kongruenzgruppe als orthogonalaffine Gruppe).** *Gegeben ein invariantes Skalarprodukt  $s$  zu einer Kongruenzebene  $(E, K)$  sind die Kongruenzen genau alle Affinitäten mit  $s$ -orthogonalem linearen Anteil, in Formeln*

$$K = \{\varphi \in \mathrm{Aff} E \mid \vec{\varphi} \in O(s)\}$$

*Beweis.* Weil unsere Kongruenzgruppe nach Annahme alle Richtungsvektoren enthält, haben wir schon mal  $K = \{\varphi \in \mathrm{Aff} E \mid \vec{\varphi} \in \vec{K}\}$ . Damit folgt das Korollar direkt aus unserer Proposition 4.1.2.10.  $\square$

## Übungen

*Übung 4.1.2.12.* Jede Drehspiegelgruppe wird von ihren Spiegelungen erzeugt.

*Übung 4.1.2.13 (Eindeutigkeit von Kongruenzebenen).* Ein **Isomorphismus von Kongruenzebenen**  $(E, K)$  und  $(F, L)$  ist ein Isomorphismus  $\varphi : E \xrightarrow{\sim} F$  von affinen Räumen, unter dem sich die jeweils ausgezeichneten Kongruenzgruppen entsprechen, in Formeln  $L = \varphi K \varphi^{-1}$ . Man zeige, daß je zwei Kongruenzebenen  $E, F$  isomorph sind. Man zeige genauer, daß es für beliebige Paare von je zwei verschiedenen Punkten  $(p, q) \in E \times E$  sowie  $(b, d) \in F \times F$  genau zwei Isomorphismen  $\phi, \psi : E \xrightarrow{\sim} F$  von Kongruenzebenen gibt, die  $(p, q)$  in  $(b, d)$  überführen. Man mag etwa zeigen, daß jedes Beispiel zu dem in 4.1.1.24 gegebenen Beispiel isomorph sein muß.

*Übung 4.1.2.14 (Gleichsinnige Kongruenzen).* Die einzige gleichsinnige Kongruenz einer Kongruenzebene mit mehr als einem Fixpunkt ist die Identität. Jede gleichsinnige Kongruenz einer Kongruenzebene ohne Fixpunkt ist eine Translation. Jede gleichsinnige Kongruenz unserer Kongruenzebene  $\mathbb{C}$  aus 4.1.1.24 mit Fixpunkt  $p$  hat die Gestalt  $p + z \mapsto p + \lambda z$  für  $\lambda \in \mathbb{C}$  mit  $|\lambda| = 1$ .

*Übung 4.1.2.15 (Gegensinnige Kongruenzen).* Jede gegensinnige Kongruenz einer Kongruenzebene stabilisiert genau eine reelle affine Gerade. Jede gegensinnige Kongruenz unserer Kongruenzebene  $\mathbb{C}$  aus 4.1.1.24, die  $\mathbb{R}$  stabilisiert, hat die Gestalt  $z \mapsto a + \bar{z}$  für  $a \in \mathbb{R}$ .

*Übung 4.1.2.16 (Ähnlichkeiten).* Ein Isomorphismus einer Kongruenzebene mit sich selber heißt eine **Ähnlichkeitsabbildung** oder **Ähnlichkeit**. Man zeige, daß die Ähnlichkeiten unserer Kongruenzebene  $\mathbb{C}$  aus 4.1.1.24 genau alle Abbildungen sind, die eine der beiden Gestalten  $z \mapsto az + b$  oder  $z \mapsto a\bar{z} + b$  haben mit  $a, b \in \mathbb{C}$  und  $a \neq 0$ . Man folgere, daß alle Ähnlichkeiten einer Kongruenzebene, die keine Kongruenzen sind, genau einen Fixpunkt haben müssen, und argumentiere heuristisch, daß sie entweder „Drehstreckungen“ oder „Spiegelstreckungen“ sein müssen.

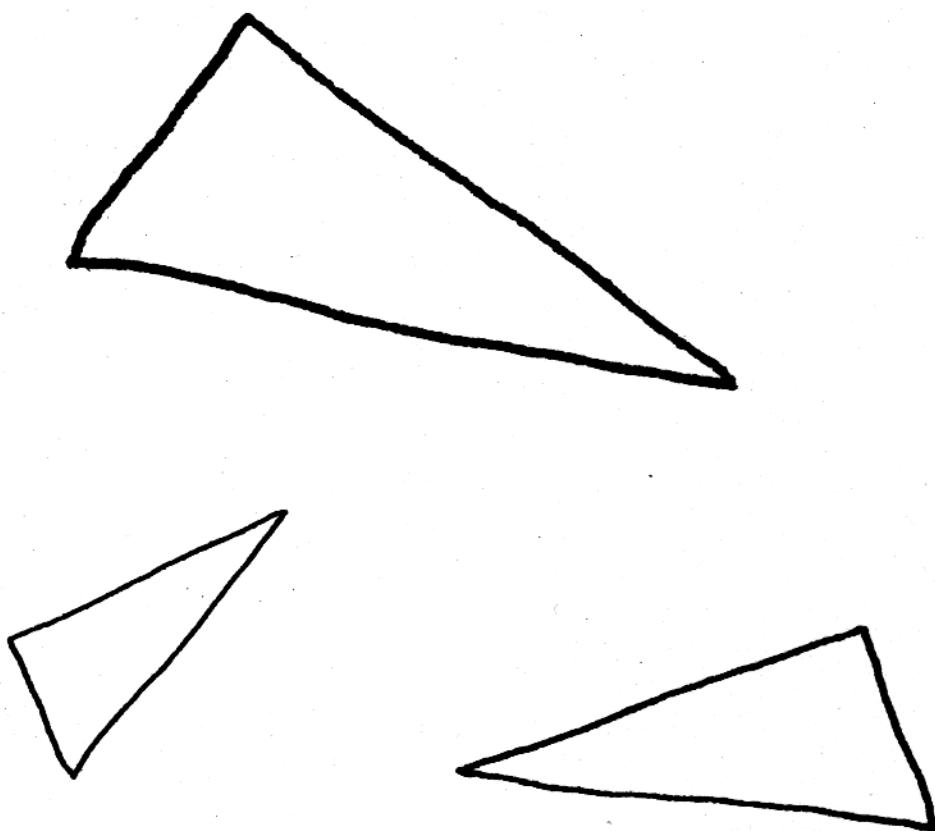
### 4.1.3 Geometrie von Skalarprodukträumen

4.1.3.1. Im Vorhergehenden haben wir aus der räumlichen Anschauung heraus den Begriff des Skalarprodukts entwickelt. Im folgenden bauen wir umgekehrt für allgemeine Vektorräume mit Skalarprodukt eine sich an dieser räumlichen Anschauung orientierende Begrifflichkeit auf und zeigen, wie sich viele im Raum unserer Anschauung offensichtliche Tatsachen algebraisch formalisieren und auf diesen Kontext verallgemeinern lassen. Ich schreibe eine Weile wieder Vektoren mit Pfeil, damit man die  $i$ -te Komponente  $v_i$  eines Vektors  $\vec{v} = (v_1, \dots, v_n) \in \mathbb{R}^n$  und den  $i$ -ten Vektor  $\vec{v}_i$  einer Familie  $\vec{v}_1, \dots, \vec{v}_n$  von Vektoren besser auseinanderhalten kann.

4.1.3.2. Ich beginne mit Erinnerungen einiger grundlegender Begriffe. Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  heißt eine bilineare Abbildung  $b : V \times V \rightarrow K$  wie in 3.2.3.8 eine **Bilinearform auf  $V$** . Wie in 3.6.3.1 heißt eine Bilinearform  $b$  **symmetrisch**, wenn gilt  $b(\vec{v}, \vec{w}) = b(\vec{w}, \vec{v})$  für alle  $\vec{v}, \vec{w} \in V$ . Ist  $K$  ein angeordneter Körper, so heißt eine Bilinearform  $b$  wie in 4.1.1.2 **positiv definit**, wenn gilt  $\vec{v} \neq \vec{0} \Rightarrow b(\vec{v}, \vec{v}) > 0$ . Ein **Skalarprodukt** auf einem Vektorraum über einem angeordneten Körper ist wie in 4.1.1.2 eine symmetrische positiv definite Bilinearform.

*Beispiel 4.1.3.3.* Auf  $V = \mathbb{R}^n$  erhält man ein Skalarprodukt durch die Vorschrift

$$\langle \vec{v}, \vec{w} \rangle := v_1 w_1 + \dots + v_n w_n$$



Einige Dreiecke, die durch Ähnlichkeiten im Sinne von ?? ineinander überführt werden können. Man nennt sie deshalb auch **ähnliche Dreiecke**.

für  $\vec{v} = (v_1, \dots, v_n)$  und  $\vec{w} = (w_1, \dots, w_n)$ . Es heißt das **Standard-Skalarprodukt**. Man findet für das Standardskalarprodukt oft die alternative Notation  $\vec{v} \cdot \vec{w}$ . Im Formalismus der Matrixmultiplikation und mit unserer Interpretation von Elementen des  $\mathbb{R}^n$  als Spaltenvektoren und Elementen von  $\mathbb{R}$  als reellen  $(1 \times 1)$ -Matrizen können wir es auch schreiben als Produkt eines Zeilenvektors mit einem Spaltenvektor  $\langle \vec{v}, \vec{w} \rangle := \vec{v}^\top \circ \vec{w}$ .

**4.1.3.4 (Motivation für Skalarprodukte im Komplexen).** Für die nun folgende Erweiterung des Begriffs eines Skalarprodukts ins Komplexe kenne ich keine anschauliche Begründung. Es wird sich jedoch erweisen, daß das Zusammenwirken der algebraischen Abgeschlossenheit der komplexen Zahlen mit den Positivitäts-eigenschaften eines Skalarprodukts Resultate liefert, die auch interessante Konsequenzen für reelle Vektorräume haben. Beispiele dafür sind die Sätze über die Normalform orthogonaler Matrizen 4.1.11.3 oder über die Hauptachsentransformation 4.2.2.7.

**Definition 4.1.3.5.** Ein **Skalarprodukt** auf einem komplexen Vektorraum  $V$  ist eine Abbildung  $V \times V \rightarrow \mathbb{C}$ ,  $(\vec{v}, \vec{w}) \mapsto \langle \vec{v}, \vec{w} \rangle$  derart, daß für alle  $\vec{u}, \vec{v}, \vec{w} \in V$  und  $\lambda, \mu \in \mathbb{C}$  gilt:

1.  $\langle \vec{u}, \vec{v} + \vec{w} \rangle = \langle \vec{u}, \vec{v} \rangle + \langle \vec{u}, \vec{w} \rangle$  und  $\langle \vec{v}, \lambda \vec{w} \rangle = \lambda \langle \vec{v}, \vec{w} \rangle$ ;
2.  $\langle \vec{u} + \vec{v}, \vec{w} \rangle = \langle \vec{u}, \vec{w} \rangle + \langle \vec{v}, \vec{w} \rangle$  und  $\langle \mu \vec{v}, \vec{w} \rangle = \bar{\mu} \langle \vec{v}, \vec{w} \rangle$ . Bei Herausziehen eines Skalars  $\mu$  im ersten Eintrag muß also besagter Skalar konjugiert werden;
3.  $\langle \vec{v}, \vec{w} \rangle = \overline{\langle \vec{w}, \vec{v} \rangle}$ , insbesondere also  $\langle \vec{v}, \vec{v} \rangle \in \mathbb{R}$ ;
4.  $\vec{v} \neq \vec{0} \Rightarrow \langle \vec{v}, \vec{v} \rangle > 0$ .

**4.1.3.6.** Nebenbei bemerkt folgt hier 2 schon aus 1 und 3, aber es kann auch nicht schaden, diese Formeln nochmal explizit hinzuschreiben. Ganz allgemein heißt eine Abbildung  $f : V \rightarrow W$  von komplexen Vektorräumen **schiefflinear**, wenn gilt  $f(\vec{v} + \vec{w}) = f(\vec{v}) + f(\vec{w})$  und  $f(\mu \vec{v}) = \bar{\mu} f(\vec{v})$  für alle  $\vec{v}, \vec{w} \in V$  und  $\mu \in \mathbb{C}$ . Die ersten beiden Teile unserer Definition können also dahingehend zusammengefaßt werden, daß unser Skalarprodukt schiefflinear ist im ersten Eintrag und linear im zweiten. Eine Abbildung  $V \times V \rightarrow \mathbb{C}$ , die nur diese beiden Bedingungen 1 und 2 erfüllt, nennt man eine **Sesquilinearform**. Gilt zusätzlich 3, so heißt die Sesquilinearform **hermitesch** nach dem französischen Mathematiker Hermite. Das Standardbeispiel ist  $V = \mathbb{C}^n$  mit dem Skalarprodukt  $\langle \vec{v}, \vec{w} \rangle = \bar{v}_1 w_1 + \dots + \bar{v}_n w_n$  für  $\vec{v} = (v_1, \dots, v_n)$  und  $\vec{w} = (w_1, \dots, w_n)$ . Mithilfe der Matrixmultiplikation kann dies Skalarprodukt auch geschrieben werden als

$$\langle \vec{v}, \vec{w} \rangle = \bar{\vec{v}}^\top \circ \vec{w}$$

Der Strich über einer Matrix mit komplexen Einträgen meint dabei das komplexe Konjugieren aller Einträge.

**4.1.3.7 (Diskussion der Terminologie).** Viele Autoren verwenden die abweichende Konvention, nach der im komplexen Fall ein Skalarprodukt linear im ersten und schieflinear im zweiten Eintrag sein soll. Ich ziehe die hier gegebene Konvention vor, da dann bei der Interpretation von  $\langle \vec{v}, \vec{w} \rangle$  als „ $\vec{v}$  auf  $\vec{w}$  angewendet“ dieses Anwenden von  $\vec{v}$  linear ist. In der physikalischen Literatur findet man meist die abweichende Notation  $\langle \vec{v} | \vec{w} \rangle$ .

**Definition 4.1.3.8.** Einen reellen beziehungsweise komplexen Vektorraum mit Skalarprodukt nennen wir einen reellen beziehungsweise komplexen **Skalarproduktraum**. In einem reellen oder komplexen Skalarproduktraum definiert man die **Skalarproduktnorm** oder kurz **Norm**  $\|\vec{v}\| \in \mathbb{R}$  eines Vektors  $\vec{v}$  durch die Formel

$$\|\vec{v}\| := \sqrt{\langle \vec{v}, \vec{v} \rangle}$$

Vektoren  $\vec{v}$  der Norm  $\|\vec{v}\| = 1$  heißen **normal**. Mit dem **Abstand** zwischen zwei Vektoren  $\vec{v}, \vec{w}$  meinen wir die Norm  $\|\vec{v} - \vec{w}\|$  ihrer Differenz. Zwei Vektoren  $\vec{v}, \vec{w}$  heißen **orthogonal** und man schreibt  $\vec{v} \perp \vec{w}$ , wenn gilt  $\langle \vec{v}, \vec{w} \rangle = 0$ . Man sagt dann auch,  $\vec{v}$  und  $\vec{w}$  **stehen senkrecht aufeinander**. Manchmal verwendet man das Symbol  $\perp$  auch für allgemeinere Teilmengen  $A, B$  eines Skalarproduktraums und schreibt  $A \perp B$  als Abkürzung für die Aussage ( $\vec{v} \perp \vec{w} \forall \vec{v} \in A, \vec{w} \in B$ ).

**4.1.3.9.** In einem reellen oder komplexen Skalarproduktraum gilt  $\|\lambda \vec{v}\| = |\lambda| \|\vec{v}\|$  für alle Vektoren  $\vec{v}$  und alle Skalare  $\lambda \in \mathbb{R}$  beziehungsweise  $\lambda \in \mathbb{C}$ . In der Tat haben wir ja

$$\|\lambda \vec{v}\|^2 = \langle \lambda \vec{v}, \lambda \vec{v} \rangle = \bar{\lambda} \lambda \langle \vec{v}, \vec{v} \rangle = |\lambda|^2 \|\vec{v}\|^2$$

**4.1.3.10.** Einen komplexen Skalarproduktraum nennt man einen **unitären Raum** und im Kontext der Definition allgemeiner Hilberträume auch einen **Prähilbertraum** oder im endlichdimensionalen Fall einen **endlichdimensionalen Hilbertraum**.

**Vorschau 4.1.3.11 (Diskussion der Terminologie).** Einen reellen Skalarproduktraum nennt man vielfach einen „euklidischen Vektorraum“. Ich schließe mich dieser Terminologie nicht an und erkläre stattdessen einen euklidischen Vektorraum in 4.1.5.1 als einen reellen Vektorraum mit einem „nur bis auf einen Skalar eindeutig bestimmten Skalarprodukt“.

**4.1.3.12.** Stehen zwei Vektoren  $\vec{v}, \vec{w}$  eines Skalarproduktraums senkrecht aufeinander, so gilt der **Satz des Pythagoras**

$$\|\vec{v} + \vec{w}\|^2 = \|\vec{v}\|^2 + \|\vec{w}\|^2$$

In der Tat folgt ja aus  $\vec{v} \perp \vec{w}$  schon

$$\langle \vec{v} + \vec{w}, \vec{v} + \vec{w} \rangle = \langle \vec{v}, \vec{v} \rangle + \langle \vec{v}, \vec{w} \rangle + \langle \vec{w}, \vec{v} \rangle + \langle \vec{w}, \vec{w} \rangle = \langle \vec{v}, \vec{v} \rangle + \langle \vec{w}, \vec{w} \rangle$$

Im Reellen gilt hier auch die Umkehrung. Im Komplexen ist dahingegen die Identität  $\|\vec{v} + \vec{w}\|^2 = \|\vec{v}\|^2 + \|\vec{w}\|^2$  gleichbedeutend zu  $\operatorname{Re}\langle \vec{w}, \vec{v} \rangle = 0$ .

**Definition 4.1.3.13.** Eine Familie  $(\vec{v}_i)_{i \in I}$  von Vektoren eines Skalarproduktraums heißt ein **Orthonormalsystem**, wenn die Vektoren  $\vec{v}_i$  alle die Norm 1 haben und paarweise aufeinander senkrecht stehen, wenn also in Formeln mit dem Kronecker-delta aus 3.2.4.2 gilt

$$\langle \vec{v}_i, \vec{v}_j \rangle = \delta_{ij}$$

Ein Orthonormalsystem, das eine Basis ist, heißt eine **Orthonormalbasis**.

4.1.3.14. Eine Teilmenge  $T$  eines Skalarproduktraums heißt ein **Orthonormal-system** beziehungsweise eine **Orthonormalbasis**, wenn die Vektoren von  $T$  alle die Norm 1 haben, paarweise aufeinander senkrecht stehen und im Fall einer Orthonormalbasis zusätzlich eine Basis bilden. Das bedeutet in anderen Worten, daß unsere Teilmenge als durch sich selbst indizierte Familie die jeweilige in 4.1.3.13 für Familien formulierte Eigenschaft hat.

4.1.3.15. Ist  $V$  ein Skalarproduktraum und  $(\vec{v}_i)_{i \in I}$  ein Orthonormalsystem und  $\vec{w} = \sum \lambda_i \vec{v}_i$  die Darstellung eines Vektors  $\vec{w} \in V$ , so erhalten wir durch Davor-multiplizieren von  $\vec{v}_j$  sofort  $\lambda_j = \langle \vec{v}_j, \vec{w} \rangle$ . Insbesondere ist jedes Orthonormalsystem linear unabhängig.

**Proposition 4.1.3.16.** Jeder endlichdimensionale reelle oder komplexe Skalarprodukt Raum besitzt eine Orthonormalbasis.

*Beweis.* Ist unser Raum der Nullraum, so tut es die leere Menge. Sonst finden wir einen von Null verschiedenen Vektor und erhalten, indem wir ihn mit dem Kehrwert seiner Norm multiplizieren, sogar einen Vektor  $\vec{v}_1$  der Norm Eins. Die lineare Abbildung  $\langle \vec{v}_1, \cdot \rangle$  ist nicht die Nullabbildung und hat folglich nach der Dimensionsformel 3.2.2.5 als Kern einen Untervektorraum einer um Eins kleineren Dimension. Eine offensichtliche Induktion beendet den Beweis.  $\square$

4.1.3.17. Gegeben ein Skalarproduktraum  $V$  und eine Teilmenge  $T \subset V$  setzen wir

$$T^\perp := \{v \in V \mid v \perp t \ \forall t \in T\}$$

und nennen diese Menge den **Orthogonalraum** von  $T$  in  $V$ . Offensichtlich ist der Orthogonalraum einer beliebigen Teilmenge  $T \subset V$  ein Untervektorraum von  $V$ .

**Proposition 4.1.3.18 (Orthogonales Komplement).** Gegeben ein Skalarprodukt Raum  $V$  und ein endlichdimensionaler Untervektorraum  $U \subset V$  ist der Orthogonalraum von  $U$  in  $V$  auch ein Vektorraumkomplement, in Formeln

$$V = U \oplus U^\perp$$

*Ergänzung 4.1.3.19.* Die Proposition gilt auch für Skalarprodukträume über einem beliebigen angeordneten Körper. Der Beweis muß für diesen Fall allerdings umgeschrieben werden, da in dieser Allgemeinheit auch ein endlichdimensionaler Skalarproduktraum nicht notwendig eine Orthonormalbasis hat.

*Beweis.* Natürlich gilt  $U \cap U^\perp = 0$ . Es reicht also zu zeigen, daß jeder Vektor  $\vec{w} \in V$  dargestellt werden kann als

$$\vec{w} = \vec{p} + \vec{r}$$

mit  $\vec{p} \in U$  und  $\vec{r} \in U^\perp$ . Nach 4.1.3.16 besitzt nun  $U$  eine Orthonormalbasis  $\vec{v}_1, \dots, \vec{v}_n$ . Machen wir den Ansatz  $\vec{p} = \sum \lambda_i \vec{v}_i$ , so folgt  $\langle \vec{v}_i, \vec{w} \rangle = \langle \vec{v}_i, \vec{p} \rangle = \lambda_i$  und damit die Eindeutigkeit von  $\vec{p}$ . Andererseits steht aber mit diesen  $\lambda_i$  der Vektor  $\vec{r} = \vec{w} - \sum \lambda_i \vec{v}_i$  auch tatsächlich senkrecht auf allen  $\vec{v}_i$ , denn wir finden

$$\langle \vec{v}_j, \vec{r} \rangle = \langle \vec{v}_j, \vec{w} \rangle - \sum \lambda_i \langle \vec{v}_j, \vec{v}_i \rangle = \langle \vec{v}_j, \vec{w} \rangle - \lambda_j = 0 \quad \square$$

4.1.3.20. Sagen wir von zwei Untervektorräumen eines Skalarproduktraums, sie seien **orthogonal**, so ist gemeint, daß jeder Vektor des einen Teilraums zu jedem Vektor des anderen Teilraums orthogonal ist.

4.1.3.21. Gegeben  $U \subset V$  ein Untervektorraum eines Skalarproduktraums verstehen wir unter einem **orthogonalen Komplement** von  $U$  in  $V$  einen Untervektorraum  $W \subset V$ , der sowohl ein Vektorraumkomplement ist als auch orthogonal zu  $U$ . Wenn es ein derartiges orthogonales Komplement gibt, muß es offensichtlich der Orthogonalraum  $W = U^\perp$  sein. Es kann aber im Fall unendlichdimensionaler Skalarprodukträume durchaus vorkommen, daß der Orthogonalraum von  $U$  kein Vektorraumkomplement ist und daß damit der Untervektorraum  $U$  kein orthogonales Komplement besitzt. Ein Beispiel dafür gibt Übung 4.1.3.29.

4.1.3.22. Besitzt ein Untervektorraum eines Skalarproduktraums  $U \subset V$  ein orthogonales Komplement, haben wir also  $V = U \oplus U^\perp$ , so kann jeder Vektor  $\vec{w} \in V$  eindeutig geschrieben werden als  $\vec{w} = \vec{p} + \vec{r}$  mit  $\vec{p} \in U$  und  $\vec{r} \in U^\perp$ . Die Abbildung  $\vec{w} \mapsto \vec{p}$  ist dann offensichtlich linear und heißt die **orthogonale Projektion** auf den Untervektorraum  $U$ . Sie ist in der Terminologie von 3.2.2.19 die Projektion auf  $U$  längs  $U^\perp$ . Man beachte, daß die orthogonale Projektion von  $\vec{w}$  auf  $U$  genau derjenige Punkt  $\vec{p}$  unseres Untervektorraums  $U$  ist, der den kleinsten Abstand zu  $\vec{w}$  hat. Für jeden Vektor  $\vec{v} \neq \vec{0}$  aus unserem Untervektorraum gilt nämlich nach Pythagoras

$$\|(\vec{p} + \vec{v}) - \vec{w}\|^2 = \|\vec{p} - \vec{w}\|^2 + \|\vec{v}\|^2 > \|\vec{p} - \vec{w}\|^2$$

*Vorschau 4.1.3.23.* Man beachte, daß unsere orthogonale Projektion mit Ausnahme des Extremfalls  $U = V$  keineswegs eine orthogonale Abbildung im Sinne von 4.1.4.1 ist.

**Satz 4.1.3.24.** 1. Für beliebige Vektoren  $\vec{v}, \vec{w}$  eines reellen oder komplexen Skalarproduktraums gilt die **Cauchy-Schwarz'sche Ungleichung**

$$|\langle \vec{v}, \vec{w} \rangle| \leq \|\vec{v}\| \|\vec{w}\|$$

mit Gleichheit genau dann, wenn  $\vec{v}$  und  $\vec{w}$  linear abhängig sind;

2. Für beliebige Vektoren  $\vec{v}, \vec{w}$  eines reellen oder komplexen Skalarproduktraums gilt die **Dreiecksungleichung**

$$\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$$

mit Gleichheit genau dann, wenn einer unserer Vektoren ein nichtnegatives Vielfaches des anderen ist, in Formeln  $\vec{v} \in \mathbb{R}_{\geq 0} \vec{w}$  oder  $\vec{w} \in \mathbb{R}_{\geq 0} \vec{v}$ .

*Ergänzung 4.1.3.25.* Dieser Satz zeigt insbesondere, daß unsere Skalarprodukt-norm auch im Sinne der Analysis ?? eine Norm ist.

4.1.3.26 (**Verschiedene Ansätze zum Beweis der Dreiecksungleichung**). Man mag versucht sein, die Dreiecksungleichung zu beweisen, indem man eine Ecke des Dreiecks orthogonal auf die gegenüberliegende Kante projiziert und bemerkt, daß die beiden anderen Kanten dabei nach Pythagoras nur kürzer werden können. Leider führt diese anschaulich besonders überzeugende Beweisidee bei der Ausformulierung in ein unangenehmes Dickicht von Fallunterscheidungen, so daß ich die im folgenden gegebene weniger anschauliche Darstellung vorgezogen habe.

*Beweis.* Um Teil 1 zu zeigen, nehmen wir zunächst  $\|\vec{v}\| = 1$  an. Das Bild  $\vec{p}$  eines weiteren Vektors  $\vec{w}$  unter der orthogonalen Projektion auf die Gerade  $\mathbb{R}\vec{v}$  wird dann nach 4.1.3.18 oder genauer seinem Beweis gegeben durch die Formel  $\vec{p} = \langle \vec{v}, \vec{w} \rangle \vec{v}$ . Erklären wir  $\vec{r}$  durch  $\vec{w} = \vec{p} + \vec{r}$ , so steht demnach oder auch nach elementarer Rechnung  $\vec{r}$  senkrecht auf  $\vec{v}$  und wir erhalten unter Zuhilfenahme des Pythagoras

$$|\langle \vec{v}, \vec{w} \rangle|^2 = \|\vec{p}\|^2 \leq \|\vec{p}\|^2 + \|\vec{r}\|^2 = \|\vec{w}\|^2$$

Das zeigt die Ungleichung  $|\langle \vec{v}, \vec{w} \rangle| \leq \|\vec{v}\| \|\vec{w}\|$  mit Gleichheit genau dann, wenn gilt  $\vec{r} = \vec{0}$  alias wenn  $\vec{w}$  ein Vielfaches von  $\vec{v}$  ist. Diese Ungleichung muß aber offensichtlich erhalten bleiben, wenn wir darin  $\vec{v}$  durch ein Vielfaches ersetzen, und so erhalten wir dann für beliebige Vektoren  $\vec{v}, \vec{w}$  eines beliebigen Skalarproduktraums die Cauchy-Schwarz'sche Ungleichung  $|\langle \vec{v}, \vec{w} \rangle| \leq \|\vec{v}\| \|\vec{w}\|$  mit

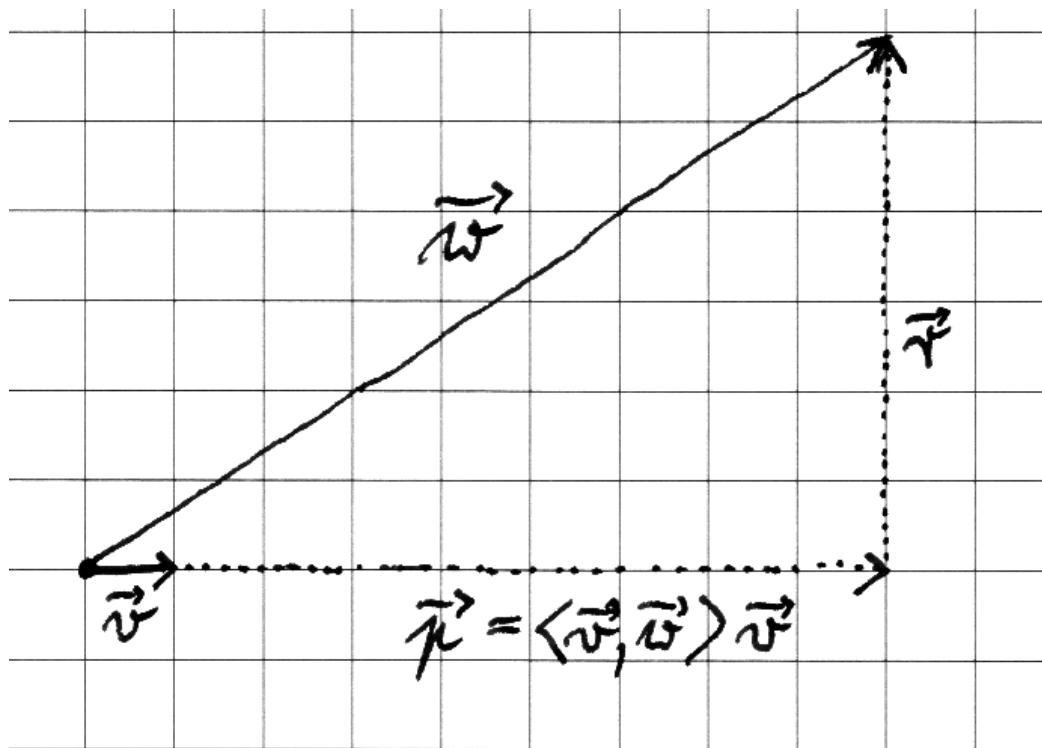


Illustration zum Beweis der Cauchy-Schwarz'schen Ungleichung. Wir haben darin  $\vec{v} = (1, 0)$ ,  $\vec{w} = (9, 6)$ ,  $\langle \vec{v}, \vec{w} \rangle = 9$ ,  $\vec{p} = (9, 0)$ ,  $\vec{r} = (0, 6)$ .

Gleichheit genau dann, wenn  $\vec{v}$  und  $\vec{w}$  linear abhängig sind. Daraus hinwiederum ergibt sich, indem man beide Seiten quadriert, sofort die Dreiecksungleichung  $\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$ . Der Beweis der letzten Aussage von Teil 2 sei dem Leser zur Übung überlassen.  $\square$

*Alternativer Beweis der Ungleichung von Cauchy-Schwarz.* Man findet

$$f(t) := \langle \vec{v} + t\vec{w}, \vec{v} + t\vec{w} \rangle = \langle \vec{v}, \vec{v} \rangle + 2t \operatorname{Re} \langle \vec{v}, \vec{w} \rangle + t^2 \langle \vec{w}, \vec{w} \rangle \geq 0 \quad \forall t \in \mathbb{R}$$

Aus  $\langle \vec{w}, \vec{w} \rangle = 0$  folgt  $\operatorname{Re} \langle \vec{v}, \vec{w} \rangle = 0$  für alle  $\vec{v}$ . Haben wir  $\langle \vec{w}, \vec{w} \rangle \neq 0$ , so findet man das Minimum unserer Funktion von  $t$  mit Hilfe der Bedingung  $f'(t_0) = 0$  bei  $t_0 = -\operatorname{Re} \langle \vec{v}, \vec{w} \rangle / \|\vec{w}\|^2$ . Aus  $f(t_0) \geq 0$  folgt dann unmittelbar die Cauchy-Schwarz'sche Ungleichung. Ich selbst ziehe den anderen Beweis vor, weil er meine Anschauung mehr anspricht und ähnlich für alle angeordneten Grundkörper funktioniert. Der zweite Beweis lässt sich dahingegen leichter auf „positiv semidefinite hermitesche Formen“ verallgemeinern.  $\square$

4.1.3.27. Ist  $V$  ein Skalarproduktraum und  $\vec{v}_1, \dots, \vec{v}_n$  ein endliches Orthonormalsystem, so gilt für jeden Vektor  $\vec{w} \in V$  die sogenannte **Bessel'sche Ungleichung**

$$\|\vec{w}\|^2 \geq \sum_{i=1}^n |\langle \vec{v}_i, \vec{w} \rangle|^2$$

In der Tat ist nach Pythagoras für jeden Vektor  $\vec{w} \in V$  seine orthogonale Projektion  $\vec{p}$  auf den von unserem Orthonormalsystem erzeugten Teilraum höchstens so lang wie der Vektor selbst, in Formeln  $\|\vec{w}\| \geq \|\vec{p}\|$  alias  $\|\vec{w}\|^2 \geq \|\vec{p}\|^2$ . Setzen wir in diese Erkenntnis unsere Darstellung  $\vec{p} = \sum \langle \vec{v}_i, \vec{w} \rangle \vec{v}_i$  der orthogonalen Projektion aus dem Beweis von 4.1.3.18 ein, so ergibt sich unsere Ungleichung.

## Übungen

*Übung 4.1.3.28.* Gegeben ein Skalarproduktraum  $V$  mit einem endlichdimensionalen Untervektorraum  $U \subset V$  gilt  $U = (U^\perp)^\perp$ .

*Ergänzende Übung 4.1.3.29 (Schwierigkeiten mit orthogonalen Projektionen).* Man zeige, daß die Menge  $L^2_{\mathbb{R}}(\mathbb{N}) \subset \operatorname{Ens}(\mathbb{N}, \mathbb{R})$  aller reellen Folgen  $a_0, a_1, \dots$  mit  $\sum a_i^2 < \infty$  im Raum aller Folgen einen Untervektorraum bildet und daß wir auf diesem Untervektorraum durch die Vorschrift  $\langle (a_i), (b_i) \rangle = \sum a_i b_i$  ein Skalarprodukt einführen können. Dann betrachte man in  $L^2_{\mathbb{R}}(\mathbb{N})$  den Untervektorraum  $U$  aller Folgen mit höchstens endlich vielen von Null verschiedenen Folgengliedern und zeige  $U^\perp = 0$ . Insbesondere ist in diesem Fall  $U^\perp$  kein orthogonales Komplement zu  $U$ . Proposition 4.1.3.18 gilt also im allgemeinen nicht mehr, wenn wir unendlichdimensionale Untervektorräume  $U$  betrachten. Sie gilt jedoch wieder und sogar genau dann, wenn besagte Untervektorräume  $U$  zusätzlich „vollständig“ sind, vergleiche ??.

*Übung 4.1.3.30.* Man zeige, daß die Cauchy-Schwarz'sche Ungleichung allgemeiner für jede hermitesche Sesquilinearform gilt, bei der das Produkt eines Vektors mit sich selbst nie negativ ist.

*Übung 4.1.3.31.* Ist  $V$  ein reeller Skalarproduktraum und  $(\vec{v}_1, \dots, \vec{v}_n)$  eine Orthonormalbasis und  $\Phi : \mathbb{R}^n \xrightarrow{\sim} V$  der zugehörige Vektorraumisomorphismus nach 3.1.6.13, so entspricht unter  $\Phi$  das Standardskalarprodukt auf dem  $\mathbb{R}^n$  dem vorgegebenen Skalarprodukt auf  $V$ , in Formeln  $\langle x, y \rangle = \langle \Phi(x), \Phi(y) \rangle$  für alle  $x, y \in \mathbb{R}^n$ . Dasselbe gilt entsprechend im Komplexen und auch allgemeiner für Orthonormalsysteme, bei denen  $\Phi$  dann den Homomorphismus  $x \mapsto x_1 \vec{v}_1 + \dots + x_n \vec{v}_n$  meint und kein Isomorphismus zu sein braucht.

*Übung 4.1.3.32.* Man zeige, daß für einen Skalarproduktraum über einem beliebigen angeordneten Körper immer noch die Variante

$$\langle \vec{v}, \vec{w} \rangle^2 \leq \langle \vec{v}, \vec{v} \rangle \langle \vec{w}, \vec{w} \rangle$$

der Cauchy-Schwarz'schen Ungleichung gilt mit Gleichheit genau dann, wenn  $\vec{v}$  und  $\vec{w}$  linear abhängig sind.

#### 4.1.4 Orthogonale und unitäre Abbildungen

**Definition 4.1.4.1.** Eine Abbildung  $f : V \rightarrow W$  von Skalarprodukträumen heißt **skalarproduktverträglich** oder **orthogonal** im Reellen und **unitär** im Komplexen, wenn sie linear ist und das Skalarprodukt erhält, in Formeln

$$\langle f(v), f(w) \rangle = \langle v, w \rangle \quad \forall v, w \in V$$

4.1.4.2. Bisher hatten wir die Orthogonalität linearer Abbildungen nur im Fall von Automorphismen von Skalarprodukträumen eingeführt. In der vorgehenden Definition dehnen wir diesen Begriff auf den Fall von Homomorphismen zwischen Skalarprodukträumen aus.

**Lemma 4.1.4.3 (Kriterien für die Orthogonalität einer linearen Abbildung).** *Für eine lineare Abbildung von einem endlichdimensionalen reellen oder komplexen Skalarproduktraum in einen weiteren Skalarproduktraum über demselben Grundkörper sind gleichbedeutend:*

1. *Unsere Abbildung überführt eine Orthonormalbasis des Ausgangsraums in ein Orthonormalsystem;*
2. *Unsere Abbildung überführt jede Orthonormalbasis des Ausgangsraums in ein Orthonormalsystem;*
3. *Unsere Abbildung ist orthogonal beziehungsweise unitär.*

*Beweis.*  $3 \Rightarrow 2 \Rightarrow 1$  sind offensichtlich und wir müssen nur noch  $1 \Rightarrow 3$  zeigen. Bezeichne dazu  $f : V \rightarrow W$  unsere Abbildung und  $B \subset V$  eine Orthonormalbasis, die es nach 4.1.3.16 geben muß, da wir den Ausgangsraum unserer Abbildung endlichdimensional angenommen hatten. Es gilt zu zeigen  $\langle f(v), f(w) \rangle = \langle v, w \rangle \forall v, w \in V$ . Wir wissen nach Annahme bereits, daß das gilt für alle  $v, w \in B$ . Da beide Seiten bilinear beziehungsweise sesquilinear sind als Abbildungen  $V \times V \rightarrow \mathbb{R}$  beziehungsweise  $V \times V \rightarrow \mathbb{C}$ , folgt es dann jedoch leicht für alle  $v, w \in V$ .  $\square$

**Definition 4.1.4.4.** Gegeben ein reeller Skalarproduktraum  $V$  bilden die orthogonalen Automorphismen von  $V$  eine Untergruppe der  $\mathrm{GL}(V)$ , die wir  $\mathrm{O}(V)$  notieren. Gegeben ein komplexer Skalarproduktraum  $V$  bilden die unitären Automorphismen von  $V$  eine Untergruppe der  $\mathrm{GL}(V)$ , die wir  $\mathrm{U}(V)$  notieren.

**Definition 4.1.4.5.** Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem Körper  $K$  bilden die Automorphismen von  $V$  mit Determinante Eins eine Untergruppe der Gruppe aller Automorphismen von  $V$ . Sie heißt die **spezielle lineare Gruppe** zu  $V$  und wird

$$\mathrm{SL}(V) \subset \mathrm{GL}(V)$$

notiert. Im Fall  $V = K^n$  schreibt man auch  $\mathrm{SL}(n; K) \subset \mathrm{GL}(n; K)$ .

**Definition 4.1.4.6.** Für jeden endlichdimensionalen reellen Skalarproduktraum  $V$  bezeichne  $\mathrm{SO}(V) \subset \mathrm{GL}(V)$  die Untergruppe aller orthogonalen Automorphismen mit Determinante Eins. Sie heißt die **spezielle orthogonale Gruppe** von  $V$ .

**Definition 4.1.4.7.** Für einen endlichdimensionalen komplexen Skalarproduktraum  $V$  bezeichnet  $\mathrm{SU}(V) \subset \mathrm{GL}(V)$  die Untergruppe aller unitären Automorphismen mit Determinante Eins. Sie heißt die **spezielle unitäre Gruppe** von  $V$ .

**Satz 4.1.4.8 (Klassifikation endlichdimensionaler Skalarprodukträume).** 1.

*Zwischen je zwei reellen Skalarprodukträumen derselben endlichen Dimension gibt es einen orthogonalen Isomorphismus. Zu jeder Dimension gibt es einen reellen Skalarproduktraum;*

2. *Zwischen je zwei komplexen Skalarprodukträumen derselben endlichen Dimension gibt es einen unitären Isomorphismus. Zu jeder Dimension gibt es einen komplexen Skalarproduktraum.*

*Beweis.* Wir wählen mit 4.1.3.16 in beiden Räumen jeweils eine Orthonormalbasis und erklären unseren Isomorphismus durch die Vorschrift, daß er von einer beliebig gewählten Bijektion zwischen den entsprechenden Basen herkommen soll. Nach 4.1.4.3 ist er dann orthogonal beziehungsweise unitär.  $\square$

**Satz 4.1.4.9.** 1. (**Matrizen orthogonaler Endomorphismen**). Eine Matrix  $A \in \text{Mat}(n; \mathbb{R})$  beschreibt einen orthogonalen Endomorphismus des  $\mathbb{R}^n$  mit seinem Standardskalarprodukt genau dann, wenn ihre Transponierte ihre Inverse ist. In Formeln gilt also

$$(A \circ) \in O(\mathbb{R}^n) \Leftrightarrow A^\top A = I$$

2. (**Matrizen unitärer Endomorphismen**). Eine Matrix  $A \in \text{Mat}(n; \mathbb{C})$  beschreibt einen unitären Endomorphismus des  $\mathbb{C}^n$  mit seinem Standardskalarprodukt genau dann, wenn die Konjugierte ihrer Transponierten ihre Inverse ist. In Formeln gilt also

$$(A \circ) \in U(\mathbb{C}^n) \Leftrightarrow \bar{A}^\top A = I$$

*Beispiel 4.1.4.10.* Eine komplexe  $(1 \times 1)$ -Matrix ist unitär genau dann, wenn ihr einziger Eintrag eine komplexe Zahl vom Absolutbetrag Eins ist, also in der komplexen Zahlenebene auf dem Einheitskreis liegt.

*Beweis.* Wir zeigen gleich den komplexen Fall. Die Identität  $\langle Av, Aw \rangle = \langle v, w \rangle$  ist nach unserer Interpretation des Skalarprodukts in Termen der Matrixmultiplikation in 4.1.3.6 gleichbedeutend zu  $(\bar{A}v)^\top (Aw) = \bar{v}^\top w$  alias zu  $\bar{v}^\top \bar{A}^\top Aw = \bar{v}^\top w$ . Gilt  $\bar{A}^\top A = I$ , so stimmt das natürlich für alle  $v, w \in \mathbb{C}^n$ . Stimmt es umgekehrt für alle  $v, w \in \mathbb{C}^n$ , so insbesondere auch für die Vektoren der Standardbasis  $e_i, e_j$ . Damit erhalten wir von der Mitte ausgehend die Gleichungskette  $(\bar{A}^\top A)_{ij} = e_i^\top \bar{A}^\top A e_j = e_i^\top e_j = \delta_{ij} \forall i, j$  alias  $\bar{A}^\top A = I$ .  $\square$

**Definition 4.1.4.11.** Eine reelle Matrix  $A \in \text{Mat}(n; \mathbb{R})$  heißt **orthogonal**, wenn gilt  $A^\top A = I$ . Eine komplexe Matrix  $A \in \text{Mat}(n; \mathbb{C})$  heißt **unitär**, wenn gilt  $\bar{A}^\top A = I$ . Der vorhergehende Satz 4.1.4.9 oder auch direkte Rechnung zeigen, daß diese Matrizen Untergruppen von  $\text{GL}(n; \mathbb{R})$  beziehungsweise  $\text{GL}(n; \mathbb{C})$  bilden. Sie heißen die **orthogonale Gruppe** beziehungsweise die **unitäre Gruppe**.

Man notiert sie

$$O(n) := \{A \in \text{GL}(n; \mathbb{R}) \mid A^\top A = I\}$$

$$U(n) := \{A \in \text{GL}(n; \mathbb{C}) \mid \bar{A}^\top A = I\}$$

Die Notation  $O(n)$  kennen wir bereits aus 4.1.1.5. Die Elemente der orthogonalen beziehungsweise unitären Gruppen mit Determinante Eins bilden jeweils Untergruppen. Sie heißen die die **spezielle orthogonale Gruppe** beziehungsweise die **spezielle unitäre Gruppe**. Man notiert sie

$$SO(n) := \{A \in O(n) \mid \det A = 1\}$$

$$SU(n) := \{A \in U(n) \mid \det A = 1\}$$

Die Gruppe  $SU(2)$  heißt auch die **Spingruppe**.

**4.1.4.12 (Betrag der Determinante orthogonaler oder unitärer Matrizen).** Die Determinante einer unitären oder orthogonalen Matrix hat stets den Betrag Eins. In der Tat folgt aus  $\bar{A}^\top A = I$  unmittelbar

$$1 = \det(\bar{A}^\top A) = \det(\bar{A}^\top) \det(A) = \det(\bar{A}) \det(A) = \overline{\det(A)} \det(A)$$

Wir können insbesondere  $\mathrm{SO}(n)$  auch als die Gruppe aller orientierungserhaltenden orthogonalen Automorphismen des  $\mathbb{R}^n$  beschreiben.

**4.1.4.13 (Eigenwerte orthogonaler oder unitärer Matrizen).** Jeder Eigenwert eines unitären oder orthogonalen Endomorphismus eines Skalarproduktraums hat den Betrag Eins, da derartige Abbildungen die Normen von Vektoren erhalten.

**Satz 4.1.4.14 (Satz vom Fußball).** *Jede orthogonale Selbstabbildung eines dreidimensionalen reellen euklidischen Vektorraums, die die Orientierung erhält, hat mindestens einen von Null verschiedenen Fixvektor.*

4.1.4.15. Anschaulich gesprochen ist unsere Abbildung demnach eine Drehung um eine Drehachse, eben um die von einem Fixvektor erzeugte Gerade. Wird bei einem Fußballspiel der Ball also vor dem Anpfiff zur zweiten Halbzeit wieder in die Mitte gelegt, so befinden sich zwei gegenüberliegende Punkte auf dem Ball jeweils an genau derselben Stelle wie vor dem Anpfiff zur ersten Halbzeit.

*Beweis.* Sei  $D : V \rightarrow V$  unsere Abbildung. Das charakteristische Polynom von  $D$  hat den Leiterterm  $-\lambda^3$  und den konstanten Term  $\det(D) = 1$ . Nach dem Zwischenwertsatz hat es also mindestens eine positive reelle Nullstelle. Da nach 4.1.4.13 als reelle Eigenwerte einer orthogonalen Abbildung nur  $\pm 1$  in Frage kommen, muß diese positive reelle Nullstelle bei 1 liegen. Also ist 1 ein Eigenwert von  $D$  und  $D$  hat einen Fixvektor.  $\square$

## Übungen

*Übung 4.1.4.16 (Variante zum Satz vom Fußball).* Jede orthogonale Selbstabbildung eines dreidimensionalen reellen Skalarproduktraums, die die Orientierung nicht erhält, besitzt einen Eigenvektor zum Eigenwert  $(-1)$ . Hinweis: Man erinnere den Beweis des Satzes vom Fußball 4.1.4.14.

*Übung 4.1.4.17.* Die von den speziellen Elementarmatrizen in  $\mathrm{GL}(n; \mathbb{R})$  erzeugte Untergruppe ist die spezielle lineare Gruppe  $\mathrm{SL}(n; \mathbb{R})$ . Hinweis: Im Fall  $n = 2$  ist etwas Arbeit nötig, der allgemeine Fall ist dann nicht mehr schwer.

*Übung 4.1.4.18 (Orthogonale Endomorphismen des  $\mathbb{R}^3$ ).* Die Gruppe  $\mathrm{SO}(3)$  besteht anschaulich gesprochen aus allen Drehungen des „Koordinatenraums“ um den Ursprung. Ist genauer  $V$  ein dreidimensionaler reeller Skalarproduktraum,

so hat jedes  $U \in \mathrm{SO}(V)$  in einer geeigneten Orthonormalbasis eine Matrix der Gestalt

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & s & c \end{pmatrix}$$

mit  $s^2 + c^2 = 1$ . Hinweis: Satz vom Fußball 4.1.4.14. Man zeige weiter, etwa mit Hilfe von 4.1.4.16: Nicht orientierungstreue orthogonale Selbstabbildungen des  $\mathbb{R}^3$  können stets dargestellt werden als eine Drehung gefolgt von einer Spiegelung an der zur Drehachse senkrechten Ebene. In anderen Worten haben sie in einer geeigneten Orthonormalbasis für geeignete  $s, c$  mit  $s^2 + c^2 = 1$  eine Matrix der Gestalt

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & c & -s \\ 0 & s & c \end{pmatrix}$$

*Übung 4.1.4.19.* Man zeige, daß wir einen Isomorphismus  $S^1 \xrightarrow{\sim} \mathrm{SO}(2)$  erhalten durch die Abbildungsvorschrift  $z \mapsto {}_{(1,i)}[z \cdot]_{(1,i)}$  alias die Abbildung, die  $z \in S^1 \subset \mathbb{C}$  die Matrix der  $\mathbb{R}$ -linearen Abbildung  $(z \cdot) : \mathbb{C} \rightarrow \mathbb{C}$  bezüglich der angeordneten  $\mathbb{R}$ -Basis  $(1, i)$  des  $\mathbb{R}$ -Vektorraums  $\mathbb{C}$  zuordnet.

*Übung 4.1.4.20.* Gegeben ein zweidimensionaler reeller Skalarproduktraum  $Z$  ist die Gruppe  $\mathrm{SO}(Z)$  kommutativ und für  $s \in \mathrm{O}(Z) \setminus \mathrm{SO}(Z)$  gilt  $s^2 = 1$  sowie  $srs^{-1} = r^{-1} \forall r \in \mathrm{SO}(Z)$ . Hinweis: Wenn man eine geometrische Argumentation sucht, mag es geschickt sein, mit dem Beweis der letzteren Aussagen zu beginnen.

*Übung 4.1.4.21.* Gegeben zwei Strahlen in einem reellen Skalarproduktraum gibt es stets einen orthogonalen Automorphismus unseres Raums, der den einen Strahl in den anderen überführt.

## 4.1.5 Euklidische Räume

4.1.5.1. Eine **euklidische Struktur** auf einem reellen Vektorraum  $V$  ist ein eindimensionaler Untervektorraum  $S \subset \mathrm{Bil}(V)$ , der mindestens ein Skalarprodukt enthält. Einen **euklidischen Vektorraum** erklären wir als einen reellen Vektorraum mit einer ausgezeichneten euklidischen Struktur. Unter einem **euklidischen Raum** verstehen wir einen reellen affinen Raum mit einer ausgezeichneten euklidischen Struktur auf seinem Richtungsraum. Eine **euklidische Ebene**  $(E, S)$  ist ein zweidimensionaler euklidischer Raum.

4.1.5.2 (**Diskussion der Terminologie**). In der Literatur versteht man unter einem „euklidischen Vektorraum“ für gewöhnlich das, was wir einen Skalarproduktraum nennen, also einen reellen Vektorraum mit einem ausgezeichneten Skalarprodukt. Ich denke jedoch, daß die hier gewählte Terminologie Euklid eher gerecht wird, in

dessen wegweisender geometrisch-axiomatischer Modellierung der Ebene keine „Strecke der Länge Eins“ vorkommt.

*Vorschau 4.1.5.3.* In anderen Zusammenhängen werden wir später auch euklidische Räume über beliebigen angeordneten Körpern betrachten. In der linearen Algebra will ich diesen Begriff jedoch auf den Fall des Grundkörpers der reellen Zahlen beschränken. Wenn das besonders betont werden soll, rede ich von einem „reellen euklidischen Raum“.

**4.1.5.4.** Gegeben ein euklidischer Vektorraum  $(V, S)$  setzen wir ganz allgemein  $O(V, S) = O(V, s)$  für ein und jedes Skalarprodukt  $s \in S$  und nennen diese Gruppe die **orthogonale Gruppe** unseres euklidischen Vektorraums. Die Elemente dieser Gruppe nennen wir die **orthogonalen Automorphismen von  $V$** . Gegeben ein euklidischer Raum  $(E, S)$  verstehen wir unter einem **orthogonalaffinen Automorphismus von  $E$**  eine Affinität mit orthogonalem linearen Anteil und notieren die Gruppe aller orthogonalaffinen Automorphismen  $O_{\text{aff}}(E, S)$ .

*Beispiele 4.1.5.5.* Ein nulldimensionaler reeller Vektorraum besitzt gar keine euklidische Struktur. Ein eindimensionaler reeller Vektorraum besitzt genau eine euklidische Struktur. Zweidimensionale euklidische Räume diskutieren wir gleich in 4.1.5.7. Ein besonders relevantes schmutziges Beispiel für einen dreidimensionalen euklidischen Raum wird der „Raum unserer Anschauung“ werden mit der in 4.1.6 konstruierten euklidischen Struktur der „unter allen Bewegungen invarianten Bilinearformen“. Die Vorgabe einer euklidischen Struktur erlaubt im allgemeinen die Definition von Winkeln und von „orthogonalen Projektionen“. Sie erlaubt es jedoch nicht, Vektoren in natürlicher Weise eine reelle Zahl als ihre „Norm“ zuzuordnen. Vielmehr muß dazu erst eine „Längeneinheit“ gewählt werden, wie in 4.1.5.12 genauer diskutiert wird.

**4.1.5.6 (Drehspiegelgruppen und euklidische Strukturen).** Für jeden zweidimensionalen reellen Vektorraum  $Z$  erhalten wir zueinander inverse Bijektionen

$$\{\text{Euklidische Strukturen } S \subset \text{Bil}(Z)\} \xleftrightarrow{\sim} \{\text{Drehspiegelgruppen } O \subset \text{GL}(Z)\}$$

dadurch, daß wir jeder euklidischen Struktur  $S$  ihre orthogonale Gruppe  $O(Z, S)$  zuordnen und umgekehrt jeder Drehspiegelgruppe  $O$  die Menge  $S_O$  der unter allen Gruppenelementen invarianten Bilinearformen. Diese Aussage ist nur eine Umformulierung von Satz 4.1.2.8 über invariante Skalarprodukte zu Drehspiegelgruppen und Proposition 4.1.2.10 von Drehspiegelgruppen als orthogonale Gruppen in der Terminologie der euklidischen Strukturen.

**4.1.5.7 (Kongruenzebenen und euklidische Ebenen).** Für jeden zweidimensionalen reellen affinen Raum  $E$  erhalten wir zueinander inverse Bijektionen

$$\{\text{Euklidische Strukturen } S \subset \text{Bil}(\vec{E})\} \xleftrightarrow{\sim} \{\text{Kongruenzgruppen } K \subset \text{Aff}^\times(E)\}$$

dadurch, daß wir jeder Struktur  $S$  ihre orthogonalaffine Gruppe  $O_{\text{aff}}(E, S)$  zuordnen und umgekehrt jeder Kongruenzgruppe  $K$  die Menge  $S_K$  der unter ihren linearen Anteilen invarianten Bilinearformen. Diese Aussage ist nur eine Umformulierung von Korollar 4.1.2.9 über invariante Skalarprodukte zu Kongruenzgruppen und Korollar 4.1.2.11 von Kongruenzgruppen als orthogonalaffine Gruppen in unsere neue Terminologie der euklidischen Strukturen. In diesem Sinne sind unsere beiden Konzepte also zwei Seiten derselben Medaille. Die eine ist algebraischen Rechnungen besser zugänglich, die andere spricht eher die geometrische Anschauung an.

4.1.5.8. Eine lineare Abbildung von euklidischen Vektorräumen heißt **euklidisch**, wenn sie injektiv ist und jedes Skalarprodukt der euklidischen Struktur des Zielraums zu einem Skalarprodukt der euklidischen Struktur des Ausgangsraums einschränkt. Jeder von Null verschiedene Teilraum eines euklidischen Vektorraums besitzt genau eine euklidische Struktur, für die die Einbettung eine euklidische Abbildung wird. Sie heißt die auf unserem Teilraum **induzierte euklidische Struktur**. Einen euklidischen Automorphismus eines euklidischen Vektorraums nennen wir eine **lineare Ähnlichkeitsabbildung**.

4.1.5.9. Unter einem **Morphismus von euklidischen Räumen** verstehen wir eine affine Abbildung, deren linearer Anteil **euklidisch** ist. Einen Automorphismus eines euklidischen Raums nennen wir eine **Ähnlichkeitsabbildung** oder kurz eine **Ähnlichkeit**.

4.1.5.10. Eine **Betragswurzel** aus einem eindimensionalen reellen Vektorraum  $F$  ist ein Paar  $(L, \pm q)$  bestehend aus einem eindimensionalen orientierten reellen Vektorraum  $L$  und einer bis auf Vorzeichen wohlbestimmten bilinearen Abbildung  $\pm q : L \times L \rightarrow F$  mit  $l \neq 0 \Rightarrow \pm q(l, l) \neq 0$ . Genauer verstehen wir hier unter einer „bis auf Vorzeichen wohlbestimmten bilinearen Abbildung“ eine Menge aus zwei bilinearen Abbildungen, von denen die eine die Negative der anderen ist. Eine Betragswurzel eines eindimensionalen reellen Vektorraums ist eindeutig bestimmt bis auf eindeutigen Isomorphismus. Ist genauer  $(L', \pm q')$  ein zweites Paar wie oben, so gibt es genau einen orientierungsverträglichen Isomorphismus  $i : L \xrightarrow{\sim} L'$  mit  $\pm q'(il, il) = \pm q(l, l)$  für alle  $l \in L$ . Unsere Betragswurzel verdient mithin einen bestimmten Artikel und eine Notation. Ich verwende die Notation

$$L := \sqrt{|F|}$$

für die Betragswurzel von  $F$ . Diejenige Abbildung  $F \rightarrow L_{\geq 0}$ , die  $f \in F$  das  $l \in L_{\geq 0}$  mit  $\pm q(l, l) = f$  zuordnet, notieren wir  $l = \sqrt{|f|}$  und nennen  $l$  die **Betragswurzel von  $f$** .

*Vorschau* 4.1.5.11. Allgemeiner kann man analog für jeden Gruppenhomomorphismus  $\varphi : \mathbb{R}^\times \rightarrow \mathbb{R}_{>0}$  eine Vorschrift angeben, die jedem eindimensiona-

len reellen Vektorraum  $F$  in natürlicher Weise einen orientierten eindimensionalen reellen Vektorraum  $\varphi(F)$  zuordnet und jedem Vektor  $f \in F$  einen Vektor  $\varphi(f) \in \varphi(F)_{\geq 0}$ . Das soll jedoch hier nicht weiter ausgeführt werden.

**4.1.5.12 (Längen von Vektoren in euklidischen Vektorräumen).** Gegeben eine euklidische Struktur  $S$  auf einem reellen Vektorraum  $V \neq 0$  notieren wir die Betragswurzel ihres Dualraums

$$\mathbb{L} = \mathbb{L}(V) = \mathbb{L}(V, S) := \sqrt{|S^\top|}$$

und nennen sie die **Längengerade** unseres euklidischen Vektorraums  $V$ . Jeder Vektor  $v \in V$  liefert ein Element  $\lambda_v \in S^\top$  durch die Vorschrift  $\lambda_v(s) := s(v, v)$ . Dessen Betragswurzel nennen wir die **Länge**  $\|v\| \in \mathbb{L}_{\geq 0}$  von  $v$  und setzen also in Formeln

$$\|v\| := \sqrt{|\lambda_v|}$$

Damit gilt offensichtlich  $\|gv\| = \|v\| \forall g \in O(V, S)$  und  $\|\alpha v\| = |\alpha| \|v\| \forall \alpha \in \mathbb{R}$ .

**4.1.5.13.** Für jede euklidische lineare Abbildung  $f : V \rightarrow W$  von euklidischen Vektorräumen gibt es genau eine lineare Abbildung

$$\mathbb{L}(f) : \mathbb{L}(V) \rightarrow \mathbb{L}(W)$$

mit  $\|v\| \mapsto \|f(v)\| \forall v \in V$ . Sie ist stets ein Isomorphismus, den wir insbesondere verwenden, um die Längengerade jedes von Null verschiedenen Untervektoraums eines euklidischen Vektorraums stillschweigend mit der Längengerade des ursprünglichen Vektorraums zu identifizieren.

**4.1.5.14.** Unter der **Längengerade eines euklidischen Raums** verstehen wir die Längengerade seines Richtungsraums.

*Beispiel 4.1.5.15.* Ist  $Z$  ein zweidimensionaler reeller Vektorraum und  $m \in Z \setminus 0$  ein fester von Null verschiedener Vektor, so gilt für unsere Norm  $\|v\|_m \in \mathbb{R}_{\geq 0}$  aus 4.1.2.7 in der zugehörigen Längengerade  $\mathbb{L}(Z)$  per definitionem die Identität

$$\|v\| = \|v\|_m \|m\|$$

**4.1.5.16 (Terminologisches zum Begriff einer Drehung).** Wir vereinbaren, daß wir von nun an unter einer **Drehung** einen orientationserhaltenden orthogonalaffinen Automorphismus eines euklidischen Raums der Dimension Zwei oder Drei verstehen wollen, der mindestens einen Fixpunkt hat. Unter einer **linearen Drehung** oder auch kurz **Drehung** verstehen wir einen orientationserhaltenden orthogonalen Automorphismus eines euklidischen Vektorraums  $V$  der Dimension Zwei oder Drei alias in der in 4.1.4.6 eingeführten Terminologie und Notation ein Element seiner speziellen orthogonalen Gruppe  $SO(V)$ . Im dreidimensionalen Fall nennen wir jede von einer Drehung punktweise festgehaltene Gerade eine

**Drehachse** unserer Drehung. Im zweidimensionalen Fall nennen wir jeden von einer Drehung festgehaltenen Punkt ein **Drehzentrum** unserer Drehung und wissen aus 4.1.2.14, daß jede gleichsinnige Kongruenz eine Drehung oder eine Verschiebung sein muß.

### Übungen

*Übung 4.1.5.17 (Vorbereitung für Winkel).* Gegeben ein euklidischer Isomorphismus  $\varphi : Y \xrightarrow{\sim} Z$  von zweidimensionalen euklidischen Vektorräumen betrachten wir den induzierten Gruppenisomorphismus  $O(\varphi) : O(Y) \xrightarrow{\sim} O(Z)$  gegeben durch  $r \mapsto \varphi \circ r \circ \varphi^{-1}$ . Gegeben zwei Isomorphismen  $\varphi, \psi : Y \xrightarrow{\sim} Z$  mit orientationserhaltender Verknüpfung  $\varphi \circ \psi^{-1} : Z \xrightarrow{\sim} Z$  zeige man, daß sie denselben Isomorphismus

$$O(\varphi) = O(\psi) : SO(Y) \xrightarrow{\sim} SO(Z)$$

zwischen den jeweiligen Drehgruppen induzieren. Andernfalls zeige man  $O(\varphi) = O(\psi) \circ \text{inv}$  für  $\text{inv} : SO(Z) \xrightarrow{\sim} SO(Z)$  das Invertieren. Hinweis: 4.1.4.20.

*Übung 4.1.5.18.* Gegeben ein endlichdimensionaler euklidischer Raum  $E$  und darin eine affine Hyperebene  $H \subset V$  gibt es genau einen orthogonalen Automorphismus  $s : E \rightarrow E$  mit unserer Hyperebene als Fixpunktmenge, in Formeln mit  $H = E^s$ . Diese Abbildung  $s$  heißt die **orthogonale Spiegelung an der Hyperebene  $H$**  oder kürzer die **Spiegelung an  $H$** .

## 4.1.6 Euklidischer Raum und Anschauung\*

4.1.6.1. Ich erinnere an die Begriffsbildung einer Kongruenzebene 4.1.1.10. Im folgenden will ich erklären, wie man in ähnlicher Weise eine Modellierung des schmutzigen Raums unserer Anschauung aus dem Bewegungsbegriff heraus entwickeln kann.

**Definition 4.1.6.2.** Unter einer **Bewegungsgruppe** eines dreidimensionalen reellen affinen Raums  $R$  verstehen wir eine alle Translationen umfassende Untergruppe  $B$  seiner Automorphismengruppe, in Formeln

$$\vec{R} \subset B \subset \text{Aff}^\times R$$

derart, daß es für je zwei Paare  $(F, H)$  und  $(F', H')$  von Teilmengen von  $R$  bestehend aus einer Halbebene und einer Halbgerade auf ihrem Rand genau einen Automorphismus  $b \in B$  gibt, der sie ineinander überführt, also mit  $bF = F'$  und  $bH = H'$ . In Formeln meinen wir hier Paare  $(F, H)$  von Teilmengen  $H \subset F \subset R$ , die in der Gestalt  $H = p + \mathbb{R}_{\geq 0} \vec{v}$  und  $F = p + \mathbb{R} \vec{v} + \mathbb{R}_{\geq 0} \vec{w}$  geschrieben werden

können, mit  $p \in R$  einem Punkt und  $\vec{v}, \vec{w} \in \vec{R}$  linear unabhängigen Richtungsvektoren. Die Elemente einer Bewegungsgruppe nennen wir **Bewegungen**. Unter einem **Bewegungsraum** verstehen wir ein Paar  $(R, B)$  bestehend aus einem dreidimensionalen reellen affinen Raum  $R$  und einer ausgezeichneten Bewegungsgruppe  $B \subset \text{Aff}^\times R$ .

**4.1.6.3 (Diskussion der Terminologie).** In der Literatur wird der Begriff einer „Bewegung“ vielfach auch verwendet für gewisse Selbstabbildungen von euklidischen Räumen, die die Orientierung nicht erhalten. Unsere Bewegungen werden in dieser Terminologie als „eigentliche Bewegungen“ bezeichnet.

**4.1.6.4 (Bezug zur Anschauung).** Man mag sich den „schmutzigen Raum  $\mathbb{E}$  unserer Anschauung“ als einen Bewegungsraum denken. Die Elemente von  $\mathbb{E}$  sind dabei „alle möglichen Orte im Raum“. Manche dieser Orte können direkt als Kirchturmspitzen, Zimmerecken und dergleichen angegeben werden, die Übrigen gilt es sich vorzustellen. Affine Geraden in  $\mathbb{E}$  denke man sich als Sichtlinien, wie in 3.3.1.9 und 3.3.3.3 besprochen. Bei Bewegungen denke man an, nun, eben anschauliche Bewegungen. Kippen wir etwa einen Stuhl um, so werden die Enden der Stuhlbeine, die Ecken der Sitzfläche, ja überhaupt alle seine Punkte jeweils in andere Punkte des Raums unserer Anschauung überführt, und diese Abbildung läßt sich, das entspricht zumindest unserer Erfahrung, zu einer bijektiven Selbstabbildung des Raums unserer Anschauung fortsetzen, die Sichtlinien in Sichtlinien überführt und die nach 3.3.3.1 folglich einer affinen Abbildung  $\mathbb{E} \rightarrow \mathbb{E}$  entsprechen muß. Unsere ausgezeichnete Bewegungsgruppe  $B$  modelliert die Menge aller derartigen Selbstabbildungen des Raums unserer Anschauung. Unsere Bedingung an eine Bewegungsgruppe aus 4.1.6.2 bedeutet anschaulich, daß man etwa jedes Messer aus einer festen Position heraus durch genau eine Bewegung in eine Position bringen kann, in der der Übergang vom Griff zur Klinge an einer vorgegebenen Stelle stattfindet, die Messerspitze in eine vorgegebene Richtung zeigt und der Schnitt den Raum entlang einer vorgegebenen Halbebene zerteilen würde. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist und daß der in der Schule erlernte Koordinatenzirkus von der Realität viel weiter entfernt ist.

*Ergänzung 4.1.6.5.* Ich wage die Vermutung, daß Säuglinge nicht zuletzt deshalb so gerne herumgetragen und herumgefahren werden, weil ihnen das eine genauere Untersuchung dieser bemerkenswerten mathematischen Struktur ermöglicht, die der Raum unserer Anschauung nun einmal ist. Bewegen Sie nur einmal selbst den Kopf hin und her und versuchen Sie, von Ihrer jahrelangen Erfahrung zu abstrahieren und neu zu entdecken, in wie interessanter Weise sich dabei die Sinneseindrücke im Auge ändern!

**Satz 4.1.6.6 (Euklidische Strukturen und Bewegungsgruppen).** *Gegeben ein*

*dreidimensionaler reeller affiner Raum  $R$  erhalten wir zueinander inverse Bijektionen*

$$\{\text{Euklidische Strukturen } S \subset \text{Bil}(\vec{R})\} \xleftrightarrow{\sim} \{\text{Bewegungsgruppen } B \subset \text{Aff}^\times(R)\}$$

*dadurch, daß wir jeder euklidischen Struktur  $S$  auf  $\vec{R}$  als Bewegungsgruppe die Gruppe  $B_S := \text{SO}_{\text{aff}}(R, S)$  aller orientierungserhaltenden orthogonalaffinen Affinitäten von  $R$  zuordnen und umgekehrt jeder Bewegungsgruppe  $B$  die Menge  $S$  aller darunter invarianten Bilinearformen auf dem Richtungsraum.*

*Beweis.* Daß unsere Konstruktion jeder euklidischen Struktur auf  $\vec{R}$  eine Bewegungsgruppe zuordnet, scheint mir offensichtlich. Daß man aus dieser Bewegungsgruppe die euklidische Struktur zurückgewinnen kann, daß also unsere Abbildung von links nach rechts injektiv ist, mag man daraus erkennen, daß die Restriktionen aller Bewegungen, die eine vorgegebene affine Ebene stabilisieren, auf besagte Ebene notwendig eine Kongruenzgruppe der besagten affinen Ebene bilden und so auf dem Richtungsraum dieser affinen Ebene nach 4.1.5.7 eine euklidische Struktur induzieren. Eine euklidische Struktur auf einem reellen Vektorraum der Dimension mindestens Zwei wird aber offensichtlich durch ihre Restriktionen auf alle zweidimensionalen Untervektorräume bereits eindeutig festgelegt. Es bleibt damit nur noch zu zeigen, daß unsere Abbildung surjektiv ist. Das leistet der im Anschluß bewiesene Satz 4.1.6.9.  $\square$

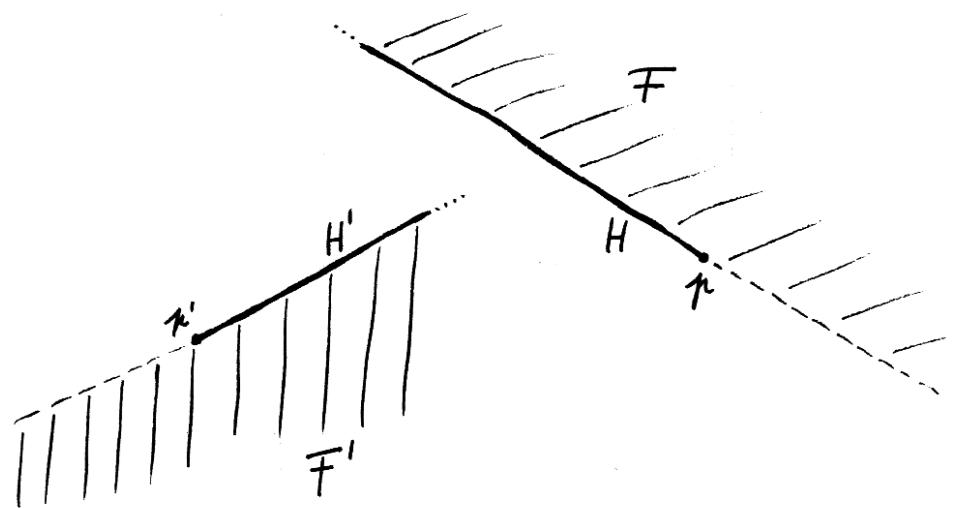
**Definition 4.1.6.7.** Sei  $V$  ein dreidimensionaler reeller Vektorraum. Eine **Halbraumfahne** in  $V$  ist ein Paar  $(H, A)$  von Teilmengen bestehend aus einer Halbebene und einem Strahl auf ihrem Rand. In Formeln ausgedrückt soll es also linear unabhängige Vektoren  $v, w \in V$  geben mit  $H = \mathbb{R}_{\geq 0}v + \mathbb{R}w$  und  $A = \mathbb{R}_{\geq 0}w$ .

**Definition 4.1.6.8.** Sei  $V$  ein dreidimensionaler reeller Vektorraum. Eine Untergruppe  $D \subset \text{GL}(V)$  heiße eine **Drehungsgruppe**, wenn es für je zwei Halbraumfahnen in  $V$  genau ein Element  $d \in D$  gibt, das sie ineinander überführt. Die Elemente einer ausgezeichneten Drehungsgruppe sprechen wir im folgenden als **Drehungen** an.

**Satz 4.1.6.9 (Drehungsgruppen und euklidische Strukturen).** *Gegeben ein dreidimensionaler reeller Vektorraum  $V$  erhalten wir zueinander inverse Bijektionen*

$$\{\text{Euklidische Strukturen } S \subset \text{Bil}(V)\} \xleftrightarrow{\sim} \{\text{Drehungsgruppen } D \subset \text{GL}(V)\}$$

*dadurch, daß wir jeder euklidischen Struktur  $S$  ihre spezielle orthogonale Gruppe  $\text{SO}(V, S)$  zuordnen und umgekehrt jeder Drehungsgruppe  $D$  die Menge  $S_D$  der unter all ihren Elementen invarianten Bilinearformen.*



Zwei Paare von Teilmengen des Raums bestehend aus je einer Halbebene und einer Halbgerade auf ihrem Rand.

*Beweis.* Der Nachweis, daß  $\mathrm{SO}(V, S)$  in der Tat eine Drehungsgruppe ist, bleibe dem Leser überlassen. Um zu sehen, daß gegeben ein unter einer Drehungsgruppe invariantes Skalarprodukt jede invariante Bilinearform ein skalares Vielfaches desselben ist, muß man nur bemerken, daß die einen zweidimensionalen Teilraum stabilisierenden Elemente einer Drehungsgruppe auf diesem Teilraum eine Drehspiegelgruppe induzieren und nach 4.1.5.6 folglich die Restriktion einer invarianten Bilinearform auf jeden zweidimensionalen Teilraum ein skalares Vielfaches der Restriktion unseres invarianten Skalarprodukts ist. Es bleibt nur noch zu zeigen, daß es für jede Drehungsgruppe mindestens ein invariantes Skalarprodukt gibt. Das zeigen wir nach einigen Vorbereitungen in 4.1.6.14.  $\square$

**Lemma 4.1.6.10.** *Sei  $(V, D)$  ein dreidimensionaler reeller Vektorraum mit ausgezeichneter Drehungsgruppe. Gegeben ein Vektor  $v \in V \setminus \{0\}$  gibt es genau eine nichttriviale Drehung  $r_v \in D \setminus \mathrm{id}$  mit  $r_v(v) = v$  und  $r_v^2 = \mathrm{id}$ , und diese Drehung hat einen zweidimensionalen Eigenraum zum Eigenwert  $(-1)$ . Wir nennen  $r_v$  die Achsenspiegelung an der Ursprungsgerade  $\mathbb{R}v$ .*

4.1.6.11. In der schmutzigen Anschauung kann  $r_v$  beschrieben werden als die Drehung um die von  $v$  erzeugte Gerade mit dem Winkel  $180^\circ$ .

*Beweis.* Wie bereits erwähnt ist es klar, daß alle Drehungen, die einen zweidimensionalen Teilraum  $Z \subset V$  stabilisieren, auf  $Z$  eine Drehspiegelgruppe im Sinne von 4.1.2.2 induzieren. Sei nun  $r$  eine nichttriviale Drehung mit  $r(v) = v$  und  $r^2 = \mathrm{id}$ . Nach 3.6.6.29 ist  $r$  diagonalisierbar mit Eigenwerten  $\pm 1$ . Da  $r$  nichttrivial ist mit positiver Determinante, müssen seine Eigenwerte mit Multiplizitäten  $1, -1, -1$  sein. Folglich ist  $\mathbb{R}v$  der Eigenraum von  $r$  zum Eigenwert Eins und in jedem zweidimensionalen Teilraum, der  $v$  enthält, muß auch ein Eigenvektor zum Eigenwert  $(-1)$  liegen. Damit muß  $r$  jede derartige Ebene auf sich selbst abbilden und darauf unsere Spiegelung aus dem Beweis von 4.1.5.6 induzieren, die wir dort  $r_v$  notiert hatten. Das zeigt die Eindeutigkeit von  $r$  und unsere Behauptung über den  $(-1)$ -Eigenraum. Um die Existenz zu zeigen, wählen wir  $w \in V$  linear unabhängig zu  $v$  und betrachten die Drehung  $r = r_{v,w}$ , die die Halbraumfahne  $(\mathbb{R}v + \mathbb{R}_{\geq 0}w, \mathbb{R}_{\geq 0}v)$  in die Halbraumfahne  $(\mathbb{R}v - \mathbb{R}_{\geq 0}w, \mathbb{R}_{\geq 0}v)$  überführt. Offensichtlich gilt  $r^2 = \mathrm{id}$  und nach 3.6.6.29 ist dann  $r$  diagonalisierbar mit Eigenwerten  $\pm 1$ . Sicher ist  $v$  ein Eigenvektor von  $r$  zu einem positiven Eigenwert, also zum Eigenwert Eins, also ein Fixvektor. Das zeigt dann auch die in unserem Lemma behauptete Existenz der Achsenspiegelung  $r_v$ .  $\square$

**Lemma 4.1.6.12.** *Sei  $(V, D)$  ein dreidimensionaler reeller Vektorraum mit ausgezeichneter Drehungsgruppe. Gegeben  $t \in D$  und  $m \in V$  folgt aus  $tm \in \mathbb{R}_{\geq 0}m$  dann bereits  $tm = m$ .*

4.1.6.13. In der schmutzigen Anschauung entspricht das der Erkenntnis, daß beim Drehen um eine Achse besagte Achse weder gestreckt noch gestaucht wird.

*Beweis.* Ohne Beschränkung der Allgemeinheit dürfen wir  $m \neq 0$  annehmen. Dann betrachten wir die Achsen Spiegelung  $r_m$  nach 4.1.6.10 und wählen im zweidimensionalen Teilraum  $Z$  der Fixpunkte von  $(-r_m)$  einen Vektor  $w \neq 0$ . Wegen  $tr_m = r_m t$  gilt dann auch  $tw \in Z$ . Nach 4.1.2.6 werden je zwei Strahlen in einem zweidimensionalen Vektorraum mit ausgezeichneter Drehspiegelgruppe durch eine Spiegelung vertauscht, es gibt also  $u \in Z \setminus 0$  mit  $r_u(\mathbb{R}_{\geq 0}w) = \mathbb{R}_{\geq 0}tw$ . Andererseits zeigt unsere Diskussion des Senkrechstehens in Kongruenzebenen 4.1.1.17 bereits  $r_u(m) = -m$  und  $r_w(m) = -m$ . Es folgt  $r_u r_w = t$ , da beide Abbildungen  $\mathbb{R}_{\geq 0}m$  festhalten und  $\mathbb{R}_{\geq 0}w$  in  $\mathbb{R}_{\geq 0}tw$  überführen. So erhalten wir schließlich  $tm = r_u r_w m = m$ .  $\square$

**Lemma 4.1.6.14 (Existenz invarianter Skalarprodukte).** *Sei  $(V, D)$  ein dreidimensionaler reeller Vektorraum mit ausgezeichneter Drehungsgruppe. So gibt es auf  $V$  ein  $D$ -invariantes Skalarprodukt.*

*Beweis.* Wir wählen einen Vektor  $m \in V \setminus 0$ . Für jeden zweidimensionalen Teilraum  $Z \subset V$  und jede Drehung  $d \in D$  mit  $d(m) \in Z$  gibt es nach 4.1.5.6 genau ein Skalarprodukt auf  $Z$ , das invariant ist unter allen Drehungen, die  $Z$  stabilisieren, und das  $d(m)$  die Norm Eins gibt. Lemma 4.1.6.12 zeigt, daß dies Skalarprodukt auf  $Z$  nicht von der Wahl von  $d$  abhängt. Folglich sind alle diese Skalarprodukte Einschränkungen eines wohldefinierten Skalarprodukts auf  $V$ . Die Konstruktion zeigt weiter, daß für jede Drehung  $d \in D$  und jeden zweidimensionalen Teilraum  $Z \subset V$  die Abbildung  $d : Z \xrightarrow{\sim} d(Z)$  verträglich ist mit den jeweiligen Skalarprodukten. Folglich ist unser Skalarprodukt auf  $V$  invariant unter  $D$ .  $\square$

*Ergänzung 4.1.6.15 (Verallgemeinerung auf beliebige Dimensionen).* Ich skizziere Analoga unserer Sätze 4.1.5.6 und 4.1.6.9 für reelle Vektorräume beliebiger endlicher Dimension. Man mag für jeden reellen Vektorraum  $V$  endlicher Dimension  $n$  eine **vollständige Halbraumfahne** erklären als eine Folge von Teilmengen  $F_0 \subset F_1 \subset \dots \subset F_{n-1} \subset F_n \subset V$  derart, daß es linear unabhängige Vektoren  $v_1, \dots, v_n \in V$  gibt mit  $F_i = \mathbb{R}v_1 + \dots + \mathbb{R}v_{i-1} + \mathbb{R}_{\geq 0}v_i$ . Eine Untergruppe  $O \subset \mathrm{GL}(V)$  mag man dann eine **Drehspiegelgruppe** nennen, wenn es für je zwei vollständige Halbraumfahnen genau ein  $k \in O$  gibt, das die eine Fahne in die andere überführt. Man mag weiter eine **fastvollständige Halbraumfahne** erklären als eine Folge von Teilmengen  $F_0 \subset F_1 \subset \dots \subset F_{n-1} \subset V$  derart, daß es linear unabhängige Vektoren  $v_1, \dots, v_{n-1} \in V$  gibt mit  $F_i = \mathbb{R}v_1 + \dots + \mathbb{R}v_{i-1} + \mathbb{R}_{\geq 0}v_i$ . Eine Untergruppe  $D \subset \mathrm{GL}(V)$  mag man weiter eine **Drehungsgruppe** nennen, wenn es für je zwei fastvollständige Halbraumfahnen genau ein Element  $d \in D$

gibt, die die eine Fahne in die andere überführt. In dieser Allgemeinheit zeigen unsere Argumente, daß es für jede Drehspiegelgruppe bis auf konstante Vielfache genau ein invariantes Skalarprodukt gibt, und daß im Fall einer von Zwei verschiedenen Dimension dasselbe auch für jede Drehungsgruppe gilt. Im ebenen Fall gilt das jedoch nur unter der zusätzlichen Annahme, daß unsere Drehungsgruppe eine im Sinne der Topologie „abgeschlossene“ Untergruppe ist. Wählen wir genauer ein Komplement  $V \subset \mathbb{R}$  des  $\mathbb{Q}$ -Untervektorräums  $\mathbb{Q} \subset \mathbb{R}$ , so finden wir einen Gruppenisomorphismus  $\mathbb{R}/\mathbb{Z} \cong V \times \mathbb{Q}/\mathbb{Z}$  und dann auch einen Gruppenisomorphismus  $S^1 \cong V \times \mathbb{Q}/\mathbb{Z}$ . Es gibt mithin durchaus unstetige nichttriviale Gruppenhomomorphismen  $\psi : S^1 \rightarrow \mathbb{R}_{>0}$  für  $S^1$  die Gruppe der komplexen Zahlen vom Betrag Eins, und dann bilden alle Abbildungen der Gestalt  $z \mapsto \psi(a)z$  mit  $a \in S^1$  eine Drehungsgruppe in  $\text{Aut}_{\mathbb{R}}(\mathbb{C})$  im Sinne der obigen Definition, für die kein invariantes Skalarprodukt existiert. Mehr dazu findet man in [Pic49, Bae50] und unter dem Stichwort des **Helmholtz'schen Raumproblems**.

#### 4.1.7 Zweistrahlen und Winkel

4.1.7.1. Unter einem **Zweistrahl** in einem Vektorraum  $V$  über einem angeordneten Körper verstehen wir ein ungeordnetes Paar alias eine zweielementige Multi-menge  ${}_{\mu}\{A, B\}$  von Strahlen. Unter einem **angeordneten Zweistrahl** verstehen wir ein Paar  $(A, B)$  von Strahlen.

4.1.7.2. Gegeben ein zweidimensionaler euklidischer Vektorraum  $Z$  ist die Gruppe seiner orientierungserhaltenden orthogonalen Selbstabbildungen alias linearen Drehungen  $\text{SO}(Z)$  nach 4.1.4.20 kommutativ und für jeden angeordneten Zweistrahl  $(A, B)$  in  $Z$  gibt es genau ein Element  $d \in \text{SO}(Z)$  mit  $d(A) = B$ .

4.1.7.3. Wir betrachten die Zuordnung  $W$ , die jedem orientierten zweidimensionalen euklidischen Vektorraum  $(Z, \varepsilon)$  die Gruppe seiner linearen Drehungen zuordnet. Wir nennen diese Gruppe die **Winkelgruppe von**  $(Z, \varepsilon)$  und notieren sie

$$W(Z, \varepsilon) := \text{SO}(Z)$$

Wir notieren  $W(Z, \varepsilon)$  im Gegensatz zu  $\text{SO}(Z)$  additiv. Wir bezeichnen die Elemente unserer Gruppen je nachdem, ob wir ihre Verknüpfung multiplikativ oder additiv notieren, als **Drehungen** oder als **Winkel** und noch genauer als **konkrete Winkel**. Einen Winkel  $k \in W(Z, \varepsilon)$  nennen wir **positiv** beziehungsweise **negativ**, wenn für ein und jedes  $v \in Z \setminus 0$  das Paar  $(v, k(v))$  in Bezug auf die Orientierung  $\varepsilon$  eine positiv orientierte beziehungsweise eine negativ orientierte Basis von  $Z$  ist. Wir bezeichnen die Menge der nicht negativen Winkel mit

$$W(Z, \varepsilon)^+ \subset W(Z, \varepsilon)$$

Es gibt zwei Winkel, die weder negativ noch positiv sind, nämlich den Nullwinkel und einen weiteren Winkel, den wir später genauer diskutieren und den „gestreckten Winkel“ nennen werden.

*Beispiel 4.1.7.4 (Winkelgruppe der Zahlenebene).* Wir erinnern den Körper der komplexen Zahlen und genauer das bis auf eindeutigen Isomorphismus eindeutig bestimmte Tripel  $(\mathbb{C}, i, \kappa)$  aus 3.2.7.4 mit  $\kappa : \mathbb{R} \hookrightarrow \mathbb{C}$ . Wir erinnern auf dem  $\mathbb{R}$ -Vektorraum  $\mathbb{C}$  das Skalarprodukt  $\langle z, w \rangle := \operatorname{Re} \bar{z}w$  und versehen  $\mathbb{C}$  mit der dadurch bestimmten euklidischen Struktur. Wir versehen den  $\mathbb{R}$ -Vektorraum  $\mathbb{C}$  mit seiner **Standardorientierung**  $st$ , für die  $(1, i)$  eine positiv orientierte angeordnete Basis ist. Die Abbildung, die jedem  $z \in S^1$  die Multiplikation  $(z \cdot)$  zuordnet, liefert dann einen Isomorphismus  $S^1 \xrightarrow{\sim} W(\mathbb{C}, st)$  der Kreisgruppe mit der Winkelgruppe von  $\mathbb{C}$  und eine Bijektion

$$\{z \in S^1 \mid \operatorname{Im}(z) \geq 0\} \xrightarrow{\sim} W(\mathbb{C}, st)^+$$

zwischen dem „abgeschlossenen oberen Halbkreis“ und der Menge der nichtnegativen Winkel von  $(\mathbb{C}, st)$ .

**4.1.7.5 (Abstrakte Winkel).** Nach 4.1.5.17 induzieren je zwei orientierungserhaltende mit den euklidischen Strukturen verträgliche Isomorphismen zwischen zweidimensionalen orientierten euklidischen Vektorräumen  $(Y, \eta)$  und  $(Z, \varepsilon)$  denselben Isomorphismus  $W(Y, \eta) \xrightarrow{\sim} W(Z, \varepsilon)$  zwischen ihren Winkelgruppen. Dieser Isomorphismus induziert darüber hinaus eine Bijektion  $W(Y, \eta)^+ \xrightarrow{\sim} W(Z, \varepsilon)^+$  zwischen den jeweiligen Teilmengen nichtnegativer Winkel. Das Datum aus einer Gruppe mit ausgezeichneter Teilmenge  $W(Z, \varepsilon)^+ \subset W(Z, \varepsilon)$  ist folglich eindeutig bestimmt bis auf eindeutigen Isomorphismus. Es verdient damit eine Notation und einen Namen. Ich schlage dafür die Notationen

$$\mathbb{W}^+ \subset \mathbb{W}$$

vor und nenne  $\mathbb{W}$  die **abstrakte Winkelgruppe** und  $\mathbb{W}^+$  die **abstrakte Winkelmenge**. Elemente von  $\mathbb{W}$  heißen **Winkel**, Elemente von  $\mathbb{W}^+$  **nichtnegative Winkel** und Elemente von  $\mathbb{W} \setminus \mathbb{W}^+$  **negative Winkel**. Das einem abstrakten Winkel  $\vartheta \in \mathbb{W}$  durch die Wahl einer Orientierung  $\varepsilon$  von  $Z$  zugeordnete Element von  $\operatorname{SO}(Z)$  nenne ich die **Drehung um den Winkel**  $\vartheta$  und notiere es  $R_\vartheta = R_\vartheta^{(\varepsilon)}$  mit einem  $R$  für „Rotation“. Jedem angeordneten Zweistrahl  $(A, B)$  in einem orientierten zweidimensionalen euklidischen Vektorraum  $(Z, \varepsilon)$  ordnen wir dann ein wohlbestimmtes Element

$$\vartheta = \angle(A, B) \in \mathbb{W}$$

der abstrakten Winkelgruppe zu als dasjenige  $\vartheta \in \mathbb{W}$  mit  $R_\vartheta(A) = B$ . Wir nennen diesen Winkel  $\vartheta$  den **gerichteten Winkel von  $A$  nach  $B$** . Jedem Zweistrahl  $\mu\{A, B\}$  in einem beliebigen euklidischen Vektorraum ordnen wir weiter

ein wohlbestimmtes Element

$$\vartheta = \angle(A, B) \in \mathbb{W}^+$$

der Winkelmenge zu als denjenigen eindeutig bestimmten nichtnegativen Winkel  $\vartheta \in \mathbb{W}^+$ , für den es einen zweidimensionalen Teilraum  $Z$  und eine Orientierung  $\varepsilon$  von  $Z$  gibt mit  $A, B \subset Z$  und  $R_\vartheta^{(\varepsilon)}(A) = B$ . Wir nennen dies Element  $\vartheta$  der Winkelmenge den **von den Strahlen  $A$  und  $B$  eingeschlossenen Winkel**.

4.1.7.6. Die Zuordnung, die jedem zweidimensionalen euklidischen Vektorraum  $Z$  die Gruppe  $\mathrm{SO}(Z)$  seiner orientierungserhaltenden Automorphismen zuordnet, liefert keine bis auf eindeutigen Isomorphismus wohlbestimmte Gruppe  $\mathbb{SO}$ , weil manche euklidischen Isomorphismen von  $Z$  zu sich selber, genauer die orientationsumkehrenden Isomorphismen, das Invertieren  $\mathrm{inv} : \mathrm{SO}(Z) \xrightarrow{\sim} \mathrm{SO}(Z)$  induzieren.

4.1.7.7. Wir erklären eine Abbildung  $|\cdot| : \mathbb{W} \rightarrow \mathbb{W}^+$  durch die Vorschrift

$$|\alpha| := \begin{cases} \alpha & \alpha \in \mathbb{W}^+; \\ -\alpha & \alpha \notin \mathbb{W}^+, \end{cases}$$

und nennen  $|\alpha|$  den **Betrag des Winkels**  $\alpha$ . Für jeden angeordneten Zweistrahlgang  $(A, B)$  in einem orientierten zweidimensionalen euklidischen Vektorraum gilt dann

$$\angle(A, B) = |\angle(A, B)|$$

4.1.7.8 (**Additivität von Winkeln**). Gegeben Strahlen  $A, B, C$  in einem zweidimensionalen orientierten euklidischen Vektorraum gilt in der Winkelgruppe  $\mathbb{W}$  offensichtlich die Identität

$$\angle(A, B) + \angle(B, C) = \angle(A, C)$$

4.1.7.9. Mit der Standardorientierung auf  $\mathbb{C}$  liefern unsere Konstruktionen aus 4.1.7.4 unmittelbar einen Isomorphismus

$$\mathrm{wk} : S^1 \xrightarrow{\sim} \mathbb{W}$$

zwischen der Kreisgruppe und der Winkelgruppe, den **Standardisomorphismus** von der Kreisgruppe zur Winkelgruppe. Er induziert eine Bijektion  $\mathrm{wk} : \{z \in S^1 \mid \mathrm{Im}(z) \geq 0\} \xrightarrow{\sim} \mathbb{W}^+$ , wir nennen sie die **Standardbijektion**. Die Umkehrabbildung des Standardisomorphismus ist ein Isomorphismus  $\mathrm{kw} := \mathrm{wk}^{-1}$  von der Winkelgruppe in die Kreisgruppe, also in Formeln

$$\mathrm{kw} : \mathbb{W} \xrightarrow{\sim} S^1$$

Wir nennen ihn den **Standardisomorphismus** von der Winkelgruppe zur Kreisgruppe. Unsere allgemeinen Erkenntnisse 3.5.3.19 über Nullstellen von Polynomen zeigen, daß es für jedes  $n \in \mathbb{N}_{\geq 1}$  höchstens  $n$  Winkel  $\vartheta \in \mathbb{W}$  gibt mit  $n\vartheta = 0$ . Eine genauere Untersuchung des Körpers der komplexen Zahlen zeigt, daß es sogar stets genau  $n$  derartige Winkel gibt.

**4.1.7.10 (Einige spezielle Winkel).** Wir diskutieren nun die wichtigsten Winkel und die zugehörigen Elemente der Kreisgruppe.

1. Das neutrale Element der Winkelgruppe nennen wir den **Nullwinkel**  $0 \in \mathbb{W}$ . Es gehört zur Menge  $\mathbb{W}^+$  der nichtnegativen Winkel. Unter unserem Standardisomorphismus  $\text{kw} : \mathbb{W} \xrightarrow{\sim} S^1$  entspricht dies Element der komplexen Zahl 1. Für einen Zweistrahl  ${}_\mu\{A, B\}$  in einem euklidischen Vektorraum ist  $\angle(A, B) = 0$  gleichbedeutend zu  $A = B$ .
2. Man sieht mithilfe unseres Isomorphismus  $\text{kw} : \mathbb{W} \xrightarrow{\sim} S^1$  aus 4.1.7.9, daß es in der Winkelgruppe genau ein Element  $\vartheta$  gibt mit  $2\vartheta = 0$  aber  $\vartheta \neq 0$ . Es heißt der **gestreckte Winkel**  $\gamma$  und gehört auch zur Menge  $\mathbb{W}^+$  der nichtnegativen Winkel. Unter unserem Standardisomorphismus  $\text{kw} : \mathbb{W} \xrightarrow{\sim} S^1$  entspricht dies Element der komplexen Zahl  $-1$ . Für einen Zweistrahl  ${}_\mu\{A, B\}$  in einem euklidischen Vektorraum ist  $\angle(A, B)$  der gestreckte Winkel genau dann, wenn gilt  $A = -B$ .
3. Man sieht mithilfe unseres Isomorphismus  $\text{kw} : \mathbb{W} \xrightarrow{\sim} S^1$  aus 4.1.7.9, daß es in der Winkelgruppe genau zwei Elemente  $\alpha$  gibt mit  $4\alpha = 0$  aber  $2\alpha \neq 0$ , und daß genau Eines davon in der Winkelmenge liegt. Dies Element der Winkelmenge  $\rho \in \mathbb{W}^+$  heißt der **rechte Winkel**. Unter unserem Standardisomorphismus  $\text{kw} : \mathbb{W} \xrightarrow{\sim} S^1$  entspricht der rechte Winkel der komplexen Zahl  $i$ . Für einen Zweistrahl  ${}_\mu\{A, B\}$  in einem euklidischen Vektorraum ist  $\angle(A, B)$  der rechte Winkel genau dann, wenn gilt  $A \perp B$  alias  $v \perp w \forall v \in A, w \in B$  im Sinne von 4.1.5.1.

**4.1.7.11 (Sinus und Cosinus).** Für den  $\mathbb{R}^2$  mit seiner Standardorientierung und seinem Standardskalarprodukt erhalten wir per definitionem einen kanonischen Isomorphismus  $\mathbb{W} \xrightarrow{\sim} \text{SO}(\mathbb{R}^2)$ ,  $\vartheta \mapsto R_\vartheta$ . Wir erklären Abbildungen **Sinus** und **Cosinus**  $\sin, \cos : \mathbb{W} \rightarrow \mathbb{R}$  durch die Vorschrift

$$R_\vartheta \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos \vartheta \\ \sin \vartheta \end{pmatrix}$$

**4.1.7.12.** Der Cosinus induziert offensichtlich eine Bijektion  $\cos : \mathbb{W}^+ \xrightarrow{\sim} [-1, 1]$  zwischen unserer Winkelmenge und dem reellen Intervall  $[-1, 1]$ . Der rechte Winkel hat offensichtlich  $\cos(\rho) = 0$  als Cosinus, der Nullwinkel  $\cos(0) = 1$  und der

gestreckte Winkel  $\cos(\gamma) = -1$ . Für alle Winkel  $\vartheta \in \mathbb{W}$  gilt  $\sin^2 \vartheta + \cos^2 \vartheta = 1$  und für alle nichtnegativen Winkel  $\vartheta \in \mathbb{W}^+$  gilt  $\sin \vartheta \geq 0$  und mithin  $\sin \vartheta = \sqrt{1 - \cos^2 \vartheta}$ .

4.1.7.13. Unser kanonischer Isomorphismus  $\mathbb{W} \xrightarrow{\sim} \mathrm{SO}(\mathbb{R}^2)$ ,  $\vartheta \mapsto R_\vartheta$  wird in diesen Notationen gegeben durch die Vorschrift

$$\vartheta \mapsto \begin{pmatrix} \cos \vartheta & -\sin \vartheta \\ \sin \vartheta & \cos \vartheta \end{pmatrix}$$

Unser Standardisomorphismus mit der Kreisgruppe  $\mathrm{wk} : \mathbb{W} \xrightarrow{\sim} S^1$  wird in diesen Notationen gegeben durch die Vorschrift  $\vartheta \mapsto \cos \vartheta + i \sin \vartheta$ .

**Vorschau 4.1.7.14 (Bezug zur Analysis).** In der Analysis ?? führt man Sinus und Cosinus meist als Funktionen  $\sin, \cos : \mathbb{R} \rightarrow \mathbb{R}$  ein. Wenn ich auf dem Unterschied zu unseren hier erklärten Funktionen  $\sin, \cos : \mathbb{W} \rightarrow \mathbb{R}$  bestehen will, unterscheide ich zwischen dem „analytischen“ und dem „geometrischen“ Sinus beziehungsweise Cosinus und notiere Erstere  $\sin_a, \cos_a : \mathbb{R} \rightarrow \mathbb{R}$  und Letztere  $\sin_g, \cos_g : \mathbb{W} \rightarrow \mathbb{R}$ . Per definitionem gilt dann für die Komposition

$$\mathrm{wk} \circ u : \mathbb{R} \rightarrow \mathbb{W}$$

der Umlaufabbildung  $u : \mathbb{R} \rightarrow S^1$ ,  $t \mapsto \exp it$  mit unserem Standardisomorphismus  $\mathrm{wk} : S^1 \xrightarrow{\sim} \mathbb{W}$  aus 4.1.7.9 die Beziehung

$$\sin_a = \sin_g \circ \mathrm{wk} \circ u \quad \text{und} \quad \cos_a = \cos_g \circ \mathrm{wk} \circ u.$$

Mehr dazu besprechen wir in 4.1.8.1 im Zusammenhang mit Winkelmaßen.

4.1.7.15 (**Winkel zwischen Vektoren**). Wir erklären den **Winkel**

$$\angle(v, w) \in \mathbb{W}^+$$

zwischen zwei von Null verschiedenen Vektoren  $v \neq 0 \neq w$  eines euklidischen Vektorraums als den von den zugehörigen Strahlen  $\mathbb{R}_{\geq 0}v$  und  $\mathbb{R}_{\geq 0}w$  im Sinne von 4.1.7.5 eingeschlossenen Winkel. Wir zeigen nun für diesen Winkel und ein beliebiges Skalarprodukt der vorgegebenen euklidischen Struktur die Formel

$$\cos_g(\angle(v, w)) = \frac{\langle v, w \rangle}{\|v\| \|w\|}$$

Per definitionem reicht es, sie für zweidimensionale Skalarprodukträume zu zeigen. Weiter reicht es, sie für Vektoren der Norm Eins zu zeigen. Da beide Seiten gleich bleiben, wenn wir unsere Vektoren durch ihre Bilder unter einem Isomorphismus von Skalarprodukträumen ersetzen, dürfen wir sogar annehmen, daß unser Skalarproduktraum die komplexe Zahlenebene  $\mathbb{C}$  ist mit  $\langle z, w \rangle = \mathrm{Re}(\bar{z}w)$  und daß gilt  $z = 1$ . In diesem Fall ist die Behauptung jedoch offensichtlich.

*Vorschau 4.1.7.16.* In 4.6.4.6 werden wir das kanonische „flächenwertige Skalarprodukt“ eines euklidischen Vektorraums kennenlernen und sehen, wie man die reelle Zahl  $\langle v, w \rangle / (\|v\| \|w\|)$  aus 4.1.7.15 auch und in besonders natürlicher Weise als einen „Quotient von zwei Flächen“ verstehen kann.

### Übungen

*Übung 4.1.7.17 (Ähnliche Zweistrahlen und Winkel).* Zwei angeordnete Zweistrahlen  $(A, B)$  und  $(A', B')$  in orientierten zweidimensionalen euklidischen Vektorräumen  $Z, Z'$  lassen sich genau dann durch einen orientierungserhaltenden Isomorphismus euklidischer Vektorräume ineinander überführen, wenn sie denselben gerichteten Winkel einschließen, wenn also gilt

$$\angle(A, B) = \angle(A', B')$$

Von zwei Zweistrahlen  $\mu\{A, B\}$  und  $\mu\{A', B'\}$  in endlichdimensionalen euklidischen Vektorräumen  $Z, Z'$  lässt sich genau dann einer der beiden durch eine euklidische lineare Abbildung in den anderen überführen, wenn sie denselben ungerichteten Winkel einschließen, wenn also gilt

$$\angle(A, B) = \angle(A', B')$$

### 4.1.8 Winkelmaße und Winkel im Dreieck

4.1.8.1 (**Allgemeine Winkelmaße**). Wir versehen die Winkelgruppe  $\mathbb{W}$  mit der induzierten Topologie ?? zur natürlichen Topologie ?? auf dem Endomorphismenraum eines zweidimensionalen reellen Vektorraums. Aus der Analysis ?? wissen wir, daß es stetige nichtkonstante Gruppenhomomorphismen

$$w : \mathbb{R} \rightarrow \mathbb{W}$$

von der additiven Gruppe der reellen Zahlen in die Winkelgruppe gibt, daß alle derartigen Gruppenhomomorphismen surjektiv sind und daß sich je Zwei von ihnen nur um das Vorschalten der Multiplikation mit einer von Null verschiedenen reellen Zahl unterscheiden. Jeder derartige Gruppenhomomorphismus hat weiter, immer nach ??, einen Kern der Gestalt  $\mathbb{Z}b$  für wohlbestimmtes  $b > 0$  und induziert mithin Bijektionen

$$w : [0, b) \xrightarrow{\sim} \mathbb{W}$$

Diese Bijektionen kann man verwenden, um Elemente der Winkelgruppe durch reelle Zahlen zu beschreiben. Man beschränkt sich hierbei in der Mathematik meist auf Gruppenhomomorphismen  $w$  mit der Eigenschaft, daß für einen orientierten zweidimensionalen euklidischen Vektorraum  $V$  und einen Vektor  $\vec{v} \in V$

ungleich Null und hinreichend kleines  $t > 0$  das Paar  $(\vec{v}, w(t)(\vec{v}))$  eine positiv orientierte Basis ist. Derartige Gruppenhomomorphismen werden durch obiges  $b$  bereits eindeutig festgelegt. Die Umkehrabbildung der zugehörigen Bijektion heißt dann das durch  $b$  gegebene **Winkelmaß**.

- 4.1.8.2 (**Gebräuchliche Winkelmaße**).
1. Auf der Schule wird der Gruppenhomomorphismus  $w$  meist so gewählt, daß  $b = 360$  die kleinste positive Zahl ist, die auf die Identität abgebildet wird. Das hat den Vorteil, daß alle  $n \in \mathbb{N}$  mit  $1 \leq n \leq 6$  Teiler von 360 sind, so daß die Winkelmaße vieler Winkel in einfachen geometrischen Figuren natürliche Zahlen werden. Man deutet das Anwenden dieses Gruppenhomomorphismus durch ein hochgestelltes  $^\circ$  an, also etwa  $w : 45 \mapsto 45^\circ$ , und spricht von **Grad**. Die Umkehrabbildung notieren wir  $\text{Grad} : \mathbb{W} \xrightarrow{\sim} [0, 360)$ .
  2. Bei Vermessungsarbeiten wird der Gruppenhomomorphismus  $w$  meist so gewählt, daß  $b = 400$  die kleinste positive Zahl ist, die auf die Identität abgebildet wird. Dabei wird üblicherweise „im Uhrzeigersinn“ gemessen, als da heißt, wenn man eine Uhr so auf die Erde legt, daß man sie von oben lesen kann, hat der Winkel von zwölf Uhr nach drei Uhr in dieser Konvention das Winkelmaß 100. Die Wahl 400 hat den Vorteil, daß einem rechten Winkel als Winkelmaß die Zahl 100 entspricht. Das ist beim Arbeiten mit Digitalanzeigen besonders praktisch. Man deutet das Anwenden dieses Gruppenhomomorphismus durch ein nachgestelltes gon an, und spricht von **Neugrad** oder **Gon**.
  3. Beim Bedienen eines Taschenrechners arbeitet man oft mit einer Wahl des Gruppenhomomorphismus  $w$ , die zusätzlich zu ihrer Verträglichkeit mit der Orientierung dadurch ausgezeichnet ist, daß der „Geschwindigkeitsvektor“ von  $t \mapsto w(t)(\vec{v})$  für alle  $t$  und  $\vec{v}$  dieselbe Länge hat wie  $\vec{v}$ . Das bedeutet dann die Wahl  $b = 2\pi$ , und hier ist das  $\pi = 3,1415\dots$  aus der Analysis gemeint, also das Verhältnis zwischen Umfang und Durchmesser einer Kreislinie nach **??**. Für diese Wahl gilt die Beziehung  $\cos_g \circ w = \cos_a$  zwischen geometrischem und analytischem Cosinus und die analoge Beziehung für den Sinus. Man deutet das Anwenden dieses Gruppenhomomorphismus durch ein nachgestelltes rad an und spricht von **Radian** oder deutsch **Bogenmaß**.
  4. In der Mathematik ist es üblich, zwar mit der Wahl  $b = 2\pi$  zu arbeiten, also im eben eingeführten Bogenmaß, informell aber so zu tun, als ob man die Wahl  $b = 2$  getroffen habe und dies durch das Symbol  $\pi$  andeute. Die dabei entstehenden Ausdrücke haben den Vorteil, daß sie informell besonders

gut verständlich sind. Sie haben den Nachteil, daß man aus dem Kontext erschließen muß, ob ein Winkel  $\alpha \in \mathbb{W}$  oder vielmehr eine reelle Zahl  $\alpha \in \mathbb{R}$  gemeint ist.

5. Es gibt Bestrebungen, eine neue Konvention einzuführen, bei der man statt mit  $\pi$  mit  $\tau := 2\pi$  arbeitet.

Zum Beispiel sind die Bezeichnungen für einen im Gegenuhrzeigersinn orientierten rechten Winkel in den verschiedenen Notationssystemen

$$90^\circ = 300 \text{ gon} = \pi/2 = \tau/4 \approx 1,5708 \text{ rad}$$

**4.1.8.3 (Unsere Konventionen).** Wir arbeiten im folgenden mit  $b = 2\pi$  und verwenden die Bijektion  $w : (-\pi, \pi] \xrightarrow{\sim} \mathbb{W}$ , die von unserem Gruppenhomomorphismus  $w = \text{wk} \circ u : \mathbb{R} \rightarrow \mathbb{W}$  aus 4.1.7.14 induziert wird. Wir erinnern an die in 4.1.7.14 erklärten Identitäten  $\cos_g \circ \text{wk} \circ u = \cos_a$  und  $\sin_g \circ \text{wk} \circ u = \sin_a$ . Die Umkehrabbildung zu  $w : (-\pi, \pi] \xrightarrow{\sim} \mathbb{W}$  notieren wir

$$\text{Rad} : \mathbb{W} \xrightarrow{\sim} (-\pi, \pi]$$

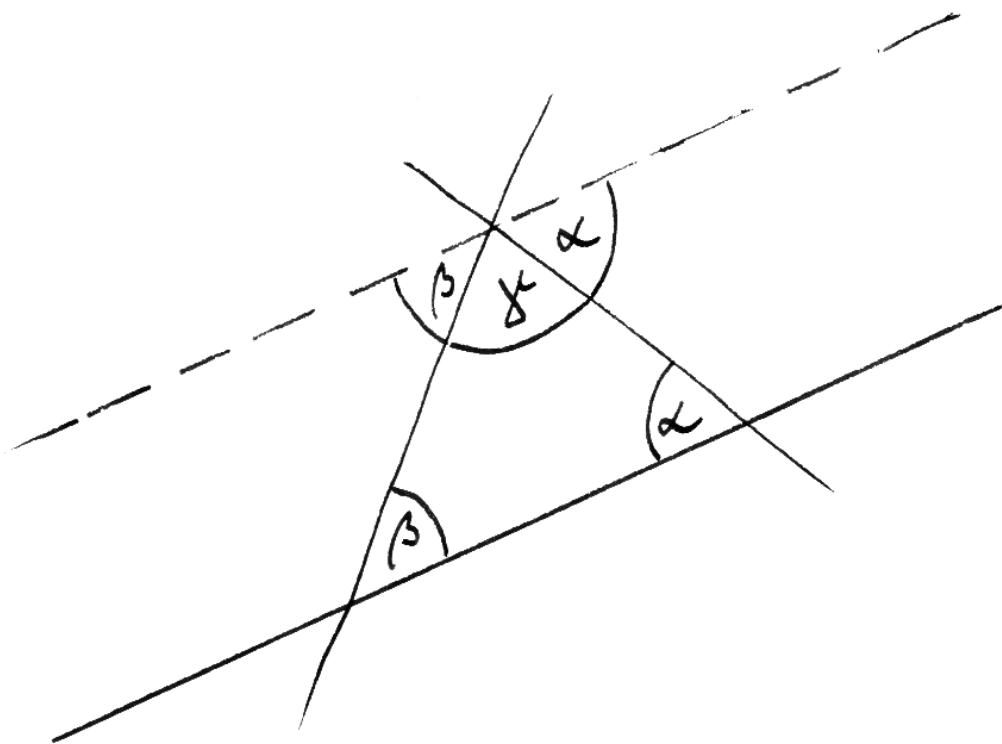
mit Rad als Abkürzung für **Radian**. Damit haben wir also  $\cos_a \circ \text{Rad} = \cos_g$  und  $\sin_a \circ \text{Rad} = \sin_g$  und  $\text{Rad}(0,56 \text{ rad}) = 0,56$ . Gegeben ein angeordneter Zweistrahl  $(A, B)$  bezeichnet mithin

$$\text{Rad } \angle(A, B) \in (-\pi, \pi]$$

das Bogenmaß des zugehörigen Elements der Winkelgruppe. Gegeben linear unabhängige Vektoren  $v, w$  ist ihr Winkelmaß  $\text{Rad } \angle(v, w)$  positiv genau dann, wenn sie eine positiv orientierte Basis bilden, und für  $v \neq 0$  haben wir  $\text{Rad } \angle(v, -v) = \pi$ . Schließlich gilt in unseren Konventionen für jeden Winkel  $\alpha \in \mathbb{W}$  auch noch die Beziehung  $\text{Rad } |\alpha| = |\text{Rad } \alpha|$ .

**4.1.8.4 (Terminologie).** Im folgenden werden wir oft einfach nur **Winkel** sagen und es dem Leser überlassen, aus dem Kontext zu erschließen, ob damit Zweistrahlen, angeordnete Zweistrahlen, Elemente von Winkelgruppen, Elemente von Winkelmengen oder auch eines der üblichen Winkelmaße gemeint sind. Oft läßt man auch die Spezifizierung des Winkelmaßes aus der Notation weg und hofft, daß der Leser aus dem Kontext erschließen kann, ob ein abstrakter Winkel oder sein Maß gemeint ist, und in letzterem Fall, nach welcher Konvention denn nun gemessen werden soll.

*Beispiel 4.1.8.5.* Die drei Vektoren der Standardbasis des  $\mathbb{R}^3$  bilden ein gleichseitiges Dreieck und der Winkel an jeder Ecke sollte folglich das Bogenmaß  $\pi/3$  haben. In der Tat finden wir für  $v = e_3 - e_1$  und  $w = e_2 - e_1$  als Skalarprodukt  $\langle v, w \rangle = 1$  und wegen  $\|v\| = \|w\| = \sqrt{2}$  ergibt sich für den Winkel in der Tat  $\cos \angle(v, w) = 1/2$  und  $\text{Rad } \angle(v, w) = \pi/3$ .



Der auf der Schule übliche Beweis dafür, daß die Winkelsumme im Dreieck  $180^\circ$  beträgt.

4.1.8.6. Unter einem **Dreieck** in einem affinen Raum verstehen wir eine Menge von drei nicht kollinearen Punkten. Standardmäßig bezeichnen man diese Punkte mit  $A, B, C$  und nennt sie die **Ecken** des Dreiecks. Für ein Dreieck in einer euklidischen Ebene  $E$  notieren wir

$$\alpha := \angle(B - A)(C - A)$$

seinen **Winkel bei**  $A$  und notieren analog  $\beta, \gamma$  seine Winkel bei  $B, C$ .

**Proposition 4.1.8.7 (Winkelsumme im Dreieck).** *Gegeben ein Dreieck in einer euklidischen Ebene ist die Summe seiner drei Winkel der gestreckte Winkel.*

*Beweis.* Sei  $E$  unsere euklidische Ebene. Seien  $A, B, C \in E$  die Ecken unseres Dreiecks. Wir kürzen die „Kantenvektoren“ ab zu  $\vec{a} := B - C, \vec{b} := C - A$  und  $\vec{c} := A - B$ . Wählen wir eine Orientierung auf  $\vec{E}$ , so wissen wir wegen der Additivität 4.1.7.8 der orientierten Winkel bereits

$$\angle(\vec{a}, -\vec{b}) + \angle(-\vec{b}, \vec{c}) + \angle(\vec{c}, -\vec{a}) = \angle(\vec{a}, -\vec{a})$$

Wenn wir in der Mitte beide Vektoren negativ machen, ändert sich der orientierte Winkel nicht. Wir haben also etwas übersichtlicher auch

$$\angle(\vec{a}, -\vec{b}) + \angle(\vec{b}, -\vec{c}) + \angle(\vec{c}, -\vec{a}) = \angle(\vec{a}, -\vec{a})$$

Andererseits gilt  $\vec{a} + \vec{b} + \vec{c} = \vec{0}$ . Aus dieser Identität folgt, daß  $(\vec{a}, -\vec{b}), (\vec{b}, -\vec{c})$  und  $(\vec{c}, -\vec{a})$  drei gleich orientierte Basen sind, da die entsprechenden Basiswechselmatrizen alle positive Determinante haben. Wir können also, indem wir andernfalls die andere Orientierung wählen, alle drei positiv orientiert annehmen. Dann aber stimmen die orientierten mit den nichtorientierten Winkeln überein und wir erhalten

$$\gamma + \alpha + \beta = \angle(\vec{a}, -\vec{a})$$

□

4.1.8.8. Aus unserer Gleichung  $\alpha + \beta + \gamma = \angle(\vec{a}, -\vec{a})$  in der Winkelgruppe  $\mathbb{W}$  folgt

$$\text{Rad } \gamma + \text{Rad } \alpha + \text{Rad } \beta \in \pi + 2\pi\mathbb{Z}$$

Für jeden Winkel  $\vartheta$  eines Dreiecks gilt aber offensichtlich auch  $\text{Rad}(\vartheta) \in (0, \pi)$ . Da damit alle drei Summanden links zu  $(0, \pi)$  gehören müssen und da weiter gilt  $(0, 3\pi) \cap (\pi + 2\pi\mathbb{Z}) = \{\pi\}$ , folgt sogar

$$\text{Rad } \alpha + \text{Rad } \beta + \text{Rad } \gamma = \pi$$

Natürlich können wir genausogut mit dem Gradmaß  $\text{Grad} : \mathbb{W}^+ \xrightarrow{\sim} [0, 180]$  arbeiten und erhalten so die äquivalente Aussage

$$\text{Grad } \alpha + \text{Grad } \beta + \text{Grad } \gamma = 180$$

Sie entspricht vermutlich am ehesten dem, was Sie in der Schule gelernt haben.

4.1.8.9 (**Weitere Notationen für Dreiecke**). Gegeben ein Dreieck mit den Ecken  $A, B, C$  in einer euklidischen Ebene  $E$  bezeichne

$$a := \|B - C\|$$

je nach Kontext die  $m$ -Norm  $a \in \mathbb{R}$  der der Ecke  $A$  gegenüberliegenden Seite für fest gewähltes  $m \in \vec{E} \setminus 0$  oder ihre abstrakte Länge  $a \in \mathbb{L}(\vec{E})$  im Sinne von 4.1.5.12. Meist wird es auf diesen Unterschied gar nicht ankommen und wir reden unterschiedslos von der „Seitenlänge“. Analog erklären wir die Seitenlängen  $b$  und  $c$ .

4.1.8.10. Gegeben ein Dreieck mit den Ecken  $A, B, C$  in einer euklidischen Ebene  $E$  mit einem rechten Winkel bei  $C$  gilt

$$\cos(\beta) = a/c$$

In der Tat gibt es nach 4.1.2.13 einen Isomorphismus von euklidischen Ebenen  $E \xrightarrow{\sim} \mathbb{R}^2$  mit  $B \mapsto 0$  und  $C \mapsto e_1$ . Nach einer Streckung dürfen wir annehmen, daß  $A$  auf dem Einheitskreis zu liegen kommt und  $C$  auf  $\mathbb{R}_{>0}e_1$ . Dann gilt also  $c = 1$  und  $a = \cos(\beta)$  nach unserer Definition des Cosinus.

4.1.8.11. Dreiecke  $\{A, B, C\}$  und  $\{A', B', C'\}$  in einer euklidischen Ebene heißen **kongruent**, wenn es eine Kongruenz  $k$  gibt mit  $k(\{A, B, C\}) = \{A', B', C'\}$ . Ein Dreieck mit einer Anordnung seiner Ecken nenne ich ein **angeordnetes Dreieck** und notiere es  $(A, B, C)$ . Angeordnete Dreiecke  $(A, B, C)$  und  $(A', B', C')$  in einer euklidischen Ebene heißen **angeordnet kongruent**, wenn es eine Kongruenz  $k$  gibt mit  $k(A, B, C) = (A', B', C')$ .

## Übungen

*Übung 4.1.8.12.* Man zeige den **Cosinus-Satz**  $a^2 + b^2 - 2ab \cos \gamma = c^2$  für jedes Dreieck mit positiven Seitenlängen  $a, b, c$  und jeweils den entsprechenden Seiten gegenüberliegenden nichtorientierten Winkeln  $\alpha, \beta, \gamma$ . Man zeige in denselben Notationen auch den **Sinus-Satz**

$$\frac{\sin \alpha}{a} = \frac{\sin \beta}{b} = \frac{\sin \gamma}{c}$$

Hinweis: Man wähle eine Seite als horizontale Seite aus und berechne die Höhe unseres Dreiecks auf verschiedene Weisen. Hier meinen  $a, b, c$  die  $m$ -Normen der jeweiligen Seiten in Bezug auf einen festen von Null verschiedenen Richtungsvektor  $m$ .

*Übung 4.1.8.13.* Je zwei angeordnete Dreiecke  $(A, B, C)$  und  $(A', B', C')$  einer euklidischen Ebene mit zwei gleichen Seiten  $a = a'$  sowie  $b = b'$  und gleichem

eingeschlossenen Winkel  $\gamma = \gamma'$  sind angeordnet kongruent. Gilt statt  $\gamma = \gamma'$  eine der Gleichheiten  $\alpha = \alpha'$  oder  $\beta = \beta'$ , so brauchen unsere angeordneten Dreiecke nicht kongruent sein.

*Übung 4.1.8.14.* Je zwei angeordnete Dreiecke  $(A, B, C)$  und  $(A', B', C')$  einer euklidischen Ebene mit gleichen Seiten  $c = c'$  sowie gleichen anliegenden Winkeln  $\alpha = \alpha'$  und  $\beta = \beta'$  sind angeordnet kongruent. Dasselbe gilt auch unter der Annahme ( $c = c'$  und  $\alpha = \alpha'$  und  $\gamma = \gamma'$ ). Hinweis: Sinussatz und vorhergehende Übungen.

*Übung 4.1.8.15.* Je zwei angeordnete Dreiecke  $(A, B, C)$  und  $(A', B', C')$  einer euklidischen Ebene mit drei gleichen Seiten  $a = a'$ ,  $b = b'$ ,  $c = c'$  sind angeordnet kongruent. Hinweis: Cosinussatz und vorhergehende Übungen.

*Übung 4.1.8.16.* Gegeben Strahlen  $F, G, H$  in einem orientierten zweidimensionalen euklidischen Vektorraum liefert die Additivität der orientierten Winkel 4.1.7.8 für ihre Bogenmaße die Regel

$$\text{Rad } \angle(F, G) + \text{Rad } \angle(G, H) \in \text{Rad } \angle(F, H) + 2\pi\mathbb{Z}$$

*Übung 4.1.8.17.* Gegeben von Null verschiedene Vektoren  $v, w$  in einem orientierten zweidimensionalen reellen euklidischen Vektorraum haben wir stets die Alternative  $\text{Rad } \angle(v, w) + \text{Rad } \angle(w, -v) = \pm\pi$ .

*Ergänzende Übung 4.1.8.18 (Winkelsumme im Vieleck).* Sei in einer orientierten euklidischen Ebene  $E$  eine sich periodisch wiederholende Folge  $p_0, \dots, p_n = p_0, p_{n+1} = p_1, \dots$  mit  $p_1, \dots, p_n$  paarweise verschieden gegeben derart, daß die halboffenen Segmente  $[p_{i-1}, p_i]$  für  $1 \leq i \leq n$  paarweise disjunkt sind. Es gebe einen Richtungsvektor  $\vec{v} \neq 0$  derart, daß  $p_0 + \mathbb{R}_{>0}\vec{v}$  keines unserer Segmente trifft und daß  $(\vec{v}, p_1 - p_0)$  eine positiv orientierte Basis von  $\vec{E}$  ist. So gilt in unseren Konventionen 4.1.8.3 die Identität

$$\sum_{i=1}^n \text{Rad } \angle(p_i - p_{i-1}, p_{i+1} - p_i) = 2\pi$$

Hinweis: Gibt es zwei Ecken  $p_r \neq p_s$  derart, daß das offene Segment  $(p_r, p_s)$  keines unserer Segmente  $[p_{i-1}, p_i]$  trifft und daß alle Ecken in ein- und derselben abgeschlossenen Halbebene zur Gerade durch  $p_r$  und  $p_s$  liegen, so führt „Zerlegen in zwei Polygonzüge durch Einfügen einer doppelten Kante  $[p_r, p_s]$ “ zusammen mit vollständiger Induktion zum Ziel. Gibt es keine zwei derartigen Ecken, so erkennt man „unschwer“, daß unser Polygonzug „konvex“ ist in dem Sinne, daß für je zwei Ecken  $p_r \neq p_s$  mit  $s \neq r \pm 1$  das offene Segment  $(p_r, p_s)$  keines unserer Segmente  $[p_{i-1}, p_i]$  trifft, und dann kommen wir wieder durch „Zerlegen in zwei Polygonzüge“ und Induktion ans Ziel.

### 4.1.9 Kreuzprodukt und Spatprodukt

**Satz 4.1.9.1.** Gegeben ein dreidimensionaler orientierter reeller Skalarprodukt Raum  $V$  gibt es genau eine alternierende bilineare Abbildung  $V \times V \rightarrow V$  mit der Eigenschaft  $(\vec{v}_1, \vec{v}_2) \mapsto \vec{v}_3$  für jede orientierte Orthonormalbasis  $\vec{v}_1, \vec{v}_2, \vec{v}_3$ . Sie heißt das **Kreuzprodukt** wegen der für unsere Abbildung allgemein gebräuchlichen Notation

$$(\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$$

4.1.9.2. Aus der Definition folgt sofort, daß  $(\vec{v} \times \vec{w})$  auf  $\vec{v}$  und  $\vec{w}$  senkrecht steht, indem wir etwa eine angeordnete Orthonormalbasis derart wählen, daß  $\vec{v}$  und  $\vec{w}$  im Erzeugnis der ersten beiden Basisvektoren liegen.

4.1.9.3 (Diskussion von Varianten des Begriffs und der Terminologie). Eine mit den benötigten Einheiten versehene Variante des Kreuzprodukts für dreidimensionale euklidische Vektorräume diskutieren wir in 4.6.4.9. Andere Autoren bezeichnen unser Kreuzprodukt als **Vektorprodukt**, da es als Resultat eben Vektoren liefert im Gegensatz zum Skalarprodukt, das Skalare liefert. Ich habe für das Kreuzprodukt alias Vektorprodukt auch schon die alternative Notation  $[\vec{v}, \vec{w}]$  gesehen, die aber erst im Kontext von ?? ihre Verträglichkeit mit an wieder anderer Stelle üblichen Notationen zeigt. Noch seltener sieht man die Notation  $\vec{v} \wedge \vec{w}$ , die hinwiederum in 4.6.5.29 ihre Verträglichkeit mit dem dort eingeführten „Dachprodukt“  $\wedge$  zeigt. Ich mag diese letzte Notation nicht, denn das Dachprodukt in seiner üblichen Definition ist im Gegensatz zu unserem Kreuzprodukt durchaus assoziativ.

*Beweis.* Ohne Beschränkung der Allgemeinheit dürfen wir annehmen,  $V$  sei der  $\mathbb{R}^3$  mit seinem Standard-Skalarprodukt und seiner Standard-Orientierung. Wenn es in diesem Fall überhaupt eine bilineare Abbildung  $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$  mit den im Satz geforderten Eigenschaften gibt, dann muß diese offenichtlich durch die Vorschrift

$$\left( \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \right) \mapsto \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ v_3 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{pmatrix}$$

gegeben werden. Es bleibt damit nur noch zu zeigen, daß die durch diese Formel definierte bilineare Abbildung, die wir schon mal  $(\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$  notieren und für den Rest dieses Beweises das **konkrete Kreuzprodukt** nennen, auch wirklich die im Satz geforderte Eigenschaft hat. In Anbetracht der Jägerzaunformel 3.6.2.3 gilt für unser konkretes Kreuzprodukt offensichtlich schon mal die Identität

$$\langle \vec{u}, \vec{v} \times \vec{w} \rangle = \det(\vec{u} | \vec{v} | \vec{w})$$

Umgekehrt legt aber diese Eigenschaft für alle  $\vec{u} \in \mathbb{R}^3$ , ja sogar schon für  $\vec{u} = \vec{e}_1, \vec{e}_2, \vec{e}_3$  auch bereits den Vektor  $\vec{v} \times \vec{w}$  fest. Daraus folgern wir hinwiederum für alle Drehungen  $A \in \text{SO}(3)$  die Identität

$$(A\vec{v}) \times (A\vec{w}) = A(\vec{v} \times \vec{w})$$

In der Tat folgt diese Identität von Vektoren, wenn wir zeigen können, daß die Skalarprodukte beider Seiten mit allen Vektoren  $\vec{u}$  oder auch mit allen Vektoren  $A\vec{u}$  übereinstimmen. Dafür rechnen wir einfach  $\langle A\vec{u}, A(\vec{v} \times \vec{w}) \rangle = \langle \vec{u}, \vec{v} \times \vec{w} \rangle = \det(\vec{u}|\vec{v}|\vec{w}) = \det A(\vec{u}|\vec{v}|\vec{w}) = \det(A\vec{u}|A\vec{v}|A\vec{w}) = \langle A\vec{u}, (A\vec{v}) \times (A\vec{w}) \rangle$ . Also gilt in der Tat  $A(\vec{v} \times \vec{w}) = (A\vec{v}) \times (A\vec{w})$  für alle  $A \in \text{SO}(3)$ . Da sich aber je zwei orientierte Orthonormalbasen des  $\mathbb{R}^3$  durch eine Drehung  $A \in \text{SO}(3)$  ineinander überführen lassen, folgt unmittelbar, daß unser konkretes Kreuzprodukt die im Satz geforderte Eigenschaft hat.  $\square$

*Ergänzung 4.1.9.4.* Für den Ausdruck  $\langle \vec{u}, \vec{v} \times \vec{w} \rangle = \det(\vec{u}|\vec{v}|\vec{w})$  aus dem vorhergehenden Beweis mit  $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^3$  findet man manchmal auch die Notation  $\langle \vec{u}, \vec{v}, \vec{w} \rangle$  und die Bezeichnung als **Spatprodukt**, die darauf anspielt, daß diese Determinante ja nach 3.6.2.6 bis auf ein Vorzeichen gerade das Volumen des durch die fraglichen drei Vektoren gegebenen Parallelepipseds angibt. Die Kristalle des Feldspats haben aber nun oft die Gestalt eines Parallelepipseds, weswegen derartige Körper auch als **Spatte** bezeichnet werden. In 4.6.4.3 diskutieren wir eine Variante des Spatprodukts für beliebige dreidimensionale euklidische Vektorräume.

**4.1.9.5 (Die schmutzige Anschauung für das Kreuzprodukt).** Setzen wir im Fall eines linear unabhängigen Paares  $(\vec{v}, \vec{w})$  in obiger Formel  $\langle \vec{u}, \vec{v} \times \vec{w} \rangle = \det(\vec{u}|\vec{v}|\vec{w})$  für die Beziehung von Kreuzprodukt, Skalarprodukt und Determinante den Vektor

$$\vec{u} = (\vec{v} \times \vec{w}) / \|\vec{v} \times \vec{w}\|$$

ein, so erkennen wir aus der anschaulichen Bedeutung 3.6.2.6 der Determinante als Volumen, daß wir uns die Länge von  $\vec{v} \times \vec{w}$  gerade als das Volumen des von  $\vec{u}, \vec{v}, \vec{w}$  aufgespannten Spats alias die Fläche des von  $\vec{v}, \vec{w}$  aufgespannten Parallelograms denken dürfen. Damit erkennen wir, daß das Kreuzprodukt anschaulich wie folgt interpretiert werden kann: Für  $\vec{v}, \vec{w}$  linear abhängig gilt  $\vec{v} \times \vec{w} = \vec{0}$ ; Sonst ist  $\vec{v} \times \vec{w}$  der Vektor, der senkrecht steht auf  $\vec{v}$  und  $\vec{w}$ , dessen Länge der anschaulichen Fläche des von  $\vec{v}$  und  $\vec{w}$  aufgespannten Parallelogramms entspricht, und dessen Richtung dadurch festgelegt wird, daß  $(\vec{v} \times \vec{w}, \vec{v}, \vec{w})$  eine orientierte Basis ist.

## Übungen

*Übung 4.1.9.6 (Einzigkeit des Kreuzprodukts).* Man zeige: Gegeben ein dreidimensionaler reeller Skalarproduktraum  $V$  bilden die bilinearen Abbildungen

$\varphi : V \times V \rightarrow V$  mit der Eigenschaft  $\varphi(Av, Aw) = A\varphi(v, w)$  für alle  $v, w \in V$  und  $A \in \mathrm{SO}(V)$  einen eindimensionalen Untervektorraum des Vektorraums aller Abbildungen  $V \times V \rightarrow V$ . Es besteht insbesondere keine Hoffnung, neben dem Kreuzprodukt noch weitere „geometrisch bedeutsame“ bilineare Verknüpfungen auf  $V$  zu finden. Hinweis: Ohne Beschränkung der Allgemeinheit sei  $V$  der  $\mathbb{R}^3$  mit dem Standardskalarprodukt. Es gibt eine Drehung mit  $e_1 \mapsto e_2$  und  $e_2 \mapsto -e_1$ . Man folgere, daß  $\varphi$  alternierend sein muß. Es gibt eine Drehung mit  $e_1 \mapsto e_2$  und  $e_2 \mapsto e_1$  und Drehachse  $e_2 + e_1$ . Man folgere, daß  $\varphi(e_1, e_2)$  auf  $e_2 + e_1$  senkrecht stehen muß.

*Übung 4.1.9.7.* Gegeben ein dreidimensionaler orientierter reeller Skalarprodukt Raum zeige man  $\vec{u} \times (\vec{v} \times \vec{w}) = \langle \vec{u}, \vec{w} \rangle \vec{v} - \langle \vec{u}, \vec{v} \rangle \vec{w}$ .

#### 4.1.10 Abstandserhaltende Abbildungen

**Proposition 4.1.10.1.** *Gegeben reelle Skalarprodukträume  $V, W$  ist eine Abbildung  $f : V \rightarrow W$  linear und orthogonal genau dann, wenn sie den Ursprung auf den Ursprung abbildet und alle Abstände erhält, in Formeln  $f(0) = 0$  und*

$$\|f(v) - f(w)\| = \|v - w\| \quad \forall v, w \in V$$

4.1.10.2. Man beachte, daß die Linearität von  $f$  nicht vorausgesetzt, sondern vielmehr aus unseren Annahmen gefolgert wird.

*Beweis.* Zunächst beachten wir die **Polarisierungsidentität**

$$2\langle v, w \rangle = \|v + w\|^2 - \|v\|^2 - \|w\|^2$$

oder für diesen Beweis besser ihre Variante  $2\langle v, w \rangle = \|v\|^2 + \|w\|^2 - \|v - w\|^2$ . Da unsere Abbildung den Ursprung und alle Abstände erhält, erhält sie auch die Norm aller Vektoren, und wir folgern schon einmal

$$\langle f(v), f(w) \rangle = \langle v, w \rangle \quad \forall v, w \in V$$

Um weiter  $f(\lambda v) = \lambda f(v)$  zu zeigen, beachten wir

$$\langle f(\lambda v) - \lambda f(v), f(u) \rangle = \langle \lambda v, u \rangle - \lambda \langle v, u \rangle = 0$$

für alle  $u \in V$  und folgern  $\langle f(\lambda v) - \lambda f(v), z \rangle = 0$  für alle  $z$  im Erzeugnis des Bildes  $f(V)$ . Nehmen wir dann speziell  $z = f(\lambda v) - \lambda f(v)$ , so ergibt sich erst  $\|f(\lambda v) - \lambda f(v)\|^2 = 0$  und dann  $f(\lambda v) = \lambda f(v)$ . In derselben Weise finden wir

$$\langle f(v + w) - f(v) - f(w), f(u) \rangle = \langle v + w, u \rangle - \langle v, u \rangle - \langle w, u \rangle = 0$$

für alle  $u \in V$  und folgern  $f(v + w) = f(v) + f(w)$ , womit dann auch die Linearität von  $f$  gezeigt wäre.  $\square$

4.1.10.3. Ein **affiner Skalarproduktraum** ist ein Paar bestehend aus einem reellen affinen Raum und einem Skalarprodukt auf seinem Richtungsraum. Gegeben zwei Punkte  $p, q$  definieren wir dann ihren **Abstand** alias ihre **Distanz** als die Norm des zugehörigen Richtungsvektors, in Formeln

$$d(p, q) := \|p - q\|$$

Eine Abbildung  $f : E \rightarrow E'$  zwischen affinen Skalarprodukträumen, die alle Abstände erhält, nennt man auch **isometrisch** oder eine **Isometrie**. Die Terminologie geht auf griechisch  $\iota\sigmao\varsigma$  für deutsch „gleich“ zurück. In Formeln fordern wir von einer Isometrie also

$$d(f(p), f(q)) = d(p, q) \quad \forall p, q \in E$$

*Ergänzung 4.1.10.4.* Dieselbe Begriffsbildung verwendet man auch allgemeiner für Abbildungen zwischen sogenannten „metrischen Räumen“, wie sie etwa in ?? erklärt werden. Ist eine Isometrie bijektiv, so spricht man von einem **isometrischen Isomorphismus**.

*Ergänzung 4.1.10.5 (Diskussion der Terminologie).* Ich habe auch schon die alternative Terminologie gesehen, in der nur unsere isometrischen Isomorphismen als „Isometrien“ bezeichnet werden und unsere Isometrien als „isometrische Abbildungen“.

**Satz 4.1.10.6 (Isometrien zwischen affinen Skalarprodukträumen).** Eine Abbildung zwischen affinen Skalarprodukträumen ist eine Isometrie genau dann, wenn sie affin ist mit orthogonalem linearem Anteil.

*Beweis.* Sei  $\varphi : E \rightarrow F$  unsere Abbildung und sei  $p \in E$  beliebig gewählt. Erklären wir  $\vec{\varphi}_p : \vec{E} \rightarrow \vec{F}$  durch  $\varphi(p + \vec{v}) = \varphi(p) + \vec{\varphi}_p(\vec{v})$ , so bildet  $\vec{\varphi}_p : \vec{E} \rightarrow \vec{F}$  offensichtlich den Ursprung auf den Ursprung ab und erhält alle Abstände. Nach der Proposition 4.1.10.1 ist folglich  $\vec{\varphi}_p$  linear und orthogonal und nach 3.3.1.17 ist damit  $\varphi$  affin mit orthogonalem linearem Anteil. Der Beweis der Gegenrichtung kann dem Leser überlassen bleiben.  $\square$

4.1.10.7 (Diskussion der Terminologie). Aus der Schule kennen Sie vermutlich bereits **Punktspiegelungen** an einem Punkt  $p$ , die durch die Vorschrift  $p + \vec{v} \mapsto p - \vec{v}$  gegeben werden. Wir wollen jedoch vereinbaren, daß mit **Spiegelungen** stets lineare oder affine Abbildungen mit einer Fixpunktmenge der Kodimension Eins gemeint sind, deren Quadrat die Identität ist. Punktspiegelungen heißen zwar verwirrenderweise ähnlich, sind aber nur im eindimensionalen Fall Spiegelungen in unserem Sinne.

4.1.10.8. Gegeben ein euklidischer Raum  $E$  verstehen wir unter dem **Abstand** zweier Punkte  $p, q \in E$  das Element  $\|p - q\| \in \mathbb{L}(\vec{E})$  der zugehörigen Längengrade. Eine Selbstabbildung  $f : E \rightarrow E$  heißt **abstandserhaltend**, wenn gilt

$$\|p - q\| = \|f(p) - f(q)\| \quad \forall p, q \in E$$

Aus dem Vorhergehenden folgt, daß die abstandserhaltenden Selbstabbildungen eines endlichdimensionalen euklidischen Raums genau seine orthogonalaffinen Automorphismen aus 4.1.5.4 sind. Insbesondere sind die abstandserhaltenden Selbstabbildungen einer euklidischen Ebene nach 4.1.5.7 genau ihre Kongruenzen.

**Satz 4.1.10.9 (Abstandserhaltende Selbstabbildungen euklidischer Räume).** *Jede abstandserhaltende Selbstabbildung  $\varphi : E \rightarrow E$  eines endlichdimensionalen euklidischen Raums  $E$  läßt sich eindeutig darstellen als die Hintereinanderausführung*

$$\varphi = (+\vec{w}) \circ d$$

*einer abstandserhaltenden Selbstabbildung  $d : E \rightarrow E$  mit Fixpunkt gefolgt von einer Verschiebung um einen Richtungsvektor  $\vec{w}$ , der unter dieser abstandserhaltenden Selbstabbildung  $d$  invariant ist, in Formeln  $\vec{d}(\vec{w}) = \vec{w}$ .*

4.1.10.10. Gegeben eine abstandserhaltende Selbstabbildung  $\varphi$  eines endlichdimensionalen euklidischen Raums  $E$  gibt es also in Formeln ausgedrückt genau ein Paar  $(d, \vec{w})$  bestehend aus einer abstandserhaltenden Selbstabbildung  $d$  mit mindestens einem Fixpunkt sowie einem Richtungsvektor  $\vec{w}$  derart, daß gilt

$$\varphi = (+\vec{w}) \circ d \quad \text{und} \quad \vec{d}(\vec{w}) = \vec{w}.$$

Offensichtlich gilt dann sogar  $\varphi = (+\vec{w}) \circ d = d \circ (+\vec{w})$ . Natürlich haben  $d$  und  $\varphi$  denselben linearen Anteil, in Formeln  $\vec{d} = \vec{\varphi}$ . Jede abstandserhaltende Selbstabbildung kann also nochmal anders gesagt dargestellt werden durch eine Abbildungsvorschrift der Gestalt  $\varphi(p + \vec{u}) = p + A(\vec{u}) + \vec{w}$  mit  $p \in E$  und  $A \in O(\vec{E})$  orthogonal und  $\vec{w} \in \vec{E}^A$  einem Fixvektor von  $A$ .

*Beweis.* Wir beginnen mit einer Vorüberlegung. Gegeben ein orthogonaler Automorphismus  $f$  eines endlichdimensionalen Skalarproduktraums  $V$  ist der Fixpunkttraum  $\ker(f - \text{id}) = V^f$  das orthogonale Komplement von  $\text{im}(f - \text{id})$  in  $V$ , in Formeln

$$V^f = \text{im}(f - \text{id})^\perp$$

In der Tat zeigt die Dimensionsformel 3.2.2.5 in Verbindung mit 4.1.3.18, daß es ausreicht, die Inklusion  $V^f \subset \text{im}(f - \text{id})^\perp$  zu zeigen. Aus  $f(\vec{w}) = \vec{w}$  folgt aber offensichtlich  $\langle \vec{w}, f(\vec{v}) - \vec{v} \rangle = \langle f(\vec{w}), f(\vec{v}) \rangle - \langle \vec{w}, \vec{v} \rangle = 0$  für alle  $\vec{v} \in V$ . Nun beginnt der eigentliche Beweis. Natürlich kann man für einen beliebigen Punkt

$q \in E$  stets einen Vektor  $\vec{v} \in \vec{E}$  finden mit  $\varphi(q) = q + \vec{v}$  und folglich  $\varphi(q + \vec{u}) = q + \vec{v} + \vec{\varphi}(\vec{u}) \forall \vec{u} \in \vec{E}$ . Gegeben ein Richtungsvektor  $\vec{w}$  besitzt damit  $(-\vec{w}) \circ \varphi$  genau dann einen Fixpunkt, wenn es  $\vec{u} \in \vec{E}$  gibt mit

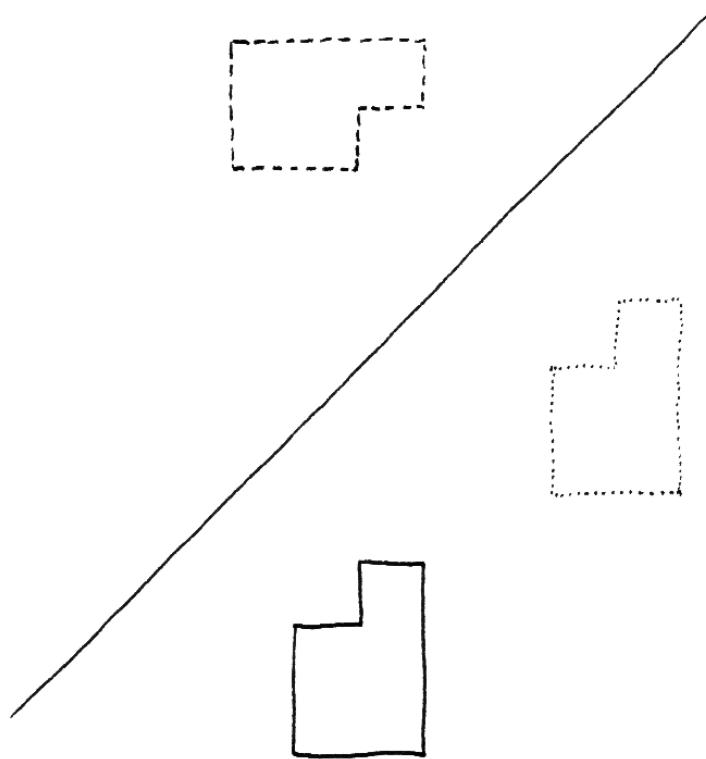
$$q + \vec{u} = q + \vec{v} + \vec{\varphi}(\vec{u}) - \vec{w}$$

alias  $(\vec{u} - \vec{\varphi}(\vec{u})) + \vec{w} = \vec{v}$ . Wegen der Zerlegung  $\vec{E} = \text{im}(\vec{\varphi} - \text{id}) \oplus \vec{E}^{\vec{\varphi}}$  aus unserer Vorüberlegung gibt es also genau ein  $\vec{w} \in \vec{E}^{\vec{\varphi}}$  derart, daß  $(-\vec{w}) \circ \varphi$  einen Fixpunkt hat.  $\square$

**Beispiel 4.1.10.11 (Abstandserhaltende Selbstabbildungen der Gerade).** Jede abstandserhaltende Selbstabbildung einer Gerade ist entweder eine Verschiebung  $x \mapsto x + a$  oder eine Spiegelung  $x \mapsto b - x$ : In der Tat, ist der lineare Anteil unserer Selbstabbildung die Identität, so handelt es sich nach 4.1.10.10 um eine Verschiebung; ist ihr linearer Anteil dagegen das Negative der Identität, so muß in der Darstellung nach 4.1.10.10 der Vektor  $\vec{w}$  der Nullvektor sein und wir haben für ein festes  $p$  eine Abbildung der Gestalt  $p + u \mapsto p - u$  vor uns. Diese Abbildung mag man als eine Spiegelung am Punkt  $p$  auffassen, sie kann etwas weniger geometrisch auch in der Form  $x \mapsto 2p - x$  geschrieben werden.

**Beispiel 4.1.10.12 (Abstandserhaltende Selbstabbildungen der Ebene).** Jede abstandserhaltende Selbstabbildung einer euklidischen Ebene ist entweder (1) eine Verschiebung oder (2) eine von der Identität verschiedene Drehung um einen Punkt oder (3) eine **Gleitspiegelung**, als da heißt eine Spiegelung an einer Gerade gefolgt von einer Verschiebung in Richtung eben dieser Gerade. In der Tat erhalten wir nach 4.1.10.10 unseren Fall (1) für die Abbildungen mit der Identität als linearem Anteil; Fall (2) für die Abbildungen mit einer von der Identität verschiedenen Drehung als linearem Anteil; und Fall (3) für die Abbildungen mit einer Spiegelung als linearem Anteil. Die Spiegelung an einer Gerade finden wir in unserer Liste als spezielle Gleitspiegelung wieder.

**Beispiel 4.1.10.13 (Abstandserhaltende Selbstabbildungen des Raums).** Jede abstandserhaltende Selbstabbildung eines dreidimensionalen euklidischen Raums ist entweder (1) eine **Verschraubung** alias eine nichttriviale Drehung um eine Achse gefolgt von einer Verschiebung in Richtung eben dieser Achse, oder (2) eine **Drehspiegelung** alias eine Drehung um eine Achse gefolgt von einer Spiegelung an einer Ebene senkrecht zu besagter Achse, oder (3) eine **Gleitspiegelung** alias eine Spiegelung an einer Ebene gefolgt von einer Verschiebung um einen Richtungsvektor besagter Ebene. In der Tat erhalten wir nach 4.1.10.10 unseren Fall (1) für die Abbildungen mit einer Drehung als linearem Anteil; Fall (2) für die Abbildungen mit linearem Anteil bestehend aus einem nichttrivialen Drehblock und einem Eintrag  $(-1)$  auf der Diagonalen; und Fall (3) für die Abbildungen mit einer Spiegelung an einer Ebene als linearem Anteil. Die Verschiebungen



Das Bild der durchgezeichneten Figur unter einer Verschiebung (gepunktet) und unter einer Gleitspiegelung (gestrichelt). Durchgezogen eingezeichnet ist auch die Gerade, längs derer die Gleitspiegelung geschieht. Unsere Gleitspiegelung ist natürlich, wie von unserem Satz 4.1.10.9 vorhergesagt, die Verknüpfung einer Isometrie mit mindestens einem Fixpunkt, hier einer Spiegelung, mit einer Translation in einer unter dem linearen Anteil dieser Isometrie invarianten Richtung, hier in Richtung der Spiegelachse.

finden wir in unserer Liste als spezielle Verschraubungen wieder, die Identität als eine spezielle Verschiebung, und die Spiegelung an einer Ebene als eine spezielle Gleitspiegelung.

### Übungen

*Übung 4.1.10.14.* Man betrachte die komplexe Zahlenebene als euklidische Ebene und betrachte die Drehung  $d$  mit Fixpunkt  $p \in \mathbb{C}$  im Uhrzeigersinn um den rechten Winkel, in Formeln gegeben durch  $d : p + z \mapsto p + iz$ . Man schreibe für einen beliebigen Richtungsvektor  $w \in \mathbb{C}$  die Verknüpfung  $(w+) \circ d$  wieder als eine Drehung. Was ist der Fixpunkt dieser neuen Drehung?

*Übung 4.1.10.15.* Jeder zweidimensionale reelle affine Raum  $E$  mit einem Skalarprodukt auf seinem Richtungsraum wird zu einer euklidischen Ebene, wenn wir als Kongruenzen alle Abbildungen  $k : E \rightarrow E$  nehmen mit

$$\|k(p) - k(q)\| = \|p - q\| \quad \forall p, q \in \mathbb{R}$$

*Übung 4.1.10.16 (Dreispiegelungssatz).* Man zeige, daß sich jedes Element der Kongruenzgruppe einer euklidischen Ebene als Verknüpfung von einer, zwei oder drei Spiegelungen darstellen läßt.

*Übung 4.1.10.17.* Welcher Fall im vorhergehenden Beispiel 4.1.10.13 deckt die sogenannten **räumlichen Punktspiegelungen** ab, die für einen festen Punkt  $p$  durch die Vorschrift  $p + \vec{v} \mapsto p - \vec{v}$  gegeben werden?

*Ergänzende Übung 4.1.10.18.* Sei  $E$  ein euklidischer Raum. Man zeige:

1. Eine bijektive affine Abbildung  $\varphi : E \xrightarrow{\sim} E$  ist genau dann eine Ähnlichkeitsabbildung, wenn für jeden orientierungserhaltenden abstandserhaltenden Automorphismus  $g$  von  $E$  auch  $\varphi \circ g \circ \varphi^{-1}$  abstandserhaltend ist;
2. Eine bijektive affine Abbildung  $\varphi : E \rightarrow E$  ist genau dann eine Ähnlichkeitsabbildung, wenn sie alle Winkel zwischen Strahlen im Richtungsraum im Sinne von 4.1.7.15 erhält;
3. Jede Ähnlichkeit mit einem Fixpunkt  $p \in E$  läßt sich eindeutig darstellen als die Verknüpfung eines abstandserhaltenden Automorphismus, der besagten Punkt  $p$  festhält, mit einer Streckung oder Stauchung der Gestalt  $p + \vec{v} \mapsto p + \lambda \vec{v}$  für wohlbestimmtes  $\lambda \in \mathbb{R}_{>0}$ ;
4. Jede Ähnlichkeit, die nicht abstandserhaltend ist, besitzt genau einen Fixpunkt.

Hinweis: Letztere Aussage kann man besonders elegant mit dem Banach'schen Fixpunktsatz ?? einsehen.

### 4.1.11 Normalformen und Matrixzerlegungen

**Satz 4.1.11.1 (Spektralsatz für unitäre Automorphismen).** *Gegeben ein unitärer Automorphismus eines endlichdimensionalen komplexen Skalarproduktraums existiert stets eine Orthonormalbasis aus Eigenvektoren.*

*Beweis.* Ist unser Raum der Nullraum, so tut es die leere Menge. Sonst finden wir nach 3.6.6.4 einen Eigenvektor und durch Renormieren natürlich auch einen Eigenvektor der Länge Eins. Da unser Automorphismus unitär ist, erhält er auch den Orthogonalraum dieses Eigenvektors und induziert auf diesem Orthogonalraum eine unitäre Abbildung. Mit Induktion über die Dimension finden wir in unserem Orthogonalraum eine Orthonormalbasis aus Eigenvektoren, und durch Hinzunehmen unseres ursprünglichen Eigenvektors der Länge Eins erhalten wir daraus die gesuchte Orthonormalbasis aus Eigenvektoren des ganzen Raums.  $\square$

**Korollar 4.1.11.2.** *Für jede unitäre Matrix  $U \in \mathrm{U}(n)$  gibt es eine weitere unitäre Matrix  $B \in \mathrm{U}(n)$  mit  $B^{-1}UB = \mathrm{diag}(z_1, \dots, z_n)$ , wobei  $z_i \in S^1 \subset \mathbb{C}$  komplexe Zahlen der Länge Eins sind.*

*Beweis.* Man findet solch eine Matrix  $B$ , indem man eine Orthonormalbasis aus Eigenvektoren von  $U : \mathbb{C}^n \rightarrow \mathbb{C}^n$  nach 4.1.11.1 als die Spalten von  $B$  nimmt: Dann gilt ja sicher  $UB = \mathrm{diag}(z_1, \dots, z_n)B$  und die Matrix  $B$  ist unitär nach Lemma 4.1.4.3.  $\square$

**Satz 4.1.11.3 (Normalform für orthogonale Matrizen).** *Gegeben ein endlichdimensionaler reeller Skalarproduktraum  $V$  und eine orthogonale Selbstabbildung  $U : V \rightarrow V$  gibt es stets eine angeordnete Orthonormalbasis  $\mathcal{B}$  von  $V$ , bezüglich derer die Matrix  ${}_{\mathcal{B}}[U]_{\mathcal{B}}$  unserer Abbildung eine blockdiagonale Gestalt der Form*

$$\mathrm{diag}\left(1, \dots, 1, -1, \dots, -1, \begin{pmatrix} c_1 & -s_1 \\ s_1 & c_1 \end{pmatrix}, \dots, \begin{pmatrix} c_r & -s_r \\ s_r & c_r \end{pmatrix}\right)$$

*hat mit  $1 > c_1 \geq \dots \geq c_r > -1$  und  $c_i^2 + s_i^2 = 1$ . Unter den angegebenen Einschränkungen wird umgekehrt besagte blockdiagonale Matrix durch unsere orthogonale Abbildung  $U$  bereits eindeutig festgelegt.*

4.1.11.4. Dieser Satz beinhaltet den Satz vom Fußball 4.1.4.14 und seine Variante 4.1.4.16 sowie die in 4.1.1.6 und 4.1.4.18 betrachteten Resultate, die sich schlicht als die Fälle  $n \leq 3$  des obigen Satzes erweisen.

*Beweis.* Der Drehblock zu  $(c_\rho, s_\rho)$  hat die komplexen Eigenwerte  $c_\rho \pm i s_\rho$ , und das zeigt bereits die behauptete Eindeutigkeit. Die Existenz ist klar im Fall  $\dim_{\mathbb{R}} V \leq 2$  nach unserer Diskussion der Gruppe  $O(2)$  aus 4.1.1.6. Zu beachten ist hierbei, daß jede ebene Spiegelung in einer geeigneten Orthonormalbasis die darstellende

Matrix  $\text{diag}(1, -1)$  hat und jede ebene Drehung in einer geeigneten Orthonormalbasis als darstellende Matrix entweder  $\text{diag}(1, 1)$  oder  $\text{diag}(-1, -1)$  oder einen Drehblock wie oben. Die Existenz folgt mit Induktion im allgemeinen, sobald wir zeigen, daß es unter der Voraussetzung  $V \geq 0$  in  $V$  stets einen von Null verschiedenen unter  $U$  invarianten Teilraum der Dimension  $\leq 2$  gibt, indem wir dann nämlich die Induktionsannahme auf diesen Teilraum und sein orthogonales Komplement anwenden. Ohne Beschränkung der Allgemeinheit dürfen wir von jetzt an  $V = \mathbb{R}^n$  mit  $n \neq 0$  annehmen und uns  $U$  als reelle Matrix denken. Nun hat  $U$  wegen  $n \neq 0$  stets einen Eigenvektor  $v = (v_1, \dots, v_n)^\top \in \mathbb{C}^n$ , sagen wir  $Uv = \lambda v$  mit  $\lambda \in \mathbb{C}$ . Dann folgt für  $\bar{v} = (\bar{v}_1, \dots, \bar{v}_n)^\top$  sofort  $U\bar{v} = \bar{\lambda}\bar{v}$  und das komplexe Erzeugnis  $\langle v, \bar{v} \rangle_{\mathbb{C}}$  dieser beiden Vektoren ist sicher auch ein  $U$ -stabiler Teilraum von  $\mathbb{C}^n$  der Dimension Eins oder Zwei. Der Schnitt  $\langle v, \bar{v} \rangle_{\mathbb{C}} \cap \mathbb{R}^n$  ist also ein  $U$ -stabiler Teilraum von  $\mathbb{R}^n$  einer Dimension  $\leq 2$ . Dieser Schnitt ist aber auch nicht Null, denn er enthält sowohl  $v + \bar{v}$  als auch  $i(v - \bar{v})$ , die wegen  $v \neq 0$  nicht beide verschwinden können.  $\square$

4.1.11.5. Der vorhergehende Beweis illustriert in meinen Augen sehr gut, wie wunderbar unsere Theorie durch ihre Erweiterung ins Komplexe vereinfacht wird. Ich selbst kenne jedenfalls keinen vergleichbar transparenten Beweis der obigen Klassifikation, der ohne die komplexen Zahlen auskommt.

**Satz 4.1.11.6 (Gram-Schmidt).** *Seien  $v_1, \dots, v_k$  linear unabhängige Vektoren eines reellen oder komplexen Skalarproduktraums. So existiert in unserem Skalarproduktraum genau ein Orthonormalsystem  $w_1, \dots, w_k$  mit*

$$w_i \in \mathbb{R}_{>0} v_i + \langle v_{i-1}, \dots, v_1 \rangle \quad \forall i$$

**Ergänzung 4.1.11.7 (Bezug zur Definition einer Bewegungsgruppe).** Ist  $V$  ein dreidimensionaler reeller Skalarproduktraum, so gibt es zu je zwei Tripeln bestehend aus einem Halbraum, einer Halbebene auf seinem Rand und einem Strahl auf deren Rand genau eine orthogonale Abbildung, die das eine Tripel in das andere überführt. Etwas präziser und in Formeln meinen wir hier Tripel von Teilmengen  $(H, E, A)$  von  $V$  derart, daß es linear unabhängige Vektoren  $v_1, v_2, v_3$  gibt mit  $A = \mathbb{R}_{\geq 0} v_1$  und  $E = \mathbb{R}_{\geq 0} v_2 + \mathbb{R} v_1$  und  $H = \mathbb{R}_{\geq 0} v_3 + \mathbb{R} v_2 + \mathbb{R} v_1$ . In der Tat sagt uns Gram-Schmid, daß jedes solche Tripel  $(H, E, A)$  durch genau eine Orthonormalbasis  $w_1, w_2, w_3$  beschrieben werden kann. Der letzte Vektor  $w_3$  wird dabei im übrigen durch die beiden anderen bereits bis auf ein Vorzeichen festgelegt, und Analoges gilt in beliebiger endlicher Dimension. Das zeigt den Bezug des Satzes von Gram-Schmid zu unserer Definition einer Bewegungsgruppe 4.1.6.8.

*Beweis.* Nach 4.1.3.18 können wir  $v_i$  eindeutig zerlegen als  $v_i = p_i + r_i$  mit  $p_i$  der orthogonalen Projektion von  $v_i$  auf  $\langle v_{i-1}, \dots, v_1 \rangle$  und  $r_i$  im orthogonalen Komplement dieses Teilraums. Wegen der linearen Unabhängigkeit der  $v_i$  gilt

hier  $r_i \neq 0$ . Für die Vektoren  $w_i := r_i/\|r_i\|$  gilt dann  $w_j \in \langle v_j, \dots, v_1 \rangle$  und  $w_i \perp \langle v_{i-1}, \dots, v_1 \rangle$  und damit  $\langle w_i, w_j \rangle = 0$  für  $i > j$ . Da andererseits auch gilt  $\langle w_i, w_i \rangle = 1$  nach Konstruktion, bilden sie in der Tat ein Orthonormalsystem, und unsere Konstruktion zeigt zusätzlich

$$w_i = v_i/\|r_i\| - p_i/\|r_i\| \in \mathbb{R}_{>0}v_i + \langle v_{i-1}, \dots, v_1 \rangle$$

Um die Eindeutigkeit zu zeigen, bemerken wir zunächst  $w_j \in \langle v_j, \dots, v_1 \rangle$  und folgern mit Dimensionsbetrachtungen  $\langle w_j, \dots, w_1 \rangle = \langle v_j, \dots, v_1 \rangle$ . So folgt

$$\langle w_i \rangle = \langle v_{i-1}, \dots, v_1 \rangle^\perp \cap \langle v_i, \dots, v_1 \rangle$$

Diese Bedingung legt  $w_i$  fest bis auf Multiplikation mit einem Skalar der Länge Eins. Es ist dann klar, daß  $w_i$  durch die zusätzliche Bedingung im Satz sogar eindeutig festgelegt wird.  $\square$

**4.1.11.8 (Orthogonalisierungsverfahren nach Gram-Schmidt).** In Worten läuft der Beweis wie folgt ab: Gegeben ist eine endliche angeordnete linear unabhängige Teilmenge unseres Skalarproduktraums. Wir beginnen mit dem ersten Vektor und normieren ihn auf Länge Eins. Dann nehmen wir uns den zweiten Vektor vor, machen ihn senkrecht zum ersten Vektor, indem wir seine orthogonale Projektion auf die vom ersten Vektor erzeugte Gerade von ihm abziehen, und normieren den so entstehenden Vektor wieder auf Länge Eins. Dann nehmen wir uns den dritten Vektor vor, machen ihn senkrecht zu den ersten beiden Vektoren, indem wir seine orthogonale Projektion auf die von den ersten beiden Vektoren erzeugte Ebene von ihm abziehen, und normieren den so entstehenden Vektor wieder auf Länge Eins. Und so machen wir immer weiter, bis wir alle Eingaben verarbeitet haben. Mit dem Normieren eines von Null verschiedenen Vektors ist dabei das Multiplizieren unseres Vektors mit dem Inversen seiner Länge gemeint. Wir schreiben das nun noch in Formeln mit den Notationen des vorhergehenden Satzes. Für unsere Basen gilt sicher  $\langle w_{i-1}, \dots, w_1 \rangle \subset \langle v_{i-1}, \dots, v_1 \rangle$  und Dimensionsvergleich liefert sogar die Gleichheit dieser Erzeugnisse. Nach der Formel für orthogonale Projektionen aus dem Beweis von 4.1.3.18 können wir also die  $w_i$  induktiv bestimmen durch die Formeln

$$\begin{aligned} r_1 &= v_1 \\ w_1 &= r_1/\|r_1\| \\ &\vdots \\ r_i &= v_i - \sum_{\nu=1}^{i-1} \langle w_\nu, v_i \rangle w_\nu \\ w_i &= r_i/\|r_i\| \\ &\vdots \end{aligned}$$

Das ist das **Gram-Schmidt'sche Orthogonalisierungsverfahren** oder etwas ungewöhnlich aber genauer **Orthonormalisierungsverfahren**.

**Korollar 4.1.11.9 (Iwasawa-Zerlegung für  $\mathrm{GL}(n; \mathbb{R})$ ).** Bezeichne  $A \subset \mathrm{GL}(n; \mathbb{R})$  die Menge aller Diagonalmatrizen mit positiven Einträgen auf der Diagonale und  $N \subset \mathrm{GL}(n; \mathbb{R})$  die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale. So liefert die Multiplikation eine Bijektion

$$\mathrm{O}(n) \times A \times N \xrightarrow{\sim} \mathrm{GL}(n; \mathbb{R})$$

*Ergänzung 4.1.11.10.* Eine Zerlegung einer Matrix  $M$  als Produkt  $M = QR$  mit  $Q$  orthogonal und  $R$  einer oberen Dreiecksmatrix gibt es auch für nicht notwendig invertierbare Matrizen. Sie wird als **QR-Zerlegung** bezeichnet, lässt sich nach Householder effektiv berechnen, und spielt eine wichtige Rolle in der Numerik.

*Beweis.* Sicher gilt  $A \cap N = \{I\}$ , folglich definiert die Multiplikation eine Injektion

$$A \times N \hookrightarrow \mathrm{GL}(n; \mathbb{R})$$

Deren Bild  $AN$  ist eine Untergruppe, die Gruppe der oberen Dreiecksmatrizen mit positiven Diagonaleinträgen, und wegen  $\mathrm{O}(n) \cap AN = \{I\}$  definiert die Multiplikation schon mal eine Injektion  $\mathrm{O}(n) \times AN \hookrightarrow \mathrm{GL}(n; \mathbb{R})$ . Es bleibt, deren Surjektivität zu zeigen. Dazu betrachten wir in  $\mathbb{R}^n$  die Standardbasis  $\mathcal{S}$ , eine beliebige angeordnete Basis  $\mathcal{B}$  und die im Gram-Schmidt-Verfahren daraus entstehende angeordnete Orthonormalbasis  $\mathcal{A}$ . Unser Satz liefert für die zugehörige Basiswechselmatrix obere Dreiecksgestalt mit positiven Diagonaleinträgen, in Formeln

$${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \in AN$$

Aus der Identität  ${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{S}} = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{S}}$  folgt dann die Surjektivität der Multiplikation  $AN \times \mathrm{O}(n) \rightarrow \mathrm{GL}(n; \mathbb{R})$ . Invertieren liefert den Rest.  $\square$

**Korollar 4.1.11.11 (Iwasawa-Zerlegung für  $\mathrm{GL}(n; \mathbb{C})$ ).** Bezeichne  $A \subset \mathrm{GL}(n; \mathbb{C})$  die Menge aller Diagonalmatrizen mit reellen positiven Einträgen auf der Diagonale und  $N \subset \mathrm{GL}(n; \mathbb{C})$  die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale. So liefert die Multiplikation eine Bijektion

$$\mathrm{U}(n) \times A \times N \xrightarrow{\sim} \mathrm{GL}(n; \mathbb{C})$$

*Beweis.* Der Beweis geht analog wie im reellen Fall 4.1.11.9.  $\square$

**Definition 4.1.11.12.** Eine Matrix  $M$  heißt **symmetrisch**, wenn sie mit ihrer eigenen Transponierten übereinstimmt, in Formeln  $M^\top = M$ . Eine symmetrische Matrix  $M \in \mathrm{Mat}(n; \mathbb{R})$  heißt **positiv definit**, wenn gilt  $x^\top M x \leq 0 \Rightarrow x = 0$ . Sie heißt **positiv semidefinit**, wenn gilt  $x^\top M x \geq 0 \forall x \in \mathbb{R}^n$ .

**Korollar\* 4.1.11.13 (Cholesky-Zerlegung).** Gegeben eine positiv definite symmetrische Matrix  $M \in \text{Mat}(n; \mathbb{R})$  gibt es genau eine untere Dreiecksmatrix  $L$  mit positiven Diagonaleinträgen und der Eigenschaft

$$M = LL^\top$$

4.1.11.14. Das  $L$  steht hier für englisch „lower triangular“.

*Beweis.* Wir betrachten auf dem  $\mathbb{R}^n$  das durch die Vorschrift  $s(x, y) := x^\top My$  erklärte Skalarprodukt  $s = s_M$ . Wenden wir nun das Gram-Schmidt-Verfahren in Bezug auf dies neue Skalarprodukt an auf die Standardbasis  $e_1, \dots, e_n$  des  $\mathbb{R}^n$ , so erhalten wir eine neue Basis  $w_1, \dots, w_n$  des  $\mathbb{R}^n$  mit  $w_i^\top M w_j = \delta_{i,j}$  und  $w_i \in \mathbb{R}_{>0} e_i + \langle e_{i-1}, \dots, e_1 \rangle$ . Die Matrix  $N := (w_1 | \dots | w_n)$  mit den  $w_i$  in den Spalten ist also eine obere Dreiecksmatrix mit der Eigenschaft  $N^\top M N = I$ . Mit  $L = (N^\top)^{-1}$  ergibt sich dann die gesuchte Zerlegung. Deren Eindeutigkeit zeigt man, indem man den Beweis rückwärts liest.  $\square$

*Ergänzung 4.1.11.15.* Das Invertieren einer oberen Dreiecksmatrix  $N$  mit positiven Diagonaleinträgen ist im Prinzip unproblematisch. Bei der numerischen Berechnung der Cholesky-Zerlegung empfiehlt es sich jedoch, das Invertieren gleich mit dem Algorithmus des Gram-Schmidt'schen Orthogonalisierungsverfahrens zu verschmelzen. Mehr dazu mögen Sie in der Numerik lernen.

## Übungen

*Übung 4.1.11.16.* Eine lineare Abbildung von komplexen Skalarprodukträumen ist unitär genau dann, wenn sie die Norm aller Vektoren erhält. Hinweis: Man beginne mit einer Variante der Polarisierungsidentität.

*Übung 4.1.11.17.* Man zeige: Gegeben ein endlichdimensionaler reeller Skalarproduktraum  $V$  und darin eine lineare Hyperebene  $H \subset V$  gibt es genau eine orthogonale lineare Abbildung  $s : V \rightarrow V$  mit unserer Hyperebene als Fixpunktmenge, in Formeln  $H = V^s$ . Diese Abbildung  $s$  heißt die **orthogonale Spiegelung an der Hyperebene  $H$**  oder auch kürzer die **Spiegelung an  $H$** .

*Übung 4.1.11.18.* Man zeige, daß sich zwei Vektoren eines endlichdimensionalen reellen Skalarproduktraums genau dann durch eine orthogonale Abbildung ineinander überführen lassen, wenn sie dieselbe Länge haben.

*Übung 4.1.11.19 (Zeichnen eines Würfels).* Man zeige: Zeichnet man einen massiven Würfel so, daß an einer Ecke alle drei angrenzenden Flächen zu sehen sind, so treffen sich auf dem Papier die drei von dieser Ecke ausgehenden Kanten jeweils in einem **echt stumpfen Winkel**, also einem Winkel mit negativem geometrischen Cosinus. Zeichnet man also ein räumliches Koordinatensystem perspektivisch korrekt von einem Punkt des positiven Oktanten  $(\mathbb{R}_{>0})^3$  aus gesehen, so

müssen sich je zwei positive Koordinatenachsen in einem echt stumpfen Winkel treffen.

*Ergänzende Übung 4.1.11.20.* Jede orthogonale Selbstabbildung mit Determinante  $(-1)$  eines dreidimensionalen reellen Skalarproduktraums ist die Verknüpfung einer Drehung um eine Achse mit einer Spiegelung an der zu dieser Achse senkrechten Hyperebene.

*Ergänzende Übung 4.1.11.21.* Jede bezüglich Inklusion maximale kommutative Untergruppe der Drehgruppe  $\mathrm{SO}(3)$  ist entweder die Gruppe aller Drehungen um eine Achse oder konjugiert zur Gruppe aller Diagonalmatrizen aus  $\mathrm{SO}(3)$ .

*Übung 4.1.11.22.* Sei  $V$  ein reeller Skalarproduktraum. Man zeige:

1. Eine endliche Familie  $v_1, \dots, v_n$  von Vektoren von  $V$  ist orthonormal genau dann, wenn die zugehörige Abbildung  $\Phi : \mathbb{R}^n \rightarrow V$  orthogonal ist für das Standard-Skalarprodukt auf  $\mathbb{R}^n$ .
2. Gegeben endliche angeordnete Basen  $\mathcal{A}, \mathcal{B}$  von  $V$  mit  $\mathcal{A}$  orthonormal ist  $\mathcal{B}$  orthonormal genau dann, wenn die Basiswechselmatrix  ${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$  orthogonal ist. Hinweis: Man betrachte das kommutative Diagramm

$$\begin{array}{ccc} V & \xleftarrow{\mathrm{id}} & V \\ \Phi_{\mathcal{B}} \uparrow & & \uparrow \Phi_{\mathcal{A}} \\ \mathbb{R}^n & \xleftarrow{{}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}} & \mathbb{R}^n \end{array}$$

Man formuliere und zeige auch die analogen Aussagen im Komplexen.

*Übung 4.1.11.23.* Ein Endomorphismus eines endlichdimensionalen komplexen Skalarproduktraums ist genau dann unitär, wenn er diagonalisierbar ist und wenn zusätzlich alle Eigenwerte den Betrag Eins haben.

*Ergänzende Übung 4.1.11.24.* Bezeichne  $R_{\varphi}^x \in \mathrm{SO}(3)$  die Drehung um die  $x$ -Achse  $\mathbb{R}\mathbf{e}_1$  mit dem Winkel mit Bogenmaß  $\varphi$ , in Formeln

$$R_{\varphi}^x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \varphi & -\sin \varphi \\ 0 & \sin \varphi & \cos \varphi \end{pmatrix}$$

Bezeichne  $R_{\varphi}^z \in \mathrm{SO}(3)$  die Drehung um die  $z$ -Achse  $\mathbb{R}\mathbf{e}_3$  mit dem Winkel mit Bogenmaß  $\varphi$ , in Formeln

$$R_{\varphi}^z = \begin{pmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Man zeige: Jede Drehung  $U \in \mathrm{SO}(3)$  läßt sich darstellen als

$$U = R_\varphi^z R_\psi^x R_\vartheta^z$$

mit  $\psi \in [0, \pi]$  und  $\varphi, \vartheta \in [0, 2\pi)$ , und unter der Voraussetzung  $e_3 \neq \pm U(e_3)$  ist diese Darstellung sogar eindeutig. Die fraglichen Winkel heißen dann die **Euler'schen Winkel** unserer Drehung  $U$ . Hinweis: Aus der Anschauung, deren Formalisierung Ihnen überlassen bleiben möge, finden wir  $\psi \in [0, \pi]$  und  $\varphi \in [0, 2\pi)$  mit  $R_\varphi^z R_\psi^x(e_3) = U(e_3)$ . Es folgt  $U^{-1} R_\varphi^z R_\psi^x = R_{-\vartheta}^z$  für geeignetes  $\vartheta \in [0, 2\pi)$ .

*Ergänzende Übung 4.1.11.25 (Springgruppe und Quaternionen).* Wir erhalten einen Isomorphismus  $\mathrm{SU}(2) \xrightarrow{\sim} \{q \in \mathbb{H} \mid |q| = 1\}$  der Springgruppe mit der Gruppe der Quaternionen der Norm Eins, indem wir bemerken, daß bei unserer Konstruktion der Quaternionen im Beweis von 3.5.6.3 beide Seiten dieselbe Untergruppe von  $\mathrm{Mat}(2; \mathbb{C})$  sind.

*Ergänzende Übung 4.1.11.26 (Springgruppe und Drehgruppe).* Sei  $\mathfrak{su}(2) := \{A \in \mathrm{Mat}(2; \mathbb{C}) \mid A + \bar{A}^\top = 0, \mathrm{tr} A = 0\}$  der dreidimensionale reelle Vektorraum der schieferhermitischen spurlosen  $(2 \times 2)$ -Matrizen. Man zeige: Die Vorschrift  $\langle A, B \rangle := -\mathrm{tr}(AB)$  liefert ein Skalarprodukt auf  $\mathfrak{su}(2)$  und wir erhalten einen surjektiven Gruppenhomomorphismus  $\rho : \mathrm{SU}(2) \twoheadrightarrow \mathrm{SO}(\mathfrak{su}(2))$  mit Kern  $\pm I$  durch die Vorschrift  $\rho(U) : A \mapsto UAU^{-1}$ . Insbesondere gibt es also einen surjektiven Gruppenhomomorphismus

$$\mathrm{SU}(2) \twoheadrightarrow \mathrm{SO}(3)$$

mit Kern  $\pm I$ . Hinweis: Um die Surjektivität zu zeigen, kann man den Satz 4.1.11.24 über die Eulerschen Winkel verwenden und zeigen, daß die von den drei Einbettungen  $\mathbb{C} \hookrightarrow \mathbb{H}$  mit  $i_{\mathbb{C}} \mapsto i, j, k$  nach 4.1.11.25 induzierten Einbettungen  $S^1 \hookrightarrow \mathrm{SU}(2)$  unter Nachschalten von  $\rho$  die Kreislinie surjektiv auf die Gruppen der Drehungen um drei paarweise orthogonale Achsen in  $\mathfrak{su}(2)$  abbilden. Ein konzeptionelles Argument wird in ?? ausgeführt.

*Übung 4.1.11.27.* Man zeige: Für jede komplexe quadratische Matrix  $A$  gibt es eine unitäre Matrix  $U$  derart, daß  $UAU^{-1}$  obere Dreiecksgestalt hat. Hinweis: Trigonalisierbarkeit und Gram-Schmidt.

*Ergänzende Übung 4.1.11.28.* Man zeige, daß die orthogonale Gruppe eines endlichdimensionalen reellen Skalarproduktraums von Spiegelungen an Hyperebenen erzeugt wird. Hinweis: Normalform 4.1.11.3.

*Ergänzende Übung 4.1.11.29 (Iwasawa-Zerlegung für  $\mathrm{SL}(n; \mathbb{C})$ ).* Bezeichne  $A \subset \mathrm{SL}(n; \mathbb{C})$  die Menge aller Diagonalmatrizen mit reellen positiven Einträgen auf der Diagonale und  $N \subset \mathrm{GL}(n; \mathbb{C})$  die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale. So liefert die Multiplikation eine Bijektion

$$\mathrm{SU}(n) \times A \times N \xrightarrow{\sim} \mathrm{SL}(n; \mathbb{C})$$

Hinweis: Man gehe vom Fall 4.1.11.11 der  $\mathrm{GL}(n; \mathbb{C})$  aus.

*Übung 4.1.11.30.* Gegeben eine nicht notwendig quadratische Matrix  $A$  mit Einträgen in einem angeordneten Körper haben  $A$  und  $A^\top A$  denselben Rang.

*Übung 4.1.11.31 (Ausgleichsrechnung).* Gegeben  $A \in \mathrm{Mat}(m \times n; \mathbb{R})$  und  $b \in \mathbb{R}^m$  nimmt die Funktion  $x \mapsto \|Ax - b\|$  genau an denjenigen Stellen  $x \in \mathbb{R}^n$  ihr Minimum an, für die gilt  $A^\top Ax = A^\top b$ . Hinweis: Nach 4.1.11.30 ist letztere Gleichung stets lösbar. Man prüfe nun für beliebige  $x, b, h$  die Identität

$$\|A(x + h) - b\|^2 - \|Ax - b\|^2 = \|Ah\|^2 + 2h^\top(A^\top Ax - A^\top b)$$

In typischen Anwendungen ist  $Ax = b$  ein überbestimmtes und deshalb unlösbares Gleichungssystem, etwa mit einer Proportionalitätskonstanten  $x$  als einziger Variablen, die man aus einer durch Meßfehler gestörten Meßreihe bestimmen will. Hat  $A$  den Rang  $n$ , so ist unser Minimum  $x$  sogar eindeutig bestimmt, wie man obiger Identität auch leicht ansieht. Etwas allgemeiner könnten wir für Meßwerte  $(a_1, b_1), \dots, (a_m, b_m)$  Koeffizienten  $x_1, x_2$  so suchen, daß  $a \mapsto x_1 + x_2 a$  unsere Meßreihe  $a_i \mapsto b_i$  möglichst gut beschreibt. Hier ist zu beachten, daß wir statt  $x \mapsto ax + b$  wie üblich die Buchstaben ganz anders verwenden.

### 4.1.12 Selbstdjungierte Endomorphismen

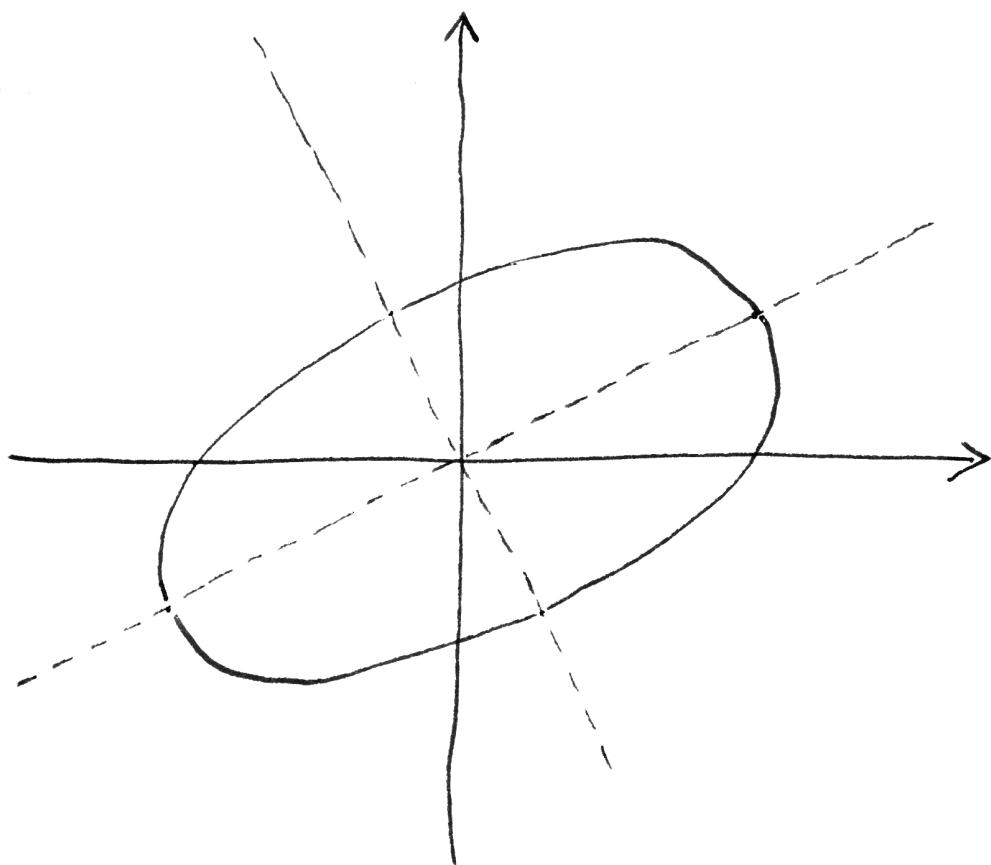
**Satz 4.1.12.1 (Hauptachsentransformation).** *Gegeben eine homogene quadratische Form auf dem  $\mathbb{R}^n$  alias eine Funktion  $q : \mathbb{R}^n \rightarrow \mathbb{R}$  der Gestalt  $q(x_1, \dots, x_n) = \sum_{i \leq j} c_{ij} x_i x_j$  gibt es stets eine Drehung  $U \in \mathrm{SO}(n)$  und Skalare  $\lambda_1, \dots, \lambda_n \in \mathbb{R}$  mit*

$$(q \circ U)(y_1, \dots, y_n)^\top = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2$$

*Des weiteren ist die Multimenge  $\{\lambda_1, \dots, \lambda_n\}$  durch  $q$  bereits eindeutig bestimmt.*

4.1.12.2. Dieser Satz wird sich als ein einfaches Korollar des Spektralsatzes erweisen und soll der Motivation dienen. Wir gegen den Beweis im Anschluß an 4.1.12.20. In 4.2.2.7 diskutieren wir Hauptachsentransformationen noch ausführlicher.

4.1.12.3 (Anschauung für Hauptachsentransformationen). Man kann sich die Bedeutung dieses Satzes auf zwei Weisen veranschaulichen: Entweder „aktiv“ in dem Sinne, daß der Graph unserer Funktion  $q$  unter der Drehung  $U^{-1}$  oder präziser der Abbildung  $U^{-1} \times \mathrm{id}$  in den Graphen unserer Linearkombination von Quadranten übergeht; Oder „passiv“ in dem Sinne, daß unsere Funktion beim Einführen neuer Koordinaten mit Koordinatenachsen in Richtung der Spaltenvektoren von  $U$  in den neuen Koordinaten ausgedrückt die fragliche Form annimmt, in Formeln  $q(y_1 \vec{v}_1 + \dots + y_n \vec{v}_n) = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2$  für  $\vec{v}_i$  die Spalten von  $U$ , also für



Dieses Bild zeigt die Ellipse, auf der die positiv definite quadratische Form  $17x^2 - 12xy + 8y^2$  bei einer geeigneten Wahl des Maßstabs den Wert Eins annimmt. Gestrichelt sind die Hauptachsen eingetragen, die in diesem Fall die Richtungsvektoren  $(2, 1)$  und  $(-1, 2)$  haben.

$U = (\vec{v}_1 | \dots | \vec{v}_n)$  und folglich  $U(y_1, \dots, y_n)^\top = y_1 \vec{v}_1 + \dots + y_n \vec{v}_n$ . Die Menge der von den Spalten der Matrix  $U$  erzeugten Geraden heißen dann ein System von **Hauptachsen** für unsere quadratische Form  $q$ . Die Multimenge der  $\lambda_i$  nennen wir die Multimenge der **Eigenwerte** unserer quadratischen Form.

**Beispiel 4.1.12.4 (Transformation einer Hyperbel auf ihre Hauptachsen).** Die Identität  $xy = (1/4)((x+y)^2 - (x-y)^2)$  zeigt, daß im Fall der quadratischen Form  $q(x, y) = xy$  die Hauptachsen gerade die Diagonale die Nebendiagonale sind, also die Ursprungsgeraden mit den Gleichungen  $x = \pm y$ . Mögliche Drehungen  $U$ , die unsere Form auf ihre Hauptachsen transformieren, sind also die Drehungen um die Winkel  $45^\circ + n \cdot 90^\circ$  mit  $n = 0, 1, 2, 3$ . Eine Matrix für eine derartige Drehung ist

$$U = \begin{pmatrix} \sqrt{2}^{-1} & -\sqrt{2}^{-1} \\ \sqrt{2}^{-1} & \sqrt{2}^{-1} \end{pmatrix}$$

Schreiben wir genauer  $x = x_1$  und  $y = x_2$ , so nimmt unsere Form die Gestalt  $q(x_1, x_2) = x_1 x_2$  an und für den Koordinatenwechsel  $(x_1, x_2)^\top = U(y_1, y_2)^\top$  alias  $x_1 = 2^{-1/2}y_1 - 2^{-1/2}y_2$  und  $x_2 = 2^{-1/2}y_1 + 2^{-1/2}y_2$  oder gleichbedeutend  $U^{-1}(x_1, x_2)^\top = (y_1, y_2)^\top$  alias  $y_1 = 2^{-1/2}x_1 + 2^{-1/2}x_2$  und  $y_2 = 2^{-1/2}x_1 - 2^{-1/2}x_2$  ergibt sich

$$q(x_1, x_2) = x_1 x_2 = \frac{1}{2}y_1^2 - \frac{1}{2}y_2^2$$

**Definition 4.1.12.5.** Gegeben Skalarprodukträume  $V, W$  heißen lineare Abbildungen  $f : V \rightarrow W$  und  $g : W \rightarrow V$  zueinander **adjungiert**, wenn gilt

$$\langle f(v), w \rangle = \langle v, g(w) \rangle \quad \forall v \in V, w \in W$$

4.1.12.6. Ich kann für das Konzept adjungierter Abbildungen leider keinerlei Anschauung anbieten. Die adjungierte Abbildung darf nicht mit der adjungierten oder besser adjunkten Matrix aus 3.6.4.6 verwechselt werden, mit der sie außer der Bezeichnung rein gar nichts zu tun hat.

4.1.12.7 (**Eindeutigkeit von Adjungierten**). Jede lineare Abbildung  $f$  zwischen Skalarprodukträumen hat höchstens eine Adjungierte: Sind nämlich  $g, h$  beide adjungiert zu  $f$ , so folgt  $\langle v, g(w) - h(w) \rangle = 0 \quad \forall v, w$  und insbesondere für  $v = g(w) - h(w)$  und damit  $g(w) = h(w) \quad \forall w$ .

4.1.12.8 (**Adjungierte in Koordinaten**). Versehen wir  $\mathbb{R}^n, \mathbb{R}^m$  jeweils mit dem Standardskalarprodukt, so wird für  $A \in \text{Mat}(m \times n; \mathbb{R})$  die adjungierte Abbildung zu  $A : \mathbb{R}^n \rightarrow \mathbb{R}^m$  gegeben durch die transponierte Matrix als  $A^\top : \mathbb{R}^m \rightarrow \mathbb{R}^n$ . Ebenso wird im Komplexen die adjungierte Abbildung zu  $A : \mathbb{C}^n \rightarrow \mathbb{C}^m$  gegeben durch  $\bar{A}^\top : \mathbb{C}^m \rightarrow \mathbb{C}^n$ . In der Tat finden wir mühelos

$$\langle Ax, y \rangle = (\bar{Ax})^\top y = \bar{x}^\top \bar{A}^\top y = \langle x, \bar{A}^\top y \rangle \quad \forall x \in \mathbb{C}^m, y \in \mathbb{C}^n$$

4.1.12.9 (**Existenz von Adjungierten im endlichdimensionalen Fall**). Wir folgern aus der Klassifikation endlichdimensionaler Skalarprodukträume 4.1.4.8 mit Hilfe der vorhergehenden Bemerkung, daß jede lineare Abbildung von endlichdimensionalen reellen oder komplexen Skalarprodukträumen genau eine Adjungierte besitzt.

4.1.12.10 (**Eine Abbildung ohne Adjungierte im Unendlichdimensionalen**). Wir betrachten den freien  $\mathbb{R}$ -Vektorraum  $V = W$  über  $\mathbb{N}$  mit der Basis  $(e_n)_{n \in \mathbb{N}}$  und dem Skalarprodukt, für das diese Basis ein Orthonormalsystem ist. Die lineare Abbildung  $f : V \rightarrow V$  mit  $e_n \mapsto (e_1 + \dots + e_n)$  besitzt keine Adjungierte, denn diese müßte  $e_1$  auf einen Vektor  $v \in V$  werfen mit  $\langle v, e_n \rangle = 1$  für alle  $n$  und solch einen Vektor gibt es nicht.

**Definition 4.1.12.11.** Ein Endomorphismus eines reellen oder komplexen Skalarproduktraums heißt **selbstadjungiert**, wenn er zu sich selbst adjungiert ist.

4.1.12.12 (**Anschaufung für selbstadjungierte Endomorphismen**). Die „schiefadjungierten“ alias zu ihrem Negativen adjungierten Endomorphismen eines endlichdimensionalen Skalarproduktraums  $V$  mag man sich als die Richtungsvektoren des „Tangentialraums im neutralen Element an die Gruppe der unitären Automorphismen“ vorstellen. Ist in der Tat  $\gamma : \mathbb{R} \rightarrow \mathrm{GL}(V)$  eine differenzierbare Abbildung mit  $\gamma(0) = \mathrm{id}$  und  $\langle \gamma(t)v, \gamma(t)w \rangle = \langle v, w \rangle$  für alle  $v, w \in V$  und alle Zeiten  $t$ , so folgt

$$\langle \gamma'(0)v, w \rangle + \langle v, \gamma'(0)w \rangle = 0$$

für alle  $v, w \in V$  alias  $\gamma'(0)$  schiefadjungiert. Ist umgekehrt  $A$  schiefadjungiert, gilt also für die darstellende Matrix  $A$  bezüglich einer Orthonormalbasis  $A + \bar{A}^\top = 0$ , so ist  $\gamma : t \mapsto \exp(tA)$  ein Weg mit

$$\gamma(t)\overline{\gamma(t)^\top} = \exp(tA)\overline{\exp(tA)^\top} = \exp(tA + t\bar{A}^\top) = \exp(0) = \mathrm{I}$$

für alle  $t$ , der mithin ganz in der unitären Gruppe verläuft. Das gibt hoffentlich eine gewisse Vorstellung für schiefadjungierte Endomorphismen und macht anschaulich klar, daß sie mit einem vorgegebenen Teilraum auch dessen orthogonales Komplement stabilisieren. Selbstadjungierte Endomorphismen sind dann die i-fachen der schiefadjungierten Endomorphismen, und mehr als die so vererbte Anschaufung kann ich für diese Bedingung auch nicht anbieten. Geometrisch aber liefert der Spektralsatz oder besser sein Korollar 4.1.12.38 eine sehr explizite Beschreibung: Die selbstadjungierten Endomorphismen eines endlichdimensionalen Skalarproduktraums sind genau diejenigen Endomorphismen, die in einer geeigneten Orthogonalbasis durch eine Diagonalmatrix mit reellen Einträgen dargestellt werden.

**4.1.12.13 (Symmetrisch beziehungsweise hermitesch heißt selbstadjungiert).** Eine reelle  $(n \times n)$ -Matrix  $A$  beschreibt eine selbstadjungierte Abbildung  $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$  in Bezug auf das Standardskalarprodukt genau dann, wenn sie symmetrisch ist, in Formeln  $A = A^\top$ . Das folgt sofort aus 4.1.12.7. Eine komplexe  $(n \times n)$ -Matrix  $A$  beschreibt ähnlich eine selbstadjungierte Abbildung  $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$  in Bezug auf das Standardskalarprodukt genau dann, wenn sie die Identität  $A = \bar{A}^\top$  erfüllt. Solche Matrizen heißen auch **hermitesch**.

**Lemma 4.1.12.14 (Selbstadjungierte Abbildungen in Orthonormalbasen).** Sei  $V$  ein endlichdimensionaler Skalarproduktraum und  $f : V \rightarrow V$  eine lineare Abbildung. So sind gleichbedeutend:

1. Die Abbildung  $f$  ist selbstadjungiert;
2. Es gibt eine angeordnete Orthonormalbasis  $\mathcal{B} = (v_1, \dots, v_n)$  von  $V$  derart, daß die Matrix  ${}_{\mathcal{B}}[f]_{\mathcal{B}}$  hermitesch ist;
3. Für jede angeordnete Orthonormalbasis  $\mathcal{B} = (v_1, \dots, v_n)$  von  $V$  ist die Matrix  ${}_{\mathcal{B}}[f]_{\mathcal{B}}$  hermitesch.

*Beweis.* (1)  $\Rightarrow$  (3): Die Einträge  $a_{ji}$  unserer Matrix sind definiert durch die Vorschrift  $f(v_i) = \sum_j a_{ji} v_j$ . Im Fall einer Orthonormalbasis folgt  $a_{ji} = \langle v_j, f(v_i) \rangle$ . Ist dann  $f$  selbstadjungiert, so folgt

$$a_{ji} = \langle v_j, f(v_i) \rangle = \langle f(v_j), v_i \rangle = \overline{\langle v_i, f(v_j) \rangle} = \overline{a_{ij}}$$

(3)  $\Rightarrow$  (2) bietet keine Schwierigkeiten. Um (2)  $\Rightarrow$  (1) zu zeigen bemerken wir, daß die Identität  $\langle f(v), w \rangle = \langle v, f(w) \rangle$  für alle  $v, w$  folgt, sobald wir sie für alle  $v, w$  aus einer festen Basis  $\mathcal{B}$ , ja aus einem beliebigen Erzeugendensystem zeigen können. Das aber folgt dann aus der Hermitizität der Matrix von  $f$  mit der Rechnung, die wir bereits durchgeführt haben.  $\square$

**Satz 4.1.12.15 (Spektralsatz für selbstadjungierte Endomorphismen).** Für jeden selbstadjungierten Endomorphismus eines reellen oder komplexen endlichdimensionalen Skalarproduktraums besitzt unser Vektorraum eine Orthonormalbasis aus Eigenvektoren, und auch im komplexen Fall sind alle Eigenwerte eines selbstadjungierten Endomorphismus reell.

**4.1.12.16.** Einen noch allgemeineren Spektralsatz für „normale“ Endomorphismen dürfen Sie später als Übung 4.3.2.19 selbst beweisen. Er enthält sowohl den Spektralsatz für selbstadjungierte Endomorphismen als auch den Spektralsatz für unitäre Endomorphismen als Spezialfälle.

*Erster Beweis.* Sei  $V$  unser Skalarproduktraum und  $f : V \rightarrow V$  selbstadjungiert. Gegeben  $0 \neq v \in V$  und  $\lambda \in \mathbb{C}$  mit  $f(v) = \lambda v$  folgern wir von der Mitte ausgehend die Gleichungskette

$$\bar{\lambda} \langle v, v \rangle = \langle \lambda v, v \rangle = \langle f(v), v \rangle = \langle v, f(v) \rangle = \langle v, \lambda v \rangle = \lambda \langle v, v \rangle$$

und daraus folgt bereits  $\lambda \in \mathbb{R}$ . Weiter ist das orthogonale Komplement  $v^\perp$  eines Eigenvektors  $v$  stabil unter  $f$ , denn aus  $\langle v, w \rangle = 0$  folgt  $\langle v, f(w) \rangle = \langle f(v), w \rangle = \bar{\lambda} \langle v, w \rangle = 0$ . Bis hierher brauchen wir noch nicht einmal  $V$  als endlichdimensional vorzusetzen. Nun können wir den Beweis im Komplexen mit Induktion beenden: Im Fall  $V = 0$  ist der Satz klar. Sonst finden wir einen Eigenvektor  $v_1$  von  $f$ , den wir ohne Beschränkung der Allgemeinheit normiert annehmen dürfen. Dann wenden wir auf die auf seinem orthogonalen Komplement induzierte Abbildung  $f : v_1^\perp \rightarrow v_1^\perp$  die Induktionsvoraussetzung an und finden darin eine Orthonormalbasis  $v_2, \dots, v_n$  aus Eigenvektoren von  $f$ . Damit ist  $v_1, \dots, v_n$  die gesuchte Orthonormalbasis von  $V$  aus Eigenvektoren von  $f$  und der komplexe Fall ist erledigt. Im reellen Fall überlegen wir uns zunächst, daß die darstellende Matrix von  $f$  in Bezug auf eine Orthonormalbasis von  $V$  symmetrisch sein muß. Diese Matrix hat im Fall  $\dim_{\mathbb{R}} V > 0$ , wenn sie also nicht die  $(0 \times 0)$ -Matrix ist, mindestens einen komplexen Eigenwert, und da sie auch einen selbstadjungierten Endomorphismus eines komplexen Vektorraums darstellt, muß dieser Eigenwert nach unseren Überlegungen zu Beginn des Beweises sogar reell sein. Zu diesem Eigenwert finden wir dann wieder einen Eigenvektor aus  $V$ , und der Beweis läuft von da an wie im komplexen Fall.  $\square$

*Zweiter Beweis im Reellen.* Man betrachte auf  $V \setminus 0$  die zu  $f$  gehörige quadratische Form  $q(v) := \langle f(v), v \rangle$  und die zum Skalarprodukt gehörige quadratische Form  $n(v) := \langle v, v \rangle = \|v\|^2$  und deren Quotienten

$$v \mapsto R(v) := \frac{q(v)}{n(v)}$$

Sie heißt der **Raleigh-Quotient**, deshalb der Buchstabe  $R$ . Schränken wir diese Funktion ein auf die Einheitssphäre  $\{v \mid \|v\| = 1\}$ , so nimmt sie dort nach Heine-Borel ?? und ?? ihr Maximum an, etwa an einer Stelle  $v_+$ . Da unsere Funktion konstant ist auf jeder Geraden durch den Nullpunkt, muß sie an derselben Stelle auch als Funktion  $V \setminus 0 \rightarrow \mathbb{R}$  ihr Maximum annehmen. Wir betrachten nun für  $w \in V$  die für hinreichend kleines  $t \in \mathbb{R}$  wohldefinierte Funktion  $t \mapsto R(v_+ + tw)$ , ausgeschrieben

$$R(v_+ + tw) = \frac{q(v_+ + tw)}{n(v_+ + tw)} = \frac{\langle f(v_+ + tw), v_+ + tw \rangle}{\langle v_+ + tw, v_+ + tw \rangle}$$

Sie ist offensichtlich differenzierbar, folglich muß ihre Ableitung bei  $t = 0$  verschwinden. Dann verschwindet also, wenn wir diese Ableitung mithilfe der Quotientenregel berechnen, auch der Zähler, und wir folgern

$$(\langle f(w), v_+ \rangle + \langle f(v_+), w \rangle) \langle v_+, v_+ \rangle - 2 \langle f(v_+), v_+ \rangle \langle v_+, w \rangle = 0$$

für alle  $w \in V$ . Mithilfe der Selbstadjungiertheit von  $f$  folgern wir insbesondere

$$w \perp v_+ \Rightarrow w \perp f(v_+)$$

Das liefert offensichtlich  $f(v_+) \in \mathbb{R}v_+$  und wir haben einen Eigenvektor gefunden. Der Rest des Arguments läuft von da an wie beim ersten Beweis.  $\square$

**4.1.12.17 (Vergleich beider Beweise).** Der zweite Beweis vermeidet zwar den Fundamentalsatz der Algebra, benutzt jedoch einen wesentlichen Teil derjenigen Resultate aus der reellen Analysis, aus denen wir in ?? auch den Fundamentalsatz der Algebra herleiten. Anschaulich scheint mir die im zweiten Beweis versteckte Erkenntnis recht klar: Durch den Punkt der Ellipse  $\{v \mid \langle f(v), v \rangle = 1\}$ , der am nächsten am Ursprung liegt, geht in der Tat eine Hauptachse. Dasselbe gilt natürlich für den Punkt, der dem Ursprung am fernsten liegt, als da heißt, der kleinstmögliche Wert des Raleigh-Quotienten ist auch ein Eigenwert und jede Stelle, an der er angenommen wird, ist ein Eigenvektor unseres selbstadjungierten Operators zu diesem Eigenwert.

**Korollar 4.1.12.18 (Spektralsatz für hermitesche Matrizen).** Für jede hermitesche Matrix  $A \in \text{Mat}(n; \mathbb{C})$  gibt es eine unitäre Matrix mit Determinante Eins  $U \in \text{SU}(n)$  derart, daß  $\bar{U}^\top AU = U^{-1}AU$  diagonal ist mit reellen Einträgen.

**4.1.12.19.** Die Gleichung  $U^\top AU = U^{-1}AU$  folgt aus unserer Identität  $\bar{U}^\top = U^{-1}$ , die ja für jede unitäre Matrix  $U$  gilt.

*Beweis.* Nach dem Spektralsatz für selbstadjungierte Abbildungen 4.1.12.15 finden wir eine Orthonormalbasis  $(v_1, \dots, v_n)$  von  $\mathbb{C}^n$  aus Eigenvektoren von  $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$  zu reellen Eigenwerten. Die Matrix  $U := (v_1 | \dots | v_n)$  ist also unitär mit  $AU = U \text{diag}(\lambda_1, \dots, \lambda_n)$  für  $\lambda_i \in \mathbb{R}$ . Indem wir notfalls noch eine Spalte einer komplexen Zahl vom Betrag Eins multiplizieren, können wir sogar um  $\det U = 1$  erreichen.  $\square$

**Korollar 4.1.12.20 (Spektralsatz für reelle symmetrische Matrizen).** Gegeben eine symmetrische Matrix  $A \in \text{Mat}(n; \mathbb{R})$  gibt es stets eine orthogonale Matrix mit Determinante Eins  $U \in \text{SO}(n)$  derart, daß  $U^\top AU = U^{-1}AU$  diagonal ist.

*Beweis.* Wie im komplexen Fall in 4.1.12.18.  $\square$

*Beweis des Satzes über Hauptachsentransformationen 4.1.12.1.* Für unsere quadratische Form  $q(x_1, \dots, x_n) = \sum_{i \leq j} c_{ij}x_i x_j$  finden wir eine symmetrische Matrix  $A \in \text{Mat}(n; \mathbb{R})$  mit

$$q(x) = x^\top A x$$

für den Spaltenvektor  $x = (x_1, \dots, x_n)^\top$ , indem wir als diagonale Matrixeinträge  $a_{ii} = c_{ii}$  nehmen und außerhalb der Diagonalen  $a_{ij} = a_{ji} = c_{ij}/2$  setzen. Nach dem Spektralsatz für symmetrische Matrizen 4.1.12.20 gibt es dann eine Drehung  $U \in \text{SO}(n)$  mit  $U^{-1}AU = U^\top AU = \text{diag}(\lambda_1, \dots, \lambda_n)$  für geeignete  $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ , nämlich für die Eigenwerte von  $A$  mit ihren Vielfachheiten. Es folgt

$$q(Uy) = y^\top U^\top AU y = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2$$

In 4.2.2.7 gebe ich noch einen zweiten Beweis, der ohne Koordinaten auskommt und mir dadurch transparenter scheint.  $\square$

**Definition 4.1.12.21.** Eine hermitesche Matrix  $P \in \text{Mat}(n; \mathbb{C})$  heißt **positiv definit**, wenn gilt  $x \neq 0 \Rightarrow \bar{x}^\top Px > 0$ . Sie heißt **positiv semidefinit**, wenn gilt  $\bar{x}^\top Px \geq 0 \forall x \in \mathbb{C}^n$ .

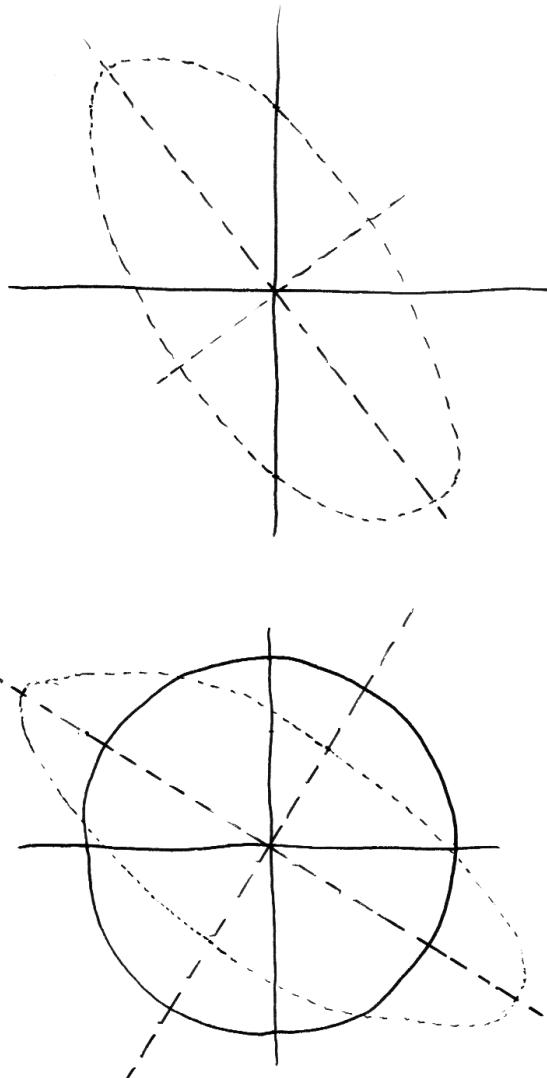
*Beispiel 4.1.12.22.* Gegeben eine beliebige Matrix  $A \in \text{Mat}(n; \mathbb{C})$  ist  $\bar{A}^\top A$  stets positiv semidefinit, denn es gilt  $\bar{x}^\top \bar{A}^\top Ax = \overline{\bar{A}x}^\top Ax \geq 0 \forall x \in \mathbb{C}^n$ . Gegeben eine invertierbare Matrix  $A \in \text{GL}(n; \mathbb{C})$  zeigt dasselbe Argument, daß  $\bar{A}^\top A$  positiv definit ist.

**Satz 4.1.12.23 (Polarzerlegung von Automorphismen).** Sei  $n \in \mathbb{N}$ .

1. *Jede Matrix  $A \in \text{GL}(n; \mathbb{R})$  besitzt eine eindeutige Darstellung als Produkt  $A = UP$  mit  $U \in \text{O}(n)$  orthogonal und  $P$  symmetrisch positiv definit;*
2. *Jede Matrix  $A \in \text{GL}(n; \mathbb{C})$  besitzt eine eindeutige Darstellung als Produkt  $A = UP$  mit  $U \in \text{U}(n)$  unitär und  $P$  hermitesch positiv definit.*

4.1.12.24. Offensichtlich bilden die Determinanten der Polarzerlegung einer invertierbaren Matrix die Polarzerlegung ihrer Determinante. So erhalten wir Polarzerlegungen in  $\text{SL}(n; \mathbb{R})$  und  $\text{SL}(n; \mathbb{C})$ . In dieser und noch größerer Allgemeinheit heißt sie oft **Cartan-Zerlegung**. Ich will jedoch lieber auch ganz allgemein von der Polarzerlegung reden, da diese Terminologie so viel Anschauung transportiert.

*Beispiele 4.1.12.25.* Im Fall  $\text{GL}(1; \mathbb{R})$  ist das die Zerlegung  $a = (a/|a|) \cdot |a|$  einer von Null verschiedenen reellen Zahl als das Produkt von einem Vorzeichen mit einer positiven reellen Zahl. Im Fall  $\text{GL}(1; \mathbb{C})$  ist es die Zerlegung  $a = (a/|a|) \cdot |a|$  einer von Null verschiedenen komplexen Zahl als das Produkt von einer komplexen Zahl auf dem Einheitskreis mit einer positiven reellen Zahl. Dieser Fall hat



Die Polarzerlegung der Scherung  $(x, y) \mapsto (x, y - x)$  stellt diese Abbildung dar als Verknüpfung einer Streckung beziehungsweise Stauchung längs orthogonaler Achsen mit einer Drehung. Im unteren Bild sieht man durchgezogen den Einheitskreis, und gestrichelt sein Bild unter dem selbstadjungiertem Faktor der Verscherung nebst den Hauptachsen, längs derer der Einheitskreis dabei gestreckt beziehungsweise gestaucht wird. Im oberen Bild sieht man dann den verscherten Einheitskreis alias die mit dem orthogonalen Faktor der Verscherung verdrehte Ellipse aus dem unteren Bild. Auch noch gestrichelt eingezeichnet sind die Hauptachsen dieser Ellipse.

wohl auch unserer Zerlegung ihren Namen gegeben. Im Fall  $\mathrm{GL}(3; \mathbb{R})$  beschreibt  $A$  eine Abbildung  $A : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ . Nimmt man die Abbildung  $A$  als orientierungs-erhaltend an, so mag man sich ihre Polarzerlegung dahingehend denken, daß sich unsere Abbildung in eindeutiger Weise darstellen läßt als Verknüpfung einer Abbildung, die entlang geeigneter paarweise orthogonaler Koordinatenachsen dehnt oder staucht, mit einer Abbildung, die dreht. Wenden wir etwa  $A$  auf den mit Schaumgummi oder was auch immer gefüllt gedachten Raum an, so ist allein der positiv definite Faktor  $P$  für die Materialspannungen verantwortlich: Eine Kugel unseres Materials wird bei Anwenden von  $A$ , „erst mit  $P$  zu einem Ellipsoid verzerrt und dann noch mit  $U$  gedreht“.

*Beweis.* Wir zeigen das im reellen Fall, im Komplexen muß man nur von jeder transponierten Matrix zusätzlich noch die komplexe Konjugierte nehmen. Wir beginnen mit dem Nachweis der Eindeutigkeit. Gegeben eine Zerlegung  $A = UP$  wie oben haben wir sicher  $A^\top A = P^\top U^\top UP = P^\top P = P^2$ . Jede Orthonormalbasis aus Eigenvektoren von  $P$  ist also auch eine Orthonormalbasis aus Eigenvektoren von  $A^\top A$  und  $P$  muß die Matrix sein, die auf Eigenvektoren von  $A^\top A$  zum Eigenwert  $\lambda$  jeweils operiert durch den Skalar  $\sqrt{\lambda}$ . Das zeigt die Eindeutigkeit unserer Zerlegung. Andererseits folgt aus  $A^\top Av = \lambda v$  sofort  $v^\top A^\top Av = \lambda \|v\|^2 = \|Av\|^2$  und somit  $\lambda > 0$ . Wir können also  $P$  symmetrisch und positiv definit finden mit  $P^2 = A^\top A$ . Für  $U = AP^{-1}$  folgt dann  $U^\top U = P^{-1}A^\top AP^{-1} = I$  und folglich ist  $U$  orthogonal.  $\square$

4.1.12.26. Jetzt diskutieren wir dasselbe noch einmal koordinatenfrei und in etwas größerer Allgemeinheit.

**Definition 4.1.12.27.** Ein selbstadjungierter Endomorphismus  $P$  eines Skalarproduktraums  $V$  mit Skalarprodukt  $\langle \cdot, \cdot \rangle$  heißt **positiv definit**, wenn gilt  $x \neq 0 \Rightarrow \langle x, Px \rangle > 0$ . Er heißt **positiv semidefinit**, wenn gilt  $\langle x, Px \rangle \geq 0 \forall x \in V$ .

4.1.12.28. Im endlichdimensionalen Fall ist das gleichbedeutend dazu, daß alle Eigenwerte positiv beziehungsweise nichtnegativ sind. Die Begriffsbildung ist aber auch im Fall unendlichdimensionaler Räume relevant.

**Definition 4.1.12.29.** Unter einer **partiellen Isometrie** von Skalarprodukträumen versteht man eine lineare Abbildung, deren Restriktion auf den Orthogonalraum ihres Kerns isometrisch ist.

**Satz\* 4.1.12.30 (Polar-Zerlegung von Endomorphismen).** *Jeder Endomorphismus  $A$  eines endlichdimensionalen Skalarproduktraums  $V$  besitzt eine eindeutige Darstellung als Produkt  $A = UP$  mit  $P$  selbstadjungiert positiv semidefinit und  $U$  einer partiellen Isometrie derart, daß gilt  $(\ker U)^\perp = \mathrm{im} P$ .*

4.1.12.31. Dieser Satz gilt sowohl für komplexe als auch für reelle Vektorräume. Er verallgemeinert unseren Satz 4.1.12.23 über die Polarzerlegung von Automorphismen. Natürlich gibt es für diesen Satz auch eine Fassung für Matrizen und für den vorhergehenden Satz 4.1.12.23 auch eine Fassung für Automorphismen abstrakter endlichdimensionaler Skalarprodukträume. In ?? zeigen wir sogar eine Fassung im unendlichdimensionalen Fall, genauer für sogenannte „beschränkte Operatoren auf Hilberträumen“. Eine Verallgemeinerung in eine wieder andere Richtung ist die sogenannte „Singulärwertzerlegung“ 4.2.3.29, für die ich jedoch kein so schönes Eindeutigkeitskriterium kenne.

*Beweis.* Wir beginnen mit der Eindeutigkeit. Gegeben eine derartige Zerlegung  $A = UP$  können wir sicher auch eine orthogonale Abbildung  $M$  finden mit  $A = MP$ . Es folgt  $\bar{A}^T A = P^2$  und folglich ist  $P$  eindeutig bestimmt als die einzige positiv semidefinite selbstadjugierte Abbildung  $P$  mit  $P^2 = \bar{A}^T A$ . Dann ist auch  $U$  eindeutig festgelegt auf dem Bild (im  $P$ ), und unsere letzte Bedingung impliziert  $U = 0$  auf  $(\text{im } P)^\perp$  und legt damit auch  $U$  eindeutig fest. Um die Existenz zu zeigen, gehen wir diese Argumentation rückwärts durch. Das Argument des vorhergehenden Beweises zeigt, daß es ein selbstadjungiertes positiv semidefinites  $P$  gibt mit  $P^2 = \bar{A}^T A$ . Wegen  $\langle Av, Av \rangle = \langle v, \bar{A}^T Av \rangle = \langle v, P^2 v \rangle = \langle Pv, Pv \rangle$  gilt  $\ker A = \ker P$ . Das ist aber auch das orthogonale Komplement des Bildes  $U := \text{im } P$ . Bezeichnet also  $Q : V \rightarrow U$  die orthogonale Projektion auf  $U$  und  $J : U \hookrightarrow V$  die Einbettung, so haben wir mit  $A = AJQ$ . Nun induziert  $P$  einen Isomorphismus  $P_U : U \xrightarrow{\sim} U$  und wir können die Komposition  $C = AJP_U^{-1} : U \rightarrow V$  betrachten. Dann gilt einerseits  $CQP = CP_U Q = AJQ = A$  und andererseits ist  $C$  isometrisch. Dann ist  $U = CQ$  eine partielle Isometrie mit den gewünschten Eigenschaften.  $\square$

*Ergänzung 4.1.12.32 (Existenz von Adjungierten, koordinatenfrei).* Lineare Abbildungen  $f, g$  zwischen komplexen Skalarprodukträumen sind in anderen Formeln ausgedrückt genau dann zueinander adjungiert, wenn das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\text{can}_V} & V^\top \\ f \downarrow & & \downarrow g^\top \\ W & \xrightarrow{\text{can}_W} & W^\top \end{array}$$

kommutiert, mit  $g^\top : V^\top \rightarrow W^\top$  der „transponierten“ alias „dualen“ Abbildung zu  $g : W \rightarrow V$  und  $\text{can}_V : V \rightarrow V^\top$  der Abbildung  $v \mapsto \langle v, \cdot \rangle$  und  $\text{can}_W$  analog definiert. Diese „kanonischen“ Abbildungen  $\text{can}$  landen zwar wie behauptet im Dualraum, da unsere Skalarprodukte linear sind im zweiten Eintrag, sie sind jedoch selbst nur im reellen Fall linear und im komplexen Fall vielmehr schief-linear im Sinne von 4.1.3.6. Man überzeugt sich dennoch leicht, daß diese kanonischen Abbildungen im endlichdimensionalen Fall Bijektionen sein müssen,

und da die Verknüpfung einer linearen und einer schiefflinearen Abbildung schiefflinear ist und die Verknüpfung von zwei schiefflinearen Abbildung linear, liefert das einen alternativen Beweis für die Existenz und Eindeutigkeit der adjungierten Abbildung im endlichdimensionalen Fall. Noch bequemer wird die Argumentation, wenn man wie im nächsten Abschnitt den komplex konjugierten Vektorraum einführt.

*Ergänzung 4.1.12.33.* Zu jedem komplexen Vektorraum  $V$  bilden wir den **komplex konjugierten Vektorraum**  $\bar{V}$ , indem wir die additive Gruppe von  $V$  nehmen, die Operation von  $a \in \mathbb{C}$  auf  $v \in V$  jedoch abändern zu einer Operation  $a \cdot v$ , die mit der ursprünglichen Operation  $av$  verknüpft ist durch die Formel  $a \cdot v = \bar{a}v$  alias  $\bar{a} \cdot v = av$ . Es ist in diesem Zusammenhang praktisch, für jedes Element  $v \in V$  dasselbe Element in seiner Eigenschaft als Element des komplex konjugierten Vektorraums  $\bar{v} \in \bar{V}$  zu notieren, so daß wir unseren Punkt für die neue Operation der Skalare gleich wieder weglassen können und unsere zweite Formel besonders suggestiv in der Form

$$\bar{a}\bar{v} = \overline{av}$$

geschrieben werden kann. Für jede  $\mathbb{C}$ -lineare Abbildung  $f : V \rightarrow W$  von komplexen Vektorräumen ist dieselbe Abbildung auch eine  $\mathbb{C}$ -lineare Abbildung  $\bar{f} : \bar{V} \rightarrow \bar{W}$  der komplex konjugierten Räume. Wir bezeichnen diese Abbildung dennoch mit einem neuen Symbol  $\bar{f} : \bar{V} \rightarrow \bar{W}$  und nennen sie die **konjugierte Abbildung**. Sind  $\mathcal{A}$  und  $\mathcal{B}$  angeordnete Basen von  $V$  und  $W$ , so hat die konjugierte Abbildung die konjugierte Matrix, in Formeln

$$\bar{\mathcal{B}}[\bar{f}]_{\bar{\mathcal{A}}} = \overline{\mathcal{B}[f]_{\mathcal{A}}}$$

Hier kriegen die Basen wie die einzelnen Vektoren einen Querstrich, um daran zu erinnern, daß sie im konjuguierten Vektorraum zu verstehen sind. Eine koordinatenfreie Konstruktion der adjungierten Abbildung erhält man nun wie folgt: Jedes Skalarprodukt  $\langle \cdot, \cdot \rangle$  auf  $V$  liefert eine injektive  $\mathbb{C}$ -lineare Abbildung

$$\begin{aligned} \text{can} : \bar{V} &\hookrightarrow V^\top \\ \bar{v} &\mapsto \langle v, \cdot \rangle \end{aligned}$$

des konjuguierten Raums zu  $V$  in den Dualraum von  $V$ . Lineare Abbildungen  $f, g$  zwischen komplexen Skalarprodukträumen sind in diesem Formalismus adjungiert genau dann, wenn das Diagramm

$$\begin{array}{ccc} \bar{V} & \xrightarrow{\text{can}} & V^\top \\ \bar{f} \downarrow & & \downarrow g^\top \\ \bar{W} & \xrightarrow{\text{can}} & W^\top \end{array}$$

kommutiert, mit  $g^\top : V^\top \rightarrow W^\top$  der „transponierten“ alias „dualen“ Abbildung zu  $g : W \rightarrow V$ . Im endlichdimensionalen Fall sind unsere kanonischen Abbildungen can in den Horizontalen jedoch nach Dimensionsvergleich Isomorphismen. In diesem Fall liefert also das obige kommutative Diagramm auch einen alternativen Beweis für die Existenz und Eindeutigkeit adjungierter Abbildungen.

### Übungen

*Übung 4.1.12.34 (Inhomogene reelle quadratische Formen).* Gegeben eine Polynomfunktion vom Grad höchstens Zwei mit reellen Koeffizienten alias eine Abbildung  $q : \mathbb{R}^n \rightarrow \mathbb{R}$  der Gestalt

$$q(x_1, \dots, x_n) = \sum_{i \leq j} c_{ij}x_i x_j + \sum_i b_i x_i + a$$

gibt es eine Isometrie  $B : \mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$  mit

$$(q \circ B)(y_1, \dots, y_n) = \lambda_1 y_1^2 + \dots + \lambda_k y_k^2 + \mu y_n + \nu$$

für geeignetes  $k$  und geeignete reelle  $\lambda_i \neq 0$  und  $\mu \geq 0$  und ( $k = n \Rightarrow \mu = 0$ ) und ( $\mu > 0 \Rightarrow \nu = 0$ ). Unter den gegebenen Annahmen sind zusätzlich die Multi- menge der  $\lambda_i$  sowie  $\mu$  und  $\nu$  eindeutig bestimmt. Man sagt dann, die **quadratische Form  $q$  gehe unter unserer Bewegung  $B$  in ihre Standardform über**. Im Fall  $n \neq 1$  können wir zusätzlich erreichen, daß  $B$  orientationserhaltend ist. Hinweis: Man mag unser  $\mu$  beschreiben als das Minimum der Norm des Gradienten und, wenn dieses Minimum Null ist, unser  $\nu$  als den Wert an einer kritischen Stelle.

*Übung 4.1.12.35.* Man finde eine Bewegung, die die Quadrik  $xy + 3x$  in ihre Standardform 4.1.12.34 überführt.

*Übung 4.1.12.36.* Man zeige, daß sich die Nullstellenmenge einer inhomogenen reellen quadratischen Form  $ax^2 + by^2 + cxy + dx + ey + f$  in zwei Variablen stets als Urbild des Doppelkegels  $\{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 = z^2\}$  unter einer Isometrie  $\mathbb{R}^2 \hookrightarrow \mathbb{R}^3$  schreiben lässt, es sei denn, die Nullstellenmenge unserer quadratischen Form ist leer oder besteht aus zwei parallelen Geraden.

*Übung 4.1.12.37.* Bei einem unitären Isomorphismus zwischen Skalarprodukträumen ist die adjugierte Abbildung die inverse Abbildung.

*Ergänzende Übung 4.1.12.38.* Man zeige: Ein Endomorphismus eines endlichdimensionalen Skalarproduktraums ist genau dann selbstadjungiert, wenn es dazu eine Orthonormalbasis aus Eigenvektoren gibt und alle Eigenwerte reell sind.

*Übung 4.1.12.39.* Gegeben eine symmetrische positiv definite reelle  $(n \times n)$ -Matrix  $A$  hat die Funktion  $y \mapsto \langle y, Ay \rangle / 2 - \langle b, y \rangle$  ihr einziges globales Minimum bei der Lösung der Gleichung  $Ax = b$ .

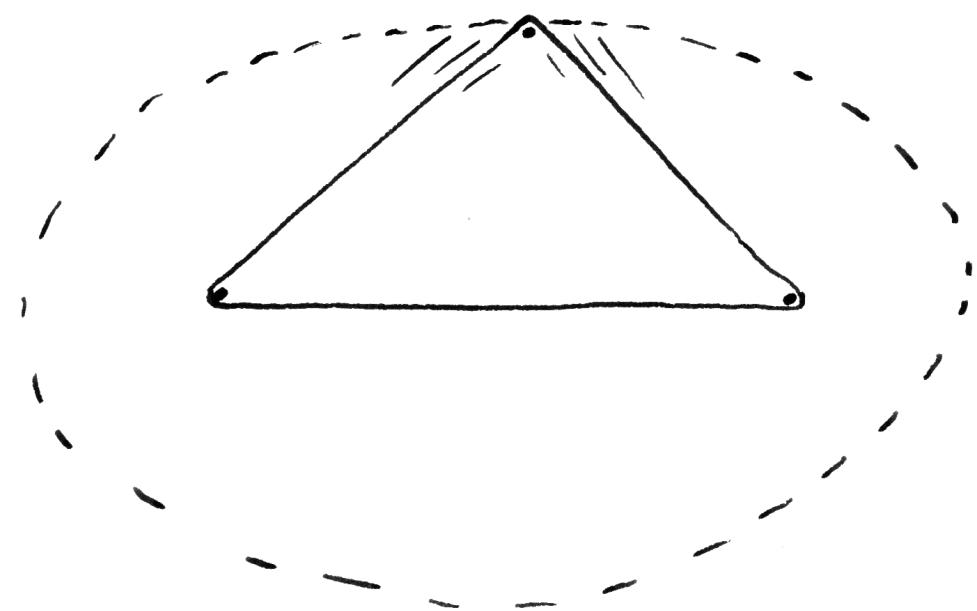
**4.1.12.40 (Elliptische Beete).** Gärtner erstellen elliptische Beete wie folgt: Sie schlagen zwei Pfosten ein, legen eine Seilschlinge darum, und fahren mit einem dritten Pfosten soweit außen, wie die Seilschlinge es erlaubt, um die beiden fest eingeschlagenen Pfosten herum. Eine einfache Rechnung zeigt, daß man so die Lösungsmenge einer quadratischen Gleichung und, da unsere Lösungsmenge beschränkt ist und nicht nur aus einem Punkt besteht, notwendig eine Ellipse erhält: Wenn man definieren müßte, welche Teilmengen einer affinen reellen Ebene denn nun Ellipsen heißen sollen, würde man nämlich genau diese Eigenschaft zur Definition erheben, und 4.1.12.34 zeigt, daß das auch unserer Anschauung entspricht, nach der eine Ellipse eine „zusammengedrückte Kreislinie“ sein sollte. Die beiden Pfosten heißen die **Brennpunkte** unserer Ellipse. Das hat hinwiederum mit dem Grenzfall der Parabel zu tun, zu dem wir gelangen, indem wir einen Pfosten vom anderen Pfosten weg auf geradem Wege ins Unendliche schieben und gleichzeitig das Seil so verlängern, daß immer gleich viel Spiel bleibt. Wäre die Ellipse ein Spiegel, so sollte anschaulich klar sein, daß sich das von einer Laterne auf einem der Pfosten ausgesandte Licht beim anderen Pfosten wieder sammeln muß. Im Grenzfall der Parabel wird sich folglich parallel aus der Richtung des unendlich fernen Pfostens einfallendes Licht beim anderen Pfosten sammeln und ihn, wenn auf dem unendlich fernen Pfosten statt einer Laterne die Sonne steht, möglicherweise sogar entzünden: Deshalb heißt er der Brennpunkt der Parabel, und von diesem Beispiel überträgt man das Wort auf Ellipsen und von dort weiter auf Hyperbeln, bei denen statt der Summe die Differenz der Abstände zu den beiden „Brennpunkten“ konstant ist.

*Übung 4.1.12.41 (Polar-Zerlegung von Endomorphismen, Variante).* Sei  $V$  ein endlichdimensionaler Skalarproduktraum. Man zeige, daß jeder Endomorphismus  $A \in \text{End } V$  auch eine eindeutige Darstellung als Produkt  $A = P'U'$  besitzt mit  $P'$  selbstadjungiert positiv semidefinit und  $U'$  einer partiellen Isometrie derart, daß gilt  $\text{im } U' = (\ker P')^\perp$ .

*Übung 4.1.12.42.* Man gebe eine von Null verschiedene komplexe symmetrische nilpotente  $(2 \times 2)$ -Matrix an. Gibt es auch eine von Null verschiedene reelle symmetrische nilpotente  $(2 \times 2)$ -Matrix?

*Ergänzende Übung 4.1.12.43.* Bezeichne  $S \subset \text{Mat}(n; \mathbb{R})$  den Untervektorraum der symmetrischen Matrizen. Gegeben eine symmetrische Matrix  $P \in S$  betrachte man die lineare Abbildung  $f_P : S \rightarrow S$  gegeben durch die Vorschrift  $f_P : A \mapsto PAP$ . Man zeige für die Determinante von  $f_P$  im Sinne von 3.6.4.3 die Formel  $\det(f_P) = (\det P)^{n+1}$ . Hinweis: Man ziehe sich auf den Fall zurück, daß  $P$  diagonal ist.

*Übung 4.1.12.44.* Man zeige, daß vier paarweise verschiedene Elemente der Zahlenkugel  $\mathbb{C} \sqcup \{\infty\}$  genau dann ein reelles Doppelverhältnis haben, wenn sie auf einem gemeinsamen verallgemeinerten Kreis liegen.



Konstruktion elliptischer Beete

*Übung 4.1.12.45 (Reelle Formen und schiefflineare Involutionen).* Unter einer **reellen Form eines komplexen Vektorraums**  $V$  versteht man einen reellen Untervektorraum  $V_{\mathbb{R}} \subset V$  derart, daß  $V_{\mathbb{R}}$  ganz  $V$  als  $\mathbb{C}$ -Vektorraum erzeugt und daß jede über  $\mathbb{R}$  linear unabhängige Teilmenge unseres Untervektorraums  $V_{\mathbb{R}}$  auch über  $\mathbb{C}$  linear unabhängig ist in  $V$ . Unter einer **schiefflinearen Involution** eines komplexen Vektorraums  $V$  versteht man eine schiefflineare Abbildung  $\bar{\theta} : V \rightarrow V$  mit  $\bar{\theta}^2 = \text{id}_V$ . Man zeige: Gegeben ein komplexer Vektorraum  $V$  liefert die Vorschrift, die jeder schiefflinearen Involution von  $V$  ihre Fixpunktmenge zuordnet, eine Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{schiefflineare Involutionen} \\ \bar{\theta} : V \rightarrow V \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{l} \text{reelle Formen} \\ V_{\mathbb{R}} \subset V \end{array} \right\} \\ \bar{\theta} & \mapsto & V^{\bar{\theta}} \end{array}$$

## 4.2 Allgemeine Bilinearformen

### 4.2.1 Fundamentalmatrix

**Definition 4.2.1.1.** Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  erinnern wir daran, daß wir in 4.1.3 bilineare Abbildungen  $b : V \times V \rightarrow K$  in den Grundkörper auch **Bilinearformen auf  $V$**  genannt hatten. Die Menge aller Bilinearformen auf einem  $K$ -Vektorraum  $V$  notieren wir

$$\text{Bil}_K(V) = \text{Bil}(V)$$

Sie bilden einen Untervektorraum im Vektorraum  $\text{Ens}(V \times V, K)$  aller Abbildungen von  $V \times V$  nach  $K$ . In der alternativen in 3.2.3.8 eingeführten Notation hätten wir  $\text{Bil}_K(V) = \text{Hom}^{(2)}(V \times V, K)$ .

**Satz 4.2.1.2 (Fundamentalmatrix einer Bilinearform auf  $K^n$ ).** *Gegeben ein Körper  $K$  und eine natürliche Zahl  $n \in \mathbb{N}$  erhalten wir eine Bijektion*

$$\begin{aligned} F : \quad \text{Bil}(K^n) &\xrightarrow{\sim} \text{Mat}(n; K) \\ b &\mapsto [b] \end{aligned}$$

*dadurch, daß wir jeder Bilinearform  $b$  ihre **Fundamentalmatrix**  $F(b) := [b]$  zuordnen, deren Einträge die Werte unserer Bilinearform auf Paaren von Vektoren der Standardbasis sind, in Formeln  $[b]_{ij} := b(e_i, e_j)$ . Die Umkehrabbildung kann beschrieben werden durch die Abbildungsvorschrift  $F \mapsto b_F$  mit  $b_F(v, w) = v^\top F w$ .*

*Beweis.* Die erste Aussage folgt unmittelbar aus Übung 3.2.3.9, nach der eine bilineare Abbildung festgelegt und festlegbar ist durch ihre Werte auf Paaren von Basisvektoren. Um unsere Beschreibung der Umkehrabbildung zu prüfen, reicht es aus, für jede Matrix  $F$  die Identität  $[b_F] = F$  alias  $b_F(e_i, e_j) = F_{ij} \forall i, j$  zu zeigen. Das hinwiederum folgt unmittelbar aus  $b_F(e_i, e_j) = F_{ij} = e_i^\top F e_j$ .  $\square$

**Satz 4.2.1.3 (Fundamentalmatrix einer Bilinearform im Abstrakten).** *Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem Körper  $K$  erhalten wir für jede angeordnete Basis  $\mathcal{A} = (v_1, \dots, v_n)$  von  $V$  eine Bijektion*

$$\begin{aligned} F_{\mathcal{A}} : \quad \text{Bil}(V) &\xrightarrow{\sim} \text{Mat}(n; K) \\ b &\mapsto [b] = [b]_{\mathcal{A}, \mathcal{A}} \end{aligned}$$

*dadurch, daß wir jeder Bilinearform  $b$  ihre **Fundamentalmatrix**  $F_{\mathcal{A}}(b) := [b]$  bezüglich unserer Basis  $\mathcal{A}$  zuordnen vermittels der Vorschrift  $[b]_{ij} = b(v_i, v_j)$ . Die Umkehrabbildung kann in diesem Fall beschrieben werden durch die Abbildungsvorschrift  $F \mapsto b_F$  mit*

$$b_F(v, w) = {}_{\mathcal{A}}[v]^\top \circ F \circ {}_{\mathcal{A}}[w]$$

*Beweis.* Die erste Aussage folgt wieder unmittelbar aus der Erkenntnis 3.2.3.9, daß eine bilineare Abbildung festgelegt und festlegbar ist durch ihre Werte auf Paaren von Basisvektoren. Für die zweite Aussage zeigen wir nun zur Abwechslung einmal  $b_{F(b)} = b$  alias  $b_{F(b)}(v, w) = b(v, w)$  für alle  $v, w$ . Dazu müssen wir ja nur zeigen  $b_{F(b)}(v_i, v_j) = b(v_i, v_j)$  für alle  $i, j$  alias

$${}_{\mathcal{A}}[v_i]^{\top} \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[v_j] = (F_{\mathcal{A}}(b))_{ij}$$

Das ist jedoch klar wegen  ${}_{\mathcal{A}}[v_i] = e_i$ . □

**4.2.1.4 (Notationsfragen).** Die Notation  $[b]_{\mathcal{A}, \mathcal{A}}$  für die darstellende Matrix hat den Vorteil, daß sie sich als Spezialisierung eines noch allgemeineren Falls versteht. Wir können etwa für Vektorräume  $U, V$  mit angeordneten Basen  $\mathcal{A} = (u_1, \dots, u_n)$  und  $\mathcal{B} = (v_1, \dots, v_m)$  eine bilineare Abbildung  $b : U \times V \rightarrow K$  beschreiben durch eine  $(n \times m)$ -Matrix  $[b] = [b]_{\mathcal{A}, \mathcal{B}}$  mit Einträgen  $[b]_{ij} = b(u_i, v_j)$ . Ist noch allgemeiner  $b : U \times V \rightarrow W$  eine bilineare Abbildung in einen weiteren Vektorraum und sind  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  Basen unserer Räume, so erhalten wir eine Abbildung

$$c[b]_{\mathcal{A}, \mathcal{B}} = [b] : \mathcal{A} \times \mathcal{B} \times \mathcal{C} \rightarrow K$$

durch die Vorschrift, daß  $[b](u_i, v_j, w_k)$  der Koeffizient von  $w_k$  bei einer Darstellung des Vektors  $b(u_i, v_k) \in W$  in der Basis  $\mathcal{C} = \{w_1, \dots, w_l\}$  von  $W$  sein möge. Da sich solch ein „Zahlenwürfel“ alias „räumliche Matrix“ eh schlecht hinschreiben läßt, hilft die Wahl einer Anordnung der Basen auch nicht mehr weiter und ich bin zu einer Darstellung übergegangen, die die Wahl derartiger Anordnungen nicht benötigt. Wie es noch allgemeiner geht, besprechen wir in 4.2.1.10.

**4.2.1.5.** Wenn man viel zu rechnen hat, mag es praktisch sein, Matrizen von Bilinearformen als  $[b]_{ij}$  zu indizieren und Matrizen von linearen Abbildungen zur Unterscheidung anders als zuvor  ${}^k[f]_j$  und Skalare systematisch von rechts an Vektoren zu schreiben, also  $f(\vec{v}_j) = \sum_i \vec{w}_k {}^k[f]_j$  für  $f : V \rightarrow W$  und entsprechende Basen sowie  $b(\vec{v}_i, \vec{v}_j) = [b]_{ij}$  und für allgemeinere bilineare Abbildungen  $b : U \times V \rightarrow W$  entsprechend

$$b(\vec{u}_i, \vec{v}_j) = \sum_k \vec{w}_k {}^k[b]_{ij}$$

Für eine lineare Abbildung  $f : W \rightarrow X$  ergäbe sich dann etwa die angenehm übersichtliche Formel  ${}^l[f \circ b]_{ij} = \sum_k {}^l[f]_k {}^k[b]_{ij}$ . Die Darstellung eines Vektors  $v \in V$  wäre  $v = \sum \vec{v}_j {}^j[v]$  und die lineare Abbildung  $b(\cdot, v)$  mit  $u \mapsto b(u, v)$  hätte die Matrix  ${}^k[b(\cdot, v)]_i = \sum_j {}^k[b]_{ij} {}^j[v]$ . Die Darstellung einer Linearform  $\lambda : U \rightarrow K$  schließlich wäre der Zeilenvektor mit Einträgen  $[\lambda]_i = \lambda(\vec{u}_i)$  und das Auswerten auf  $u = \sum \vec{u}_j {}^j[u]$  wäre  $\lambda(u) = \sum [\lambda]_i {}^i[u]$ .

**4.2.1.6 (Fundamentalmatrizen symmetrischer Bilinearformen).** Eine Bilinearform ist symmetrisch genau dann, wenn ihre Fundamentalmatrix bezüglich einer gegebenen Basis symmetrisch ist. Ist also in Formeln  $V$  ein  $K$ -Vektorraum und  $\mathcal{B}$  eine angeordnete Basis von  $V$  und  $b : V \times V \rightarrow K$  eine Bilinearform, so gilt

$$b \text{ symmetrisch} \Leftrightarrow F_{\mathcal{B}}(b) \text{ symmetrisch}$$

In der Tat, ist  $(v_1, \dots, v_n)$  unsere angeordnete Basis, so gilt für symmetrisches  $b$  ja  $b(v_i, v_j) = b(v_j, v_i)$  und damit die Identität  $F_{ij} = F_{ji}$  für die Einträge  $F_{ij} = b(v_i, v_j)$  der Fundamentalmatrix  $F = F_{\mathcal{B}}(b)$ . Bezeichnet ganz allgemein  $\tau : V \times V \xrightarrow{\sim} V \times V$  das Vertauschen  $\tau : (v, w) \mapsto (w, v)$ , so haben wir für jede Bilinearform  $b$  offensichtlich die Identität  $F_{\mathcal{B}}(b \circ \tau) = F_{\mathcal{B}}(b)^T$ . Ist also die Fundamentalmatrix symmetrisch, in Formeln  $F_{\mathcal{B}}(b)^T = F_{\mathcal{B}}(b)$ , so folgt mit 4.2.1.3 sofort  $b \circ \tau = b$  alias  $b$  symmetrisch.

**4.2.1.7 (Fundamentalmatrizen alternierender Bilinearformen).** Eine Bilinearform ist alternierend genau dann, wenn ihre Fundamentalmatrix bezüglich einer gegebenen Basis antisymmetrisch ist und auf der Diagonale verschwindet. Wir nennen derartige quadratische Matrizen auch **alternierend**.

**Proposition 4.2.1.8 (Fundamentalmatrix und Basiswechsel).** Gegeben ein Körper  $K$  und ein endlichdimensionaler  $K$ -Vektorraum  $V$  mit zwei angeordneten Basen  $\mathcal{A}, \mathcal{B}$  gilt zwischen den Fundamentalmatrizen einer Bilinearform  $b \in \text{Bil}(V)$  in Bezug auf unsere beiden Basen die Beziehung

$${}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}^T \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}} = F_{\mathcal{B}}(b)$$

**4.2.1.9.** Man berechnet also in Worten gesagt die Fundamentalmatrix einer Bilinearform bezüglich einer Basis aus ihrer Fundamentalmatrix bezüglich einer anderen Basis, indem man von rechts die Basiswechselmatrix dranmultipliziert und von links ihre Transponierte.

*Beweis.* Gegeben  $v, w \in V$  gilt

$$\begin{aligned} b(v, w) &= {}_{\mathcal{B}}[v]^T \circ F_{\mathcal{B}}(b) \circ {}_{\mathcal{B}}[w] \\ b(v, w) &= {}_{\mathcal{A}}[v]^T \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[w] \\ &= ({}_{\mathcal{A}}[\text{id}]_{\mathcal{B}} \circ {}_{\mathcal{B}}[v])^T \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}} \circ {}_{\mathcal{B}}[w] \\ &= {}_{\mathcal{B}}[v]^T \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}^T \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}} \circ {}_{\mathcal{B}}[w] \end{aligned}$$

Gilt für Matrizen  $F, G \in \text{Mat}(n \times m; K)$  jedoch  $v^T F w = v^T G w$  für alle Spaltenvektoren  $v \in K^n, w \in K^m$ , so folgt durch Einsetzen der Vektoren der Standardbasis  $F = G$ . Damit liefern unsere Gleichungen die gewünschte Identität  ${}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}^T \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}} = F_{\mathcal{B}}(b)$ .  $\square$

*Ergänzung 4.2.1.10.* Seien  $K$  ein Körper oder allgemeiner ein Kring und  $r \geq 0$  eine natürliche Zahl und  $M_1, \dots, M_r, N$  Mengen. Wir setzen

$$\text{Mat}_K(M_1 \curlyvee \dots \curlyvee M_r, N) := \left\{ \begin{array}{l} \text{Abbildungen} \\ T : M_1 \times \dots \times M_r \times N \rightarrow K \\ \text{derart, daß es für beliebige } m_1, \dots, m_r \\ \text{höchstens endlich viele } n \text{ gibt mit} \\ \text{mit } T(m_1, \dots, m_r, n) \neq 0 \end{array} \right\}$$

und nennen derartige Abbildungen **Multimatrizen**. Gegeben  $K$ -Vektorräume  $V_1, \dots, V_r, W$  mit Basen  $\mathcal{A}_1, \dots, \mathcal{A}_r, \mathcal{B}$  erhalten wir dann eine Bijektion

$$\text{Hom}_K(V_1 \curlyvee \dots \curlyvee V_r, W) \xrightarrow{\sim} \text{Mat}_K(\mathcal{A}_1 \curlyvee \dots \curlyvee \mathcal{A}_r, \mathcal{B})$$

durch die Vorschrift  $f \mapsto [f]$  mit der Multimatrix  $[f] = {}_{\mathcal{B}}[f]_{\mathcal{A}_1, \dots, \mathcal{A}_r}$  gegeben durch

$$f(v_1, v_2, \dots, v_r) = \sum_{w \in \mathcal{B}} [f](v_1, v_2, \dots, v_r, w) w$$

für beliebige Tupel  $(v_1, v_2, \dots, v_r) \in \mathcal{A}_1 \times \dots \times \mathcal{A}_r$  von Basisvektoren. All unsere bisherigen Matrixbildungen ordnen sich dieser allgemeinen Konvention unter. In der üblichen Weise hinschreiben lassen sich unsere Multimatrizen aber nur in wenigen Spezialfällen:

1. Im Fall einer linearen Abbildung zwischen endlichdimensionalen Räumen und nach Wahl einer Anordnung auf beiden Basen, das sind dann unsere Matrizen  ${}_{\mathcal{B}}[f]_{\mathcal{A}}$  linearer Abbildungen. Im Spezialfall einer Abbildung in den Grundkörper mit seiner Standardbasis  $\mathcal{S}(1)$  erhalten wir unsere Darstellung  ${}_{\mathcal{S}(1)}[f]_{\mathcal{A}} = [f]_{\mathcal{A}}$  einer Linearform als Zeilenmatrix;
2. Im Fall einer bilinearen Abbildung in den Grundkörper  $b : V_1 \times V_2 \rightarrow K$  von endlichdimensionalen Räumen und nach Wahl einer Anordnung auf beiden Basen, das sind dann Matrizen  ${}_{\mathcal{S}(1)}[b]_{\mathcal{A}_1, \mathcal{A}_2}$  mit der Konvention für die Zeilen und Spalten, daß sie als  $[b]_{i,j} := [b](v_i, w_j, 1)$  dargestellt werden sollen. Im Spezialfall  $V_1 = V_2 = V$  und  $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$  erhalten wir dann unsere Fundamentalmatrix  $F_{\mathcal{A}}(b) = {}_{\mathcal{S}(1)}[b]_{\mathcal{A}, \mathcal{A}} = [b]_{\mathcal{A}, \mathcal{A}}$ ;
3. Im Fall einer 0-linearen Abbildung in einen endlichdimensionalen Vektorraum  $V$  mit angeordneter Basis  $\mathcal{B}$  erhalten wir unsere Darstellung  ${}_{\mathcal{B}}[v]$  eines Vektors  $v \in V$  als Spaltenmatrix.

## 4.2.2 Hauptachsentransformation

**Definition 4.2.2.1.** Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  versteht man unter einer **homogenen quadratischen Form auf  $V$**  oder kurz **quadratischen**

**Form** eine Abbildung  $q : V \rightarrow K$  derart, daß es eine Bilinearform  $b$  auf  $V$  gibt mit  $q(v) = b(v, v)$ .

4.2.2.2. Gegeben ein Körper  $K$  heißt eine quadratische Form auf dem  $K^n$  auch eine **quadratische Form über  $K$  in  $n$  Variablen**. Eine quadratische Form über  $\mathbb{Q}$  in drei Variablen wäre etwa  $x^2 + 6xy + zx - 13z^2$ .

*Ergänzung 4.2.2.3 (Quadratische Formen und kritische Stellen).* In der Analysis, etwa in ??, können Sie lernen, wie man eine hinreichend differenzierbare Funktion  $\mathbb{R}^n \rightarrow \mathbb{R}$  etwa um den Ursprung bis zu zweiter Ordnung approximieren kann durch eine polynomiale Funktion vom Totalgrad höchstens Zwei alias die Summe einer Konstanten mit einer Linearform und einer quadratischen Form. Ist die fragliche Linearform Null alias hat der Graph unserer Funktion am Ursprung eine horizontale Tangentialebene alias hat unsere Funktion am Ursprung eine „kritische Stelle“, so wird sie dort bis zur Ordnung Zwei approximiert durch die fragliche quadratische Form plus die Konstante. So führt uns das Studium von Funktionen mehrerer Veränderlichen in der Umgebung ihrer kritischen Stellen ganz natürlich auf das Studium quadratischer Formen.

4.2.2.4 (**Quadratische Formen und symmetrische Bilinearformen**). Ist die Charakteristik des Grundkörpers  $K$  ungleich Zwei, so liefert für jeden  $K$ -Vektorraum  $V$  die Vorschrift „werte auf zweimal demselben Vektor aus“ eine Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{symmetrische Bilinearformen} \\ \text{auf dem Vektorraum } V \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{quadratische} \\ \text{Formen auf } V \end{array} \right\} \\ a & \mapsto & (v \mapsto a(v, v)) \end{array}$$

In der Tat liefern dann die Bilinearform  $b$  und die symmetrische Bilinearform  $a$  mit  $a(v, w) := (b(v, w) + b(w, v))/2$  dieselbe quadratische Form, mithin ist unsere Abbildung surjektiv. Weiter wird die symmetrische Bilinearform  $a$  durch  $q$  eindeutig bestimmt mittels der Relation  $2a(v, w) = q(v + w) - q(v) - q(w)$ , mithin ist unsere Abbildung auch injektiv. Wir nennen über einem Körper einer Charakteristik ungleich Zwei eine quadratische Form **nichtausgeartet**, wenn die zugehörige symmetrische Bilinearform nichtausgeartet ist.

4.2.2.5 (**Bilinearformen und lineare Abbildungen**). Übung 3.2.3.16 liefert uns für jeden Vektorraum  $V$  einen kanonischen Isomorphismus

$$\begin{array}{ccc} \text{Bil}(V) & \xrightarrow{\sim} & \text{Hom}(V, V^\top) \\ a & \mapsto & \hat{a} \end{array}$$

zwischen dem Raum der Bilinearformen auf  $V$  und dem Raum der linearen Abbildungen von  $V$  in seinen Dualraum  $V^\top$ , gegeben durch die Abbildungsvorschrift  $a \mapsto \hat{a}$  mit  $\hat{a} : w \mapsto a(\ , w)$  alias  $(\hat{a}(w))(v) = a(v, w)$ .

4.2.2.6 (**Bilinearformen und selbstadjungierte Endomorphismen**). Gegeben ein endlichdimensionaler reeller Skalarproduktraum  $E$  erhalten wir eine natürliche Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{selbstadjungierte} \\ \text{Endomorphismen von } E \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{l} \text{symmetrische} \\ \text{Bilinearformen auf } E \end{array} \right\} \\ f & \mapsto & (a : (v, w) \mapsto \langle f(v), w \rangle) \end{array}$$

Bezeichnet in der Tat  $s$  unser Skalarprodukt, so ist unser  $\hat{s}$  aus 4.2.2.5 offensichtlich eine Injektion und damit ein Isomorphismus  $\hat{s} : E \xrightarrow{\sim} E^\top$ . Gegeben eine weitere Bilinearform  $a$  können wir den Endomorphismus  $f := \hat{s}^{-1} \circ \hat{a}$  von  $E$  bilden und erhalten so eine Bijektion  $\text{Bil}(E) \xrightarrow{\sim} \text{End } E$ . Formal wird  $f$  charakterisiert durch die Formel  $\langle f(v), w \rangle = a(v, w)$  für alle  $w$ . Insbesondere ist der Endomorphismus  $f$  genau dann selbstadjungiert, wenn die Bilinearform  $a$  symmetrisch ist.

**Satz 4.2.2.7 (Hauptachsentransformation abstrakt).** *Gegeben eine quadratische Form  $q : E \rightarrow \mathbb{R}$  auf einem endlichdimensionalen reellen Skalarproduktraum  $E$  gibt es stets eine Orthonormalbasis  $\vec{v}_1, \dots, \vec{v}_n$  von  $E$  und Skalare  $\lambda_1, \dots, \lambda_n \in \mathbb{R}$  mit*

$$q(y_1 \vec{v}_1 + \dots + y_n \vec{v}_n) = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2 \quad \forall y_1, \dots, y_n \in \mathbb{R}$$

4.2.2.8. Den Spezialfall  $E = \mathbb{R}^n$  mit dem Standardskalarprodukt hatten wir bereits in 4.1.12.1 diskutiert. Die von den  $\vec{v}_i$  erzeugten Geraden nennen wir wieder ein System von **Hauptachsen** für unsere?? quadratische Form  $q$ . Beim Beweis wird sich wieder herausstellen, daß die Multimenge der  $\lambda_i$  durch unsere quadratische Form eindeutig bestimmt ist. Wir nennen sie die Multimenge der **Eigenwerte** unserer quadratischen Form. Weiter wird sich herausstellen, daß die von den Hauptachsen zu einem festen Eigenwert erzeugten Teilräume eindeutig bestimmt sind. Wir nennen sie die **Eigenräume** unserer quadratischen Form. Sowohl die Hauptachsen als auch die Eigenwerte hängen hierbei von dem auf dem zugrundeliegenden Vektorraum gewählten Skalarprodukt ab.

**Vorschau 4.2.2.9 (Hauptachsentransformation für euklidische Vektorräume).** Gegeben eine quadratische Form  $q$  auf einem endlichdimensionalen euklidischen Vektorraum  $V$  gibt es stets eine Zerlegung in paarweise orthogonale Teiräume  $V = V_1 \oplus \dots \oplus V_r$  und „inverse Flächen“  $\lambda_1, \dots, \lambda_r \in \mathbb{L}^{-2}$  mit

$$q(v_1 + \dots + v_r) = \lambda_1 \|v_1\|^2 + \dots + \lambda_r \|v_r\|^2$$

für beliebige  $v_i \in V_i$ . Gilt außerdem  $\lambda_1 > \dots > \lambda_r$  und  $V_i \neq 0 \ \forall i$ , so werden die  $V_i$  und die  $\lambda_i$  durch unsere quadratische Form  $q$  bereits eindeutig festgelegt

und wir nennen wieder die  $V_i$  die **Eigenräume** und die  $\lambda_i$  die **Eigenwerte** unserer quadratischen Form auf unserem euklidischen Vektorraum und die Dimensionen der  $V_i$  die **Vielfachheiten** der jeweiligen Eigenwerte. Diese Umformulierung von 4.2.2.7 wird Ihnen leicht fallen, sobald Sie sich mit dem entsprechenden Formalismus vertraut gemacht haben, wie er etwa in 4.6.1.16 erklärt wird.

*Erster Beweis.* Ohne Beschränkung der Allgemeinheit dürfen wir annehmen,  $E$  sei der  $\mathbb{R}^n$  mit seinem Standardskalarprodukt. In diesem Fall hatten wir den Satz bereits als 4.1.12.1 bewiesen. Allerdings war der dort gegebene Beweis in meinen Augen zu sehr von Koordinaten abhängig, um transparent zu sein. Ich gebe deshalb hier noch einen zweiten Beweis, der mir natürlicher scheint.  $\square$

*Zweiter Beweis.* In diesem Beweis notieren wir Vektoren wieder ohne Pfeil. Nach 4.2.2.4 finden wir zu unserer quadratischen Form  $q$  eine symmetrische Bilinearform  $a$  mit  $q(v) = a(v, v) \forall v \in E$ , und nach 4.2.2.6 finden wir zu  $a$  weiter einen selbstadjungierten Endomorphismus  $f$  von  $E$  mit  $a(v, w) = \langle f(v), w \rangle \forall v, w \in E$ . Der Spektralsatz 4.1.12.15 liefert uns dann eine Orthonormalbasis  $v_1, \dots, v_n$  von  $E$  aus Eigenvektoren von  $f$ , so daß also gilt  $f(v_i) = \lambda_i v_i$  für geeignete  $\lambda_i \in \mathbb{R}$ . Unser Satz folgt unmittelbar.  $\square$

### 4.2.3 Klassifikation symmetrischer Bilinearformen

4.2.3.1. Unter einer **Klassifikation** einer gewissen Art von mathematischen Strukturen versteht man im allgemeinen die Angabe einer Liste von „Standardstrukturen“ derart, daß jede Struktur der vorgegebenen Art zu genau einer der Strukturen besagter Liste „isomorph“ ist. Oft sind derartige Listen sehr schwer anzugeben, und man ist schon froh, wenn man eine Liste von „Standardstrukturen“ angeben kann derart, daß jede Struktur der vorgegebenen Art zu mindestens einer der Strukturen besagter Liste „isomorph“ ist. Meist wird in der Darstellung das jeweilige Konzept von Isomorphie nicht explizit gemacht und muß vom Leser erraten werden. In der Sprache der Kategorientheorie ?? können wir das viel genauer sagen: Eine Klassifikation der Objekte einer Kategorie bedeutet die Angabe eines Repräsentantensystems für die Isomorphieklassen von Objekten unserer Kategorie.

*Beispiel 4.2.3.2 (Klassifikation endlich erzeugter Vektorräume).* Für die Struktur eines endlich erzeugten Vektorraums über einem vorgegebenen Körper  $K$  bilden die Vektorräume  $K^n$  für  $n \in \mathbb{N}$  eine solche Liste, denn jeder endlich erzeugte  $K$ -Vektorraum ist isomorph zu genau einem  $K^n$ . Man sagt deshalb auch, die endlich erzeugten Vektorräume seien „klassifiziert durch ihre Dimension“. Ähnlich und noch einfacher werden die endlichen Mengen klassifiziert durch ihre Kardi-

nalität. Ähnlich aber schwieriger werden die endlich erzeugten reellen oder komplexen Skalarprodukträume klassifiziert durch ihre Dimension.

*Beispiel 4.2.3.3 (Klassifikation endlicher Gruppen).* Die Klassifikation endlicher Gruppen haben wir in 2.2.3.9 begonnen: Bis auf Isomorphie gibt es nur je eine Gruppe  $G$  der Kardinalitäten  $|G| = 1, 2, 3$ . Dahingegen gibt es bis auf Isomorphie genau zwei Gruppen der Kardinalität Vier.

*Beispiel 4.2.3.4 (Klassifikation linearer Abbildungen).* Lineare Abbildungen zwischen endlich erzeugten Vektorräumen werden „klassifiziert durch die Dimensionen der beteiligten Vektorräume und den Rang der Abbildung“. Nennen wir genauer lineare Abbildungen  $f : V \rightarrow W$  und  $f' : V' \rightarrow W'$  „isomorph“, wenn es Vektorraumisomorphismen  $\phi : V \xrightarrow{\sim} V'$  und  $\psi : W \xrightarrow{\sim} W'$  gibt mit  $\psi f = f' \phi$ , so daß also das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow \phi & & \downarrow \psi \\ V' & \xrightarrow{f'} & W' \end{array}$$

kommutiert, so ist jede lineare Abbildung isomorph zu genau einer linearen Abbildung  $K^n \rightarrow K^m$  mit einer Matrix in Smith-Normalform nach 3.2.5.7.

**4.2.3.5 (Klassifikation der symmetrischen Bilinearformen).** Im folgenden sollen grundlegende Resultate zur Klassifikation symmetrischer Bilinearformen über einem vorgegebenen Körper  $K$  vorgestellt werden. Klassifiziert werden sollen genauer Paare  $(V, a)$  bestehend aus einem endlichdimensionalen Vektorraum  $V$  mit einer symmetrischen Bilinearform  $a : V \times V \rightarrow K$ , wobei zwei derartige Paare  $(V, a)$  und  $(V', a')$  isomorph heißen, wenn es einen Vektorraumisomorphismus  $\varphi : V \xrightarrow{\sim} V'$  gibt mit  $a(v, w) = a'(\varphi(v), \varphi(w))$  für alle  $v, w \in V$ . Eine derartige Klassifikation ist eng mit der Struktur des Körpers verknüpft und im allgemeinen schwierig. Wir geben zumindest im Fall eines algebraisch abgeschlossenen Körpers einer Charakteristik ungleich Zwei in 4.2.3.14 sowie im Fall  $K = \mathbb{R}$  in 4.2.3.23 Klassifikationen an. Die Klassifikation im Fall  $K = \mathbb{Q}$  ist ein interessantes Problem der Zahlentheorie.

**4.2.3.6 (Physikalische Motivation).** In der speziellen Relativitätstheorie modelliert man die Welt, in der wir leben, als einen vierdimensionalen reellen affinen Raum  $X$  aller „Raum-Zeit-Punkte“ alias „Ereignisse“. Wählen wir ein räumliches Koordinatensystem und einen Beginn der Zeitrechnung und eine Zeiteinheit, so können wir  $X$  mit dem  $\mathbb{R}^4$  identifizieren und jedes Ereignis wird spezifiziert durch eine Zeitkoordinate und drei Raumkoordinaten, also durch ein Vierupel von reellen Zahlen  $(t, x, y, z)$ . Das Licht breitet sich mit Lichtgeschwindigkeit aus. Genau dann wird also eine Explosion am Raumzeitpunkt  $p = (t, x, y, z)$  gesehen bei  $p' = (t', x', y', z')$ , wenn gilt

$$t' \geq t \quad \text{und} \quad c^2(t' - t)^2 - (x' - x)^2 - (y' - y)^2 - (z' - z)^2 = 0$$

für  $c$  die Lichtgeschwindigkeit. Betrachten wir auf dem Raum  $\mathbb{R}^4$  die sogenannte **Lorentzmetrik** alias die symmetrische Bilinearform  $l$  mit der Fundamentalmatrix  $\text{diag}(c^2, -1, -1, -1)$ , so kann die Zweite unserer Bedingungen auch umgeschrieben werden zur Bedingung  $l(\vec{v}, \vec{v}) = 0$  für  $\vec{v} = p' - p$ . Wenn Sie bereits die Definition einer Metrik kennen, seien Sie gewarnt, daß diese Lorentzmetrik im Sinne der in der Mathematik üblichen Terminologie keine Metrik ist. Nun vergessen wir wieder unsere Koordinaten und modellieren die Welt, in der wir leben, als einen vierdimensionalen reellen affinen Raum  $X$  mitsamt einer symmetrischen Bilinearform

$$l : \vec{X} \times \vec{X} \rightarrow \mathbb{R}$$

auf seinem Richtungsraum. Wir fordern, daß deren Fundamentalmatrix bezüglich mindestens einer Basis die oben angegebene Gestalt hat und daß sie die Ausbreitung des Lichts in der Weise beschreibt, daß  $l(\vec{v}, \vec{v}) = 0$  gleichbedeutend ist dazu, daß eine Explosion am Raumzeitpunkt  $p \in X$  entweder bei  $p + \vec{v}$  oder bei  $p - \vec{v}$  gesehen werden kann. Manchmal nennt man die Menge  $\{\vec{v} \mid l(\vec{v}, \vec{v}) = 0\}$  auch den **Lichtkegel** und seine Elemente **lichtartige Vektoren**. Wir werden später zeigen, daß jede weitere symmetrische Bilinearform  $l'$  mit der Eigenschaft  $l'(\vec{v}, \vec{v}) = 0 \Leftrightarrow l(\vec{v}, \vec{v}) = 0$  bereits ein Vielfaches von  $l$  sein muß. Die Wahl eines möglichen  $l$  bedeutet die Wahl einer Längeneinheit oder gleichbedeutend einer Zeiteinheit in der speziellen Relativitätstheorie. Das ist jedoch nicht, was an dieser Stelle diskutiert werden soll. Wir stellen uns die viel einfachere Frage, ob unsere Bilinearform nicht etwa bezüglich einer anderen Basis zum Beispiel  $\text{diag}(1, 1, 1, -1)$  als Fundamentalmatrix haben könnte. Das geht nun zwar nicht, aber wir wollen eben unter anderem verstehen, warum es nicht geht, und entwickeln dazu die Anfänge der allgemeinen Theorie der symmetrischen Bilinearformen.

**4.2.3.7 (Klassifikation quadratischer Formen).** In Charakteristik ungleich Zwei ist nach 4.2.2.4 die Klassifikation symmetrischer Bilinearformen gleichbedeutend zur Klassifikation quadratischer Formen. Genauer meinen wir hier die Klassifikation von Paaren  $(V, q)$  bestehend aus einem endlichdimensionalen Vektorraum  $V$  mit einer quadratischen Form  $q : V \rightarrow K$ , wobei zwei derartige Paare  $(V, q)$  und  $(V', q')$  isomorph heißen mögen, wenn es einen Vektorraumisomorphismus  $\varphi : V \xrightarrow{\sim} V'$  gibt mit  $q(v) = q'(\varphi(v))$  für alle  $v \in V$ .

**4.2.3.8 (Klassifikation quadratischer Formen auf der reellen Ebene).** Über dem Körper  $K = \mathbb{R}$  kann jede quadratische Form in zwei Variablen durch linearen Koordinatenwechsel in genau eine der folgenden fünf Formen überführt werden: Den „parabolischen Topf“  $x^2 + y^2$ , die „Sattelfläche“  $x^2 - y^2$ , den „umgestülpten parabolischen Topf“  $-x^2 - y^2$ , das „Tal“  $x^2$ , das „umgestülpte Tal“  $-x^2$  und die „Ebene“ 0. Formal sagt uns das der Trägheitssatz von Sylvester 4.2.3.23.

**4.2.3.9 (Klassifikation quadratischer Formen auf der komplexen Ebene).** Über einem algebraisch abgeschlossenen Körper  $K$  kann jede quadratische Form in

zwei Variablen durch linearen Koordinatenwechsel in genau eine der folgenden drei Formen überführt werden: Das Produkt linear unabhängiger Linearformen  $xy$ , das Quadrat einer von Null verschiedenen Linearform  $x^2$ , und die Nullform 0. In der Tat hat unsere Form Gestalt  $ax^2 + bxy + cy^2$  mit  $a, b, c \in K$ . Ist  $a \neq 0$ , so setzen wir  $y = 1$ , faktorisieren das so entstehende Polynom in einer Variablen, und finden uns in einem der beiden ersten Fälle wieder. Ist  $c \neq 0$ , so machen wir es analog. Der Fall  $a = c = 0$  ist eh einfach. Dasselbe gilt allgemeiner mit demselben Beweis, wenn das Quadrieren eine Surjektion  $K \rightarrow K$  ist und  $K$  nicht die Charakteristik Zwei hat.

**4.2.3.10 (Klassifikation quadratischer Formen auf Skalarprodukträumen).** Lassen wir nur orthogonale Koordinatenwechsel zu, so kann jede quadratische Form auf  $\mathbb{R}^2$  in genau eine Form der Gestalt  $\lambda x^2 + \mu y^2$  überführt werden mit  $\lambda \leq \mu$  reell: Das sagt uns der Satz über die Hauptachsentransformation 4.2.2.7, der auch seinerseits ein Klassifikationsproblem löst: Die Klassifikation quadratischer Formen auf endlichdimensionalen reellen Skalarprodukträumen. Hier sind die zu klassifizierenden Strukturen Tripel  $(V, s, q)$  mit  $V$  einem endlichdimensionalen reellen Vektorraum,  $s : V \times V \rightarrow \mathbb{R}$  einem Skalarprodukt und  $q : V \rightarrow \mathbb{R}$  einer quadratischen Form. Zwei derartige Tripel  $(V, s, q)$  und  $(V', s', q')$  heißen isomorph, wenn es einen Vektorraumisomorphismus  $\varphi : V \xrightarrow{\sim} V'$  gibt mit  $s(v, w) = s'(\varphi(v), \varphi(w))$  und  $q(v) = q'(\varphi(v))$  für alle  $v, w \in V$ . Die Klassifikation derartiger Tripel leistet also wie gesagt der Satz über die Hauptachsentransformation 4.2.2.7.

**Satz 4.2.3.11 (Existenz einer Orthogonalbasis).** Sei  $V$  ein endlichdimensionaler Vektorraum über einem Körper  $K$  mit  $\text{char } K \neq 2$ . So gibt es für jede symmetrische Bilinearform  $a$  auf  $V$  eine **Orthogonalbasis** alias eine Basis  $\mathcal{B} = (v_1, \dots, v_n)$  von  $V$  mit

$$i \neq j \Rightarrow a(v_i, v_j) = 0$$

**4.2.3.12.** Der Wortbestandteil „orthogonal“ möge Sie nicht dazu verleiten, sich hier für  $b$  ein Skalarprodukt vorzustellen. Dieser Fall wurde eh bereits durch 4.1.3.16 erledigt. Sie mögen stattdessen etwa an die Nullform  $b = 0$  denken oder an die Lorentzmetrik 4.2.3.6.

**Beweis.** Gilt für jeden Vektor  $v \in V$  bereits  $a(v, v) = 0$ , so folgt  $2a(v, w) = a(v + w, v + w) - a(v, v) - a(w, w) = 0$  für alle  $v, w$ . Wegen  $2 \neq 0$  in  $K$  folgt  $a = 0$  und jede Basis ist orthogonal. Sonst gibt es einen Vektor  $v_1 \in V$  mit  $a(v_1, v_1) \neq 0$ . Dann ist

$$\begin{aligned} \varphi : V &\rightarrow K \\ w &\mapsto a(v_1, w) \end{aligned}$$

eine lineare Abbildung mit  $v_1 \notin \ker \varphi$ . Aus Dimensionsgründen gilt sicher  $Kv_1 \oplus \ker \varphi = V$ . Mit Induktion über die Dimension dürfen wir annehmen, daß  $\ker \varphi$  eine Orthogonalbasis  $(v_2, \dots, v_n)$  besitzt. Dann ist aber  $(v_1, v_2, \dots, v_n)$  eine Orthogonalbasis von  $V$ .  $\square$

**Definition 4.2.3.13.** Ist  $V$  ein endlichdimensionaler Vektorraum und  $b$  eine Bilinearform auf  $V$ , so erklären wir den **Rang** von  $b$  als den Rang einer Fundamentalmatrix

$$\operatorname{rg}(b) = \operatorname{rg} F_B(b)$$

in Bezug auf eine und jede angeordnete Basis  $\mathcal{B}$  von  $V$ . Nach unserer Formel 4.2.1.8 für die Umrechnung zwischen den Fundamentalmatrizen zu verschiedenen Basen hängt diese Zahl in der Tat nicht von der Basis  $\mathcal{B}$  ab.

**4.2.3.14 (Klassifikation komplexer quadratischer Formen).** Ist  $K$  ein Körper einer Charakteristik  $\operatorname{char} K \neq 2$  und ist das Quadrieren  $x \mapsto x^2$  eine Surjektion  $K \rightarrow K$  und ist  $V$  ein endlichdimensionaler  $K$ -Vektorraum mit einer symmetrischen Bilinearform, so können wir die im Satz 4.2.3.11 gefundene Orthogonalbasis offensichtlich sogar dahingehend ändern, daß die Fundamentalmatrix die Gestalt  $\operatorname{diag}(1, \dots, 1, 0, \dots, 0)$  hat. Die Zahl der Einsen ist hierbei wohldefiniert als der Rang unserer Bilinearform. Insbesondere werden also komplexe quadratische Formen klassifiziert durch ihren Rang und die Dimension des zugrundeliegenden Vektorraums.

**Definition 4.2.3.15.** Eine Bilinearform auf einem Vektorraum  $V$  heißt **nichtausgeartet**, wenn es für jedes  $v \in V \setminus 0$  ein  $w \in W$  gibt mit  $b(v, w) \neq 0$  und umgekehrt auch für jedes  $w \in W \setminus 0$  ein  $v \in V$  mit  $b(v, w) \neq 0$ . Andernfalls heißt unsere Bilinearform **ausgeartet**.

**Definition 4.2.3.16.** Gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  und eine Bilinearform  $b : V \times V \rightarrow K$  erklären wir den **Ausartungsraum** alias das **Radikal** von  $V$  als den Untervektorraum

$$\operatorname{rad} b := \{v \in V \mid b(w, v) = 0 \quad \forall w \in V\}$$

Wir werden dieses Konzept im wesentlichen nur für symmetrische oder alternierende Bilinearformen verwenden und verzichten deshalb darauf, unseren Ausartungsraum feiner „Rechtsausartungsraum“ zu nennen und zusätzlich noch einen „Linksausartungsraum“ einzuführen.

**Satz 4.2.3.17 (Rang und Dimension des Radikals).** *Der Rang und die Dimension des Radikals einer Bilinearform  $b$  auf einem endlichdimensionalen Vektorraum  $V$  sind verknüpft durch die Beziehung*

$$\operatorname{rg}(b) + \dim(\operatorname{rad}(b)) = \dim V$$

4.2.3.18. Eine Bilinearform auf einem endlichdimensionalen Vektorraum ist insbesondere genau dann nichtausgeartet, wenn sie maximalen Rang hat.

*Beweis.* Ist  $\mathcal{B}$  eine angeordnete Basis von  $V$ , so können wir  $F_{\mathcal{B}}(b)$  auch verstehen als die Matrix der Abbildung  $\hat{b} : V \rightarrow V^{\top}$ , die jedem  $w \in V$  die Linearform „paare mit  $w$  unter  $b$ “ alias  $(\hat{b}(w))(v) := b(v, w)$  zuordnet. Genauer und in Formeln haben wir

$${}_{\mathcal{B}^{\top}}[\hat{b}]_{\mathcal{B}} = F_{\mathcal{B}}(b)$$

In der Tat, setzen wir  $\mathcal{B} = (v_1, \dots, v_n)$  und machen den Ansatz  $\hat{b}(v_i) = a_{1i}v_1^{\top} + \dots + a_{ni}v_n^{\top}$ , so liefert das Auswerten der Linearformen auf beiden Seiten dieser Gleichung auf dem Basisvektor  $v_j$  die Identität  $b(v_i, v_j) = (\hat{b}(v_j))(v_i) = a_{ij}$  und damit die Gleichheit aller Einträge unserer beiden Matrizen. Insbesondere gilt  $\text{rg}(b) = \text{rg}(\hat{b}) = \dim(\text{im } \hat{b})$ . Wegen  $\text{rad}(b) = \ker(\hat{b})$  folgt unsere Identität damit aus der Dimensionsformel 3.2.2.5, angewandt auf die lineare Abbildung  $\hat{b} : V \rightarrow V^{\top}$ .  $\square$

*Ergänzung 4.2.3.19.* Die Identität  ${}_{\mathcal{B}^{\top}}[\hat{b}]_{\mathcal{B}} = F_{\mathcal{B}}(b)$  aus dem vorhergehenden Beweis liefert auch einen zweiten Zugang zu unserer Formel 4.2.1.8 über das Verhalten der Fundamentalmatrix unter Basiswechsel: Wir rechnen einfach

$$F_{\mathcal{B}}(b) = {}_{\mathcal{B}^{\top}}[\hat{b}]_{\mathcal{B}} = {}_{\mathcal{B}^{\top}}[\text{id}]_{\mathcal{A}^{\top}} \circ {}_{\mathcal{A}^{\top}}[\hat{b}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}} = ({}_{\mathcal{A}}[\text{id}]_{\mathcal{B}})^{\top} \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\text{id}]_{\mathcal{B}}$$

unter Verwendung unserer Formel 3.2.9.16 für die Matrix der transponierten Abbildung.

*Ergänzung 4.2.3.20 (Bilinearformen und lineare Abbildungen).* Übung 3.2.3.16 liefert uns wie in 4.2.2.5 für jeden Vektorraum  $V$  einen kanonischen Isomorphismus

$$\begin{array}{ccc} \text{Bil}(V) & \xrightarrow{\sim} & \text{Hom}(V, V^{\top}) \\ b & \mapsto & \hat{b} \end{array}$$

zwischen dem Raum der Bilinearformen auf  $V$  und dem Raum der linearen Abbildungen von  $V$  in seinen Dualraum  $V^{\top}$ , gegeben durch die Abbildungsvorschrift  $b \mapsto \hat{b}$  mit  $\hat{b} : w \mapsto b(\ , w)$  alias  $(\hat{b}(w))(v) = b(v, w)$ . In ?? verwende ich die alternative Notation  $\hat{b} = \text{can}_b^2$  und betrachte zusätzlich auch noch  $\text{can}_b^1 : V \rightarrow V^{\top}$  gegeben durch  $v \mapsto b(v, \ )$ .

**Definition 4.2.3.21.** Eine quadratische Form  $q : V \rightarrow \mathbb{R}$  auf einem reellen Vektorraum  $V$  heißt

1. **positiv definit**, wenn gilt  $v \neq 0 \Rightarrow q(v) > 0$ ;
2. **positiv semidefinit**, wenn gilt  $q(v) \geq 0 \quad \forall v \in V$ ;

3. **negativ definit**, wenn gilt  $v \neq 0 \Rightarrow q(v) < 0$ ;
4. **negativ semidefinit**, wenn gilt  $q(v) \leq 0 \quad \forall v \in V$ ;
5. **indefinit**, wenn es  $v, w \in V$  gibt mit  $q(v) > 0$  und  $q(w) < 0$ .

Dieselben Bezeichnungen verwendet man auch für reelle symmetrische Matrizen  $A \in \text{Mat}(n; \mathbb{R})$ , wenn die zugehörige quadratische Form  $q_A : \mathbb{R}^n \rightarrow \mathbb{R}$  gegeben durch  $q_A(v) = v^\top A v$  die entsprechende Eigenschaft hat. Allgemeiner verwenden wir sie auch im Fall eines beliebigen angeordneten Grundkörpers. Positive definite Matrizen kennen wir bereits aus 4.1.12.21 im Fall von reellen symmetrischen und, über die hier diskutierte Terminologie hinausgehend, im Fall von komplexen hermiteschen Matrizen.

**4.2.3.22 (Prüfen von Definitheitseigenschaften).** Um die Definitheitseigenschaften einer reellen symmetrischen quadratischen Matrix zu bestimmen, bringt man sie am einfachsten durch Basiswechsel in Diagonalgestalt, wie im Beweis von 4.2.3.11 erklärt. Bei kleineren Matrizen kann auch das Hauptminoren-Kriterium 4.2.3.25 schnell zum Ziel führen.

**Satz 4.2.3.23 (Sylvester'scher Trägheitssatz).** *Gegeben ein endlichdimensionaler  $\mathbb{R}$ -Vektorraum  $V$  mit einer symmetrischen Bilinearform  $a$  gibt es stets eine angeordnete Basis  $\mathcal{B} = (v_1, \dots, v_n)$ , in der die Fundamentalmatrix von  $a$  die Gestalt*

$$F_{\mathcal{B}}(a) = \text{diag}(1, \dots, 1, -1, \dots, -1, 0, \dots, 0)$$

*annimmt. Die Zahl der Einsen, Minus-Einsen und Nullen wird hierbei durch besagte Bilinearform bereits eindeutig festgelegt.*

**4.2.3.24.** Die Differenz zwischen der Zahl der Minus-Einsen und der Zahl der Einsen heißt in diesem Kontext die **Signatur** unserer symmetrischen Bilinearform. Ich nenne das Tripel  $(p, m, n)$  aus der Zahl der Einsen, der Minus-Einsen und der Nullen den **Typ** unserer quadratischen Form. Die Signatur ist dann  $p - m$  und der Rang  $p + m$ . Das Supremum über die Dimensionen aller „negativ definiten“ Teilräume, also das  $m$ , nennt man den **Index** unserer Bilinearform. Er ist auch im Fall unendlichdimensionaler Vektorräume über einem angeordneten Körper mit einer symmetrischen Bilinearform noch sinnvoll definiert, kann aber dann den Wert  $\infty$  annehmen.

*Beweis.* Die Existenz einer Basis mit den geforderten Eigenschaften folgt unmittelbar aus der Existenz einer Orthogonalbasis 4.2.3.11, indem wir deren Vektoren mit geeigneten Skalaren multiplizieren. Die Zahl der Nullen ist wohlbestimmt als die Dimension des Radikals  $V_0$ . Ich behaupte, daß die Zahl der Einsen beziehungsweise Minus-Einsen beschrieben werden kann als die jeweils maximal mögliche

Dimension für einen Teilraum, auf dem unsere Bilinearform positiv definit beziehungsweise negativ definit ist. Sind in der Tat  $V_+ \subset V$  und  $V_- \subset V$  Teilräume der maximal möglichen Dimension mit dieser Eigenschaft, ja sogar irgendwelche Teilräume mit dieser Eigenschaft, so folgt  $V_- \cap V_0 = 0$  und  $V_+ \cap (V_- \oplus V_0) = 0$  und damit

$$\dim V_+ + \dim V_- + \dim V_0 \leq \dim V$$

Für jede Orthogonalbasis  $B$  bezeichne nun  $B_+$ ,  $B_-$  und  $B_0$  die Teilmenge derjenigen Basisvektoren, deren Paarung mit sich selber eine positive Zahl beziehungsweise eine negative Zahl beziehungsweise Null ergibt. So haben wir natürlich

$$|B_+| + |B_-| + |B_0| = \dim V$$

Da aber wegen der Maximalität von  $V_\pm$  offensichtlich gilt  $|B_\pm| \leq \dim V_\pm$  und da  $|B_0| \leq \dim V_0$  eh klar ist, muß bei diesen letzten Ungleichungen überall Gleichheit gelten.  $\square$

**Satz 4.2.3.25 (Hauptminoren-Kriterium für positive Definitheit).** *Eine reelle symmetrische  $(n \times n)$ -Matrix ist positiv definit genau dann, wenn für alle  $l \leq n$  die quadratische Untermatrix, die man durch Wegstreichen der letzten  $l$  Spalten und der untersten  $l$  Zeilen erhält, eine positive Determinante hat.*

4.2.3.26. Unser Kriterium wird auch als **Hurwitz-Kriterium** zitiert. Es gilt mit demselben Beweis auch für Matrizen mit Einträgen in einem beliebigen angeordneten Körper. Die naheliegende Verallgemeinerung mit positiv semidefinit und nichtnegativen Determinanten gilt nicht, wie schon das Beispiel der Diagonalmatrix  $\text{diag}(0, -1)$  zeigt. Weitere Definitheitskriterien speziell für Matrizen mit nichtnegativen Einträgen außerhalb der Diagonalen findet man in ??.

*Beweis.* Wählen wir eine Orthogonalbasis der zu unserer Matrix gehörigen symmetrischen Bilinearform auf  $\mathbb{R}^n$ , so hat die Determinante der zugehörigen diagonalen Fundamentalmatrix nach unserer Transformationsformel 4.2.1.8 für die Fundamentalmatrizen zu verschiedenen Basen dasselbe Vorzeichen wie die Determinante unserer Ausgangsmatrix. Ist also unsere Ausgangsmatrix nicht positiv definit und hat positive Determinante, so existiert ein zweidimensionaler Teilraum, auf dem sie negativ definit ist. Dieser Teilraum schneidet die Hyperebene  $(\mathbb{R}^{n-1} \times 0) \subset \mathbb{R}^n$  nach dem Dimensionssatz 3.2.2.9 nicht nur in Null. Ist also unsere Ausgangsmatrix nicht positiv definit und hat positive Determinante, so ist die quadratische Untermatrix, die man durch Wegstreichen der letzten Spalte und der untersten Zeile erhält, nicht positiv definit. Eine offensichtliche Induktion beendet den Beweis.  $\square$

**Satz 4.2.3.27 (Satz über Hauptachsentransformationen, Variante).** *Gegeben ein endlichdimensionaler  $\mathbb{R}$ -Vektorraum mit zwei symmetrischen Bilinearformen,*

von denen die Erste ein Skalarprodukt ist, besitzt unser Vektorraum eine Basis, die sowohl orthonormal ist für die erste als auch orthogonal für die zweite Bilinearform.

4.2.3.28. Ist also in Formeln  $V$  unser endlichdimensionaler reeller Vektorraum und  $s$  ein Skalarprodukt auf  $V$  und  $a$  eine weitere symmetrische Bilinearform, so besitzt  $V$  eine Basis  $(v_1, \dots, v_n)$  mit  $s(v_i, v_j) = \delta_{ij}$  und  $a(v_i, v_j) = 0$  für  $i \neq j$ . Dieselbe Aussage gilt mit demselben Beweis auch für endlichdimensionale komplexe Vektorräume mit zwei hermiteschen Bilinearformen, von denen die erste ein Skalarprodukt ist.

*Beweis.* Das ist nur eine Umformulierung des Satzes über Hauptachsentransformationen 4.2.2.7. Es ist aber schneller, den Beweis zu wiederholen. Wir finden nach 4.2.2.6 einen bezüglich unseres Skalarprodukts  $s$  selbstadjungierten Endomorphismus  $A$  von  $V$  mit

$$a(v, w) = s(Av, w) \quad \forall v, w \in V$$

Nach dem Spektralsatz 4.1.12.15 besitzt  $V$  eine Orthonormalbasis  $v_1, \dots, v_n$  in Bezug auf  $s$  aus Eigenvektoren von  $A$ . Sie leistet das Gewünschte.  $\square$

**Korollar 4.2.3.29 (Singulärwertzerlegung).** Gegeben eine lineare Abbildung zwischen endlichdimensionalen reellen oder komplexen Skalarprodukträumen gibt es stets eine Orthonormalbasis des Definitionsbereichs, die auf eine Familie von paarweise orthogonalen Vektoren des Wertebereichs abgebildet wird.

4.2.3.30. In geeigneten Orthonormalbasen ist die Matrix unserer Abbildung mit hin eine Diagonalmatrix mit nichtnegativen Einträgen auf der Diagonalen. Diese Einträge sind wohldefiniert als die Quadratwurzeln der Eigenwerte des Produkts unserer Abbildung mit ihrer Adjungierten. Sie heißen die **Singulärwerte** unserer Abbildung.

4.2.3.31. Die Singulärwertzerlegung verallgemeinert unsere Polarzerlegungen von Automorphismen 4.1.12.23 und Endomorphismen 4.1.12.30: Wir erhalten genauer eine Polarzerlegung aus einer Singulärwertzerlegung, indem wir „zunächst die Vektoren unserer Orthonormalbasis mit einer positiv semidefiniten Abbildung auf die Länge ihrer Bilder strecken oder stauchen, und die so auf die richtige Länge gebrachten Vektoren durch eine Drehung in die richtigen Richtungen bringen“.

4.2.3.32. In der Sprache der Matrizen ausgedrückt besagt unser Korollar, daß es für jede reelle beziehungsweise komplexe Matrix  $A$  orthogonale beziehungsweise unitäre quadratische Matrizen  $C, K$  gibt derart, daß  $CAK = D$  diagonal ist mit nichtnegativen Einträgen. Diese Einträge sind dann wieder wohldefiniert und heißen die **Singulärwerte** unserer Matrix. Die Darstellung als Produkt  $A = C^{-1}DK^{-1}$  schließlich heißt eine **Singulärwertzerlegung** unserer Matrix  $A$ .

*Beweis.* Sei  $f : V \rightarrow W$  unsere Abbildung. Wir betrachten auf  $V$  zusätzlich zum Skalarprodukt  $s = s_V$  die positiv semidefinite symmetrische beziehungsweise hermitesche Bilinearform  $a(u, v) := s_W(f(u), f(v))$ . Die vorhergehenden Varianten 4.2.3.27 und 4.2.3.28 des Satzes über Hauptachsentransformationen liefern dann unmittelbar die Behauptung.  $\square$

4.2.3.33 (**Gram'sche Determinante und Volumen**). Gegeben ein reeller Skalarproduktraum  $V$  mit Vektoren  $v_1, \dots, v_n$  heißt die quadratische Matrix mit den Skalarprodukten  $\langle v_i, v_j \rangle$  als Einträgen auch die **Gram'sche Matrix** unserer Vektoren und ihre Determinante die **Gram'sche Determinante**. Bilden unsere Vektoren eine Basis, so ist die Gram'sche Matrix die Fundamentalmatrix unseres Skalarprodukts bezüglich dieser Basis. Sind die Vektoren  $v_1, \dots, v_n$  linear abhängig, so ist die Gram'sche Determinante offensichtlich Null. Sind sie linear unabhängig, so mag man die Wurzel der Gram'schen Determinante in der schmutzigen Anschauung als das „Volumen des von den Vektoren  $v_1, \dots, v_n$  in ihrem Erzeugnis aufgespannten Parallelpipeds“ verstehen. Sei in der Tat ohne Beschränkung der Allgemeinheit  $V = \mathbb{R}^n$  mit seinem Standardskalarprodukt. Für die Matrix  $M := (v_1 | \dots | v_n)$  mit unseren Vektoren in den Spalten bedeutet dann, wie bereits in 3.6.2.6 diskutiert, in der schmutzigen Anschauung  $|\det M|$  das Volumen unseres Parallelpipeds. Unsere Gram'sche Matrix aber ist in diesem Fall gerade das Produkt  $M^\top M$  und dessen Determinante ergibt sich zu  $\det(M^\top M) = (\det M)^2$  wie behauptet.

## Übungen

*Übung 4.2.3.34.* Ist  $s$  ein Skalarprodukt auf einem Vektorraum über einem angeordneten Körper und  $v_1, \dots, v_n$  eine endliche Familie von Vektoren von  $V$ , so ist die Matrix  $(s(v_i, v_j))_{ij}$  positiv semidefinit. Es reicht hierfür sogar, die Bilinearform  $s$  symmetrisch und positiv semidefinit anzunehmen. Hinweis: Man betrachte den Beweis von Satz 4.2.3.29 zur Singulärwertzerlegung.

*Ergänzende Übung 4.2.3.35.* Unter einer **bilinearen Paarung** von zwei Vektorräumen  $V, W$  über demselben Grundkörper  $K$  versteht man eine bilineare Abbildung  $b : V \times W \rightarrow K$ . Solch eine Paarung heißt **nichtausgeartet**, wenn es für jedes  $v \in V \setminus \{0\}$  ein  $w \in W$  gibt mit  $b(v, w) \neq 0$  und umgekehrt auch für jedes  $w \in W \setminus \{0\}$  ein  $v \in V$  mit  $b(v, w) \neq 0$ . Andernfalls heißt unsere Paarung **ausgeartet**. Man zeige das **Lemma von Mackey**: Gegeben eine nichtausgeartete Paarung  $b : V \times W \rightarrow K$  zwischen zwei Vektorräumen  $V, W$  unendlicher Dimension mit abzählbarer Basis gibt es stets eine Basis  $(v_n)_{n \in \mathbb{N}}$  von  $V$  und eine Basis  $(w_n)_{n \in \mathbb{N}}$  von  $W$  derart, daß gilt  $b(v_i, w_j) = \delta_{ij}$ . Hinweis: Man beginne mit zwei beliebigen Basen und wechsle geeignet Basen.

*Ergänzende Übung 4.2.3.36.* Gegeben zwei Vektorräume  $V, W$  mit einer bilinearen Paarung  $b : V \times W \rightarrow K$  und eine Teilmenge  $T \subset W$  setzen wir ganz allgemein

$$T^\perp := \{v \in V \mid b(v, t) = 0 \quad \forall t \in T\}$$

und nennen  $T^\perp$  wie in 4.1.3.17 den **Orthogonalraum von  $U$** . Gegeben zwei Vektorräume  $V, W$  mit einer nichtausgearteten Paarung  $b : V \times W \rightarrow K$  und ein Untervektorraum  $U \subset W$  zeige man für die Dimension des Orthogonalraums  $U^\perp$  von  $U$  die Formel  $\dim U + \dim U^\perp = \dim V$ .

*Ergänzende Übung 4.2.3.37 (Restriktionen reeller quadratischer Formen).* Sei  $V$  ein endlichdimensionaler reeller Vektorraum mit einer quadratischen Form alias symmetrischen Bilinearform  $s$  und sei  $U \subset V$  ein Untervektorraum der Kodimension  $\text{codim}(U \subset V) = 1$ . Sei  $(V, s)$  vom Typ  $(p, m, n)$  in der Terminologie aus 4.2.3.24. So gibt es für den Typ von  $U$  nur die vier Alternativen  $(p-1, m, n), (p, m-1, n), (p, m, n-1)$  und  $(p-1, m-1, n+1)$ . Des weiteren werden von diesen Alternativen alle, die keine negativen Einträge haben, auch tatsächlich realisiert. Hinweis: Am einfachsten ist der Fall  $U^\perp + U = V$ . Sonst gilt  $V^\perp \subset U^\perp \subset U$  und man unterscheidet die Fälle  $V^\perp = U^\perp$  und  $V^\perp \neq U^\perp$ . Im zweiten Fall wählt man  $v \in V \setminus U$  beliebig und findet  $w \in U^\perp$  mit  $s(v, w) \neq 0$ . Dann ist die Form nichtausgeartet auf  $\langle v, w \rangle$  und das orthogonale Komplement  $\langle v, w \rangle^\perp$  dieser Ebene ist auch ein Vektorraumkomplement und der Fall ist erledigt. Im ersten Fall kann man zu  $U/U^\perp \subset V/U^\perp$  übergehen. Da dann die Form auf  $U/U^\perp$  nicht ausgeartet ist, ist wieder das orthogonale Komplement ein Vektorraumkomplement und das Argument ist schnell fertig.

*Ergänzende Übung 4.2.3.38 (Signatur auf Subquotienten).* Sei  $V$  ein endlichdimensionaler reeller Vektorraum mit einer nichtausgearteten quadratischen Form alias symmetrischen Bilinearform  $s$  und sei  $S \subset V$  ein Untervektorraum, auf dem die Restriktion unserer Bilinearform verschwindet. So hat die auf  $S^\perp/S$  induzierte Form dieselbe Signatur wie die ursprüngliche Form. Hinweis: Man mag sich mit Induktion auf den Fall  $\dim S = 1$  zurückziehen und diesen Fall auf die vorhergehende Übung 4.2.3.37 zurückführen.

*Ergänzende Übung 4.2.3.39.* Man zeige, daß im Raum aller invertierbaren symmetrischen reellen quadratischen Matrizen zwei Matrizen genau dann zu derselben Wegzusammenhangskomponente gehören, wenn sie denselben Typ im Sinne von 4.2.3.24 haben.

*Ergänzende Übung 4.2.3.40.* Gegeben zwei verschiedene Punkte der Ebene  $p, q \in \mathbb{R}^2$  und eine positive Zahl  $b < \|p - q\|$  zeige man, daß die Punkte  $r \in \mathbb{R}^2$  mit  $\|r - p\| - \|r - q\| = b$  einen Hyperbelast bilden, als da heißt, daß die Menge dieser Punkte unter einer geeigneten Bewegung in die Menge der Lösungen mit positiver  $x$ -Koordinate eines Gleichungssystems der Gestalt  $x^2 - \mu y^2 = c$  mit

$\mu, c$  positiv übergeht. Gegeben zwei verschiedene Punkte der Ebene  $p, q \in \mathbb{R}^2$  und eine positive Zahl  $a > \|p - q\|$  zeige man weiter, daß die Punkte  $r \in \mathbb{R}^2$  mit  $\|r - p\| + \|r - q\| = a$  eine Ellipse bilden, als da heißt, daß die Menge dieser Punkte unter einer geeigneten Bewegung in die Menge der Lösungen eines Gleichungssystems der Gestalt  $x^2 + \mu y^2 = c$  mit  $\mu, c$  positiv übergeht. So erstellen übrigends Gärtner elliptische Beete: Sie rammen zwei Pflöcke ein, legen um diese eine Seilschlaufe und fahren mit einem dritten Pflock in der Schlaufe um diese beiden Pflöcke herum, soweit außen wie möglich.

*Übung 4.2.3.41 (Inhomogene quadratische Formen).* Man zeige: Gegeben eine Polynomfunktion vom Grad höchstens Zwei mit Koeffizienten in einem Körper  $K$  mit  $\text{char } K \neq 2$ , also eine Abbildung  $q : K^n \xrightarrow{\sim} K$  der Gestalt

$$q(x_1, \dots, x_n) = \sum_{i \leq j} c_{ij} x_i x_j + \sum_i b_i x_i + a$$

gibt es entweder einen Automorphismus von affinen Räumen  $D : K^n \rightarrow K^n$  mit

$$(q \circ D)(y_1, \dots, y_n) = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2 + c$$

oder einen Automorphismus von affinen Räumen  $D : K^n \rightarrow K^n$  mit

$$(q \circ D)(y_1, \dots, y_n) = \lambda_1 y_1^2 + \dots + \lambda_{n-1} y_{n-1}^2 + y_n$$

für geeignete  $\lambda_i, c \in K$ . Hier können wir sogar erreichen, daß alle  $\lambda_i$  in einem vorgegebenen Repräsentantensystem des Quotienten  $K^\times / (K^\times)^2$  disjunkt vereinigt mit der Null liegen, im Fall  $K = \mathbb{R}$  also etwa in  $\{-1, 0, 1\}$  oder im Fall eines algebraisch abgeschlossenen Körpers in  $\{0, 1\}$ .

*Übung 4.2.3.42 (Klassifikation inhomogener quadratischer Formen).* Gegeben ein Körper  $K$  und ein affiner Raum  $E$  über  $K$  verstehen wir unter einer **inhomogenen quadratischen Form auf  $E$**  eine Abbildung  $Q : E \rightarrow K$ , die sich schreiben läßt in der Gestalt  $Q(p + \vec{v}) = q(\vec{v}) + a(p + \vec{v})$  mit  $q : \vec{E} \rightarrow K$  einer quadratischen Form auf  $\vec{E}$  und  $a : E \rightarrow K$  affin. Man diskutiere die Klassifikation inhomogener quadratischer Formen auf endlichdimensionalen affinen Räumen über den Körpern  $\mathbb{R}$  und  $\mathbb{C}$ . Hinweis: 4.2.3.41.

*Übung 4.2.3.43 (Klassifikation von Geradenpaaren im Raum).* Man zeige, daß die möglichen Vorgaben bestehend aus einem ungeordneten Paar von Geraden in einem dreidimensionalen affinen Raum über einem festen Körper in genau vier Isomorphieklassen zerfallen. In der Schule lernt man diese man üblicherweise als „gleich, parallel, sich schneidend und windschief“ kennen.

#### 4.2.4 Satz von Witt\*

4.2.4.1. Seien  $(V, a)$  und  $(W, b)$  Vektorräume mit symmetrischen Bilinearformen. Eine lineare Abbildung  $f : V \rightarrow W$  heißt **isometrisch**, wenn gilt

$$a(u, v) = b(f(u), f(v)) \quad \forall u, v \in V$$

**Satz 4.2.4.2 (von Witt).** *Seien  $K$  ein Körper einer Charakteristik  $\text{char } K \neq 2$  und  $V$  ein  $K$ -Vektorraum endlicher Dimension und  $b : V \times V \rightarrow K$  eine nicht ausgeartete symmetrische Bilinearform. Ist  $U \subset V$  ein Untervektorraum und  $\varphi : U \hookrightarrow V$  eine isometrische Injektion, so gibt es eine Fortsetzung von  $\varphi$  zu einem isometrischen Isomorphismus  $\varphi : V \xrightarrow{\sim} V$ .*

*Beispiel 4.2.4.3.* Ist etwa der  $\mathbb{R}^4$  versehen mit der Lorentzmetrik, so können je zwei von Null verschiedene lichtartige Vektoren ineinander überführt werden durch einen Automorphismus, der die Lorentzmetrik erhält.

*Beweis.* Es reicht, die Existenz einer Fortsetzung von  $\varphi$  auf einen echt größeren Teilraum nachzuweisen. Wir unterscheiden zwei Fälle.

*Fall 1:* Die Einschränkung  $b : U \times U \rightarrow K$  unserer Form ist ausgeartet. Dann gibt es  $u \in U \setminus \{0\}$  mit  $b(u, v) = 0 \quad \forall v \in U$ . Wir suchen zunächst ein  $u_1 \in V$  mit  $b(u, u_1) = 1$  und finden es, da  $b$  auf  $V$  nicht ausgeartet ist. Indem wir notfalls  $u_1$  durch  $u_1 + \lambda u$  mit  $\lambda \in K$  ersetzen, dürfen wir  $b(u_1, u_1) = 0$  annehmen, und nach Annahme gilt  $u_1 \notin U$ . Ebenso finden wir  $u_2 \in V$  mit  $b(u_2, \varphi(v)) = b(u_1, v)$  für alle  $v \in U$ , ja sogar für alle  $v \in V$ . Wieder können wir, indem wir notfalls  $u_2$  durch  $u_2 + \mu\varphi(u)$  ersetzen,  $b(u_2, u_2) = 0$  annehmen. Dann aber können wir  $\varphi$  ausdehnen auf  $U + \langle u_1 \rangle$  durch die Vorschrift  $\varphi(u_1) = u_2$ . Das erledigt den Fall, daß  $b$  auf  $U$  ausgeartet ist.

*Fall 2:* Die Einschränkung von  $b$  auf  $U$  ist nichtausgeartet. In diesem Fall argumentieren wir mit Induktion über  $\dim_K U$ . Für die Induktionsbasis sei  $U = \langle u \rangle$  eindimensional. Dann gilt also  $b(u, u) \neq 0$  und ebenso  $b(\varphi(u), \varphi(u)) \neq 0$ . Gälte  $b(u + \varphi(u), u + \varphi(u)) = 0 = b(u - \varphi(u), u - \varphi(u))$ , so folgte  $2b(u, u) + 2b(u, \varphi(u)) = 0 = 2b(u, u) - 2b(u, \varphi(u))$  und damit  $4b(u, u) = 0$  alias  $b(u, u) = 0$ . Da das nicht sein kann, dürfen wir, indem wir notfalls  $\varphi$  durch  $-\varphi$  ersetzen, für  $v := u - \varphi(u)$  annehmen, daß gilt  $b(v, v) \neq 0$ . Dann betrachten wir die lineare Abbildung  $s = s_v$  mit  $s(v) = -v$  und  $s(w) = w \quad \forall w \in v^\perp$ . Sie ist isometrisch und hat die Eigenschaft  $s : u + \varphi(u) \mapsto u + \varphi(u)$  und  $s : u - \varphi(u) \mapsto \varphi(u) - u$  und folglich  $s : u \mapsto \varphi(u)$ . Diese Abbildung dehnt folglich  $\varphi$  sogar orthogonal auf ganz  $V$  aus. Für den Induktionsschritt sei  $\dim_K U > 1$ . Dann können wir sicher  $U = W \oplus W_U^\perp$  zerlegen mit  $W \neq 0 \neq W_U^\perp$ , wobei mit  $W_U^\perp$  der Orthogonalraum in  $U$  gemeint ist. Zu unserem  $\varphi : U \hookrightarrow V$  gibt es nach Induktionsannahme einen mit der Bilinearform verträglichen Automorphismus  $s : V \xrightarrow{\sim} V$  mit  $s|W = \varphi|W$ .

Also ist  $s^{-1} \circ \varphi : U \hookrightarrow V$  die Identität auf  $W$  und seine Restriktion zu einer Einbettung  $W_U^\perp \hookrightarrow W^\perp$  läßt sich wieder nach Induktion zu einem isometrischen Isomorphismus  $t : W^\perp \xrightarrow{\sim} W^\perp$  ausdehnen. Dann ist  $(\text{id}_W \oplus t) : V \xrightarrow{\sim} V$  eine Ausdehnung von  $s^{-1} \circ \varphi$  und damit  $s \circ (\text{id}_W \oplus t)$  die gesuchte Ausdehnung von  $\varphi$ .  $\square$

## Übungen

*Übung 4.2.4.4 (Variante des Satzes von Witt für ausgeartete Bilinearformen).* Man gebe ein Gegenbeispiel zum Satz von Witt an im Fall einer ausgearteten symmetrischen Bilinearform. Man zeige andererseits, daß die Aussage des Satzes weiter gilt, wenn wir ausgeartete Bilinearformen  $b$  erlauben, dafür aber zusätzlich  $U \cap \text{rad}(b) = \varphi(U) \cap \text{rad}(b) = 0$  fordern.

### 4.2.5 Alternierende Bilinearformen

4.2.5.1. Man erinnere aus 3.6.3.1, daß eine Bilinearform **alternierend** heißt, wenn Null herauskommt, sobald wir zweimal denselben Vektor einsetzen. Ich kann für dieses Konzept leider keine Anschauung anbieten.

**Satz 4.2.5.2 (Klassifikation alternierender Bilinearformen).** Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem Körper  $K$  und eine alternierende Bilinearform  $\omega : V \times V \rightarrow K$  besitzt  $V$  stets eine angeordnete Basis  $\mathcal{B}$ , bezüglich derer die Fundamentalmatrix von  $\omega$  die Gestalt

$$F_{\mathcal{B}}(\omega) = \begin{pmatrix} & & & \\ & \boxed{0 & -1} & & \\ & \boxed{1 & 0} & & \\ & & \ddots & \\ & & & \boxed{0 & -1} \\ & & & \boxed{1 & 0} \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

hat. Die Zahl der Zweierblöcke hängt hierbei nicht von der Wahl der Basis ab.

*Vorschau 4.2.5.3.* Eine Variante für freie abelsche Gruppen mit alternierender nicht ausgearteter Bilinearform wird in ?? bewiesen.

*Beweis.* Ist unsere Form nicht Null, so finden wir  $v, w \in V$  mit  $\omega(v, w) \neq 0$ . Durch Multiplikation von  $v$  mit einem Skalar erreichen wir sogar  $\omega(v, w) = 1$

und damit  $\omega(w, v) = -1$ . Diese beiden Vektoren  $v, w$  können wir schon einmal als die ersten beiden Vektoren unserer Basis in spe festhalten. Wir betrachten nun die Linearformen  $\omega(v, \cdot) : V \rightarrow K$  und  $\omega(w, \cdot) : V \rightarrow K$ . Sie sind beide nicht Null und ihre Kerne sind verschieden, genauer liegt  $v$  im Kern der ersten, nicht aber der zweiten Abbildung und  $w$  im Kern der Zweiten, nicht aber der Ersten. Für den Schnitt

$$S = \{u \in V \mid \omega(v, u) = 0 = \omega(w, u)\}$$

haben wir also  $\dim S = \dim V - 2$  und  $(Kv \oplus Kw) \cap S = 0$ . Aus Dimensionsgründen folgt

$$V = (Kv \oplus Kw) \oplus S$$

und eine offensichtliche Induktion über die Dimension beendet den Beweis der Existenz. Die Zahl der Nullen nach den Zweierkästchen kann beschrieben werden als die Dimension des Radikals unserer Bilinearform und ist deshalb ebenso wie die Zahl der Zweierkästchen von der Wahl der Basis unabhängig.  $\square$

**4.2.5.4.** Eine im Sinne von 4.2.3.35 nichtausgeartete alternierende Bilinearform heißt auch eine **symplektische Form**, und ein mit einer symplektischen Form versehener Vektorraum heißt ein **symplektischer Vektorraum**. Symplektische Vektorräume spielen in der Hamilton'schen Mechanik eine wichtige Rolle. Nach 4.2.5.2 ist die Dimension eines endlichdimensionalen symplektischen Vektorraums stets gerade.

### Übungen

*Übung 4.2.5.5.* In einem endlichdimensionalen symplektischen Vektorraum können je zwei von Null verschiedene Vektoren durch einen die symplektische Form erhaltenden Automorphismus ineinander überführt werden.

*Übung 4.2.5.6.* Gegeben eine symmetrische Bilinearform auf einem endlichdimensionalen Vektorraum  $V$  über einem Körper der Charakteristik Zwei existiert stets eine Zerlegung in paarweise orthogonale Teile  $V = V_d \oplus V_a$  derart, daß die Restriktion auf  $V_d$  eine Orthogonalbasis besitzt und die Restriktion auf  $V_a$  alternierend ist. Man zeige durch ein dreidimensionales Beispiel, daß selbst im Fall nichtausgearteter Formen die Dimensionen von  $V_d$  und  $V_a$  durch unsere Bilinearform keineswegs eindeutig festgelegt werden.

*Ergänzende Übung 4.2.5.7.* Gegeben eine alternierende Bilinearform  $\omega$  auf einem Vektorraum  $V$  der Dimension  $2n$  zeige man, daß man eine alternierende  $(2n)$ -Multilinearform  $\omega^{\wedge n}$  auf  $V$  erklären kann durch die Vorschrift

$$\omega^{\wedge n}(v_1, \dots, v_{2n}) := \sum_{\sigma \in R} \operatorname{sgn}(\sigma) \omega(v_{\sigma(1)}, v_{\sigma(2)}) \dots \omega(v_{\sigma(2n-1)}, v_{\sigma(2n)})$$

mit  $R \subset S_{2n}$  der Menge aller Permutationen von  $\{1, \dots, 2n\}$  mit den Eigenschaften  $\sigma(2i-1) < \sigma(2i)$  für alle  $i$  und  $\sigma(1) < \sigma(3) < \dots < \sigma(2n-1)$ . Für  $g \in \mathrm{GL}(V)$  zeige man  $(\omega \circ (g \times g))^{\wedge n} = (\det g)\omega^{\wedge n}$ . Weiter zeige man, daß für  $\omega$  eine symplektische Form die Multilinearform  $\omega^{\wedge n}$  von Null verschieden ist. Sobald Sie einmal mit dem Dachprodukt  $\wedge$  in der äußeren Algebra  $\bigwedge V^*$  vertraut sind, können Sie  $\omega^{\wedge n}$  auch als die  $n$ -te Potenz  $\omega^{\wedge n} = \omega \wedge \dots \wedge \omega$  in der äußeren Algebra verstehen, daher die Notation.

*Ergänzende Übung 4.2.5.8.* Sei  $K$  ein Körper. Gegeben eine alternierende Matrix  $A \in \mathrm{Mat}(2n; K)$  alias eine Matrix mit  $A = -A^\top$  und mit Nullen auf der Diagonale erklären wir ihre **Pfaff'sche Determinante**  $\mathrm{Pf}(A)$  mithilfe ihrer alternierenden Bilinearform  $\omega_A(v, w) := v^\top A w$  und der zugehörigen Multilinearform  $\omega_A^{\wedge n}$  aus 4.2.5.7 durch die Identität

$$\omega_A^{\wedge n} = \mathrm{Pf}(A) \det$$

im eindimensionalen Raum  $\mathrm{Alt}^{2n}(K^{2n})$  aller Multilinearformen auf dem  $K^{2n}$ . Für  $B \in \mathrm{Mat}(2n; K)$  folgere man

$$\mathrm{Pf}(B^\top A B) = (\det B) \mathrm{Pf}(A)$$

Weiter zeige man  $\mathrm{Pf}(S) = 1$  für  $S \in \mathrm{Mat}(2n; K)$  die blockdiagonale Matrix mit  $n$  Blöcken  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  und folgere, daß das Quadrat der Paff'schen Determinante die übliche Determinante ist, in Formeln

$$\mathrm{Pf}(A)^2 = \det(A)$$

*Ergänzende Übung 4.2.5.9.* Gegeben ein symplektischer Vektorraum  $(V, \omega)$  heißt ein Vektorraumautomorphismus  $g : V \xrightarrow{\sim} V$  **symplektisch**, wenn gilt  $\omega(gv, gw) = \omega(v, w) \forall v, w \in V$ . Man zeige, daß jeder symplektische Automorphismus  $g$  eines endlichdimensionalen symplektischen Vektorraums die Determinante  $\det(g) = 1$  hat. Hinweis: 4.2.5.7.

*Ergänzende Übung 4.2.5.10.* Gegeben ein Vektorraum  $V$  erhalten wir eine symplektische Form  $\omega$  auf  $V \oplus V^*$  durch die Vorschrift

$$\omega((v, \phi), (w, \psi)) := \phi(w) - \psi(v)$$

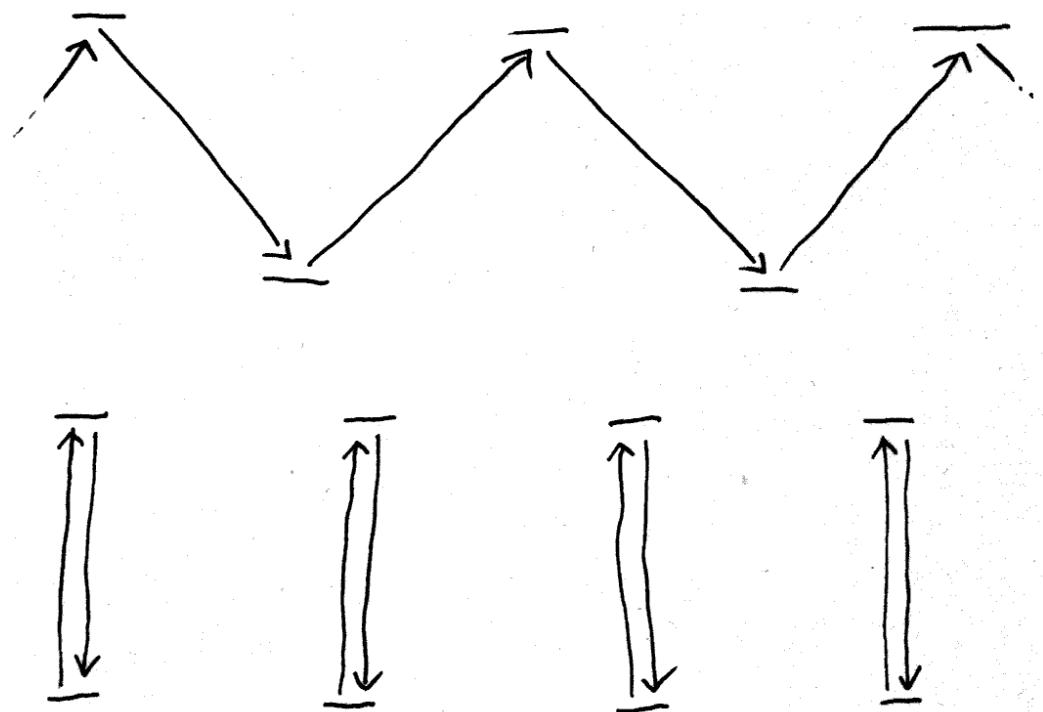
## 4.2.6 Relativistische Raumzeit\*

4.2.6.1 (**Erinnerungen zu klassischem Raum und klassischer Zeit**). In der Modellierung von Zeit und Raum für die Belange der Newton'schen Mechanik in ?? oder 4.1.6.4 haben wir erst einmal ignoriert, daß die Erde sich um sich selber dreht

und dabei gleichzeitig um die Sonne rast, die sich hinwiederum mit unvorstellbarer Geschwindigkeit um das Zentrum der Milchstraße bewegt, und so weiter, und sind schlicht von einem dreidimensionalen affinen Raum ausgegangen, von dessen Punkten man einige ganz explizit als Kirchturmspitzen, Zimmerecken und dergleichen angeben kann. Dann haben wir eine Gruppe von „Bewegungen“ unseres Raums postuliert und verwendet, um den eindimensionalen Raum der Längen einzuführen, in dem das Pariser Urmeter eine Basis auszeichnet. Zusätzlich haben wir einen orientierten eindimensionalen affinen Raum aller „Zeitpunkte“ postuliert und in dessen Richtungsraum die Basis „Sekunde“ mithilfe von Tag und ausgezeichnet. In diesem Rahmen ist dann schon klar, was gemeint ist, wenn wir sagen, die Lichtgeschwindigkeit betrage so in etwa 300 000 Kilometer pro Sekunde.

**4.2.6.2 (Motivation für relativistische Raumzeit).** Sobald wir jedoch dies alles nicht mehr ignorieren, ist es plötzlich gar nicht mehr so klar: Es gibt dann sozusagen gar keinen „festen Raum“ mehr, in dem unsere Lichtgeschwindigkeit konstant sein könnte, sondern „alles ist relativ“. Denken wir uns etwa zwei Raketen, die in entgegengesetzter Richtung aneinander vorbeifliegen, und einen Lichtstrahl, der in Richtung der einen Rakete zwischen ihnen hindurchsaust. Müßte in diesem Fall nicht von den beiden Besatzungen für diesen Lichtstrahl eine unterschiedliche Geschwindigkeit gemessen werden? Statt im weiteren stets von „Rakete Eins“ und „Rakete Zwei“ zu reden, denken wir uns der Klarheit der Darstellung halber lieber den einen Beobachter in einem sehr langen Zug und nennen ihn den Schaffner, und denken uns den anderen Beobachter auf einem Bahnhof, durch den der besagte Zug fährt, und nennen ihn den Bahnhofsvorsteher. Der Schaffner mißt seinen Zug sorgfältig aus und setzt sich genau in die Mitte. Gerade zu dem Zeitpunkt, zu dem sich Schaffner und Bahnhofsvorsteher gegenüberstehen, sehen beide auch noch die Vorder- und die Rücklichter des Zuges aufleuchten. Daraus ziehen sie jedoch unterschiedliche Schlüsse. Der Schaffner sagt: Na klar, die sind gleichzeitig angegangen. Der Bahnhofsvorsteher dahingegen meint: Als diese Lampen ihr Licht ausgesandt haben, das ist ja nun eine kleine Weile her, war die Lokomotive noch näher am Bahnhof als der Schlußwagen, folglich müssen die Lichter des Schlußwagens etwas früher angegangen sein, damit ihr Licht dennoch meine Augen zur selben Zeit erreichen konnte wie das Licht aus den Lampen der Lokomotive. Wer hat aber denn nun recht? Unmittelbar würde man wohl erst einmal sagen: Der Bahnhofsvorsteher hat recht, denn er bewegt sich nicht; Dann aber erinnert man sich, daß ja auch der Bahnhof selbst durchs Weltall rast und daß es sich auch um unsere zwei Raketen handeln könnte, und dann fällt uns die Entscheidung möglicherweise schon nicht mehr so leicht, wer von beiden denn nun recht hat.

**4.2.6.3 (Das Konzept einer absoluten Zeit muß aufgegeben werden).** Die „Re-



Dies Bild zeigt eine ruhende und eine bewegte „Lichtuhr“, bestehend aus zwei Spiegeln und einem Zähler, der zählt, wie oft ein Lichtstrahl dazwischen hin- und hersaust. Offensichtlich scheint die bewegte Lichtuhr langsamer zu gehen als die

Zeit im Koordinatensystem der ruhenden Lichtuhr. Hier müssen wir uns denken, daß im ruhenden Koordinatensystem ganz viele Lichtuhren aufgestellt und synchronisiert wurden wie oben schematisch dargestellt. Der Beobachter im bewegten System wird jedoch einwenden, daß von seinem Gesichtspunkt aus

diese ganzen Uhren keineswegs synchron gehen.

lativitätstheorie“ löst diesen Widerspruch wie folgt auf: Beide haben recht und wir müssen unsere Vorstellung von einer „absoluten Zeit“ aufgeben. Was für den einen Beobachter gleichzeitig ist, ist es für den anderen noch lange nicht! Präziser modelliert man in der Relativitätstheorie Raum und Zeit gemeinsam als eine Menge von „Raum-Zeit-Punkten“ oder „Ereignissen“. Das Aufleuchten eines Vorderlichts unseres Zuges etwa wäre solch ein Ereignis, oder auch das Aufleuchten eines Rücklichts. Jeder unserer beiden Beobachter ordnet jedem derartigen Ereignis in einer Weise, die wir noch ausführlich diskutieren werden, vier reelle Zahlen zu: Drei Raumkoordinaten und eine Zeitkoordinate. Und in unserem speziellen Fall würde eben der Schaffner den beiden fraglichen Aufleucht-Ereignissen dieselbe Zeitkoordinate zuordnen, der Bahnhofsvorsteher dahingegen verschiedene Zeitkoordinaten.

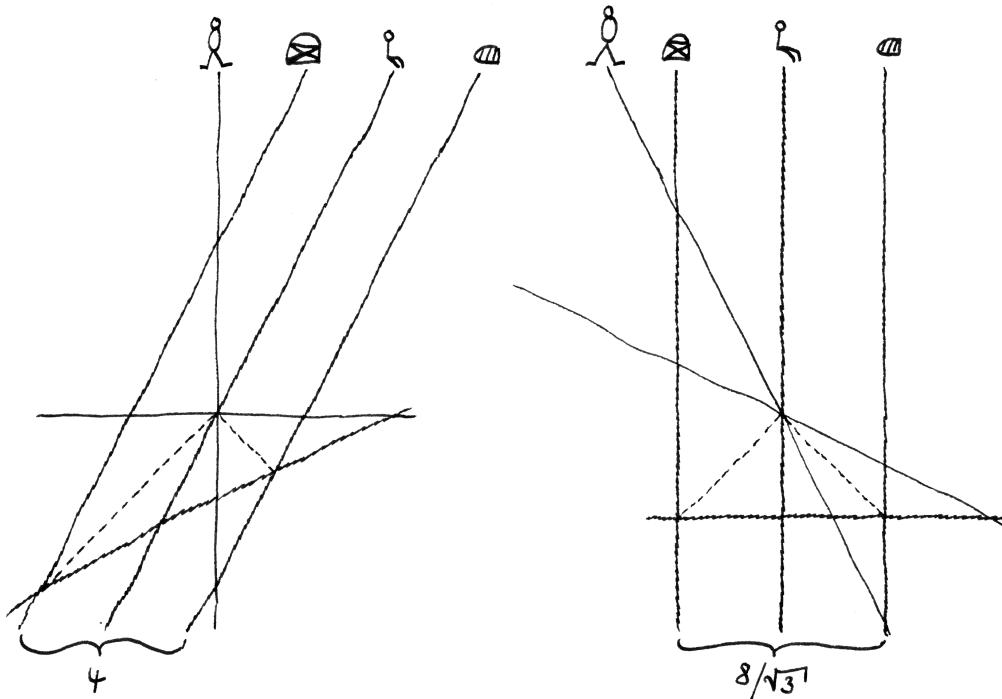
**4.2.6.4 (Längenkontraktion).** Das hat hinwiederum auch für die Längenmessung Konsequenzen: Der Bahnhofsvorsteher würde ja wohl vernünftigerweise die Länge des Zuges erklären, indem er gleichzeitig in seinem Sinne die Ortskoordinaten von Lokomotive und Schlußwagen bestimmt und die Differenz bildet. Er wird dabei eine kürzere Länge erhalten als der Schaffner, der seinerseits behaupten würde, der Bahnhofsvorsteher habe etwas früher den Ort der Lokomotive bestimmt und erst etwas später den Ort des Schlußwagens. Wie ist es aber nun um die Breite des Zuges bestellt? Nun, beide messen in der Tat dieselbe Breite für unseren Zug, was die absonderliche Konsequenz hat, daß der Bahnhofsvorsteher mit vollem Recht behaupten wird, ein Zollstock, mit dem der Schaffner die Breite des Zuges gemessen hat, verkürze sich, wenn der Schaffner ihn nun in Richtung des Zuges dreht, um damit die Länge des Zuges auszumessen. Man mache sich jedoch auch bewußt, daß ein Zollstock ja genau genommen aus einer großen Menge von Atomen besteht, deren wechselseitige Position durch elektromagnetische Kräfte bestimmt wird, also in gewisser Weise durch den Austausch von Lichtsignalen. Nach diesen informellen Vorüberlegungen beginnen wir nun mit der präzisen Formulierung,

**4.2.6.5.** In der **Relativitätstheorie** modelliert man Raum und Zeit zusammen als eine Menge

$$X$$

Deren Elemente heißen **Raum-Zeit-Punkte** oder auch **Ereignisse**. Die Menge  $X$  selbst nennt man die **Raumzeit**. Die Bewegung einer Fliege etwa wird durch eine Teilmenge von  $X$  beschrieben. Ort und Zeit einer Klausur wird beschrieben durch ein Element von  $X$  oder, da eine Klausur ja eine Weile dauert und in einem nicht ganz kleinen Hörsaal stattfindet, vielleicht auch eher durch eine Teilmenge von  $X$ . Die Ausbreitung des Lichts modellieren wir durch eine Teilmenge

$$\mathcal{L}^+ \subset X^2$$



Diese Bilder stellen die Sichtweisen des Bahnhofsvorsteher und des Schaffners in 4.2.6.3 dar. Beide benutzen Einheiten, in denen die Lichtgeschwindigkeit Eins ist. Die Lichtbewegung ist jeweils gestrichelt eingetragen. Im linken Schaubild hat der Bahnhofsvorsteher Ort gegen Zeit aufgetragen von Rücklicht, Schaffner und Vorderlicht, wobei seine Zeitachse senkrecht nach oben zeigt und seine Ortsachse waagerecht nach rechts. Der Zug fährt halbe Lichtgeschwindigkeit, und die Zackenlinie durch die beiden „Lampen-gehen-an-Punkte“ besteht aus Ereignissen, denen der Schaffner allen dieselbe Zeitkoordinate geben würde, sagen wir die Zeitkoordinate Null. Das rechte Schaubild hat der Schaffner gezeichnet. Beide wählen ihre Orts- und Zeitkoordinaten  $(x(p), t(p)) \in \mathbb{R}^2$  für den Bahnhofsvorsteher beziehungsweise  $(x'(p), t'(p)) \in \mathbb{R}^2$  für den Schaffner eines Ereignisses  $p$  derart, daß für je zwei Ereignisse  $p, q$  gilt

$$(x(p) - x(q))^2 - (t(p) - t(q))^2 = (x'(p) - x'(q))^2 - (t'(p) - t'(q))^2$$

Sie finden so die Umrechnung  $x' = (\sqrt{1 + b^2})x + bt$  und  $t' = bx + (\sqrt{1 + b^2})t + 4/\sqrt{3}$  mit  $b = -\sqrt{1/3}$ . Wie Sie sehen, scheint dem Schaffner sein Zug um den Faktor  $2/\sqrt{3}$  länger als dem Bahnhofsvorsteher.

Wir denken uns diese Teilmenge in der schmutzigen Anschauung als die Menge aller Paare von Raum-Zeit-Punkten  $(p, q) \in X^2$  derart, daß eine am Raum-Zeitpunkt  $p$  stattfindende Explosion am Raum-Zeitpunkt  $q$  gesehen würde. Wir sagen dann,  $q$  liege **kausal lichtartig zu**  $p$ . Um mathematische Präzision zu erreichen, vereinbaren wir explizit  $(p, p) \in \mathcal{L}^+ \forall p \in X$ .

4.2.6.6. In der **speziellen Relativitätstheorie** nimmt man zusätzlich an, daß  $X$  so mit der Struktur eines vierdimensionalen reellen affinen Raums versehen werden kann, daß die folgenden beiden Verträglichkeiten zwischen  $\mathcal{L}^+$  und dieser Struktur gelten: Erstens soll  $\mathcal{L}^+$  stabil sein unter der diagonalen Operation des Richtungsraums  $\vec{X}$  auf  $X^2$ . Liegt also  $q$  kausal lichtartig zu  $p$ , so soll auch  $q + v$  kausal lichtartig zu  $p + v$  liegen für jeden Richgungsvektor  $v \in \vec{X}$ . Und zweitens soll die Menge der **kausal lichtartigen Vektoren**

$$\vec{\mathcal{L}}^+ := \{v \in \vec{X} \mid (p, p + v) \in \mathcal{L}^+ \forall p \in X\}$$

die „Hälfte einer Quadrik vom Typ  $(1, 1, 1, -1)$ “ sein, es soll also in Formeln linear unabhängige Linearformen  $x, y, z, t : \vec{X} \rightarrow \mathbb{R}$  geben mit

$$\vec{\mathcal{L}}^+ = \{v \in \vec{X} \mid x(v)^2 + y(v)^2 + z(v)^2 - t(v)^2 = 0, t(v) \geq 0\}$$

Einen Vektor, der entweder selbst kausal lichtartig ist oder dessen Negatives kausal lichtartig ist, heißt **lichtartig**. Die Elemente der konvexen Hülle der Menge der kausal lichtartigen Vektoren nennt man dann **kausal**, ihre Negativen **antikausal**, die weder kausalen noch antikausalen Vektoren **raumartig** und die weder raumartigen noch lichtartigen Vektoren **zeitartig**. In unserer Terminologie ist also der Nullvektor weder raumartig noch zeitartig. Die Bezeichnung als „kausaler Vektor“ soll das fundamentale Postulat zum Ausdruck bringen, daß ein Ereignis nur Ereignisse beeinflussen kann, die von ihm aus durch die Addition derartiger Vektoren erreichbar sind, daß also „keine Wirkung schneller als mit Lichtgeschwindigkeit ausgeübt werden kann“.

## Übungen

*Übung 4.2.6.7 (Der Schaffner will den Zollstock in einen Gulli werfen).* Nehmen wir in 4.2.6.4 einmal an, der Zollstock des Schaffners sei etwas länger als der Durchmesser eines offenen Gullis auf dem Bahnhof. Der Schaffner streckt den Arm aus dem Fenster und läßt den Zollstock genau zum richtigen Zeitpunkt genau waagerecht runterfallen. Paßt er dann dank Längenkontraktion doch durch die Öffnung des Gullis, oder eben nicht? Wie beschreibt der Bahnhofsvorsteher, was er sieht?

### 4.2.7 Relativistische Längeneinheiten\*

4.2.7.1. Die Papierebene haben wir in 4.1.1.10 als Kongruenzebene durch die Angabe einer ausgezeichneten Gruppe von Kongruenzen modelliert und haben gesehen, wie dieses Datum eine euklidische Struktur 4.1.5.1 auf dem Richtungsraum liefert und damit nach 4.1.5.12 eine Gerade von Längeneinheiten. Für den Anschauungsraum der klassischen Mechanik kann man genauso vorgehen, vergleiche 4.1.6. Im Fall des Raumzeit gehen wir stattdessen davon aus, daß wir in ihrem Richtungsraum den Lichtkegel kennen, und zeigen im folgenden, wie man davon ausgehend eine „pseudoeuklidische Struktur“ erklären kann, aus der wir dann ein Gerade von „relativistischen Längeneinheiten“ konstruieren.

**Lemma 4.2.7.2 (Bestimmung quadratischer Formen aus ihren Nullstellen).**

*Haben zwei nichtausgeartete indefinite quadratische Formen auf einem endlichdimensionalen reellen Vektorraum dieselben Nullstellen, so sind sie linear abhängig alias gleich bis auf eine multiplikative Konstante.*

*Beweis.* Sicher reicht es zu zeigen, daß jede quadratische Form  $q : \mathbb{R}^n \rightarrow \mathbb{R}$ , die für  $0 < s < n$  auf der Nullstellenmenge  $\mathcal{L}$  des Polynoms  $x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_n^2$  verschwindet, ein skalares Vielfaches dieses Polynoms sein muß. Schränken wir unsere Form auf die Ebene ein, auf der alle Koordinaten außer  $x_1$  und  $x_n$  verschwinden, so wird sie nach 3.5.4.5 ein skalares Vielfaches von  $x_1^2 - x_n^2 = (x_1 + x_n)(x_1 - x_n)$ . Schränken wir unsere Form allgemeiner auf eine Ebene  $\{r\vec{v} + t\vec{w}\}$  ein mit  $\vec{v} \in \mathbb{R}^s \times 0$  und  $\vec{w} \in 0 \times \mathbb{R}^{n-s}$  Vektoren der euklidischen Norm  $\|\vec{v}\| = \|\vec{w}\| = 1$ , so gibt es aus demselben Grund  $a(\vec{v}, \vec{w}) \in \mathbb{R}^\times$  mit

$$q(r\vec{v} + t\vec{w}) = a(\vec{v}, \vec{w})(r^2 - t^2)$$

von  $r^2 - t^2 = (r + t)(r - t)$ . Auswerten auf  $\vec{v}$  zeigt  $a(\vec{v}, \vec{w}_1) = a(\vec{v}, \vec{w}_2)$  für alle  $\vec{w}_1, \vec{w}_2$  und Auswerten auf  $\vec{w}$  zeigt ebenso  $a(\vec{v}_1, \vec{w}) = a(\vec{v}_2, \vec{w})$  für alle  $\vec{v}_1, \vec{v}_2$ . Die Behauptung folgt.  $\square$

4.2.7.3. Unter einer **bilinearen Struktur** auf einem reellen Vektorraum  $V$  verstehen wir einen eindimensionalen Untervektorraum  $S \subset \text{Bil}(V)$  im Raum der Bilinearformen auf  $V$ . Ein **bilinear strukturierter Vektorraum** ist ein Paar  $(V, S)$  aus einem reellen Vektorraum mit einer bilinearen Struktur  $S$ . Den **Nullkegel** in einem strukturierten Vektorraum  $(V, S)$  erklären wir als die Menge aller Vektoren  $v \in V$  mit  $s(v, v) = 0 \forall s \in S$ . Eine lineare Abbildung  $f : V \rightarrow W$  von bilinear strukturierten Vektorräumen  $(V, S), (W, T)$  heißt **strukturverträglich**, wenn die Bilinearformen aus  $S$  genau die Rückzüge von Bilinearformen aus  $T$  sind. Einen strukturverträglichen Automorphismus eines bilinear strukturierten Vektorraums nennen wir eine **lineare Ähnlichkeitsabbildung**.

4.2.7.4. Eine bilineare Struktur  $S$ , deren von Null verschiedene Elemente nicht-ausgeartete symmetrische Bilinearformen sind, nennen wir eine **pseudoeuklidische Struktur**. Ist auf dem eindimensionalen Raum  $S$  zusätzlich eine Orientierung ausgezeichnet, reden wir von einer **orientiert pseudoeuklidischen Struktur**. Gegeben eine pseudoeuklidische Struktur  $S$ , deren von Null verschiedene Elemente einen Typ  $(m, n)$  haben mit  $m \neq n$ , erklären wir ihre **Standardorientierung** als diejenige Orientierung von  $S$ , die die Formen mit  $m > n$  als positiv orientiert auszeichnet.

*Beispiel 4.2.7.5.* Der Richtungsraum der „Raumzeit der speziellen Relativitätstheorie“ trägt eine nach 4.2.7.2 durch den Lichtkegel wohlbestimmte pseudoeuklidische Struktur  $S$ . Gegeben  $s \in S$  vom Typ  $(3, 1)$  gilt für einen Richtungsvektor  $v$  ganz allgemein

$$\begin{aligned} s(v, v) > 0 &\Leftrightarrow v \text{ ist raumartig} \\ s(v, v) = 0 &\Leftrightarrow v \text{ ist lichtartig} \\ s(v, v) < 0 &\Leftrightarrow v \text{ ist zeitartig} \end{aligned}$$

4.2.7.6. Gegeben ein bilinear strukturierter Vektorraum  $(V, S)$  erklären wir seine **Längengerade**  $\mathbb{L} = \mathbb{L}(V, S)$  wie im euklidischen Fall als die Betragswurzel 4.1.5.10 aus dem Dualraum von  $S$ , in Formeln

$$\mathbb{L}(V, S) := \sqrt{|S^\top|}$$

Die Längengerade ist also ein orientierter eindimensionaler reeller Vektorraum. Wie im euklidischen Fall erklären wir die **Länge**

$$\|\cdot\| : V \rightarrow \mathbb{L}$$

durch die Vorschrift  $\|v\| := \sqrt{|\lambda_v|}$  für  $\lambda_v : S \rightarrow \mathbb{R}$  gegeben durch  $s \mapsto s(v, v)$  und haben  $\|\alpha v\| = |\alpha| \|v\| \quad \forall \alpha \in \mathbb{R}$ . Für jede strukturverträgliche Abbildung  $f : V \rightarrow W$  von bilinear strukturierten Vektorräumen gibt es genau eine lineare Abbildung  $\mathbb{L}(f) : \mathbb{L}(V) \rightarrow \mathbb{L}(W)$  mit  $\|v\| \mapsto \|f(v)\| \quad \forall v \in V$ .

*Beispiel 4.2.7.7.* Die positiven Elemente der Längengerade des Richtungsraums der Raumzeit der speziellen Relativitätstheorie heißen **relativistische Zeiteinheiten** oder gleichbedeutend **relativistische Längeneinheiten**.

4.2.7.8. Einen linearen Automorphismus eines bilinear strukturierten Vektorraums  $(V, S)$  nennen wir **orthogonal**, wenn er jede Bilinearform  $s \in S$  erhält. Die Gruppe aller orthogonalen Automorphismen eines von  $(V, S)$  nennen wir seine **orthogonale Gruppe** und notieren sie

$$\mathrm{O}(V) = \mathrm{O}(V, S)$$

Ist  $V$  darüber hinaus endlichdimensional, so erklären wir weiter seine **spezielle orthogonale Gruppe**

$$\mathrm{SO}(V) = \mathrm{SO}(V, S)$$

als die Untergruppe  $\mathrm{SO}(V) \subset \mathrm{O}(V)$  aller orientierungserhaltenden orthogonalen Automorphismen von  $V$ . Im Fall einer pseudoeuklidischen Struktur haben offensichtlich alle Elemente von  $\mathrm{O}(V)$  bereits die Determinante  $\pm 1$ .

4.2.7.9. Gegeben ein reeller affiner Raum  $E$  mit einer bilinearen Struktur auf seinem Richtungsraum nennen wir diejenigen Affinitäten, deren Richtungsanteil orthogonal ist, die **orthogonalen Affinitäten**. Die Gruppe aller orthogonalen Affinitäten notieren wir  $\mathrm{O}_{\mathrm{aff}}(E)$  und nennen sie die **orthogonalaffine Gruppe**. Diejenigen Affinitäten, deren Richtungsanteil eine lineare Ähnlichkeit ist, nennen wir **Ähnlichkeiten**. Die Gruppe der Ähnlichkeiten notieren wir  $\mathrm{GO}_{\mathrm{aff}}(E)$ .

### Übungen

*Übung 4.2.7.10.* Gegeben der Vektorraum  $V = \mathbb{R}^2$  mit der symmetrischen Bilinearform  $\langle(x_1, x_2), (y_1, y_2)\rangle = x_1y_2 + x_2y_1$  zeige man, daß die orthogonale Gruppe  $\mathrm{O}(V)$  beschrieben werden kann als

$$\mathrm{O}(V) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix} \mid a \in \mathbb{R}^\times \right\}$$

Man verwendet vielfach die Notation  $\mathbb{R}^{p+q}$  für den Vektorraum  $\mathbb{R}^{p+q}$  mit der symmetrischen Bilinearform zur Fundamentalmatrix  $\mathrm{diag}(\mathrm{I}_p, -\mathrm{I}_q)$  und die Notation  $\mathrm{O}(p, q) := \mathrm{O}(\mathbb{R}^{p+q})$ . Man zeige, daß die eben beschriebene Gruppe  $\mathrm{O}(V)$  isomorph ist zu  $\mathrm{O}(1, 1)$ . Man mag die ersten Elemente oben „hyperbolische Rotationen“ nennen und die letzteren Elemente „hyperbolische Spiegelungen“.

### 4.2.8 Affine Struktur durch Lichtkegel\*

**Satz 4.2.8.1 (Alexandroff).** Auf einer Menge  $X$  mit einer Relation  $\mathcal{L}^+ \subset X^2$  existiert höchstens eine Struktur als reeller affiner Raum der Dimension  $\dim_{\mathbb{R}} X = 4$  derart, daß es linear unabhängige Linearformen  $x, y, z, t$  auf dem zugehörigen Richtungsraum  $\vec{X}$  gibt mit

$$\mathcal{L}^+ = \{(p, p+v) \mid v \in \vec{X} \text{ mit } x(v)^2 + y(v)^2 + z(v)^2 - t(v)^2 = 0 \text{ und } t(v) \geq 0\}$$

*Beweis.* Das folgt unmittelbar aus der anschließenden Proposition 4.2.8.3.  $\square$

4.2.8.2. Dieser Satz sagt uns, daß in der speziellen Relativitätstheorie die Struktur der Raumzeit als reeller affiner Raum bereits durch die Vorgabe der Lichtkegel eindeutig bestimmt ist. Eine analoge Aussage für die klassische Mechanik ist Satz 3.3.3.1, nach dem die Struktur des Raums der klassischen Mechanik als reeller affiner Raum bereits durch die Vorgabe der Sichtlinien eindeutig bestimmt ist.

**Proposition 4.2.8.3.** *Man betrachte auf  $X := \mathbb{R}^4$  die Relation*

$$\mathcal{L}^+ := \{(p, p + (x, y, z, t)^\top) \in X^2 \mid x^2 + y^2 + z^2 - t^2 = 0, t \geq 0\}$$

*Alle Bijektionen  $\phi : X \xrightarrow{\sim} X$ , die diese Relation festhalten, die also in Formeln die Eigenschaft  $(\phi \times \phi)(\mathcal{L}^+) = \mathcal{L}^+$  haben, sind affin.*

*Beweis.* Wir gehen in mehreren Schritten vor.

1. Geraden mit lichtartigem Richtungsvektor können allein mithilfe der Daten  $(X, \mathcal{L}^+)$  beschrieben werden als die maximalen Teilmengen  $L \subset X$  mit der Eigenschaft, daß für alle  $p, q \in L$  gilt  $(p, q) \in \mathcal{L}^+$  oder  $(q, p) \in \mathcal{L}^+$ . Unsere Bijektion  $\phi$  überführt folglich Geraden mit lichtartigem Richtungsvektor in ebensolche.
2. Gegeben ein Ereignis  $p \in X$  bezeichne  $\mathcal{L}_p^+ := \{x \in X \mid (p, x) \in \mathcal{L}^+\}$  den „vom Ereignis  $p$  ausgehenden Lichtkegel“ und  $\mathcal{L}_p^- := \{x \in X \mid (x, p) \in \mathcal{L}^+\}$  den „beim Ereignis  $p$  endenden inversen Lichtkegel“ und

$$\mathcal{L}_p := \mathcal{L}_p^+ \cup \mathcal{L}_p^-$$

den „beidseitigen Lichtkegel zu  $p$ “. Von einem Punkt  $p$  ausgehende Lichtstrahlen können allein mithilfe der Daten  $(X, \mathcal{L}^+)$  beschrieben werden als Schnitte des von  $p$  ausgehenden Lichtkegels mit durch  $p$  laufenden Geraden mit lichtartigem Richtungsvektor. Bei einem Punkt  $p$  ankommende Lichtstrahlen können ebenso allein mithilfe der Daten  $(X, \mathcal{L}^+)$  beschrieben werden als Schnitte des bei  $p$  endenden inversen Lichtkegels mit durch  $p$  laufenden Geraden mit lichtartigem Richtungsvektor.

3. Auf der Raumzeit  $X$  betrachten wir die kleinste transitive und reflexive Relation  $\mathcal{K}^+$  im Sinne von ??, die die Relation  $\mathcal{L}^+$  umfaßt. Explizit haben wir also  $(p, q) \in \mathcal{K}^+$  genau dann, wenn es eine Sequenz  $p = p_0, p_1, \dots, p_n = q$  von Ereignissen gibt mit  $(p_{i-1}, p_i) \in \mathcal{L}^+$  für  $i = 1, \dots, n$ . Es scheint mir klar, daß  $(p, q) \in \mathcal{K}^+$  gleichbedeutend ist dazu, daß  $q - p$  kausal ist. Wann also  $q$  kausal zu  $p$  liegt oder umgekehrt, ist auch bereits durch die Daten  $(X, \mathcal{L}^+)$  festgelegt. Wann weder das eine noch das andere gilt, wann also  $p$  raumartig zu  $q$  liegt, ist mithin auch bereits durch die Daten  $(X, \mathcal{L}^+)$  festgelegt.

4. Wir zeigen nun, daß auch Geraden mit raumartigem Richtungsvektor allein mithilfe der Daten  $(X, \mathcal{L}^+)$  beschrieben werden können. Gegeben zwei verschiedene Punkte  $p, q \in X$  mit raumartigem Verbindungsvektor  $q - p$  setzen wir dazu

$$N(p, q) := \{r \in X \mid \mathcal{L}_p \cap \mathcal{L}_q \cap \mathcal{L}_r = \emptyset\}$$

In der anschließenden Bemerkung 4.2.8.4 geben wir eine explizite Beschreibung dieser Menge  $N(p, q)$ . Sie zeigt, daß ein Punkt  $r \in X \setminus \{p, q\}$  genau dann auf

der Geraden durch  $p$  und  $q$  liegt, wenn gilt  $r \in N(p, q)$  und wenn es zusätzlich weder einen von  $r$  ausgehenden noch einen bei  $r$  ankommenden Lichtstrahl gibt, der ganz in  $N(p, q)$  enthalten ist. Das zeigt, daß auch Geraden mit raumartigem Richtungsvektor allein mithilfe der Daten  $(X, \mathcal{L}^+)$  beschrieben werden können.

5. Zu je zwei Geraden mit raumartigem Richtungsvektor, die sich in genau einem Punkt  $p$  treffen, bildet nun die Vereinigung aller raumartigen Geraden, die unsere beiden vorgegebenen Geraden in verschiedenen Punkten treffen, zusammen mit  $p$  eine affine Ebene in  $X$ , und wir erhalten so alle affinen Ebenen in  $X$ . Also macht unsere Bijektion  $\phi$  affine Ebenen zu affinen Ebenen und damit beliebige affine Geraden alias Schnitte verschiedener affiner Ebenen mit mindestens zwei Punkten zu affinen Geraden. Dann aber muß unsere Abbildung nach 3.3.3.1 bereits affin sein.  $\square$

4.2.8.4. Hier holen wir die explizite Beschreibung der Menge  $N(p, q)$  nach, die im vorhergehenden Beweis benötigt wurde. Gegeben  $r \in X \setminus \{p, q\}$  sind wir in genau einem der folgenden Fälle:

1.  $r$  liegt auf einer Gerade mit  $p$  und  $q$ . Dann gilt offensichtlich  $r \in N(p, q)$ ;
2.  $r$  spannt mit  $p$  und  $q$  eine affine Ebene auf, deren von Null verschiedene Richtungsvektoren sämtlich raumartig sind. Dann gilt offensichtlich  $r \notin N(p, q)$ ;
3.  $r$  spannt mit  $p$  und  $q$  eine affine Ebene auf, auf deren Richtungsraum unsere Bilinearform ausgeartet ist. Für derartige  $r$  gilt  $r \in N(p, q) \Leftrightarrow r \in \mathcal{L}_p \cup \mathcal{L}_q$ . Um das zu sehen, müssen wir etwas rechnen. Da unsere Fragestellung unter Streckungen invariant ist, dürfen wir nach der Variante 4.2.4.4 des Satzes von Witt ohne Beschränkung der Allgemeinheit  $p = (0, 0, 0, 0)$ ,  $q = (2, 0, 0, 0)$  und  $r = (x, 0, t, t)$  annehmen mit  $t \neq 0$ . Dann ist  $r \in N(p, q)$  gleichbedeutend zur Unlösbarkeit des Gleichungssystems

$$\begin{aligned}\lambda^2 + \mu^2 + \nu^2 - \tau^2 &= 0 \\ (\lambda - 2)^2 + \mu^2 + \nu^2 - \tau^2 &= 0 \\ (\lambda - x)^2 + \mu^2 + (\nu - t)^2 - (\tau - t)^2 &= 0\end{aligned}$$

Durch Subtraktion der obersten Gleichung von den beiden anderen erhalten wir das äquivalente System

$$\begin{aligned}\lambda^2 + \mu^2 + \nu^2 - \tau^2 &= 0 \\ \lambda &= 1 \\ x^2 - 2\lambda x + t^2 - 2\nu t - t^2 + 2\tau t &= 0\end{aligned}$$

und weiter das äquivalente System

$$\begin{aligned}1 + \mu^2 + (\nu + \tau)(\nu - \tau) &= 0 \\ x^2 - 2x &= 2t(\nu - \tau)\end{aligned}$$

und schließlich das äquivalente System

$$1 + \mu^2 + (\nu + \tau)(x^2 - 2x)/2t = 0$$

Dies System aber ist unlösbar für  $x^2 - 2x = 0$  und lösbar sonst, was genau unserer Behauptung entspricht.

4.  $r$  spannt mit  $p$  und  $q$  eine affine Ebene auf, auf deren Richtungsraum unsere Bilinearform indefinit ist. In diesem Fall zeigen wir

$$r \in N(p, q) \Leftrightarrow \begin{aligned} r &\text{ liegt raumartig zum einen und kausal oder} \\ &\text{antikausal zum anderen unserer beiden Punkte } p, q, \\ &\text{liegt jedoch mit keinem der beiden auf einer Lichtgerade.} \end{aligned}$$

Der Nachweis geschieht wieder durch Rechnung. Diesmal dürfen wir ohne Beschränkung der Allgemeinheit  $p = (0, 0, 0, 0)$ ,  $q = (2, 0, 0, 0)$  und  $r = (x, 0, 0, t)$  mit  $t \neq 0$  annehmen. Dann ist  $r \in N(p, q)$  äquivalent zur Unlösbarkeit des Gleichungssystems

$$\begin{aligned} \lambda^2 + \mu^2 + \nu^2 - \tau^2 &= 0 \\ (\lambda - 2)^2 + \mu^2 + \nu^2 - \tau^2 &= 0 \\ (\lambda - x)^2 + \mu^2 + \nu^2 - (\tau - t)^2 &= 0 \end{aligned}$$

Wie zuvor gelangen wir durch Subtraktion der ersten Gleichungen von den anderen zum äquivalenten Gleichungssystem

$$\begin{aligned} 1 + \mu^2 + \nu^2 - \tau^2 &= 0 \\ x^2 - 2x + 2\tau t - t^2 &= 0 \end{aligned}$$

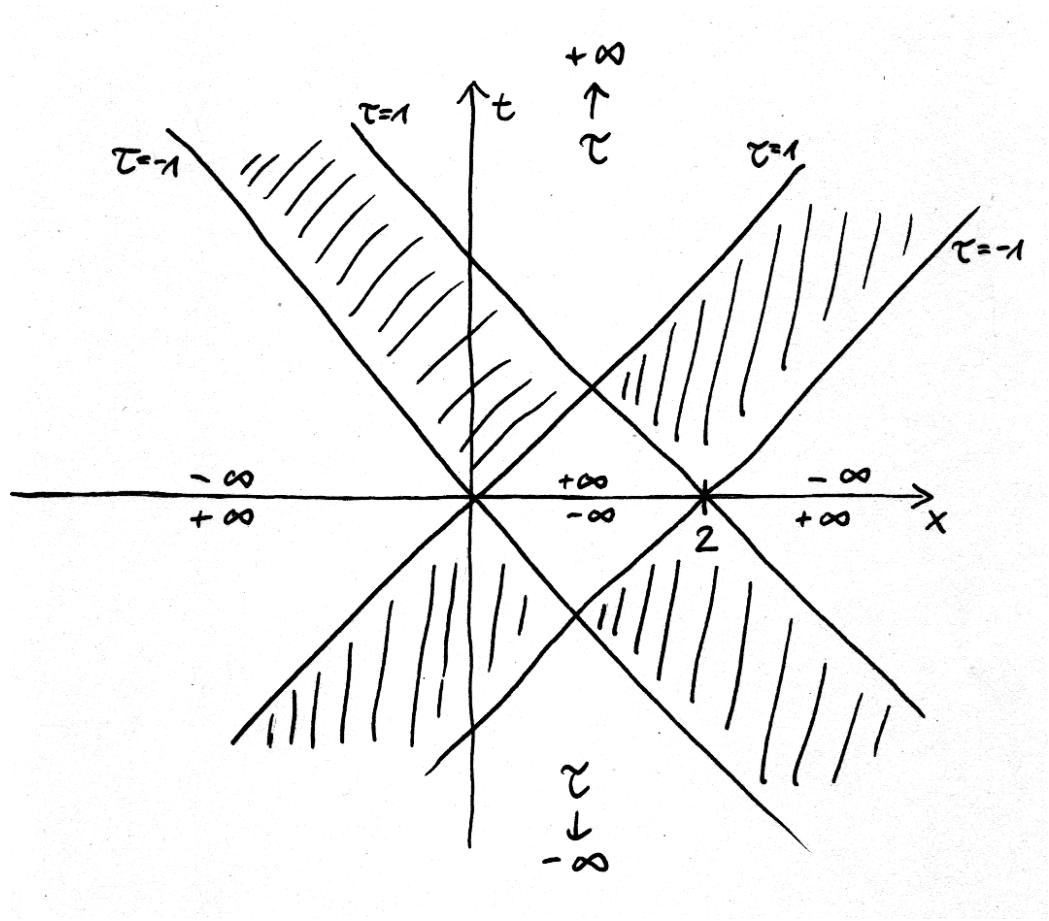
Die zweite Gleichung liefert  $\tau = (t^2 + 2x - x^2)/2t$  und das System ist genau dann lösbar wenn für dies  $\tau = \tau(x, t)$  gilt  $\tau^2 \geq 1$ . Suchen wir die  $(x, t) \in \mathbb{R}^2$  mit  $t \neq 0$  und  $\tau(x, t) = 1$ , so ergibt sich

$$2(t - x) = (t - x)(t + x)$$

alias  $t = x$  oder  $t = 2 - x$ . Suchen wir die  $(x, t) \in \mathbb{R}^2$  mit  $t \neq 0$  und  $\tau(x, t) = -1$ , so ergibt sich analog

$$-2(t + x) = (t - x)(t + x)$$

alias  $t = -x$  oder  $t = x - 2$ . Wir erhalten auf diese Weise nebenstehendes Bild für die Stellen, an denen  $\tau$  den Wert Eins beziehungsweise Minus Eins annimmt. Es folgt, daß  $\tau^2$  in den offenen schraffierten Bereichen kleiner ist als Eins, so daß wir dort keine Lösungen haben. Ebenso folgt, daß  $\tau^2$  in allen übrigen Bereichen größer als Eins ist, so daß wir dort Lösungen haben. Keine Lösungen finden wir also genau dann, wenn  $r$  strikt raumartig zu einem unserer Punkte  $p, q$  und strikt zeitartig zum anderen liegt.



BlahBlah

## 4.3 Hauptaumzerlegung und Jordanzerlegung

### 4.3.1 Motivation durch Differentialgleichungen\*

4.3.1.1. Wie in ?? im Reellen und beim Beweis von ?? im Komplexen besprochen wird, erklärt man die Exponentialabbildung auf komplexen quadratischen Matrizen durch die Exponentialreihe

$$\begin{aligned}\exp : \text{Mat}(n; \mathbb{C}) &\rightarrow \text{Mat}(n; \mathbb{C}) \\ A &\mapsto \sum_{k=0}^{\infty} \frac{1}{k!} A^k\end{aligned}$$

Wie dort besprochen wird, spielt diese Abbildung eine zentrale Rolle bei der Lösung von Systemen linearer Differentialgleichungen mit konstanten Koeffizienten. Ist genauer  $A \in \text{Mat}(n; \mathbb{C})$  eine quadratische Matrix und  $c \in \mathbb{C}^n$  ein Spaltenvektor, so gibt es genau eine differenzierbare Abbildung  $\gamma : \mathbb{R} \rightarrow \mathbb{C}^n$  mit Anfangswert  $\gamma(0) = c$  und  $\dot{\gamma}(t) = A\gamma(t)$  für alle  $t \in \mathbb{R}$ , nämlich die Abbildung

$$\gamma(t) = \exp(tA)c$$

Fast noch grundlegender zeigen wir in ??, und diesen Beweis könnten Sie mit den Kenntnissen von Analysis 2 auch jetzt schon verstehen, daß jeder stetige Gruppenhomomorphismus  $\varphi : \mathbb{R} \rightarrow \text{GL}(V)$  in die Automorphismengruppe eines endlichdimensionalen reellen oder komplexen Vektorraums  $V$  die Gestalt  $\varphi(t) = \exp(tA)$  hat für genau ein  $A \in \text{End } V$ . Es ist also wichtig, die Exponentialabbildung für Matrizen  $A \mapsto \exp A$  zu verstehen.

4.3.1.2. Um die Exponentialabbildung für Matrizen  $A \mapsto \exp A$  zu verstehen bemerkst man zunächst die Formel  $\exp(PAP^{-1}) = P(\exp A)P^{-1}$  für invertierbares  $P$ . Sie folgt direkt aus der Definition. Des weiteren erklären wir in ??, warum für kommutierende quadratische Matrizen  $A, B$  stets gilt

$$\exp(A + B) = (\exp A)(\exp B)$$

In 4.3.3.1 werden wir im folgenden die „Jordan-Zerlegung“ herleiten, nach der sich jede komplexe quadratische Matrix  $A$  auf genau eine Weise zerlegen lässt als eine Summe  $A = D + N$  mit  $D$  diagonalisierbar und  $N$  nilpotent und  $DN = ND$ . Ist zusätzlich  $P$  invertierbar mit  $PDP^{-1} = \text{diag}(\lambda_1, \dots, \lambda_n)$ , so folgt

$$\begin{aligned}\exp A &= (\exp D)(\exp N) \\ &= P^{-1} \exp(\text{diag}(\lambda_1, \dots, \lambda_n)) P \exp N \\ &= P^{-1} \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P \exp N \\ \exp tA &= P^{-1} \text{diag}(e^{t\lambda_1}, \dots, e^{t\lambda_n}) P \exp tN\end{aligned}$$

Hierbei bricht die Reihe für  $\exp tN$  ab und wir erhalten so ein recht befriedigendes qualitatives Bild und mit der „Jordan’schen Normalform“ 4.3.4.5 und etwas mehr Rechnen auch eine sehr explizite Beschreibung der Lösungen unserer Differentialgleichung  $\dot{\gamma}(t) = A\gamma(t)$  und für stetige Gruppenhomomorphismen  $\mathbb{R} \rightarrow \mathrm{GL}(n; \mathbb{C})$ .

## Übungen

*Ergänzende Übung 4.3.1.3.* Die Exponentialabbildung von reellen Matrizen liefert eine Bijektion

$$\exp : \{\text{symmetrische Matrizen}\} \xrightarrow{\sim} \{\text{positiv definite symmetrische Matrizen}\}$$

### 4.3.2 Hauptraumzerlegung

**Definition 4.3.2.1.** Gegeben ein Endomorphismus  $f : V \rightarrow V$  eines Vektorraums  $V$  und ein Skalar  $\lambda$  aus dem Grundkörper  $K$  erklären wir den **Eigenraum von  $f$  zum Eigenwert  $\lambda$**  durch

$$\mathrm{Eig}(f; \lambda) = \mathrm{Eig}(f|V; \lambda) := \{v \in V \mid f(v) = \lambda v\} = \ker(f - \lambda \mathrm{id})$$

und den **Hauptraum von  $f$  zum Eigenwert  $\lambda$**  durch

$$\mathrm{Hau}(f; \lambda) = \mathrm{Hau}(f|V; \lambda) := \bigcup_{n \geq 0} \ker(f - \lambda \mathrm{id})^n$$

Der Eigenraum zum Eigenwert  $\lambda$  besteht also aus allen Eigenvektoren zum Eigenwert  $\lambda$  und dem Nullvektor. Die Elemente des Hauptraums zum Eigenwert  $\lambda$  heißen die **Hauptvektoren zum Eigenwert  $\lambda$** . Der Nullvektor ist insbesondere ein Hauptvektor zu jedem Eigenwert. Ist  $\lambda \in K$  kein Eigenwert von  $f$ , so haben wir  $\mathrm{Eig}(f; \lambda) = 0$  und offensichtlich oder nach 4.3.2.6 auch  $\mathrm{Hau}(f; \lambda) = 0$ .

**4.3.2.2 (Eigenräume zu den Eigenwerten Null und Eins).** Der Eigenraum zum Eigenwert Null einer linearen Abbildung  $f : V \rightarrow V$  ist ihr Kern

$$\mathrm{Eig}(f|V; 0) = \ker f$$

Der Eigenraum zum Eigenwert Eins einer linearen Abbildung  $f : V \rightarrow V$  besteht aus den Fixpunkten unserer Abbildung, in Formeln

$$\mathrm{Eig}(f|V; 1) = V^f$$

**Beispiel 4.3.2.3 (Hauptraum zum Eigenwert Null und Nilpotenz).** Der Hauptraum zum Eigenwert Null des durch Ableiten gegebenen Endomorphismus des Raums der Polynomfunktionen  $\partial : \mathbb{R}[t] \rightarrow \mathbb{R}[t]$  ist der ganze Raum, in Formeln  $\text{Hau}(\partial; 0) = \mathbb{R}[t]$ . Allgemeiner hat ein Endomorphismus  $f : V \rightarrow V$  eines Vektorraums die Eigenschaft  $\text{Hau}(f; 0) = V$  genau dann, wenn es für jeden Vektor  $v \in V$  ein  $n \in \mathbb{N}$  gibt mit  $f^n(v) = 0$ . Ein Endomorphismus  $f$  eines Vektorraums mit dieser Eigenschaft heißt **lokal nilpotent**. Der Hauptraum zum Eigenwert Null des durch Ableiten gegebenen Endomorphismus  $\partial : \mathcal{C}^\infty \rightarrow \mathcal{C}^\infty$  des Raums der glatten reellwertigen Funktionen  $\mathcal{C}^\infty := \mathcal{C}_\mathbb{R}^\infty(\mathbb{R})$  auf der reellen Zahlengeraden besteht aus den Polynomfunktionen, in Formeln

$$\text{Hau}(\partial|_{\mathcal{C}^\infty}; 0) = \mathbb{R}[t]$$

Präziser zeigt man in der Analysis, daß eine glatte Funktion  $\mathbb{R} \rightarrow \mathbb{R}$  genau dann durch ein Polynom vom Grad höchstens  $n$  dargestellt werden kann, wenn ihre  $(n + 1)$ -te Ableitung die Nullfunktion ist.

**Definition 4.3.2.4.** Gegeben eine Abbildung  $f : X \rightarrow X$  von einer Menge in sich selbst nennen wir eine Teilmenge  $Y \subset X$  **stabil unter**  $f$ , wenn gilt  $f(Y) \subset Y$  alias  $x \in Y \Rightarrow f(x) \in Y$ .

**4.3.2.5 (Stabilität der Haupt- und Eigenräume).** Gegeben ein Endomorphismus  $f : V \rightarrow V$  eines Vektorraums  $V$  sind alle seine Eigenräume und Haupträume Untervektorräume. Sie sind auch offensichtlich stabil unter unserem Endomorphismus  $f$ , ja sogar unter jedem Endomorphismus  $g : V \rightarrow V$ , der mit  $f$  kommutiert. Ist noch allgemeiner  $g : V \rightarrow W$  eine lineare Abbildung und sind  $x \in \text{End } V$  und  $y \in \text{End } W$  gegeben mit  $gx = yg$ , so gilt

$$g(\text{Eig}(x; \lambda)) \subset \text{Eig}(y; \lambda) \quad \text{und} \quad g(\text{Hau}(x; \lambda)) \subset \text{Hau}(y; \lambda).$$

**4.3.2.6 (Verschwinden von Haupt- und Eigenräumen).** Ist der Hauptraum zu einem Eigenwert  $\lambda$  nicht Null, so ist auch der zugehörige Eigenraum nicht Null. Ist in der Tat ein Vektor  $v \neq 0$  gegeben mit  $(f - \lambda \text{id})^n v = 0$  für ein  $n \in \mathbb{N}$ , so gibt es auch ein kleinstmögliches derartiges  $n \geq 1$ , und dann ist  $(f - \lambda \text{id})^{n-1} v$  ein Eigenvektor zum Eigenwert  $\lambda$ .

**Proposition 4.3.2.7 (Direktheit der Summe der Haupträume).** Gegeben ein Vektorraum  $V$  über einem Körper  $K$  und ein Endomorphismus  $f : V \rightarrow V$  von  $V$  und paarweise verschiedene Skalare  $\lambda_1, \dots, \lambda_r \in K$  liefern die Einbettungen der Haupträume eine Injektion

$$\text{Hau}(f; \lambda_1) \oplus \dots \oplus \text{Hau}(f; \lambda_r) \hookrightarrow V$$

*Vorschau 4.3.2.8.* In 4.7.8.8 will ich erklären, in welchem Sinne das sogar gilt, wenn wir alle Skalare  $\lambda \in K$  gleichzeitig betrachten.

*Beweis.* Wir beginnen mit einer Vorüberlegung und zeigen zunächst für  $\lambda \neq \mu$ , daß ein Hauptvektor  $v \neq 0$  zum Eigenwert  $\lambda$  nie ein Eigenvektor zum Eigenwert  $\mu$  sein kann. In der Tat hätten wir sonst für hinreichend großes  $n$  eine Identität der Gestalt

$$0 = (f - \lambda \text{id})^n(v) = (\mu - \lambda)^n(v)$$

und es folgte  $v = 0$ . In anderen Worten induziert  $(f - \mu \text{id})$  für  $\lambda \neq \mu$  eine Injektion

$$(f - \mu \text{id}) : \text{Hau}(f; \lambda) \hookrightarrow \text{Hau}(f; \lambda)$$

auf dem Hauptaum zu  $\lambda$ . Seien nun  $v_1, \dots, v_r$  Hauptvektoren zu paarweise verschiedenen Eigenwerten  $\lambda_1, \dots, \lambda_r$ . Es gilt zu zeigen, daß aus  $v_1 + \dots + v_r = 0$  folgt  $v_1 = \dots = v_r = 0$ . Sicher finden wir ein  $n \in \mathbb{N}$  mit  $(f - \lambda_i \text{id})^n v_i = 0$  für alle  $i$ . Wenden wir nun  $(f - \lambda_2 \text{id})^n \dots (f - \lambda_r \text{id})^n$  auf unsere Identität  $v_1 + \dots + v_r = 0$  an, so folgt bereits  $(f - \lambda_2 \text{id})^n \dots (f - \lambda_r \text{id})^n(v_1) = 0$  und damit nach unserer Vorüberlegung zu Injektionen auf Hauträumen  $v_1 = 0$ . Dasselbe Argument zeigt  $v_i = 0$  für alle  $i$ .  $\square$

*Beispiel 4.3.2.9 (Lineare Unabhängigkeit der Funktionen  $t^n e^{\lambda t}$ ).* Wir zeigen, daß im  $\mathbb{R}$ -Vektorraum  $\mathcal{C}^\infty := \mathcal{C}_\mathbb{R}^\infty(\mathbb{R})$  der glatten reellwertigen Funktionen die Funktionen  $t \mapsto t^n e^{\lambda t}$  eine linear unabhängige Familie  $(t^n e^{\lambda t})_{(n, \lambda) \in \mathbb{N} \times \mathbb{R}}$  bilden. In der Tat, betrachten wir den durch das Ableiten gegebenen Endomorphismus  $\partial : \mathcal{C}^\infty \rightarrow \mathcal{C}^\infty$ , so liegen alle  $t^n e^{\lambda t}$  für festes  $\lambda$  im  $\lambda$ -Hauptaum  $\text{Hau}(\partial; \lambda)$ . Wegen 4.3.2.7 reicht es also, für jedes feste  $\lambda$  die lineare Unabhängigkeit der  $t^n e^{\lambda t}$  zu zeigen. Diese folgt hinwiederum unmittelbar aus unserer Erkenntnis 3.5.3.19, daß ein reelles Polynom nur dann überall den Wert Null annimmt, wenn es das Nullpolynom ist. In derselben Weise zeigt man auch, daß im  $\mathbb{C}$ -Vektorraum  $\mathcal{C}^\infty(\mathbb{R})$  aller beliebig oft differenzierbaren Funktionen  $\mathbb{R} \rightarrow \mathbb{C}$  die Funktionen  $t \mapsto t^n e^{\lambda t}$  für komplexe  $\lambda$  eine linear unabhängige Familie  $(t^n e^{\lambda t})_{(n, \lambda) \in \mathbb{N} \times \mathbb{C}}$  bilden, vergleiche ??.

**Satz 4.3.2.10 (Fitting-Zerlegung).** Gegeben ein Endomorphismus eines endlich-dimensionalen Vektorraums besitzt der Hauptaum zum Eigenwert Null genau ein unter unserem Endomorphismus stabiles Komplement und die Restriktion unseres Endomorphismus auf dies Komplement ist ein Isomorphismus.

*Beweis.* Bezeichnet  $f : V \rightarrow V$  unseren Endomorphismus, so zeigen wir zunächst, daß für hinreichend großes  $n \gg 0$  unser Vektorraum  $V$  in die direkte Summe

$$(\ker f^n) \oplus (\text{im } f^n) \xrightarrow{\sim} V$$

zerfällt. Die Bilder der  $f^\nu$  bilden in der Tat für wachsendes  $\nu$  eine monoton fallende Folge von Untervektorräumen. Da  $V$  nach Annahme endliche Dimension hat, gibt es eine Stelle  $n$ , ab der diese Folge konstant wird. Für dieses  $n$  muß die Surjektion  $f^n : (\text{im } f^n) \rightarrow (\text{im } f^{2n})$  aus Dimensionsgründen ein Isomorphismus sein, also haben wir  $(\ker f^n) \cap (\text{im } f^n) = 0$ , und nochmaliger Dimensionsvergleich mit der Dimensionsformel 3.2.2.5 zeigt über 3.2.2.16 die behauptete Zerlegung. Sie heißt die **Fitting-Zerlegung**. Ab derselben Stelle  $n$  muß aus Dimensionsgründen auch die aufsteigende Folge der Untervektorräume  $(\ker f^\nu)$  stagnieren, so daß gilt  $(\ker f^n) = \text{Hau}(f; 0)$ . Ist schließlich  $W \subset V$  ein  $f$ -stabiler Teilraum mit  $W \cap (\ker f^n) = 0$ , so folgt  $f(W) = W$  und damit  $W \subset (\text{im } f^n)$ . Das zeigt die behauptete Eindeutigkeit.  $\square$

**Proposition 4.3.2.11 (Hauptraumdimension als Nullstellenordnung).** *Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums stimmt die Dimension jedes Hauptraums überein mit der Vielfachheit des entsprechenden Eigenwerts als Nullstelle des charakteristischen Polynoms.*

4.3.2.12. Man nennt diese Vielfachheit auch die **algebraische Vielfachheit** des Eigenwerts, im Gegensatz zu seiner **geometrischen Vielfachheit**, unter der man die Dimension des zugehörigen Eigenraums versteht.

*Beweis.* Sei  $f : V \rightarrow V$  unser Endomorphismus und  $\lambda$  ein Skalar. Die Fitting-Zerlegung zu  $(f - \lambda \text{id})$  zerlegt  $V$  in die direkte Summe des  $\lambda$ -Hauptraums und eines  $f$ -stabilen Komplements

$$V = \text{Hau}(f; \lambda) \oplus W$$

derart, daß  $\lambda$  kein Eigenwert von  $f : W \rightarrow W$  ist. Auf dem Hauptraum ist  $(f - \lambda \text{id})$  nilpotent. Nach 3.2.6.15 finden wir also darin eine Basis, bezüglich derer die Matrix von  $(f - \lambda \text{id})$  obere Dreiecksgestalt hat mit Nullen auf der Diagonalen. Bezüglich derselben Basis hat die Matrix von  $f$  obere Dreiecksgestalt mit lauter Einträgen  $\lambda$  auf der Diagonalen. Ergänzen wir diese Basis durch eine Basis des Komplements  $W$  zu einer Basis von  $V$ , so ist die zugehörige Matrix von  $f : V \rightarrow V$  blockdiagonal. Unsere Formel 3.6.6.10 für die Determinante einer blockdiagonalen Matrix liefert dann für das charakteristische Polynom die Darstellung

$$\chi_f(T) = (\lambda - T)^d \cdot \chi_{f|W}(T)$$

für  $d := \dim \text{Hau}(f; \lambda)$  die Dimension des  $\lambda$ -Hauptraums und  $\chi_{f|W}(T)$  ein Polynom ohne Nullstelle bei  $\lambda$ .  $\square$

**Satz 4.3.2.13 (Hauptraumzerlegung).** *Ein Vektorraum endlicher Dimension über einem algebraisch abgeschlossenen Körper zerfällt unter jedem Endomorphismus in die direkte Summe seiner Haupträume.*

4.3.2.14. Ist  $f : V \rightarrow V$  unser Endomorphismus und sind  $\lambda_1, \dots, \lambda_n$  seine Eigenwerte, so gilt also in Formeln  $\text{Hau}(f; \lambda_1) \oplus \dots \oplus \text{Hau}(f; \lambda_n) \xrightarrow{\sim} V$  unter der durch die Addition gegebenen Abbildung.

4.3.2.15. Der Satz gilt mit dem ersten Beweis auch, wenn wir statt der algebraischen Abgeschlossenheit des Grundkörpers nur voraussetzen, daß das charakteristische Polynom unseres Endomorphismus über unserem Körper vollständig in Linearfaktoren zerfällt.

*Erster Beweis.* Der Satz folgt mit der Direktheit der Summe der Haupträume 4.3.2.7 und Dimensionsvergleich unmittelbar aus Proposition 4.3.2.11, nach der die Dimensionen der Haupträume mit den Vielfachheiten der entsprechenden Eigenwerte als Nullstellen des charakteristischen Polynoms zusammenfallen.  $\square$

*Zweiter Beweis.* Gegeben ein Skalar  $\lambda$  zeigt die Fittingzerlegung, wenn wir sie auf  $(f - \lambda \text{id})$  anwenden, daß der Hauptraum  $\text{Hau}(f; \lambda)$  ein  $f$ -stabiles Komplement hat. Mit Induktion über die Dimension folgt, daß unser Vektorraum von seinen Haupträumen erzeugt wird. Die Direktheit der Summe der Haupträume kennen wir schon aus 4.3.2.7.  $\square$

## Übungen

*Ergänzende Übung 4.3.2.16.* Ein Vektorraum über einem algebraisch abgeschlossenen Körper zerfällt unter einem Endomorphismus in die direkte Summe seiner Haupträume genau dann, wenn unser Endomorphismus **lokal endlich** ist, als da heißt, jeder Vektor liegt in einem endlichdimensionalen unter unserem Endomorphismus stabilen Teilraum.

*Ergänzende Übung 4.3.2.17.* Gegeben ein diagonalisierbarer Endomorphismus  $f$  eines Vektorraums  $V$  und ein unter  $f$  stabiler Teilraum  $W \subset V$  gilt stets  $f(W) = W \cap f(V)$ . Man gebe auch ein Gegenbeispiel für allgemeines  $f$ .

*Ergänzende Übung 4.3.2.18 (Simultane Eigenvektoren).* Für jede Menge von paarweise kommutierenden trigonalisierbaren Endomorphismen eines von Null verschiedenen endlichdimensionalen Vektorraums gibt es mindestens einen simultanen Eigenvektor. Hinweis: 4.3.2.5

*Übung 4.3.2.19 (Spektralsatz für normale Endomorphismen).* Ein Endomorphismus eines Skalarproduktraums heißt **normal**, wenn er einen Adjungierten besitzt und mit seinem Adjungierten kommutiert. Man zeige: Ein Endomorphismus eines endlichdimensionalen komplexen Skalarproduktraums ist genau dann normal, wenn es dazu eine Orthonormalbasis aus Eigenvektoren gibt. Hinweis: Kommutierende Endomorphismen stabilisieren die Eigenräume aller beteiligten Endomorphismen. Ist  $A^*$  adjungiert zu  $A$ , so sind  $A + A^*$  und  $i(A - A^*)$  selbstadjungiert. Alternativer Zugang: Man beginne mit einem gemeinsamen Eigenvektor

von  $A$  und  $A^*$  und wiederhole von dort ausgehend den Beweis des Spektralsatzes für selbstadjungierte Endomorphismen.

*Ergänzende Übung 4.3.2.20.* Gegeben ein Vektorraum mit einem lokal endlichen Endomorphismus besitzt der Hauptraum zu Null stets genau ein unter besagtem Endomorphismus stabiles Komplement.

*Ergänzung 4.3.2.21 (Ein Nullhauptraum ohne stabiles Komplement).* Betrachten wir Vektorräume unendlicher Dimension, so besitzt der Hauptraum zum Eigenwert Null eines Endomorphismus im allgemeinen kein unter besagtem Endomorphismus stabiles Komplement mehr. Betrachten wir zum Beispiel den Vektorraum  $V$  aller Abbildungen von der Menge  $\{(i, j) \in \mathbb{N}^2 \mid i \geq j\}$  in unseren Grundkörper und den Endomorphismus, der „jede Zeile eins nach unten rückt und die unterste Zeile zu Null macht“. Der Hauptraum  $H$  zum Eigenwert Null besteht aus allen Funktionen, die nur auf endlich vielen Zeilen von Null verschieden sind. Nun betrachten wir den Vektor  $v \in V$  mit

$$v(i, j) = \begin{cases} 1 & i = 2j; \\ 0 & \text{sonst.} \end{cases}$$

Sein Bild ist im in 4.4.5.4 diskutierten Quotientenvektorraum  $\bar{v} \in V/H$  ein von Null verschiedener Vektor, der im Bild jeder Potenz unseres Endomorphismus liegt. In  $V$  selbst gibt es jedoch keinen derartigen von Null verschiedenen Vektor, folglich kann  $H \subset V$  kein unter unserem Endomorphismus stabiles Komplement besitzen.

### 4.3.3 Jordanzerlegung

**Satz 4.3.3.1 (Jordanzerlegung).** Seien  $V$  ein endlichdimensionaler Vektorraum über einem algebraisch abgeschlossenen Körper und  $x \in \text{End } V$  ein Endomorphismus von  $V$ . So gibt es genau eine Zerlegung  $x = x_s + x_n$  mit  $x_s$  diagonalisierbar,  $x_n$  nilpotent und  $x_s x_n = x_n x_s$ .

4.3.3.2. Statt den Grundkörper algebraisch abgeschlossen anzunehmen, reicht für die Gültigkeit unseres Satzes auch die Annahme aus, daß das charakteristische Polynom unseres Endomorphismus über unserem Körper vollständig in Linearfaktoren zerfällt. Der Beweis bleibt derselbe.

4.3.3.3. Daß der Endomorphismus jetzt plötzlich  $x$  heißt, obwohl er sonst immer  $f$  hieß, hat keine tieferen Gründe. Es hat jedoch den Vorteil, den Buchstaben  $f$  freizumachen für andere lineare Abbildungen.

4.3.3.4. Der untere Index  $s$  bei  $x_s$  steht für **semisimple**, die deutsche Übersetzung dafür ist **halbeinfach**. In der Situation des Satzes heißt  $x_s$  der **halbeinfache** und  $x_n$  der **nilpotente Anteil** von  $x$ . Die Zerlegung aus dem Satz bezeichnet man genauer auch als **additive Jordan-Zerlegung**, wenn man Verwechslungen mit der „multiplikativen Jordan-Zerlegung“ aus 4.3.3.20 befürchtet.

*Vorschau* 4.3.3.5. Ganz allgemein heißt ein Endomorphismus  $x$  eines  $k$ -Vektorraums  $V$  **halbeinfach**, wenn  $V$  mit der Struktur als  $k[T]$ -Modul, bei der die Variable  $T$  durch  $x$  operiert, halbeinfach ist im Sinne von ?? alias die Summe seiner einfachen Untermoduln. Mit den dort eingeführten Methoden zeigt man leicht, daß das gleichbedeutend dazu ist, daß unser Endomorphismus  $x$  „nach Erweiterung der Skalare zum algebraischen Abschluß“ diagonalisierbar ist. Ersetzen wir im Satz die Bedingung „diagonalisierbar“ durch die Bedingung „halbeinfach“, so bleibt er auch ohne alle Forderungen an das charakteristische Polynom gültig für im Sinne von ?? „vollkommene“ Grundkörper, wie Sie im Rahmen der sogenannten „Galoistheorie“ als Übung ?? zeigen mögen.

*Beweis.* Gegeben ein Endomorphismus  $x$  eines Vektorraums endlicher Dimension über einem algebraisch abgeschlossenen Körper erklären wir einen weiteren Endomorphismus  $x_s$  durch die Vorschrift, daß er auf dem Hauptaum  $\text{Hau}(x; \lambda)$  von  $x$  zum Eigenwert  $\lambda$  jeweils durch die Multiplikation mit  $\lambda$  operieren soll. Dann ist  $x_s$  diagonalisierbar, und setzen wir  $x_n = x - x_s$ , so ist  $x_n$  nilpotent und  $x_s$  kommutiert mit  $x$  und dann auch mit  $x_n$ . Das zeigt die Existenz unserer Zerlegung. Ist  $x = s + n$  eine weitere Zerlegung mit  $s$  diagonalisierbar,  $n$  nilpotent und  $sn = ns$ , so folgt zunächst  $sx = xs$  und dann, da  $s$  die Hauträume von  $x$  stabilisieren muß, auch  $sx_s = x_s s$ . So erkennen wir, daß  $x, s, n, x_s$  und  $x_n$  paarweise kommutieren. Natürlich ist dann  $x_n - n$  nilpotent. Da  $s$  die Hauträume von  $x$  stabilisiert und da nach 3.6.6.19 auch die Restriktion von  $s$  auf besagte Hauträume

diagonalisierbar ist, folgt aus der Definition von  $x_s$ , daß auch  $x_s - s$  diagonalisierbar sein muß. Aus  $x_n - n = s - x_s$  folgt dann aber sofort, daß beide Seiten Null sein müssen. Das zeigt die Eindeutigkeit unserer Zerlegung.  $\square$

*Ergänzung 4.3.3.6 (Halbeinfacher Anteil als Wert eines Polynoms).* In der Situation des Satzes lassen sich  $x_s$  und  $x_n$  sogar als Polynome in  $x$  ohne konstanten Term ausdrücken, als da heißt, es gibt  $P, Q \in T\mathbb{C}[T]$  mit  $x_s = P(x)$  und  $x_n = Q(x)$ . In der Tat, falls  $N$  so groß ist, daß gilt  $\text{Hau}(x; \lambda) = \ker(x - \lambda)^N$  für alle  $\lambda$ , so erhält man ein mögliches  $P$  aus dem chinesischen Restsatz ?? als simultane Lösung der Kongruenzen  $P \equiv \lambda \pmod{(T - \lambda)^N}$  für alle Eigenwerte  $\lambda$  von  $x$  und für  $\lambda = 0$ , und ein mögliches  $Q$  ist dann  $T - P(T)$ . Ich mag die in der Literatur übliche Argumentation mit diesen Polynomen nicht, sie sind mir zu willkürlich. Stattdessen ziehe ich die Argumentation mit der Funktionalität der Jordan-Zerlegung vor, die im Anschluß diskutiert wird.

**Satz 4.3.3.7 (Funktionalität der Jordan-Zerlegung).** *Gegeben eine lineare Abbildung von endlichdimensionalen Vektorräumen über einem algebraisch abgeschlossenen Körper  $f : V \rightarrow W$  und  $x \in \text{End } V$  sowie  $y \in \text{End } W$  Endomorphismen folgt aus  $fx = yf$  bereits  $fx_s = y_s f$  und  $fx_n = y_n f$ .*

*Beweis.* Aus  $fx = yf$  folgt zunächst  $f(\text{Hau}(x; \lambda)) \subset \text{Hau}(y; \lambda)$ . Nach der im Beweis von 4.3.3.1 gegebenen Beschreibung der Jordan-Zerlegung impliziert das unmittelbar  $fx_s = y_s f$  und dann auch  $fx_n = y_n f$ .  $\square$

4.3.3.8. Stabilisiert speziell ein Endomorphismus eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper einen vorgegebenen Teilraum, so stabilisieren nach 4.3.3.7 auch sein halbeinfacher und sein nilpotenter Anteil besagten Teilraum.

*Ergänzung 4.3.3.9.* Unsere Sätze über die Jordan-Zerlegung 4.3.3.1 und deren Funktionalität 4.3.3.7 gelten analog, wenn man statt der Endlichdimensionalität der darin auftauchenden Vektorräume nur fordert, daß die fraglichen Endomorphismen  $x$  und  $y$  im Sinne von 4.3.2.16 lokal endlich sein sollen, und von  $x_n$  und  $y_n$  schwächer nur fordert, daß sie im Sinne von 4.3.2.3 lokal nilpotent sein sollen.

## Übungen

*Übung 4.3.3.10.* Gegeben kommutierende Endomorphismen  $x, y$  eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper gilt  $(x + y)_s = x_s + y_s$  und  $(x + y)_n = x_n + y_n$ .

*Weiterführende Übung 4.3.3.11.* Gegeben  $x, y$  kommutierende lokal endliche Endomorphismen eines Vektorraums über einem algebraisch abgeschlossenen Körper. Ist auch  $x + y$  lokal endlich und es gilt  $(x + y)_s = x_s + y_s$  sowie  $(x + y)_n = x_n + y_n$ .

*Ergänzende Übung 4.3.3.12 (Operatornorm und Spektralradius).* Sei  $x$  ein Endomorphismus eines von Null verschiedenen endlichdimensionalen komplexen normierten Vektorraums  $V$  im Sinne von **??**. Bezeichne  $\|\cdot\|$  die zugehörige Operatornorm auf  $\text{End } V$  im Sinne von **??**. Man zeige, daß die Folge  $\sqrt[n]{\|x^n\|}$  für  $n \rightarrow \infty$  gegen das Maximum der Beträge der Eigenwerte alias den **Spektralradius** von  $x$  strebt. Hinweis: Zunächst folgere man aus **??**, daß der fragliche Grenzwert nicht von der auf unserem Vektorraum gewählten Norm abhängt. Dann behandle man den diagonalisierbaren Fall mithilfe der Maximumsnorm in Bezug auf eine geeignete Basis. Schließlich behandle man den allgemeinen Fall mithilfe der Jordan-Zerlegung und erinnere **??**.

*Ergänzende Übung 4.3.3.13 (Bilder halbeinfacher Anteile).* Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem algebraisch abgeschlossenen Körper und ein Endomorphismus  $x : V \rightarrow V$  haben wir stets

$$\text{im } x \supset \text{im } x_s$$

Hinweis: Das Bild von  $x_s$  ist genau die Summe der Hauträume zu von Null verschiedenen Eigenwerten und das Bild von  $x$  umfaßt offensichtlich diese Summe. Alternativ erkennt man  $\text{im } x \supset \text{im}(x_s^N)$  für hinreichend großes  $N$  durch Entwicklung von  $x_s^N = (x - x_n)^N$  nach der binomischen Formel und Ausklammern von  $x$ , und die Behauptung folgt wegen  $\text{im } x_s = \text{im } x_s^N$ .

*Ergänzende Übung 4.3.3.14 (Automorphismen der Ordnung Zwei).* Jeder Endomorphismus der Ordnung zwei eines Vektorraums über einem Körper einer von zwei verschiedenen Charakteristik ist diagonalisierbar. Hinweis: Später zeigen wir das als **??**. Jeder Endomorphismus der Ordnung vier eines komplexen Vektorraums ist diagonalisierbar. Hinweis: Man zerlege zunächst in Eigenräume unter dem Quadrat unseres Endomorphismus. Allgemeiner werden Sie in 4.3.3.15 zeigen, daß jeder Endomorphismus endlicher Ordnung eines komplexen Vektorraums diagonalisierbar ist.

*Ergänzende Übung 4.3.3.15 (Automorphismen endlicher Ordnung).* Sei  $K$  ein algebraisch abgeschlossener Körper der Charakteristik Null. Sei  $V$  ein  $K$ -Vektorraum und  $\varphi : V \rightarrow V$  ein Automorphismus „endlicher Ordnung“, als da heißt, es gebe  $n \geq 1$  mit  $\varphi^n = \text{id}$ . So ist  $V$  die direkte Summe der Eigenräume von  $\varphi$ . Allgemeiner zeige man das auch unter der schwächeren Voraussetzung, daß die Charakteristik kein Teiler der Ordnung  $n$  unseres Automorphismus ist. Hinweis: Man behandle zunächst den endlichdimensionalen Fall mithilfe der Jordan-Zerlegung und beachte dabei, daß nach 3.4.3.10 höhere Potenzen eines nilpotenten Endomorphismus stets größere Kerne haben müssen, solange nicht beide fraglichen Potenzen bereits Null sind. Fortgeschrittene erkennen einen Spezialfall des Satzes von Maschke **??**.

*Ergänzende Übung 4.3.3.16.* Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper besteht ein Hauptraum des transponierten Endomorphismus des Dualraums genau aus allen Linearformen, die auf allen Haupträumen zu anderen Eigenwerten des ursprünglichen Endomorphismus verschwinden.

*Ergänzung 4.3.3.17.* Ein Endomorphismus  $f$  eines Vektorraums heißt **unipotent**, wenn  $(f - \text{id})$  nilpotent ist. Ein Endomorphismus  $f$  eines Vektorraums heißt **lokal unipotent**, wenn  $(f - \text{id})$  lokal nilpotent ist. Oft wird aber hier das Wörtchen „lokal“ auch weggelassen.

*Ergänzende Übung 4.3.3.18.* Ein unipotenter Endomorphismus endlicher Ordnung eines Vektorraums über einem Körper der Charakteristik Null ist bereits die Identität. Hinweis: 4.3.3.15.

*Ergänzende Übung 4.3.3.19.* Das Produkt von zwei kommutierenden nilpotenten Endomorphismen ist nilpotent. Das Produkt von zwei kommutierenden unipotenten Endomorphismen ist unipotent. Das Produkt von zwei kommutierenden halbeinfachen Endomorphismen ist halbeinfach.

*Ergänzende Übung 4.3.3.20 (Multiplikative Jordan-Zerlegung).* Jeder Automorphismus  $x$  eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper lässt sich auf genau eine Weise darstellen als Produkt  $x = x_u x_s$  mit  $x_s$  halbeinfach alias „semisimple“ alias diagonalisierbar,  $x_u$  unipotent und  $x_u x_s = x_s x_u$ . Hinweis: Ist  $x = x_s + x_n$  die additive Jordan-Zerlegung, so betrachte man  $x = x_s(\text{id} + x_s^{-1}x_n)$ . Man zeige weiter, daß dieselbe Aussage auch für lokal endliche Automorphismen eines beliebigen Vektorraums gilt, diesmal mit  $x_u$  lokal unipotent, und zeige die zu 4.3.3.7 analogen Funktionalitätseigenschaften.

*Ergänzende Übung 4.3.3.21.* Gegeben ein Endomorphismus  $A$  eines endlichdimensionalen komplexen Vektorraums  $V$  liegt  $\mathbb{Z}$  im Kern des Gruppenhomomorphismus  $\varphi_A : \mathbb{R} \rightarrow \text{GL}(V)$  gegeben durch  $t \mapsto \exp(tA)$  genau dann, wenn  $A$  diagonalisierbar ist mit sämtlichen Eigenwerten aus  $2\pi i\mathbb{Z}$ . Weiter ist  $\varphi_A$  genau dann nicht injektiv, wenn  $A$  diagonalisierbar ist mit rein imaginären Eigenwerten, und wenn der von seinen Eigenwerten aufgespannte  $\mathbb{Q}$ -Vektorraum höchstens die Dimension Eins hat.

*Ergänzende Übung 4.3.3.22 (Schmelzfunktionalität der Jordanzerlegung).* Gegeben über einem algebraisch abgeschlossenen Körper eine multilinearare Abbildung  $\varphi : V_1 \times \dots \times V_r \rightarrow W$  sowie lokal endliche Endomorphismen  $x_i \in \text{End } V_i$  und  $y \in \text{End } W$  mit  $\varphi \circ (x_1 \times \dots \times x_r) = y \circ \varphi$  gilt auch

$$\varphi \circ ((x_1)_s \times \dots \times (x_r)_s) = y_s \circ \varphi$$

Das gilt sogar für  $r = 0$  und bedeutet in diesem Fall, daß für jeden Vektor  $w \in W$  gilt  $yw = w \Rightarrow y_s w = w$ .

### 4.3.4 Jordan'sche Normalform

**Definition 4.3.4.1.** Gegeben  $r \geq 1$  definieren wir eine  $(r \times r)$ -Matrix  $J(r)$ , genannt der **nilpotente Jordan-Block der Größe  $r$** , durch die Vorschrift  $J(r)_{i,j} = 1$  für  $j = i + 1$  und  $J(r)_{i,j} = 0$  sonst. Insbesondere ist also  $J(1)$  die  $(1 \times 1)$ -Matrix mit dem einzigen Eintrag Null.

**Satz 4.3.4.2 (Normalform nilpotenter Endomorphismen).** Gegeben ein nilpotenter Endomorphismus  $N$  eines endlichdimensionalen Vektorraums gibt es stets eine angeordnete Basis  $\mathcal{B}$  derart, daß die Matrix unseres Endomorphismus in dieser Basis blockdiagonal ist mit nilpotenten Jordanblöcken auf der Diagonalen, in Formeln

$$\mathcal{B}[N]_{\mathcal{B}} = \text{diag}(J(r_1), \dots, J(r_n))$$

Die positiven natürlichen Zahlen  $r_1, \dots, r_n$  sind hierbei durch unseren nilpotenten Endomorphismus eindeutig bestimmt bis auf Reihenfolge.

*Ergänzung 4.3.4.3 (Klassifikation nilpotenter Endomorphismen).* Der vorhergehende Satz leistet im Sinne von 4.2.3.1 die Klassifikation aller Paare  $(V, N)$  bestehend aus einem endlichdimensionalen Vektorraum  $V$  über einem fest vorgegebenen Körper mitsamt einem nilpotenten Endomorphismus  $N$ . Zwei Paare  $(V, A)$  und  $(W, B)$  bestehend aus einem  $k$ -Vektorraum mit einem Endomorphismus nennen wir dazu „isomorph“ und schreiben  $(V, A) \cong (W, B)$ , wenn es einen Isomorphismus  $\phi : V \xrightarrow{\sim} W$  gibt mit  $B \circ \phi = \phi \circ A$ , so daß wir also ein kommutatives Diagramm erhalten der Gestalt

$$\begin{array}{ccc} V & \xrightarrow{A} & V \\ \downarrow \phi & & \downarrow \phi \\ W & \xrightarrow{B} & W \end{array}$$

Für jeden Körper  $k$  werden in diesem Sinne also die Paare bestehend aus einem endlichdimensionalen  $k$ -Vektorraum und einem nilpotenten Endomorphismus desselben klassifiziert durch endliche Multimengen von positiven natürlichen Zahlen.

*Beweis.* Die Eindeutigkeit ist unproblematisch: Ist  $N : V \rightarrow V$  unser nilpotenter Endomorphismus mit Matrix  $\text{diag}(J(r_1), \dots, J(r_n))$ , so finden wir für  $n \geq 1$  unmittelbar

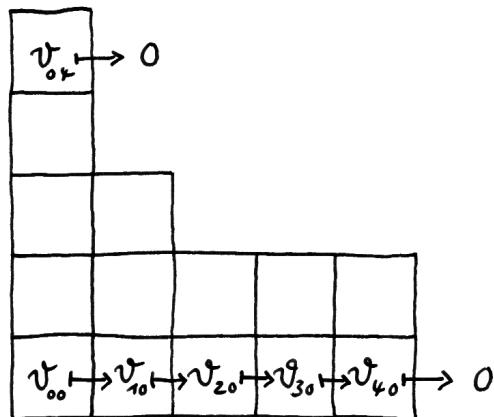
$$\dim(\text{im } N^{n-1}) - \dim(\text{im } N^n) = |\{i \mid r_i \geq n\}|$$

Die Kenntnis aller dieser Zahlen legt aber die Multimenge der  $r_i$  bereits fest. Die Existenz folgt unmittelbar aus Lemma 4.3.4.4, das wir gleich im Anschluß beweisen.  $\square$

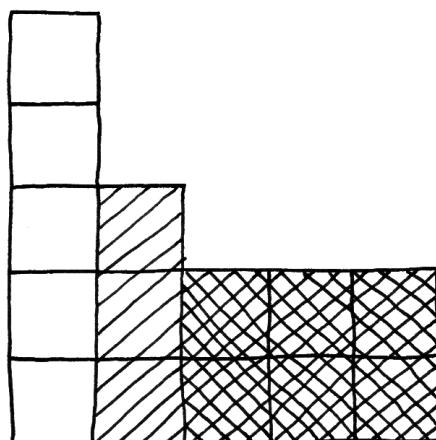
$$J(r) = \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \quad r$$

Der nilpotente Jordan-Block  $J(r)$  der Größe  $r$ . Steht auf der Diagonalen statt der Nullen ein Skalar  $\lambda$ , so nennen wir die entsprechende Matrix einen **Jordan-Block der Größe  $r$  zum Eigenwert  $\lambda$**  und notieren diese Matrix

$$J(r; \lambda) := J(r) + \lambda I_r$$



Ich denke mir eine nilpotente Abbildung gerne in der hier gezeigten Weise. Die Kästchen stehen für Basisvektoren, unser Vektorraum hätte also die Dimension 14. Die Abbildung schiebt jedes Kästchen um eins nach links beziehungsweise nach Null, wenn es dabei aus unserem Bild herausfällt. Die Matrix dieser Abbildung hat in der geeignet angeordneten Kästchenbasis offensichtlich Normalform, und die Längen der Zeilen entsprechen hierbei den Größen der Jordanblöcke.



Schraffiert eine Basis des Bildes von  $N$ , kreuzweise schraffiert eine Basis des Bildes von  $N^2$ . Die Höhe der zweiten Spalte ist also genau  $\dim(\text{im } N) - \dim(\text{im } N^2)$ .

**Lemma 4.3.4.4.** *Ist  $N : V \rightarrow V$  ein nilpotenter Endomorphismus eines endlich-dimensionalen Vektorraums  $V$ , so gibt es eine Basis  $B$  von  $V$  derart, daß  $B \sqcup \{0\}$  stabil ist unter  $N$  und daß jedes Element von  $B$  unter  $N$  höchstens ein Urbild in  $B$  hat. Wir nennen solch eine Basis eine **Jordan-Basis**.*

*Beweis.* Wir betrachten die Sequenz

$$\ker N \hookrightarrow V \twoheadrightarrow \text{im } N$$

Mit Induktion über die Dimension von  $V$  dürfen wir annehmen, daß wir für das Bild von  $N$  eine derartige Basis bereits gefunden haben, sagen wir die Basis  $A$ . Jetzt ergänzen wir  $\{a \in A \mid N(a) = 0\}$  durch irgendwelche  $b_1, \dots, b_s$  zu einer Basis des Kerns von  $N$  und wählen Urbilder  $c_1, \dots, c_r \in V$  für die Elemente von  $A \setminus N(A)$  und behaupten, daß

$$B = A \cup \{b_1, \dots, b_s\} \cup \{c_1, \dots, c_r\}$$

eine Basis von  $V$  ist mit den geforderten Eigenschaften. Nach Konstruktion ist  $B \sqcup \{0\}$  stabil unter  $N$  und jedes Element von  $B$  hat unter  $N$  höchstens ein Urbild in  $B$ . Wir müssen also nur noch zeigen, daß  $B$  eine Basis von  $V$  ist. Dazu schreiben wir  $B$  als die Vereinigung der beiden Mengen

$$\begin{aligned} \{a \in A \mid N(a) \neq 0\} &\cup \{c_1, \dots, c_r\} \\ \{a \in A \mid N(a) = 0\} &\cup \{b_1, \dots, b_s\} \end{aligned}$$

und bemerken, daß die erste Menge ein System von Urbildern unter  $N$  für unsere Basis  $A$  von ( $\text{im } N$ ) ist, wohingegen die zweite eine Basis von ( $\ker N$ ) ist. Damit ist unsere große Vereinigung eine Basis von  $V$  nach 3.2.2.6.  $\square$

**Korollar 4.3.4.5 (Jordan'sche Normalform).** *Gegeben ein Endomorphismus  $f$  eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper gibt es eine angeordnete Basis  $\mathcal{B}$  unseres Vektorraums derart, daß die Matrix unseres Endomorphismus bezüglich dieser Basis blockdiagonal ist mit Jordan-Blöcken auf der Diagonale, in Formeln*

$${}_{\mathcal{B}}[f]_{\mathcal{B}} = \text{diag}(\text{J}(r_1; \lambda_1), \dots, \text{J}(r_t; \lambda_t))$$

*Die Jordan-Blöcke auf der Diagonale sind hierbei durch unseren Endomorphismus wohlbestimmt bis auf Reihenfolge.*

$$b_1 \mapsto 0$$

$$b_2 \mapsto 0$$

$$c_1 \mapsto \bullet \mapsto 0$$

$$c_2 \mapsto \bullet \mapsto \bullet \mapsto 0$$

$$c_3 \mapsto \bullet \mapsto \bullet \mapsto 0$$

$$c_4 \mapsto \bullet \mapsto \bullet \mapsto \bullet \mapsto \bullet \mapsto \bullet \mapsto 0$$

Zum Beweis von 4.3.4.4. Die fetten Punkte stellen die Elemente der Basis  $A$  des Bildes im  $N$  dar. Die  $c_i$  zusammen mit den  $a \in A$  mit  $N(a) \neq 0$  bilden ein System von Urbildern unter  $N$  der Elemente von  $A$ .

$$\begin{pmatrix} \begin{matrix} 5 & 1 \\ 0 & 5 \end{matrix} & & & & & 0 \\ & \ddots & & & & \\ & & \begin{matrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{matrix} & & & \\ & & & \ddots & & \\ & & & & \ddots & 7 \end{pmatrix}$$

Ein Matrix in Jordan'scher Normalform mit drei Jordanblöcken. Genau dann hat eine komplexe  $(6 \times 6)$ -Matrix  $A$  diese Jordan'sche Normalform, wenn ihr charakteristisches Polynom eine einfache Nullstelle bei 7 und eine fünffache Nullstelle bei 5 hat und  $\ker(A - 5I)$  zweidimensional ist sowie  $\ker(A - 5I)^2$  vierdimensional.

**4.3.4.6 (Jordan'sche Normalform als Lösung eines Klassifikationsproblems).** Dieser Satz leistet im Fall eines algebraisch abgeschlossenen Grundkörpers  $K$  im Sinne von 4.2.3.1 die Klassifikation der endlichdimensionalen  $K$ -Vektorräume mit einem ausgezeichneten Endomorphismus, in Bezug auf den in 4.3.4.3 erklärten Isomorphie-Begriff. Genauer werden solche Daten „klassifiziert durch endliche Multimengen von Paaren aus  $(K \times \mathbb{N}_{\geq 1})$ “. Man beachte den fundamentalen Unterschied zur „Smith-Normalform“ 3.2.6.11.

*Ergänzung 4.3.4.7 (Das Klassifikationsproblem für allgemeine Grundkörper).* Im Fall eines beliebigen Grundkörpers  $K$  wird die entsprechende Klassifikationsaufgabe in ?? gelöst: Endlichdimensionale  $K$ -Vektorräume mit einem ausgezeichneten Endomorphismus werden in Bezug auf den in 4.3.4.3 erklärten Isomorphiebegriff „klassifiziert durch endliche Multimengen von Elementen des Produkts  $((\text{irnp } K[X]) \times \mathbb{N}_{\geq 1})$ “ mit der Notation  $\text{irnp } K[X]$  für die Menge aller irreduziblen normierten Polynome aus  $K[X]$ .

**4.3.4.8.** Unser Korollar 4.3.4.5 gilt mit demselben Beweis auch, wenn wir statt der algebraischen Abgeschlossenheit des Grundkörpers nur voraussetzen, daß das charakteristische Polynom unseres Endomorphismus über unserem Körper vollständig in Linearfaktoren zerfällt. Gegeben eine quadratische Matrix ist die explizite Berechnung einer „Jordan-Basis“ im allgemeinen nicht ganz einfach. Hierzu gibt es auch Algorithmen, mit denen ich Sie jedoch nicht belasten will, da die explizite Berechnung einer Jordan-Basis in der Praxis selten gebraucht wird. Wichtig an diesem Korollar sind vielmehr die darin enthaltenen strukturellen Aussagen über Endomorphismen von Vektorräumen.

*Beweis.* Sei  $f$  unser Endomorphismus. Der Satz über die Hauptraumzerlegung 4.3.2.13 zeigt, daß wir ohne Beschränkung der Allgemeinheit annehmen dürfen, daß es einen Skalar  $\lambda$  gibt, für den  $(f - \lambda \text{id})$  nilpotent ist. Der Satz über die Normalform nilpotenter Endomorphismen 4.3.4.2 beendet dann den Beweis.  $\square$

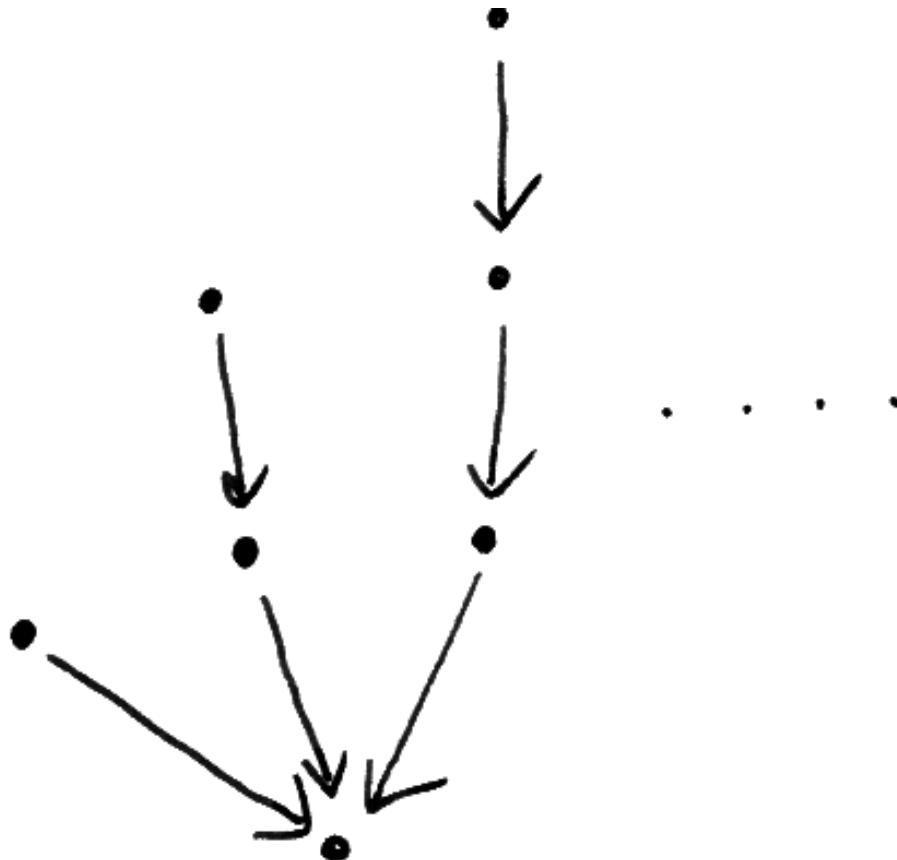
*Ergänzung 4.3.4.9 (Beispiele für lokal nilpotente Endomorphismen).* Lemma 4.3.4.4 über die Existenz einer Jordan-Basis gilt sogar ohne die Voraussetzung, daß  $V$  endlichdimensional ist. Um das zu zeigen, müssen wir nur die Induktion statt über die Dimension von  $V$  über die Nilpotenzordnung von  $N$  laufen lassen und 3.1.9.20 verwenden. Für einen lokal nilpotenten Endomorphismus  $N$  findet man jedoch im Allgemeinen keine Jordan-Basis mehr, nebenstehendes Bild zeigt ein Gegenbeispiel. Im Fall abzählbarer Dimension kann man noch zeigen, daß es stets eine Jordan-Basis gibt, wenn der Schnitt der Bilder aller Potenzen Null ist. Das beruht auf dem „Satz von Ulm“ aus der Logik. Im Fall beliebiger Dimension gilt auch das nicht mehr, ja wir finden im allgemeinen noch nicht einmal eine Basis  $B$  derart, daß  $B \sqcup \{0\}$  unter  $N$  stabil ist. Betrachten wir zum Beispiel den Raum  $V$  aller Abbildungen von der Menge  $\{(i, j) \in \mathbb{N}^2 \mid i \geq j\}$  nach  $\mathbb{R}$ , die nur in endlich

vielen Zeilen nicht identisch Null sind, und den Endomorphismus  $N : V \rightarrow V$ , der „jede Zeile um eins nach unten drückt und die nullte Zeile annulliert“, in Formeln  $(N(f))(i, j) = f(i, j + 1)$  falls  $i > j$  und  $(N(f))(i, j) = 0$  falls  $i = j$ . Sicher hat  $V/NV$  eine abzählbare Basis, so daß  $A := B \setminus NB$  abzählbar sein müßte. Andererseits ist in unserem Beispiel der Schnitt der Bilder aller Potenzen  $\bigcap_{n=1}^{\infty} N^n$  der Nullraum, und das zeigt  $B \sqcup \{0\} = A \cup NA \cup N^2A \cup \dots$  im Widerspruch dazu, daß  $V$  selbst keine abzählbare Basis besitzt. Das alles habe ich in Diskussion mit Martin Ziegler gelernt.

### Übungen

*Übung 4.3.4.10 (Jacobson-Morozov).* Sei  $N : V \rightarrow V$  ein nilpotenter Endomorphismus eines Vektorraums  $V$ . So besitzt  $V$  genau eine endliche Filtrierung  $(V^{\geq r})_{r \in \mathbb{Z}}$  derart, daß für alle  $r$  gilt  $N(V^{\geq r}) \subset V^{\geq r+2}$  und für alle  $r \in \mathbb{N}$  zusätzlich

$$N^r : V^{\geq -r}/V^{\geq -r+1} \xrightarrow{\sim} V^{\geq r}/V^{\geq r+1}$$



Eine Basis mit der Eigenschaft aus Lemma 4.3.4.4 nennen wir auch eine **Jordan-Basis**. Dieses Bild zeigt einen lokal nilpotenten Endomorphismus, für den keine Jordan-Basis existiert. Die fetten Punkte stehen für Basisvektoren, die Pfeile zeigen, wie sie abgebildet werden. Wir erhalten so eine lokal nilpotente Abbildung, bei der der Schnitt der Bilder aller Potenzen nicht Null ist. Dennoch ist kein Element des zugehörigen Vektorraums „unendlich divisibel“, folglich kann es in diesem Fall keine Jordan-Basis geben.

## 4.4 Quotienten

In diesem Abschnitt wird die Gruppentheorie weiter ausgebaut. Insbesondere lernen Sie die Klassifikation der endlich erzeugten abelschen Gruppen kennen. Man versteht unter solch einer Klassifikation die Angabe einer Liste von endlich erzeugten abelschen Gruppen derart, daß jede endlich erzeugte abelsche Gruppe zu genau einer Gruppe dieser Liste isomorph ist. Die Klassifikation endlich erzeugter Vektorräume über einem vorgegebenen Körper  $K$  kennen Sie bereits: Jeder solche Vektorraum  $K$  ist isomorph zu genau einem  $K^n$  mit  $n \in \mathbb{N}$ , und dieses  $n$  heißt dann auch die Dimension des  $K$ -Vektorraums  $V$ . Wir werden sehen, daß die Klassifikation der endlich erzeugten abelschen Gruppen raffinierter ist.

### 4.4.1 Nebenklassen

4.4.1.1. Ist  $(G, \perp)$  eine Menge mit Verknüpfung und sind  $A, B \subset G$  Teilmengen, so schreiben wir  $A \perp B = \{a \perp b \mid a \in A, b \in B\} \subset G$  und erhalten auf diese Weise eine Verknüpfung auf der Menge aller Teilmengen von  $G$ , der sogenannten Potenzmenge  $\mathcal{P}(G)$ . Ist unsere ursprüngliche Verknüpfung assoziativ, so auch die induzierte Verknüpfung auf der Potenzmenge. Wir kürzen in diesem Zusammenhang oft die einelementige Menge  $\{a\}$  mit  $a$  ab, so daß also zum Beispiel  $a \perp B$  als  $\{a\} \perp B$  zu verstehen ist.

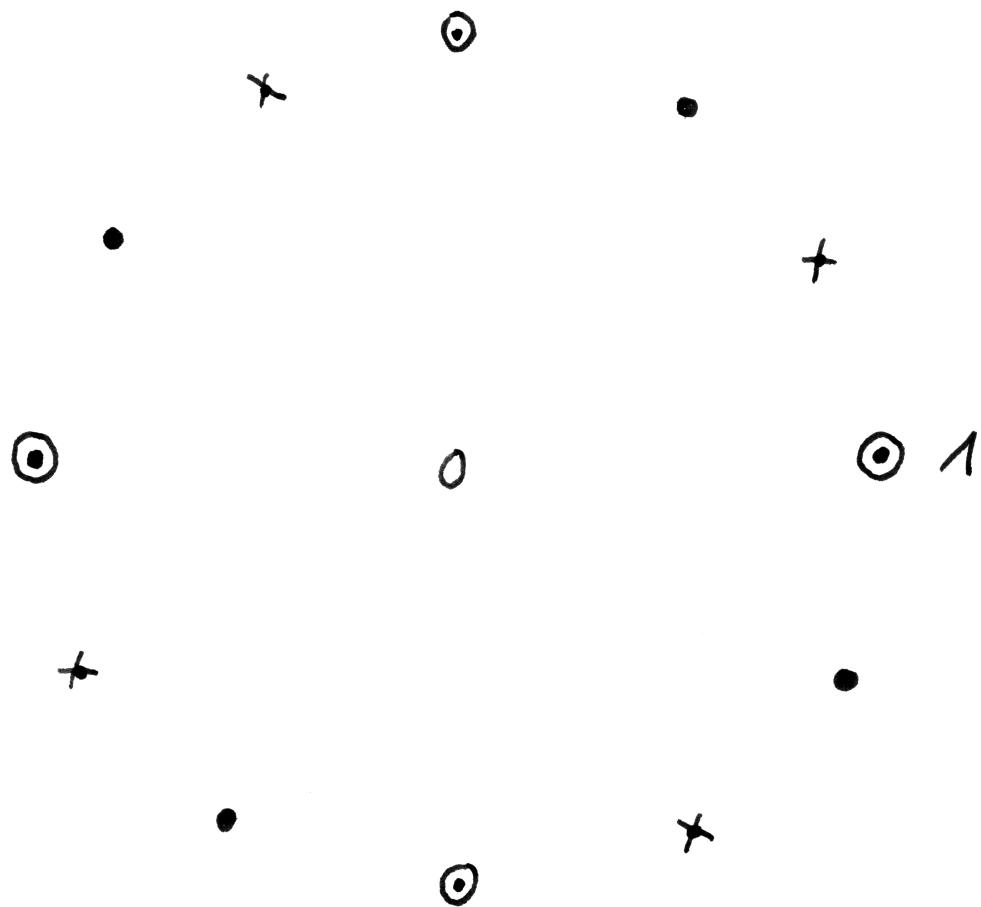
**Definition 4.4.1.2.** Ist  $G$  eine Gruppe,  $H \subset G$  eine Untergruppe und  $g \in G$  ein Element, so nennen wir die Menge  $gH$  die **Linksnebenklasse von  $g$  unter  $H$**  und die Menge  $Hg$  die **Rechtsnebenklasse von  $g$  unter  $H$** . Diese Nebenklassen sind also Teilmengen von  $G$ . Ein Element einer Nebenklasse nennt man einen **Repräsentanten** der besagten Nebenklasse. Weiter betrachten wir in  $G$  die beiden Mengensysteme

$$\begin{aligned} G/H &= \{gH \mid g \in G\} \\ H\backslash G &= \{Hg \mid g \in G\} \end{aligned}$$

aller Links- beziehungsweise Rechtsnebenklassen von  $H$  in  $G$ . Die Elemente von  $G/H$  und von  $H\backslash G$  sind also Teilmengen von  $G$ . Die Symbole  $G/H$  sowie  $H\backslash G$  bezeichnen dementsprechend Teilmengen der Potenzmenge  $\mathcal{P}(G)$  von  $G$ .

4.4.1.3 (**Disjunktheit der Nebenklassen**). Gegeben  $G \supset H$  eine Gruppe mit einer Untergruppe sind die  $H$ -Rechtsnebenklassen in  $G$  paarweise disjunkt. In der Tat folgt aus  $g \in xH$  alias  $g = xh$  für  $h \in H$  bereits  $gH = xhH = xH$ . Analoges gilt für die Linksnebenklassen.

*Beispiel 4.4.1.4.* Im Fall  $G = \mathbb{Z} \supset H = m\mathbb{Z}$  haben wir die Menge der Nebenklassen  $\mathbb{Z}/m\mathbb{Z}$  bereits in 3.5.2.4 diskutiert und sogar selbst mit der Struktur einer Gruppe, ja sogar mit der Struktur eines Rings versehen. Im allgemeinen trägt



Die drei Nebenklassen der Gruppe  $\{\pm 1, \pm i\}$  der vierten Einheitswurzeln in der Gruppe der zwölften Einheitswurzeln. Da diese Gruppe kommutativ ist, fallen hier Rechtsnebenklassen und Linksnabenklassen zusammen.

$G/H$  nur dann eine natürliche Gruppenstruktur, wenn wir an unsere Untergruppe  $H$  zusätzliche Forderungen stellen, vergleiche 4.4.2.

**Satz 4.4.1.5 (Lagrange).** *Gegeben eine endliche Gruppe teilt die Kardinalität jeder Untergruppe die Kardinalität der ganzen Gruppe. Ist  $G$  eine endliche Gruppe und  $H \subset G$  eine Untergruppe, so gilt genauer*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H \setminus G|$$

*Beweis.* Jedes Element von  $G$  gehört zu genau einer Links- beziehungsweise Rechtsnebenklasse unter  $H$ , und jede dieser Nebenklassen hat genau  $|H|$  Elemente.  $\square$

4.4.1.6. In anderen Worten kann man diesen Beweis etwa im Fall der Linksnebenklassen auch dahingehend formulieren, daß alle Fasern der offensichtlichen Abbildung  $\text{can} : G \rightarrow G/H$  genau  $|H|$  Elemente haben, denn diese Fasern sind gerade die Linksnebenklassen von  $H$  in  $G$ .

**Definition 4.4.1.7.** Gegeben eine Gruppe  $G$  mit einer Untergruppe  $H$  heißt die Zahl  $|G/H|$  der Restklassen auch der **Index von  $H$  in  $G$** .

## Übungen

*Ergänzende Übung 4.4.1.8.* Haben zwei Untergruppen ein- und derselben Gruppe endlichen Index, so hat auch ihr Schnitt endlichen Index.

*Ergänzende Übung 4.4.1.9.* Seien  $G \supset H$  eine Gruppe und eine Untergruppe. Man zeige, daß es eine Bijektion zwischen  $G/H$  und  $H \setminus G$  gibt.

*Ergänzende Übung 4.4.1.10.* Haben zwei endliche Untergruppen einer Gruppe teilerfremde Kardinalitäten, so besteht ihr Schnitt nur aus dem neutralen Element.

*Übung 4.4.1.11.* Sei  $\varphi : G \rightarrow L$  ein Gruppenhomomorphismus und seien  $H \subset G$  sowie  $H' \subset G'$  Untergruppen. Gilt  $\varphi(H) \subset H'$ , so gibt es genau eine Abbildung  $\bar{\varphi} : G/H \rightarrow G'/H'$  derart, daß im Diagramm

$$\begin{array}{ccccc} H & \longrightarrow & G & \longrightarrow & G/H \\ \downarrow & & \downarrow & & \downarrow \\ H' & \longrightarrow & G' & \longrightarrow & G'/H' \end{array}$$

auch das rechte Rechteck kommutiert, und die nichtleeren Fasern dieser Abbildung  $\bar{\varphi}$  sind die Mengen  $\bar{\varphi}^{-1}(\varphi(g)H') = \{gxH \mid x \in \varphi^{-1}(H')\}$  und haben insbesondere alle dieselbe Kardinalität wie  $\varphi^{-1}(H')/H$ . Sind weiter zwei der vertikalen Abbildungen unseres Diagramms Bijektionen, so auch die Dritte. Allgemeinere Aussagen liefert später das Neunerlemma 4.4.7.5.

*Ergänzende Übung 4.4.1.12 (Zu unipotenten oberen Dreiecksmatrizen).* Sei  $R$  ein Ring und  $n \geq 2$ . Gegeben  $i, j \leq n$  mit  $i \neq j$  betrachten wir die Untergruppen  $U_{ij} := I + RE_{ij} \subset \mathrm{GL}(n; R)$  und die Untergruppe  $U \subset \mathrm{GL}(n; R)$  aller oberen Dreiecksmatrizen mit Einträgen in  $R$ . Man zeige, daß das Aufmultiplizieren in beliebiger aber fest gewählter Reihenfolge stets eine Bijektion

$$\prod_{i < j} U_{ij} \xrightarrow{\sim} U$$

induziert. Hinweis: Man betrachte rechts die Folge von Untergruppen  $U_\nu := \{A \mid A_{ij} = 0 \text{ für } 0 < |i - j| \leq \nu\}$  und verwende 4.4.1.11. Allgemeiner zeige man, daß für jede Permutation  $w \in S_n$  die Multiplikation bei beliebiger aber fester Reihenfolge der Faktoren eine Bijektion  $\prod_{i < j, w(i) < w(j)} U_{ij} \xrightarrow{\sim} U \cap w^{-1}Uw$  liefert. Hinweis: Natürlich gilt stets  $U_{w(i)w(j)}w = wU_{ij}$ .

## 4.4.2 Normalteiler und Nebenklassengruppen

**Satz 4.4.2.1 (Universelle Eigenschaft surjektiver Gruppenhomomorphismen).** Seien  $G$  eine Gruppe,  $s : G \twoheadrightarrow Q$  ein surjektiver Gruppenhomomorphismus und  $\varphi : G \rightarrow H$  ein beliebiger Gruppenhomomorphismus. Genau dann existiert ein Gruppenhomomorphismus  $\bar{\varphi} : Q \rightarrow H$  mit  $\varphi = \bar{\varphi} \circ s$ , wenn gilt  $\ker(\varphi) \supset \ker(s)$ .

4.4.2.2. Dieser Gruppenhomomorphismus  $\bar{\varphi}$  ist dann natürlich eindeutig bestimmt. In diesem Sinne kann man unseren Satz auch dahingehend zusammenfassen, daß das Vorschalten eines surjektiven Gruppenhomomorphismus  $s : G \twoheadrightarrow Q$  für jede weitere Gruppe  $H$  eine Bijektion

$$(\circ s) : \mathrm{Grp}(Q, H) \xrightarrow{\sim} \{\varphi \in \mathrm{Grp}(G, H) \mid \ker(\varphi) \supset \ker(s)\}$$

liefert. Der Übersichtlichkeit halber stelle ich die in diesem Satz auftauchenden Gruppen und Morphismen auch noch wieder anders in einem Diagramm dar:

$$\begin{array}{ccc} G & \xrightarrow{s} & Q \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & H & \end{array}$$

Man sagt dann,  $\varphi$  faktorisiere in eindeutiger Weise über  $s$ .

*Beweis.* Offensichtlich gilt  $s^{-1}(s(x)) = x \ker(s)$  für alle  $x \in G$ . Die Fasern von unseres surjektiven Gruppenhomomorphismus  $s$  sind also genau die Nebenklassen unter  $\ker(s)$ . Damit ist  $\varphi$  konstant auf den Fasern von  $s$  und wir finden nach der universellen Eigenschaft von Surjektionen 2.1.5.11 schon einmal genau eine Abbildung  $\bar{\varphi}$  wie behauptet. Man prüft ohne weitere Schwierigkeiten, daß sie sogar ein Gruppenhomomorphismus sein muß.  $\square$

*Beispiel 4.4.2.3.* Wir haben etwa

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\text{can}} & \mathbb{Z}/8\mathbb{Z} \\ \varphi : n \mapsto i^n \searrow & & \downarrow \bar{\varphi} \\ & & \mathbb{C}^\times \end{array}$$

oder in Worten: Die Abbildung  $\varphi : n \mapsto i^n$  faktorisiert über  $\mathbb{Z}/8\mathbb{Z}$  und induziert so einen Gruppenhomomorphismus  $\bar{\varphi} : \mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{C}^\times, \bar{n} \mapsto i^n$ .

**4.4.2.4 (Surjektive Gruppenhomomorphismen mit demselben Kern).** Gegeben eine Gruppe  $G$  und zwei surjektive Gruppenhomomorphismen  $s : G \twoheadrightarrow Q$  und  $t : G \twoheadrightarrow P$  mit demselben Kern  $\ker(s) = \ker(t)$  sind die Gruppenhomomorphismen  $\bar{t} : Q \rightarrow P$  mit  $\bar{t} \circ s = t$  und  $\bar{s} : P \rightarrow Q$  mit  $\bar{s} \circ t = s$  nach 4.4.2.1 zueinander inverse Isomorphismen  $Q \xrightarrow{\sim} P \xrightarrow{\sim} Q$ . Salopp gesprochen wird also bei einem surjektiven Gruppenhomomorphismus „das Ziel bereits durch die Ausgangsgruppe und den Kern festgelegt bis auf eindeutigen Isomorphismus“.

**4.4.2.5.** Die vorstehenden Überlegungen legen die Frage nahe, welche Untergruppen einer gegebenen Gruppe denn als Kerne von von unserer Gruppe ausgehenden Gruppenhomomorphismen in Frage kommen. Das diskutieren wir im folgenden.

**Definition 4.4.2.6.** Eine Untergruppe  $N$  einer Gruppe  $G$  heißt **normal** oder auch ein **Normalteiler von  $G$** , wenn in  $G$  die  $N$ -Rechtsnebenklassen mit den  $N$ -Linksnebenklassen übereinstimmen, wenn also gilt

$$gN = Ng \quad \forall g \in G$$

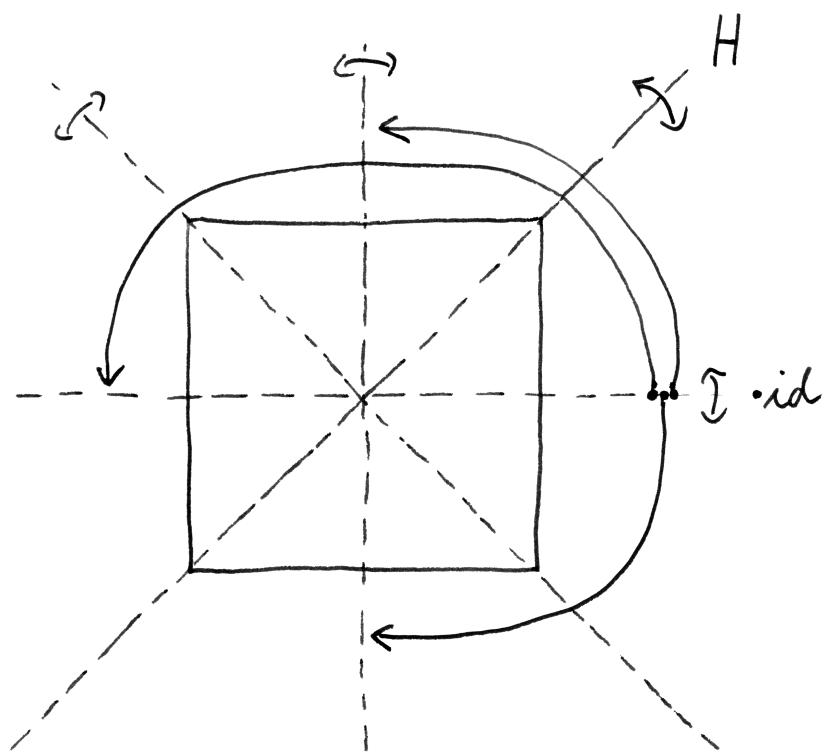
Die Aussage „ $N \subset G$  ist ein Normalteiler“ kürzt man oft ab mit  $N \triangleleft G$ .

*Beispiele 4.4.2.7.* In einer kommutativen Gruppe ist jede Untergruppe ein Normalteiler. In der Gruppe  $S_3$  der Permutationen von 3 Elementen ist die Untergruppe  $S_2 \subset S_3$  aller Permutationen, die die dritte Stelle festhalten, kein Normalteiler.

**4.4.2.8 (Diskussion der Terminologie).** Normal zu sein ist für eine Untergruppe etwas ganz Besonderes. In diesem Licht betrachtet ist unsere Terminologie gewöhnungsbedürftig. Aber gut, vielleicht ist ja bei Menschen auch normal zu sein etwas ganz Besonderes.

**4.4.2.9.** Man sieht leicht, daß der Kern eines Gruppenhomomorphismus stets ein Normalteiler sein muß. Wir zeigen nun, daß auch umgekehrt jeder Normalteiler der Kern eines surjektiven Gruppenhomomorphismus ist.

**Satz 4.4.2.10.** Seien  $G$  eine Gruppe und  $N \subset G$  ein Normalteiler. So gilt:



Die acht Symmetrien des Quadrats. Eine Linksnebenklasse  $gH$  der von der Spiegelung an der Nordost-Diagonalen erzeugten Untergruppe besteht aus den beiden Symmetrien des Quadrats, die die obere rechte Ecke in eine vorgegebene weitere Ecke überführen. Eine Rechtsnebenklasse  $Hg$  besteht dagegen aus den beiden Symmetrien des Quadrats, bei denen die obere rechte Ecke von einer vorgegebenen weiteren Ecke herkommt. Insbesondere ist  $H$  kein Normalteiler in der Gruppe der acht Symmetrien des Quadrats.

1. Die Menge  $G/N$  der Nebenklassen ist abgeschlossen unter der induzierten Verknüpfung auf der Potenzmenge  $\mathcal{P}(G)$  von  $G$  und wird mit dieser Verknüpfung eine Gruppe, die **Nebenklassengruppe** oder auch der **Quotient von  $G$  nach  $N$** ;
2. Die Abbildung  $G \rightarrow G/N$ , die jedem Element seine Nebenklasse zuordnet, ist ein surjektiver Gruppenhomomorphismus mit Kern  $N$ .

*Beweis.* Es gilt  $(gN)(g_1N) = gNg_1N = gg_1NN = gg_1N$ , also ist unsere Menge stabil unter der Verknüpfung. Das Assoziativgesetz gilt eh, das neutrale Element ist  $N$ , und das Inverse zu  $gN$  ist  $g^{-1}N$ . Die zweite Aussage ist eh klar.  $\square$

*Beispiel 4.4.2.11.* Die Nebenklassengruppe  $\mathbb{Z}/m\mathbb{Z}$  kennen wir bereits aus 3.5.2.4, wo wir darauf sogar noch eine Multiplikation erklärt hatten, die sie zu einem Ring macht. Sie hat genau  $m$  Elemente.

**Satz 4.4.2.12 (Isomorphiesatz).** Jeder Homomorphismus  $\varphi : G \rightarrow H$  von Gruppen induziert einen Isomorphismus  $\bar{\varphi} : G/\ker \varphi \xrightarrow{\sim} \text{im } \varphi$ .

*Beispiel 4.4.2.13.* In unserem Beispiel 4.4.2.3 liefert uns der Isomorphiesatz einen Isomorphismus  $\mathbb{Z}/4\mathbb{Z} \xrightarrow{\sim} \{i^n \mid n \in \mathbb{Z}\} \subset \mathbb{C}^\times$ .

*Beispiel 4.4.2.14.* Die Abbildung  $\varphi = 2 \text{ can} : \mathbb{Z} \rightarrow \mathbb{Z}/10\mathbb{Z}$ ,  $n \mapsto (2n + 10\mathbb{Z})$  hat den Kern  $\ker \varphi = 5\mathbb{Z}$  und das Bild  $\text{im } \varphi = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \subset \mathbb{Z}/10\mathbb{Z}$ . Der Isomorphiesatz liefert in diesem Fall also einen Gruppenisomorphismus

$$\mathbb{Z}/5\mathbb{Z} \xrightarrow{\sim} \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$$

*Beweis.* Das folgt sofort aus unserer Erkenntnissen 4.4.2.4 über surjektive Gruppenhomomorphismen mit demselben Kern, denn wir finden surjektive Gruppenhomomorphismen von  $G$  auf beide Seiten, die ein kommutatives Dreieck entstehen lassen und denselben Kern haben.  $\square$

**Korollar 4.4.2.15 (Noether'scher Isomorphiesatz).** Ist  $G$  eine Gruppe und sind  $K \subset H \subset G$  zwei Normalteiler von  $G$ , so induziert die Komposition von kanonischen Abbildungen  $G \rightarrow (G/K) \rightarrow (G/K)/(H/K)$  einen Isomorphismus

$$G/H \xrightarrow{\sim} (G/K)/(H/K)$$

4.4.2.16. Ist  $G$  eine Gruppe und sind  $K \subset H \subset G$  Untergruppen mit  $K$  normal in  $H$ , so werden wir bald  $(G/K)/(H/K)$  als „Raum der Bahnen einer Operation der Gruppe  $H/K$  auf der Menge  $G/K$ “ verstehen können, und unsere Abbildung ist dann immer noch wohldefiniert und nach 4.5.1.26 eine Bijektion.

*Beweis.* Nach unserer Erkenntnissen 4.4.2.4 über surjektive Gruppenhomomorphismen mit demselben Kern 4.4.2.4 reicht es zu zeigen, daß unsere Komposition den Kern  $H$  hat. Das ist jedoch klar.  $\square$

## Übungen

*Übung 4.4.2.17.* Man zeige, daß in der symmetrischen Gruppe  $S_4$  die Doppeltranspositionen aus 3.6.1.12 zusammen mit dem neutralen Element einen Normalteiler  $D \subset S_4$  bilden, und konstruiere einen Isomorphismus  $S_4/D \xrightarrow{\sim} S_3$ .

*Ergänzende Übung 4.4.2.18.* Sei  $m \in \mathbb{N}$  eine natürliche Zahl. Man zeige, daß die Vorschrift  $\varphi \mapsto \varphi(\bar{1})$  für eine beliebige Gruppe  $G$  eine Bijektion

$$\text{Grp}(\mathbb{Z}/m\mathbb{Z}, G) \xrightarrow{\sim} \{g \in G \mid g^m = 1\}$$

liefert. Man beachte, daß hierbei  $\bar{1}$  nicht das neutrale Element der additiv notierten Gruppe  $\mathbb{Z}/m\mathbb{Z}$  bezeichnet, sondern die Nebenklasse der Eins, einen Erzeuger, wohingegen  $1 \in G$  das neutrale Element der multiplikativ notierten Gruppe  $G$  meint. Wieviele Gruppenhomomorphismen gibt es von  $\mathbb{Z}/m\mathbb{Z}$  nach  $\mathbb{Z}/n\mathbb{Z}$ ?

*Übung 4.4.2.19.* Gegeben ein surjektiver Gruppenhomomorphismus  $\varphi : G \twoheadrightarrow \bar{G}$  und ein Normalteiler  $\bar{N} \subset \bar{G}$  mit Urbild  $\varphi^{-1}(\bar{N}) = N \subset G$  induziert  $\varphi$  einen Gruppenisomorphismus

$$\varphi : G/N \xrightarrow{\sim} \bar{G}/\bar{N}$$

*Übung 4.4.2.20.* Der Kern eines Gruppenhomomorphismus ist stets ein Normalteiler. Allgemeiner ist das Urbild eines Normalteilers unter einem Gruppenhomomorphismus stets ein Normalteiler, und das Bild eines Normalteilers unter einem surjektiven Gruppenhomomorphismus ist wieder ein Normalteiler.

*Ergänzende Übung 4.4.2.21.* Jede Untergruppe vom Index Zwei ist ein Normalteiler.

*Ergänzende Übung 4.4.2.22.* Jede Untergruppe von endlichem Index umfaßt einen Normalteiler von endlichem Index.

*Ergänzende Übung 4.4.2.23.* Man nennt einen Gruppenhomomorphismus  $A \rightarrow A''$  **linksspaltend**, wenn er ein Rechtsinverses besitzt, und nennt solch ein Rechtsinverses dann eine **Spaltung**. Man zeige: Jeder linksspaltende Gruppenhomomorphismus ist surjektiv. Ist  $\varphi : A \rightarrow A''$  ein Homomorphismus von abelschen Gruppen,  $A' \subset A$  sein Kern und  $\psi : A'' \rightarrow A$  ein Rechtsinverses von  $\varphi$  alias  $\varphi\psi = \text{id}$ , so erhalten wir vermittels der Vorschrift  $(a', a'') \mapsto a' + \psi(a'')$  einen Isomorphismus  $A' \times A'' \xrightarrow{\sim} A$ . Verallgemeinerungen auf den Fall nichtabelscher Gruppen besprechen wir in ??.

*Ergänzende Übung 4.4.2.24.* Man nennt einen Gruppenhomomorphismus  $A' \rightarrow A$  **rechtsspaltend**, wenn er ein Linksinverses besitzt, und nennt solch ein Linksinverses dann eine **Spaltung**. Man zeige: Jeder rechtsspaltende Gruppenhomomorphismus ist injektiv. Ist  $\psi : A' \rightarrow A$  ein Homomorphismus von abelschen Gruppen und  $\phi : A \rightarrow A'$  ein Linksinverses alias  $\phi\psi = \text{id}$  und  $A'' \subset A$  dessen Kern, so ist  $\phi$  linksspaltend und wir erhalten für  $A'' := \ker \phi$  wie in 4.4.2.23 einen Isomorphismus  $A' \times A'' \xrightarrow{\sim} A$ .

*Ergänzende Übung 4.4.2.25.* Jede Surjektion von einer abelschen Gruppe auf  $\mathbb{Z}^r$  besitzt ein Rechtsinverses. Man gebe ein Beispiel für einen surjektiven Gruppenhomomorphismus, der kein Rechtsinverses besitzt.

*Übung 4.4.2.26.* Man zeige, daß das Multiplizieren von Matrizen mit Spaltenvektoren eine Bijektion  $\text{Mat}(n \times m; \mathbb{Z}) \xrightarrow{\sim} \text{Grp}(\mathbb{Z}^m, \mathbb{Z}^n)$ ,  $A \mapsto (A \circ)$  zwischen der Menge aller  $(n \times m)$ -Matrizen mit ganzzahligen Einträgen und der Menge aller Gruppenhomomorphismen  $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$  liefert.

*Ergänzende Übung 4.4.2.27.* Seien  $A, B, C$  abelsche Gruppen. Eine Abbildung  $\varphi : A \times B \rightarrow C$  heißt **biadditiv**, wenn jedes feste  $b \in B$  einen Gruppenhomomorphismus  $A \rightarrow C$ ,  $a \mapsto \varphi(a, b)$  liefert und jedes feste  $a \in A$  einen Gruppenhomomorphismus  $B \rightarrow C$ ,  $b \mapsto \varphi(a, b)$ . Man zeige: Gegeben eine biadditive Abbildung  $\varphi : A \times B \rightarrow C$  und surjektive Homomorphismen  $s : A \twoheadrightarrow P$  sowie  $t : B \twoheadrightarrow Q$  mit  $\varphi(\ker(s) \times B) = 0 = \varphi(A \times \ker(t))$  gibt es genau eine biadditive Abbildung  $\bar{\varphi} : P \times Q \rightarrow C$  derart, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} A \times B & \xrightarrow{\varphi} & C \\ s \times t \downarrow & & \parallel \\ P \times Q & \xrightarrow{\bar{\varphi}} & C \end{array}$$

Analog erklärt man multiadditive Abbildungen für abelsche Gruppen und zeigt für diese eine analoge Aussage.

### 4.4.3 Zyklische Gruppen

**Definition 4.4.3.1.** Eine Gruppe heißt **zyklisch**, wenn sie im Sinne von 3.4.3.5 von einem einzigen Element erzeugt wird.

**Definition 4.4.3.2.** Sei  $g$  ein Element einer Gruppe  $G$ . Die **Ordnung**  $\text{ord } g$  von  $g$  ist die kleinste natürliche Zahl  $n \geq 1$  mit  $g^n = 1_G$ . Gibt es kein solches  $n$ , so setzen wir  $\text{ord } g = \infty$  und sagen,  $g$  habe **unendliche Ordnung**.

4.4.3.3. In jeder Gruppe ist das einzige Element der Ordnung 1 das neutrale Element. Elemente der Ordnung  $\leq 2$  heißen auch **Involutionen**.

**Proposition 4.4.3.4 (Struktur zyklischer Gruppen).** Ist  $G$  eine Gruppe und  $g \in G$  ein Element, so stimmt die Ordnung von  $g$  überein mit der Kardinalität der von  $g$  erzeugten Untergruppe, in Formeln  $\text{ord } g = |\langle g \rangle|$ . Genauer gilt:

1. Hat  $g$  unendliche Ordnung, so ist die Abbildung  $\nu \mapsto g^\nu$  ein Isomorphismus  $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ ;

2. Hat  $g$  endliche Ordnung  $\text{ord } g = n$ , so induziert  $\nu \mapsto g^\nu$  einen Isomorphismus  $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ .

*Beweis.* Wir betrachten den Gruppenhomomorphismus  $\varphi : \mathbb{Z} \rightarrow G$ ,  $\nu \mapsto g^\nu$ . Nach dem Isomorphiesatz 4.4.2.12 haben wir einen Isomorphismus

$$\mathbb{Z}/\ker \varphi \xrightarrow{\sim} \text{im } \varphi = \langle g \rangle$$

Nach der Klassifikation 3.4.3.4 der Untergruppen von  $\mathbb{Z}$  ist  $\ker \varphi$  von der Form  $\ker \varphi = n\mathbb{Z}$  für eindeutig bestimmtes  $n \in \mathbb{N}$ , und dann gilt notwendig  $n = \text{ord } g$  für  $g$  von endlicher Ordnung beziehungsweise  $n = 0$  für  $g$  von unendlicher Ordnung.  $\square$

4.4.3.5. Motiviert durch diese Proposition nennt man die Kardinalität einer Gruppe oft die **Ordnung der Gruppe**. Wir haben mit unserer Proposition im Übrigen auch bewiesen, daß jede Gruppe mit genau 5 Elementen isomorph ist zu  $\mathbb{Z}/5\mathbb{Z}$ , denn für jedes vom neutralen Element verschiedene Element unserer Gruppe ist  $\langle g \rangle$  eine Untergruppe mit mindestens zwei Elementen, also nach Lagrange bereits die ganze Gruppe. Wir formulieren das gleich noch allgemeiner.

*Ergänzung 4.4.3.6 (Diskussion der Notation).* Für die endlichen zyklischen Gruppen  $\mathbb{Z}/n\mathbb{Z}$  mit  $n \geq 1$  sind viele alternative Notationen gebräuchlich. Ich kenne insbesondere die alternativen Notationen  $C_n$ ,  $Z_n$  und  $\mathbb{Z}_n$ , von denen ich die letzte am wenigsten mag, da sie im Fall einer Primzahl  $n = p$  auch für die sogenannten  $p$ -adischen Zahlen benutzt wird.

**Korollar 4.4.3.7.** *Jede Gruppe von Primzahlordnung ist zyklisch. Ist genauer  $p$  eine Primzahl und  $G$  eine Gruppe mit  $|G| = p$  Elementen, so gibt es für jedes Element  $g \in G \setminus \{1_G\}$  genau einen Gruppenisomorphismus  $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} G$  mit  $\bar{1} \mapsto g$ .*

*Beweis.* Nach dem Satz von Lagrange 4.4.1.5 teilt die Ordnung jeder Untergruppe die Ordnung der ganzen Gruppe. Eine Gruppe von Primzahlordnung hat also nur genau zwei Untergruppen, nämlich die einelementige Untergruppe, die nur aus dem neutralen Element besteht, und die ganze Gruppe als Untergruppe von sich selbst. Die von einem Element, das nicht das neutrale Element ist, erzeugte Untergruppe muß also notwendig bereits die ganze Gruppe sein.  $\square$

**Korollar 4.4.3.8.** *Bei einer endlichen Gruppe  $G$  teilt die Ordnung jedes Elements  $g \in G$  die Ordnung der ganzen Gruppe und es gilt mithin*

$$g^{|G|} = 1$$

*Beweis.* Man wende den Satz von Lagrange 4.4.1.5 an auf die von unserem Element erzeugte Untergruppe. Es folgt, daß  $r := \text{ord } g = |\langle g \rangle|$  ein Teiler von  $|G|$  ist,  $|G| = ra$  mit  $a \in \mathbb{N}$ . Damit erhalten wir aber

$$g^{|G|} = g^{ra} = (g^r)^a = 1^a = 1$$

$\square$

**Korollar 4.4.3.9.** Ist  $p$  eine Primzahl, so gilt für alle ganzen Zahlen  $a \in \mathbb{Z}$  die **Fermat'sche Kongruenz**

$$a^p \equiv a \pmod{p}$$

*Beweis.* Die multiplikative Gruppe  $(\mathbb{Z}/p\mathbb{Z})^\times$  des Körpers  $\mathbb{Z}/p\mathbb{Z}$  hat genau  $p - 1$  Elemente, nach 4.4.3.8 gilt also  $b^{p-1} = 1$  für alle  $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ . Es folgt  $b^p = b$  für alle  $b \neq 0$ , und für  $b = 0$  gilt diese Gleichung eh. Mit  $b = a + p\mathbb{Z}$  ergibt sich dann die Behauptung.  $\square$

4.4.3.10. Gibt es natürliche Zahlen  $n \in \mathbb{N}$ , die

- bei Division durch 6 Rest 4 lassen,
- bei Division durch 13 Rest 2, und
- bei Division durch 11 Rest 9?

Da  $\langle 6, 13 \rangle = \langle 13, 11 \rangle = \langle 6, 11 \rangle = \langle 1 \rangle$  lautet die Antwort ja, wie man aus dem anschließenden Korollar 4.4.3.13 folgert.

**Satz 4.4.3.11.** Ist  $m = ab$  ein Produkt von zwei zueinander teilerfremden positiven natürlichen Zahlen, so liefert die Abbildung  $\kappa : n \mapsto (n + a\mathbb{Z}, n + b\mathbb{Z})$  einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

4.4.3.12. Übung 4.4.4.25 zeigt, daß die fraglichen Gruppen im Fall nicht teilerfremder Faktoren auch nicht isomorph sind.

*Beweis.* Der Kern unserer Abbildung

$$\begin{aligned} \kappa : \mathbb{Z} &\rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ n &\mapsto (n + a\mathbb{Z}, n + b\mathbb{Z}) \end{aligned}$$

besteht aus allen  $n \in \mathbb{Z}$ , die durch  $a$  und  $b$  teilbar sind, also aus allen Vielfachen von  $m$ . Unser Isomorphiesatz 4.4.2.12 liefert mithin einen Isomorphismus  $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \text{im } \kappa$ . Daraus folgt hinwiederum  $\text{im } \kappa = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ , da unsere Untergruppe  $\text{im } \kappa$  bereits selbst  $m = ab$  Elemente hat.  $\square$

**Korollar 4.4.3.13 (Chinesischer Restsatz).** Ist  $m = q_1 \dots q_s$  ein Produkt von paarweise teilerfremden ganzen Zahlen, so liefert die offensichtliche Abbildung einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_s\mathbb{Z}$$

*Beweis.* Das folgt induktiv aus dem in 4.4.3.11 behandelten Fall  $s = 2$ . Die Details mag der Leser als Übung selbst ausführen.  $\square$

*Ergänzung 4.4.3.14.* Ein Element endlicher Ordnung in einer Gruppe heißt ein **Torsionselement**. Eine Gruppe, in der alle Elemente außer dem neutralen Element unendliche Ordnung haben, heißt **torsionsfrei**. Zum Beispiel sind die abelschen Gruppen  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$  torsionsfrei. Die Menge aller Torsionselemente ist in jeder abelschen Gruppe  $A$  eine Untergruppe, die **Torsionsuntergruppe**  $A_{\text{tor}}$ . In der Tat folgt, wenn wir unsere Gruppe einmal additiv notieren, für  $x, y \in A$  aus  $nx = 0$  und  $my = 0$  bereits  $nm(x + y) = 0$ .

**Satz 4.4.3.15 (Primzahltorsion in abelschen Gruppen).** *Gegeben eine abelsche Gruppe  $A$  gilt:*

1. *Für jede Primzahl  $p$  ist die Teilmenge  $A(p)$  aller Elemente von  $p$ -Potenz-Ordnung eine Untergruppe;*
2. *Sind  $p_1, \dots, p_r$  paarweise verschiedene Primzahlen, so liefert das Verknüpfen einen injektiven Gruppenhomomorphismus*

$$A(p_1) \times \dots \times A(p_r) \hookrightarrow A$$

3. *Das Bild unseres Gruppenhomomorphismus aus Teil 2 besteht genau aus den Elementen von  $A$ , deren Ordnung endlich ist und von keinen von  $p_i$  verschiedenen Primzahlen geteilt wird.*

*Vorschau 4.4.3.16.* Dieser Satz wird sich in ?? ebenso wie der Satz 4.3.2.7 über die Direktheit der Summe der Hauträume als Spezialfall desselben allgemeinen Resultats zu „Moduln über Kringen“ erweisen.

*Beweis.* (1) Wir notieren unsere abelsche Gruppe  $A$  additiv. Gegeben  $x, y \in A$  der Ordnungen  $p^r$  und  $p^s$  liefert die Vorschrift  $(n, m) \mapsto nx + my$  einen Gruppenhomomorphismus  $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \rightarrow A$ . Offensichtlich landet er sogar in  $A(p)$  und sein Bild enthält  $x$  und  $y$ . Das zeigt die erste Behauptung.

(2) Es gilt zu zeigen, daß der Kern Null ist. Sei sonst  $(x_1, \dots, x_r)$  im Kern aber nicht Null. Ohne Beschränkung der Allgemeinheit dürfen wir  $x_1 \neq 0$  annehmen. die Gleichung

$$-x_1 = x_2 + \dots + x_r$$

zeigt dann  $(p_2 \dots p_r)^N x_1 = 0$  für hinreichend großes  $N$ , im Widerspruch zu unserer Annahme, daß die Ordnung von  $x_1$  eine Potenz von  $p_1$  sein soll.

(3) Es reicht, das für zyklische Torsionsgruppen zu zeigen. In diesem Fall folgt es aber unmittelbar aus dem chinesischen Restsatz.  $\square$

**Korollar 4.4.3.17 (Primzerlegung endlicher abelscher Gruppen).** *Sei  $E$  eine endliche abelsche Gruppe.*

1. Gegeben eine Primzahl  $p$  ist die Teilmenge  $E(p)$  aller Elemente, deren Ordnung eine  $p$ -Potenz ist, eine Untergruppe von  $p$ -Potenzordnung;
2. Sind  $p_1, \dots, p_r$  die paarweise verschiedenen Primzahlen, die in der Primfaktorzerlegung von  $|E|$  mindestens einmal vorkommen, so liefert die Verknüpfung einen Gruppenisomorphismus

$$E(p_1) \times \dots \times E(p_r) \xrightarrow{\sim} E$$

*Beweis.* Unser Korollar folgt unmittelbar aus Satz 4.4.3.15 über Primzahltorsion in abelschen Gruppen mit Ausnahme der Aussage, daß  $E(p)$  eine Gruppe von  $p$ -Potenzordnung ist. Das folgt aber für alle endlichen abelschen Gruppen, in denen jedes Element  $p$ -Potenzordnung hat, durch Induktion über die Gruppenordnung. Unser Korollar wird alternativ auch unmittelbar aus dem Klassifikationssatz für endlich erzeugte abelsche Gruppen 4.4.4.5 folgen.  $\square$

*Ergänzung 4.4.3.18 (Satz von Cauchy im abelschen Fall).* Teilt eine Primzahl  $p$  die Ordnung einer endlichen abelschen Gruppe  $E$ , so gibt es insbesondere in  $E$  ein Element der Ordnung  $p$ : In der Tat ist dann  $E(p)$  nicht trivial; es gibt darin also ein vom neutralen Element verschiedenes Element  $a$ ; dessen Ordnung ist etwa  $p^r$  mit  $r \geq 1$ ; und dann ist in additiver Notation  $p^{r-1}a$  das gesuchte Element der Ordnung  $p$ . Dieselbe Aussage gilt auch für beliebige endliche Gruppen und heißt der „Satz von Cauchy“, aber der Beweis ist dann schwieriger, vergleiche 4.5.1.35 oder ??.

## Übungen

*Ergänzende Übung 4.4.3.19 (Polynomfunktionen über endlichen Körpern).* Sei  $k$  ein endlicher Körper mit  $|k| = q$  Elementen. Man zeige  $a^q = a$  für alle  $a \in k$ . Man zeige weiter, daß der Kern unserer Surjektion  $k[X_1, \dots, X_n] \rightarrow \text{Ens}(k^n, k)$  aus 3.5.4.3 genau aus denjenigen Polynomen besteht, die sich als Summe  $P_1(X_1^q - X_1) + \dots + P_n(X_n^q - X_n)$  der Produkte von irgendwelchen Polynomen  $P_i \in k[X_1, \dots, X_n]$  mit den Polynomen  $(X_i^q - X_i)$  schreiben lassen. Hinweis: Unsere Summen von Produkten bilden einen Untervektorraum, zu dem der Untervektorraum aller Polynome, in denen kein  $X_i$  in der Potenz  $q$  oder höher vorkommt, komplementär ist.

*Übung 4.4.3.20 (Untergruppen zyklischer Gruppen).* Man zeige: Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer haben wir für beliebiges  $m \in \mathbb{N}$  eine Bijektion

$$\begin{aligned} \{\text{Teiler } d \in \mathbb{N} \text{ von } m\} &\xrightarrow{\sim} \{\text{Untergruppen von } \mathbb{Z}/m\mathbb{Z}\} \\ d &\mapsto d\mathbb{Z}/m\mathbb{Z} \end{aligned}$$

Man folgere, daß jede echte, als da heißt von der ganzen Gruppe verschiedene Untergruppe einer zyklischen Gruppe von Primzahlpotenzordnung  $\mathbb{Z}/p^r\mathbb{Z}$  in der Untergruppe  $p\mathbb{Z}/p^r\mathbb{Z} \subset \mathbb{Z}/p^r\mathbb{Z}$  enthalten sein muß. Hinweis: 3.4.3.4.

*Ergänzende Übung 4.4.3.21.* Man zeige: Jede endlich erzeugte Untergruppe von  $\mathbb{Q}$  ist zyklisch.

*Ergänzende Übung 4.4.3.22.* Man zeige, daß die additive Gruppe aller Gruppenhomomorphismen  $\text{Grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$  unter punktweiser Addition isomorph ist zu  $\mathbb{Z}/n\mathbb{Z}$ , für alle  $n \geq 1$ .

*Übung 4.4.3.23.* Man gebe alle Zahlen an, die bei Division durch 6 Rest 4 lassen, bei Division durch 13 Rest 2, und bei Division durch 11 Rest 9. Hinweis: Der euklidische Algorithmus liefert schon mal Lösungen, wenn ein Rest 1 ist und die anderen Null.

*Übung 4.4.3.24.* Man zeige, daß es in einer zyklischen Gruppe der Ordnung  $n$  genau dann Elemente der Ordnung  $d$  gibt, wenn  $d$  ein Teiler von  $n$  ist.

*Übung 4.4.3.25.* Gibt es ein Vielfaches von 17, dessen letzten Ziffern 39 lauten?

*Ergänzende Übung 4.4.3.26.* Gegeben  $x, y$  zwei Elemente endlicher Ordnung in einer abelschen Gruppe  $G$  teilt die Ordnung ihres Produkts das kleinste gemeinsame Vielfache ihrer Ordnungen, und sind die Ordnungen von  $x$  und  $y$  teilerfremd, so gilt sogar  $\text{ord}(xy) = (\text{ord } x)(\text{ord } y)$ .

*Ergänzende Übung 4.4.3.27.* In jeder endlichen abelschen Gruppe wird die maximal von einem Gruppenelement erreichte Ordnung geteilt von den Ordnungen aller Gruppenelemente. Hinweis: Bezeichnet  $M \subset \mathbb{N}$  die Menge aller Ordnungen von Elementen unserer Gruppe, so enthält  $M$  mit jeder Zahl auch alle ihre Teiler. Weiter enthält  $M$  nach 4.4.3.26 mit je zwei teilerfremden Zahlen auch ihr Produkt.

*Übung 4.4.3.28 (Verallgemeinerte Fermat'sche Kongruenz).* Gegeben Primzahlen  $p_1, \dots, p_r$  und eine Zahl  $e$  mit  $e \equiv 1 \pmod{(p_i - 1)}$   $\forall i$  zeige man für alle  $a \in \mathbb{Z}$  die Kongruenz  $a^e \equiv a \pmod{(p_1 \dots p_r)}$ . Hinweis: Man folgere das zunächst im Fall  $r = 1$  aus dem Kleinen Fermat. Für den allgemeinen Fall kombiniere man den Chinesischen Restsatz mit dem Kleinen Fermat.

*Ergänzung 4.4.3.29 (Verschlüsselung nach dem RSA-Verfahren).* Ich will versuchen, das sogenannte **RSA-Verfahren** nach Rivest, Shamir und Adleman zum öffentlichen Vereinbaren geheimer Schlüssel anhand des folgenden Schemas zu erklären.

| Geheimbereich Alice  | Öffentlicher Bereich             | Geheimbereich Bob   |
|--|----------------------------------|---|
| Alice wählt zwei große Primzahlen $p, q$ und berechnet das Produkt $N = pq$ . Sie wählt Zahlen $s, t \in \mathbb{N}$ mit $st \equiv 1 \pmod{(p-1)(q-1)}$ . Sie macht $N$ und $t$ öffentlich. |                                  |   |
|  | $N, t$                           |   |
|  |                                  | Bob wählt eine Restklasse $a \in \mathbb{Z}/N\mathbb{Z}$ , berechnet $a^t$ , und macht es öffentlich. |
|  | $a^t \in \mathbb{Z}/N\mathbb{Z}$ |   |
| Alice berechnet $(a^t)^s = a$ .  |                                  |   |

Die Restklasse  $a \in \mathbb{Z}/N\mathbb{Z}$  ist dann der gemeinsame geheime Schlüssel. Die behauptete Gleichheit von Restklassen  $(a^t)^s = a$  prüft man mit Hilfe des Ringisomorphismus

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

In  $\mathbb{Z}/p\mathbb{Z}$  haben wir ja  $a^x = a$  wann immer gilt  $x \equiv 1 \pmod{p-1}$ . In  $\mathbb{Z}/q\mathbb{Z}$  haben wir ebenso  $a^x = a$  wann immer gilt  $x \equiv 1 \pmod{q-1}$ . Falls beides gilt und erst recht falls gilt  $x \equiv 1 \pmod{(p-1)(q-1)}$  haben wir also  $a^x = a$  in  $\mathbb{Z}/N\mathbb{Z}$ . Diese Identität ist ein Spezialfall unserer verallgemeinerten Fermat'schen Kongruenz 4.4.3.28. Der Trick beim RSA-Verfahren besteht darin, daß alle derzeit bekannten Verfahren zum Faktorisieren einer großen Zahl wie  $N$  sehr viel Rechenzeit brauchen. Es ist also möglich,  $N$  zu veröffentlichen und dennoch  $p, q$  geheim zu halten, die hinwiederum für die Berechnung von  $s$  benötigt werden. Des weiteren braucht es mit allen derzeit bekannten Verfahren auch sehr viel Rechenzeit, um aus  $a^t$  auf  $a$  zurückzuschließen, also eine „ $t$ -te Wurzel modulo  $N$ “ zu finden.

#### 4.4.4 Endlich erzeugte abelsche Gruppen

**Proposition 4.4.4.1.** *Jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt, und für die Untergruppe benötigt man höchstens soviele Erzeuger wie für die ganze Gruppe.*

*Ergänzung 4.4.4.2.* Eine Untergruppe einer nicht abelschen endlich erzeugten Gruppe muß im allgemeinen keineswegs endlich erzeugt sein. Ein Beispiel geben wir in ??.

*Beweis.* Induktion über die Zahl der Erzeuger. Im Fall einer zyklischen Gruppe wissen wir nach 4.4.3.20 oder eigentlich 3.4.3.4 bereits, daß auch jede Untergruppe zyklisch ist. Sei nun unsere Gruppe  $X$  additiv notiert und sei  $x_0, \dots, x_n$  ein Erzeugendensystem. Sei  $Y \subset X$  eine Untergruppe. Nach 4.4.3.20 ist  $Y \cap \langle x_0 \rangle$  zyklisch, etwa erzeugt von  $y_0$ . Nach Induktionsannahme ist das Bild von  $Y$  in  $X/\langle x_0 \rangle$  endlich erzeugt, etwa von den Nebenklassen  $\bar{y}_1, \dots, \bar{y}_n$  gewisser Elemente  $y_1, \dots, y_n \in Y$ . Der Leser wird nun in Anlehnung an den Beweis von 3.2.2.6 unschwer zeigen können, daß  $y_0, y_1, \dots, y_n$  bereits ganz  $Y$  erzeugen.  $\square$

4.4.4.3. Unter einer **Primzahlpotenz** oder kurz **Primpotenz** verstehen wir eine natürliche Zahl der Gestalt  $q = p^e$  für  $p$  prim und  $e \geq 0$ . Unter einer **echten Primzahlpotenz** verstehen wir eine von 1 verschiedene Primzahlpotenz. Gegeben eine Primzahl  $p$  verstehen wir unter einer  **$p$ -Potenz** eine natürliche Zahl der Gestalt  $q = p^e$  für  $p$  prim und  $e \geq 0$ . Die beiden folgenden Sätze geben zwei **Klassifikationen der endlich erzeugten abelschen Gruppen**.

**Satz 4.4.4.4 (Klassifikation durch Teilerfolgen).** *Für jede endlich erzeugte abelsche Gruppe  $X$  gibt es genau ein  $s \geq 0$  und ein  $s$ -Tupel von von 1 verschiedenen natürlichen Zahlen  $(a_1, \dots, a_s) \in \{0, 2, 3, \dots\}^s$  mit  $a_i | a_{i+1}$  für  $1 \leq i < s$  derart, daß gilt*

$$X \cong \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_s\mathbb{Z}$$

**Satz 4.4.4.5 (Klassifikation durch Rang und Primzahlpotenzen).** *Für jede endlich erzeugte abelsche Gruppe  $X$  gibt es echte Primzahlpotenzen  $q_1, \dots, q_t$  und eine natürliche Zahl  $r \in \mathbb{N}$  mit*

$$X \cong \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_t\mathbb{Z} \times \mathbb{Z}^r$$

*Die Zahl  $r$  wird durch  $X$  eindeutig festgelegt und heißt der **Rang** von  $X$ . Wir notieren sie  $r = \text{rang}(X)$ . Die Primzahlpotenzen  $q_\tau$  sind eindeutig bis auf Reihenfolge.*

**Vorschau 4.4.4.6.** Die zweite Klassifikation wird sich in ?? zusammen mit der Jordan'schen Normalform als Spezialfall derselben Klassifikation von „Moduln über Hauptidealringen“ erweisen. Auch die erste Klassifikation läßt sich in dieser Allgemeinheit formulieren und beweisen, vergleiche ??.

4.4.4.7. Es wird im zweiten Satz nicht gefordert, daß die Primzahlpotenzen paarweise verschieden sein sollen. Ich erinnere daran, daß wir in 2.1.6.8 eine Multimenge von Elementen einer Menge  $P$  erklärt hatten als eine Abbildung  $P \rightarrow \mathbb{N}$ . In diesem Sinne werden also die endlich erzeugten abelschen Gruppen klassifiziert durch ihren Rang, eine natürliche Zahl, zusammen mit einer endlichen Multimenge von echten Primzahlpotenzen.

**4.4.4.8 (Übergang zwischen beiden Klassifikationen).** Um von der Darstellung im ersten Klassifikationssatz zu der im Zweiten überzugehen, kann man sich auf den Fall endlicher Gruppen beschränken, indem man die Nullen an der Ende der Folge der  $a_i$  abschneidet, die eben für den Faktor  $\mathbb{Z}^r$  verantwortlich sind. Die anderen  $a_i$  zerlegt man in ein Produkt von echten Primzahlpotenzen, und die zugehörigen Faktoren  $\mathbb{Z}/a_i\mathbb{Z}$  zerfallen dann nach dem chinesischen Restsatz entsprechend in ein Produkt zyklischer Gruppen von Primzahlpotenzordnung. Um von der Darstellung im zweiten Klassifikationssatz zu der im Ersten überzugehen, kann man sich wieder auf den Fall endlicher Gruppen beschränken. Gegeben ein Produkt zyklischer Gruppen von Primzahlpotenzordnung betrachtet man zunächst von jeder dabei auftauchenden Primzahl die höchste jeweils vorkommende Potenz und multipliziert diese zusammen: Das gibt  $a_s$ . Dann streicht man alle „verbrauchten“ Potenzen und macht genauso weiter.

**Korollar 4.4.4.9.** *Jede endliche abelsche Gruppe ist ein endliches Produkt von zyklischen Gruppen von Primzahlpotenzordnung, und die dabei auftretenden echten Primzahlpotenzen und ihre Vielfachheiten sind wohlbestimmt bis auf Reihenfolge. In Formeln erhalten wir so eine Bijektion*

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{Endliche Multimengen} \\ \text{von echten Primzahlpotenzen} \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{l} \text{Endliche abelsche Gruppen} \\ \text{bis auf Isomorphismus} \end{array} \right\} \\ {}_\mu\{q_1, q_2, \dots, q_t\} & \mapsto & \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \dots \times \mathbb{Z}/q_t\mathbb{Z} \end{array}$$

**4.4.4.10.** Man beachte bei den vorhergehenden Sätzen, daß die Faktoren keineswegs eindeutig sind „als Untergruppen unserer abelschen Gruppe“. Partielle Eindeutigkeitsaussagen liefern 4.4.3.15 und 4.4.3.17. Die Beweise werden uns bis zum Ende des Abschnitts beschäftigen. Eine erste wesentliche Zutat ist der gleich folgende Elementarteilersatz 4.4.4.13.

**Beispiel 4.4.4.11.** Die Gruppen  $(\mathbb{Z}/9\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$  und  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  sind nicht isomorph, denn sie entsprechen den beiden unterschiedlichen Multimengen von Primzahlpotenzen  ${}_\mu\{9, 9, 4\}$  und  ${}_\mu\{3, 27, 4\}$  oder alternativ den beiden unterschiedlichen Teilerfolgen  $9|36$  und  $3|108$ . Man kann das aber auch ohne alle Theorie unschwer einsehen: Die zweite Gruppe enthält Elemente der Ordnung 27, die erste nicht. Der Beweis, daß die explizit angegebenen Gruppen in unseren Klassifikationssätzen jeweils paarweise nicht isomorph sind, verfeinert diese Grundidee.

**4.4.4.12 (Endlich erzeugte torsionsfreie abelsche Gruppen).** Jede endlich erzeugte torsionsfreie abelsche Gruppe ist nach jeder unserer beiden Klassifikationen 4.4.4.4 und 4.4.4.5 isomorph zu  $\mathbb{Z}^r$  für genau ein  $r \in \mathbb{N}$ .

- Satz 4.4.4.13 (Elementarteilersatz).**
1. Gegeben eine nicht notwendig quadratische Matrix  $A$  mit ganzzahligen Einträgen gibt es stets quadratische ganzzahlig invertierbare Matrizen mit ganzzahligen Einträgen  $P$  und  $Q$  derart, daß  $B := PAQ$  eine Matrix mit Nullen außerhalb der Diagonalen ist, in der die Diagonaleinträge weiter vorn jeweils die Diagonaleinträge weiter hinten teilen, in Formeln  $i \neq j \Rightarrow B_{i,j} = 0$  und  $B_{i,i}|B_{i+1,i+1} \forall i$ ;
  2. Wir können durch geeignete Wahl von  $P$  und  $Q$  sogar zusätzlich erreichen, daß alle Diagonaleinträge nichtnegativ sind, und unter dieser Zusatzannahme werden besagte Diagonaleinträge durch die Matrix  $A$  bereits eindeutig festgelegt.

4.4.4.14. Ich nenne die Multimenge der Diagonaleinträge von  $B$  die Multimenge der **Elementarteiler der Matrix  $A$** . Den Beweis der analogen Aussage für Polynomringe dürfen Sie selbst als Übung 4.4.4.30 ausarbeiten. Eine gemeinsame Verallgemeinerung für sogenannte „Hauptidealringe“ wird in ?? dargestellt.

*Beweis.* Wir beginnen mit dem Nachweis der Existenz. Ist  $A$  die Nullmatrix, so ist nichts zu zeigen. Sonst finden wir  $P, Q$  invertierbar derart, daß  $PAQ$  oben links einen positiven Eintrag hat. Es gibt dann natürlich auch  $P_{\min}, Q_{\min}$  derart, daß  $P_{\min}AQ_{\min}$  den kleinstmöglichen positiven Eintrag hat unter allen  $PAQ$  mit positivem Eintrag dort. Dann teilt dieser Eintrag notwendig alle anderen Einträge der ersten Spalte, da wir sonst durch Zeilenoperationen, genauer durch Subtraktion eines Vielfachen der ersten Zeile von einer anderen Zeile, Multiplikation einer Zeile mit  $-1$  und Vertauschung zweier Zeilen, einen noch kleineren positiven Eintrag oben links erzeugen könnten. Ebenso teilt unser Eintrag auch alle anderen Einträge in der ersten Zeile. Durch entsprechende Zeilen- und Spaltenoperationen können wir also zusätzlich die erste Zeile und Spalte bis auf den ersten Eintrag als genüllt annehmen. Teilt nun unser positiver Eintrag oben links nicht alle anderen Einträge unserer Matrix, sagen wir nicht den Eintrag  $a_{i,j}$  mit  $i \neq 1 \neq j$ , so könnten wir durch Addieren der ersten Zeile zur  $i$ -ten Zeile gefolgt von einer Subtraktion eines Vielfachen der ersten Spalte von der  $j$ -ten Spalte einen noch kleineren positiven Eintrag an der Stelle  $(i, j)$  erzeugen, und ihn durch Zeilen- und Spaltenvertauschung in die linke obere Ecke bringen im Widerspruch zu unserer Annahme. Also teilt unser positiver Eintrag oben links alle anderen Einträge unserer Matrix und eine offensichtliche Induktion beendet den Beweis der Existenz. Um die Eindeutigkeit zu zeigen, betrachten wir für jedes  $r$  die sogenannten  **$r$ -Minoren** unserer Matrix. Man versteht darunter die Determinanten aller derjenigen  $(r \times r)$ -Matrizen, die wir aus unserer Matrix durch das Streichen von Zeilen und Spalten erhalten können. Dann bemerken wir, daß sich für gegebenes  $r \geq 1$  der größte gemeinsame Teiler  $G_r$  aller  $(r \times r)$ -Minoren unter Zeilen- und Spal-

$$\begin{pmatrix} 8 & 6 & 4 & 8 \\ 18 & 16 & 24 & 38 \\ 16 & 12 & 8 & 16 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 8 & 6 & 4 & 8 \\ 10 & 10 & 20 & 30 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$



$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 10 & 20 & 30 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 6 & 4 & 8 \\ 0 & 10 & 20 & 30 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$



$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Berechnung der Elementarteiler einer ganzzahligen Matrix durch ganzzahlige ganzzahlig invertierbare Zeilen- und Spaltenoperationen. Wir finden die Elementarteiler 2, 10, 0 jeweils mit der Vielfachheit Eins.

tenoperationen nicht ändert. Folglich sind die  $G_r = d_1 \dots d_r$  wohlbestimmt durch  $A$ , und dasselbe gilt dann auch für die  $d_i$ .  $\square$

**4.4.4.15 (Herkunft der Terminologie).** Der Begriff der „Minoren einer Matrix“ wurde meines Wissens in einer Arbeit von Arthur Cayley in Crelles Journal im Jahre 1855, Band 50, Seite 282, mit dem Titel „Sept différents mémoires d’analyse. No 3: Remarques sur la notation des fonctions algébriques“ eingeführt. Cayley war mit Sylvester befreundet, auf den wie bereits in 3.1.1.12 erwähnt die Verwendung des Begriffs einer „Matrix“ in der Mathematik zurückgeht.

*Beweis der Klassifikationen 4.4.4.4 und 4.4.4.5.* Wir notieren die abelsche Gruppe  $X$  im folgenden additiv. Gegeben ein Erzeugendensystem  $x_1, \dots, x_n$  von  $X$  erklären wir durch die Vorschrift  $(a_1, \dots, a_n) \mapsto a_1x_1 + \dots + a_nx_n$  einen surjektiven Gruppenhomomorphismus

$$\mathbb{Z}^n \twoheadrightarrow X$$

Dessen Kern ist nach 4.4.4.1 wieder eine endlich erzeugte abelsche Gruppe  $K$ , für die wir wieder einen surjektiven Gruppenhomomorphismus  $\mathbb{Z}^m \twoheadrightarrow K$  finden können. Mit der Notation  $\psi$  für die Komposition  $\mathbb{Z}^m \twoheadrightarrow K \hookrightarrow \mathbb{Z}^n$  erhalten wir also einen Isomorphismus abelschen Gruppen

$$\mathbb{Z}^n / \text{im } \psi \cong X$$

Genau wie bei Vektorräumen überlegt man sich, daß die Gruppenhomomorphismen  $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$  genau die Multiplikationen von links mit ganzzahligen  $(n \times m)$ -Matrizen sind, falls Elemente aus  $\mathbb{Z}^m$  beziehungsweise  $\mathbb{Z}^n$  als Spaltenvektoren aufgefaßt werden, vergleiche 4.4.2.26. Weiter überlegt man sich, daß auch in dieser Situation die Verknüpfung von Homomorphismen der Multiplikation von Matrizen entspricht. Bezeichnet nun  $A$  die Matrix unserer Abbildung  $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$ , und wählen wir  $P$  und  $Q$  wie im Elementarteilersatz, so ergibt sich ein kommutatives Diagramm von abelschen Gruppen

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{A} & \mathbb{Z}^n \\ Q \uparrow \wr & & P \downarrow \wr \\ \mathbb{Z}^m & \xrightarrow{D} & \mathbb{Z}^n \end{array}$$

für eine nicht notwendig quadratische Diagonalmatrix  $D$  mit nichtnegativen Einträgen  $d_1|d_2| \dots |d_r$  für  $r = \min(m, n)$ . In anderen Worten bildet der Gruppenisomorphismus  $P : \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^n$  in dieser Situation  $\text{im } \psi = \text{im } A$  bijektiv auf  $\text{im } D$  ab und wir erhalten Isomorphismen

$$X \cong \mathbb{Z}^n / \text{im } \psi = \mathbb{Z}^n / \text{im } A \cong \mathbb{Z}^n / \text{im } D$$

Für die Diagonalmatrix  $D$  mit Diagonaleinträgen  $d_i$  ist aber klar, daß  $\mathbb{Z}^n / \text{im } D$  isomorph ist zu einem Produkt der Gruppen  $\mathbb{Z}/d_i\mathbb{Z}$  mit soviel Kopien von  $\mathbb{Z}$ , wie es in unserer Matrix  $D$  mehr Spalten als Zeilen gibt, also mit  $(n - r)$  Kopien von  $\mathbb{Z}$ . Formaler kann das auch mit dem allgemeinen Resultat 4.4.6.13 begründet werden, nach dem „Produkte exakter Sequenzen wieder exakt sind“. Lassen wir von unserer Folge  $d_1|d_2|\dots|d_r$  nun alle Einsen vorne weg und ergänzen am Ende  $(n - r)$  Nullen, so erhalten wir eine Folge  $a_1|\dots|a_s$  wie in der Klassifikation durch Teilerfolgen 4.4.4.4 gefordert, und die Existenz dort ist gezeigt. Mit dem Chinesischen Restsatz 4.4.3.13 folgt dann auch sofort die Existenzaussage der Klassifikation durch Primzahlpotenzen 4.4.4.5. Um die Eindeutigkeit in unseren Klassifikationen zu zeigen bemerken wir, daß für jede endlich erzeugte abelsche Gruppe  $X$  und jede Primzahl  $p$  und alle  $n \geq 1$  der Quotient  $p^{n-1}X/p^nX$  nach 3.5.2.44 ein endlichdimensionaler Vektorraum über  $\mathbb{F}_p$  ist. Wir notieren seine Dimension

$$D_p^n(X) := \dim_{\mathbb{F}_p}(p^{n-1}X/p^nX)$$

Alternativ mag man  $D_p^n(X)$  auch als die eindeutig bestimmte natürliche Zahl  $D \in \mathbb{N}$  mit  $|p^{n-1}X/p^nX| = p^D$  charakterisieren. Man sieht nun leicht oder folgt formal mit 4.4.6.13 die Formel  $D_p^n(X \times Y) = D_p^n(X) + D_p^n(Y)$  für je zwei endlich erzeugte abelsche Gruppen  $X$  und  $Y$ . Für zyklische Gruppen  $X \cong \mathbb{Z}/a\mathbb{Z}$  finden wir schließlich

$$D_p^n(\mathbb{Z}/a\mathbb{Z}) = \begin{cases} 1 & \text{falls } p^n \text{ teilt } a; \\ 0 & \text{sonst.} \end{cases}$$

In der Tat ist das klar für  $a = p^m$ , für  $a$  teilerfremd zu  $p$  ist es eh klar, und mit dem Chinesischen Restsatz 4.4.3.11 folgt es im allgemeinen. Für jede Zerlegung  $X \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_t\mathbb{Z}$  finden wir also

$$D_p^n(X) = |\{i \mid p^n \text{ teilt } d_i\}|$$

Für  $X \cong \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_t\mathbb{Z}$  wie in 4.4.4.5 finden wir insbesondere mit den Notationen von dort

$$D_p^n(X) = r + |\{i \mid p^n \text{ teilt } q_i\}|$$

Wenden wir diese Erkenntnis an auf alle Primzahlen  $p$ , so folgt die im Satz behauptete Eindeutigkeit ohne weitere Schwierigkeiten: Wir erhalten genauer für jede Primzahl  $p$  und jedes  $n \geq 1$  die nur von unserer Gruppe abhängenden Darstellungen  $|\{i \mid q_i = p^n\}| = D_p^n(X) - D_p^{n+1}(X)$  und  $r = \lim_{n \rightarrow \infty} D_p^n(X)$  für die Zahl der zyklischen Faktoren von vorgegebener Primzahlpotenzordnung und den Rang  $r$  des freien Anteils. Die Eindeutigkeit in 4.4.4.4 hinwiederum kann man leicht aus der Eindeutigkeit in 4.4.4.5 folgern: Verschiedene Teilerfolgen führen offensichtlich zu verschiedenen Multimengen von echten Primzahlpotenzen oder verschiedenen Rängen.  $\square$

**Definition 4.4.4.16.** Gegeben eine Gruppe  $G$  heißt die kleinste Zahl  $e \geq 1$  mit  $g^e = 1 \quad \forall g \in G$  der **Exponent** unserer Gruppe. Gibt es kein solches  $e$ , so sagen wir, die Gruppe habe unendlichen Exponenten.

**Satz 4.4.4.17 (Endliche Gruppen von Einheitswurzeln).** *Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.*

4.4.4.18. Die Elemente  $\zeta$  endlicher Ordnung in der multiplikativen Gruppe eines Körpers sind per definitionem genau diejenigen Elemente, die eine Gleichung der Gestalt  $\zeta^n = 1$  erfüllen. Man nennt sie deshalb auch die **Einheitswurzeln** des Körpers.

*Beispiel 4.4.4.19.* Um uns auf den gleich folgenden Beweis einzustimmen zeigen wir zunächst beispielhaft, daß jede 18-elementige Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist. Nach 4.4.4.4 muß unsere Gruppe ja isomorph sein zu genau einer der beiden Gruppen  $\mathbb{Z}/18\mathbb{Z}$  und  $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . Es gilt also nur, die zweite Möglichkeit auszuschließen. Im zweiten Fall gäbe es jedoch in unserer Gruppe 8 Elemente der Ordnung drei und 9 Elemente, deren Ordnung drei teilt, und das steht im Widerspruch dazu, daß das Polynom  $X^3 - 1$  in unserem Körper höchstens drei Nullstellen haben kann.

*Beweis.* In jeder endlichen kommutativen Gruppe wird die maximale von einem Gruppenelement erreichte Ordnung  $n$  geteilt von den Ordnungen aller Gruppenelemente, zum Beispiel nach dem Klassifikationssatz 4.4.4.4 oder direkter nach Übung 4.4.3.27. Wäre eine endliche Untergruppe  $E$  der multiplikativen Gruppe eines Körpers nicht zyklisch, so gäbe es also  $n < |E|$  mit  $\zeta^n = 1 \quad \forall \zeta \in E$  im Widerspruch dazu, daß das Polynom  $X^n - 1$  in unserem Körper höchstens  $n$  Nullstellen haben kann.  $\square$

*Ergänzung 4.4.4.20 (Nichtspalten der Einbettung der Torsionsuntergruppe).* Gegeben eine abelsche Gruppe  $A$  bilden die Elemente endlicher Ordnung nach 4.4.3.14 stets eine Untergruppe  $A_{\text{tor}} \subset A$  und der Quotient  $A/A_{\text{tor}}$  ist offensichtlich torsionsfrei. Allerdings gibt es im Gegensatz zum Fall endlich erzeugter abelscher Gruppen im allgemeinen keinen Gruppenisomorphismus zwischen  $A$  und  $A_{\text{tor}} \times (A/A_{\text{tor}})$ . Betrachten wir etwa in der Gruppe  $A$  aller Folgen  $a_n$  mit  $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ , die wir später einmal  $A = \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$  notieren, das Element

$$v = (\overline{p^0}, 0, \overline{p^1}, 0, \overline{p^2}, 0, \dots),$$

So ist  $v$  kein Torsionselement und seine Nebenklasse  $\bar{v} \in A/A_{\text{tor}}$  ist folglich nicht Null und für alle  $i \geq 0$  gibt es  $w = w_i \in A/A_{\text{tor}}$  mit  $p^i w = v$ . Das einzige Element von  $A$ , das in dieser Weise „durch alle  $p$ -Potenzen teilbar ist“, ist jedoch die Null. Folglich existiert kein Gruppenisomorphismus zwischen  $A$  und  $A_{\text{tor}} \times (A/A_{\text{tor}})$ . Dies Beispiel ist im übrigen eine Variation von 4.3.2.21.

## Übungen

*Übung 4.4.4.21.* Sei  $k$  ein Körper. Die Matrizen vom Rang  $< r$  in  $\text{Mat}(m \times n; k)$  sind genau die Matrizen, bei denen alle  $r$ -Minoren verschwinden.

*Ergänzende Übung 4.4.4.22.* Der Rang einer endlich erzeugten abelschen Gruppe  $X$  kann beschrieben werden als die Dimension des  $\mathbb{Q}$ -Vektorraums  $\text{Grp}(X, \mathbb{Q})$  aller Gruppenhomomorphismen von  $X$  nach  $\mathbb{Q}$ , mit seiner Vektorraumstruktur als Teilraum des  $\mathbb{Q}$ -Vektorraums  $\text{Ens}(X, \mathbb{Q})$ .

*Ergänzende Übung 4.4.4.23.* Man gebe ein dreielementiges bezüglich Inklusion minimales Erzeugendensystem der Gruppe  $\mathbb{Z}$  an.

*Übung 4.4.4.24 (Untergruppen freier endlich erzeugter abelscher Gruppen).* Gegeben eine Untergruppe  $U \subset \mathbb{Z}^n$  gibt es stets einen Automorphismus  $\varphi$  von  $\mathbb{Z}^n$  und  $0 \leq r \leq n$  und positive natürliche Zahlen  $d_1 | d_2 | \dots | d_r$  mit  $\varphi(U) = \langle d_1 e_1, d_2 e_2, \dots, d_r e_r \rangle$ . Eine analoge Aussage für Polynomringe in einer Veränderlichen mögen Sie selber formulieren und beweisen. Eine gemeinsame Verallgemeinerung für „Hauptidealringe“ diskutieren wir in ??.

*Ergänzende Übung 4.4.4.25.* Gegeben  $a, b \in \mathbb{N}_{\geq 1}$  gibt es einen Gruppenisomorphismus  $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$  genau dann, wenn  $a$  und  $b$  teilerfremd sind.

*Ergänzende Übung 4.4.4.26.* Man zeige, daß für jede nichttriviale zyklische Gruppe gerader Ordnung  $2n$  in additiver Notation die Multiplikation mit  $n$  als Bild die einzige Untergruppe mit zwei Elementen hat und als Kern die einzige Untergruppe vom Index Zwei. Des weiteren zeige man, daß es nur einen surjektiven Gruppenhomomorphismus von unserer zyklischen Gruppe gerader Ordnung auf „die“ zweielementige Gruppe gibt.

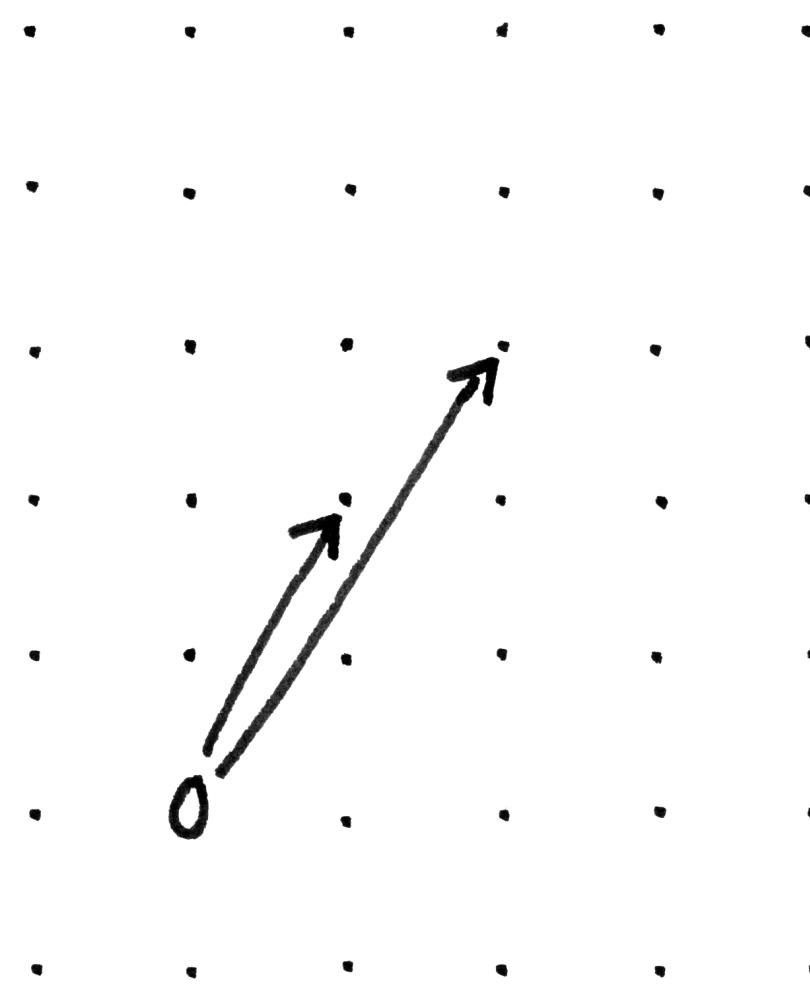
*Ergänzende Übung 4.4.4.27.* Man berechne die Elementarteiler der Matrix

$$\begin{pmatrix} 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 \\ 5 & 5 & 5 & 5 \end{pmatrix}$$

*Ergänzende Übung 4.4.4.28.* Man zeige, daß jede von Null verschiedene Zeilensmatrix als einzigen Elementarteiler den größten gemeinsamen Teiler der Matrixeinträge hat.

*Ergänzende Übung 4.4.4.29.* Sind  $a, b \in \mathbb{Z}$  teilerfremd, in Formeln  $\langle a, b \rangle = \langle 1 \rangle$ , so läßt sich das Element  $(a, b) \in \mathbb{Z}^2$  ergänzen zu einem Erzeugendensystem von  $\mathbb{Z}^2$ . Man formuliere und zeige auch die analoge Aussage für  $\mathbb{Z}^n$ .

*Ergänzende Übung 4.4.4.30 (Smith-Zerlegung).* Gegeben eine nicht notwendig quadratische Matrix  $A$  mit Einträgen im Polynomring  $k[X]$  mit Koeffizienten in



Ein Erzeugendensystem von  $\mathbb{Z}^2$

einem Körper  $k$  zeige man: (1) Es gibt quadratische im Matrizenring über  $k[X]$  invertierbare Matrizen mit polynomialem Einträgen  $P$  und  $Q$  derart, daß  $B = PAQ$  eine Matrix mit Nullen außerhalb der Diagonalen ist, in der die Diagonaleinträge weiter vorn jeweils die Diagonaleinträge weiter hinten teilen, in Formeln  $i \neq j \Rightarrow B_{i,j} = 0$  und  $B_{i,i}|B_{i+1,i+1} \forall i$ ; (2) Wir können durch geeignete Wahl von  $P$  und  $Q$  sogar zusätzlich erreichen, daß alle von Null verschiedenen Diagonaleinträge normiert sind, und unter dieser Zusatzannahme werden besagte Diagonaleinträge durch die Matrix  $A$  bereits eindeutig festgelegt.

*Vorschau 4.4.4.31.* Die Smith-Zerlegung aus der vorhergehenden Übung wird sich in ?? als ein Spezialfall des „Elementarteilersatzes für Hauptidealringe“ erweisen. Die Smith-Zerlegung ist der Schlüssel zum vertieften Verständnis der Jordan'schen Normalform und liefert auch Verallgemeinerungen über nicht notwendig algebraisch abgeschlossenen Körpern, vergleiche etwa ?? folgende.

*Übung 4.4.4.32 (Einheitengruppen von Restklassenringen).* Nach dem chinesischen Restsatz kennen wir die Einheitengruppen  $(\mathbb{Z}/m\mathbb{Z})^\times$ , sobald wir sie für jede Primzahlpotenz  $m$  kennen. In dieser Übung sollen sie zeigen:

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ ist eine ungerade Primzahl, } r \geq 1; \\ \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2, r \geq 2. \end{cases}$$

Man beachte, daß hier links die Multiplikation als Verknüpfung zu verstehen ist, rechts dahingegen die Addition. Hinweis: Nach 4.4.4.17 ist  $(\mathbb{Z}/p\mathbb{Z})^\times$  stets zyklisch. Bei ungeradem  $p$  gehe man von der Abbildung  $(\mathbb{Z}/p^r\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$  aus und zeige, daß sie surjektiv ist und daß die Restklasse von  $1 + p$  den Kern erzeugt. Dazu beachte man, daß für alle  $b \in \mathbb{Z}$  und  $n \geq 1$  gilt  $(1 + p^n + bp^{n+1})^p \in 1 + p^{n+1} + p^{n+2}\mathbb{Z}$ . Dann beachte man, daß diese Formel unter der stärkeren Annahme  $n \geq 2$  auch für  $p = 2$  gilt, und folgere, daß der Kern der Abbildung  $(\mathbb{Z}/2^r\mathbb{Z})^\times \rightarrow (\mathbb{Z}/4\mathbb{Z})^\times$  für  $r \geq 2$  von der Restklasse von 5 erzeugt wird. In diesem Fall kann eine Spaltung unserer Abbildung leicht explizit angegeben werden.

*Übung 4.4.4.33.* Gibt es eine Potenz von 17, deren Dezimaldarstellung mit den Ziffern 37 endet?

*Übung 4.4.4.34 (Primitivwurzeln in Restklassenringen).* Man zeige, daß für  $m \geq 2$  die Einheitengruppe  $(\mathbb{Z}/m\mathbb{Z})^\times$  des Restklassenrings  $\mathbb{Z}/m\mathbb{Z}$  zyklisch ist genau dann, wenn  $m$  eine Potenz einer ungeraden Primzahl oder das Doppelte einer Potenz einer ungeraden Primzahl oder Zwei oder Vier ist. Hinweis: Man beachte 4.4.4.32, den chinesischen Restsatz 4.4.3.11, und die Tatsache, daß eine zyklische Gruppe nie  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  als Quotienten haben kann. Ein Erzeuger der Einheitengruppe  $(\mathbb{Z}/m\mathbb{Z})^\times$  heißt im übrigen auch eine **Primitivwurzel modulo  $m$**  und die vorhergehende Aussage darüber, modulo welcher natürlichen Zahlen  $m$  Primitivwurzeln existieren, wird als der **Satz von Euler** zitiert. Bis heute (2011)

ungelöst ist die **Vermutung von Artin**, nach der die 2 modulo unendlich vieler Primzahlen eine Primitivwurzel sein sollte.

*Ergänzende Übung 4.4.4.35.* Eine Untergruppe eines endlichdimensionalen  $\mathbb{Q}$ -Vektorraums heißt ein  **$\mathbb{Z}$ -Gitter**, wenn sie von einer Basis unseres  $\mathbb{Q}$ -Vektorraums erzeugt wird. Man zeige: Eine endlich erzeugte Untergruppe eines endlichdimensionalen  $\mathbb{Q}$ -Vektorraums ist ein  $\mathbb{Z}$ -Gitter genau dann, wenn sie besagten Vektorraum als  $\mathbb{Q}$ -Vektorraum erzeugt. Ist  $\Gamma \subset V$  ein  $\mathbb{Z}$ -Gitter eines endlichdimensionalen  $\mathbb{Q}$ -Vektorraums und  $\varphi : V \rightarrow W$  eine surjektive lineare Abbildung, so ist  $\varphi(\Gamma)$  ein  $\mathbb{Z}$ -Gitter in  $W$ . Ist  $U \subset V$  ein Untervektorraum, so ist  $U \cap \Gamma$  ein  $\mathbb{Z}$ -Gitter in  $U$ .

*Übung 4.4.4.36 (Klassifikation ganzzahliger symmetrischer Bilinearformen).* Die Klassifikation von Paaren  $(\Gamma, s)$  bestehend aus einer endlich erzeugten freien abelschen Gruppe  $\Gamma$  und einer symmetrischen biadditiven Abbildung  $s : \Gamma \times \Gamma \rightarrow \mathbb{Z}$  ist eine interessante Aufgabe. Man zeige, daß sich für  $\Gamma$  vom Rang zwei und  $s$  positiv definit stets ein Repräsentant  $(\mathbb{Z}^2, s)$  finden läßt, dessen quadrierte Längenfunktion die Gestalt  $ax^2 + 2bxy + cy^2$  hat mit  $0 \leq 2b \leq a \leq c$ . Hinweis: Man suche in  $\Gamma$  ein von Null verschiedenes Element  $v$  kleinstmöglicher Länge; Man zeige, daß es sich zu einer Basis von  $\Gamma$  ergänzen läßt, sagen wir durch einen weiteren Vektor  $u$ ; Man mache nun für den verbesserten zweiten Basisvektor  $w$  den Ansatz  $w = \pm(u + nv)$ . Hat zusätzlich die Fundamentalmatrix von  $s$  die Determinante Eins, so finden wir unmittelbar  $a = 1$ ,  $b = 0$  und  $c = 1$  und damit gibt es bis auf Isomorphismus nur ein mögliches Paar mit diesen Eigenschaften, nämlich  $\mathbb{Z}^2$  mit dem Standardskalarprodukt.

*Ergänzung 4.4.4.37.* In der Literatur wird statt der in 4.4.4.36 erklärten Aufgabe oft implizit die Klassifikation von Tripeln  $(\Gamma, s, \omega)$  besprochen mit dem zusätzlichen Datum einer Orientierung  $\omega$ . Dann läßt sich in derselben Weise zumindest noch  $-a < 2b \leq a < c$  oder  $0 \leq 2b \leq a = c$  erreichen. Hat zusätzlich die Fundamentalmatrix von  $s$  die Determinante Eins, so finden wir immer noch  $a = 1$ ,  $b = 0$  und  $c = 1$  und damit gibt es bis auf Isomorphismus nur ein mögliches Tripel mit diesen Eigenschaften.

*Übung 4.4.4.38 (Ternäre ganzzahlige symmetrische Bilinearformen).* Zur Klassifikation von Paaren  $(\Gamma, s)$  bestehend aus einer endlich erzeugten freien abelschen Gruppe  $\Gamma$  vom Rang drei und einer positiv definiten symmetrischen biadditiven Abbildung  $s : \Gamma \times \Gamma \rightarrow \mathbb{Z}$  zeige man ähnlich, daß sich stets ein Repräsentant  $(\mathbb{Z}^3, s)$  finden läßt, für dessen Fundamentalmatrix gilt

$$0 \leq 2m_{13} \leq 2m_{12} \leq m_{11} < 2\sqrt[3]{\det M}$$

Hinweis: Man suche in  $\Gamma$  ein von Null verschiedenes Element  $v$  kleinstmöglicher Länge; Man zeige, daß es sich zu einer Basis von  $\Gamma$  ergänzen läßt, sagen

wir durch weitere Vektoren  $u_1, u_2$ ; Man mache nun für die verbesserten weiteren Basisvektoren  $w_1, w_2$  den Ansatz  $w_i = \pm(u_i + n_i v)$ . So erreicht man die ersten Ungleichungen. Für die letzte Ungleichung beachte man, daß  $\sqrt{\det M}$  nach ?? das Volumen des von einer und jeder Basis von  $\Gamma$  im Skalarprodukttraum  $V := \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$  aufgespannten Parallelipeds ist. Hat die Kugel mit Radius  $r$  mindestens das Volumen der Grundmasche, in Formeln  $4\pi r^3/3 \geq \sqrt{\det M}$ , so können die Kugeln um die Punkte aus  $\Gamma$  nicht paarweise disjunkt sein und es gibt einen von Null verschiedenen Gittervektor der Länge  $\leq 2r$ . So einen Vektor gibt es also für  $(2r)^6(\pi/6)^2 \geq \det M$  alias  $(2r)^2 \geq (6/\pi)^{2/3} \sqrt[3]{\det M}$  und wir finden  $m_{11} < 2\sqrt[3]{\det M}$ . Hat zusätzlich die Fundamentalmatrix von  $s$  die Determinante Eins, so finden wir unmittelbar einen Repräsentanten mit  $m_{11} = 1$  und  $m_{12} = m_{13} = 0$  und sehen mit 4.4.4.36, daß es bis auf Isomorphismus nur ein mögliches Paar mit diesen Eigenschaften gibt, nämlich  $\mathbb{Z}^3$  mit dem Standardskalarprodukt.

*Ergänzung 4.4.4.39.* In der Literatur wird statt der in 4.4.4.38 erklärten Aufgabe oft implizit die Klassifikation von Tripeln  $(\Gamma, s, \omega)$  besprochen mit dem zusätzlichen Datum einer Orientierung  $\omega$ . Das verkompliziert dann die Argumentation und die Ergebnisse. Mit expliziten aber weniger anschaulichen Abschätzungen läßt sich darüber hinaus unschwer  $m_{11} < (4/3)\sqrt[3]{\det M}$  zeigen.

*Ergänzung 4.4.4.40 (Symmetrische Bilinearformen und quadratische Formen).* Gegeben ein Kring  $K$  und ein  $K$ -Modul  $V$  verstehe ich unter einer **quadratischen Form auf  $V$**  wie im Fall eines Körpers  $K$  aus 4.2.2.1 eine Abbildung  $q : V \rightarrow K$  derart, daß es eine Bilinearform  $b$  auf  $V$  gibt mit  $q(v) = b(v, v)$ . In der Literatur versteht man darunter auch oft eine symmetrische Bilinearform, aber die natürliche Abbildung  $s \mapsto q_s$  von symmetrischen Bilinearformen zu quadratischen Formen gegeben durch  $q_s(v) := s(v, v)$  ist nur dann eine Bijektion, wenn die Zwei in  $K$  invertierbar ist, in Formeln  $2 \in K^\times$ . In unserer Terminologie ist etwa  $XY$  eine quadratische Form über  $\mathbb{Z}$ , die nicht von einer symmetrischen Bilinearform herkommt.

#### 4.4.5 Quotientenvektorräume

**Satz 4.4.5.1 (Universelle Eigenschaft surjektiver Homomorphismen).** Seien  $s : V \twoheadrightarrow Q$  eine surjektive lineare Abbildung und  $\varphi : V \rightarrow W$  eine beliebige lineare Abbildung. Genau dann existiert ein Homomorphismus  $\bar{\varphi} : Q \rightarrow W$  mit  $\varphi = \bar{\varphi} \circ s$ , wenn gilt  $\ker(\varphi) \supset \ker(s)$ .

4.4.5.2. Dieser Homomorphismus  $\bar{\varphi}$  ist dann natürlich eindeutig bestimmt. In diesem Sinne kann man diesen Satz auch dahingehend zusammenfassen, daß das Vorschalten eines surjektiven Homomorphismus  $s : V \twoheadrightarrow Q$  für jeden weiteren

Vektorraum  $W$  eine Bijektion

$$(\circ s) : \text{Hom}_k(Q, W) \xrightarrow{\sim} \{\varphi \in \text{Hom}_k(V, W) \mid \ker(\varphi) \supset \ker(s)\}$$

liefert. Der Übersichtlichkeit halber stelle ich die in diesem Satz auftauchenden Gruppen und Morphismen auch noch wieder anders in einem Diagramm dar:

$$\begin{array}{ccc} V & \xrightarrow{s} & Q \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & & W \end{array}$$

Man formuliert diesen Satz auch mit den Worten,  $\varphi$  **faktorisiere in eindeutiger Weise über  $s$** .

*Beweis.* Offensichtlich ist  $\varphi$  konstant auf den Fasern von  $s$ . Damit finden wir schon mal eine Abbildung  $\bar{\varphi}$  wie behauptet. Man prüft leicht, daß sie ein Homomorphismus ist.  $\square$

**4.4.5.3 (Surjektive Homomorphismen mit gleichem Kern).** Gegeben ein Vektorraum  $V$  und zwei surjektive Homomorphismen  $s : V \twoheadrightarrow Q$  und  $t : V \twoheadrightarrow P$  mit demselben Kern  $\ker(s) = \ker(t)$  sind die Homomorphismen  $\bar{t} : Q \rightarrow P$  mit  $\bar{t} \circ s = t$  und  $\bar{s} : P \rightarrow Q$  mit  $\bar{s} \circ t = s$  nach 4.4.5.1 offensichtlich zueinander inverse Isomorphismen  $Q \xrightarrow{\sim} P \xrightarrow{\sim} Q$ . Salopp gesprochen wird also bei einem surjektiven Homomorphismus „das Ziel bereits durch den Ausgangsraum und den Kern festgelegt bis auf eindeutigen Isomorphismus“.

**Satz 4.4.5.4 (Quotientenvektorraum).** Sei  $k$  ein Körper. Gegeben  $V \supset U$  ein  $k$ -Vektorraum mit einem Teilraum existiert auf der Restklassengruppe  $V/U$  aus 4.4.2.10 genau eine Struktur als  $k$ -Vektorraum  $k \times V/U \rightarrow V/U$  derart, daß die kanonische Projektion

$$\text{can} : V \twoheadrightarrow V/U$$

aus 4.4.2.10 eine  $k$ -lineare Abbildung wird. Mit dieser Vektorraumstruktur heißt  $V/U$  der **Quotient von  $V$  nach  $U$** .

*Beweis.* Wir betrachten die Abbildung

$$\begin{aligned} k \times \mathcal{P}(V) &\rightarrow \mathcal{P}(V) \\ (\lambda, A) &\mapsto \lambda \cdot A := \lambda A + U \end{aligned}$$

Für  $A = v + U$  finden wir  $\lambda \cdot A = \lambda A + U = \lambda v + U$ , so daß unsere Abbildung eine Abbildung  $k \times V/U \rightarrow V/U$  induziert, die die Eigenschaft  $\overline{\lambda v} = \lambda \cdot \bar{v}$  hat für alle  $\lambda \in k$ ,  $v \in V$ . Damit folgt sofort, daß unsere Abbildung  $k \times V/U \rightarrow V/U$  auf der abelschen Gruppe  $V/U$  eine Struktur als  $k$ -Vektorraum definiert, und daß

die Projektion  $V \twoheadrightarrow V/U$  für diese Struktur  $k$ -linear ist. Umgekehrt ist auch klar, daß das die einzige Struktur als  $k$ -Vektorraum auf der abelschen Gruppe  $V/U$  ist, für die die Projektion  $V \twoheadrightarrow V/U$  eine  $k$ -lineare Abbildung sein kann.  $\square$

*Zweiter Beweis.* Wir betrachten das Diagramm

$$\begin{array}{ccc} k \times V & \xrightarrow{m} & V \\ \downarrow & & \downarrow \\ k \times V/U & \xrightarrow{\bar{m}} & V/U \end{array}$$

mit der Skalarmultiplikation in der oberen Horizontalen. Nach Übung 4.4.2.27 und wegen  $m(k \times U) \subset U$  gibt es genau eine biadditive Abbildung in der unteren Horizontalen, die dieses Diagramm zum Kommutieren bringt. Daß die Nebengruppe  $V/U$  mit dieser Abbildung als Skalarmultiplikation ein  $k$ -Vektorraum mit den geforderten Eigenschaften ist, prüft man dann ohne weitere Schwierigkeiten.  $\square$

**4.4.5.5 (Isomorphismesatz für Vektorräume).** Jeder Vektorraumhomomorphismus  $f : V \rightarrow W$  induziert einen Vektorraumisomorphismus  $V/\ker f \xrightarrow{\sim} \text{im } f$ . Das folgt unmittelbar aus dem Isomorphismesatz für Gruppen 4.4.2.12.

**4.4.5.6.** Gegeben Vektorräume  $V \supset W \supset U$  induziert die Komposition von kanonischen Abbildungen  $V \twoheadrightarrow V/U \twoheadrightarrow (V/U)/(W/U)$  einen Vektorraumisomorphismus  $V/W \xrightarrow{\sim} (V/U)/(W/U)$ . Das folgt unmittelbar aus dem Noether'schen Isomorphismesatz 4.4.2.15.

**Definition 4.4.5.7.** Gegeben  $V \supset U$  ein Vektorraum mit einem Untervektorraum heißt die Dimension des Quotienten  $V/U$  auch die **Kodimension von  $U$  in  $V$**  und wird notiert als  $\text{codim}(U \subset V) := \dim(V/U)$ .

**4.4.5.8.** Ist  $V$  endlichdimensional, so haben wir nach dem Isomorphismesatz 4.4.5.5 und der Dimensionsformel 3.2.2.5 die Identität

$$\text{codim}(U \subset V) = \dim(V) - \dim(U)$$

Es gibt aber auch in unendlichdimensionalen Räumen durchaus Teilräume endlicher Kodimension. Eine Teilmenge eines Vektorraums ist eine lineare Hyperebene im Sinne von 3.1.5.16 genau dann, wenn sie ein Untervektorraum der Kodimension Eins ist.

## Übungen

*Übung 4.4.5.9 (Auf Quotienten induzierte multilinear Abbildungen).* Gegeben eine bilineare Abbildung  $b : V \times W \rightarrow L$  und surjektive lineare Abbildungen  $s : V \twoheadrightarrow P$  und  $t : W \twoheadrightarrow Q$  mit der Eigenschaft  $b(\ker(s) \times W) = 0 = b(V \times \ker(t))$  gibt es genau eine bilineare Abbildung  $\bar{b} : P \times Q \rightarrow L$  derart, daß das Diagramm

$$\begin{array}{ccc} V \times W & \xrightarrow{b} & L \\ s \times t \downarrow & & \parallel \\ P \times Q & \xrightarrow{\bar{b}} & L \end{array}$$

kommutiert. Analoges gilt für multilinear Abbildungen.

*Übung 4.4.5.10.* Gegeben ein Vektorraum  $V$  mit Untervektorräumen  $U, W$  zeige man, daß sich jede Linearform auf  $V$ , die auf  $U \cap W$  verschwindet, schreiben läßt als Summe einer Linearform, die auf  $U$  verschwindet, und einer Linearform, die auf  $W$  verschwindet.

*Übung 4.4.5.11 (Simultane Trigonalisierbarkeit).* Eine Menge von paarweise kommutierenden trigonalisierbaren Endomorphismen eines endlichdimensionalen Vektorraums ist stets simultan trigonalisierbar, als da heißt, es gibt eine Basis, bezüglich derer alle unsere Endomorphismen eine Matrix von oberer Dreiecksgegestalt haben. Hinweis: Existenz eines simultanen Eigenvektors 4.3.2.18 und vollständige Induktion durch betrachten des Quotienten nach dem davon erzeugten Teilraum.

*Ergänzende Übung 4.4.5.12 (Quotienten affiner Räume).* Gegeben eine surjektive affine Abbildung von affinen Räumen  $\varphi : E \twoheadrightarrow F$  zeige man, daß jede affine Abbildung  $\eta : E \rightarrow G$  mit  $\ker \vec{\eta} \supset \ker \vec{\varphi}$  in eindeutiger Weise über  $\varphi$  faktorisiert. Gegeben ein affiner Raum  $E$  und ein Teilraum  $U \subset \vec{E}$  zeige man andererseits, daß es eine surjektive affine Abbildung  $\varphi : E \twoheadrightarrow F$  gibt mit  $\ker \vec{\varphi} = U$ . Man mag  $F$  konstruieren als den Bahnenraum von  $U$  in  $E$  und mag diesen affinen Raum  $E/U$  notieren. Die zu diesem Datum gehörige surjektive affine Abbildung mag man :  $E \twoheadrightarrow E/U$  notiert werden.

## 4.4.6 Exakte Sequenzen

4.4.6.1. Beim Arbeiten mit Quotienten ermöglicht der Formalismus der „exakten Sequenzen“ oft besonders transparente Formulierungen. Wir führen deshalb im folgenden auch diese Sprache ein.

**Definition 4.4.6.2.** Eine Menge mit einem ausgezeichneten Element heißt eine **bepunktete Menge**. Das ausgezeichnete Element einer bepunkteten Menge heißt **der Basispunkt**.

**Definition 4.4.6.3.** Eine Sequenz  $X \xrightarrow{f} Y \xrightarrow{g} Z$  von bepunkteten Mengen mit basispunktverhaltenden Abbildungen heißt **exakt**, wenn das Urbild in  $Y$  des ausgezeichneten Punktes  $z \in Z$  mit dem Bild von  $X \rightarrow Y$  zusammenfällt, in Formeln  $f(X) = g^{-1}(z)$ . Eine längere Sequenz von bepunkteten Mengen heißt exakt, wenn sie an jeder Stelle exakt ist.

*Beispiel 4.4.6.4.* Sei  $\text{ens}$  die einelementige Menge. Eine Sequenz  $X \rightarrow Y \rightarrow \text{ens}$  ist exakt genau dann, wenn ihre erste Abbildung surjektiv ist. Eine Sequenz  $\text{ens} \rightarrow Y \rightarrow Z$  ist exakt genau dann, wenn ihre zweite Abbildung injektiv ist.

**Definition 4.4.6.5.** Eine **kurze exakte Sequenz** von bepunkteten Mengen ist eine Sequenz  $X \rightarrow Y \rightarrow Z$  derart, daß die Sequenz  $\text{ens} \rightarrow X \rightarrow Y \rightarrow Z \rightarrow \text{ens}$  exakt ist oder gleichbedeutend, daß  $X \rightarrow Y \rightarrow Z$  exakt ist sowie  $X \rightarrow Y$  injektiv und  $Y \rightarrow Z$  surjektiv. Wir notieren kurze exakte Sequenzen meist

$$X \hookrightarrow Y \twoheadrightarrow Z$$

**4.4.6.6 (Exakte Sequenzen von Gruppen).** Eine Gruppe fassen wir in diesem Kontext stets auf als eine bepunktete Menge mit dem neutralen Element als ausgezeichnetem Punkt. Eine Sequenz von Gruppen und Gruppenhomomorphismen

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

heißt also exakt, wenn das Bild der ersten Abbildung zusammenfällt mit dem Kern der zweiten Abbildung, in Formeln  $\text{im } f = \ker g$ .

*Beispiel 4.4.6.7.* Für jeden Homomorphismus  $x : M \rightarrow N$  von additiv notierten abelschen Gruppen ist die Sequenz

$$0 \rightarrow (\ker x) \rightarrow M \rightarrow N \rightarrow (N/\text{im } x) \rightarrow 0$$

exakt. Man nennt wegen dieser Symmetrie den Quotienten nach dem Bild auch den **Kokern** unseres Morphismus von abelschen Gruppen. Wir verwenden für den Kokern die Notation  $\text{cok } x := (N/\text{im } x)$ .

**4.4.6.8.** Die Dimensionsformel 3.2.2.5 kann in dieser Terminologie auch dahingehend formuliert werden, daß für jede kurze exakte Sequenz  $V' \hookrightarrow V \twoheadrightarrow V''$  von Vektorräumen gilt

$$\dim V = \dim V' + \dim V''$$

**Definition 4.4.6.9.** Gegeben Sequenzen  $A \xrightarrow{r} B \xrightarrow{s} C$  und  $A' \xrightarrow{r'} B' \xrightarrow{s'} C'$  verstehen wir unter einem **Homomorphismus von Sequenzen** ein Tripel  $(f, g, h)$  von Homomorphismen derart, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} A & \xrightarrow{r} & B & \xrightarrow{s} & C \\ \downarrow f & & \downarrow g & & \downarrow h \\ A' & \xrightarrow{r'} & B' & \xrightarrow{s'} & C' \end{array}$$

Solch ein Morphismus heißt ein **Isomorphismus von Sequenzen**, wenn alle drei vertikalen Abbildungen  $f, g$  und  $h$  Isomorphismen sind. Je nach Kontext meinen wir mit Homomorphismen hier Vektorraumhomomorphismen, Gruppenhomomorphismen oder schlicht Abbildungen.

4.4.6.10. Gegeben eine kurze exakte Sequenz von abelschen Gruppen  $A \xhookrightarrow{r} B \xrightarrow{s} C$  sind gleichbedeutend: (1)  $r$  besitzt ein Linksinverse, (2)  $s$  besitzt ein Rechtsinverse und (3) es gibt einen Isomorphismus der Gestalt  $(\text{id}_A, f, \text{id}_C)$  von unserer Sequenz mit der Sequenz

$$A \xrightarrow{\text{in}_1} A \oplus C \xrightarrow{\text{pr}_2} C$$

Das ist eine Umformulierung der Übungen 4.4.2.23 und 4.4.2.24. Eine kurze exakte Sequenzen mit diesen Eigenschaften heißt eine **spaltende** kurze exakte Sequenz von abelschen Gruppen. Die kurze exakte Sequenz von abelschen Gruppen  $\mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$  mit der Multiplikation mit Zwei als erster Abbildung spaltet nicht.

4.4.6.11 (**Kurze exakte Sequenzen von Vektorräumen spalten**). Arbeiten wir speziell mit Vektorräumen, so finden wir mit 3.2.10.1 für jeden Untervektorraum  $N \subset A$  einen zu  $N$  komplementären Teilraum  $U$  und nach 3.2.2.20 induziert die kanonische Abbildung einen Isomorphismus  $U \xrightarrow{\sim} A/N$ . In diesem Fall erhalten wir also zusätzlich einen Isomorphismus von kurzen exakten Sequenzen

$$\begin{array}{ccccccc} N & \hookrightarrow & N \oplus U & \twoheadrightarrow & U \\ \parallel & & \downarrow g & & \downarrow h \\ N & \hookrightarrow & A & \twoheadrightarrow & A/N \end{array}$$

Implizit ist dabei zu verstehen, daß die Morphismen der oberen Horizontale die kanonische Injektion und Projektion sein sollen.

4.4.6.12 (**Die Duale einer kurzen exakten Sequenz ist exakt**). Gegeben eine kurze exakte Sequenz von Vektorräumen ist auch die duale Sequenz eine kurze exakte Sequenz. Das ist in der Tat offensichtlich im Fall einer kurzen exakten Sequenz der Gestalt  $N \hookrightarrow N \oplus U \twoheadrightarrow U$  und folgt dann mit 4.4.6.11 im allgemeinen. Speziell ist die Transponierte einer Injektion eine Surjektion und die Transponierte einer Surjektion eine Injektion.

## Übungen

*Übung 4.4.6.13 (Quotienten und Produkte).* Gegeben zwei Sequenzen von bepunkteten Mengen  $A \rightarrow B \rightarrow C$  und  $A' \rightarrow B' \rightarrow C'$  ist ihr **Produkt**

$$(A \times A') \rightarrow (B \times B') \rightarrow (C \times C')$$

exakt genau dann, wenn die beiden Ausgangssequenzen exakt sind. Analoges gilt sowohl für das Produkt als auch für die direkte Summe einer beliebigen Familie von Sequenzen von bepunkteten Mengen. Diese Aussage präzisiert unter anderem die etwas vage Aussage, daß das „Bilden von Produkten mit dem Bilden von Quotienten kommutiert“.

*Ergänzende Übung 4.4.6.14 (Additivität der Spur).* Gegeben ein kommutatives Diagramm von endlichdimensionalen Vektorräumen mit zweimal derselben kurzen exakten Zeile

$$\begin{array}{ccccc} V' & \hookrightarrow & V & \twoheadrightarrow & V'' \\ f' \downarrow & & f \downarrow & & f'' \downarrow \\ V' & \hookrightarrow & V & \twoheadrightarrow & V'' \end{array}$$

gilt für die Spuren der Vertikalen die Identität  $\text{tr}(f) = \text{tr}(f') + \text{tr}(f'')$ . Hat allgemeiner im Fall beliebiger Vektorräume der Homomorphismus  $f$  endlichen Rang, so haben auch  $f'$  und  $f''$  endlichen Rang, und unter dieser Voraussetzung gilt für die Spuren der Vertikalen auch wieder die Identität  $\text{tr}(f) = \text{tr}(f') + \text{tr}(f'')$ .

#### 4.4.7 Mehr zu exakten Sequenzen\*

**Proposition 4.4.7.1 (Exakte Vektorraumsequenzen bis auf Isomorphismus).** *Jede exakte drei-Term-Sequenz von Vektorräumen ist isomorph zu einer Sequenz der Gestalt*

$$\begin{array}{ccccc} V_2 & \xleftarrow{\quad \left( \begin{smallmatrix} 0 & \text{id} \\ 0 & 0 \end{smallmatrix} \right) \quad} & V_1 & \xleftarrow{\quad \left( \begin{smallmatrix} 0 & \text{id} \\ 0 & 0 \end{smallmatrix} \right) \quad} & V_0 \\ \bigoplus_{V_3} & & \bigoplus_{V_2} & & \bigoplus_{V_1} \end{array}$$

4.4.7.2. Wir verwenden hier die Matrixnotation 3.2.4.12.

*Beweis.* Sei  $C \xleftarrow{r} B \xleftarrow{s} A$  unsere Sequenz. Wir setzen  $V_0 := \ker s$  und wählen ein Komplement  $V_1 \subset A$  zu  $V_0$ . Dann induziert  $s$  einen Isomorphismus  $s : V_1 \xrightarrow{\sim} \text{im } s = \ker r$  und wir wählen ein Komplement  $V_2 \subset B$  zu  $\ker r$ . Nun induziert  $r$  einen Isomorphismus  $r : V_2 \xrightarrow{\sim} \text{im } r$  und wir wählen ein Komplement  $V_3 \subset C$  zu  $\text{im } r$ . Insgesamt erhalten wir dann mit der Notation  $i_\nu$  für die Einbettung von  $V_\nu$  ein kommutatives Diagramm

$$\begin{array}{ccccc} V_2 & \xleftarrow{\quad \left( \begin{smallmatrix} 0 & \text{id} \\ 0 & 0 \end{smallmatrix} \right) \quad} & V_1 & \xleftarrow{\quad \left( \begin{smallmatrix} 0 & \text{id} \\ 0 & 0 \end{smallmatrix} \right) \quad} & V_0 \\ \bigoplus_{V_3} & & \bigoplus_{V_2} & & \bigoplus_{V_1} \\ (r,i_3) \downarrow \wr & & (s,i_2) \downarrow \wr & & (i_0,i_1) \downarrow \wr \\ C & \longleftarrow & B & \longleftarrow & A \end{array} \quad \square$$

**Korollar 4.4.7.3 (Erhaltung der Exaktheit unter Hom).** Gegeben eine exakte Sequenz  $U \xrightarrow{r} V \xrightarrow{s} W$  von Vektorräumen erhalten wir für jeden weiteren Vektorraum  $L$  exakte Sequenzen

$$\begin{array}{ccccccc} \text{Hom}(W, L) & \xrightarrow{\circ s} & \text{Hom}(V, L) & \xrightarrow{\circ r} & \text{Hom}(U, L) \\ \text{Hom}(L, U) & \xrightarrow{r \circ} & \text{Hom}(L, V) & \xrightarrow{s \circ} & \text{Hom}(L, W) \end{array}$$

*Beweis.* Das folgt unmittelbar aus der vorhergehenden Proposition 4.4.7.1 zusammen mit der Erkenntnis, daß das Bilden des Homomorphismenraums, wie in 3.2.3.12 und 3.2.3.13 ausgeführt wird, „mit endlichen direkten Summen vertauscht“.

□

**4.4.7.4 (Die Duale einer exakten Sequenz ist exakt).** Nehmen wir in diesem Korollar als  $L$  den Grundkörper, so folgt insbesondere, daß jede exakte Sequenz von Vektorräumen beim Dualisieren wieder eine exakte Sequenz liefert.

**Lemma 4.4.7.5 (Neunerlemma).** Sei gegeben ein Diagramm von Gruppen mit kurzen exakten Zeilen der Gestalt

$$\begin{array}{ccccc} A' & \rightarrow & A & \twoheadrightarrow & A'' \\ \downarrow & & \downarrow & & \downarrow \\ B' & \rightarrow & B & \twoheadrightarrow & B'' \\ \downarrow & & \downarrow & & \downarrow \\ C' & \rightarrow & C & \twoheadrightarrow & C'' \end{array}$$

und seien die senkrechten Kompositionen jeweils trivial. Sei unser Diagramm **kommutativ** in dem Sinne, daß alle vier Quadrate „kommutieren“, daß also die Komposition  $A' \rightarrow A \rightarrow B$  übereinstimmt mit der Komposition  $A' \rightarrow B' \rightarrow B$  etcetera. Sind unter diesen Voraussetzungen zwei der Spalten kurze exakte Sequenzen, so auch die dritte.

**4.4.7.6.** Wir brauchen gar nicht zu fordern, daß die Abbildungen der rechten Vertikale Gruppenhomomorphismen sind, und noch nicht einmal, daß sie Gruppen sind, wenn wir nur annehmen, daß alle Horizontalen als Sequenzen von bepunkteten Mengen isomorph sind zu Sequenzen der Gestalt  $H \hookrightarrow G \twoheadrightarrow G/H$  für eine Gruppe  $G$  mit einer Untergruppe  $H$  und dem neutralen Element von  $G$  als ausgezeichnetem Punkt in der Mitte. Der Beweis bleibt derselbe und 4.4.1.11 zeigt, daß auch in der rechten Spalte alle nichtleeren Fasern gleich viele Elemente haben. Die letzte Aussage von 4.4.1.11 etwa ist ein Spezialfall des so verallgemeinerten Neunerlemmas.

**4.4.7.7.** Das Neunerlemma kann als eine Verallgemeinerung des Noether'schen Isomorphiesatzes 4.4.2.15 verstanden werden, den man im Fall  $A' = A$  zurückgewinnt. Im Fall abelscher Gruppen werden Sie eine noch allgemeinere Aussage

eventuell später einmal als „lange exakte Homologiesequenz“ ?? kennenlernen. Der folgende Beweis ist ein schönes Beispiel für eine Beweismethode, die als **Diagrammjagd** bekannt ist.

*Beweis.* Es ist einfacher, eine allgemeinere Aussage zu zeigen: Sei ein kommutatives Diagramm von Gruppen mit kurzen exakten Zeilen

$$\begin{array}{ccccc}
 & \partial \downarrow & \partial \downarrow & \partial \downarrow & \\
 X_{i+1} & \xhookrightarrow{f} & Y_{i+1} & \xrightarrow{g} & Z_{i+1} \\
 \partial \downarrow & & \partial \downarrow & & \partial \downarrow \\
 X_i & \xhookrightarrow{f} & Y_i & \xrightarrow{g} & Z_i \\
 \partial \downarrow & & \partial \downarrow & & \partial \downarrow \\
 X_{i-1} & \xhookrightarrow{f} & Y_{i-1} & \xrightarrow{g} & Z_{i-1} \\
 \partial \downarrow & & \partial \downarrow & & \partial \downarrow \\
 & & & &
 \end{array}$$

gegeben derart, daß die Komposition aufeinanderfolgender Pfeile in den Spalten jeweils einwertig ist. Sind dann zwei der Spalten exakt, so auch die Dritte. Das Neunerlemma folgt durch die Erweiterung seines Diagramms durch triviale Gruppen nach oben und unten. Wir schreiben den Beweis gleich so auf, daß auch für die allgemeinere Situation 4.4.7.6 funktioniert, und notieren dazu die ausgezeichneten Punkte der rechten Spalte mit  $\bar{1}$ . Wir diskutieren die drei Fälle der Reihe nach.

Fall 1: Die letzten beiden Spalten sind exakt und es gilt, die Exaktheit der ersten bei  $X_i$  zu zeigen. Sei also  $x_i \in X_i$  mit  $\partial x_i = 1$ . Für  $y_i := f x_i$  folgt  $\partial y_i = 1$ , also  $y_i = \partial y_{i+1}$ . Für  $z_{i+1} := g y_{i+1}$  folgt weiter  $\partial z_{i+1} = \bar{1}$ , also  $z_{i+1} = \partial z_{i+2}$ . Wir finden nun  $y_{i+2}$  mit  $g y_{i+2} = z_{i+2}$ , also  $g \partial y_{i+2} = z_{i+1} = g y_{i+1}$ , woraus für  $\tilde{y}_{i+1} := (\partial y_{i+2})^{-1} y_{i+1}$  folgt  $y_i = \partial \tilde{y}_{i+1}$  und  $g \tilde{y}_{i+1} = \bar{1}$ . Dann aber gibt es  $\tilde{x}_{i+1}$  mit  $f \tilde{x}_{i+1} = \tilde{y}_{i+1}$  und es folgt  $f \partial \tilde{x}_{i+1} = y_i$  und somit  $\partial \tilde{x}_{i+1} = x_i$ .

Fall 2: Die beiden äußeren Spalten sind exakt und es gilt, die Exaktheit der mittleren bei  $Y_i$  zu zeigen. Sei  $y_i \in Y_i$  mit  $\partial y_i = 1$ . Für  $z_i := g y_i$  folgt  $\partial z_i = \bar{1}$ , also gibt es  $z_{i+1}$  mit  $\partial z_{i+1} = z_i$  und dann  $y_{i+1}$  mit  $g y_{i+1} = z_{i+1}$  und  $g \partial y_{i+1} = z_i = g y_i$ . Für  $\tilde{y}_i := (\partial y_{i+1})^{-1} y_i$  folgt also  $\partial \tilde{y}_i = 1$  und  $g \tilde{y}_i = \bar{1}$ . Also gibt es  $\tilde{x}_i$  mit  $f \tilde{x}_i = \tilde{y}_i$  und notwendig  $\partial \tilde{x}_i = 1$ , also  $\tilde{x}_i = \partial \tilde{x}_{i+1}$  und  $\tilde{y}_i = \partial f \tilde{x}_{i+1}$ . So erhalten wir schließlich  $y_i = \partial(y_{i+1} f(\tilde{x}_{i+1}))$ .

Fall 3: Die ersten beiden Spalten sind exakt und es gilt, die Exaktheit der letzten bei  $z_i$  zu zeigen. Sei also  $\partial z_i = \bar{1}$ . Sicher gibt es  $y_i$  mit  $g y_i = z_i$  und es folgt

$g\partial y_i = \bar{1}$ , also gibt es  $x_{i-1}$  mit  $fx_{i-1} = \partial y_i$ . Es folgt  $f\partial x_{i-1} = 1$ , also  $\partial x_{i-1} = 1$ , also gibt es  $x_i$  mit  $\partial x_i = x_{i-1}$ . Für  $\tilde{y}_i := y_i(fx_i)^{-1}$  folgt  $\partial \tilde{y}_i = 1$  und  $g(\tilde{y}_i) = z_i$ . Also gibt es  $\tilde{y}_{i+1}$  mit  $\tilde{y}_i = \partial \tilde{y}_{i+1}$  und dann gilt  $z_i = \partial g\tilde{y}_{i+1}$ .  $\square$

### Übungen

*Übung 4.4.7.8.* Man folgere den Noether'schen Isomorphiesatz 4.4.2.15 aus dem Neunerlemma.

## 4.5 Symmetrie\*

Symmetrie ist ein grundlegendes Konzept in Mathematik und Physik. Wir haben es bei der Modellierung des Anschauungsraums bereits in Aktion gesehen. Hier soll es in einem allgemeineren und formaleren Rahmen diskutiert und mit andersartigen Beispielen illustriert werden.

### 4.5.1 Gruppenwirkungen

**Definition 4.5.1.1.** Eine **Operation** oder **Wirkung** eines Monoids  $M$  auf einer Menge  $X$  ist eine Abbildung

$$\begin{aligned} M \times X &\rightarrow X \\ (g, x) &\mapsto gx \end{aligned}$$

derart, daß gilt  $g(hx) = (gh)x$  für alle  $g, h \in M$ ,  $x \in X$  sowie  $ex = x$  für das neutrale Element  $e \in M$  und alle  $x \in X$ . Eine Menge mit einer Operation eines Monoids  $M$  nennt man eine  **$M$ -Menge**. Die Aussage „ $X$  ist eine  $M$ -Menge“ schreiben wir in Formeln

$$M \backslash X$$

4.5.1.2. Die erste Eigenschaft werde ich auch als die **Assoziativität** der Operation ansprechen und beide Eigenschaften zusammen als **Unitärassoziativität**. Ich ziehe die Bezeichnung als Operation an dieser Stelle vor, da das Wort „Wirkung“ in der Physik in einer anderen Bedeutung verwendet wird.

*Ergänzung 4.5.1.3.* In derselben Weise erklärt man noch allgemeiner auch den Begriff der **Operation einer Menge  $\Omega$  auf einer Menge  $X$**  als einer Abbildung  $\Omega \times X \rightarrow X$ , von der nichts weiter zu fordern ist.

*Beispiele 4.5.1.4.* 1. Das Anwenden einer Abbildung definiert für jede Menge  $X$  eine Operation  $\text{Ens}(X) \times X \rightarrow X$  des Monoids  $\text{Ens}(X)$  auf  $X$  und eine Operation  $\text{Ens}^\times(X) \times X \rightarrow X$  der Gruppe  $\text{Ens}^\times(X)$  auf  $X$ . Insbesondere operiert so die symmetrische Gruppe  $S_n$  auf der Menge  $\{1, 2, \dots, n\}$ .

2. Das Anwenden einer linearen Abbildung definiert für jeden Vektorraum  $V$  eine Operation  $\text{End}(V) \times V \rightarrow V$  des Monoids  $\text{End}(V)$  auf  $V$  und eine Operation  $\text{GL}(V) \times V \rightarrow V$  der Gruppe  $\text{GL}(V)$  auf  $V$ .
3. Jedes Monoid  $M$  operiert mittels seiner Verknüpfung  $M \times M \rightarrow M$  auf sich selbst.
4. Jedes Monoid  $M$  operiert auf jeder Menge  $X$  mittels der **trivialen Operation**  $ax = x \ \forall a \in M, x \in X$ .

5. Ist  $M$  ein Monoid und  $X$  eine  $M$ -Menge und  $N \subset M$  ein Untermonoid, so ist  $X$  auch eine  $N$ -Menge in offensichtlicher Weise. Ist allgemeiner  $X$  eine  $M$ -Menge und  $N \rightarrow M$  ein Monoidhomomorphismus, so kann  $X$  in offensichtlicher Weise mit einer Operation von  $N$  versehen werden.
6. Ist  $X$  ein  $M$ -Menge, so ist auch die Potenzmenge  $\mathcal{P}(X)$  eine  $M$ -Menge in natürlicher Weise.

4.5.1.5. Gegeben ein Monoid  $M$  und eine Menge  $X$  induziert das Exponentialgesetz  $\text{Ens}(M \times X, X) \xrightarrow{\sim} \text{Ens}(M, \text{Ens}(X, X))$  aus 2.1.6.5 eine Bijektion

$$\left\{ \begin{array}{l} \text{Operationen des Monoids } M \\ \text{auf der Menge } X \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Monoidhomomorphismen} \\ M \rightarrow \text{Ens}(X) \end{array} \right\}$$

In gewisser Weise ist also eine Operation eines Monoids  $M$  auf einer Menge  $X$  „dasselbe“ wie ein Monoidhomomorphismus  $M \rightarrow \text{Ens}(X)$ . Ist  $G$  eine Gruppe, so erhalten wir insbesondere eine Bijektion

$$\left\{ \begin{array}{l} \text{Operationen der Gruppe } G \\ \text{auf der Menge } X \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Gruppenhomomorphismen} \\ G \rightarrow \text{Ens}^{\times}(X) \end{array} \right\}$$

In gewisser Weise ist also eine Operation einer Gruppe  $G$  auf einer Menge  $X$  „dasselbe“ wie ein Gruppenhomomorphismus  $G \rightarrow \text{Ens}^{\times}(X)$ .

4.5.1.6. Ist ganz allgemein  $X \times Y \rightarrow Z$  eine Abbildung, etwa  $(x, y) \mapsto x \top y$ , und sind  $A \subset X$  und  $B \subset Y$  Teilmengen, so notieren wir  $(A \top B) \subset Z$  die Teilmenge

$$(A \top B) = \{x \top y \mid x \in A, y \in B\}$$

Wir haben diese Notationen in Spezialfällen bereits oft verwendet, zum Beispiel, wenn wir das Erzeugnis eines Vektors in einem reellen Vektorraum als  $\langle v \rangle = \mathbb{R}v$  schreiben, oder wenn wir das Erzeugnis von zwei Teilräumen  $U, W$  eines Vektorraums  $V$  als  $U + W$  schreiben.

**Definition 4.5.1.7.** Sei  $X$  eine Menge mit einer Operation eines Monoids  $M$ , also eine  $M$ -Menge.

1. Die Menge aller **Fixpunkte von  $M$  in  $X$**  notiert man

$$X^M := \{x \in X \mid ax = x \ \forall a \in M\}$$

In vielen Situationen nennt man die Fixpunkte auch **Invarianten**.

2. Der **Fixator** oder auch **Stabilisator** eines Punktes  $x \in X$  ist die Menge

$$M_x := \{a \in M \mid ax = x\}$$

Sie ist ein Untermonoid von  $M$ . Im Fall einer Gruppenwirkung ist sie sogar eine Untergruppe und heißt die **Standgruppe** oder **Isotropiegruppe** des Punktes  $x$ .

3. Gegeben eine Teilmenge  $Y \subset X$  unterscheiden wir zwischen ihrem **Stabilisator**  $\{a \in M \mid aY \subset Y\}$ , ihrem **Fixator** oder **mengenweisen Fixator**  $\{a \in M \mid aY = Y\}$  und schließlich ihrem **punktweisen Fixator**  $\{a \in M \mid ay = y \forall y \in Y\}$ . Alle drei sind Untermonoide und die letzten beiden im Fall einer Gruppenoperation sogar Untergruppen. Den Fixator nennen wir insbesondere im Fall, daß  $Y$  mehr als nur ein Element besitzt und daß eine Gruppe operiert, die **Symmetriegruppe von  $Y$** . Natürlich kann der Fixator von  $Y \subset X$  auch beschrieben werden als der Fixator des Punktes  $Y \in \mathcal{P}(X)$  für die auf der Potenzmenge  $\mathcal{P}(X)$  induzierte Operation. Wir notieren ihn  $M_Y$ .
4. Eine  $M$ -Menge  $X$  heißt **frei**, wenn es eine Teilmenge  $Z \subset X$  gibt derart, daß die Operation  $M \times X \rightarrow X$  eine Bijektion  $M \times Z \xrightarrow{\sim} X$  induziert. Sie mögen als Übung zeigen, daß eine Menge mit Gruppenwirkung genau dann frei ist, wenn die Standgruppen aller ihrer Punkte trivial sind, in Formeln  $(gx = x \text{ für ein } x \in X) \Rightarrow (g = e)$ .
5. Für  $Z \subset X$ ,  $N \subset M$  schreiben wir kurz  $NZ$  für die Menge  $NZ := \{bz \mid b \in N, z \in Z\}$ . Für jede Teilmenge  $Z \subset X$  ist  $MZ$  eine  $M$ -Menge in offensichtlicher Weise. Eine Teilmenge  $Z \subset X$  heißt  **$N$ -stabil**, wenn gilt  $NZ \subset Z$ , wenn also  $N$  im Stabilisator der Teilmenge  $Z$  liegt. Ist  $N = G$  eine Untergruppe von  $M$ , so wird jede  $G$ -stabile Teilmenge  $Z$  sogar von allen Elementen von  $G$  festgehalten, in Formeln

$$(GZ \subset Z) \Rightarrow (g(Z) = Z \forall g \in G)$$

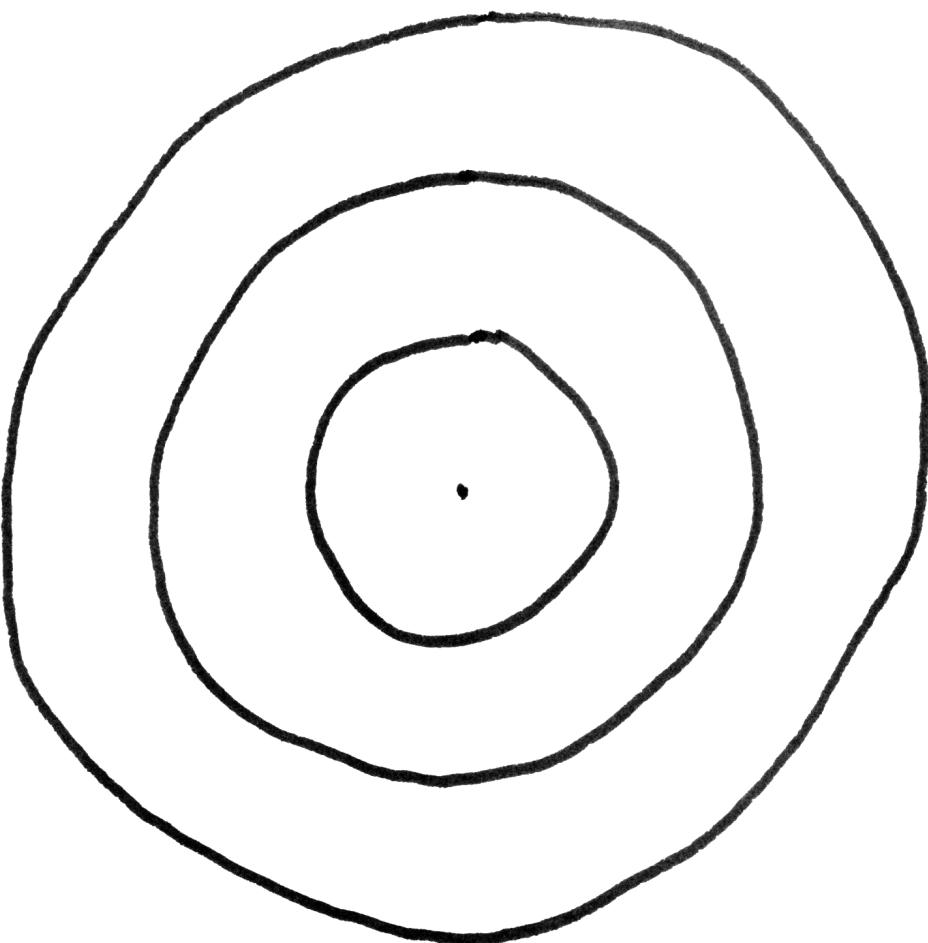
6. Sei  $x \in X$ . Die Menge

$$Mx := \{ax \mid a \in M\} \subset X$$

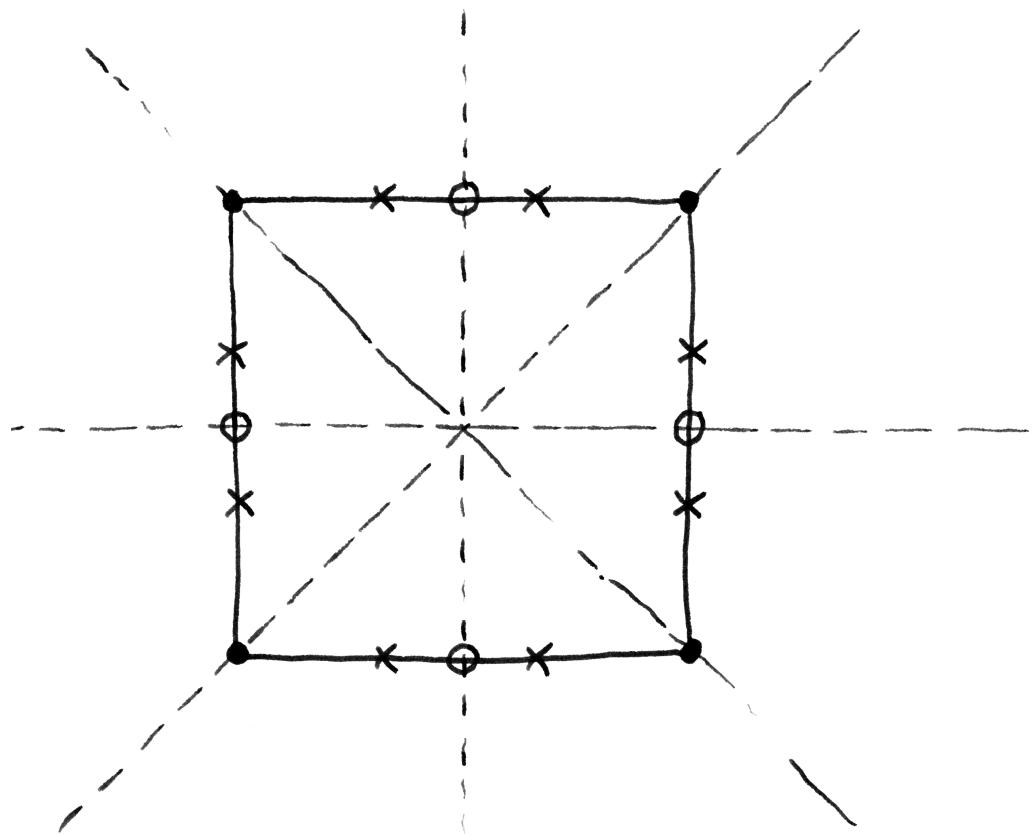
heißt die **Bahn** von  $x$ . Auf Englisch und Französisch sagt man dazu **orbit**.

7. Eine Operation heißt **transitiv**, wenn es ein  $x \in X$  gibt mit  $X = Mx$ . Im Fall einer Gruppenwirkung gilt dann  $X = Gx$  für alle  $x \in X$  und  $X$  heißt ein **homogener Raum** für  $G$ .
8. Eine Menge  $X$  mit einer freien transitiven Operation einer Gruppe  $G$  heißt ein **prinzipaler homogener  $G$ -Raum** oder auch ein  **$G$ -Torsor**.

4.5.1.8. Ist  $G$  eine Gruppe und  $H \subset G$  eine Untergruppe, so sind per definitionem die Rechtsnebenklassen von  $H$  in  $G$  genau die Bahnen der durch Multiplikation gegebenen Operation von  $H$  auf  $G$ .



Einige Bahnen von  $S^1$  auf  $\mathbb{C}$



Einige Bahnen der Symmetriegruppe eines Quadrats

4.5.1.9. Ist  $G$  eine Gruppe und  $H \subset G$  eine Untergruppe, so ist die Menge der Linksnebenklassen  $X = G/H$  eine  $G$ -Menge in offensichtlicher Weise.

*Beispiele* 4.5.1.10. In jedem eindimensionalen Vektorraum über einem Körper  $k$  bilden die von Null verschiedenen Vektoren einen Torsor über der multiplikativen Gruppe  $k^\times$  unseres Körpers. Jeder affine Raum ist ein Torsor über seinem Richtungsraum. Jede Menge mit genau zwei Elementen ist in natürlicher Weise ein  $(\mathbb{Z}/2\mathbb{Z})$ -Torsor. Jede Gruppe  $G$  kann in offensichtlicher Weise aufgefaßt werden als ein  $G$ -Torsor.

4.5.1.11 (**Diskussion der Terminologie**). Die Wirkung eines Monoids auf der leeren Menge ist in unseren Konventionen nicht transitiv. Hier sind jedoch auch andere Konventionen gebräuchlich, zum Beispiel nennt Bourbaki die Wirkung einer Gruppe auf der leeren Menge durchaus transitiv. Noch mehr Terminologie zu Mengen mit Gruppenwirkung führen wir in ?? ein.

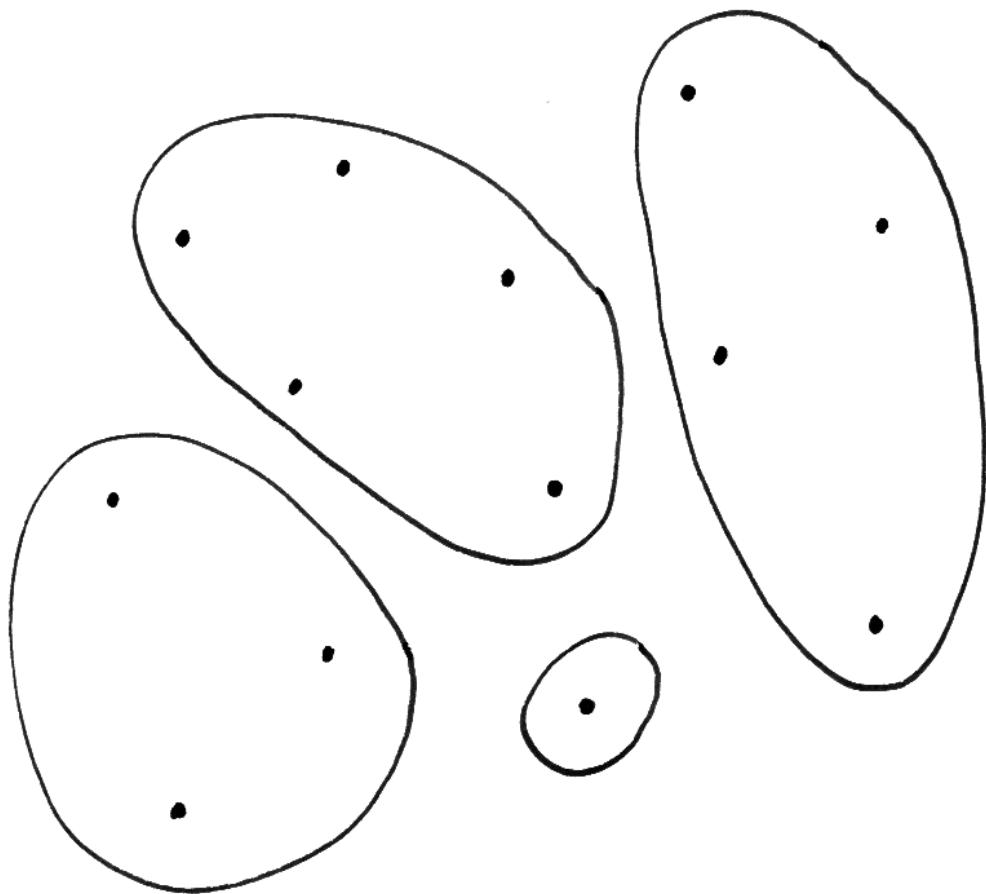
*Ergänzung* 4.5.1.12 (**Begriff eines Torsors, Varianten**). Es gibt auch Varianten des Torsor-Begriffs, bei denen man nicht auf eine vorgegebene Gruppe Bezug nimmt.

1. Man kann einen **Torsor** definieren als eine Menge  $X$  mitsamt einer ausgezeichneten Untergruppe  $G \subset \text{Ens}^\times(X)$ , die frei und transitiv auf  $X$  wirkt.
2. Man kann einen Torsor auch definieren als eine Menge  $X$  nebst einer Äquivalenzrelation auf  $X \times X$  mit gewissen Eigenschaften, die ich hier nicht ausschreibe. Von der üblichen Definition aus gesehen erklären wir dabei die Äquivalenzrelation dadurch, daß ihre Äquivalenzklassen genau die Graphen der durch die Gruppenelemente gegebenen Selbstabbildungen von  $X$  sind.
3. Man kann einen Torsor schließlich auch definieren kann als eine Menge  $X$  nebst einer Abbildung  $\varphi : X \times X \times X \rightarrow X$  mit gewissen Eigenschaften, die ich hier nicht ausschreibe. Von der üblichen Definition aus gesehen setzen wir dazu  $\varphi(x, gx, y) = gy$ .

**Lemma 4.5.1.13 (Zerlegung in Bahnen).** *Gegeben eine Menge mit Gruppenoperation sind je zwei Bahnen entweder gleich oder disjunkt.*

*Ergänzung* 4.5.1.14. Im Fall der Operation eines Monoids gibt im allgemeinen keine Zerlegung in Bahnen: Man betrachte für ein Gegenbeispiel etwa die Operation durch Addition des additiven Monoids  $\mathbb{N}$  auf  $\mathbb{Z}$ .

4.5.1.15. Unter einer **Partition einer Menge**  $X$  versteht man ein System  $\mathcal{U} \subset \mathcal{P}(X)$  von paarweise disjunkten nichtleeren Teilmengen, deren Vereinigung ganz  $X$  ist. In dieser Terminologie besagt unser Lemma also, daß die Bahnen unter der Operation einer Gruppe auf einer Menge eine Partition besagter Menge bilden.



Eine Partition einer Menge mit dreizehn Elementen durch vier Teilmengen.

*Beweis.* Sei  $G \setminus X$  unsere Menge mit Gruppenoperation. Wegen unserer Forderung  $ex = x$  an eine Gruppenoperation liegt jedes  $x \in X$  in einer  $G$ -Bahn, nämlich in der  $G$ -Bahn  $Gx$ . Andererseits folgt aus  $Gx \cap Gy \neq \emptyset$  schon  $Gx = Gy$ : In der Tat liefert  $gx = hy$  wegen  $Gg = G$  unter Verwendung der Assoziativitätsbedingung an eine Gruppenoperation ja  $Gx = Ggx = Ghy = Gy$ . Die Bahnen sind also auch paarweise disjunkt.  $\square$

**Definition 4.5.1.16.** Gegeben eine Menge mit Gruppenoperation bezeichnet man das Mengensystem der Bahnen auch als den **Bahnenraum**. Ist  $G \setminus X$  unsere Menge mit Gruppenoperation, so ist der Bahnenraum in Formeln ausgedrückt also die Teilmenge  $\{Gx \mid x \in X\} \subset \mathcal{P}(X)$  der Potenzmenge von  $X$ . Wir notieren den Bahnenraum meist  $G \setminus X$  oder  $X/G$  oder  $X/G$ . Wir haben eine kanonische Surjektion  $\text{can} : X \twoheadrightarrow G \setminus X$ ,  $x \mapsto Gx$ , die jedem Element von  $X$  seine Bahn zuordnet.

4.5.1.17 (**Diskussion der Notation**). Alle Notationen für den Bahnenraum haben ihre Tücken: Die Notation  $G \setminus X$  könnte auch die in 2.1.2.6 eingeführte Differenzmenge bedeuten, die Notation  $X/G$  hinwiederum könnte auch für den Bahnenraum einer Rechtsoperation stehen, wie wir ihn gleich einführen werden. Was im Einzelfall gemeint ist, muß aus dem Kontext erschlossen werden. Die Notation  $X/G$  vermeidet zwar diese Probleme, ist aber unüblich und umständlich.

*Beispiel 4.5.1.18.* Wir betrachten die Menge  $X = \mathbb{C}$  der komplexen Zahlen mit der Operation von  $G = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$  durch Multiplikation. Die Standgruppen sind  $G_x = 1$  falls  $x \neq 0$  und  $G_0 = S^1$ . Die Bahnen sind genau alle Kreise um den Nullpunkt mit Radius  $r \geq 0$ . Die Einbettung  $\mathbb{R}_{\geq 0} \hookrightarrow \mathbb{C}$  induziert eine Bijektion mit dem Bahnenraum  $\mathbb{R}_{\geq 0} \xrightarrow{\sim} (S^1 \setminus \mathbb{C})$ .

4.5.1.19 (**Universelle Eigenschaft des Bahnenraums**). Gegeben eine Menge mit Gruppenoperation  $G \setminus X$  und eine Abbildung in eine weitere Menge  $\varphi : X \rightarrow Y$  mit der Eigenschaft  $\varphi(gx) = \varphi(x)$  für alle  $g \in G, x \in X$  existiert genau eine Abbildung  $\bar{\varphi} : G \setminus X \rightarrow Y$  mit  $\bar{\varphi} \circ \text{can} = \varphi$ , im Diagramm

$$\begin{array}{ccc} X & \xrightarrow{\text{can}} & G \setminus X \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & Y & \end{array}$$

In der Tat können und müssen wir  $\bar{\varphi}(Gx)$  als das einzige Element der Menge  $\varphi(Gx)$  definieren. Das ist ein Spezialfall der universellen Eigenschaft von Surjektionen 2.1.5.11. Man mag es auch als einen Spezialfall der universellen Eigenschaft des Raums der Äquivalenzklassen einer Äquivalenzrelation im Sinne von 3.4.2.6 verstehen.

**Definition 4.5.1.20.** Sei  $X$  eine Menge und  $M$  ein Monoid. Eine **Rechtsoperation von  $M$  auf  $X$**  ist eine Abbildung

$$\begin{aligned} X \times M &\rightarrow X \\ (x, a) &\mapsto xa \end{aligned}$$

derart, daß  $x(ab) = (xa)b$  für alle  $a, b \in M$ ,  $x \in X$ , und daß gilt  $xe = x$  für das neutrale Element  $e \in M$  und alle  $x \in X$ . Eine Menge mit einer Rechtsoperation eines Monoids  $M$  nennt man auch eine  **$M$ -Rechtsmenge**.

*Beispiel 4.5.1.21.* Ist  $M$  ein Monoid und  $X$  eine  $M$ -Menge und  $E$  eine weitere Menge, so wird der Abbildungsraum  $\text{Ens}(X, E)$  zu einer  $M$ -Rechtsmenge mittels der Operation „durch Vorschalten“  $(fa)(x) := f(ax)$ .

**4.5.1.22 (Beziehung von Rechts- und Linksoperationen).** Ist  $G$  eine Gruppe, so wird jede  $G$ -Rechtsmenge  $X$  zu einer  $G$ -Menge durch die Operation  $gx = xg^{-1}$ , die Begriffsbildung einer  $G$ -Rechtsmenge ist also für Gruppen in gewisser Weise obsolet. Sie dient im wesentlichen dem Zweck, in manchen Situationen suggestivere Notationen zu ermöglichen. Unsere Begriffe für Linksoperationen wie Bahn, Standgruppe et cetera verwenden wir analog auf für Rechtsoperationen. Den Bahnenraum notieren wir in diesem Fall stets  $X/G$ . Die kanonische Abbildung  $X \rightarrow X/G$  hat dann offensichtlich eine zu 4.5.1.19 analoge universelle Eigenschaft.

**4.5.1.23.** Unter dem Exponentialgesetz  $\text{Ens}(X \times M, X) \xrightarrow{\sim} \text{Ens}(M, \text{Ens}(X, X))$  aus 2.1.6.5 entsprechen die Rechtsoperationen eines Monoids  $M$  auf einer Menge  $X$  gerade den Monoidhomomorphismen  $M^{\text{opp}} \rightarrow \text{Ens}^\times(X)$ . Hierbei meint  $M^{\text{opp}}$  das opponierte Monoid nach 2.2.3.33, die entsteht, indem wir die Menge  $M$  mit der opponierten Verknüpfung  $a^\circ b^\circ = (ba)^\circ$  versehen. In diesem Sinne ist also eine  $M$ -Rechtsoperation dasselbe wie eine Linksoperation von  $M^{\text{opp}}$ .

*Ergänzung 4.5.1.24.* Sei  $G$  eine Gruppe. Eine freie transitive  $G$ -Rechtsmenge nennen wir einen  **$G$ -Rechtstorsor** oder auch kurz einen  **$G$ -Torsor** in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, ob im jeweils vorliegenden Fall eine Menge mit freier und transitiver Rechts- oder mit freier und transitiver Linksoperation gemeint ist.

**4.5.1.25 (Operationen auf dem projektiven Raum).** Wir erinnern für einen Körper  $K$  und  $n \in \mathbb{N}$  aus ?? den projektiven Raum

$$\mathbb{P}^n K := (K^{n+1} \setminus \{0\}) / K^\times$$

Sicher operiert die Gruppe  $\text{GL}(n+1; K)$  auf dem projektiven Raum  $\mathbb{P}^n K$ . Die offensichtliche Operation von  $\text{GL}(2; K)$  auf  $\mathbb{P}^1 K$  entspricht unter unserer Identifikation von  $K \sqcup \{\infty\}$  mit  $\mathbb{P}^1 K$  durch  $x \mapsto \langle 1, x \rangle$  und  $\infty \mapsto \langle 0, 1 \rangle$  der Operation

von  $\mathrm{GL}(2; K)$  auf  $K \sqcup \{\infty\}$ , unter einer Matrix durch die Transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : x \mapsto \frac{c + dx}{a + bx}$$

wirkt. Der Punkt  $\infty$  muß hier mit etwas Sorgfalt ins Spiel gebracht werden und ich schreibe nicht alle Fälle aus. Man sie jedoch leicht erschließen, wenn man weiß, daß diese Operation im Fall  $K = \mathbb{R}$  stetig ist für die natürliche Topologie aus ??.

Zum Beispiel geht  $\infty$  im Fall  $b \neq 0$  nach  $d/b$ .

## Übungen

*Übung 4.5.1.26 (Noether'scher Isomorphiesatz, Variante).* Seien  $H \supset N$  eine Gruppe mit einem Normalteiler und  $X$  eine Menge mit  $H$ -Operation. So gibt es auf dem Bahnenraum  $X/N$  genau eine Operation der Quotientengruppe  $H/N$  mit der Eigenschaft  $(hN)(Nx) = Nhx$ . Ist speziell  $G \supset H \supset N$  eine Gruppe mit zwei Untergruppen und ist  $N$  ein Normalteiler in  $H$ , so induziert die Komposition  $G \rightarrow G/N \rightarrow (G/N)/(H/N)$  eine Bijektion  $G/H \xrightarrow{\sim} (G/N)/(H/N)$ .

*Übung 4.5.1.27.* Unter der Operation von  $\mathrm{GL}(n+1; \mathbb{Q})$  auf dem projektiven Raum  $\mathbb{P}^n \mathbb{Q}$  operiert bereits die Gruppe  $\mathrm{SL}(n; \mathbb{Z})$  aller  $(n \times n)$ -Matrizen mit ganzzahligen Einträgen und Determinante Eins transitiv. Hinweis: 4.4.4.29.

*Übung 4.5.1.28.* Ist  $E$  ein affiner Raum über einem Körper der Charakteristik Null und  $G \subset \mathrm{Aff}^\times E$  eine endliche Untergruppe seiner Automorphismengruppe, so besitzt  $G$  stets einen Fixpunkt in  $E$ . Hinweis: Man betrachte den Schwerpunkt einer Bahn.

*Übung 4.5.1.29 (Smith-Normalformen als Bahnrepräsentanten).* Sei  $K$  ein Körper. Man zeige, daß wir eine Operation der Gruppe  $\mathrm{GL}(n; K) \times \mathrm{GL}(m; K)$  auf der Menge  $\mathrm{Mat}(n \times m; K)$  erhalten durch die Vorschrift  $(A, B)M = AMB^{-1}$ . Man zeige weiter, daß die Bahnen unserer Operation genau die nichtleeren Fasern der durch den Rang gegebenen Abbildung  $\mathrm{rk} : \mathrm{Mat}(n \times m; K) \rightarrow \mathbb{N}$  sind. Hinweis: Smith-Normalform 3.2.6.11.

*Übung 4.5.1.30 (Jordan-Normalformen als Bahnrepräsentanten).* Sei  $K$  ein Körper. Man zeige, daß wir eine Operation der Gruppe  $\mathrm{GL}(n; K)$  auf der Menge  $\mathrm{Mat}(n; K)$  erhalten durch die Vorschrift  $A \cdot M := AMA^{-1}$ . Man zeige, wie für einen algebraisch abgeschlossenen Körper  $K$  die Theorie der Jordan'schen Normalform eine Bijektion liefert zwischen dem Bahnenraum zu dieser „Operation durch Konjugation“ und der Menge aller endlichen Multimengen von Paaren aus  $\mathbb{N}_{\geq 1} \times K$ , deren erste Komponenten sich zu  $n$  aufaddieren.

*Ergänzende Übung 4.5.1.31.* Sei  $K$  ein Körper. Man zeige, daß der Teilraum der quadratischen Formen  $Q \subset \mathrm{Ens}(K^n, K)$  stabil ist unter der Rechtsoperation der

Gruppe  $\mathrm{GL}(n; K)$  durch Vorschalten auf  $\mathrm{Ens}(K^n, K)$ . Man diskutiere, inwiefern die Frage nach der Klassifikation der quadratischen Formen im wesentlichen die Frage nach einem Repräsentantensystem für die Bahnen dieser Operation ist.

*Ergänzende Übung 4.5.1.32.* Man gebe für jedes ungerade  $n$  einen Gruppenisomorphismus  $\mathrm{SO}(n) \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{O}(n)$  an; Man zeige, daß es für gerades  $n$  keinen derartigen Isomorphismus gibt.

*Ergänzende Übung 4.5.1.33.* Ein Gitter in  $\mathbb{C}$  ist eine Untergruppe  $\Gamma \subset \mathbb{C}$ , die man als Gruppenerzeugnis einer  $\mathbb{R}$ -Basis von  $\mathbb{C}$  erhalten kann. Auf der Menge Gitt aller Gitter in  $\mathbb{C}$  operiert  $\mathbb{C}^\times$  in offensichtlicher Weise. Man zeige, daß es genau zwei  $\mathbb{C}^\times$ -Bahnen in Gitt gibt, deren Elemente nichttriviale Isotopiegruppen haben, nämlich die Bahnen der beiden Gitter  $\mathbb{Z} + \mathbb{Z}i$  und  $\mathbb{Z} + \mathbb{Z}e^{\pi i/3}$ .

*Ergänzende Übung 4.5.1.34.* Man finde ein Repräsentantensystem für die Bahnen unter der offensichtlichen Wirkung von  $\mathrm{GL}(n; \mathbb{Z}) \times \mathrm{GL}(m; \mathbb{Z})$  auf dem Matrizenraum  $\mathrm{Mat}(n \times m; \mathbb{Q})$ . Hinweis: 4.4.4.13.

*Übung 4.5.1.35.* In dieser Übung sollen Sie den **Satz von Cauchy** zeigen: Jeder Primfaktor der Ordnung einer endlichen Gruppe tritt auch als Ordnung eines Elements besagter Gruppe auf. Man zeige der Reihe nach:

1. Für eine Primzahl  $p$  und  $G = \mathrm{GL}(n; \mathbb{F}_p)$  und die Untergruppe  $N \subset G$  der unipotenten oberen Dreiecksmatrizen ist  $p$  kein Teiler von  $|G/N|$  und  $|N|$  eine Potenz von  $p$ ;
2. Jede endliche Untergruppe  $\Gamma \subset G$  ohne Elemente der Ordnung  $p$  operiert mit trivialen Standgruppen auf  $G/N$ , folglich muß ihre Ordnung  $|\Gamma|$  zu  $p$  teilerfremd sein;
3. Jede endliche Gruppe  $\Gamma$  läßt sich als Untergruppe in  $\mathrm{GL}(n; \mathbb{F}_p)$  für  $n = |\Gamma|$  oder kanonischer in  $\mathrm{GL}(\mathbb{F}_p\langle\Gamma\rangle)$  einbetten.

Einen anderen Beweis, bei dem vollständig innerhalb der Gruppentheorie argumentiert wird, können Sie in ?? finden. Er scheint mir jedoch im ganzen eher komplizierter.

## 4.5.2 Bahnformel

**Lemma 4.5.2.1 (Bahnen als Quotienten).** *Seien  $G$  eine Gruppe,  $X$  eine  $G$ -Menge und  $x \in X$  ein Punkt. So induziert die Abbildung  $G \rightarrow X$ ,  $g \mapsto gx$  eine Bijektion*

$$G/G_x \xrightarrow{\sim} Gx$$

*zwischen dem Quotienten nach der Standgruppe von  $x$  und der Bahn von  $x$ .*

*Beweis.* Für jede  $G_x$ -Linksnebenklasse  $L \subset G$  im Sinne von 4.4.1.2 besteht die Menge  $Lx$  nur aus einem Punkt, für  $L = gG_x$  haben wir genauer  $Lx = gG_xx = \{gx\}$ . Die Abbildung im Lemma wird nun definiert durch die Bedingung, daß sie jeder Nebenklasse  $L \in G/G_x$  das einzige Element von  $Lx$  zuordnet. Diese Abbildung ist offensichtlich surjektiv. Sie ist aber auch injektiv, denn aus  $gG_xx = hG_xx$  folgt  $gx = hx$ , also  $h^{-1}g \in G_x$ , also  $gG_x = hG_x$ .  $\square$

*Zweiter Beweis.* Die durch das Anwenden auf  $x \in X$  gegebene Abbildung  $G \rightarrow Gx$  und die kanonische Surjektion  $G \rightarrow G/G_x$  sind Surjektionen mit denselben Fasern. Die Behauptung folgt so aus 2.1.5.11.  $\square$

4.5.2.2. Ist  $G$  eine endliche Gruppe und  $X$  eine  $G$ -Menge, so folgt mit dem vorhergehenden Lemma 4.5.2.1 aus dem Satz von Lagrange 4.4.1.5 für alle  $x \in X$  insbesondere die sogenannte **Bahnformel**

$$|G| = |G_x| \cdot |Gx|$$

Die Kardinalität jeder Bahn teilt also die Kardinalität der ganzen Gruppe, und die Kardinalität der Standgruppen ist konstant auf den Bahnen. Genauer prüft man für beliebiges  $G$  die Formel  $G_{gx} = gG_xg^{-1}$  für  $g \in G, x \in X$ . Ist weiter  $X$  endlich und  $X = X_1 \sqcup \dots \sqcup X_n$  seine Zerlegung in Bahnen und  $x(i) \in X_i$  jeweils ein Element, so folgt

$$|X| = |X_1| + \dots + |X_n| = |G|/|G_{x(1)}| + \dots + |G|/|G_{x(n)}|$$

*Beispiel 4.5.2.3.* Seien  $k \leq n$  natürliche Zahlen. Auf der Menge  $X$  aller  $k$ -elementigen Teilmengen der Menge  $\{1, 2, \dots, n\}$  operiert die symmetrische Gruppe  $S_n$  transitiv. Die Standgruppe des Punktes  $x \in X$ , der durch die  $k$ -elementige Teilmenge  $\{1, 2, \dots, k\}$  gegeben wird, ist isomorph zu  $S_k \times S_{n-k}$ . Die Bahnformel liefert folglich  $|X| = n!/(k!(n-k)!)$  in Übereinstimmung mit unseren Erkenntnissen aus 1.1.1.19. Ähnlich kann man auch die in 2.1.5.19 diskutierten Formeln für die Multinomialkoeffizienten herleiten.

*Beispiel 4.5.2.4 (Zahl der Drehsymmetrien eines Würfels).* Wir können unsere Bahnformel auch umgekehrt anwenden. Nehmen wir zum Beispiel an, wir wollten die Drehungen zählen, die einen Würfel in sich überführen. Die Gruppe  $G$  dieser Drehungen operiert sicher transitiv auf der Menge  $E$  der acht Ecken des Würfels und die Standgruppe jeder Ecke  $p$  hat drei Elemente. Wir folgern  $|G| = |G_p| \cdot |E| = 3 \cdot 8 = 24$ .

## Übungen

*Ergänzende Übung 4.5.2.5.* Sind  $Q, H$  Untergruppen einer Gruppe  $G$ , so induziert die Einbettung  $Q \hookrightarrow G$  eine Bijektion  $Q/(Q \cap H) \xrightarrow{\sim} QH/H$ . Gemeint ist auf

der rechten Seite der Bahnenraum der Operation von rechts durch Multiplikation der Gruppe  $H$  auf der Teilmenge  $QH \subset G$ .

*Ergänzende Übung 4.5.2.6.* Ist  $G$  eine Gruppe und  $X$  eine  $G$ -Menge und  $Y$  eine  $G$ -Rechtsmenge, so erklärt man ihr **balanciertes Produkt**

$$Y \times_{/G} X$$

als die Menge aller  $G$ -Bahnen in  $Y \times X$  unter der Operation  $g(y, x) = (yg^{-1}, gx)$ .

Man zeige: Sind  $P, Q$  Untergruppen einer Gruppe  $G$  mit Schnitt  $S := P \cap Q$ , so induziert die Multiplikation eine Bijektion

$$P \times_{/S} Q \xrightarrow{\sim} PQ$$

*Ergänzende Übung 4.5.2.7.* Ist in der Bruhat-Zerlegung 4.5.6.1 der Körper  $k$  ein endlicher Körper  $k = \mathbb{F}_q$ , so wird die Kardinalität der Doppelnebenklasse  $BxB$  für  $x \in \mathcal{S}_n$  und  $B$  die oberen Dreicksmatrizen gegeben durch die Formel

$$|BxB| = |B|q^{l(x)}$$

mit  $l(x)$  der Zahl der Fehlstände der Permutation  $x$ . Hinweis: Man wende auf die  $(B \times B)$ -Bahnen von  $x \in \mathcal{S}_n \subset G$  die Bahnformel an.

### 4.5.3 Konjugationsklassen

**Definition 4.5.3.1.** Ist  $G$  eine Gruppe und  $x \in G$  ein Element, so ist die Abbildung

$$\begin{aligned} \text{int}_x : G &\rightarrow G \\ g &\mapsto xgx^{-1} \end{aligned}$$

ein Isomorphismus der Gruppe  $G$  mit sich selber. Er heißt die **Konjugation mit  $x$** . Ganz allgemein nennt man einen Isomorphismus einer Gruppe mit sich selber auch einen **Automorphismus** der Gruppe. Die Automorphismen einer Gruppe  $G$  bilden selber eine Gruppe mit der Verknüpfung von Abbildungen als Verknüpfung. Sie heißt die **Automorphismengruppe** von  $G$  und wir verwenden für sie die beiden Notationen  $\text{Aut}(G) = \text{Grp}^\times(G)$ . Diejenigen Automorphismen einer Gruppe, die sich als Konjugation mit einem geeigneten Gruppenelement schreiben lassen, heißen **innere Automorphismen** und auf englisch **interior automorphisms**, daher die Notation  $\text{int}$ . Sicher gilt  $\text{int}_x \circ \text{int}_y = \text{int}_{xy}$ , folglich ist  $\text{int} : x \mapsto \text{int}(x) := \text{int}_x$  ein Gruppenhomomorphismus  $\text{int} : G \rightarrow \text{Grp}^\times(G)$  und insbesondere eine Operation der Gruppe  $G$  auf der Menge  $G$ , die **Operation durch Konjugation**

$$\begin{aligned} G \times G &\rightarrow G \\ (x, y) &\mapsto \text{int}_x(y) = xyx^{-1} \end{aligned}$$

Die Bahnen dieser Operation heißen die **Konjugationsklassen** unserer Gruppe.

*Beispiele 4.5.3.2.* Die Konjugationsklassen in einer kommutativen Gruppe sind einelementig. Die Theorie der Jordan'schen Normalform beschreibt die Konjugationsklassen in  $\mathrm{GL}(n; \mathbb{C})$ , vergleiche 4.5.1.30.

### Übungen

*Ergänzende Übung 4.5.3.3.* Sei  $A$  eine zyklische Gruppe der Ordnung  $n \in \mathbb{N}$ . So gibt es genau einen Ringisomorphismus  $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{End} A$ , und dieser Ringisomorphismus induziert einen Isomorphismus zwischen der Einheitengruppe  $(\mathbb{Z}/n\mathbb{Z})^\times$  und der Automorphismengruppe von  $A$ .

*Ergänzende Übung 4.5.3.4.* Man gebe jeweils ein Repräsentantensystem an für die Konjugationsklassen der Gruppe aller Isometrien des affinen Skalarprodukt- raums  $\mathbb{R}^2$  und der Untergruppe ihrer orientierungserhaltenden Isometrien.

*Ergänzende Übung 4.5.3.5.* Wir betrachten die Gruppen  $G \supset K$  der Ähnlichkeiten und der Kongruenzen einer euklidischen Ebene. Man zeige, daß  $K$  stabil ist unter der Konjugation mit  $g \in G$  und daß die Konjugationsklassen von  $G$ , die in  $K$  enthalten sind, wie folgt beschrieben werden können:

1. Die Identität bildet für sich allein eine Konjugationsklasse;
2. Alle Verschiebungen, die nicht die Identität sind, bilden eine Konjugations- klasse;
3. Alle Spiegelungen an affinen Geraden bilden eine Konjugationsklasse;
4. Alle Gleitspiegelungen, die keine Spiegelungen sind, bilden eine Konjugati- onsklasse;
5. Für jeden Winkel  $\theta$  mit  $0 < \theta \leq 180^\circ$  bilden alle Drehungen um einen beliebigen Punkt und um einen Winkel mit dem Betrag  $\theta$  eine Konjugati- onsklasse.

Darüber hinaus gibt es keine weiteren Konjugationsklassen von  $G$  in  $K$ . Hinweis: 4.1.10.12.

*Ergänzende Übung 4.5.3.6.* Wir betrachten die Gruppen  $G \supset B$  der Ähnlichkeiten und der Bewegungen eines dreidimensionalen euklidischen Raums. Man zeige, daß  $B$  stabil ist unter der Konjugation mit  $g \in G$  und daß die Konjugati- onsklassen von  $G$ , die in  $B$  enthalten sind, wie folgt beschrieben werden können:

1. Die Identität bildet für sich allein eine Konjugationsklasse;
2. Alle Verschiebungen, die nicht die Identität sind, bilden eine Konjugations- klasse;

3. Für jeden Winkel  $\theta$  mit  $0 < \theta \leq 180^\circ$  bilden alle Drehungen um eine beliebige Achse und um einen Winkel mit dem Betrag  $\theta$  eine Konjugationsklasse;
4. Für jeden Winkel  $\theta$  mit  $0 < \theta \leq 180^\circ$  bilden alle Verschraubungen um einen Winkel mit dem Betrag  $\theta$ , die keine Drehungen sind, eine Konjugationsklasse.

Darüber hinaus gibt es keine weiteren Konjugationsklassen von  $G$  in  $B$ . Hinweis: 4.1.10.13.

#### 4.5.4 Endliche Untergruppen von Bewegungsgruppen

4.5.4.1. Die orthogonalaffinen orientierungserhaltenden Automorphismen eines euklidischen Raums  $R$  der Dimension drei nennen wir seine **Bewegungen**. Die Gruppe  $B$  aller Bewegungen von  $R$  nennen wir die **Bewegungsgruppe von  $R$** . Gegeben eine Teilmenge des Raums  $T \subset R$  nennen wir eine Bewegung  $b \in B$  mit  $b(T) = T$  eine **Symmetriebewegung von  $T$** . Die Symmetriebewegungen einer Teilmenge  $T \subset R$  bilden eine Untergruppe seiner Bewegungsgruppe. Bis auf Isomorphismus gibt es nur einen dreidimensionalen euklidischen Raum und man mag sich darunter den Anschauungsraum denken. Der folgende Satz ist in dieser Anschauung und in Bezug auf die aus der Schule bekannten platonischen Körper formuliert in der Hoffnung, daß er durch diesen Stilbruch verständlicher wird. Das exakte Formulieren im Rahmen der in dieser Vorlesung entwickelten Sprache holen wir später nach.

**Satz 4.5.4.2 (Endliche Untergruppen von Bewegungsgruppen).** *Jede endliche Untergruppe der Bewegungsgruppe ist genau eine der folgenden Gruppen:*

1. Eine **zyklische Gruppe**  $C_k$  mit  $k \geq 1$  Elementen, bestehend aus allen Drehungen zu einer festen Drehachse um Winkel der Gestalt  $2\pi n/k$ . Der Fall  $k = 1$  deckt hier den Fall der trivialen Gruppe ab, die nur aus der Identität besteht.
2. Eine **Diedergruppe**  $D_k$  mit  $2k$  Elementen für  $k \geq 2$ . Im Fall  $k > 2$  ist das die Gruppe aller Symmetriebewegungen eines ebenen gleichseitigen  $k$ -Ecks, aufgefaßt als räumliche Figur. Im Fall  $k = 2$  ist es die Gruppe aller derjenigen Drehungen, die von einem Paar sich schneidender orthogonaler Geraden jede in sich überführen.
3. Eine **Tetraedergruppe**  $T$  aller 12 Symmetriebewegungen eines Tetraeders.
4. Eine **Würfelgruppe**  $W$  aller 24 Symmetriebewegungen eines Würfels.

*5. Eine Ikosaedergruppe I aller 60 Symmetriebewegungen eines Ikosaeders.*

4.5.4.3. Will man diesen Satz einem Laien erklären, der mit dem Gruppenbegriff nicht vertraut ist, so mag man nach 3.4.3.7 auch einfacher von endlichen Mengen von Bewegungen reden, die mit je zwei Bewegungen stets auch deren Hintereinanderausführung enthalten. Vom mathematischen Standpunkt aus mag man das Resultat als eine Aufzählung der „Konjugationsklassen von endlichen Untergruppen der Bewegungsgruppe“ ansehen, also der Bahnen unter der Operation durch Konjugation unserer Bewegungsgruppe auf der Menge ihrer endlichen Untergruppen. Die endlichen Untergruppen der Isometriegruppe des Anschauungsraums werden in 4.5.4.25 diskutiert.

4.5.4.4. Das Evozieren der platonischen Körper stellt insofern einen Stilbruch dar, als wir uns zumindest implizit darauf verständigt hatten, alle unsere Überlegungen ausschließlich im Rahmen der Mengenlehre durchzuführen. Ein möglicher **Würfel** ist schnell beschrieben, man mag als Ecken für irgendeine Orthonormalbasis  $(\vec{v}_1, \vec{v}_2, \vec{v}_3)$  die acht Vektoren  $\pm \vec{v}_1 \pm \vec{v}_2 \pm \vec{v}_3$  nehmen, im  $\mathbb{R}^3$  also etwa  $(\pm 1, \pm 1, \pm 1)$ . Die Ecken eines **Tetraeders** erhält man, wenn man nur die vier Ecken dieses Würfels nimmt, bei denen das Produkt der Koordinaten Eins ist. Den **Ikosaeder** besprechen wir in 4.5.4.12 noch ausführlich. Zu den fünf sogenannten „platonischen Körpern“ rechnet man außer diesen dreien noch den **Oktaeder** und den **Dodekaeder**. Die Eckenmenge eines Oktaeders bilden etwa die drei Vektoren der Standardbasis des  $\mathbb{R}^3$  mitsamt ihren Negativen. Die Eckenmenge eines Dodekaeders mag man anschaulich als die Menge der „Flächenmitten eines Ikosaeders“ beschreiben und formal als die Menge der „Pole der Polordnung drei“ im Sinne des gleich folgenden Beweises im Fall der Symmetriegruppe eines Ikosaeders. Die Bezeichnungen Tetraeder, Oktaeder, Dodekaeder und Ikosaeder für die platonischen Körper außer dem Würfel kommen von den griechischen Worten für die Anzahlen 4, 8, 12 und 20 ihrer Flächen und dem griechischen Wort  $\varepsilon\delta\rho\alpha$  für „Sitz“ und dann auch „Sitzfläche“ her. Man findet für den Würfel wegen seiner 6 Flächen manchmal auch die Bezeichnung „Hexaeder“. „Dieder“ heißt eigentlich „Zweiflach“, womit wohl gemeint ist, daß er in gewisser Weise zwei Flächen hat, da man ihn ja wie einen Bierdeckel von beiden Seiten verschieden anmalen könnte.

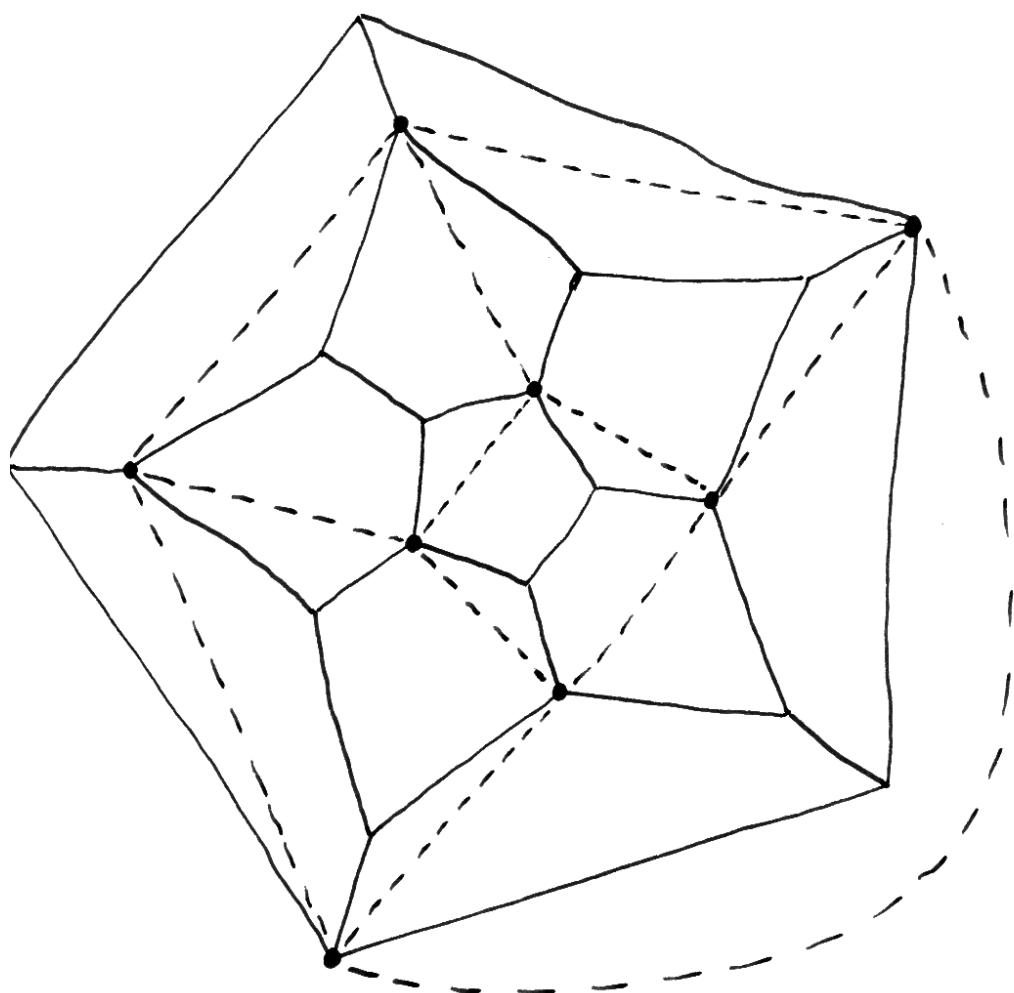
4.5.4.5. Die Diedergruppe  $D_4$  mag man sich auch als die Gruppe aller acht räumlichen Bewegungen veranschaulichen, die einen Bierdeckel in sich überführen. Sie wird deshalb auch die **Bierdeckelgruppe** genannt.

*Ergänzung 4.5.4.6 (Beziehungen zur Kristallographie).* Unser Satz 4.5.4.2 ist ein möglicher Ausgangspunkt der Kristallographie: Unter einem ***n*-dimensionalen Kristall** verstehen wir hier eine Teilmenge  $K$  eines  $n$ -dimensionalen euklidischen Raums  $E$ , etwa die Menge der Orte der Atome eines Kristallgitters, mit der Eigenschaft, daß (1) die Translationen aus ihrer Symmetriegruppe den Richtungsraum

aufspannen und daß es (2) eine positive untere Schranke gibt für die Längen aller von Null verschiedenen Translationen aus besagter Symmetriegruppe. Die zweite Eigenschaft schließt etwa den Fall aus, daß unsere Teilmenge einfach der ganze besagte Raum ist. Unter der **Punktgruppe**  $P$  eines Kristalls verstehen wir die Untergruppe  $P \subset O(\vec{E})$  aller linearen Anteile von Symmetrien unseres Kristalls, unter seiner **Drehgruppe**  $D \subset SO(\vec{E})$  die Menge aller orientationserhaltenden Elemente der Punktgruppe. Man zeigt, daß die Punktgruppe eines Kristalls stets endlich sein muß, und daß als Drehgruppen von räumlichen, als da heißt dreidimensionalen Kristallen nur die Gruppen  $C_k$  und  $D_k$  mit  $k \in \{1, 2, 3, 4, 6\}$  sowie die Tetraedergruppe und die Würfelgruppe auftreten können. Die Einteilung nach Drehgruppen entspricht in etwa, aber leider nicht ganz genau, der in der Kristallographie gebräuchlichen Einteilung in die sieben **Kristallsysteme**. Genauer entsprechen dem „kubischen System“ die Würfelgruppe und die Tetraedergruppe, dem „tetragonalen System“ die Drehgruppen  $C_4$  und  $D_4$ , dem „hexagonalen System“ die Drehgruppen  $C_6$  und  $D_6$ , dem „trigonalen System“ die Drehgruppen  $C_3$  und  $D_3$ , aber das „orthorhombische“, „monokline“ und „trikline System“ lassen sich erst anhand ihrer Punktgruppen unterscheiden. Auch in den übrigen Fällen liefert die Punktgruppe eine feinere Klassifikation. Für sie gibt es 32 Möglichkeiten, nach denen die Kristalle in die sogenannten **Kristallklassen** eingeteilt werden. Die eigentliche Klassifikation beschreibt alle als Symmetriegruppen von räumlichen Kristallen möglichen Bewegungsgruppen des Anschauungsraums bis auf Konjugation mit orientationstreuen Automorphismen des unserem euklidischen Raum zugrundeliegenden affinen Raums. Das darf nicht dahingehend mißverstanden werden, daß diese Automorphismengruppe durch Konjugation auf der Menge der möglichen Symmetriegruppen räumlicher Kristalle operieren würde, aber in vielen Fällen sind eben doch zwei derartige Symmetriegruppen konjugiert zueinander, und dann betrachtet man sie als zur selben Klasse gehörig. Es gibt im Raum genau 230 Kristallklassen. Erlaubt man auch Konjugation mit nicht orientationstreuen Automorphismen, so sinkt die Zahl der Klassen auf 219. Das **achtzehnte Hilbert'sche Problem** fragte unter anderem danach, ob es analog in jeder Dimension nur endlich viele Möglichkeiten für wesentlich verschiedene Kristalle gibt. Bieberbach konnte dafür einen Beweis geben.

**4.5.4.7 (Beziehungen zwischen den Symmetriegruppen platonischer Körper).** Eine Würfelgruppe kann auch als die Gruppe aller Symmetriebewegungen desjenigen Oktaeders aufgefaßt werden, dessen Ecken die Mittelpunkte der Flächen des Würfels sind. Ähnlich kann eine Ikosaedergruppe auch als Gruppe aller Symmetriebewegungen eines Dodekaeders aufgefaßt werden. Die Kantenmitten eines Tetraeders bilden die Ecken eines Oktaeders, so erhält man eine Einbettung der Tetraedergruppe in die Würfelgruppe.

**4.5.4.8 (Symmetriegruppen platonischer Körper als abstrakte Gruppen).** Die



Einer der fünf eingeschriebenen Würfel eines Dodekaeders, mit gestrichelt  
eingezeichneten Kanten.

Diedergruppe  $D_2$  ist isomorph zur Klein'schen Vierergruppe  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Sie kann vielleicht übersichtlicher auch beschrieben werden als die Gruppe aller Drehungen, die von einem Tripel paarweise orthogonaler Geraden jede in sich überführen. Neben der Identität liegen darin also die Drehungen um  $180^\circ$  um jede dieser drei Geraden. Die Tetraedergruppe kann man in die symmetrische Gruppe  $S_4$  einbetten mittels ihrer Operation auf den Ecken des Tetraeders. Wir erhalten so einen Isomorphismus der Tetraedergruppe mit der alternierenden Gruppe  $A_4$  aller geraden Permutationen von vier Elementen. Die Würfelgruppe operiert auf der Menge der vier räumlichen Diagonalen des Würfels und wir erhalten so einen Isomorphismus  $W \cong S_4$ . Die Ikosaedergruppe operiert auf der Menge der fünf eingeschriebenen Würfel eines Dodekaeders, von denen einer in nebenstehendem Bild schematisch dargestellt ist. Mit etwas Geduld kann man direkt einsehen, daß diese Operation einen Isomorphismus der Ikosaedergruppe  $I$  mit der alternierenden Gruppe  $A_5$  aller geraden Permutationen von 5 Elementen liefert. In ?? werden wir erklären, wie man das auch mit weniger Geduld aber mehr Gruppentheorie einsehen kann, und in ?? werden wir zusätzlich einen Isomorphismus dieser Gruppe mit der Gruppe  $\mathrm{SL}(2; \mathbb{F}_5)/\{\pm \mathrm{id}\}$  herleiten.

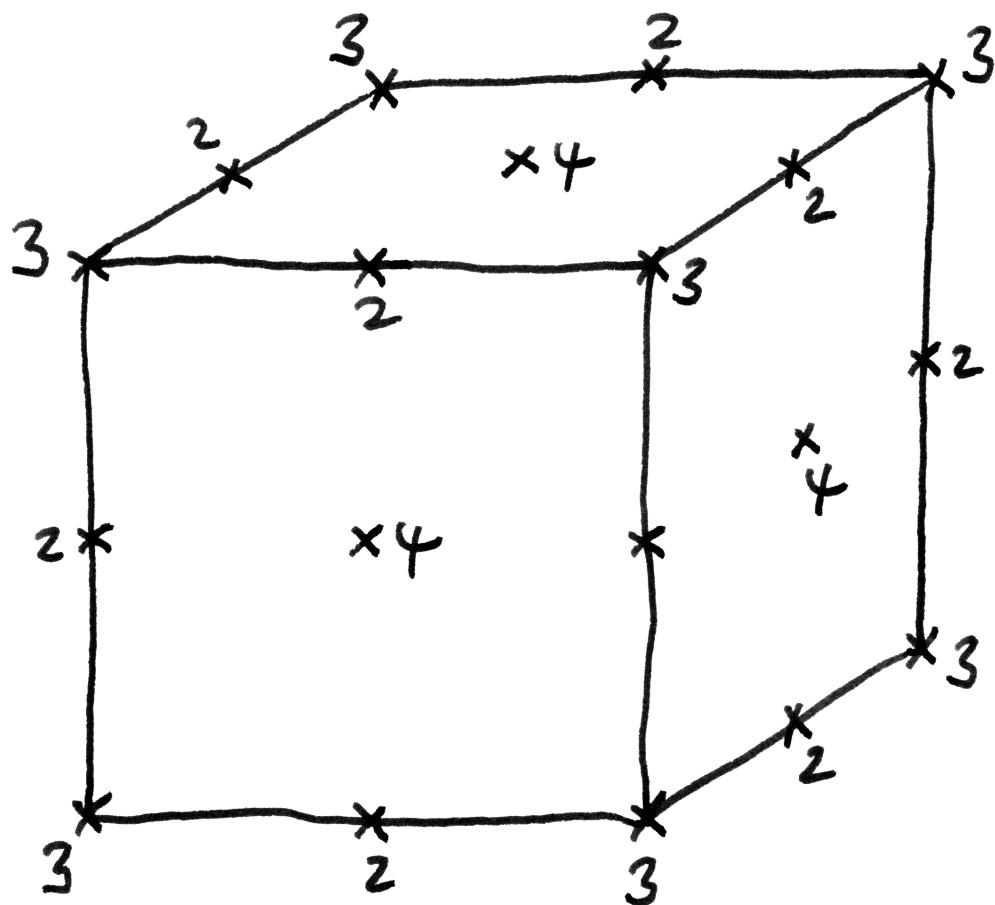
*Beweis von Satz 4.5.4.2.* Nach 4.5.1.28 besitzt jede endliche Gruppe von Automorphismen eines reellen affinen Raums mindestens einen Fixpunkt, genauer ist der Schwerpunkt 3.3.4.2 jeder Bahn ein Fixpunkt. Folglich reicht es, die endlichen Untergruppen der Drehgruppe  $\mathrm{SO}(3)$  zu klassifizieren. Sei also  $G \subset \mathrm{SO}(3)$  eine endliche Untergruppe. Für jede nichttriviale Drehung  $g \in \mathrm{SO}(3) \setminus \{1\}$  erklären wir ihre „Pole“ als die beiden Schnittpunkte ihrer Drehachse mit der Einheitssphäre  $S^2$ . Sei  $P$  die Menge aller Pole von Elementen von  $G \setminus \{1\}$ . Natürlich ist  $P$  eine endliche Menge und  $G$  operiert auf  $P$ . Wir zählen nun die Menge

$$M := \{(g, p) \in G \times S^2 \mid g \neq 1, gp = p\}$$

aller Paare  $(g, p)$  mit  $g \in G \setminus \{1\}$  und  $p$  einem Pol von  $g$  auf zwei Weisen. Einerseits gehört jedes von 1 verschiedene Gruppenelement  $g \in G \setminus \{1\}$  zu genau zwei Polen, andererseits gehört jeder Pol  $p \in P$  mit Standgruppe  $G_p$  zu genau  $|G_p| - 1$  von 1 verschiedenen Gruppenelementen. Zusammen erhalten wir so

$$2(|G| - 1) = |M| = \sum_{p \in P} (|G_p| - 1)$$

Sei nun  $P = P_1 \sqcup \dots \sqcup P_r$  die Bahnzerlegung von  $P$  und seien  $p_i \in P_i$  fest gewählt. Die Standgruppe von  $p_i$  habe sagen wir  $n_i \geq 2$  Elemente. Die zugehörige Bahn hat dann  $|P_i| = |G|/n_i$  Elemente und alle Standgruppen zu Polen  $p \in P_i$  haben  $|G_p| = n_i$  Elemente. Die Kardinalität der Standgruppe eines Pols nennen wir abkürzend auch die **Polordnung**. Insbesondere ist also  $n_i$  die Polordnung des Pols



Die „von vorne sichtbaren“ Pole der Würfelgruppe mit den Kardinalitäten der jeweiligen Standgruppen

$p_i$ . Fassen wir dann die Pole jeder Bahn in unserer Summe zu einem Summanden zusammen, so können wir in unserer Gleichung die rechte Seite umformen zu  $\sum_{i=1}^r (|G|/n_i)(n_i - 1)$  und Wegteilen von  $|G|$  liefert die Gleichung

$$2 - \frac{2}{|G|} = \sum_{i=1}^r \left(1 - \frac{1}{n_i}\right)$$

Jeder Summand auf der rechten Seite ist mindestens  $1/2$ , der Ausdruck links ist aber kleiner als 2. Es kommen also nur bis zu drei Bahnen von Polen in Betracht. Wir machen nun eine Fallunterscheidung nach der Zahl  $r$  der Bahnen von Polen.

**Fall 0:** Es gibt überhaupt keine Pole. In diesem Fall besteht  $G$  nur aus dem neutralen Element und wir haben die triviale Gruppe  $C_1$  vor uns.

**Fall 1:** Ganz  $P$  ist eine Bahn. Das ist unmöglich, denn es muß gelten  $|G| \geq 2$  wenn es überhaupt Pole geben soll, und damit hätten wir  $2 - \frac{2}{|G|} \geq 1 > 1 - \frac{1}{n_1}$  im Widerspruch zu unserer Gleichung.

**Fall 2:** Es gibt genau zwei Bahnen  $P_1$  und  $P_2$  in  $P$ . Wir haben dann

$$\frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2}$$

Natürlich haben wir  $n_i \leq |G|$  und damit notwendig  $n_1 = n_2 = |G|$ . Alle Pole werden also von der Gruppe festgehalten, es gibt folglich nur zwei Pole, die sich notwendig gegenüberliegen müssen. Damit sind wir im Fall der zyklischen Gruppen  $C_k$  mit  $k = n_1 = n_2 > 1$ .

**Fall 3:** Es gibt genau drei Bahnen  $P_1$ ,  $P_2$  und  $P_3$  in  $P$ , wir haben also

$$\frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} - 1$$

Wir dürfen annehmen  $n_1 \leq n_2 \leq n_3$ . Sicher gilt dann  $n_1 = 2$ , sonst wäre die rechte Seite  $\leq 0$ . Haben wir auch  $n_2 = 2$ , so kann  $n_3$  beliebige Werte annehmen und wir haben  $|G| = 2n_3$ . Die Bahn  $P_3$  besteht dann aus zwei Polen, die sich notwendig gegenüberliegen müssen, da sonst bereits die Bewegung eines dieser beiden Pole mit einer nichttrivialen Drehung und den anderen ein drittes Element der Bahn  $P_3$  liefern würde. Alle Gruppenelemente permutieren die beiden Pole aus  $P_3$  und unsere Gruppe wird damit eine Diedergruppe. Bleibt der Fall  $n_2 > 2$ . Hier sind  $(2, 4, 4)$  und  $(2, 3, 6)$  unmöglich für  $(n_1, n_2, n_3)$ , da ja gilt  $\frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$ . Also bleiben nur die Fälle  $(2, 3, 3)$ ,  $(2, 3, 4)$  und  $(2, 3, 5)$  und man berechnet leicht die zugehörigen Gruppenordnungen zu 12, 24, und 60.

Den Stand unseres Beweises bis hierher können wir wie folgt zusammenfassen: Wir haben eine Abbildung konstruiert – man mag sie die **Bahnpolordnungsabbildung** nennen – die jeder endlichen Untergruppe der Drehgruppe eine endliche Multimenge natürlicher Zahlen zuordnet, und haben gezeigt, daß in ihrem Bild höchstens die folgenden Multimengen liegen:

$$\emptyset, {}_\mu\{k, k\} \text{ und } {}_\mu\{2, 2, k\} \text{ für } k \geq 2, {}_\mu\{2, 3, 3\}, {}_\mu\{2, 3, 4\}, \text{ und } {}_\mu\{2, 3, 5\}.$$

Wir müssen nun noch zeigen, daß (1) die angegebenen Multimengen genau das Bild unserer Bahnpolordnungsabbildung sind, und daß (2) je zwei Drehgruppen mit demselben Bild unter der Bahnpolordnungsabbildung zueinander konjugiert sind. Wenn wir das alles gezeigt haben, so folgt, daß die Bahnpolordnungsabbildung eine Bijektion

$$\left\{ \begin{array}{l} \text{endliche Untergruppen} \\ \text{der Drehgruppe } SO(3), \\ \text{bis auf Konjugation} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \emptyset, {}_\mu\{k, k\} \text{ und } {}_\mu\{2, 2, k\} \text{ für } k \geq 2, \\ {}_\mu\{2, 3, 3\}, {}_\mu\{2, 3, 4\}, {}_\mu\{2, 3, 5\} \end{array} \right\}$$

liefert. Zusammen mit der beim Beweis erzeugten Anschauung zeigt das dann unseren Satz. Die Existenz endlicher Untergruppen der Drehgruppe mit derartigen Polbahnen und Polordnungen scheint mir anschaulich klar. Zum Beispiel hat die Würfelgruppe drei Polbahnen, als da sind: Eine Bahn aus den 8 Ecken zur Polordnung 3; eine Bahn aus den auf Länge Eins normierten 12 Mittelpunkten der Kanten, zur Polordnung 2; und eine Bahn aus den auf Länge Eins normierten 6 Mittelpunkten der Flächen, zur Polordnung 4. Diese Anschauung läßt sich auch leicht zu einem formalen Beweis präzisieren in allen Fällen mit Ausnahme des Ikosaeder-Falls (2, 3, 5). In diesem Fall folgt die Existenz formal erst aus 4.5.4.12. Daß je zwei zyklische Gruppen derselben endlichen Ordnung und je zwei Diedergruppen derselben endlichen Ordnung in der Drehgruppe zueinander konjugiert sind, scheint mir offensichtlich. Die folgenden beiden Lemmata 4.5.4.10 und 4.5.4.11 zeigen, daß auch je zwei Gruppen mit gegebenen Bahnpolordnungen oder, wie wir von jetzt an abkürzend sagen werden, zu gegebenem **Typ**  $(2, 3, n)$  in der Drehgruppe zueinander konjugiert sind. Damit vervollständigen sie den Beweis unseres Satzes.  $\square$

4.5.4.9. Man mag eine Teilmenge eines dreidimensionalen euklidischen Raums eine **platonische Eckenmenge** nennen, wenn die Gruppe ihrer Symmetriebewegungen endlich ist und transitiv auf unserer Teilmenge operiert und jedes ihrer Elemente von mindestens drei Symmetriebewegungen festgehalten wird. Man mag einen **platonischen Körper** erklären als die konvexe Hülle einer platonischen Eckenmenge. Unsere Überlegungen zeigen dann, daß es bis auf Ähnlichkeit in unserem Raum genau fünf platonische Körper gibt.

- Lemma 4.5.4.10.**
1. Jede endliche Untergruppe einer Drehgruppe von einem der beiden Typen  $(2, 3, 4)$  oder  $(2, 3, 5)$  ist maximal unter allen endlichen Untergruppen der Drehgruppe;
  2. Eine endliche Drehgruppe von einem der Typen  $(2, 3, n)$  mit  $n \geq 3$  kann beschrieben werden als der Stabilisator jeder ihrer beiden kleineren Bahnen von Polen.

*Beweis.* Nach unseren bisherigen Erkenntnissen kommen bei endlichen Drehgruppen für die Paare (Ordnung eines Pols, Kardinalität seiner Bahn) nur die Paare  $(n, 1), (n, 2), (2, n), (3, 4), (3, 8), (3, 20), (4, 6)$  und  $(5, 12)$  in Frage. Für jeden Pol müssen sich bei Übergang zu einer echt größeren Gruppe nach der Bahnformel entweder seine Polordnung oder die Kardinalität seiner Bahn oder beide vervielfachen. Das ist aber bei  $(4, 6)$  und  $(5, 12)$  unmöglich und wir erhalten die erste Behauptung. In den drei Fällen der zweiten Behauptung enthält weiter jede Bahn von Polen mindestens drei Punkte, also auch zwei verschiedene sich nicht gegenüberliegende Punkte. Folglich operiert sogar der Stabilisator in  $\mathrm{SO}(3)$  der Bahn  $P_i$  treu auf  $P_i$  und ist insbesondere endlich. Nun muß  $P_i$  auch unter diesem Stabilisator eine Bahn von Polen sein. Wenn die Symmetriegruppe von  $P_i$  größer sein will als die Drehgruppe, von der wir ausgegangen sind, muß sie also an den Polen aus  $P_i$  größere Polordnungen haben. Wieder ist das unmöglich bei  $(3, 4), (3, 8), (3, 20), (4, 6)$  und  $(5, 12)$ .  $\square$

**Lemma 4.5.4.11.** Sind zwei endliche Drehgruppen vom selben Typ  $(2, 3, n)$  mit  $n \geq 3$  gegeben und sind  $P_3$  und  $\tilde{P}_3$  jeweils zugehörige Polbahnen kleinstmöglicher Kardinalität, so gibt es eine Drehung, die  $P_3$  in  $\tilde{P}_3$  überführt.

*Beweis.* Für die Operation der Drehgruppe  $\mathrm{SO}(3)$  auf Paaren von Vektoren  $(p, q)$  durch  $g(p, q) := (gp, gq)$  ist klar, daß die Standgruppe jedes linear unabhängigen Paars trivial ist. Gegeben eine endliche Untergruppe  $G \subset \mathrm{SO}(3)$  und eine Bahn von Polen  $P_i$  ist insbesondere die Standgruppe eines Paars  $(p, q)$  mit  $p \neq \pm q$  trivial. Nach dieser Vorüberlegung betrachten wir die drei Fälle der Reihe nach.

Im Fall  $(2, 3, 3)$  haben wir  $|P_3| = 4$ . Folglich gibt es in  $P_3 \times P_3$  ein Paar mit trivialer Standgruppe, das also eine 12-elementige Bahn hat, die wegen  $|P_3 \times P_3| = 16$  notwendig aus allen  $(p, q)$  mit  $p \neq q$  bestehen muß. Je zwei verschiedene Punkte aus  $P_3$  haben also denselben Abstand. Ich hoffe, daß damit sowohl die Aussage des Lemmas im Fall  $n = 3$  klar wird als auch, daß die Punkte aus  $P_3$  die Ecken eines Tetraeders bilden.

Im Fall  $(2, 3, 4)$  haben wir  $|P_3| = 6$ . Folglich gibt es in  $P_3 \times P_3$  ein Paar mit trivialer Standgruppe, das also eine 24-elementige Bahn hat, die wegen  $|P_3 \times P_3| = 36$  notwendig aus allen  $(p, q)$  mit  $p \neq \pm q$  bestehen muß. Die anderen Bahnen müssen

aus Paaren mit nichttrivialer Standgruppe bestehen, und da die Bahn der sechs Paare der Gestalt  $(p, p)$  noch nicht genug Elemente liefert, muß auch noch eine Bahn aus Paaren der Gestalt  $(p, -p)$  vorkommen. Wir sehen so einerseits, daß  $P_3$  stabil ist unter Punktspiegelung am Ursprung, und andererseits, daß je zwei voneinander verschiedene Pole aus  $P_3$ , die sich nicht gegenüberliegen, denselben Abstand haben. So erkennen wir hoffentlich sowohl die Aussage des Lemmas im Fall  $n = 4$  als auch, daß die Elemente von  $P_3$  die Ecken eines Oktaeders bilden müssen.

Im Fall  $(2, 3, 5)$  haben wir  $|P_3| = 12$  und  $|P_3 \times P_3| = 144$ . Wieder haben wir an Bahnen in  $|P_3 \times P_3|$  die zwölfelementige Bahn aller Paare  $(p, p)$ , möglicherweise noch eine zwölfelementige Bahn aller Paare  $(p, -p)$ , und daneben nur Bahnen mit 60 Elementen. Es folgt, daß  $P_3 \times P_3$  in vier Bahnen zerfällt, und zwar die Bahn der Paare gleicher Pole, die Bahn der Paare von sich gegenüberliegenden Polen, und zwei weitere Bahnen von Polpaaren. Nehmen wir irgendeinen Pol  $p \in P_3$ , so bilden die Bilder von jedem Pol  $q \in P_3$  mit  $q \neq \pm p$  unter den Drehungen aus unserer Gruppe mit Fixpunkt  $p$  ein regelmäßiges Fünfeck, denn die Polordnung der Pole aus  $P_3$  war ja 5. Für zwei verschiedene Ecken eines regelmäßigen Fünfecks gibt es zwei Möglichkeiten für ihren Abstand, deren Verhältnis nebenbei bemerkt nach ?? oder elementargeometrischen Überlegungen gerade der goldene Schnitt ist. Unsere beiden 60-elementigen Bahnen müssen sich also im Abstand zwischen den Polen ihrer Paare unterscheiden. Zu jedem Pol aus  $P_3$  gibt es damit außer dem Pol selbst und dem gegenüberliegenden Pol noch 5 „nahe“ Pole und 5 „weite“ Pole. Nun bilden zwei sich gegenüberliegende Pole aus  $P_3$  mit jedem weiteren Pol ein Dreieck, das nach dem Satz des Thales bei diesem weiteren Pol einen rechten Winkel hat, wobei dieser Pol notwendig zu einem von unseren beiden sich gegenüberliegenden Polen nah sein muß und zum anderen weit, da ja zu jedem unserer sich gegenüberliegenden Pole von den zehn verbleibenden Polen fünf nah und fünf weit sein müssen. Da unser Dreieck eine Hypotenuse der Länge 2 hat, wird dadurch der Abstand zwischen nahen Polen und der zwischen weiten Polen bereits vollständig beschrieben und hängt insbesondere nicht von unserer Gruppe ab. Damit erkennen wir, daß im Fall  $(2, 3, 5)$  die Bahn  $P_3$  bestehen muß aus (1) zwei gegenüberliegenden Punkten  $N$  und  $S = -N$  sowie (2) zwei regelmäßigen Fünfecken der fünf zu  $N$  nahen Pole und der fünf zu  $S$  nahen Pole mit jeweils von der speziellen Gruppe unabhängigem Abstand der Ecken dieser Fünfecke zu den jeweiligen Polen. Jede Ecke des „nördlichen“ Fünfecks muß aber auch einer Ecke des „südlichen“ Fünfecks gegenüberliegen. Unser Lemma folgt unmittelbar.  $\square$

**Lemma 4.5.4.12 (Existenz der Ikosaedergruppe).** *Es gibt endliche Untergruppen der Drehgruppe  $\text{SO}(3)$  mit Elementen der Ordnungen drei und fünf.*

*Beweis.* Wir betrachten die Menge  $\mathcal{D} \subset \mathcal{P}(S^2)$  aller gleichseitigen Dreiecke mit Ecken auf der Einheitssphäre, die nicht in einer Ebene mit dem Ursprung liegen,

formal also

$$\mathcal{D} = \left\{ \{a, b, c\} \mid \begin{array}{l} a, b, c \in \mathbb{R}^3, \|a\| = \|b\| = \|c\| = 1, \\ \|a - b\| = \|b - c\| = \|c - a\|, \\ \langle a, b, c \rangle_{\mathbb{R}} = \mathbb{R}^3. \end{array} \right\}$$

Gegeben ein Dreieck  $\Delta \in \mathcal{D}$  und eine Ecke  $a \in \Delta$  definieren wir das **umgeklappte Dreieck**  $\Delta^a \in \mathcal{D}$  als das eindeutig bestimmte gleichseitige Dreieck  $\Delta^a \in \mathcal{D}$  mit  $\Delta \cap \Delta^a = \{b, c\}$ . Definieren wir zu einem Dreieck  $\Delta \in \mathcal{D}$  die Menge

$$\mathcal{D}(\Delta)$$

als die kleinste Teilmenge  $\mathcal{D}(\Delta) \subset \mathcal{D}$ , die  $\Delta$  enthält und stabil ist unter dem Umklappen von Dreiecken, so gilt offensichtlich  $\mathcal{D}(\Delta) = \mathcal{D}(\Delta')$  für alle  $\Delta' \in \mathcal{D}(\Delta)$ . Ist  $r \in O(3)$  orthogonal, so gilt sicher  $\{ra, rb, rc\}^{ra} = r(\{a, b, c\}^a)$  für jedes Dreieck  $\{a, b, c\} \in \mathcal{D}$ , das mit  $r$  gedrehte Dreieck am Bild  $r(a)$  der Ecke  $a$  umklappen liefert also dasselbe wie das an der Ecke  $a$  umgeklappte Dreieck mit  $r$  drehen, und insbesondere gilt  $r(\mathcal{D}(\Delta)) = \mathcal{D}(r\Delta)$ . Haben wir nun zusätzlich  $|r(\Delta) \cap \Delta| \geq 2$ , so folgt  $r\Delta \in \mathcal{D}(\Delta)$  und damit  $\mathcal{D}(r\Delta) = \mathcal{D}(\Delta)$ . Nach diesen Vorüberlegungen gehen wir nun aus von einem regelmäßigen Fünfeck, bilden darauf die Pyramide mit Spitze  $N$  und aufsteigenden Kanten von derselben Länge wie die Kanten des Fünfecks, und schrumpfen oder strecken diese Pyramide so, daß wir sie als „Polkappe“ in die Einheitssphäre legen können. Dann gehen offensichtlich die fünf gleichseitigen Dreiecke dieser Polkappe durch Umklappen auseinander hervor. Bezeichne  $\mathcal{D}^* \subset \mathcal{D}$  die kleinste unter Umklappen stabile Menge von Dreiecken, die diese fünf Dreiecke umfaßt. Wir zeigen im folgenden, daß  $\mathcal{D}^*$  endlich ist: Dann bilden alle Drehungen, die  $\mathcal{D}^*$  in sich überführen, offensichtlich eine endliche Untergruppe der Drehgruppe mit Elementen der Ordnungen drei und fünf und wir sind fertig. Um zu zeigen, daß  $\mathcal{D}^*$  endlich ist, bilden wir zu  $\mathcal{D}^*$  einen Graphen im Sinne von 4.5.4.22 wie folgt: Als Graphenecken nehmen wir alle fünfelementigen Teilmengen von  $\mathcal{D}^*$  vom Typ „Polkappe“, die also aus einem festen Dreieck mit ausgezeichneter Ecke durch wiederholtes Umklappen unter Festhalten dieser einen ausgezeichneten Ecke gewonnen werden können. Nun verbinden wir zwei verschiedene derartige Graphenecken durch eine Graphenkannte genau dann, wenn sie mindestens ein Dreieck gemeinsam haben. So erhält man aus  $\mathcal{D}^*$  einen zusammenhängenden Graphen mit den Eigenschaften aus Übung 4.5.4.22: Jede Graphenecke hat genau fünf Nachbarn, und je zwei benachbarte Graphenecken haben genau zwei gemeinsame Nachbarn. Nach Übung 4.5.4.22 ist ein zusammenhängender Graph mit diesen Eigenschaften jedoch endlich und damit muß auch unsere Menge von Dreiecken  $\mathcal{D}^*$  endlich gewesen sein.  $\square$

*Ergänzung 4.5.4.13.* Die obigen Überlegungen kann man dahingehend zusammenfassen, daß gegeben ein gleichseitiges Dreieck  $\Delta = \{a, b, c\}$ , für das es eine

Drehung  $r$  um die Ursprungsgerade durch  $a$  gibt mit  $r^5 = \text{id}$  und  $r : b \mapsto c$ , die Menge  $\mathcal{D}(\Delta)$  der daraus durch Umklappen entstehenden Dreiecke endlich ist. Die hier geforderte Eigenschaft hat sicher jedes Dreieck, das anschaulich gesprochen „Fläche eines Ikosaeders“ ist. Es gibt aber auch noch andere gleichseitige Dreiecke mit dieser Eigenschaft, nämlich diejenigen gleichseitigen Dreiecke, die anschaulich gesprochen die „Diagonale unseres Ausgangsfünfecks“ als Seitenlänge haben.

*Ergänzung 4.5.4.14.* Mit welchen platonischen Körpern kann man den Raum füllen? Ich vermute, das geht nur mit Würfeln: Die anderen sollten als Winkel zwischen an einer Kante angrenzenden Flächen nie einen Winkel der Gestalt  $2\pi/n$  haben.

*Ergänzung 4.5.4.15.* Vielleicht ist es vernünftig, platonische Körper zu definieren über die Mengen ihrer Ecken, die man wohl wie folgt charakterisieren kann: Man definiere für eine endliche Teilmenge  $E$  des Raums ihre **Abständezahl**  $A(E)$  als die Zahl der möglichen von Null verschiedenen verschiedenen Abstände zwischen ihren Elementen. Eine endliche Teilmenge  $E$  einer Sphäre heißt nun Tetraeder bei  $|E| = 4$ ,  $A(E) = 1$ , Würfel bei  $|E| = 8$ ,  $A(E) = 3$ , Oktaeder bei  $|E| = 6$ ,  $A(E) = 2$ , Ikosaeder bei  $|E| = 12$ ,  $A(E) = 3$ , Dodekaeder bei  $|E| = 20$ ,  $A(E) = 4$ . Stimmt das eigentlich? Möglicherweise sollte man bei allen außer dem Tetraeder noch fordern, daß  $E$  stabil ist unter Punktspiegelung am Ursprung.

## Übungen

*Übung 4.5.4.16.* Man berechne den Cosinus des Winkels zwischen zwei Seitenflächen eines Tetraeders. Hinweis: Man argumentiere, daß die Normalenvektoren auf die Flächen eines Tetraeders die Ecken eines Tetraeders bilden. Man bemerke, daß die Standardbasisvektoren im  $\mathbb{R}^4$  einen Tetraeder bilden. Wieviele Tetraeder kann man längs einer gemeinsamen Kante zusammenlegen? Bleibt dann noch Luft? Hier mag ein Taschenrechner helfen.

*Weiterführende Übung 4.5.4.17.* Gegeben ein zusammenhängender ebener Graph, bei dem an jeder Ecke drei Kanten ankommen, leite man aus der Eulerschen Formel  $E - K + F = 2$  her, daß es eine Fläche mit höchstens fünf Kanten geben muß. Hier haben wir die unbeschränkte Fläche mitgezählt.

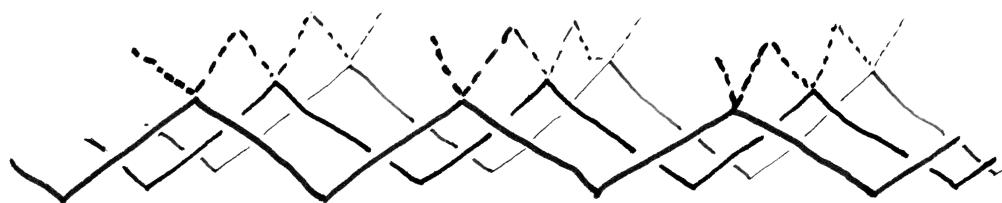
*Ergänzende Übung 4.5.4.18 (Kristallgitter des Diamants).* Seien  $v_1, \dots, v_4$  Richtungsvektoren des dreidimensionalen Anschauungsraums, die vom Schwerpunkt eines Tetraeders zu seinen vier Ecken zeigen. Wir betrachten alle Linearkombinationen  $\sum_{i=1}^4 n_i v_i$  mit  $\sum_{i=1}^4 n_i \in \{0, 1\}$  und behaupten, daß diese Linearkombinationen gerade die Punkte beschreiben, an denen in einem Diamant die Kohlenstoffatome sitzen. In der Tat sind unsere Linearkombinationen paarweise verschieden, die „einzig“ Relation  $v_1 + v_2 + v_3 + v_4 = 0$  unserer Vektoren

führt aufgrund unserer Einschränkungen nicht zu Mehrdeutigkeiten, und unsere Linearkombinationen lassen sich auch beschreiben als die Elemente des von den Richtungsvektoren  $v_1 - v_2, v_1 - v_3$  und  $v_1 - v_4$  erzeugten Gitters mitsamt dem um  $v_1$  verschobenen Gitter. Jeder Punkt hat vier nächste Nachbarn, der Nullpunkt etwa  $v_1, \dots, v_4$ , und zu diesen ist er gebunden im Diamantkristall. Anschaulich mag man sich eine Lage von parallelen horizontalen Zick-Zack-Linien denken, die Zick-Zacks darin nach oben und unten, dann eine weitere horizontale Lage senkrecht dazu, bei denen die Tiefpunkte immer gerade die Hochpunkte der Lage darunter berühren, und so weiter, und schließlich an jedem dieser Berührungs-punkte ein Kohlenstoffatom.

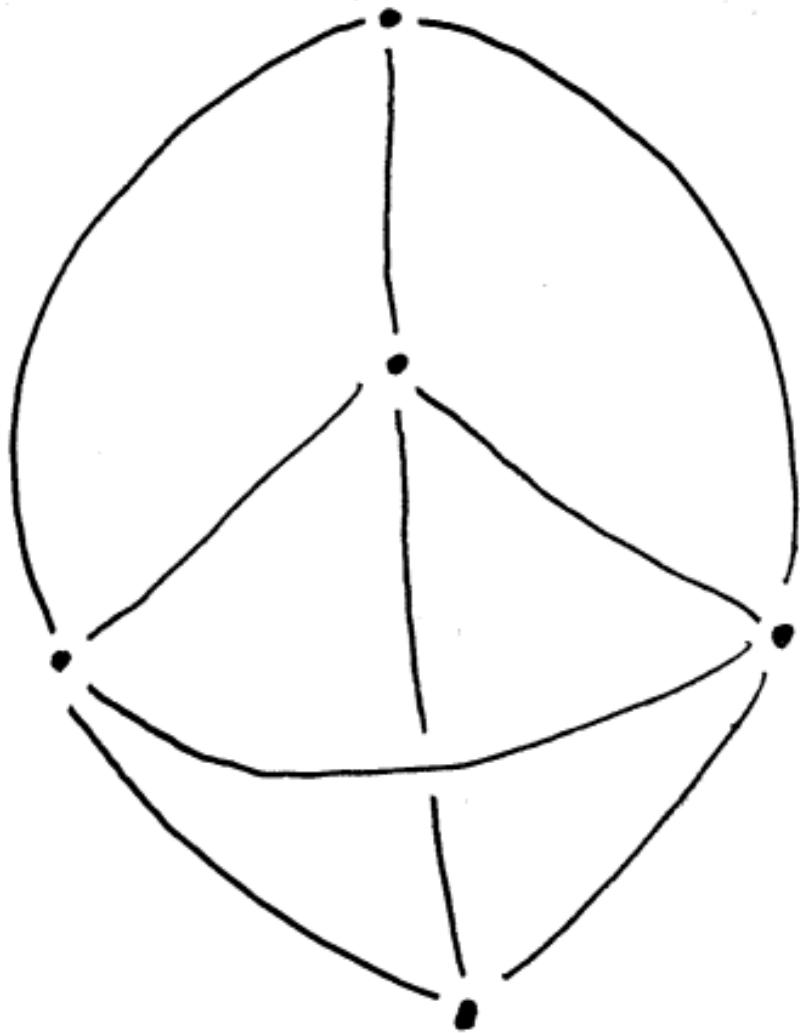
*Ergänzende Übung 4.5.4.19.* Man konstruiere einen surjektiven Gruppenhomomorphismus  $\mathcal{S}_4 \twoheadrightarrow \mathcal{S}_3$ . Hinweis: Geometrisch mag man sich die  $\mathcal{S}_4$  nach 4.5.4.8 als die Gruppe der Symmetriebewegungen eines Würfels denken und den fraglichen Gruppenhomomorphismus konstruieren über die Operation dieser Gruppe auf der Menge der drei Mittelsenkrechten auf den Flächen des Würfels. Später werden wir verstehen, daß dieser Homomorphismus etwas ganz besonderes ist: Surjektive nicht bijektive Gruppenhomomorphismen  $\mathcal{S}_n \twoheadrightarrow G$  einer symmetrischen Gruppe auf irgendeine andere Gruppe gibt es unter der Annahme  $n \geq 5$  nur für  $|G| = 2$  und dann jeweils nur genau Einen, vergleiche ??.

*Ergänzende Übung 4.5.4.20.* Die Multiplikation definiert einen Isomorphismus zwischen der Gruppe aller Symmetrien aus  $O(3)$  eines Ikosaeders und dem Produkt der Gruppe seiner Symmetriebewegungen mit der zweielementigen Gruppe, die von der Punktspiegelung am Ursprung erzeugt wird. Insbesondere ist die „nichtorientierte Ikosaedergruppe“ keineswegs isomorph zur symmetrischen Gruppe  $\mathcal{S}_5$ .

4.5.4.21. Unter einem **Graphen** oder genauer einem **kombinatorischen Graphen** (ungerichtet, ohne mehrfache Kanten, ohne Schleifen) verstehen wir ein Paar  $(E, K)$  bestehend aus einer Menge  $E$  und einem System  $K \subset \mathcal{P}(E)$  von zweielementigen Teilmengen von  $E$ . Die Elemente von  $E$  heißen die **Ecken** unseres Graphen, die Elemente von  $K$  seine **Kanten**. Zwei verschiedene Ecken, die zu einer gemeinsamen Kante gehören, heißen **benachbart**. Ein **Isomorphismus** zwischen zwei Graphen ist eine Bijektion zwischen ihren Eckenmengen, die eine Bijektion zwischen ihren Kantenmengen induziert. Zwei Graphen heißen **isomorph**, wenn es zwischen ihnen einen Isomorphismus gibt. Die Äquivalenzklassen der kleinsten Äquivalenzrelation auf der Eckenmenge eines Graphen, unter der benachbarte Elemente äquivalent sind, heißen die **Zusammenhangskomponenten** unseres Graphen. Ein Graph heißt **zusammenhängend**, wenn er aus einer einzigen Zusammenhangskomponente besteht.



Versuch einer graphischen Darstellung der räumlichen Struktur des Diamantkristalls. Die durchgezogenen und gestrichelten Linien sind nur der Transparenz halber verschiedenartig gezeichnet und bedeuten die Bindungen zwischen den Kohlenstoffatomen, die jeweils an den Ecken der Zick-Zack-Linien sitzen. Die hier gezeichnete Struktur gilt es nun übereinanderzuschichten, so daß sich jeweils die Ecken treffen.



Ein zusammenhängender Graph mit fünf Punkten, von denen drei vier Nachbarn haben und zwei nur drei Nachbarn. Die beiden Punkte „auf halber Höhe auf dem Rand“ haben drei gemeinsame Nachbarn.

*Übung 4.5.4.22.* Man zeige: Ein zusammenhängender Graph, in dem jede Ecke genau fünf (vier, drei) Nachbarn besitzt und je zwei benachbarte Ecken genau zwei gemeinsame Nachbarn, ist notwendig endlich und sogar isomorph zu jedem weiteren Graphen mit diesen beiden Eigenschaften. Den so charakterisierten Graphen mag man den „Kantengraphen des Ikosaeders (Oktaeders, Tetraeders)“ nennen. Hinweis: Ausprobieren.

*Übung 4.5.4.23 (Endliche Untergruppen der  $SU(2)$ ).* Man zeige, daß die Gruppe  $SU(2)$  nur zwei Elemente  $g$  besitzt mit  $g^2 = 1$ , nämlich  $g = \pm \text{id}$ . Man zeige, daß jede endliche Untergruppe ungerader Kardinalität  $n$  von  $SU(2)$  konjugiert ist zur Untergruppe  $\{\text{diag}(\zeta^r, \zeta^{-r}) \mid 1 \leq r \leq n\}$  für  $\zeta = \exp(2\pi i/n)$ . Man zeige, daß die endlichen Untergruppen gerader Kardinalität von  $SU(2)$  genau die Urbilder von endlichen Untergruppen von  $SO(3)$  unter unserer Surjektion  $SU(2) \rightarrow SO(3)$  aus 4.1.11.26 sind, die wir nach 4.5.4.2 bereits kennen. Das benötigt den Satz von Cauchy 4.5.1.35.

*Übung 4.5.4.24 (Ikosaeder).* Es gibt in der Einheitssphäre zwölfelementige Teilmengen, die stabil sind unter der Drehung mit den Winkeln  $\pm 2\pi/5$  um die Ursprungsgeraden durch jeden ihrer Punkte, und je zwei derartige Teilmengen lassen sich durch eine Drehung ineinander überführen.

*Übung 4.5.4.25 (Endliche Untergruppen der Isometriegruppe des Raums).* Jede Wahl eines von Null verschiedenen Richtungsvektors versieht den Anschauungsraum mit einer Metrik. Alle diese Metriken unterscheiden sich nur um eine positive reelle Konstante und liefern folglich dieselben Isometrien. Die Gruppe aller Isometrien des Anschauungsraums ist damit wohldefiniert. Sie kann im übrigen auch beschrieben werden als die von allen Bewegungen und allen Punktspiegelungen erzeugte Gruppe von Selbstabbildungen. Diejenigen Isometrien des Anschauungsraums, die eine gegebene Teilmenge festhalten, nenne ich ihre **Isometriesymmetrien** oder im folgenden auch kurz **Symmetrien**. Man zeige, daß jede endliche Untergruppe der Gruppe der Isometrien alias abstandserhaltenden Selbstabbildungen des Anschauungsraums konjugiert ist zu genau einer Untergruppe der folgenden Liste:

1. Der Gruppe aller Symmetrien beziehungsweise Symmetriebewegungen eines Tetraeders, Würfels, oder Ikosaeders, insgesamt 6 Fälle mit den Kardinalitäten 24, 12, 48, 24, 120, 60;
2. Der Gruppe aller Symmetrien bzw. Symmetriebewegungen eines regelmäßigen  $k$ -eckigen Bierdeckels,  $k \geq 3$ , also 2 Fälle für jedes  $k$  von Gruppen der Kardinalitäten  $4k$  und  $2k$ ;
3. Der Gruppe aller Symmetrien beziehungsweise Symmetriebewegungen einer regelmäßigen  $k$ -eckigen Schale,  $k \geq 3$ , also 2 Fälle für jedes  $k$  von Gruppen der Kardinalitäten  $2k$  und  $k$ ;

4. Der Gruppe aller Symmetrien beziehungsweise Symmetriebewegungen, die von einem Tripel bestehend aus drei durch einen gemeinsamen Punkt laufenden paarweise orthogonalen Geraden jede der drei Geraden stabilisieren und eine beziehungsweise zwei dieser Geraden punktweise festhalten. In Formeln übersetzt und nach den entsprechenden Identifikationen also einer der Untergruppen  $\text{diag}(\pm 1, 1, 1)$ ,  $\text{diag}(\pm 1, \pm 1, 1)$ ,  $\text{diag}(\pm 1, \pm 1, \pm 1)$  oder ihrer Schnitte mit der Drehgruppe  $\text{SO}(3)$ , insgesamt 6 Fälle mit den Kardinalitäten 2, 1, 4, 2, 8, 4;

*Übung 4.5.4.26 (Existenz des Ikosaeders, Alternative).* Die Würfelgruppe ist isomorph zur Gruppe  $S_4$  aller Permutationen seiner Raumdiagonalen. Die Drehungen an Raumdiagonalen erzeugen darin die Untergruppe  $A_4$  aller geraden Permutationen seiner Raumdiagonalen. Es gibt zwei Möglichkeiten, jeder Fläche des Würfels ein Paar von parallelen Kanten derselben Fläche so zuzuordnen, daß diese Wahl stabil ist unter  $A_4$ . Jetzt sollen einige der Kanten des Ikosaeders in der Mitte der Flächen unseres Würfels liegen, parallel zu den jeweils ausgewählten beiden Kanten, und nun muß man nur noch ihre Länge so bestimmen, daß die Abstände zwischen „benachbarten Kantenenden“ gleich der Kantenlängen sind. Man muß dann allerdings noch etwas argumentieren, um zu zeigen, daß die so gewonnene Menge von „Ecken des Ikosaeders“ Symmetrien der Ordnung fünf hat.

#### 4.5.5 Diskussion der Eulerformel\*

4.5.5.1. Indem man bei unseren platonischen Körpern die Zahlen  $E, K, F$  der Ecken, Kanten und Flächen bestimmt, prüft man unmittelbar in allen fünf Fällen die **Eulerformel**

$$E - K + F = 2$$

Diese Beziehung gilt allgemeiner für jede „kompakten konvexen dreidimensionalen Polyeder“, nur habe ich gar nicht definiert, was das eigentlich sein soll, und habe selbst bei den platonischen Körpern nur definiert, was für Teilmengen des Raums nun diesen Namen verdienen sollen, und nicht, wie denn nun die „Kanten“ oder „Flächen“ dieser Gebilde definiert werden sollen, die wir bereits so unbekümmert gezählt haben. Eine Formalisierung des Begriffs eines „dreidimensionalen konvexen Polyeders“ und seiner „Ecken, Kanten und Flächen“ wird in 3.3.5.18 ausgeführt, aber das schien mir hier unangemessen und sogar irreführend, da unsere Eulerformel anderer Natur ist. Im folgenden formuliere ich sehr präzise eine sehr allgemeine Fassung dieser Formel, gebe jedoch statt eines Beweises nur einige sehr unvollkommene heuristische Argumente.

4.5.5.2. Ich erinnere den Begriff eines Homöomorphismus aus ?? . Man bemerke, daß  $\mathbb{R}^2$  nicht homöomorph ist zu  $\mathbb{R}^1$ . In  $\mathbb{R}^2$  ist nämlich das Komplement jedes

Punktes zusammenhängend, in  $\mathbb{R}^1$  dahingegen ist das Komplement jedes Punktes unzusammenhängend.

**Satz 4.5.5.3 (Topologische Eulerformel).** Sei  $S^2 = A_1 \sqcup \dots \sqcup A_n$  eine Zerlegung der Einheitssphäre  $S^2 := \{x \in \mathbb{R}^3 \mid \|x\| = 1\}$  in endlich viele paarweise disjunkte Teilmengen  $A_i$ , die die beiden folgenden Eigenschaften hat:

1. Für jeden Index  $i$  ist  $A_1 \sqcup \dots \sqcup A_i$  abgeschlossen in  $S^2$ ;
2. Jedes  $A_i$  ist homöomorph zu  $\mathbb{R}^2$  oder  $\mathbb{R}^1$  oder  $\mathbb{R}^0$  alias einem Punkt.

So gilt die **Euler-Formel**  $E - K + F = 2$  für  $E, F$  und  $K$  die Zahl der jeweils zu  $\mathbb{R}^0, \mathbb{R}^1$  und  $\mathbb{R}^2$  homöomorphen  $A_i$ .

4.5.5.4. Die Bezeichnungen  $E, K$  und  $F$  stehen für „Ecken, Kanten und Flächen“. Man prüft die Formel leicht explizit für die durch die Zentralprojektion eines platonischen Körpers auf die Einheitssphäre gegebene Zerlegung derselben in die Bilder seiner Ecken, Kanten und Flächen. Besitzt allgemeiner ein lokal kompakter Hausdorffraum  $X$  eine Zerlegung

$$X = A_1 \sqcup \dots \sqcup A_n$$

in endlich viele paarweise disjunkte Teilmengen derart, daß für jeden Index  $i$  gilt  $A_1 \sqcup \dots \sqcup A_i \subset X$  und daß jedes  $A_i$  homöomorph ist zu  $\mathbb{R}^{d(i)}$  für ein  $d(i) \geq 0$ , so ist  $\sum_i (-1)^{d(i)}$  unabhängig von der Wahl einer derartigen Zerlegung. Den Beweis der topologischen Euler-Formel 4.5.5.3 und auch dieser allgemeineren Aussage für beliebige lokal kompakte Hausdorffräume können Sie in ?? finden. Er benötigt vertiefte Kenntnisse in Topologie.

4.5.5.5 (Diskussion einiger nicht erlaubter Zerlegungen). Um die Aussage des Satzes herauszuarbeiten, will ich einige nicht erlaubte Zerlegungen angeben. Betrachten wir die ganze Einheitssphäre als eine einzige Fläche, so gilt unsere Formel sicher nicht. Die Einheitssphäre ist aber auch nicht homöomorph zu  $\mathbb{R}^2$ , zum Beispiel, da sie kompakt ist. Zerlegen wir die Einheitssphäre in den Äquator und die beiden Hemisphären, so gilt unsere Formel ebensowenig. Der Äquator ist aber auch nicht homöomorph zu  $\mathbb{R}^1$ , zum Beispiel, da er kompakt ist. Zerlegen wir den Äquator in einen Punkt und eine Kante, so gelten unserer Annahmen und unsere Formel. Malen wir noch einen zweiten in derselben Weise zerlegten Äquator daneben, so wird sie wieder falsch. Das liegt daran, daß die „ringförmige Fläche“ zwischen unseren beiden Äquatoren nicht homöomorph ist zu  $\mathbb{R}^2$ , was hier nicht formal gezeigt werden soll. Verbinden wir aber die beiden ausgewählten Punkte auf unseren beiden Äquatoren noch durch eine Kante, so wird unsere Formel wieder richtig und die Bedingungen des Satzes sind auch wieder erfüllt.

**4.5.5.6 (Heuristische Begründung der Eulerformel).** Wir gehen aus von der Zerlegung der Einheitssphäre in einen Punkt und sein Komplement. In diesem Fall gilt die Eulerformel. Jetzt argumentieren wir induktiv und gehen von einer Zerlegung der Einheitssphäre in Ecken, Kanten und Flächen aus, in der wir die Eulerformel bereits geprüft haben.

1. Ergänzen wir eine Ecke, indem wir eine bereits existierende Kante in zwei Kanten zerteilen, so entsteht eine neue Zerlegung mit einer zusätzlichen Ecke und einer zusätzlichen Kante.
2. Ergänzen wir eine Kante, indem wir zwei Ecken auf dem Rand einer bereits vorhandenen Fläche innerhalb dieser Fläche durch eine Kante verbinden, so entsteht eine neue Zerlegung mit einer zusätzlichen Kante und einer zusätzlichen Fläche, da ja unsere Fläche von unserer neuen Kante in zwei Teile geschnitten wird.

Induktiv folgt so die Eulerformel für alle Zerlegungen der Einheitssphäre in Ecken, Kanten und Flächen, die wir auf diese Weise induktiv konstruieren können. Die Schwäche der vorhergehenden Argumentation ist zusätzlich zur allgemeinen Unschärfe der darin verwendeten Begriffe, daß nicht klar ist, welche Zerlegungen der Einheitssphäre in Ecken, Kanten und Flächen wir denn mit dem im Beweis beschriebenen Verfahren induktiv erreichen können. Da aber diese Fragen nur mit dem Aufbau eines entsprechend starken Begriffsapparats befriedigend geklärt werden können, will ich sie hier nicht weiter verfolgen.

## 4.5.6 Bruhatzerlegung\*

**Satz 4.5.6.1 (Bruhatzerlegung).** Gegeben ein Kring  $R$  und eine natürliche Zahl  $n \geq 1$  zerfällt die Gruppe  $\mathrm{GL}(n; R)$  unter der beidseitigen Operation der Untergruppe der invertierbaren oberen Dreiecksmatrizen  $B \subset \mathrm{GL}(n; R)$  in die disjunkte Vereinigung

$$\mathrm{GL}(n; R) = \bigsqcup_{w \in \mathcal{S}_n} B w B$$

der Doppelnebenklassen der Permutationsmatrizen.

*Beweis.* Multiplikation mit oberen Dreiecksmatrizen von rechts bedeutet solche Spaltenoperationen, bei denen eine Spalte mit einem invertierbaren Skalar multipliziert oder ein Vielfaches einer Spalte zu einer Spalte weiter rechts addiert wird. Ähnlich bedeutet die Multiplikation mit oberen Dreiecksmatrizen von links solche Zeilenoperationen, bei denen eine Zeile mit einem invertierbaren Skalar multipliziert oder ein Vielfaches einer Zeile zu einer Zeile weiter oben addiert wird. Also besteht für jede Permutationsmatrix  $w$  die Nebenklasse  $Bw$  aus gewissen

„Zahnlückenmatrizen“ und die Nebenklasse  $wB$  aus gewissen „Regaleinräummatrizen“, wie nebenstehendes Bild andeuten mag. Man erkennt so einerseits, daß aus  $Bw \cap vB \neq \emptyset$  folgt  $v(i) \leq w(i)$  für  $1 \leq i \leq n$ , wobei wir unsere Permutationsmatrizen nun als echte Permutationen aufgefaßt haben. Das zeigt  $v = w$  und wir erkennen, daß die Doppelnebenklassen  $BwB$  für  $w \in S_n$  paarweise disjunkt sind. Andererseits können wir eine beliebige invertierbare Matrix  $g$  durch Davormultiplizieren von  $b \in B$  stets in eine Regaleinräummatrix transformieren: Wir beginnen dazu mit der ersten Spalte, nehmen darin den tiefsten von Null verschiedenen Eintrag, und benutzen Zeilenoperationen „nach oben“, um alle Einträge darüber auch auszuräumen. Dann streichen wir die Zeile dieses Eintrags und machen immer so weiter. Das zeigt, daß die Doppelnebenklassen  $BwB$  auch die ganze Gruppe überdecken.  $\square$

4.5.6.2. Für die meisten Matrizen  $g$  wird der tiefste von Null verschiedene Eintrag jedesmal in der untersten noch nicht gestrichenen Zeile auftauchen. Dann liegt die Matrix in der Doppelnebenklasse  $Bw_oB$  der Permutationsmatrix mit Einsen in der Nebendiagonalen und Nullen sonst. Die zugehörige Permutation  $w_o \in S_n$  ist die Permutation, die „die Reihenfolge umdreht“. Diese Doppelnebenklasse heißt die **dicke Zelle**.

*Ergänzung 4.5.6.3.* Sei weiter  $w_o$  die Permutationsmatrix mit Einsen in der Nebendiagonalen und Nullen sonst, der also die Permutation  $w_o \in S_n$  entspricht, die „die Reihenfolge umdreht“. Dann besteht  $L := w_o B w_o$  genau aus allen invertierbaren unteren Dreiecksmatrizen. Die mit  $w_o$  verschobene dicke Zelle kann also auch beschrieben werden als

$$w_o B w_o B = LB$$

Bezeichnet  $U := U(n; R)$  die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale, so besteht  $L \cap U$  nur aus der Einheitsmatrix und wir haben  $LU = LB$ . Mithin liefert die Multiplikation eine Bijektion

$$L \times U \xrightarrow{\sim} LB$$

auf die mit  $w_o$  verschobene dicke Zelle. In der Numerik nennt man diese Darstellung einer Matrix aus der verschobenen dicken Zelle  $LB$  als Produkt einer unteren mit einer oberen Dreiecksmatrix die **LR-Zerlegung** für „Links-Rechts“ oder **LU-Zerlegung** für „lower-upper“. Allgemeiner zeigt man, daß für eine beliebige Permutation  $w \in S_n$  die Abbildung  $(a, u) \mapsto awu$  eine Bijektion

$$L \times (U \cap w^{-1}Uw) \xrightarrow{\sim} LwB$$

liefert. Die Surjektivität folgt hierbei in den Notationen von 4.4.1.12 aus der Erkenntnis, daß das Aufmultiplizieren in einer beliebigen aber festen Reihenfolge eine Bijektion  $\prod_{i < j, w(i) > w(j)} U_{ij} \times (U \cap w^{-1}Uw) \xrightarrow{\sim} U$  liefert und daß gilt  $wU_{ij} = U_{w(i)w(j)}w \in Lw$  für alle Faktoren des großen Produkts.

$$\begin{array}{c}
 \left( \begin{array}{ccc} 1 & & \\ & 1 & \\ & & 1 \end{array} \right) \rightsquigarrow \left( \begin{array}{cccc} * & * & * & \\ & * & & \\ & & * & * \\ * & * & * & * \end{array} \right) \\
 =_{\mathcal{U}} =_{\mathcal{UB}} \\
 \left( \begin{array}{cccc} * & * & * & * \\ * & & * & * \\ * & & * & \\ * & & & \end{array} \right) =_{\mathcal{Bv}}
 \end{array}$$

Die Nebenklassen einer Permutationsmatrix unter der Operation der oberen Dreiecksmatrizen. Das Symbol \* steht für einen beliebigen Matrixeintrag, das Symbol  $\cdot$  für einen invertierbaren Matrixeintrag.

## Übungen

*Übung 4.5.6.4.* Seien  $R$  ein Ring. Wir betrachten in  $\mathrm{GL}(n; R)$  die Untergruppen  $B, U$  und  $U^- := w_\circ U w_\circ$  der obereren Dreiecksmatrizen, oberen Dreiecksmatrizen mit Einsen auf der Diagonale und unteren Dreiecksmatrizen mit Einsen auf der Diagonale. Man zeige, daß für jedes  $w \in \mathcal{S}_n$  die Abbildung  $(b, u) \mapsto bwu$  eine Bijektion

$$B \times (U \cap w^{-1}U^-w) \xrightarrow{\sim} BwB$$

induziert. Man zeige: Für je zwei Permutationen  $v, w \in \mathcal{S}_n$  mit  $l(vw) = l(v) + l(w)$  für  $l(\sigma)$  wie in 3.6.1.3 die Zahl der Fehlstände einer Permutation  $\sigma$  liefert die Multiplikation eine Bijektion

$$BvB \times_{/B} BwB \xrightarrow{\sim} BvwB$$

des balancierten Produkts nach 4.5.2.6 unserer Doppelnebenklassen mit einer weiteren Doppelnebenklasse. Ist dahingegen  $s \in \mathcal{S}_n$  eine Permutation mit nur einem Fehlstand und  $w \in \mathcal{S}_n$  beliebig und gilt  $l(sw) \leq l(w)$ , so haben wir  $l(sw) = l(w) - 1$  und

$$BsBwB = BswB \sqcup BwB$$

*Übung 4.5.6.5.* Genau dann besitzt eine invertierbare quadratische Matrix mit Koeffizienten in einem Kring eine LU-Zerlegung, wenn alle Untermatrizen, die durch Streichen von hinteren Spalten und gleichviel unteren Zeilen entstehen, alle auch invertierbar sind.

## 4.6 Multilineare Algebra

### 4.6.1 Tensorprodukte

**Satz 4.6.1.1.** Seien  $r \geq 0$  eine natürliche Zahl und  $V_1, \dots, V_r$  Vektorräume über einem Körper  $K$ . So gilt:

1. Es gibt ein Paar  $(T, \tau)$  bestehend aus einem  $K$ -Vektorraum  $T$  und einer multilinear Abbildung  $\tau : V_1 \times \dots \times V_r \rightarrow T$  derart, daß für jeden weiteren  $K$ -Vektorraum  $W$  das Vorschalten von  $\tau$  eine Bijektion

$$(\circ \tau) : \text{Hom}_K(T, W) \xrightarrow{\sim} \text{Hom}_K^{(r)}(V_1 \times \dots \times V_r, W)$$

zwischen der Menge aller linearen Abbildungen  $T \rightarrow W$  und der Menge aller multilinear Abbildungen  $V_1 \times \dots \times V_r \rightarrow W$  induziert. Wir nennen solch ein  $\tau : V_1 \times \dots \times V_r \rightarrow T$  eine **universelle multilineare Abbildung**;

2. Gegeben ein weiteres derartiges Paar  $(S, \sigma)$  existiert genau eine lineare Abbildung  $c : T \rightarrow S$  mit  $c \circ \tau = \sigma$  und genau eine lineare Abbildung  $d : S \rightarrow T$  mit  $d \circ \sigma = \tau$  und diese Abbildungen sind zueinander inverse Isomorphismen zwischen  $T$  und  $S$ .

*Beweis der Eindeutigkeit 4.6.1.2.* Die Existenz und Eindeutigkeit von  $c$  folgt sofort aus der universellen Eigenschaft von  $(T, \tau)$ . Die Existenz und Eindeutigkeit von  $d$  folgt ebenso aus der universellen Eigenschaft von  $(S, \sigma)$ . Schließlich gilt  $(d \circ c) \circ \tau = \tau = \text{id}_T \circ \tau$  und damit folgt  $d \circ c = \text{id}_T$  wieder nach der universellen Eigenschaft von  $\tau$ . Die Identität  $c \circ d = \text{id}_S$  zeigt man genauso.  $\square$

4.6.1.2. Unsere Paare sind nach Teil 2 „eindeutig bestimmt bis auf eindeutigen Isomorphismus“, wenn sie denn existieren. Insbesondere kommt es auf die genaue Konstruktion ebensowenig an wie auf die genaue Konstruktion der natürlichen oder der reellen Zahlen. Solch ein Paar verdient damit eine eigene Notation und den bestimmten Artikel. Man nennt  $T$  das **Tensorprodukt der  $V_i$**  und notiert es im Fall  $r > 0$  als

$$T := V_1 \otimes \dots \otimes V_r$$

und notiert die universelle multilineare Abbildung  $(v_1, \dots, v_r) \mapsto v_1 \otimes \dots \otimes v_r$ . Im Fall  $r = 1$  nimmt man üblicherweise  $T = V_1$  und wählt als universelle multilinear alias 1-lineare alias lineare Abbildung die Identität, so daß es nicht drauf ankommt, ob  $V_1$  das Tensorprodukt mit nur einem Faktor oder eben den Vektorraum  $V_1$  bezeichnet. Im Fall  $r = 0$  nimmt man üblicherweise als  $T = K$  den Grundkörper und wählt als universelle multilineare alias 0-lineare alias beliebige Abbildung  $\rightarrow K$  vom leeren Produkt alias der einelementigen Menge nach  $K$  die Abbildung  $* \mapsto 1$ .

**4.6.1.3 (Arbeiten in Strukturen bis auf eindeutigen Isomorphismus).** Ich will nicht verschweigen, daß es durchaus seine Tücken hat, mit bis auf eindeutigen Isomorphismus wohlbestimmten Objekten zu arbeiten. Es bedeutet, die definierenden Eigenschaften nie aus den Augen zu verlieren, und das erfordert eine gewisse Übung. In manchen Situationen haben wir diese Übung bereits. Wenn wir etwa

$$2 \cdot 2 = 4$$

behaupten, könnten wir uns daran erinnern, daß die natürlichen Zahlen nach 3.4.1.5 ja eigentlich nur ein bis auf eindeutigen Isomorphismus wohlbestimmtes Paar  $(N, s)$  aus einer Menge  $N$  und einer Abbildung  $s : N \rightarrow N$  mit gewissen Eigenschaften sind; daß zu diesen Eigenschaften die Forderung gehört, daß nur ein Element von  $N$  nicht im Bild von  $s$  liegt; daß wir für dieses Element die Notation 0 vereinbart hatten; daß wir die Notationen  $1 := s(0)$ ,  $2 := s(1)$ ,  $3 := s(2)$  und  $4 := s(3)$  vereinbart hatten; und so weiter. Wir bewegen uns hier also in einem System von Konstruktionen und Konventionen, das allein aus den Daten und Eigenschaften aufgebaut ist, die unsere Struktur der natürlichen Zahlen bis auf eindeutigen Isomorphismus charakterisieren. Bei der Arbeit mit anderen bis auf eindeutigen Isomorphismus wohlbestimmten Objekten wie etwa unseren Tensorprodukten verhält es sich genauso. Es fehlt Ihnen nur möglicherweise noch die Übung und mir kann es leicht passieren, daß ich manche Konstruktionen und Konventionen nicht explizit genug einführe und bespreche.

*Erster Beweis der Existenz 4.6.1.1.* Um die Existenz in Teil 1 zu zeigen wählen wir Basen  $B_i \subset V_i$  und bemerken, daß die offensichtlichen Abbildungen Bijektionen

$$\text{Hom}_K^{(r)}(V_1 \times \dots \times V_r, W) \xrightarrow{\sim} \text{Ens}(B_1 \times \dots \times B_r, W) \xrightarrow{\sim} \text{Hom}_K(K\langle B_1 \times \dots \times B_r \rangle, W)$$

liefern. Wir können also als Tensorprodukt den freien Vektorraum über dem Produkt der Basen  $T := K\langle B_1 \times \dots \times B_r \rangle$  nehmen mit derjenigen multilineararen Abbildung  $\tau$ , die dadurch charakterisiert wird, daß sie Tupel von Basisvektoren  $(b_1, \dots, b_r)$  auf das Element  $\text{can}(b_1, \dots, b_r)$  des freien Vektorraums wirft.  $\square$

**4.6.1.4 (Basen allgemeiner Tensorprodukte).** Gegeben Vektorräume  $V_1, \dots, V_r$  über einem Körper  $K$  und Basen  $B_i \subset V_i$  bilden die Tensoren  $b_1 \otimes \dots \otimes b_r$  mit  $b_i \in B_i$  eine Basis des Tensorprodukts  $V_1 \otimes \dots \otimes V_r$ . Das folgt sofort aus dem vorhergehenden Beweis. Speziell folgt  $\dim(V \otimes W) = \dim(V) \dim(W)$ .

*Zweiter Beweis der Existenz 4.6.1.1.* Ich gebe noch einen alternativen Beweis für die Existenz universeller multilinearer Abbildungen, der ohne den Basisexistenzsatz und damit ohne Auswahlaxiom und Zorn'sches Lemma auskommt und mir natürlicher und im Grunde auch einfacher scheint. Er benötigt jedoch die

Konstruktion des Quotientenvektorraums, die wir erst in 4.4.5.4 kennenlernen. Der Einfachheit halber schreibe ich die Details nur für bilineare Abbildungen aus. Wir beginnen mit dem freien  $K$ -Vektorraum  $K\langle V \times W \rangle$  über der Menge  $V \times W$ . Darin betrachten wir den Untervektorraum  $U \subset K\langle V \times W \rangle$ , der erzeugt wird von allen Ausdrücken

$$\begin{aligned} & (v + v', w) - (v, w) - (v', w) \\ & (\lambda v, w) - \lambda(v, w) \\ & (v, w + w') - (v, w) - (v, w') \\ & (v, \lambda w) - \lambda(v, w) \end{aligned}$$

für  $v, v' \in V$ ,  $w, w' \in W$  und  $\lambda \in K$ . Schließlich definieren wir  $T$  als den Quotientenvektorraum

$$T := K\langle V \times W \rangle / U$$

und erklären  $\tau : V \times W \rightarrow T$  als die Abbildung, die jedem Paar  $(v, w)$  die Nebenklasse  $\tau(v, w) := \text{can}(v, w) + U$  von  $\text{can}(v, w)$  zuordnet. Die Bilinearität von  $\tau$  folgt dann unmittelbar aus der Definition des herausgeteilten Untervektorraums  $U$ . Um die im Satz behauptete universelle Eigenschaft nachzuweisen, arbeiten wir mit dem Diagramm

$$\begin{array}{ccccc} V \times W & \longrightarrow & K\langle V \times W \rangle & \longrightarrow & T \\ & \searrow & \downarrow & \nearrow & \\ & & R & & \end{array}$$

Für jede Abbildung  $b : V \times W \rightarrow R$  gibt es nach der universellen Eigenschaft des freien Vektorraums über einer vorgegebenen Menge genau eine  $K$ -lineare Abbildung  $\tilde{b} : K\langle V \times W \rangle \rightarrow R$  mit  $\tilde{b} \circ \text{can} = b$ . Ist hier  $b$  bilinear, so gilt offensichtlich  $\tilde{b}(U) = 0$ , also gibt es nach der universellen Eigenschaft des Quotientenvektorraums genau eine lineare Abbildung  $\hat{b} : T \rightarrow R$  mit  $\hat{b}\tau(v, w) = b(v, w)$ . Diese Abbildung  $\hat{b}$  ist eindeutig bestimmt durch  $b$ , da die  $\tau(v, w)$  das Tensorprodukt als Vektorraum erzeugen.  $\square$

**4.6.1.5 (Elemente von Tensorprodukten).** Bereits unsere universellen bilinearen Abbildungen  $V \times W \rightarrow V \otimes W$ ,  $(v, w) \mapsto v \otimes w$  sind im allgemeinen weder injektiv noch surjektiv. Genauer sind sie nur injektiv im Fall  $V = W = 0$ , denn es gilt ja stets  $\lambda v \otimes w = v \otimes \lambda w$ . Weiter sind sie nur surjektiv, wenn einer der beiden Räume eine Dimension  $\leq 1$  hat. Im Fall  $V = \mathbb{R}^2$  und  $W = \mathbb{R}^2$  etwa können wir unsere universelle bilineare Abbildung als eine stetig differenzierbare Abbildung  $\mathbb{R}^4 \rightarrow \mathbb{R}^4$  auffassen, die auf den Teilmengen  $\{(\lambda v, \lambda^{-1}w) \mid \lambda \in \mathbb{R}^\times\}$  konstant ist, und für eine derartige Abbildung ist hoffentlich zumindest anschaulich klar, daß sie nicht surjektiv sein kann. Formal behandeln Sie das in Übung 4.6.1.31.

4.6.1.6 (**Tensorpotenzen**). Gegeben ein Vektorraum  $V$  über einem Körper  $K$  und eine natürliche Zahl  $r \in \mathbb{N}$  vereinbaren wir

$$V^{\otimes r} := \underbrace{V \otimes \dots \otimes V}_{r \text{ Faktoren}}$$

und verstehen insbesondere  $V^{\otimes 0} := K$  im Sinne von 4.6.1.2. Gegeben  $v \in V$  schreiben wir kurz  $v^{\otimes r} := v \otimes \dots \otimes v$  für das Bild von  $(v, \dots, v)$  unter der universellen multilinear Abbildung  $V^{\times r} \rightarrow V^{\otimes r}$  und verstehen im Sinne von 4.6.1.2 insbesondere  $v^{\otimes 0} := 1 \in K$ .

*Beispiel 4.6.1.7 (Tensorprodukte und physikalische Einheiten).* Wir betrachten den schmutzigen Raum unserer Anschauung als einen dreidimensionalen euklidischen affinen Raum  $\mathbb{E}$ . Dessen schmutzige Längengerade  $\mathbb{L}$  besitzt die beiden Basen Meter m und Kilometer km und es gilt  $km = 1000 \text{ m}$ . In  $\mathbb{L}^{\otimes 2}$  erhalten wir mithin  $(\text{km})^{\otimes 2} = 10^6 \text{ m}^{\otimes 2}$ . In unserem Formalismus ist also in der Tat und wie es sich gehört ein Quadratkilometer eine Million Quadratmeter. Es ist üblich, in diesem Kontext die Klammern und Tensorzeichen wegzulassen, so daß unsere Identität die möglicherweise besser vertraute Gestalt

$$\text{km}^2 = 10^6 \text{ m}^2$$

annimmt. Allgemeiner gilt für zwei beliebige Vektoren  $v, w$  eines eindimensionalen Vektorraums  $L$  mit  $v = \lambda w$  im Tensorquadrat  $L^{\otimes 2}$  aufgrund der Bilinearität der universellen bilinearen Abbildungen die Identität  $v^{\otimes 2} = \lambda^2(w^{\otimes 2})$ .

4.6.1.8 (**Lineare Abbildungen aus Tensorprodukten**). Seien  $V, W$  Vektorräume. Die Elemente der Gestalt  $v \otimes w$  erzeugen das Tensorprodukt als Vektorraum und sogar als abelsche Gruppe. Geben wir eine Abbildung von einem Tensorprodukt in einen Vektorraum  $R$  an durch eine Vorschrift der Gestalt  $v \otimes w \mapsto b(v, w)$ , so ist der Leser implizit gefordert, die Bilinearität der Abbildung  $b : V \times W \rightarrow R$  zu prüfen, und gemeint ist dann eigentlich die durch die universelle Eigenschaft definierte lineare Abbildung  $\hat{b} : V \otimes W \rightarrow R$ . Analoge Vereinbarungen treffen wir für Abbildungen aus Tensorprodukten mit einer beliebigen Zahl von Faktoren.

**Definition 4.6.1.9.** Sind  $f : V \rightarrow V'$  und  $g : W \rightarrow W'$  lineare Abbildungen, so definieren wir eine lineare Abbildung  $f \otimes g : V \otimes W \rightarrow V' \otimes W'$  durch die Vorschrift

$$(f \otimes g)(v \otimes w) := f(v) \otimes g(w)$$

in unserer Konvention 4.6.1.8. Wir nennen  $f \otimes g$  das **Tensorprodukt der Abbildungen  $f$  und  $g$** . Analog erklären wir das Tensorprodukt einer beliebigen endlichen Familie von linearen Abbildungen. Gegeben eine lineare Abbildung  $f : V \rightarrow W$  verwenden wir weiter die Abkürzung  $f^{\otimes r} := (f \otimes \dots \otimes f) : V^{\otimes r} \rightarrow W^{\otimes r}$ .

**Proposition 4.6.1.10 (Assoziativität von Tensorprodukten).** *Sind  $V_1, \dots, V_n$  Vektorräume und  $0 \leq i \leq j \leq \dots \leq k \leq n$  Indizes, so liefert die Abbildungsvorschrift  $v_1 \otimes \dots \otimes v_n \mapsto (v_1 \otimes \dots \otimes v_i) \otimes (v_{i+1} \otimes \dots \otimes v_j) \otimes \dots \otimes (v_{k+1} \otimes \dots \otimes v_n)$  einen Isomorphismus*

$$V_1 \otimes \dots \otimes V_n \xrightarrow{\sim} (V_1 \otimes \dots \otimes V_i) \otimes (V_{i+1} \otimes \dots \otimes V_j) \otimes \dots \otimes (V_{k+1} \otimes \dots \otimes V_n)$$

4.6.1.11. Die Abbildungsvorschrift ist hier im Sinne unserer Vereinbarung 4.6.1.8 zu lesen. Leere Tensoren sind zu verstehen als das ausgezeichnete Element des leeren Tensorprodukts alias die Eins des Grundkörpers. Ich habe statt  $0 = i_0 \leq i_1 \leq i_2 \leq \dots \leq i_r = n$  etwas weniger korrekt  $0 \leq i \leq j \leq \dots \leq k \leq n$  geschrieben um Subindizes zu vermeiden.

*Beweis.* Wir prüfen leicht, daß unsere Abbildung eine Bijektion zwischen einer Basis des Ausgangsraums und einer Basis des Zielraums induziert.  $\square$

**Proposition 4.6.1.12 (Kommutativität von Tensorprodukten).** *Sind  $V_1, \dots, V_n$  Vektorräume und ist  $\sigma \in S_n$  eine Permutation, so liefert die Abbildungsvorschrift  $v_1 \otimes \dots \otimes v_n \mapsto v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(n)}$  einen Isomorphismus*

$$V_1 \otimes \dots \otimes V_n \xrightarrow{\sim} V_{\sigma(1)} \otimes \dots \otimes V_{\sigma(n)}$$

*Beweis.* Wir prüfen leicht, daß unsere Abbildung eine Bijektion zwischen einer Basis des Ausgangsraums und einer Basis des Zielraums induziert.  $\square$

4.6.1.13 (**Identifikationen zwischen längeren Tensorausdrücken**). Wir sehen mit 4.6.1.10, daß es bei Tensorprodukten mit mehreren Faktoren „nicht auf eventuelle Klammerung ankommt und Faktoren  $K$  weggelassen werden dürfen“. Präziser formuliert erhalten wir so natürliche Isomorphismen zwischen verschiedenen Tensorprodukten mit mehreren Faktoren. Unter Verwendung der Vertauschungsisomorphismen 4.6.1.12 erkennen wir weiter, daß es hier auch auf die Reihenfolge der Tensorfaktoren nicht ankommt. Das alles ist in dieser Situation noch derart explizit, daß mir eine stärkere Formalisierung unangemessen scheint. Der entsprechende Formalismus ist der einer „Schmelzkategorie“, der in Ansätzen in 4.6.2 und im Vollausbau in ?? folgende besprochen wird.

4.6.1.14 (**Negative Tensorpotenzen im eindimensionalen Fall**). Im Fall eines eindimensionalen Vektorraums  $L$  über einem Körper  $K$  erklären wir die  $r$ -te Tensorpotenz von  $L$  sogar für alle  $r \in \mathbb{Z}$ , indem wir unsere Definition 4.6.1.6 für nichtnegative Tensorpotenzen ergänzen durch die Vorschrift, daß negative Tensorpotenzen zu verstehen sein mögen als die entsprechenden positiven Potenzen des Dualraums, in Formeln

$$L^{\otimes r} := (L^\top)^{\otimes(-r)} \quad \text{für } r < 0.$$

Erklären wir dann weiter für jedes  $l \in L \setminus 0$  und  $r < 0$  den Vektor  $l^{\otimes r} \in L^{\otimes r}$  als  $l^{\otimes r} := (l^\top)^{\otimes r}$  mit  $l^\top \in L^\top$  definiert durch  $l^\top(l) = 1$ , so haben wir  $(\lambda l)^{\otimes r} = \lambda^r(l^{\otimes r})$  für alle  $\lambda \in K^\times$  und  $r \in \mathbb{Z}$  und es gibt für beliebige  $r, s \in \mathbb{Z}$  eindeutig bestimmte Isomorphismen

$$L^{\otimes r} \otimes L^{\otimes s} \xrightarrow{\sim} L^{\otimes(r+s)}$$

mit der Eigenschaft  $l^{\otimes r} \otimes l^{\otimes s} \mapsto l^{\otimes(r+s)}$  für alle  $l \in L \setminus 0$ . Schließlich gibt es in diesem Fall zu jedem Isomorphismus  $f : L \xrightarrow{\sim} M$  für alle  $r \in \mathbb{Z}$  einen ausgezeichneten Isomorphismus  $f^{\otimes r} : L^{\otimes r} \xrightarrow{\sim} M^{\otimes r}$  mit  $l^{\otimes r} \mapsto f(l)^{\otimes r}$  für alle  $l \in L \setminus 0$ . Es ist auch in diesem Zusammenhang üblich, die Abkürzung  $l^r := l^{\otimes r}$  sowie  $L^r := L^{\otimes r}$  zu verwenden. Insbesondere ist damit  $l^{-1}$  die duale Basis zu  $l$ .

**4.6.1.15 (Orientierung von Tensorpotenzen).** Gegeben ein orientierter eindimensionaler Vektorraum  $L$  über einem angeordneten Körper erhält man aus jeder Orientierung von  $L$  eine Orientierung aller Tensorpotenzen  $L^{\otimes r}$  durch die Vorschrift, daß für  $l \in L_{>0}$  ein positiver Vektor auch seine Potenzen  $l^r$  positiv sein sollen. Die damit auf den geraden Potenzen  $L^{\otimes 2r}$  gegebene Orientierung hängt dann noch nicht einmal von der auf  $L$  gewählten Orientierung ab. Im Fall des Dualraums  $L^{-1}$  eines eindimensionalen Raums stimmt diese Orientierung mit der in 3.6.5.14 erklärten Orientierung eines Dualraums überein.

**Beispiel 4.6.1.16 (Beispiele für Tensorpotenzen).** In der schmutzigen Anschauung mag man sich die positiven Elemente einiger Tensorpotenzen der Längengerade  $\mathbb{L}$  wie folgt vorstellen: Elemente von  $\mathbb{L}^{\otimes 2}$  als Flächenmaße, Elemente von  $\mathbb{L}^{\otimes 3}$  als Volumenmaße, Elemente von  $\mathbb{L}^{\otimes(-1)}$  als „lineare Dichten“ wie etwa die Belegung eines Wanderwegs mit Personen pro Länge, Elemente von  $\mathbb{L}^{\otimes(-2)}$  als „Flächendichten“ wie etwa die Bevölkerungsdichte in Personen pro Fläche, und Elemente von  $\mathbb{L}^{\otimes(-3)}$  als „Volumendichten“ wie etwa die Dichte eines Gases in Zahl der Moleküle pro Volumen.

**Beispiel 4.6.1.17.** Wir erinnern den Richtungsraum  $\vec{\mathbb{T}}$  der Zeitachse und seine Basis  $s$  mit dem Namen **Sekunde** ebenso wie seine Basis  $min$  mit dem Namen **Minute** und seine Basis  $std$  mit dem Namen **Stunde**. Zwischen diesen Basen besteht die Relation  $min = 60s$  und  $60min = std$ . Den Raum

$$\vec{\mathbb{T}}^\top \otimes \mathbb{L} = \mathbb{L} \otimes \vec{\mathbb{T}}^{-1}$$

oder vielmehr seine nichtnegativen Elemente in Bezug auf die offensichtliche Orientierung nennen wir **absolute Geschwindigkeiten**. Mit der Abkürzung  $m/s := m \otimes s^{-1}$  und ihren Analoga gelten in diesem Raum etwa die Identitäten

$$m/s = 3600m/3600s = 3,6 \text{ km/std}$$

**4.6.1.18 (Matrix des Tensorprodukts linearer Abbildungen).** Gegeben Vektorräume  $V, W$  mit angeordneten Basen  $\mathcal{A} = (v_1, \dots, v_n)$  und  $\mathcal{B} = (w_1, \dots, w_m)$  bilden wir in  $V \otimes W$  die angeordnete Basis

$$\begin{aligned}\mathcal{A} \otimes \mathcal{B} := & (v_1 \otimes w_1, v_1 \otimes w_2, \dots, v_1 \otimes w_m, \\ & v_2 \otimes w_1, v_2 \otimes w_2, \dots, v_2 \otimes w_m, \\ & \dots \quad \dots \quad \dots \\ & v_n \otimes w_1, v_n \otimes w_2, \dots, v_n \otimes w_m)\end{aligned}$$

Gegeben zusätzlich weitere Vektorräume  $V', W'$  mit angeordneten Basen  $\mathcal{A}' = (v'_1, \dots, v'_{n'})$  und  $\mathcal{B}' = (w'_1, \dots, w'_{m'})$  und lineare Abbildungen  $f : V \rightarrow V'$  und  $g : W \rightarrow W'$  können wir die Matrix  ${}_{\mathcal{A}' \otimes \mathcal{B}'}[f \otimes g]_{\mathcal{A} \otimes \mathcal{B}}$  von  $f \otimes g$  in den Basen  $\mathcal{A} \otimes \mathcal{B}$  und  $\mathcal{A}' \otimes \mathcal{B}'$  wie folgt durch die Matrizen  $A = {}_{\mathcal{A}'}[f]_{\mathcal{A}}$  und  $B = {}_{\mathcal{B}'}[g]_{\mathcal{B}}$  ausdrücken: Haben wir etwa  $A = (a_{ij})$ , so wird

$${}_{\mathcal{A}' \otimes \mathcal{B}'}[f \otimes g]_{\mathcal{A} \otimes \mathcal{B}} = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{n'1}B & \dots & a_{n'n}B \end{pmatrix}$$

Auf der rechten Seite ist die Matrix geblockt geschrieben, es handelt sich ja eigentlich um eine  $(n'm' \times nm)$ -Matrix. Sie heißt auch das **Kronecker-Produkt** der Matrizen  $A$  und  $B$  und wird  $A \otimes B$  notiert, so daß wir unsere Identität oben also auch schreiben können in der Form

$${}_{\mathcal{A}' \otimes \mathcal{B}'}[f \otimes g]_{\mathcal{A} \otimes \mathcal{B}} = {}_{\mathcal{A}'}[f]_{\mathcal{A}} \otimes {}_{\mathcal{B}'}[g]_{\mathcal{B}}$$

Um diese Identität zu prüfen beginnen wir mit den Identitäten

$$f(v_i) = \sum_j a_{ji}v'_j \quad \text{und} \quad g(w_k) = \sum_l b_{lk}w'_l$$

und folgern

$$(f \otimes g)(w_i \otimes w_k) = \sum_{j,l} a_{ji}b_{lk}v'_j \otimes w'_l$$

Die Einträge der Matrix von  $f \otimes g$  sind also alle Produkte von einem Eintrag der Matrix von  $f$  mit einem Eintrag der Matrix von  $g$ . Daß diese Einträge dann auch noch an den oben beschriebenen Stellen der Matrix von  $f \otimes g$  stehen, mag sich der Leser am einfachsten selbst überlegen.

**Proposition 4.6.1.19 (Adjunktion von Tensor und Hom).** Gegeben Vektorräume  $U, V, W$  erhalten wir durch die Vorschrift  $f \mapsto \tilde{f}$  mit  $\tilde{f}(u \otimes v) = (f(u))(v)$  einen Isomorphismus

$$\text{Hom}(U, \text{Hom}(V, W)) \xrightarrow{\sim} \text{Hom}(U \otimes V, W)$$

*Vorschau 4.6.1.20.* Diese Aussage bedeutet in einer Terminologie, die Sie in dieser Vorlesung nicht mehr lernen werden, daß „die Funktoren  $\otimes V$  und  $\text{Hom}(V, \cdot)$  zueinander adjungiert sind“. Ich verwende in diesem Kontext gerne die alternative Notation  $(V \Rightarrow W) := \text{Hom}(V, W)$ .

*Beweis.* Beide Seiten sind in offensichtlicher und mit der angegebenen Abbildung verträglicher Weise in Bijektion zur Menge  $\text{Hom}^{(2)}(U \times V, W)$  aller bilinearen Abbildungen  $U \times V \rightarrow W$ .  $\square$

**Satz 4.6.1.21 (Homomorphismenräume als Tensorprodukt).** *Gegeben ein Körper  $K$  liefert für beliebig vorgegebene  $K$ -Vektorräume  $V, W$  die Abbildungsvorschrift  $f \otimes w \mapsto (v \mapsto f(v)w)$  eine Bijektion*

$$\text{can} : V^\top \otimes W \xrightarrow{\sim} \{f \in \text{Hom}(V, W) \mid \text{rg}(f) < \infty\}$$

*zwischen dem Tensorprodukt des Dualraums von  $V$  mit  $W$  und dem Raum aller Homomorphismen endlichen Ranges.*

*Beispiel 4.6.1.22.* Unsere vektoriellen Geschwindigkeiten aus 3.3.1.12 können wir mithin auch verstehen als Elemente des Tensorprodukts  $\vec{\mathbb{T}}^{-1} \otimes \vec{\mathbb{E}} = \text{Hom}(\vec{\mathbb{T}}, \vec{\mathbb{E}})$  des Richtungsraums  $\vec{\mathbb{E}}$  unseres Anschauungsraums  $\mathbb{E}$  mit dem Dualraum des Raums der Zeitspannen.

4.6.1.23. Das Bild der Verknüpfung  $V^\top \times W \rightarrow V^\top \otimes W \hookrightarrow \text{Hom}(V, W)$  besteht genau aus allen Homomorphismen vom Rang Eins oder Null.

4.6.1.24. Ist  $v_1, \dots, v_n \in V$  eine Basis von  $V$  und  $v_1^\top, \dots, v_n^\top \in V^\top$  die duale Basis von  $V^\top$ , so können wir im Satz die inverse Abbildung explizit angeben durch die Vorschrift  $f \mapsto v_1^\top \otimes f(v_1) + \dots + v_n^\top \otimes f(v_n)$ . Ist zusätzlich  $w_1, \dots, w_m$  eine Basis von  $W$ , so wird  $v_i^\top \otimes w_j$  abgebildet auf diejenige lineare Abbildung, deren Matrix in Bezug auf die gegebenen Basen die Basismatrix  $E_{ji}$  aus 3.2.5.3 ist, in Formeln

$${}_{\mathcal{B}}[\text{can}(v_i^\top \otimes w_j)]_{\mathcal{A}} = E_{ji}$$

für  $\mathcal{A} = (v_1, \dots, v_n)$  und  $\mathcal{B} = (w_1, \dots, w_m)$  unsere angeordneten Basen von  $V$  und  $W$ . Im Fall endlichdimensionaler Räume kann der Satz also leicht mit Basen überprüft werden. Der Beweis gilt den unendlichdimensionalen Fällen.

*Beweis.* Wir beginnen mit der Injektivität. Jeder Tensor auf der linken Seite kann offensichtlich in der Form  $f_1 \otimes w_1 + \dots + f_r \otimes w_r$  dargestellt werden mit den  $w_i$  linear unabhängig. Geht er nach Null, so folgt  $f_1(v)w_1 + \dots + f_r(v)w_r = 0$  für alle  $v \in V$ . Daraus aber folgt  $f_1(v) = \dots = f_r(v) = 0$  für alle  $v \in V$  und damit  $f_1 = \dots = f_r = 0$  und unser Tensor war schon Null. Das zeigt die Injektivität. Unsere kanonischen Abbildung landet im Unterraum der Homomorphismen endlichen

Ranges, da ja das Bild von  $\text{can}(f_1 \otimes w_1 + \dots + f_r \otimes w_r)$  stets im Erzeugnis  $\langle w_1, \dots, w_r \rangle$  der  $w_i$  liegt. Es liegt aber sogar jeder Homomorphismus endlichen Ranges  $\varphi : V \rightarrow W$  im Bild von  $\text{can}$ , denn ist  $w_1, \dots, w_r$  eine Basis von  $\text{im } \varphi$  und setzen wir  $f_i := w_i^\top \circ \varphi$ , so gilt offensichtlich

$$\text{can}(f_1 \otimes w_1 + \dots + f_r \otimes w_r) = \varphi \quad \square$$

**Korollar 4.6.1.25 (Tensorprodukt und Dualität).** *Gegeben Vektorräume  $V, W$  liefert die Abbildung  $f \otimes g \mapsto (v \otimes w \mapsto f(v)g(w))$  eine Injektion*

$$V^\top \otimes W^\top \hookrightarrow (V \otimes W)^\top$$

vom Tensorprodukt der Dualräume in den Dualraum des Tensorprodukts. Sie ist ein Isomorphismus genau dann, wenn einer unserer beiden Räume endlichdimensional ist.

4.6.1.26. Im Fall endlichdimensionaler Räume kann das Korollar leicht mit Basen überprüft werden. Der Beweis gilt den unendlichdimensionalen Fällen. Im Fall eines eindimensionalen Raums  $L$  liefert uns die Korollar induktiv natürliche Isomorphismen  $L^{\otimes(-r)} \xrightarrow{\sim} (L^{\otimes r})^\top$ .

*Beweis.* Wir argumentieren mit dem Diagramm

$$\begin{array}{ccc} (V \otimes W)^\top & \xlongequal{\quad} & \text{Hom}(V \otimes W, K) \\ & \uparrow \wr & \\ & \text{Hom}(V, \text{Hom}(W, K)) & \\ & \parallel & \\ V^\top \otimes W^\top & \xhookrightarrow{\quad} & \text{Hom}(V, W^\top) \end{array}$$

Der vertikale Isomorphismus kommt aus 4.6.1.19, die horizontale Injektion aus 4.6.1.21. Daß deren Komposition genau die im Korollar beschriebene Abbildung ist, mag der Leser selbst prüfen.  $\square$

## Übungen

*Übung 4.6.1.27 (Orientierter Flächeninhalt).* Sei  $V$  ein orientierter zweidimensionaler euklidischer Vektorraum mit Längengerade  $\mathbb{L}$ . Man zeige, daß es genau eine alternierende bilineare Abbildung

$$\omega : V \times V \rightarrow \mathbb{L}^{\otimes 2}$$

gibt mit  $\omega(v, w) = \|v\| \otimes \|w\|$  wann immer  $v \perp w$  orthogonale Vektoren sind und  $(v, w)$  eine orientierte Basis von  $V$ .

*Übung 4.6.1.28.* Gegeben Vektorräume  $U, V, W$  kommutiert das Diagramm

$$\begin{array}{ccc} U^\top \otimes V \otimes V^\top \otimes W & \xrightarrow{\quad} & \text{Hom}(U, V) \otimes \text{Hom}(V, W) \\ \downarrow & & \downarrow \\ U^\top \otimes W & \xrightarrow{\quad} & \text{Hom}(U, W) \end{array}$$

mit den von den kanonischen Injektionen 4.6.1.21 induzierten Horizontalen, dem Verknüpfen von linearen Abbildungen als rechter Vertikale, und in der linken Vertikalen der Verknüpfung

$$U^\top \otimes V \otimes V^\top \otimes W \rightarrow U^\top \otimes K \otimes W \xrightarrow{\sim} U^\top \otimes W$$

der vom Auswerten  $\text{id} \otimes \text{ev} \otimes \text{id}$  induzierten Abbildung gefolgt vom Isomorphismus  $U^\top \otimes K \otimes W \xrightarrow{\sim} U^\top \otimes W$ ,  $f \otimes \lambda \otimes w \mapsto \lambda(f \otimes w)$ . Die eben erklärte Abbildung in der linken Vertikalen bezeichnet man in dieser und ähnlichen Situationen auch als die **Verjüngung von Tensoren**.

*Übung 4.6.1.29.* Gegeben Vektorräume  $W, V, V'$  liefert  $w \otimes (v, v') \mapsto (w \otimes v, w \otimes v')$  einen Isomorphismus  $W \otimes (V \oplus V') \xrightarrow{\sim} (W \otimes V) \oplus (W \otimes V')$ . Analoges gilt auch für den ersten Tensorfaktor.

*Übung 4.6.1.30.* Besitzt ein von Null verschiedenes Element eines Tensorprodukts eine Darstellung der Gestalt  $v \otimes w$ , so sind seine möglichen Darstellungen dieser Gestalt genau alle Ausdrücke  $\lambda v \otimes \lambda^{-1}w$  mit  $\lambda \in K^\times$  einer Einheit des Grundkörpers  $K$ .

*Übung 4.6.1.31.* Seien  $V, W$  Vektorräume über demselben Grundkörper. Man zeige, daß die universelle bilineare Abbildung  $V \times W \rightarrow V \otimes W$  genau dann surjektiv ist, wenn einer der beiden beteiligten Räume eine Dimension  $\leq 1$  hat. Hinweis: 4.6.1.23.

*Übung 4.6.1.32.* Gegeben ein topologischer Raum  $X$  und ein endlichdimensionaler reeller Vektorraum  $V$  zeige man, daß die offensichtliche Abbildung einen Vektorraumisomorphismus  $\mathcal{C}(X, \mathbb{R}) \otimes_{\mathbb{R}} V \xrightarrow{\sim} \mathcal{C}(X, V)$  induziert. Hier bezeichnet  $\mathcal{C}(X, V)$  den Raum aller stetigen Abbildungen von  $X$  nach  $V$ .

*Ergänzende Übung 4.6.1.33.* Jede exakte Sequenz von Vektorräumen bleibt beim Darantensorieren eines weiteren Vektorraums exakt. Hinweis: 4.4.7.1, oder alternativ 4.7.8.11 und 4.4.6.13.

*Übung 4.6.1.34.* Gegeben ein Endomorphismus  $f \in \text{End } V$  eines Vektorraums mit  $f \otimes f = \text{id}$  in  $\text{End}(V \otimes V)$  gilt  $f = \pm \text{id}$ .

*Ergänzende Übung 4.6.1.35.* Gegeben ein Körper  $K$  und  $K$ -Vektorräume  $V, W$  und Endomorphismen endlichen Ranges  $f \in \text{End } V$  und  $g \in \text{End } W$  hat auch  $f \otimes g \in \text{End}(V \otimes W)$  endlichen Rang und es gilt

$$\text{tr}(f \otimes g) = \text{tr}(f) \text{tr}(g)$$

*Ergänzende Übung 4.6.1.36.* Hinweis: 3.6.4.15. Gegeben ein Körper  $K$  und endlichdimensionale  $K$ -Vektorräume  $V, W$  der Dimensionen  $n, m$  und Endomorphismen  $f \in \text{End } V$  und  $g \in \text{End } W$  gilt

$$\det(f \otimes g) = (\det(f))^m (\det(g))^n$$

*Ergänzende Übung 4.6.1.37 (Tensorprodukt und Orientierung).* Seien  $V$  ein Vektorraum und  $L$  ein eindimensionaler Vektorraum über demselben angeordneten Körper. Gegeben eine Orientierung  $\varepsilon$  von  $V$  und eine Orientierung  $\eta$  von  $L$  gibt es genau eine Orientierung  $\varepsilon \otimes \eta$  von  $V \otimes L$  mit

$$(\varepsilon \otimes \eta)(v_1 \otimes l, \dots, v_n \otimes l) = \varepsilon(v_1, \dots, v_n) \eta(l)^n$$

für jede angeordnete Basis  $(v_1, \dots, v_n)$  von  $V$  und jede angeordnete Basis alias jeden von Null verschiedenen Vektor  $l \in L$ .

*Übung 4.6.1.38 (Evaluationspaarung im Tensorkalkül).* Für jeden Vektorraum  $V$  über einem Körper  $K$  definiert das Auswerten oder lateinisierend „Evaluieren“ eine bilineare Abbildung, die **Evaluationspaarung**  $\text{ev} : V^\top \times V \rightarrow K$ ,  $(\xi, v) \mapsto \xi(v)$ . Man zeige, daß sie unter dem Isomorphismus aus 4.6.1.19 einerseits der Identität auf  $V^\top$  entspricht und andererseits, wenn wir die Faktoren vertauschen, der Evaluation  $\text{ev} : V \rightarrow V^{\top\top}$  aus 3.2.9.22.

*Ergänzende Übung 4.6.1.39.* Gegeben ein Körper  $K$  induziert die Multiplikation einen Isomorphismus  $K[X] \otimes_K K[Y] \xrightarrow{\sim} K[X, Y]$  zwischen dem Tensorprodukt zweier Polynomringe in einer Variablen und dem Polynomring in zwei Variablen.

*Ergänzende Übung 4.6.1.40.* Die Multiplikation induziert einen Isomorphismus von reellen Vektorräumen  $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}[X] \xrightarrow{\sim} \mathbb{R}[X]$ . Analoges gilt, wenn man  $\mathbb{R} \supset \mathbb{Q}$  ersetzt durch ein beliebiges Paar  $K \supset k$  bestehend aus einem Körper mit einem Teilkörper.

*Ergänzende Übung 4.6.1.41.* Gegeben Vektorräume  $V, W$  über einem Körper  $K$  und ein Untermonoid  $G \subset \text{End}(W)$  ist die offensichtliche lineare Abbildung ein Isomorphismus  $V \otimes (W^G) \xrightarrow{\sim} (V \otimes W)^G$ . Der obere Index  $G$  steht hier für den Teilraum der  $G$ -Invarianten.

*Ergänzende Übung 4.6.1.42.* Gegeben Körper  $k \subset K$  und ein  $k$ -Vektorraum  $V$  wird  $V_K = K \otimes_k V$  in offensichtlicher Weise ein  $K$ -Vektorraum. Man sagt, er entstehe aus  $V$  durch **Erweiterung der Skalare**. Die „kanonische“  $k$ -lineare Abbildung  $\text{can} : V \rightarrow V_K$ ,  $v \mapsto 1 \otimes v$  hat dann die universelle Eigenschaft, daß für jeden  $K$ -Vektorraum  $W$  das Vorschalten von  $\text{can} : V \rightarrow V_K$  eine Bijektion

$$\text{Hom}_K(V_K, W) \xrightarrow{\sim} \text{Hom}_k(V, W)$$

liefert. Weiter ist das Bild unter  $\text{can}$  jeder  $k$ -Basis von  $V$  eine  $K$ -Basis von  $V_K$ , und gegeben ein weiterer  $k$ -Vektorraum  $W$  induziert die  $k$ -lineare Abbildung  $V \otimes_k W \rightarrow V_K \otimes_K W_K$ ,  $v \otimes w \mapsto \text{can}(v) \otimes \text{can}(w)$  einen Isomorphismus

$$(V \otimes_k W)_K \xrightarrow{\sim} V_K \otimes_K W_K$$

Ist  $V$  oder  $K$  endlichdimensional über  $k$ , so liefert auch die  $k$ -lineare Abbildung  $\text{Hom}_k(V, W) \rightarrow \text{Hom}_K(V_K, W_K)$  gegeben durch  $f \mapsto \text{id} \otimes f$  einen Isomorphismus

$$(\text{Hom}_k(V, W))_K \xrightarrow{\sim} \text{Hom}_K(V_K, W_K)$$

und insbesondere „vertauscht das Erweitern der Skalare mit dem Bilden des Dualraums“ sowohl unter der Annahme  $\dim_k K < \infty$  als auch unter der Annahme  $\dim_k V < \infty$ . In voller Allgemeinheit vertauschen diese Operationen jedoch nicht. Im Spezialfall  $\mathbb{R} \subset \mathbb{C}$  bezeichnet man  $V_{\mathbb{C}}$  als **Komplexifizierung** von  $V$ .

*Ergänzende Übung 4.6.1.43.* Ist  $V$  ein  $k$ -Vektorraum und  $f : V \rightarrow V$  ein Endomorphismus endlichen Ranges und  $k \subset K$  eine Körpererweiterung, so gilt  $\text{tr}_k(f|V) = \text{tr}_K(\text{id} \otimes f|V_K)$ .

*Ergänzung 4.6.1.44.* Ein alternativer vom Tensorprodukt unabhängiger Zugang zur Komplexifizierung wird in ?? erklärt. Etwas allgemeiner können wir, nun wieder mit unserem Tensorprodukt, für jeden Körperhomomorphismus  $\varphi : k \hookrightarrow K$  zu einem  $k$ -Vektorraum  $V$  den  $k$ -Vektorraum  $K \otimes_k^{\varphi} V$  erklären. Ist speziell  $\varphi$  die komplexe Konjugation  $c : \mathbb{C} \rightarrow \mathbb{C}$ , so erhalten wir einen Isomorphismus  $\mathbb{C} \otimes_{\mathbb{C}}^c V \xrightarrow{\sim} \bar{V}$  mit unserem komplex konjugierten Vektorraum  $\bar{V}$  aus 4.1.12.33 vermittels der Abbildungsvorschrift  $1 \otimes v \mapsto \bar{v}$ .

*Ergänzende Übung 4.6.1.45.* Gegeben ein Vektorraum  $V$  und eine Teilmenge  $T \subset V$  setzen wir  $T^\perp = \{f \in V^\top \mid f(t) = 0 \quad \forall t \in T\}$ . Ist  $V$  endlichdimensional und  $W \subset V$  ein Teilraum, so zeige man, daß unter der Identifikation  $\text{End } V \xrightarrow{\sim} V \otimes V^\top$  die Identität  $\text{id}_V$  stets im Teilraum  $W \otimes V^\top + V \otimes W^\perp$  landet.

*Ergänzende Übung 4.6.1.46.* Gegeben ein endlichdimensionaler  $K$ -Vektorraum  $V$  kommutiert das Diagramm

$$\begin{array}{ccc} \sum_{i=1}^n v_i \otimes v_i^\top & \in & V \otimes V^\top \xrightarrow{\text{ev}} K \\ \downarrow & & \downarrow \wr \\ \text{id} & \in & \text{End } V \xrightarrow{\text{tr}} K \end{array}$$

Hier meint  $v_1, \dots, v_n$  eine beliebige Basis von  $V$  und  $v_1^\top, \dots, v_n^\top$  die duale Basis von  $V^\top$  und die mittlere Vertikale die in 4.6.1.21 erklärte Injektion und ev das Auswerten im Sinne von 4.6.1.38. Die lineare Abbildung  $K \rightarrow V \otimes V^\top$  mit  $1 \mapsto \sum_{i=1}^n v_i \otimes v_i^\top$  nennen wir auch die **Expansion der Identität** und notieren sie

$$\text{ex} : K \rightarrow V \otimes V^\top$$

Hat  $V$  unendliche Dimension, so kommutiert das rechte Quadrat immer noch, wenn wir unten links nur Endomorphismen endlichen Ranges betrachten und ihre Spur wie in 3.2.6.19 nehmen. Allerdings sind dann unser Tensorausdruck und unsere Expansion der Identität nicht mehr sinnvoll definiert und die Identität gehört auch nicht mehr zu den Endomorphismen endlichen Ranges.

*Ergänzende Übung 4.6.1.47.* Gegeben Mengen  $X, Y$  und ein beliebiger Körper  $K$  liefert die offensichtliche Abbildung  $f \otimes g \mapsto f \boxtimes g$  gegeben durch die Vorschrift  $(f \boxtimes g)(x, y) := f(x)g(y)$  eine Injektion

$$\text{Ens}(X, K) \otimes \text{Ens}(Y, K) \hookrightarrow \text{Ens}(X \times Y, K)$$

Man mag sich dazu auf 4.6.1.25 stützen. Alternativ mag man auch unabhängig zeigen, daß für  $g_1, \dots, g_n \in \text{Ens}(Y, K)$  linear unabhängig und  $f_1, \dots, f_n \in \text{Ens}(X, K)$  beliebig aus  $\sum f_i(x)g_i(y) = 0$  für alle  $x, y$  bereits folgt, daß alle  $f_i$  die Nullfunktion sein müssen. Betrachtet man hier statt einem Körper  $K$  einen Kring, so ist die analoge Aussage im allgemeinen nicht mehr richtig, vergleiche ??.

*Ergänzende Übung 4.6.1.48.* Gegeben Vektorräume  $V, V', W, W'$  liefert das Tensorieren von Abbildungen eine Injektion

$$\text{Hom}(V, V') \otimes \text{Hom}(W, W') \hookrightarrow \text{Hom}(V \otimes W, V' \otimes W')$$

Hinweis: Man mag  $V$  und  $W$  als direkte Summe eindimensionaler Räume schreiben und 4.7.8.12 anwenden. Alternative: Man mag ohne Beschränkung der Allgemeinheit annehmen, daß unsere Vektorräume frei sind über den Mengen  $X, X', Y, Y'$ , und kann dann unter Verwendung von 4.6.1.47 beide Seiten in verträglicher Weise einbetten in den Raum  $\text{Ens}(X \times X' \times Y \times Y', K)$  aller Abbildungen von besagtem Produkt in den Grundkörper  $K$ .

*Übung 4.6.1.49.* Bezeichne  $\tau : V \otimes V \rightarrow V \otimes V$  die Vertauschung der Tensorfaktoren. Man zeige, daß in Charakteristik Zwei der Teilraum der  $\tau$ -Invarianten erzeugt wird von allen  $(v \otimes w + w \otimes v)$  zusammen mit allen  $(v \otimes v)$ . Man zeige, daß in anderer Charakteristik Erstere ausreichen.

*Übung 4.6.1.50.* Bezeichne  $\sigma : V \otimes V \otimes V \rightarrow V \otimes V \otimes V$  die zyklische Vertauschung der Tensorfaktoren. Man zeige, daß in Charakteristik Drei der Teilraum der  $\sigma$ -Invarianten erzeugt wird von allen  $(u \otimes v \otimes w + v \otimes w \otimes u + w \otimes u \otimes v)$  zusammen mit allen  $(v \otimes v \otimes v)$ . Man zeige, daß in anderer Charakteristik Erstere ausreichen.

## 4.6.2 Multiverknüpfung multilinearer Abbildungen\*

*Beispiel 4.6.2.1.* Gegeben Vektorräume  $U', U'', U, V, W$  und eine bilineare Abbildung  $f : U \times V \rightarrow W$  sowie eine bilineare Abbildung  $g : U' \times U'' \rightarrow U$  erhalten

wir offensichtlich eine trilineare Abbildung

$$U' \times U'' \times V \rightarrow W$$

durch die Vorschrift  $(u', u'', v) \mapsto f(g(u', u''), v)$ . Gegeben zusätzlich ein ausgezeichneter Vektor  $v \in V$  erhalten wir eine bilineare Abbildung

$$U' \times U'' \rightarrow W$$

durch die Vorschrift  $(u', u'') \mapsto f(g(u', u''), v)$ . Diese Konstruktionen sind beide Spezialfälle für die „Multiverknüpfung“ multilinearer Abbildungen, die wir im folgenden besprechen.

**4.6.2.2 (Notation für multilineare Abbildungen).** Seien  $K$  ein Körper,  $n \geq 0$  eine natürliche Zahl und  $V_1, \dots, V_n, W$  Vektorräume über  $K$ . Wir verwenden im folgenden für Mengen von multilinearen Abbildungen die alternative Notation

$$\text{Mod}_K(V_1 \curlyvee \dots \curlyvee V_n, W) := \text{Hom}_K^{(n)}(V_1 \times \dots \times V_n, W)$$

Da durch die Verwendung des Symbols  $\curlyvee$  als Trenner keine Verwechslungsgefahr mit linearen Abbildungen aus dem Produktvektorraum besteht, können wir den oberen Index  $(n)$  auf der linken Seite weglassen. Im Fall  $n = 0$  notieren wir diese Menge  $\text{Mod}_K(\curlyvee, W)$ . Das Kürzel  $\text{Mod}_K$  steht für „ $K$ -Modul“, ein Synonym für „ $K$ -Vektorraum“.

**4.6.2.3 (Multiverknüpfung multilinearer Abbildungen).** Seien  $K$  ein Körper und  $n, m \geq 0$  und  $U_1, \dots, U_m, V_1, \dots, V_n, W$  Vektorräume über  $K$ . Seien  $f$  eine multilineare Abbildung

$$f \in \text{Mod}_K(V_1 \curlyvee \dots \curlyvee V_n, W)$$

und  $\varphi : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$  eine Abbildung und

$$g_i \in \text{Mod}_K(U_{\varphi^{-1}(i)}, V_i)$$

multilineare Abbildungen von der auf die Faser  $\varphi^{-1}(i)$  eingeschränkte Familie mit der induzierten Anordnung. Ausgeschrieben meinen wir also

$$g_i \in \text{Mod}_K(U_{\nu(1)} \curlyvee \dots \curlyvee U_{\nu(r)}, V_i)$$

für  $\nu(1) < \dots < \nu(r)$  die der Größe nach geordneten Elemente der Faser  $\varphi^{-1}(i)$ . So erklären wir in der hoffentlich offensichtlichen Weise die **Multiverknüpfung** unserer multilinearen Abbildungen, eine multilineare Abbildung

$$f \circ (\varphi, g_1 \curlyvee \dots \curlyvee g_n) \in \text{Mod}_K(U_1 \curlyvee \dots \curlyvee U_m, W)$$

Die Symbole  $\gamma$  sind dabei auch links nur als Trenner zu verstehen, die andeuten, daß wir mit Multiverknüpfungen arbeiten. Ist  $\varphi$  monoton wachsend und surjektiv, so lassen wir es gerne aus der Notation weg. Unsere trilineare Abbildung aus obigen Beispiel hieße dann  $f \circ (g \gamma \text{id}_V)$  und unsere letzte bilineare Abbildung wäre die Multiverknüpfung  $f \circ (g \gamma v)$  für  $v \in \text{Mult}_K(\gamma, V)$  das Bild von  $v$  unter der kanonischen Bijektion  $V \xrightarrow{\sim} \text{Mult}_K(\gamma, V)$ . Die Multiverknüpfung multilinearer Abbildungen ist „assoziativ“ in einer hoffentlich offensichtlichen Weise, die ich an dieser Stelle nicht weiter formalisieren will.

**4.6.2.4 (Multiverknüpfung universeller multilinearer Abbildungen).** Sei  $K$  ein Körper. Viele unserer Regeln für das Rechnen mit Tensorprodukten lassen sich zusammenfassen als einfache Konsequenzen der Tatsache, daß jede Multiverknüpfung universeller multilinearer Abbildungen wieder universell ist. Sind also in der obigen Notation  $f$  und alle  $g_i$  universell, so auch  $f \circ (\varphi, g_1 \gamma \dots \gamma g_n)$ . Zum Beispiel ist die Identität  $\text{id}_V : V \rightarrow V$  universell 1-linear und der Morphismus  $1 : * \rightarrow K$  universell 0-linear und  $\tau : V \times K \rightarrow V \otimes K$  universell bilinear. Es folgt, daß auch  $\tau \circ (\text{id}_V \gamma 1)$  universell 1-linear alias ein Isomorphismus ist, als da heißt, die Abbildung  $V \rightarrow V \otimes K$  gegeben durch  $v \mapsto v \otimes 1$  ist ein Isomorphismus. Das zeigt dann auch, daß das Vorschalten der 0-linearen Abbildung  $* \rightarrow K$  für jeden Vektorraum  $W$  eine Bijektion  $\text{Mod}_K(V \gamma K, W) \xrightarrow{\sim} \text{Mod}_K(V, W)$  liefert. Einen für diese und ähnliche Situationen maßgeschneiderten formalen Rahmen bilden die „Schmelzkategorien“, die in ?? eingeführt werden.

### 4.6.3 Bezug zur physikalischen Terminologie\*

**4.6.3.1 (Diskussion der Notation).** Im folgenden verwende ich die in der Physik übliche Notation mit oberen und unteren Indizes und der Konvention, daß üblicherweise die Summationsindizes einmal oben und einmal unten auftreten.

**4.6.3.2 (Kontravariante Tensoren erster Stufe sind Vektoren).** Sei  $V$  ein endlichdimensionaler Vektorraum. Unter einem **kontravarianten physikalischen Tensor erster Stufe zu  $V$**  verstehen wir eine Vorschrift  $T$ , die jeder angeordneten Basis  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$  von  $V$  ein Zahlentupel  $(T(\mathcal{B})^k)_{k=1}^n$  so zuordnet, daß für jede weitere angeordnete Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  von  $V$  mit den Einträgen  $A_k^i$  der Basiswechselmatrix gegeben durch  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  gilt

$$T(\mathcal{A})^i = \sum_k T(\mathcal{B})^k A_k^i \quad \text{alias} \quad T(\mathcal{B})^k = \sum_i T(\mathcal{A})^i (A^{-1})_i^k$$

mit den Einträgen der inversen Matrix rechts. Für jeden Vektor  $\vec{u}$  erhalten wir einen derartigen kontravarianten Tensor erster Stufe  $T = T_{\vec{u}}$  durch die Vorschrift, daß jeder angeordneten Basis dasjenige Tupel  $(T(\mathcal{B})^k)$  zuordnet werden möge,

das gegeben wird durch  $\vec{u} = \sum T(\mathcal{B})^k \vec{w}_k$ . In der Tat gilt dann

$$\vec{u} = \sum_k T(\mathcal{B})^k \vec{w}_k = \sum_{k,i} T(\mathcal{B})^k A_k^i \vec{v}_i = \sum_i T(\mathcal{A})^i \vec{v}_i$$

und somit  $T(\mathcal{A})^i = \sum_k T(\mathcal{B})^k A_k^i$ . Unsere Abbildung  $\vec{u} \mapsto T_{\vec{u}}$  liefert sogar, wie man leicht prüft, eine Bijektion zwischen der Menge  $V$  und der Menge aller kontravarianten Tensoren erster Stufe zu  $V$ .

**4.6.3.3 (Kovariante Tensoren erster Stufe sind Kovektoren).** Seien  $K$  ein Körper und  $V$  ein endlichdimensionaler  $K$ -Vektorraum. Ein **kovarianter physikalischer Tensor erster Stufe zu  $V$**  ist eine Vorschrift  $T$ , die jeder angeordneten Basis  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$  von  $V$  ein Zahlentupel  $(T(\mathcal{B})_k)_{k=1}^n$  so zuordnet, daß für jede weitere angeordnete Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  von  $V$  mit den Einträgen  $A_k^i$  der Basiswechselmatrix gegeben durch  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  gilt

$$T(\mathcal{B})_k = \sum_i A_k^i T(\mathcal{A})_i$$

Für jede Linearform  $\lambda : V \rightarrow K$  alias jedes Element des Dualraums  $\lambda \in V^\top$  erhalten wir einen derartigen kovarianten Tensor erster Stufe  $T = T_\lambda$  durch die Vorschrift, daß jeder angeordneten Basis dasjenige Tupel  $(T(\mathcal{B})_k)$  zuordnet werden möge, das gegeben wird durch die Koeffizienten der Darstellung von  $\lambda$  in der dualen Basis, in Formeln  $\lambda = \sum_k T(\mathcal{B})_k \vec{w}_k^\top$ . In der Tat gilt dann

$$T(\mathcal{B})_k = \lambda(\vec{w}_k) = \sum_i A_k^i \lambda(\vec{v}_i) = \sum_i A_k^i T(\mathcal{A})_i$$

Unsere Abbildung  $\lambda \mapsto T_\lambda$  liefert sogar, wie man leicht prüft, eine Bijektion zwischen dem Dualraum  $V^\top$  und der Menge aller kovarianten Tensoren erster Stufe zu  $V$ .

**4.6.3.4 (Kovariante Tensoren zweiter Stufe sind Bilinearformen).** Sei  $V$  ein endlichdimensionaler Vektorraum über einem Körper  $K$ . Ein **kovarianter physikalischer Tensor zweiter Stufe zu  $V$**  ist eine Vorschrift  $T$ , die jeder angeordneten Basis  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$  von  $V$  ein Zahlentupel  $(T(\mathcal{B})_{kl})_{k,l=1}^n$  so zuordnet, daß für jede weitere angeordnete Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  von  $V$  mit den Einträgen  $A_k^i$  der Basiswechselmatrix gegeben durch  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  gilt

$$T(\mathcal{B})_{kl} = \sum_{i,j} A_l^j A_k^i T(\mathcal{A})_{ij}$$

Für jede bilineare Abbildung  $b : V \times V \rightarrow K$  erhalten wir einen derartigen kovarianten Tensor zweiter Stufe  $T = T_b$  durch die Vorschrift, daß jeder angeordneten Basis

dasjenige Tupel  $(T(\mathcal{B})_{kl})$  zuordnet werden möge, das gegeben wird durch die Vorschrift  $T(\mathcal{B})_{kl} := b(\vec{w}_k, \vec{w}_l)$ . In der Tat gilt dann

$$T(\mathcal{B})_{kl} = b(\vec{w}_k, \vec{w}_l) = \sum_{i,j} A_k^i A_l^j b(\vec{v}_i, \vec{v}_j) = \sum_{i,j} A_k^i A_l^j T(\mathcal{A})_{ij}$$

Unsere Abbildung  $b \mapsto T_b$  liefert sogar, wie man leicht prüft, eine Bijektion zwischen dem Raum  $\text{Hom}_K^{(2)}(V \times V, K)$  von bilinearen Abbildungen und der Menge aller kovarianten Tensoren zweiter Stufe zu  $V$ .

**4.6.3.5 (Kontravariante Tensoren zweiter Stufe sind duale Bilinearformen).** Sei  $V$  ein endlichdimensionaler Vektorraum über einem Körper  $K$ . Ein **kontravarianter physikalischer Tensor zweiter Stufe** ist eine Vorschrift  $T$ , die jeder angeordneten Basis  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$  von  $V$  ein Zahlentupel  $(T(\mathcal{B})^{kl})_{k,l=1}^n$  so zuordnet, daß für jede weitere angeordnete Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  von  $V$  mit den Einträgen  $A_k^i$  der Basiswechselmatrix gegeben durch  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  gilt

$$T(\mathcal{A})^{ij} = \sum_{k,l} A_k^i A_l^j T(\mathcal{B})^{kl} \quad \text{alias} \quad T(\mathcal{B})^{kl} = \sum_{i,j} (A^{-1})_i^k (A^{-1})_j^l T(\mathcal{A})^{ij}$$

Für jede bilineare Abbildung  $\beta : V^\top \times V^\top \rightarrow K$  erhalten wir einen derartigen kovarianten Tensor zweiter Stufe  $T = T_\beta$  durch die Vorschrift, daß jeder angeordneten Basis dasjenige Tupel  $(T(\mathcal{B})^{kl})$  zuordnet werden möge, das gegeben wird durch die Vorschrift  $T(\mathcal{B})^{kl} := \beta(\vec{w}_k^\top, \vec{w}_l^\top)$ . In der Tat folgt aus  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  bereits  $\vec{v}_i^\top(\vec{w}_k) = A_k^i$  alias  $\vec{v}_i^\top = \sum_k A_k^i \vec{w}_k^\top$  und somit

$$T(\mathcal{A})^{ij} = \beta(\vec{v}_i^\top, \vec{v}_j^\top) = \sum_{k,l} A_k^i A_l^j \beta(\vec{w}_k^\top, \vec{w}_l^\top) = \sum_{k,l} A_k^i A_l^j T(\mathcal{B})^{kl}$$

Unsere Abbildung  $b \mapsto T_\beta$  liefert sogar, wie man leicht prüft, eine Bijektion zwischen dem Raum  $\text{Hom}_K^{(2)}(V^\top \times V^\top, K)$  von bilinearen Abbildungen und der Menge aller kontravarianten Tensoren zweiter Stufe zu  $V$ . Zusammen mit 4.6.1.25 erhalten wir dann auch eine Bijektion zwischen  $V \otimes V$  und der Menge aller kontravarianten Tensoren zweiter Stufe zu  $V$ .

**4.6.3.6 (Ko-kontravariante Tensoren zweiter Stufe sind Endomorphismen).** Sei  $V$  ein endlichdimensionaler  $K$ -Vektorraum. Ein **ko-kontravarianter physikalischer Tensor zweiter Stufe zu  $V$**  ist eine Vorschrift  $T$ , die jeder angeordneten Basis  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$  ein Zahlentupel  $(T(\mathcal{B})_k^l)_{k,l=1}^n$  so zuordnet, daß für jede weitere angeordnete Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  von  $V$  mit den Einträgen  $A_k^i$  der Basiswechselmatrix gegeben durch  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  gilt

$$T(\mathcal{B})_k^l = \sum_{i,j} (A^{-1})_j^l A_k^i T(\mathcal{A})_i^j$$

Für jede lineare Abbildung  $f : V \rightarrow V$  erhalten wir einen derartigen ko-kontravarianten Tensor zweiter Stufe  $T = T_f$  durch die Vorschrift, daß jeder angeordneten Basis dasjenige Tupel  $(T(\mathcal{B})_k^l)$  zuordnet werden möge, das gegeben wird durch die Vorschrift  $f(\vec{w}_k) = \sum_l T(\mathcal{B})_k^l \vec{w}_l$ . In der Tat gilt dann

$$\sum_l T(\mathcal{B})_k^l \vec{w}_l = f(\vec{w}_k) = \sum_i A_k^i f(\vec{v}_i) = \sum_{i,j} A_k^i T(\mathcal{A})_i^j \vec{v}_j = \sum_{i,j,l} A_k^i T(\mathcal{A})_i^j (A^{-1})_j^l \vec{w}_l$$

Unsere Abbildung  $f \mapsto T_f$  liefert sogar, wie man leicht prüft, eine Bijektion zwischen der Menge  $\text{End}_K(V)$  aller Endomorphismen von  $V$  und der Menge aller ko-kontravarianten Tensoren zweiter Stufe zu  $V$ .

**4.6.3.7 (Allgemeine physikalische Tensoren als multilinear Abbildungen).** Sei  $V$  ein endlichdimensionaler  $K$ -Vektorraum. Gegeben  $r, s \geq 0$  definiert man einen  **$r$ -ko- $s$ -kontravarianten physikalischen Tensor zu  $V$**  als eine Vorschrift  $T$ , die jeder angeordneten Basis  $\mathcal{B} = (\vec{w}_1, \dots, \vec{w}_n)$  ein von  $r$  unteren und  $s$  oberen Indizes aus  $1, \dots, n$  abhängendes Zahlentupel so zuordnet, daß die Tupel zu verschiedenen angeordneten Basen in einer Weise zusammenhängen, die ich hier nur noch im Fall  $r = 2$  und  $s = 1$  ausfühe: In diesem Fall fordert man, daß für jede weitere angeordnete Basis  $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_n)$  von  $V$  mit den Einträgen  $A_k^i$  der Basiswechselmatrix gegeben durch  $\vec{w}_k = \sum_i A_k^i \vec{v}_i$  gilt

$$T(\mathcal{B})_{kl}^m = \sum_{i,j,p} (A^{-1})_p^m A_k^i A_l^j T(\mathcal{A})_{ij}^p$$

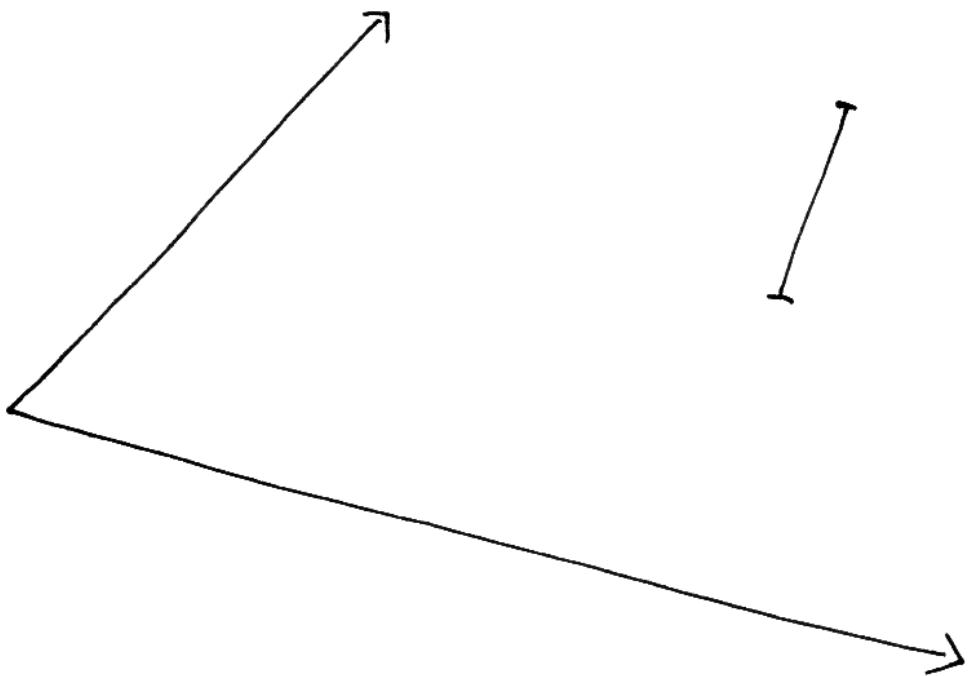
Wie zuvor kann man jeder multilineareren Abbildung  $u : V^r \times (V^\top)^s \rightarrow K$  einen  $r$ -ko- $s$ -kontravarianten Tensor  $T_u$  zuordnen, der in unserem Spezialfall  $(r, s) = (2, 1)$  gegeben wird durch  $T_u(\mathcal{B})_{kl}^m = u(\vec{w}_k, \vec{w}_l, \vec{w}_m^\top)$ , und wieder erhalten wir so eine Bijektion zwischen der Menge  $\text{Hom}_K^{(r+s)}(V^r \times (V^\top)^s, K)$  von multilineareren Abbildungen und der Menge aller  $r$ -ko- $s$ -kontravarianten Tensoren zweiter Stufe zu  $V$ . Alternativ erhalten wir mit unserem Satz 4.6.1.25 auch zu jedem Element von  $t \in (V^\top)^{\otimes r} \otimes V^{\otimes s}$  einen  $r$ -ko- $s$ -kontravarianten Tensor  $T_t$ , der in unserem Spezialfall  $(r, s) = (2, 1)$  gegeben wird durch

$$t = \sum_{m,k,l} T_t(\mathcal{B})_{kl}^m \vec{w}_k^\top \otimes \vec{w}_l^\top \otimes \vec{w}_m$$

Auch diese Zuordnung ist bijektiv und erklärt den Zusammenhang der beiden Tensorbegriffe.

#### 4.6.4 Geometrie in euklidischen Vektorräumen

**4.6.4.1.** Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem angeordneten Körper  $K$  erinnern wir seine zweielementige Orientierungsmenge  $\text{or}(V)$  aus



Das folgende ist eine nicht ganz mathematische Übung: Man schätze ab, ob das durch die eingezeichnete Längeneinheit und die anschauliche Kongruenzgruppe gegebene Skalarprodukt der beiden hier gezeichneten Vektoren größer ist als Zehn. Man verwende dabei nur ein Papier mit einer geraden Kante, das man kniffen darf, um einen rechten Winkel zu erzeugen, einen Bleistift zum Abtragen von Längen, und Augenmaß. Man beachte, wie hierbei die Kongruenzgruppe zu Anwendung kommt.

3.6.5.3 und erklären seine **Orientierungsgerade** als den eindimensionalen Vektorraum

$$\text{or}_K(V) := \{a : \text{or}(V) \rightarrow K \mid \text{Die Summe der beiden Werte von } a \text{ ist Null}\}$$

Wir erhalten eine Injektion  $\text{or}(V) \hookrightarrow \text{or}_K(V)$ , indem wir jeder Orientierung  $\varepsilon \in \text{or}(V)$  diejenige Funktion  $a \in \text{or}_K(V)$  mit  $f(\varepsilon) = 1$  zuordnen. Besagte Injektion behandeln wir von nun an in der Notation wie die Einbettung einer Teilmenge. Für jeden Vektorraumisomorphismus  $f : V \xrightarrow{\sim} W$  läßt sich unsere Bijektion  $\text{or}(f)$  zwischen den Orientierungsmengen auf genau eine Weise zu einem Isomorphismus  $\text{or}_K(f) : \text{or}_K(V) \xrightarrow{\sim} \text{or}_K(W)$  ihrer Orientierungsgeraden ausdehnen.

4.6.4.2. Ich erinnere an den Begriff 4.1.5.12 eines euklidischen Vektorraums  $V$  mit seiner Längengerade  $\mathbb{L} = \mathbb{L}(V)$ .

4.6.4.3. Für jeden endlichdimensionalen euklidischen Vektorraum  $V$  gibt es genau eine alternierende Abbildung mit  $v_1 \otimes \dots \otimes v_n \mapsto \varepsilon \otimes \|v_1\| \otimes \dots \otimes \|v_n\|$  für eine und jede angeordnete Basis  $v_1, \dots, v_n$  der Orientierung  $\varepsilon$  aus paarweise orthogonalen Vektoren, die **geometrische Volumenform**

$$\omega : V^{\otimes n} \rightarrow \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)^{\otimes n}$$

In der Tat hat jede orthogonale Matrix die Determinante  $\pm 1$  und das zeigt, daß eine alternierende Abbildung, die diese Eigenschaft für eine Basis aus paarweise orthogonalen Vektoren hat, sie für jede solche Basis haben muß. Den Fall  $n = 2$  haben Sie im orientierten Fall bereits in Übung 4.6.1.27 diskutiert. Im Fall  $n = 3$  notieren wir unsere Abbildung

$$u \otimes v \otimes w \mapsto \langle u, v, w \rangle$$

und nennen sie das **geometrische Spatprodukt**. Für jeden euklidischen Homomorphismus  $f : V \rightarrow W$  von euklidischen Vektorräumen derselben Dimension  $n$  kommutiert weiter das Diagramm

$$\begin{array}{ccc} V^{\otimes n} & \longrightarrow & \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)^{\otimes n} \\ f^{\otimes n} \downarrow & & \downarrow \text{or}_{\mathbb{R}}(f) \otimes \mathbb{L}(f)^{\otimes n} \\ W^{\otimes n} & \longrightarrow & \text{or}_{\mathbb{R}}(W) \otimes \mathbb{L}(W)^{\otimes n} \end{array}$$

Diese Erkenntnis bringt die Natürlichkeit unserer Konstruktion formal zum Ausdruck und rechtfertigt die Bezeichnung „geometrisch“. Mehr dazu diskutieren wir im Zusammenhang mit „Transformationen von Funktoren“ in 4.7.4.8.

4.6.4.4. Das Tensorquadrat der Längengerade eines euklidischen Vektorraums nennen wir seine **Gerade von Flächeneinheiten** oder kurz seine **Flächengerade**.

*Vorschau 4.6.4.5 (Flächen- und Volumenmaße).* Gegeben ein euklidischer Raum  $E$  endlicher Dimension  $n$  mit Längengerade  $\mathbb{L}$  ordnen wir in ?? jeder kompakten  $k$ -Fastfaltigkeit  $M \subset E$  ein Volumen  $\int_M 1 \in \mathbb{L}^{\otimes k}$  so zu, daß für beliebige paarweise orthogonale von Null verschiedene Richtungsvektoren  $v_1, \dots, v_k \in \vec{E}$  und jeden Punkt  $p \in E$  der kompakten  $k$ -Fastfaltigkeit  $M := p + [0, 1]v_1 + \dots + [0, 1]v_k$  das Volumen  $\int_M 1 = \|v_1\| \otimes \dots \otimes \|v_k\| \in \mathbb{L}^{\otimes k}$  zugeordnet wird und im Fall  $\dim E = 3$  der Sphäre  $S := \{q \in E \mid \|q - p\| = l\}$  mit Zentrum  $p \in E$  und Radius  $l \in \mathbb{L}$  die Fläche  $\int_S 1 = 4\pi l^{\otimes 2}$ . Auch in der Mathematik werden also salopp gesprochen „Flächen in Quadratmetern gemessen“.

4.6.4.6. Für jeden euklidischen Vektorraum  $V$  erklären wir sein **geometrisches Skalarprodukt** als die eindeutig bestimmte symmetrische bilineare Abbildung

$$\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_V : V \times V \rightarrow \mathbb{L}^{\otimes 2}$$

in seine Flächengerade derart, daß für jeden Vektor  $v \in V$  gilt  $\langle v, v \rangle = \|v\|^2$ . Es kann beschrieben werden durch die Polarisierungsidentität  $\langle v, w \rangle = \frac{1}{2}(\|v+w\|^2 - \|v\|^2 - \|w\|^2)$  oder auch durch die Formel

$$\langle ae_1 + \dots + ce_n, xe_1 + \dots + ze_n \rangle = (ax + \dots + cz)l^2$$

für beliebige paarweise orthogonale Vektoren  $e_1, \dots, e_n$  derselben Länge  $\|e_1\| = \dots = \|e_n\| = l \in \mathbb{L}$ . Für jeden euklidischen Homomorphismus  $f : V \rightarrow W$  von euklidischen Vektorräumen kommutiert dann das Diagramm

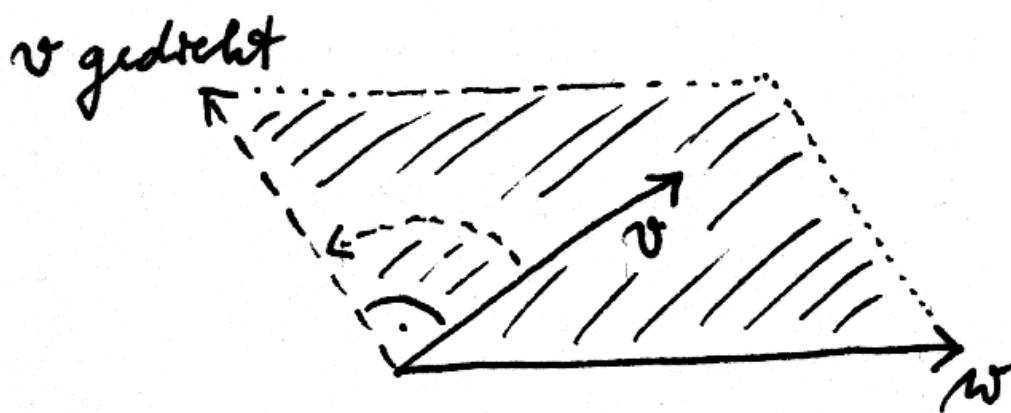
$$\begin{array}{ccc} V \times V & \xrightarrow{\langle \cdot, \cdot \rangle_V} & \mathbb{L}(V)^{\otimes 2} \\ f \times f \downarrow & & \downarrow \mathbb{L}(f)^{\otimes 2} \\ W \times W & \xrightarrow{\langle \cdot, \cdot \rangle_W} & \mathbb{L}(W)^{\otimes 2} \end{array}$$

Es bringt die Natürlichkeit unserer Konstruktion formal zum Ausdruck und rechtfertigt die Bezeichnung „geometrisch“. Mehr dazu diskutieren wir im Zusammenhang mit „Transformationen von Funktoren“ in 4.7.4.8.

4.6.4.7 (**Pythagoras**). In einem euklidischen Vektorraum sind zwei Vektoren  $v, w$  genau dann orthogonal, wenn in der zugehörigen Flächengerade  $\mathbb{L}^{\otimes 2}$  gilt

$$\|v\|^2 + \|w\|^2 = \|v + w\|^2$$

In der Tat folgt das unmittelbar aus der entsprechenden Aussage für Skalarprodukträume. Insbesondere gilt es für den Richtungsraum einer Kongruenzebene.



Anschauliche Bedeutung des geometrischen Skalarprodukts  $\langle v, w \rangle$  als Fläche

**4.6.4.8 (Zusätzliche Anschauung für das Skalarprodukt).** Man mag sich das geometrische Skalarprodukt  $\langle v, w \rangle$  im Fall eines zweidimensionalen euklidischen Vektorraums  $V$  vorstellen, indem man eine der beiden Drehungen um einen rechten Winkel auswählt, sie  $r$  nennt, und dann bemerkt, daß  $\langle v, w \rangle = \omega(rv, w)$  der orientierte Flächeninhalt von  $(rv, w)$  im Sinne von 4.6.4.3 ist für diejenige Orientierung  $\varepsilon = \varepsilon_r$  von  $V$ , die mit  $r$  verträglich ist in der Weise, daß  $(ru, u)$  für alle  $u \neq 0$  eine positiv orientierte Basis von  $V$  ist.

**4.6.4.9 (Kreuzprodukt für dreidimensionale euklidische Vektorräume).** Gegeben ein dreidimensionaler euklidischer Vektorraum  $V$  mit Längengerade  $\mathbb{L}$  gibt es genau eine alternierende bilineare Abbildung

$$\times = \times_V : V \times V \rightarrow V \otimes \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}$$

mit der Eigenschaft  $(v_1, v_2) \mapsto v_3 \otimes \varepsilon \otimes l$  für jede angeordnete Orthogonalbasis  $v_1, v_2, v_3$  der Orientierung  $\varepsilon$  aus Vektoren derselben Länge  $\|v_1\| = \|v_2\| = \|v_3\| = l \in \mathbb{L}$ . Wir nennen sie das **geometrische Kreuzprodukt** und notieren sie wieder  $(v, w) \mapsto v \times w$ . Für jeden euklidischen Homomorphismus  $f : V \rightarrow W$  von euklidischen Vektorräumen kommutiert dann das Diagramm

$$\begin{array}{ccc} V \times V & \xrightarrow{\quad \times_V \quad} & V \otimes \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V) \\ f \times f \downarrow & & \downarrow f \otimes \text{or}_{\mathbb{R}}(f) \otimes \mathbb{L}(f) \\ W \times W & \xrightarrow{\quad \times_W \quad} & W \otimes \text{or}_{\mathbb{R}}(W) \otimes \mathbb{L}(W) \end{array}$$

Es bringt die Natürlichkeit unserer Konstruktion formal zum Ausdruck und rechtfertigt die Bezeichnung „geometrisch“. Mehr dazu diskutieren wir im Zusammenhang mit „Transformationen von Funktionen“ in 4.7.4.8.

**4.6.4.10 (Spezialisierungen des geometrischen Kreuzprodukts).** Jede Orientierung auf  $V$  induziert andererseits einen Isomorphismus  $\mathbb{R} \xrightarrow{\sim} \text{or}_{\mathbb{R}}(V)$  und unser geometrisches Kreuzprodukt vereinfacht sich so im Fall eines dreidimensionalen orientierten euklidischen Vektorraums zu einem Kreuzprodukt der Gestalt

$$V \times V \rightarrow V \otimes \mathbb{L}$$

Jedes Skalarprodukt aus der euklidischen Struktur eines euklidischen Vektorraums induziert einen Isomorphismus  $\mathbb{R} \xrightarrow{\sim} \mathbb{L}$  und unser geometrisches Kreuzprodukt vereinfacht sich so im Fall eines dreidimensionalen Skalarproduktraums zu einem Kreuzprodukt der Gestalt

$$V \times V \rightarrow V \otimes \text{or}_{\mathbb{R}}(V)$$

Im Fall eines dreidimensionalen orientierten Skalarproduktraums schließlich greifen beide Vereinfachungen und wir erhalten noch einmal unser bereits in 4.1.9.1

betrachtetes Kreuzprodukt  $V \times V \rightarrow V$ . Im Fall  $V = \mathbb{R}^3$  mit seiner Standardorientierung und seinem Standardskalarprodukt schließlich spezialisiert dieses Kreuzprodukt zu dem aus der Schule bekannten Kreuzprodukt

$$(x, y, z) \times (a, b, c) = (yc - yb, za - xc, xb - ya)$$

## Übungen

*Übung 4.6.4.11.* Man diskutiere, inwiefern das geometrische Skalarprodukt für jeden endlichdimensionalen euklidischen Vektorraum  $V$  einen natürlichen Isomorphismus

$$V^\top \xrightarrow{\sim} V \otimes \mathbb{L}(V)^{\otimes(-2)}$$

induziert. Man drücke dessen Natürlichkeit durch ein kommutatives Rechteck aus.

*Übung 4.6.4.12.* Man zeige, daß 4.6.4.3 für pseudoeuklidische Vektorräume  $V$  einer endlichen Dimension unverändert gilt: Es gibt immer noch genau eine alternierende multilinear Abbildung

$$V^{\otimes n} \rightarrow \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)^{\otimes n}$$

mit  $v_1 \otimes \dots \otimes v_n \mapsto \varepsilon \otimes \|v_1\| \otimes \dots \otimes \|v_n\|$  für eine und jede angeordnete Basis  $v_1, \dots, v_n$  der Orientierung  $\varepsilon$  aus paarweise orthogonalen Vektoren. Die Längen gerade  $\mathbb{L}(V)$  und die Längen  $\|v\|$  sind dabei die in 4.2.7.6 erklärten.

## 4.6.5 Alternierende Tensoren und äußere Potenzen

4.6.5.1 (**Alternierende multilineare Abbildungen**). Gegeben Vektorräume  $V, C$  über einem Körper  $K$  und  $r \geq 0$  bezeichne

$$\text{Alt}_K(V^{\times r}, C) \subset \text{Hom}_K^{(r)}(V^{\times r}, C)$$

den Teilraum der alternierenden multilinear Abbildungen. Ich erinnere daran, daß eine multilinear Abbildung von mehreren Kopien ein- und desselben Vektorraums in einen weiteren Vektorraum **alternierend** heißt, wenn sie den Nullvektor ausgibt, wann immer man sie auf einem Tupel mit zwei oder mehr gleichen Einträgen auswertet. Wir vereinbaren zusätzlich wie in ?? die Abkürzung  $\text{Alt}_K^r(V) := \text{Alt}_K(V^{\times r}, K)$  für den Raum der alternierenden Multilinearformen. Statt „alternierend multilinear“ sagen meist kürzer nur „alternierend“. Die Determinante kann als ein Element  $\det \in \text{Alt}_K^n(K^n)$  aufgefaßt werden.

**Satz 4.6.5.2.** 1. Gegeben  $r \geq 0$  und ein Vektorraum  $V$  über einem Körper  $K$  existiert ein Paar  $(A, \alpha)$  bestehend aus einem  $K$ -Vektorraum  $A$  und einer

*alternierenden Abbildung  $\alpha : V^{\times r} \rightarrow A$  derart, daß für jeden weiteren  $K$ -Vektorraum  $C$  das Vorschalten von  $\alpha$  eine Bijektion*

$$(\circ\alpha) : \text{Hom}_K(A, C) \xrightarrow{\sim} \text{Alt}_K(V^{\times r}, C)$$

*zwischen der Menge aller linearen Abbildungen  $A \rightarrow C$  und der Menge aller alternierenden Abbildungen  $V^{\times r} \rightarrow C$  induziert. Wir nennen solch ein  $\alpha : V^{\times r} \rightarrow A$  eine **universelle  $r$ -alternierende Abbildung**;*

2. *Gegeben eine weitere universelle  $r$ -alternierende Abbildung  $\beta : V^{\times r} \rightarrow B$  existiert genau eine lineare Abbildung  $c : A \rightarrow B$  mit  $c \circ \alpha = \beta$  und genau eine lineare Abbildung  $d : B \rightarrow A$  mit  $d \circ \beta = \alpha$  und diese Abbildungen sind zueinander inverse Isomorphismen zwischen  $A$  und  $B$ .*

**4.6.5.3 (Notation für äußere Potenzen).** Der Beweis von Teil 2 ist identisch zum Beweis der Eindeutigkeit im Fall des Tensorprodukts zweier Vektorräume. Unsere Paare sind also „eindeutig bestimmt bis auf eindeutigen Isomorphismus“, wenn sie existieren. Insbesondere kommt es auf die genaue Konstruktion ebensowenig an wie auf die genaue Konstruktion der natürlichen oder der reellen Zahlen. So eine universelle  $r$ -alternierende Abbildung  $\alpha : V^{\times r} \rightarrow A$  verdient damit den bestimmten Artikel und eine Notation. Man nennt  $A$  die  **$r$ -te äußere Potenz von  $V$**  und notiert diesen Vektorraum

$$\bigwedge^r V$$

und  $(v_1, \dots, v_r) \mapsto v_1 \wedge \dots \wedge v_r$  die universelle alternierende Abbildung für  $r \geq 1$ . Im Fall  $r = 1$  wählen wir stets  $\bigwedge^1 V := V$  mit der Identität als universeller 1-linearer Abbildung  $\alpha : V^{\times 1} \rightarrow V$ , so daß unsere Notation auch in diesem Fall nicht zweideutig wird. Im Fall  $r = 0$  wählen wir üblicherweise  $\bigwedge^0 V := K$  mit der durch  $* \mapsto 1_K$  bestimmten 0-alternierenden alias beliebigen Abbildung  $\alpha : \text{ens} = V^{\times 0} \rightarrow K$ .

*Beweis.* Es bleibt nur Teil 1 zu zeigen. Dazu bilden wir in der  $r$ -ten Tensorpotenz von  $V$  das Erzeugnis  $J_r \subset V^{\otimes r}$  aller Tensoren mit zwei oder mehr gleichen Einträgen und betrachten die Verknüpfung  $\alpha : V \times \dots \times V \rightarrow V^{\otimes r} \rightarrow V^{\otimes r}/J_r$  der kanonischen multilineareren Abbildung mit der kanonischen Abbildung auf den Quotienten. Aufgrund der universellen Eigenschaften von Tensorprodukt und Quotient erhalten wir Isomorphismen

$$\text{Alt}(V^{\times r}, C) \xleftarrow{\sim} \{g \in \text{Hom}(V^{\otimes r}, C) \mid g(J_r) = 0\} \xleftarrow{\sim} \text{Hom}(V^{\otimes r}/J_r, C)$$

So sehen wir, daß  $\alpha$  die geforderte universelle Eigenschaft hat.  $\square$

**4.6.5.4 (Dachprodukt).** Sei  $V$  ein Vektorraum. Gegeben  $r, s \geq 0$  gibt es genau eine bilineare Abbildung

$$\Lambda^r V \times \Lambda^s V \rightarrow \Lambda^{r+s} V$$

derart, daß mit dem Zusammentensorieren von Tensoren in der oberen Horizontale und besagter Abbildung in der unteren Horizontale das Diagramm

$$\begin{array}{ccc} V^{\otimes r} \times V^{\otimes s} & \longrightarrow & V^{\otimes(r+s)} \\ \downarrow & & \downarrow \\ \Lambda^r V \times \Lambda^s V & \longrightarrow & \Lambda^{r+s} V \end{array}$$

kommutiert. Man folgert das unschwer aus Übung 4.4.5.9 zu auf Quotienten induzierten multilinaren Abbildungen, da die obere Horizontale unseres Diagramms sowohl  $J_r \times V^{\otimes s}$  als auch  $V^{\otimes r} \times J_s$  auf Teilmengen von  $J_{r+s}$  abbildet. Unsere so konstruierte bilineare Abbildung  $\Lambda^r V \times \Lambda^s V \rightarrow \Lambda^{r+s} V$  notieren wir  $\bar{\wedge}$ . Per definitionem gilt

$$(v_1 \wedge \dots \wedge v_p) \bar{\wedge} (w_1 \wedge \dots \wedge w_q) = v_1 \wedge \dots \wedge v_p \wedge w_1 \wedge \dots \wedge w_q$$

für alle  $v_i, w_j \in V$ . Wir folgern die Assoziativität  $(\omega \bar{\wedge} \eta) \bar{\wedge} \xi = \omega \bar{\wedge} (\eta \bar{\wedge} \xi)$  für alle  $\omega \in \Lambda^r V$ ,  $\eta \in \Lambda^s V$  und  $\xi \in \Lambda^t V$ , da allgemein multilineare und hier trilineare Abbildungen übereinstimmen, wenn sie auf Tupeln von Erzeugern dieselben Werte annehmen. Wir folgern weiter  $v_1 \wedge \dots \wedge v_p = v_1 \bar{\wedge} \dots \bar{\wedge} v_p$  für alle  $v_i \in V$ , wobei wir rechts implizit unsere Identifikation  $V = \Lambda^1 V$  aus 4.6.5.3 verwendet haben. Dadurch wird insbesondere unsere Notation  $\bar{\wedge}$  obsolet und wir dürfen und werden sie zu  $\wedge$  vereinfachen ohne Mehrdeutigkeiten befürchten zu müssen. Die Verknüpfung  $(\omega, \eta) \mapsto \omega \wedge \eta$  heißt das **Dachprodukt**, englisch **wedge-product**, französisch **produit extérieur**. Dafür gilt  $v \wedge w = -w \wedge v$  und sogar stärker  $v \wedge v = 0$  für alle  $v, w \in V$ .

**Definition 4.6.5.5.** Seien  $K$  ein Körper,  $V$  ein  $K$ -Vektorraum,  $(v_i)_{i \in I}$  eine Basis von  $V$  und  $\leq$  eine Anordnung von  $I$ . Gegeben eine endliche Teilmenge  $R \subset I$  mit  $|R| = r$  erklären wir  $v_R \in \Lambda^r V$  als das Dachprodukt

$$v_R := v_{i_1} \wedge \dots \wedge v_{i_r}$$

für  $i_1 < i_2 < \dots < i_r$  die der Größe nach geordneten Elemente von  $R$ . Im Extremfall  $r = 0$  vereinbaren wir  $v_\emptyset := 1 \in K = \Lambda^0 V$ .

**Proposition 4.6.5.6 (Basis und Dualraum für äußere Potenzen).** Seien  $K$  ein Körper,  $V$  ein  $K$ -Vektorraum und  $r \geq 0$ . So gilt:

1. Es existiert genau eine bilineare Abbildung

$$\beta : \bigwedge^r(V^\top) \times \bigwedge^r V \rightarrow K$$

mit  $((f_1 \wedge \dots \wedge f_r), (w_1 \wedge \dots \wedge w_r)) \mapsto \det(f_i(w_j));$

2. Diese bilineare Abbildung ist eine nichtausgeartete Paarung;

3. Ist  $(v_i)_{i \in I}$  eine Basis von  $V$  und wählen wir auf der Indexmenge  $I$  eine Anordnung, so bilden die Monome  $v_R$  mit  $R \subset I$  und  $|R| = r$  eine Basis der  $r$ -ten äußeren Potenz  $\bigwedge^r V$ .

4.6.5.7. Man beachte, daß unsere Abbildung von äußeren Potenzen des Dualraums zum Dualraum der äußeren Potenzen gewisse unkanonische Vorzeichenwahlen beinhaltet. Hier wären auch andere sinnvolle Wahlen von Vorzeichen denkbar, aber man muß sich halt einmal auf eine Konvention festlegen.

*Beispiel 4.6.5.8.* Eine Basis von  $\bigwedge^2 \mathbb{R}^4$  besteht etwa aus den sechs Dachprodukten  $e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4$  und  $e_3 \wedge e_4$ .

4.6.5.9. Im Zweifelsfall interpretieren wir  $\bigwedge^r V^\top$  im folgenden als  $\bigwedge^r(V^\top)$ . Unsere nichtausgeartete Paarung aus 4.6.5.6 induziert in der üblichen Weise eine natürliche Injektion  $\bigwedge^r(V^\top) \hookrightarrow (\bigwedge^r V)^\top$ . In Verbindung mit unserem kanonischen Isomorphismus  $(\bigwedge^r V)^\top \xrightarrow{\sim} \text{Alt}^r(V)$  aus 4.6.5.3 induziert sie damit auch eine natürliche Injektion

$$\bigwedge^r(V^\top) \hookrightarrow \text{Alt}^r(V)$$

Im endlichdimensionalen Fall  $\dim V < \infty$  zeigt ein Dimensionsvergleich unter Verwendung der vorhergehenden Proposition, daß alle diese Injektionen Isomorphismen sind. Im allgemeinen gilt das jedoch nicht.

*Beweis.* 1. Unsere Abbildungsvorschrift definiert offensichtlich eine bilineare Abbildung

$$(V^\top)^{\otimes r} \times V^{\otimes r} \rightarrow K$$

Diese bilineare Abbildung verschwindet offensichtlich auf allen Paaren, bei denen rechts oder links zwei Tensorfaktoren gleich sind. Nach Übung 4.4.5.9 zu auf Quotienten induzierten multilinearen Abbildungen induziert sie folglich die Abbildung, deren Existenz in der Proposition behauptet wird.

3. Alle Tensoren  $v_{i_1} \otimes \dots \otimes v_{i_r}$  für  $i_1, \dots, i_r \in I$  beliebig erzeugen nach 4.6.1.4 die  $r$ -te Tensorpotenz  $V^{\otimes r}$ . Alle Dachprodukte  $v_{i_1} \wedge \dots \wedge v_{i_r}$  erzeugen folglich die  $r$ -te äußere Potenz  $\bigwedge^r V$ . Beim Umordnen derartiger Dachprodukte ändert sich höchstens das Vorzeichen, und kommt ein Vektor doppelt vor, ist das fragliche Dachprodukt eh Null. Folglich erzeugen die Dachprodukte  $v_{i_1} \wedge \dots \wedge v_{i_r}$

mit  $i_1 < \dots < i_r$  unsere  $r$ -te äußere Potenz, und es bleibt nur, ihre lineare Unabhängigkeit nachzuweisen. Dazu betrachten wir die Koordinatenfunktionen  $f_i := v_i^\top \in V^\top$  zu unserer Basis und aus den Eigenschaften der Determinante folgt für je zwei  $r$ -elementige Teilmengen  $R, S \subset I$  unmittelbar

$$\beta(f_S, v_R) = \begin{cases} 1 & \text{falls } S = R; \\ 0 & \text{sonst.} \end{cases}$$

Das impliziert die lineare Unabhängigkeit der  $v_R$ .

2. Der vorherige Punkt zeigt auch die lineare Unabhängigkeit der  $f_S$  und zeigt so, daß unsere Paarung im Fall eines endlichdimensionalen Raums  $V$  nichtausgeartet ist. Der allgemeine Fall folgt daraus ohne weitere Schwierigkeiten.  $\square$

**4.6.5.10 (Dimensionen der äußeren Potenzen).** Aus 4.6.5.6 folgt für einen Vektorraum  $V$  endlicher Dimension  $\dim V = d < \infty$  sofort, daß die Dimensionen seiner äußeren Potenzen durch Binomialkoeffizienten gegeben werden und daß genauer gilt

$$\dim \bigwedge^r V = \binom{d}{r}$$

Insbesondere gilt  $\dim \bigwedge^d V = 1$  und  $\bigwedge^r V = 0$  für  $r > d$ . Man schreibt deshalb im endlichdimensionalen Fall oft  $\bigwedge^{\max} V := \bigwedge^{\dim V} V$ . Dieser Vektorraum ist natürlich stets eindimensional.

**4.6.5.11 (Zugang zu äußeren Potenzen über angeordnete Basen).** Im Rückblick erkennen wir, daß gegeben ein Körper  $K$  und ein  $K$ -Vektorraum  $V$  mit einer angeordneten Basis  $(\mathcal{B}, \leq)$  eine alternierende multilinear Abbildung  $V^{\times r} \rightarrow C$  in einen weiteren Vektorraum  $C$  durch ihre Werte auf streng monoton wachsenden  $r$ -Tupeln von Basisvektoren festgelegt und festlegbar ist. Bezeichnet also  $\mathcal{B}_<^{\times r}$  die Menge aller derartigen Tupel von Basisvektoren, so liefert in Formeln ausgedrückt die Restriktion eine Bijektion

$$\mathrm{Alt}^r(V^{\times r}, C) \xrightarrow{\sim} \mathrm{Ens}(\mathcal{B}_<^{\times r}, C)$$

Wir hätten die Theorie auch ähnlich wie im Fall von Tensorprodukten beliebiger Länge in der Weise entwickeln können, daß wir zunächst diese Aussage beweisen, um dann zu folgern, daß der freie Vektorraum  $K\langle\mathcal{B}_<^{\times r}\rangle$  zusammen mit der von der kanonischen Einbettung  $\mathrm{can} : \mathcal{B}_<^{\times r} \rightarrow K\langle\mathcal{B}_<^{\times r}\rangle$  unter obiger Bijektion induzierten alternierenden Abbildung

$$\alpha : V^{\times r} \rightarrow K\langle\mathcal{B}_<^{\times r}\rangle$$

eine universelle  $r$ -alternierende Abbildung ist. Dieser Zugang hat den Vorteil, daß unsere Proposition 4.6.5.6 über Basen äußerer Potenzen zu einer Tautologie wird. Sie hat den Nachteil, daß es etwas unangenehm ist, den Nachweis obiger Bijektion in Formeln auszuschreiben.

**4.6.5.12 (Äußere Potenzen und alternierende Tensoren).** Gegeben ein Vektorraum  $V$  definiert jede Permutation  $\sigma \in \mathcal{S}_r$  einen Endomorphismus seiner  $r$ -ten Tensorpotenz  $[\sigma] : V^{\otimes r} \xrightarrow{\sim} V^{\otimes r}$  durch das „Permutieren der Tensorfaktoren“, in Formeln  $[\sigma] : v_1 \otimes \dots \otimes v_r \mapsto v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(r)}$ . Wir schreiben diese Operation auch  $[\sigma] : t \mapsto t^\sigma$ . Diese Endomorphismen liefern eine Rechtsoperation, in Formeln  $t^{\sigma\tau} = (t^\sigma)^\tau$ . Um das einzusehen, können wir etwa das kommutative Diagramm

$$\begin{array}{ccc} \text{Ens}(\{1, \dots, n\}, V) & \xrightarrow{\sim} & V^n \longrightarrow V^{\otimes n} \\ \downarrow \circ\sigma & & \downarrow [\sigma] \\ \text{Ens}(\{1, \dots, n\}, V) & \xrightarrow{\sim} & V^n \longrightarrow V^{\otimes n} \end{array}$$

betrachten. Unter **alternierenden Tensoren** versteht man diejenigen Elemente von  $V^{\otimes r}$ , die beim Vertauschen von zwei Tensorfaktoren ihr Vorzeichen wechseln, in Formeln die Elemente des Teilraums

$$(V^{\otimes r})^{\text{sgn}} := \{t \in V^{\otimes r} \mid t^\sigma = (\text{sgn } \sigma)t \quad \forall \sigma \in \mathcal{S}_r\}$$

Nehmen wir nun zusätzlich an, daß unser Grundkörper Charakteristik Null oder eine Charakteristik größer als  $r$  hat, so können wir den sogenannten **Alternator**  $\text{alt} : V^{\otimes r} \rightarrow (V^{\otimes r})^{\text{sgn}}$  erklären durch die Abbildungsvorschrift

$$t \mapsto \frac{1}{r!} \sum_{\sigma \in \mathcal{S}_r} \text{sgn}(\sigma) t^\sigma$$

Wir haben  $\text{alt}(t) = t$  für jeden alternierenden Tensor  $t$ , für die Inklusion des Teilraums der alternierenden Tensoren  $\text{inkl} : (V^{\otimes r})^{\text{sgn}} \hookrightarrow V^{\otimes r}$  gilt also  $\text{alt} \circ \text{inkl} = \text{id}$ , insbesondere ist unser Alternator  $\text{alt}$  surjektiv. Bezeichne  $\text{proj} : V^{\otimes r} \rightarrow \bigwedge^r V$  die kanonische Projektion. Sicher verschwindet  $\text{alt}$  auf  $J_r = \ker(\text{proj})$ , folglich faktorisiert  $\text{alt}$  über eine wohlbestimmte Abbildung  $\bigwedge^r V \rightarrow (V^{\otimes r})^{\text{sgn}}$ . Andererseits faktorisiert auch die kanonische Projektion  $\text{proj} : V^{\otimes r} \rightarrow \bigwedge^r V$  über  $\text{alt}$  als  $\text{proj} = \text{proj} \circ \text{inkl} \circ \text{alt}$ . Zusammen folgt  $\ker(\text{alt}) = \ker(\text{proj})$ . Damit muß  $\text{proj} \circ \text{inkl}$  surjektiv und injektiv sein und ist folglich in der Tat ein Isomorpismus

$$(V^{\otimes r})^{\text{sgn}} \xrightarrow{\sim} \bigwedge^r V$$

**4.6.5.13 (Zugang zu äußeren Potenzen über alternierende Tensoren).** Manche Autoren machen es sich im Fall eines Grundkörpers der Charakteristik Null bei der Definition der äußeren Algebra eines Vektorraums  $V$  bequem, setzen schlicht  $\bigwedge^r V := (V^{\otimes r})^{\text{sgn}}$  und erklären das Dachprodukt entsprechend durch die Formel  $\omega \wedge \eta := \text{alt}(\omega \otimes \eta)$ . Das hat allerdings über die Einschränkungen an die Charakteristik hinaus den Nachteil, daß die Assoziativität des äußeren Produkts,

die wir sozusagen gratis erhalten haben, nun durch wenig transparente Rechnungen nachgewiesen werden muß. In der Physik werden Ausdrücke der Gestalt  $\text{alt}(v_1 \otimes \dots \otimes v_n)$  auch **Slater-Determinanten** genannt, da der Alternator an die Leibniz-Formel für Determinanten erinnert.

*Ergänzung 4.6.5.14 (Beziehung zum Dachprodukt der Analysis).* Man beachte, daß sich im Fall eines endlichdimensionalen Vektorraums  $V$  unser Isomorphismus  $(\Lambda^r V)^\top \xrightarrow{\sim} \text{Alt}^r(V)$  aus 4.6.5.3 mithilfe unserer Proposition 4.6.5.6 zu einem Isomorphismus  $\Lambda^r(V^\top) \xrightarrow{\sim} \text{Alt}^r(V)$  verlängern läßt. Mit den durch diese Isomorphismen gegebenen Vertikalen und dem Dachprodukt in der oberen Horizontalen und dem Dachprodukt, wie wir es im Rahmen des Stokes'schen Satzes in ?? direkt einführen, in der unteren Horizontalen kommutiert dann das Diagramm

$$\begin{array}{ccc} \Lambda^r V^\top \times \Lambda^s V^\top & \longrightarrow & \Lambda^{r+s} V^\top \\ \downarrow \wr & & \downarrow \wr \\ \text{Alt}^r(V) \times \text{Alt}^s(V) & \longrightarrow & \text{Alt}^{r+s}(V) \end{array}$$

Die hier gegebene Konstruktion des Dachprodukts benötigt zwar den größeren begrifflichen Aufwand, scheint mir aber durchsichtiger als die im Rahmen des Beweises von ?? gegebene direkte Konstruktion. Die dort gegebene direkte Konstruktion funktioniert erfreulicherweise ohne alle Einschränkungen an die Charakteristik, liefert aber nur für die Graßmann-Algebra des Dualraums eines endlichdimensionalen Vektorraums eine direkte Beschreibung.

*Vorschau 4.6.5.15.* Vom höheren Standpunkt aus mag man  $\Lambda V$  mit Dachprodukt und Shuffle-Koprodukt als ein Biabmonoid der Schmelzkategorie  $\text{gsMod}_k$  verstehen und  $\text{Alt } V = \bigoplus \text{Alt}^n V$  als das duale Objekt mit seiner Algebrenstruktur und der Isomorphismus  $\Lambda(V^\top) \xrightarrow{\sim} \text{Alt } V$  im endlichdimensionalen Fall ist das eigentlich besondere. Mehr dazu wird in ?? erklärt.

**4.6.5.16 (Maximale äußere Potenz und Determinante).** Jede lineare Abbildung  $f : V \rightarrow W$  induziert mittels der universellen Eigenschaft lineare Abbildungen  $\Lambda^r f : \Lambda^r V \rightarrow \Lambda^r W$ . Natürlich gilt auch  $\Lambda^r(f \circ g) = (\Lambda^r f) \circ (\Lambda^r g)$  und  $\Lambda^r(\text{id}) = \text{id}$ . Ist speziell  $f : V \rightarrow V$  ein Endomorphismus eines endlichdimensionalen Vektorraums, so ist  $\Lambda^{\max} f : \Lambda^{\max} V \rightarrow \Lambda^{\max} V$  ein Endomorphismus eines eindimensionalen Vektorraums alias ein Skalar. Wir zeigen nun, daß dieser Skalar genau die Determinante von  $f$  ist, in Formeln

$$\Lambda^{\max} f = \det f$$

Ist etwas allgemeiner  $f : V \rightarrow W$  eine lineare Abbildung zwischen Vektorräumen derselben endlichen Dimension  $n$  und sind  $\mathcal{A} = (v_1, \dots, v_n)$  sowie  $\mathcal{B} = (w_1, \dots, w_n)$  angeordnete Basen, so gilt

$$(\Lambda^n f)(v_1 \wedge \dots \wedge v_n) = \det(\mathcal{B}[f]_{\mathcal{A}}) w_1 \wedge \dots \wedge w_n$$

In der Tat folgt aus  $f(v_i) = \sum a_{ji}w_j$  mit kurzer Rechnung

$$\begin{aligned}
(\bigwedge f)(v_1 \wedge \dots \wedge v_n) &= f(v_1) \wedge \dots \wedge f(v_n) \\
&= (\sum a_{j1}w_j) \wedge \dots \wedge (\sum a_{ln}w_l) \\
&= \sum_{\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}} a_{\sigma(1)1}w_{\sigma(1)} \wedge \dots \wedge a_{\sigma(n)n}w_{\sigma(n)} \\
&= \sum_{\sigma \in S_n} \text{sgn}(\sigma)a_{\sigma(1)1} \dots a_{\sigma(n)n}w_1 \wedge \dots \wedge w_n \\
&= (\det(a_{ji}))w_1 \wedge \dots \wedge w_n
\end{aligned}$$

Die Multiplikationsregel für Determinanten folgt mit diesen Erkenntnissen unmittelbar aus der Relation  $\bigwedge^{\max}(f \circ g) = (\bigwedge^{\max} f) \circ (\bigwedge^{\max} g)$ . Daß die Determinante eines Endomorphismus  $f : V \rightarrow V$  verschwindet, falls dieser nicht vollen Rang hat, kann man in diesem Formalismus auch wie folgt einsehen: Man schreibt  $f$  als Verknüpfung  $V \rightarrow \text{im } f \hookrightarrow V$ , und unter der Annahme  $d = \dim V > \dim(\text{im } f)$  folgt  $\bigwedge^d(\text{im } f) = 0$ , womit dann auch die Komposition  $\bigwedge^d V \rightarrow \bigwedge^d(\text{im } f) \rightarrow \bigwedge^d V$  die Nullabbildung sein muß.

*Ergänzung 4.6.5.17.* Für einen  $K$ -Vektorraum  $V$  endlicher Dimension  $\dim V = n$  liefert das Dachprodukt nichtausgeartete Paarungen  $\bigwedge^d V \times \bigwedge^{n-d} V \rightarrow \bigwedge^n V$  im Sinne von 4.2.3.35, denn wir haben  $v_I \wedge v_J = \pm v_1 \wedge \dots \wedge v_n$ , falls  $I$  das Komplement von  $J$  ist, und Null sonst. Jeder Isomorphismus  $\omega : \bigwedge^n V \xrightarrow{\sim} K$  liefert also insbesondere einen Isomorphismus  $\hat{\omega} : \bigwedge^{n-1} V \cong V^\top$  gegeben durch  $(\hat{\omega}(\eta))(v) = \omega(\eta \wedge v)$ .

*Ergänzung 4.6.5.18 (Äußere Potenzen und Orientierung).* Gegeben ein endlichdimensionaler Vektorraum  $V$  über einem angeordneten Körper erhalten wir eine Bijektion

$$\text{or}(V) \xrightarrow{\sim} \text{or}(\bigwedge^{\max} V)$$

durch die Vorschrift  $\varepsilon \mapsto \varepsilon^\wedge$  mit  $\varepsilon^\wedge(v_1 \wedge \dots \wedge v_n) = \varepsilon(v_1, \dots, v_n)$  für eine und jede angeordnete Basis von  $V$ . Es verhält sich nun so, daß es im Rückblick eigentlich richtiger gewesen wäre, diese Bijektion zu einer Definition des Orientierungsgriffs zu machen. Das wäre nur aus didaktischen Gründen problematisch gewesen. Dafür müssen wir nun den Preis zahlen, daß verschiedene Veträglichkeiten zwischen leicht unkanonischen Wahlen zu prüfen sind, als da wären:

1. Ist  $U \hookrightarrow V \twoheadrightarrow W$  eine kurze exakte Sequenz endlichdimensionaler  $k$ -Vektorräume und sind  $\varepsilon, \eta$  Orientierungen auf  $U$  und  $W$  mit Elementen  $\hat{\varepsilon}, \hat{\eta}$  der zugehörigen offenen Halbgeraden in den jeweiligen äußeren Potenzen, so entspricht die zusammengesetzte Orientierung  $\varepsilon\eta$  auf  $V$  aus 3.6.5.17 der offenen Halbgerade vom Bild von  $\hat{\varepsilon} \otimes \hat{\eta}$  unter dem kanonischen Isomorphismus  $\bigwedge^{\max} U \otimes \bigwedge^{\max} W \xrightarrow{\sim} \bigwedge^{\max} V$  aus 4.6.5.26;

2. Ist  $V$  ein endlichdimensionaler  $k$ -Vektorraum und  $\varepsilon$  eine Orientierung auf  $V$  und  $\hat{\varepsilon}$  ein Element der zugehörigen offenen Halbgeraden in  $\bigwedge^{\max}(V)$  und  $\eta$  die zu  $\varepsilon$  duale Orientierung auf dem Dualraum  $V^\top$  nach 3.6.5.14 und  $\hat{\eta}$  ein Element der zugehörigen offenen Halbgeraden in  $\bigwedge^{\max}(V^\top)$ , so ist unter unserer ausgezeichneten Paarung  $\bigwedge^{\max}(V^\top) \times \bigwedge^{\max} V \rightarrow k$  aus 4.6.5.6 das Bild von  $(\hat{\eta}, \hat{\varepsilon})$  positiv.

**4.6.5.19 (Kanonische Form maximalen Grades).** Gegeben ein orientierter  $n$ -dimensionaler reeller Vektorraum  $V$  mit einer nichtausgearteten symmetrischen Bilinearform  $t$  kann man im eindimensionalen Raum  $\bigwedge^n V$  ein von Null verschiedenes Element  $\omega = \omega_t$  auszeichnen durch die Bedingung, daß gilt

$$\omega = \varepsilon v_1 \wedge \dots \wedge v_n$$

für jede angeordnete Basis  $v_1, \dots, v_n$  der Orientierung  $\varepsilon$  mit  $|t(v_i, v_j)| = \delta_{ij}$ . In der Tat erfüllt die Basiswechselmatrix  $A$  zwischen zwei derartigen Basen eine Gleichung der Gestalt  $A^\top JA = J'$  mit  $\det J = \det J' \neq 0$  im allgemeinen, so daß der Multiplikationssatz für Determinanten  $\det A = \pm 1$  liefert. Das Vorzeichen ergibt sich dann aus den jeweiligen Orientierungen.

**4.6.5.20.** Ist  $V$  ein  $n$ -dimensionaler pseudoeuklidischer Vektorraum mit Längengerade  $\mathbb{L}$  im Sinne von 4.2.7.6, so können wir ähnlich ein kanonisches Element

$$\omega \in \text{or}_{\mathbb{R}}(V) \otimes \bigwedge^n(V) \otimes \mathbb{L}^{\otimes(-n)}$$

erklären durch  $\omega = \varepsilon \otimes (v_1 \wedge \dots \wedge v_n) \otimes \|v_1\|^{-1} \otimes \dots \otimes \|v_n\|^{-1}$  für eine und jede angeordnete Basis  $v_1, \dots, v_n$  aus paarweise orthogonalen Vektoren mit  $\varepsilon$  der durch besagte Basis gegebenen Orientierung.

## Übungen

*Übung 4.6.5.21 (Partielles Einsetzen in alternierende Formen).* Gegeben ein Vektorraum  $V$  und eine Linearform  $\lambda \in V^\top$  zeige man, daß es für alle  $n \geq 0$  genau eine lineare Abbildung

$$i_\lambda : \bigwedge^{n+1} V \rightarrow \bigwedge^n V$$

gibt mit  $i_\lambda(v_0 \wedge \dots \wedge v_n) = \sum (-1)^\nu \lambda(v_\nu) v_0 \wedge \dots \wedge \hat{v}_\nu \wedge \dots \wedge v_n$ . Um mit Beschränkungen der Indizes keinen Ärger zu kriegen, vereinbaren wir  $\bigwedge^n V = 0$  für  $n < 0$  und setzen  $i_\lambda$  in der einzigen möglichen Weise zu allen  $n \in \mathbb{Z}$  fort. Man zeige in dieser Situation  $i_\lambda^2 = 0$  und zeige für alle  $v \in V$  die Identität  $(v \wedge) \circ i_\lambda + i_\lambda \circ (v \wedge) = (\lambda(v) \cdot)$  von Endomorphismen der äußeren Algebra. Weiter setzen wir

auch  $\text{Alt}^n(V) = 0$  für  $n < 0$  und man zeige für  $v \in V$  die Kommutativität des Diagramms

$$\begin{array}{ccc} \bigwedge^{n+1} V^\top & \xrightarrow{i_{\text{ev}(v)}} & \bigwedge^n V^\top \\ \downarrow & & \downarrow \\ \text{Alt}^{n+1}(V) & \xrightarrow{i_v} & \text{Alt}^n(V) \end{array}$$

mit der durch  $(i_v \eta)(v_1, \dots, v_n) := \eta(v, v_1, \dots, v_n)$  gegebenen beziehungsweise  $i_v = 0$  für  $n < 0$  unteren Horizontale und den Vertikalen aus 4.6.5.9 und zeige  $i_v^2 = 0$  sowie die Identität  $(\lambda \wedge) \circ i_v + i_v \circ (\lambda \wedge) = (\lambda(v) \cdot)$  von Endomorphismen der Algebra der alternierenden Formen. Der Buchstabe  $i$  steht für englisch **insertion**. Auf Deutsch heißen diese Abbildungen **Einsetzungshomomorphismen**.

*Übung 4.6.5.22.* Gegeben ein Vektorraum  $V$  und  $\omega \in \bigwedge^r V$  und  $\eta \in \bigwedge^s V$  gilt  $\omega \wedge \eta = (-1)^{rs} \eta \wedge \omega$ .

*Ergänzende Übung 4.6.5.23.* (Hinweis: 4.6.5.16). Gegeben eine  $(n \times m)$ -Matrix  $A$  und eine  $(m \times n)$ -Matrix  $B$  kann man die Determinante der  $(n \times n)$ -Matrix  $AB$  bestimmen wie folgt: Für jede  $n$ -elementige Teilmenge  $I \subset \{1, \dots, m\}$  mit Elementen  $i_1 < \dots < i_n$  möge  $A_I$  gerade aus den Spalten von  $A$  der Indizes  $i_1, \dots, i_n$  bestehen und  $B^I$  aus den Zeilen von  $B$  der Indizes  $i_1, \dots, i_n$ . So gilt die **Cauchy-Binet-Formel**

$$\det(AB) = \sum_{|I|=n} (\det A_I)(\det B^I)$$

*Übung 4.6.5.24.* Gegeben ein Endomorphismus  $f \in \text{End } V$  eines Vektorraums mit  $f^{\otimes r} = \text{id} : V^{\otimes r} \rightarrow V^{\otimes r}$  für ein  $r \geq 1$  gilt  $f = \zeta \text{id}$  mit  $\zeta^r = 1$ . Hinweis: 4.6.1.34.

*Ergänzende Übung 4.6.5.25.* Sei  $V$  ein Vektorraum. Man zeige: Das Erzeugnis  $J_r \subset V^{\otimes r}$  aller Tensoren mit zwei gleichen Einträgen fällt zusammen mit dem Erzeugnis  $J'_r \subset V^{\otimes r}$  aller Tensoren mit zwei benachbarten gleichen Einträgen.

*Weiterführende Übung 4.6.5.26.* Ist  $U \hookrightarrow V \twoheadrightarrow W$  eine kurze exakte Sequenz endlichdimensionaler Vektorräume, so induziert mit der Notation  $d = \dim W$  das Dachprodukt  $\bigwedge^{\max} U \otimes \bigwedge^d V \rightarrow \bigwedge^{\max} V$  einen Isomorphismus

$$\bigwedge^{\max} U \otimes \bigwedge^{\max} W \xrightarrow{\sim} \bigwedge^{\max} V$$

Wir nennen ihn den **kanonischen Isomorphismus**, aber man bemerke, daß an dieser Stelle auch andere sinnvolle Wahlen von Vorzeichen möglich wären. Auf eine solche Wahl muß man sich aber halt mal einigen und die hier getroffene Wahl ist verträglich mit unserem Begriff 3.6.5.17 der „zusammengesetzten Orientierung“.

*Ergänzende Übung 4.6.5.27.* Sei  $L \hookrightarrow V \twoheadrightarrow W$  eine kurze exakte Sequenz von Vektorräumen mit  $\dim L = 1$ . So faktorisiert für alle  $m \geq 1$  das Dachprodukt  $L \otimes \bigwedge^{m-1} V \rightarrow \bigwedge^m V$  über  $L \otimes \bigwedge^{m-1} W$  und wir erhalten so eine kurze exakte Sequenz

$$L \otimes \bigwedge^{m-1} W \hookrightarrow \bigwedge^m V \twoheadrightarrow \bigwedge^m W$$

Hinweis: Man mag mit vollständiger Induktion über  $m$  argumentieren.

*Ergänzende Übung 4.6.5.28.* Gegeben ein endlichdimensionaler symplektischer Vektorraum  $(V, \omega)$  der Dimension  $2n$  zeige man für die in 4.2.5.7 erklärte  $(2n)$ -Multilinearform  $\omega^{(n)}$  auf  $V$  die Identität

$$n! \omega^{(n)} = \omega^{\wedge n}$$

*Ergänzende Übung 4.6.5.29 (Kreuzprodukt als Dachprodukt).* Gegeben ein dreidimensionaler euklidischer Vektorraum  $V$  mit Längengerade  $\mathbb{L}$  nach 4.1.5.12 und Orientierungsgerade  $\text{or}_{\mathbb{R}}(V)$  betrachte man die Komposition von Isomorphismen

$$\bigwedge^2 V \xrightarrow{\sim} \text{Hom}(V, \bigwedge^3 V) \xrightarrow{\sim} V^\top \otimes \mathbb{L}^{\otimes 3} \otimes \text{or}_{\mathbb{R}}(V) \xrightarrow{\sim} \mathbb{L} \otimes \text{or}_{\mathbb{R}}(V) \otimes V$$

Hier werde die erste Abbildung durch  $\eta \mapsto \eta \wedge$  gegeben, die zweite durch das Spatprodukt 4.6.4.3 zusammen mit der Darstellung 4.6.1.21 von Homomorphismenräumen als Tensorprodukt und die dritte vom Isomorphismus  $V^\top \xrightarrow{\sim} V \otimes \mathbb{L}^{\otimes(-2)}$  aus 4.6.4.11. Man zeige, daß die Verknüpfung der Abbildung  $V \times V \rightarrow \bigwedge^2 V$ ,  $(v, w) \mapsto v \wedge w$  mit obiger Identifikation gerade unser Kreuzprodukt aus 4.6.4.9 ist.

*Übung 4.6.5.30.* Sei  $f : V \rightarrow V$  ein Endomorphismus eines endlichdimensionalen komplexen Vektorraums. Man zeige für den  $k$ -ten Koeffizienten  $a_k$  des charakteristischen Polynoms die Formel

$$a_k = (-1)^k \text{tr} \left( \bigwedge^k f \mid \bigwedge^k V \right)$$

Hinweis: Man ziehe ich auf den Fall einer oberen Dreiecksmatrix zurück. Die Formel gilt auch für beliebige Körper, da mag man sich mit einer Einbettung in einen algebraisch abgeschlossenen Körper behelfen, die nach ?? stets existiert.

## 4.7 Kategorien und Funktoren\*

Viele Konstruktionen der linearen und insbesondere der multilinear Algebra, wie etwa Dualräume, Tensorpotenzen oder äußere Potenzen, zeigen erst in der Sprache der Kategorientheorie ihre wahre Natur. Es geht bei diesen Konstruktionen nämlich keineswegs darum, irgendwelche neuen Vektorräume zu konstruieren: Wir wissen ja bereits aus 3.2.1.10, daß wir hier zumindest im Fall endlicher Dimension nichts wesentlich Neues finden können. Vielmehr geht es darum, zusammen mit diesen neuen Vektorräumen auch neue lineare Abbildungen zu konstruieren, wie etwa bei Dualräumen die transponierten Abbildungen. Erst zusammen mit diesen zusätzlichen Konstruktionen erhält man nützliche und anwendbare Begriffsbildungen.

Die Sprache der Kategorien und Funktoren liefert für derartige Konstruktionen einen begrifflichen Rahmen. Sie ist ähnlich ausdrucksstark, grundlegend und elegant wie die Sprache der Mengenlehre, auf der sie aufbaut, und gehört meines Erachtens in den Rucksack jeder Mathematikerin und jedes Mathematikers. Ich bin sogar der Ansicht, daß die „naive Mengenlehre“ aus den Grundvorlesungen am besten durch eine axiomatische Beschreibung der „Kategorie aller Mengen“ wie etwa in [LR03] formalisiert wird. So formal will ich bei der hier gegebenen Darstellung jedoch nicht werden und arbeite deshalb weiter auf der Grundlage der naiven Mengenlehre. Eine ausführlichere Behandlung der Kategorientheorie findet man zum Beispiel in [Mac98].

### 4.7.1 Kategorien

**Definition 4.7.1.1.** Eine **Kategorie**  $\mathcal{C}$  ist ein Datum bestehend aus

- einer Menge  $\text{Ob } \mathcal{C}$  von **Objekten**;
- einer Menge  $\mathcal{C}(X, Y)$  von **Morphismen** für je zwei Objekte  $X, Y \in \text{Ob } \mathcal{C}$ ;
- einer Abbildung  $\mathcal{C}(X, Y) \times \mathcal{C}(Y, Z) \rightarrow \mathcal{C}(X, Z)$ ,  $(f, g) \mapsto g \circ f$  für je drei Objekte  $X, Y, Z \in \mathcal{C}$ , genannt die **Verknüpfung** von Morphismen,

derart, daß folgende Axiome erfüllt sind:

- Die Verknüpfung ist **assoziativ**, es gilt also  $(f \circ g) \circ h = f \circ (g \circ h)$  für Morphismen  $f, g$  und  $h$ , wann immer diese Verknüpfungen sinnvoll sind;
- Für jedes Objekt  $X \in \text{Ob } \mathcal{C}$  gibt es einen Morphismus  $\text{id}_X \in \mathcal{C}(X, X)$ , die **Identität auf**  $X$ , so daß gilt  $\text{id}_X \circ f = f$  und  $g \circ \text{id}_X = g$  für Morphismen  $f$  und  $g$  wann immer diese Verknüpfungen sinnvoll sind. Die üblichen Argumente zeigen, daß es für jedes  $X$  höchstens einen derartigen Morphismus

geben kann, womit auch die Verwendung des bestimmten Artikels gerechtfertigt wäre.

4.7.1.2. Seien  $\mathcal{C}$  eine Kategorie und  $X, Y \in \text{Ob } \mathcal{C}$  Objekte. Statt  $f \in \mathcal{C}(X, Y)$  sagen wir auch,  $f$  sei ein **Morphismus von  $X$  nach  $Y$**  und schreiben kurz

$$f : X \rightarrow Y$$

Statt  $\text{id}_X$  schreiben wir oft nur  $\text{id}$ . Statt  $X \in \text{Ob } \mathcal{C}$  schreiben wir oft kürzer  $X \in \mathcal{C}$ .

4.7.1.3. Wir fordern nicht, daß die Morphismenmengen  $\mathcal{C}(X, Y)$  einer Kategorie  $\mathcal{C}$  paarweise disjunkt sein sollen. Wir erklären dahingegen die Menge aller Morphismen von  $\mathcal{C}$  als die disjunkte Vereinigung

$$\text{Mor}(\mathcal{C}) := \bigsqcup_{X, Y \in \mathcal{C}} \mathcal{C}(X, Y)$$

*Beispiel 4.7.1.4 (Kategorie der Mengen).* Als erstes Beispiel hätte ich gerne die Kategorie  $\mathcal{C} := \text{Ens}$  aller Mengen eingeführt. Das ist jedoch nicht möglich, da die „Gesamtheit aller Mengen“, wie in 2.1.3.9 ausgeführt wird, nicht als Menge angesehen werden darf. Um diese Untiefen der Logik zu umschiffen, betrachten wir feiner ein Mengensystem  $\mathfrak{U}$  alias eine Menge  $\mathfrak{U}$  von Mengen und erklären die Kategorie  $\mathfrak{U}\text{Ens}$  aller Mengen  $X \in \mathfrak{U}$ . Ihre Objekte sind beliebige Mengen  $X \in \mathfrak{U}$ , in Formeln

$$\text{Ob}(\mathfrak{U}\text{Ens}) := \mathfrak{U}$$

Für je zwei Objekte alias je zwei Mengen  $X, Y \in \mathfrak{U}$  erklären wir die Morphismenmenge als die Menge aller Abbildungen von  $X$  nach  $Y$ , in Formeln

$$\mathfrak{U}\text{Ens}(X, Y) := \text{Ens}(X, Y)$$

Die Verknüpfung ordnet jedem Paar  $(f, g)$  von Abbildungen ihre Komposition  $g \circ f$  zu. Daß diese Daten unsere Axiome erfüllen, scheint mir offensichtlich. Unser  $\text{id}_X \in \mathfrak{U}\text{Ens}(X, X)$  ist die identische Abbildung  $\text{id}_X(x) = x \forall x \in X$ .

*Vorschau 4.7.1.5 (Mengen, Klassen, Universen).* In vielen Quellen umschifft man die in 4.7.1.4 angesprochenen Untiefen der Logik, indem man nicht fordert, daß die Objekte einer Kategorie eine Menge bilden, sondern stattdessen, daß sie eine „Klasse“ bilden sollen. Das hat den Vorteil, daß man die Kategorie aller Mengen bilden kann. Es hat den Nachteil, daß man den Begriff einer Klasse einführen muß und erklären muß, wie man damit umgeht. Statt mit „Klassen“ werden wir zu gegebener Zeit mit „Universen“ arbeiten, die in 4.7.11.3 eingeführt werden. Für unsere Bedürfnisse läuft das auf dasselbe hinaus und erspart uns die Vertreibung aus dem Paradies der Mengenlehre. Ich werde aber oft kategorientheoretische Sprache auch in einem weiteren Sinn als „Metasprache“ verwenden und dabei derartige Feinheiten kurzerhand ignorieren.

| Kategorie                | Morphismen  | Kürzel                 |
|--------------------------|---|------------------------|
| {Mengen}                 | alle Abbildungen                                    | Ens                    |
| {teilgeordnete Mengen}   | monoton wachsende                                   | Ord                    |
|                          | Abbildungen   |                        |
| {Monoide}                | Morphismen von Monoiden                             | Mon                    |
| {Gruppen}                | Gruppenhomomorphismen                               | Grp                    |
| {abelsche Gruppen}       | Gruppenhomomorphismen                               | Ab                     |
| {topologische Räume}     | stetige Abbildungen                                 | Top                    |
| {bepunktete Mengen}      | Abbildungen,<br>die den Basispunkt erhalten         | Ens*                   |
| {bepunktete Räume}       | stetige Abbildungen,<br>die den Basispunkt erhalten | Top*                   |
| { $K$ -Vektorräume}      | $K$ -lineare Abbildungen                            | $K$ -Mod, Mod $_K$     |
| {Affine Räume über $K$ } | affine Abbildungen                                  | $K$ -Aff, Aff $_K$     |
| {nicht unitäre Ringe}    | Rng-Homomorphismen                                  | Rng                    |
| {Ringe}                  | Ringhomomorphismen                                  | Ring                   |
| {kommutative Ringe}      | Ringhomomorphismen                                  | Kring                  |
| { $K$ -Algebren}         | $K$ -Algebren-Homomorphismen                        | $K$ -Alg, Alg $_K$     |
| { $K$ -Ringalgebren}     | $K$ -Ringalgebren-Homomorphismen                    | $K$ -Ralg, Ralg $_K$   |
| { $K$ -Kringalgebren}    | $K$ -Kringalgebren-Homomorphismen                   | $K$ -Kralg, Kralg $_K$ |

Hier einige Beispiele von Kategorien. Als Verknüpfung von Morphismen ist für die Kategorien dieser Liste stets die Komposition von Abbildungen gemeint. Um logische Abstürze zu vermeiden, müssen wir uns genauer stets ein Mengensystem  $\mathfrak{U}$  dazudenken, aus dem die zugrundeliegende Menge der jeweiligen Struktur kommen muß und das wir in der Notation meist unterschlagen. Wenn wir es doch notieren wollen, schreiben wir

$$\mathfrak{U}\text{Mod}_K$$

und dergleichen. Wir denken uns das Mengensystem  $\mathfrak{U}$  meist als ziemlich riesig und fordern zumindest implizit für gewöhnlich, daß es unter dem Bilden von Teilmengen stabil sein möge und die reellen Zahlen enthält. Etwas genauer werden wir zu gegebener Zeit oft fordern, daß es ein „Universum“ sein soll.

*Beispiel 4.7.1.6.* Zu jedem Monoid  $M$  können wir die Kategorie  $[M]$  mit einem einzigen Objekt  $*$  bilden, deren Morphismen die Elemente von besagtem Monoid sind mit der Verknüpfung in unserem Monoid als Verknüpfung von Morphismen. Wir nennen sie die **Ein-Objekt-Kategorie** unseres Monoids. Umgekehrt ist für jedes Objekt  $X$  einer Kategorie  $\mathcal{C}$  die Menge  $\mathcal{C}(X, X)$  mit der von der Kategorienstruktur herkommenden Verknüpfung ein Monoid. In diesem Sinne ist also eine Kategorie mit einem einzigen Objekt nichts anderes als ein Monoid. Das Monoid der Morphismen von einem Objekt  $X$  zu sich selber in einer Kategorie  $\mathcal{C}$  nennen wir das Monoid der **Endomorphismen** von  $X$  und kürzen es in Zukunft oft ab mit

$$\mathcal{C}(X) := \mathcal{C}(X, X)$$

*Beispiel 4.7.1.7.* Sei  $K$  ein Körper oder allgemeiner ein Ring. Wir erklären die **Matrixkategorie**  $\text{Mat} = \text{Mat}_K = \text{Mat}(K)$  über  $K$  durch die Vorschriften

$$\text{Ob}(\text{Mat}_K) := \mathbb{N} \quad \text{und} \quad \text{Mat}_K(m, n) := \text{Mat}(n \times m; K)$$

mit der Matrixmultiplikation als Verknüpfung von Morphismen. Die Axiome sind erfüllt aufgrund unserer Rechenregeln 3.2.4.6 für die Matrixmultiplikation.

*Beispiel 4.7.1.8 (Teilgeordnete Menge als Kategorie).* Jede teilgeordnete Menge  $(A, \leq)$  kann als Kategorie aufgefaßt werden wie folgt: Objekte sind die Elemente von  $A$ ; Morphismen gibt es jeweils einen von einem Element zu jedem kleineren und zu sich selber; und die Verknüpfung von Morphismen ist die einzige Mögliche.

*Beispiel 4.7.1.9 (Kategorie der Vektorräume).* Als nächstes Beispiel hätte ich gerne die Kategorie  $\mathcal{C} = \text{Mod}_K$  aller Vektorräume über einem Körper  $K$  eingeführt. Die Notation  $\text{Mod}_K$  für Vektorräume über  $K$  steht dabei für ihre alternative Bezeichnung als  **$K$ -Moduln**. Wieder gerät man dabei in Untiefen der Logik. Um diese zu umschiffen betrachten wir wieder ein Mengensystem  $\mathfrak{U}$  und erklären dazu eine Kategorie

$$\mathfrak{U}\text{Mod}_K$$

Als Objekte dieser Kategorie nehmen wir alle  $K$ -Vektorräume, deren Grundmenge zu unserem Mengensystem  $\mathfrak{U}$  gehört. Für je zwei Vektorräume  $V, W \in \mathfrak{U}\text{Mod}_K$  erklären wir die Morphismenmenge als die Menge aller linearen Abbildungen, in Formeln

$$\mathfrak{U}\text{Mod}_K(V, W) := \text{Hom}_K(V, W)$$

Die Verknüpfung ordnet wieder jedem Paar  $(f, g)$  von Abbildungen ihre Komposition  $g \circ f$  zu. Die Axiome sind offensichtlich erfüllt.

*4.7.1.10 (Verwendung des Symbols Hom).* Das Symbol „Hom“ für Mengen von Morphismen versuche ich nach Möglichkeit zu vermeiden: Ich will es reservieren

für die sogenannten „internen Hom-Räume“. Darunter versteht man Vorschriften, die in sehr speziellen Situationen zwei Objekten einer Kategorie ein Drittes zuordnen, im Fall der Vektorräume etwa die Morphismenmenge mit ihrer natürlichen Vektorraumstruktur. Wenn die Morphismenmenge als Menge gemeint ist, sollte ich  $\text{Mod}_K(V, W)$  schreiben, aber das halte ich im Fall der Vektorräume nicht durch. Das Kürzel „ $\text{Mod}$ “ mit etwelchen oberen und unteren Indizes wird stets für Kategorien von abelschen Gruppen mit Zusatzstrukturen stehen, meist Operationen von Ringen oder Gruppen. Gehen diese Zusatzstrukturen aus dem Kontext hervor, so lasse ich die entsprechenden Indizes auch manchmal weg. Für abelsche Gruppen ohne Zusatzstrukturen benutze ich stets das Kürzel „ $\text{Ab}$ “.

- Definition 4.7.1.11.**
1. Ein Morphismus  $f \in \mathcal{C}(X, Y)$  in einer Kategorie heißt ein **Isomorphismus** oder **Iso** und als Adjektiv **iso**, wenn es einen Morphismus  $g \in \mathcal{C}(Y, X)$  gibt mit  $f \circ g = \text{id}_Y$  und  $g \circ f = \text{id}_X$ . Wir notieren Isomorphismen oft  $f : X \xrightarrow{\sim} Y$ ;
  2. Zwei Objekte  $X$  und  $Y$  einer Kategorie heißen **isomorph**, wenn es einen Iso  $f : X \xrightarrow{\sim} Y$  gibt. Man schreibt dann auch kurz  $X \cong Y$ .

*Beispiele 4.7.1.12.* Isomorphismen in der Kategorie der Mengen nennt man Bijektionen, Isomorphismen in der Kategorie der topologischen Räume Homöomorphismen, Isomorphismen in der Kategorie der Vektorräume Vektorraumisomorphismen.

4.7.1.13. Eine Kategorie, in der alle Morphismen Isomorphismen sind, heißt ein **Gruppoid**. Eine Kategorie, in denen es außer den Identitäten keine Morphismen gibt, heißt **diskret**. Natürlich ist jede diskrete Kategorie ein Gruppoid.

4.7.1.14 (**Diskussion des Begriffs eines Isomorphismus**). Bisher hatten wir verschiedentlich Isomorphismen abweichend erklärt als bijektive Homomorphismen, zum Beispiel bei Gruppen, Körpern, Vektorräumen und affinen Räumen. In allen diesen Fällen sollte es jedoch klar sein, daß die Umkehrabbildung im Sinne der Mengenlehre auch selbst wieder ein Homomorphismus ist, so daß wir in der Tat auch Isomorphismen im Sinne der Kategorientheorie vor uns haben. Ein typisches Beispiel für eine Kategorie von „Mengen mit Zusatzstrukturen“, in der bijektive Homomorphismen keine Isomorphismen zu sein brauchen, ist die Kategorie der teilgeordneten Mengen.

4.7.1.15. Viele mathematische Fragestellungen lassen sich in der Sprache der Kategorientheorie dahingehend formulieren, daß man einen Überblick über alle Objekte einer Kategorie gewinnen will, wobei man zwischen isomorphen Objekten nicht unterscheidet. Formal will man also für eine gegebene Kategorie  $\mathcal{C}$  die Menge aller Äquivalenzklassen von Objekten

$$\mathcal{C}/\cong$$

unter der Äquivalenzrelation der Isomorphie beschreiben. Man spricht dann auch von **Isomorphieklassen** von Objekten und nennt Fragestellungen dieser Art **Klassifikationsprobleme**. Zum Beispiel werden die endlich erzeugten Vektorräume über einem fest vorgegebenen Körper klassifiziert durch ihre Dimension, die endlich erzeugten abelschen Gruppen durch die Sätze 4.4.4.4 und 4.4.4.5, die endlichen Mengen durch ihre Kardinalität 2.1.1.8, und beliebige Mengen, vorsichtshalber aus einem fest vorgegebenen Mengensystem, ebenfalls durch ihre Kardinalität ??.

4.7.1.16. Unter einer **Unterkategorie** einer Kategorie versteht man ein Paar bestehend aus einer Teilmenge der Objektmenge nebst Teilmengen der Morphismenmengen für je zwei Objekte unserer Teilmenge der Objektmenge derart, daß die offensichtlichen Bedingungen erfüllt sind. Eine Unterkategorie heißt **voll**, wenn die fraglichen Teilmengen der Morphismenmengen jeweils aus allen Morphismen in der ursprünglichen Kategorie bestehen.

4.7.1.17. Zu jeder Kategorie  $\mathcal{C}$  erklären wir eine Unterkategorie, die **Isomorphismenkategorie**  $\mathcal{C}^\times$  von  $\mathcal{C}$ , durch die Vorschrift, daß sie dieselben Objekte haben soll, aber nur die Isomorphismen von  $\mathcal{C}$  als Morphismen. Die Menge aller Isomorphismen von einem Objekt  $X$  einer Kategorie  $\mathcal{C}$  in ein Objekt  $Y$  derselben Kategorie notieren wir folgerichtig  $\mathcal{C}^\times(X, Y)$ . Die Isomorphismen von einem Objekt  $X$  einer Kategorie  $\mathcal{C}$  auf sich selber heißen die **Automorphismen** von  $X$ . Sie bilden stets eine Gruppe, die **Automorphismengruppe**  $\mathcal{C}^\times(X)$  von  $X$ . Für die Automorphismengruppe  $\text{Mod}_k^\times(V)$  eines  $k$ -Vektorraums  $V$  hatten wir die Notation  $\text{GL}(V)$  vereinbart, für die Automorphismengruppe  $\text{Ens}^\times(X)$  einer Menge  $X$  die Bezeichnung als „Gruppe der Permutationen von  $X$ “.

**Definition 4.7.1.18.** Ein Objekt  $F$  einer Kategorie  $\mathcal{C}$  heißt **final**, wenn es für alle  $X \in \mathcal{C}$  genau einen Morphismus von  $X$  nach  $F$  gibt, in Formeln

$$|\mathcal{C}(X, F)| = 1 \quad \forall X \in \mathcal{C}$$

**Definition 4.7.1.19.** Ein Objekt  $K$  einer Kategorie  $\mathcal{C}$  heißt **initial** oder gleichbedeutend **kofinal**, wenn es für alle  $Y \in \mathcal{C}$  genau einen Morphismus von  $K$  nach  $Y$  gibt, in Formeln

$$|\mathcal{C}(K, Y)| = 1 \quad \forall Y \in \mathcal{C}$$

**Beispiele 4.7.1.20 (Finale und initiale Objekte in Kategorien von Mengen).** Ist  $\mathfrak{U}$  ein Mengensystem, das nicht nur aus der leeren Menge besteht, so sind die finalen Objekte von  $\mathfrak{U}\text{Ens}$  genau die einpunktigen Mengen aus  $\mathfrak{U}$ . Ist  $\mathfrak{U}$  ein Mengensystem, das nicht nur aus einelementigen Mengen besteht, so ist die leere Menge ist das einzige kofinale Objekt von  $\mathfrak{U}\text{Ens}$ , wenn sie denn zu unserem Mengensystem  $\mathfrak{U}$  dazugehört.

**4.7.1.21 (Weitere Notationen).** Zwischen je zwei finalen beziehungsweise kofinalen Objekten gibt es offensichtlich genau einen Isomorphismus. Wir erlauben uns deshalb, etwas lax von *dem* finalen beziehungsweise *dem* kofinalen Objekt zu reden, und bezeichnen „das“ finale Objekt mit  $\text{pt} = \text{pt}(\mathcal{C})$  für „Punkt“ oder  $\text{fin}(\mathcal{C})$  und Morphismen dahin mit  $\text{fin}$  für „final“. Meist verwenden wir als Bezeichnung des finalen Objekts die kleingeschriebene Bezeichnung der Kategorie, etwa  $\text{top}$  für den einelementigen topologischen Raum oder  $\text{ens}$  für die einelementige Menge. Morphismen vom finalen Objekt zu einem beliebigen Objekt notieren wir gerne em wie „embedding“ mit einem Index, der angibt, welcher Morphismus genau gemeint ist. Gegeben eine Menge  $X$  und ein Element  $x \in X$  meint etwa  $\text{em}_x : \text{ens} \rightarrow X$  die Einbettung der einelementigen Menge mit Bild  $x$ . Wir bezeichnen mit  $\text{ini} = \text{ini}(\mathcal{C})$  das initiale Objekt einer Kategorie  $\mathcal{C}$ , wenn es denn ein solches gibt.

## Übungen

*Übung 4.7.1.22.* Ein Morphismus  $f \in \mathcal{C}(X, Y)$  in einer Kategorie ist ein Isomorphismus genau dann, wenn er ein **Rechtsinverses** und ein **Linksinverses** besitzt, wenn es also Morphismen  $g, h \in \mathcal{C}(Y, X)$  gibt mit  $f \circ g = \text{id}_Y$  und  $h \circ f = \text{id}_X$ , und unter diesen Voraussetzungen gilt bereits  $g = h$ . Wir nennen diesen Morphismus dann den **inversen Morphismus zu**  $f$  und notieren ihn  $f^{-1}$ . Derartige Rechtsinverse bezeichnet man auch oft als **Schnitt** oder **Spaltung**. Allgemeiner nennt man jeden Morphismus **rechtsspaltend**, der ein Linksinverses besitzt, und jeden Morphismus **linksspaltend**, der ein Rechtsinverses besitzt

*Übung 4.7.1.23.* Kann ein Morphismus  $f \in \mathcal{C}(X, Y)$  in einer Kategorie sowohl durch Vorschalten eines Morphismus  $g \in \mathcal{C}(W, X)$  als auch durch Nachschalten eines Morphismus  $h \in \mathcal{C}(Y, Z)$  zu einem Isomorphismus gemacht werden, so muß er bereits selbst ein Isomorphismus gewesen sein.

*Übung 4.7.1.24.* Seien  $\mathcal{C}$  eine Kategorie und  $f : X \rightarrow Y$  ein Morphismus. Man zeige, daß  $f$  genau dann ein Isomorphismus ist, wenn das Vorschalten von  $f$  für jedes weitere Objekt  $Z$  eine Bijektion  $\mathcal{C}(Y, Z) \xrightarrow{\sim} \mathcal{C}(X, Z)$  induziert. Man zeige dual, daß  $f$  genau dann ein Isomorphismus ist, wenn das Nachschalten von  $f$  für jedes weitere Objekt  $Z$  eine Bijektion  $\mathcal{C}(Z, X) \xrightarrow{\sim} \mathcal{C}(Z, Y)$  induziert. Allgemeinere Aussagen in dieser Richtung macht das sogenannte Yoneda-Lemma 4.7.10.2.

*Übung 4.7.1.25.* Man finde finale und kofinale Objekte in den Kategorien der Gruppen, Ringe, topologischen Räume und Vektorräume aus einem vorgegebenen Mengensystem  $\mathfrak{U}$ .

### 4.7.2 Funktoren

**Definition 4.7.2.1.** Ein **Funktör**  $F : \mathcal{A} \rightarrow \mathcal{B}$  von einer Kategorie  $\mathcal{A}$  in eine Kategorie  $\mathcal{B}$  ist ein Datum bestehend aus

- a. einer Abbildung  $F = F_{\text{Ob}} : \text{Ob } \mathcal{A} \rightarrow \text{Ob } \mathcal{B}, X \mapsto FX$ ;
- b. einer Abbildung  $F = F_{X,Y} : \mathcal{A}(X, Y) \rightarrow \mathcal{B}(FX, FY), f \mapsto Ff$  für je zwei Objekte  $X, Y \in \text{Ob } \mathcal{A}$ ,

derart, daß gilt:

1.  $F(f \circ g) = (Ff) \circ (Fg)$  für beliebige verknüpfbare Morphismen  $f$  und  $g$  aus der Kategorie  $\mathcal{A}$ ;
2.  $F(\text{id}_X) = \text{id}_{FX}$  für jedes Objekt  $X \in \mathcal{A}$ .

Ich nenne in diesem Zusammenhang  $\mathcal{A}$  die **Ausgangskategorie** und  $\mathcal{B}$  die **Zielkategorie** des Funktors  $F$ .

*Beispiel 4.7.2.2.* Gegeben ein Körper  $K$  erhalten wir einen Funktor

$$\begin{array}{ccc} \text{Mat}_K & \rightarrow & \text{Mod}_K \\ n & \mapsto & K^n \\ A \downarrow & \mapsto & (A \circ) \downarrow \\ m & \mapsto & K^m \end{array}$$

von der Matrixkategorie 4.7.1.7 über  $K$  in die Kategorie der  $K$ -Vektorräume, indem wir wie angedeutet jedem Objekt  $n$  der Matrixkategorie den Vektorraum  $K^n$  zuordnen und jeder Matrix die durch diese Matrix gegebene lineare Abbildung. Wir nennen ihn den **Realisierungsfunktör**.

*Beispiel 4.7.2.3 (Der Richtungsraum als Funktor).* Wir erklären die Kategorie  $\text{Aff} = \text{Aff}_K$  der affinen Räume über einem gegebenen Körper  $K$ . Als Objekte nehmen wir unsere affinen Räume, als Morphismen affine Abbildungen. Das Bilden des Richtungsraums  $\text{Richt} : E \mapsto \vec{E}$  ist dann zusammen mit der Zuordnung, die jeder affinen Abbildung  $\varphi : E \rightarrow F$  ihren linearen Anteil  $\vec{\varphi} : \vec{E} \rightarrow \vec{F}$  zuordnet, ein Funktor

$$\text{Richt} : \text{Aff}_K \rightarrow \text{Mod}_K$$

*Beispiel 4.7.2.4 (Die Längengerade als Funktor).* Wir erklären die Kategorie  $\text{Euk}$  der euklidischen Vektorräume. Objekte sind wie in 4.1.5.1 reelle Vektorräume mit einer  $\mathbb{R}_{>0}$ -Bahn von Skalarprodukten, Morphismen die euklidischen Abbildungen nach 4.1.5.8. Unsere Konstruktion 4.1.5.12 der Längengerade eines euklidischen Raums und der zwischen Längengeraden induzierten Abbildungen ist dann ein Funktor

$$\mathbb{L} : \text{Euk} \rightarrow \text{Mod}_{\mathbb{R}}$$

4.7.2.5. Man gibt bei einem Funktor  $F$  meist nur die Abbildung  $X \mapsto FX$  auf den Objekten an in der Hoffnung, daß vom Leser erraten werden kann, welche Abbildung  $f \mapsto Ff$  auf den Morphismen gemeint ist.

4.7.2.6. Für jede Kategorie  $\mathcal{C}$  haben wir den **Identitätsfunktor**  $\text{Id} = \text{Id}_{\mathcal{C}}$  von besagter Kategorie zu sich selber. Sind  $F : \mathcal{A} \rightarrow \mathcal{B}$  und  $G : \mathcal{B} \rightarrow \mathcal{C}$  Funktoren, so ist auch  $G \circ F : \mathcal{A} \rightarrow \mathcal{C}$  ein Funktor.

**Lemma 4.7.2.7 (Funktoren erhalten Isomorphie).** *Ein Funktor bildet stets Isomorphismen auf Isomorphismen ab. Insbesondere haben isomorphe Objekte unter einem Funktor stets isomorphe Bilder.*

*Beweis.* Sei  $F$  unser Funktor. Mithilfe unserer Bedingung  $F(\text{id}) = \text{id}$  schließen wir:

$$\begin{aligned} f \text{ ist Isomorphismus} &\Rightarrow \text{Es gibt } g \text{ mit } f \circ g = \text{id} \text{ und } g \circ f = \text{id} \\ &\Rightarrow (Ff) \circ (Fg) = \text{id} \text{ und } (Fg) \circ (Ff) = \text{id} \\ &\Rightarrow Ff \text{ ist Isomorphismus.} \end{aligned} \quad \square$$

*Beispiel 4.7.2.8.* Für jede Kategorie  $\mathcal{C}$  bildet man die **opponierte Kategorie**  $\mathcal{C}^{\text{opp}}$ . Man setzt dazu

$$\text{Ob } \mathcal{C}^{\text{opp}} := \text{Ob } \mathcal{C} \quad \text{und} \quad \mathcal{C}^{\text{opp}}(X, Y) := \mathcal{C}(Y, X)$$

und erklärt die Verknüpfung von Morphismen in  $\mathcal{C}^{\text{opp}}$  als die vertauschte Verknüpfung. Wir notieren einen Morphismus  $f$  als  $f^\circ$ , wenn er in der opponierten Kategorie aufgefaßt werden soll, und haben also in Formeln  $g^\circ \circ f^\circ := (f \circ g)^\circ$ .

*Beispiel 4.7.2.9 (Bilden des Dualraums als Funktor).* Sei  $K$  ein Körper. Das Bilden des Dualraums mit dem Bilden der transponierten Abbildung auf dem Niveau der Homomorphismen ist auf den ersten Blick ein Funktor

$$\begin{array}{ccc} \text{Mod}_K & \rightarrow & \text{Mod}_K^{\text{opp}} \\ V & \mapsto & V^\top \\ f \downarrow & \mapsto & \uparrow f^\top \\ W & \mapsto & W^\top \end{array}$$

von der Kategorie der  $K$ -Vektorräume in ihre eigene opponierte Kategorie, vergleiche 3.2.9.15. Wenn wir es allerdings genau nehmen und ein Mengensystem  $\mathfrak{U}$  festhalten, so werden wir auf diese Weise im allgemeinen nur einen Funktor

$$\mathfrak{U}\text{Mod}_K \rightarrow \mathfrak{V}\text{Mod}_K^{\text{opp}}$$

für ein eventuell größeres Mengensystem  $\mathfrak{V}$  erhalten. Als konkretes Beispiel beachte man, daß über einem endlichen Körper der Dualraum eines abzählbaren Vektorraums im allgemeinen nicht mehr abzählbar ist. Ist jedoch unser Mengensystem  $\mathfrak{U}$  ein „Universum“ im Sinne von 4.7.11.3 und gehört die Grundmenge unseres Körpers  $K$  zu  $\mathfrak{U}$ , so ist  $\mathfrak{U}\text{Mod}_K$  sogar stabil unter dem Dualraumfunktor.

**Definition 4.7.2.10.** Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}^{\text{opp}}$  heißt auch ein **kontravarianter Funktor von  $\mathcal{A}$  nach  $\mathcal{B}$** .

4.7.2.11. Ausgeschrieben besteht ein kontravarianter Funktor von  $\mathcal{A}$  nach  $\mathcal{B}$  dem-nach aus einer Abbildung  $F : \text{Ob } \mathcal{A} \rightarrow \text{Ob } \mathcal{B}$  sowie für je zwei Objekte  $X, Y \in \mathcal{A}$  einer Abbildung  $F : \mathcal{A}(X, Y) \rightarrow \mathcal{B}(FY, FX)$  derart, daß gilt  $F(\text{id}) = \text{id}$  und  $F(f \circ g) = Fg \circ Ff$  für alle verknüpfbaren Morphismen  $f, g$ .

*Beispiel 4.7.2.12.* Gegeben Kategorien  $\mathcal{A}, \mathcal{B}$  bildet man ihr **Produkt**, eine weitere Kategorie  $\mathcal{A} \times \mathcal{B}$ , wie folgt: Man setzt  $\text{Ob}(\mathcal{A} \times \mathcal{B}) := \text{Ob } \mathcal{A} \times \text{Ob } \mathcal{B}$ , erklärt Morphismen in der Produktkategorie als Paare von Morphismen in den Ausgangskategorien, und erklärt die Verknüpfung von Morphismen in der Produktkategorie in der offensichtlichen Weise.

*Beispiel 4.7.2.13.* Das Bilden des Homomorphismenraums ist ein Funktor

$$\begin{array}{ccc} \text{Mod}_K^{\text{opp}} \times \text{Mod}_K & \rightarrow & \text{Mod}_K \\ (V, W) & \mapsto & \text{Hom}_K(V, W) \ni h \\ (f^\circ, g) \downarrow & \mapsto & \downarrow \\ (V', W') & \mapsto & \text{Hom}_K(V', W') \ni g \circ h \circ f \end{array}$$

Hier sollte der ganz rechte vertikale Pfeil eigentlich ein  $\mapsto$  sein, was ich aber mit meinem Schreibprogramm nicht hingekriegt habe. Die Notation  $\text{Hom}_K(V, W)$  betont, daß wir besagte Menge von Morphismen mit ihrer Vektorraumstruktur betrachten wollen.

*Ergänzendes Beispiel 4.7.2.14.* Das Bilden des Tensorprodukts ist ein Funktor

$$\begin{array}{ccc} \text{Mod}_K \times \text{Mod}_K & \rightarrow & \text{Mod}_K \\ (V, W) & \mapsto & V \otimes W \\ (f, g) \downarrow & \mapsto & f \otimes g \downarrow \\ (V', W') & \mapsto & V' \otimes W' \end{array}$$

*Ergänzendes Beispiel 4.7.2.15.* Das Bilden der  $r$ -ten Tensorpotenz nach 4.6.1.6 ist ein Funktor  $\text{Mod}_K \rightarrow \text{Mod}_K$ ,  $V \mapsto V^{\otimes r}$ ,  $f \mapsto f^{\otimes r}$ . Das Bilden der  $r$ -ten äußeren Potenz nach 4.6.5.3 ist ein Funktor  $\text{Mod}_K \rightarrow \text{Mod}_K$ ,  $V \mapsto \bigwedge^r V$  mit  $f \mapsto \bigwedge^r f$  nach 4.6.5.16.

*Beispiel 4.7.2.16.* Das „Vergessen der Gruppenstruktur“ ist ein Funktor  $v : \text{Grp} \rightarrow \text{Ens}$  von der Kategorie der Gruppen in die Kategorie der Mengen. Es gibt noch viele weitere derartige **Vergiß-Funktoren**.

*Beispiel 4.7.2.17.* Jeder Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  liefert in offensichtlicher Weise einen Funktor  $F^{\text{opp}} : \mathcal{A}^{\text{opp}} \rightarrow \mathcal{B}^{\text{opp}}$  zwischen den zugehörigen opponierten Kategorien. Oft notiert man ihn auch einfach  $F$ .

*Beispiel 4.7.2.18.* Gegeben ein Körper  $K$  bezeichne  $\text{Modf}_K$  mit  $f$  für „finitely generated“ die Kategorie der endlich erzeugten  $K$ -Vektorräume und  $\text{Modf}_K^\times$  die zugehörige Isomorphismenkategorie. Gegeben ein angeordneter Körper  $K$  ist das Bilden der Orientierungsmenge nach 3.6.5.3 ein Funktor

$$\text{or} : \text{Modf}_K^\times \rightarrow \text{Ens}^\times$$

**Definition 4.7.2.19.** 1. Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  heißt **treu**, wenn er Injektionen  $F : \mathcal{A}(A, A') \hookrightarrow \mathcal{B}(FA, FA')$  auf den Morphismen induziert, für alle  $A, A' \in \mathcal{A}$ .

2. Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  heißt **voll**, wenn er auf den Morphismenmengen Surjektionen  $F : \mathcal{A}(A, A') \twoheadrightarrow \mathcal{B}(FA, FA')$  induziert, für alle  $A, A' \in \mathcal{A}$ .

3. Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  heißt **volltreu**, wenn er voll und treu ist, wenn er also er Bijektionen  $F : \mathcal{A}(A, A') \xrightarrow{\sim} \mathcal{B}(FA, FA')$  auf den Morphismenmengen induziert. Ich notiere volltreue Funktoren gerne  $\xleftrightarrow{\sim}$ .

4. Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  heißt **essentiell surjektiv**, wenn er eine Surjektion auf Isomorphieklassen von Objekten induziert, wenn es also in Formeln für alle  $B \in \mathcal{B}$  ein  $A \in \mathcal{A}$  gibt mit  $FA \cong B$ .

5. Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  heißt eine **Äquivalenz von Kategorien**, wenn er volltreu und essentiell surjektiv ist. Ich notiere Äquivalenzen von Kategorien  $\xrightarrow{\sim}$ . Die doppelte Schlange soll andeuten, daß dieser Begriff schwächer ist als der Begriff eines Isomorphismus von Kategorien, wie er im Anschluß eingeführt wird.

6. Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  heißt ein **Isomorphismus von Kategorien**, wenn er bijektiv ist auf Objekten und auf Morphismen, wenn er also ein Isomorphismus ist in der Kategorie der Kategorien aus **??**. Ich notiere Isomorphismen von Kategorien  $\xrightarrow{\sim}$ .

*Beispiel 4.7.2.20.* Gegeben eine Kategorie  $\mathcal{C}$  und ein Objekt  $X \in \mathcal{C}$  erhalten wir einen Isomorphismus von Kategorien  $[\mathcal{C}(X)] \xrightarrow{\sim} \{X\}$  zwischen der Ein-Objekt-Kategorie des Monoids der Endomorphismen von  $X$  und der vollen Unterkategorie von  $\mathcal{C}$  mit dem einzigen Objekt  $X$ , indem wir die Identität auf den Morphismenmengen und die einzige mögliche Abbildung auf den Objektmengen nehmen.

*Beispiel 4.7.2.21.* Sei  $K$  ein Körper. Wir betrachten die Kategorie  $\text{Modf}_K$  aller endlichdimensionalen  $K$ -Vektorräume mit linearen Abbildungen als Morphismen. Dann ist unser Realisierungsfunktor  $n \mapsto K^n$  aus 4.7.2.2 eine Äquivalenz von Kategorien

$$\text{Mat}_K \xrightarrow{\sim} \text{Modf}_K$$

zwischen unserer Matrixkategorie  $\text{Mat}_K$  und der Kategorie der endlich erzeugten  $K$ -Vektorräume, aber unser Funktor ist natürlich kein Isomorphismus von Kategorien. Diese Aussage faßt eine Vielzahl von Aussagen der linearen Algebra zusammen und illustriert meines Erachtens recht gut die Kraft und Eleganz der Sprache der Kategorientheorie.

*Ergänzendes Beispiel 4.7.2.22 (Die Matrixkategorie eines Mengensystems).* Gegeben ein Körper  $K$  und ein Mengensystem  $\mathfrak{U}$  bilden wir die **abstrakte Matrixkategorie**  $\mathfrak{U}\text{Mat}_K$  wie folgt: Objekte sind alle Mengen aus  $\mathfrak{U}$ , in Formeln  $\text{Ob}(\mathfrak{U}\text{Mat}) := \mathfrak{U}$ . Die Morphismenmengen erklären wir durch die Vorschrift

$$\mathfrak{U}\text{Mat}_K(X, Y) := \left\{ T : X \times Y \rightarrow K \mid \begin{array}{l} \text{Für jedes } x \in X \text{ gilt} \\ T(x, y) = 0 \text{ für fast alle } y \in Y \end{array} \right\}$$

Zumindest im Fall, daß  $\mathfrak{U}$  keine überabzählbaren Mengen enthält, mag man sich als Elemente dieser Morphismenmengen Matrizen mit möglicherweise unendlich vielen Zeilen und Spalten aber höchstens endlich vielen von Null verschiedenen Einträgen in jeder Spalte denken. Die Verknüpfungen werden in der hoffentlich offensichtlichen Weise durch Summation über gleiche Indizes erklärt. Wir erhalten dann einen Funktor  $\mathfrak{U}\text{Mat}_K \rightarrow \text{Mod}_K$ , der auf Objekten durch die Konstruktion freier Vektorräume  $X \mapsto K\langle X \rangle$  über den entsprechenden Mengen gegeben wird und auf Morphismen leicht vom Leser erraten werden kann. Ist  $\mathfrak{U}$  ein „Universum“ im Sinne von 4.7.11.3, das den Körper  $K$  enthält, so erweist sich dieser Funktor sogar als eine Äquivalenz von Kategorien

$$\mathfrak{U}\text{Mat}_K \xrightarrow{\sim} \mathfrak{U}\text{Mod}_K$$

4.7.2.23. Gegeben ein Mengensystem  $\mathfrak{U}$  verstehen wir unter einer  **$\mathfrak{U}$ -Kategorie** eine Kategorie  $\mathcal{C}$ , bei der für alle Objekte  $X, Y \in \mathcal{C}$  die Morphismenmenge zu unserem Mengensystem  $\mathfrak{U}$  gehört, in Formeln  $\mathcal{C}(X, Y) \in \mathfrak{U}$ .

4.7.2.24. Die Menge aller Funktoren von einer Kategorie  $\mathcal{A}$  in eine Kategorie  $\mathcal{B}$  notieren wir

$$\text{Cat}(\mathcal{A}, \mathcal{B})$$

Sie ist eine Teilmenge  $\text{Cat}(\mathcal{A}, \mathcal{B}) \subset \text{Ens}(\text{Ob } \mathcal{A}, \text{Ob } \mathcal{B}) \times \text{Ens}(\text{Mor } \mathcal{A}, \text{Mor } \mathcal{B})$ . In 4.7.4.12 werden wir eine Kategorie erklären, deren Objekte gerade die Funktoren  $\mathcal{A} \rightarrow \mathcal{B}$  alias die Elemente von  $\text{Cat}(\mathcal{A}, \mathcal{B})$  sind, aber alles zu seiner Zeit.

*Beispiel 4.7.2.25.* Gegeben ein Mengensystem  $\mathfrak{U}$  und eine  $\mathfrak{U}$ -Kategorie  $\mathcal{C}$  und ein Objekt  $X \in \mathcal{C}$  ist die Zuordnung  $Y \mapsto \mathcal{C}(X, Y)$  ein Funktor  $\mathcal{C}(X, -) : \mathcal{C} \rightarrow \mathfrak{U}\text{Ens}$  und die Zuordnung  $Y \mapsto \mathcal{C}(Y, X)$  ein Funktor  $\mathcal{C}(-, X) : \mathcal{C} \rightarrow \mathfrak{U}\text{Ens}^{\text{opp}}$ .

*Beispiel 4.7.2.26 (Funktoren zwischen Einobjektkategorien).* Gegeben Monoide  $G, H$  und die zugehörigen Einobjektkategorien  $[G], [H]$  nach 4.7.1.6 erhalten

wir in der offensichtlichen Weise eine Bijektion zwischen der Menge aller Monoidhomomorphismen  $G \rightarrow H$  und der Menge aller Funktoren  $[G] \rightarrow [H]$ , in Formeln also eine Bijektion

$$\text{Mon}(G, H) \xrightarrow{\sim} \text{Cat}([G], [H])$$

### Übungen

*Übung 4.7.2.27.* Hat ein Funktor sogar die Eigenschaft, daß alle Morphismen, die er auf Isomorphismen abbildet, bereits zuvor Isomorphismen gewesen sein müssen, so nennt man ihn **konservativ**. Man gebe Beispiele für konservative und nichtkonservative Funktoren.

*Übung 4.7.2.28.* Jede Äquivalenz von Kategorien induziert eine Bijektion zwischen den zugehörigen Isomorphieklassen von Objekten. Zum Beispiel werden die endlichdimensionalen  $k$ -Vektorräume klassifiziert durch ihre Dimension, alias durch Elemente von  $\mathbb{N}$ , alias durch Isomorphieklassen der Matrixkategorie.

*Übung 4.7.2.29 (Zwei aus Drei für Äquivalenzen von Kategorien).* Seien  $F : \mathcal{A} \rightarrow \mathcal{B}$  und  $G : \mathcal{B} \rightarrow \mathcal{C}$  Funktoren. Sind zwei der drei Funktoren  $F, G, GF$  Äquivalenzen von Kategorien, so auch der Dritte.

*Übung 4.7.2.30.* Bilden wir zu einer Kategorie eine volle Unterkategorie, indem wir aus jeder Isomorphiekasse von Objekten ein Objekt willkürlich auswählen, so ist der Einbettungsfunktor eine Äquivalenz von Kategorien.

*Übung 4.7.2.31.* Sind in einer Kategorie  $\mathcal{C}$  je zwei Objekte isomorph, so ist für jedes Objekt  $X \in \mathcal{C}$  der offensichtliche Funktor eine Äquivalenz von Kategorien

$$[\mathcal{C}(X)] \xrightarrow{\sim} \mathcal{C}$$

zwischen der Ein-Objekt-Kategorie des Endomorphismenmonoids  $\mathcal{C}(X)$  von  $X$  und unserer Kategorie.

*Übung 4.7.2.32.* Gegeben Kategorien  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  liefert jedes Paar  $(F, G)$  von Funktoren  $F : \mathcal{A} \rightarrow \mathcal{B}$  und  $G : \mathcal{B} \rightarrow \mathcal{C}$  einen wohlbestimmten Funktor in die Produktkategorie  $(F, G) : \mathcal{A} \rightarrow \mathcal{B} \times \mathcal{C}$ .

### 4.7.3 Objekte mit Zusatzstrukturen\*

4.7.3.1. Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$  und ein Objekt  $X \in \mathcal{C}$  erklären wir eine  **$(\mathcal{S}, v)$ -Struktur auf  $X$**  als eine Äquivalenzklasse von Paaren  $(S, \varphi)$  bestehend aus einem Objekt  $S \in \mathcal{S}$  und einem Isomorphismus  $\varphi : v(S) \xrightarrow{\sim} X$  mit der Maßgabe, daß  $(S, \varphi)$  äquivalent ist zu  $(T, \psi)$ , wenn es einen Isomorphismus  $i : S \xrightarrow{\sim} T$  gibt mit  $\varphi = \psi \circ v(i)$ .

*Beispiel 4.7.3.2.* Sei  $\mathfrak{U}$  ein Mengensystem. Wir erhalten für jede Menge  $X \in \mathfrak{U}$  eine offensichtliche Bijektion zwischen der Menge aller Verknüpfungen auf  $X$ , die  $X$  zu einer Gruppe machen, und der Menge aller  $(\mathfrak{U}\text{Grp}, v)$ -Strukturen auf  $X$  für  $v : \mathfrak{U}\text{Grp} \rightarrow \mathfrak{U}\text{Ens}$  der Vergißfunktor.

*Beispiel 4.7.3.3.* Sei  $\mathfrak{U}$  ein Mengensystem. Wir erhalten für jede Menge  $X \in \mathfrak{U}$  eine offensichtliche Bijektion zwischen der Menge aller Verknüpfungen auf  $X$ , die  $X$  zu einer abelschen Gruppe machen, und der Menge aller  $(\mathfrak{U}\text{Ab}, v)$ -Strukturen auf  $X$  für  $v : \mathfrak{U}\text{Ab} \rightarrow \mathfrak{U}\text{Ens}$  der Vergißfunktor.

*Beispiel 4.7.3.4.* Sei  $\mathfrak{U}$  ein Mengensystem. Wir erhalten für jede Menge  $X \in \mathfrak{U}$  eine offensichtliche Bijektion zwischen der Menge aller Topologien auf  $X$  und der Menge aller  $(\mathfrak{U}\text{Top}, v)$ -Strukturen auf  $X$  für  $v : \mathfrak{U}\text{Top} \rightarrow \mathfrak{U}\text{Ens}$  der Vergißfunktor.

*Beispiel 4.7.3.5.* Seien  $k$  ein Körper und  $\mathfrak{U}$  ein Mengensystem. Wir erhalten für jede abelsche Gruppe  $X \in \mathfrak{U}\text{Ab}$  eine offensichtliche Bijektion zwischen der Menge aller Abbildungen  $k \times X \rightarrow X$ , die als Multiplikation mit Skalaren die Gruppe  $X$  zu einem  $k$ -Vektorraum machen, und der Menge aller  $(\mathfrak{U}\text{Mod}_k, v)$ -Strukturen auf  $X$  für  $v : \mathfrak{U}\text{Mod}_k \rightarrow \mathfrak{U}\text{Ab}$  der Vergißfunktor.

4.7.3.6. Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$  und ein Morphismus  $f \in \mathcal{C}(X, Y)$  von Objekten mit  $(\mathcal{S}, v)$ -Struktur sagen wir, unser Morphismus sei **verträglich mit der  $(\mathcal{S}, v)$ -Struktur**, wenn für beliebige Wahlen von Repräsentanten  $(S, \varphi)$  und  $(T, \psi)$  der jeweiligen  $(\mathcal{S}, v)$ -Strukturen auf  $X$  und  $Y$  unser  $f$  das Bild unter  $v$  eines Morphismus  $F : S \rightarrow T$  ist, genauer  $f = \psi \circ v(F) \circ \varphi^{-1}$ . Offensichtlich ist die Identität auf einem Objekt mit jeder  $(\mathcal{S}, v)$ -Struktur auf besagtem Objekt verträglich und die Verknüpfung von verträglichen Morphismen ist wieder verträglich. Die so erklärte Kategorie der **Objekte von  $\mathcal{C}$  mit  $(\mathcal{S}, v)$ -Struktur** notieren wir

$$\mathcal{C}_{(\mathcal{S}, v)}$$

Wir erhalten eine Äquivalenz von Kategorien  $\mathcal{S} \xrightarrow{\sim} \mathcal{C}_{(\mathcal{S}, v)}$  durch die Vorschrift  $S \mapsto (S, \text{id}_{v(S)})$ .

*Beispiel 4.7.3.7.* Gegeben ein Mengensystem  $\mathfrak{U}$  ist unsere Äquivalenz aus 4.7.3.6 sogar ein Isomorphismus

$$\mathfrak{U}\text{Grp} \xrightarrow{\sim} \mathfrak{U}\text{Ens}_{(\mathfrak{U}\text{Grp}, v)}$$

zwischen der Kategorie aller Mengen  $G \in \mathfrak{U}$  mit einer Verknüpfung, die sie zu einer Gruppe macht, und der Kategorie aller Mengen  $G \in \mathfrak{U}$  versehen mit einer Äquivalenzklasse von Paaren  $(S, \varphi)$  bestehend aus einem Objekt  $S \in \mathfrak{U}\text{Grp}$  zusammen mit einer Bijektion von Mengen  $\varphi : S \xrightarrow{\sim} G$  unter der in 4.7.3.1 gegebenen Äquivalenzrelation. Dasselbe gilt für das Vergessen der Topologie  $v : \mathfrak{U}\text{Top} \rightarrow \mathfrak{U}\text{Ens}$  oder das Vergessen der Operation der Skalare  $v : \mathfrak{U}\text{Mod}_k \rightarrow \mathfrak{U}\text{Ab}$

in der Kategorie der Moduln über einem Ring  $k$  und überhaupt in allen konkreten Anwendungen, die mir in den Sinn kommen.

4.7.3.8. Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$  nennen wir einen Morphismus  $f : X \rightarrow Y$  in  $\mathcal{C}_{(\mathcal{S}, v)}$  **initial**, wenn für alle  $W \in \mathcal{C}_{(\mathcal{S}, v)}$  gilt

$$\mathcal{C}_{(\mathcal{S}, v)}(W, X) = \{e \in \mathcal{C}(W, X) \mid fe \in \mathcal{C}_{(\mathcal{S}, v)}(W, Y)\}$$

Initiale Morphismen heißen oft **Einbettungen**. Es ist klar, daß jede Verknüpfung initialer Morphismen initial ist und daß eine Verknüpfung von zwei Morphismen in  $\mathcal{C}_{(\mathcal{S}, v)}$  nur dann initial sein kann, wenn der erste initial ist. Einen Morphismus in  $\mathcal{S}$  nennen wir  **$v$ -initial**, wenn er unter  $v$  einen  $(\mathcal{S}, v)$ -initialen Morphismus induziert.

*Beispiel 4.7.3.9.* Sei  $\mathfrak{U}$  ein Mengensystem. Im Fall der  $\mathfrak{U}$ -Mengen mit  $(\mathfrak{U}\text{Grp}, v)$ -Struktur sind genau die injektiven mit der Struktur verträglichen Abbildungen initial. Ist in der Tat  $f : X \hookrightarrow Y$  ein Gruppenhomomorphismus und  $W$  eine Gruppe, so ist eine Abbildung  $e : W \rightarrow X$  genau dann ein Gruppenhomomorphismus, wenn  $fe : W \rightarrow Y$  ein Gruppenhomomorphismus ist.

4.7.3.10. Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$  und ein Morphismus  $f : X \rightarrow Y$  in  $\mathcal{C}$  und eine  $(\mathcal{S}, v)$ -Struktur auf  $Y$  gibt es höchstens eine  $(\mathcal{S}, v)$ -Struktur auf  $X$  derart, daß  $f$  initial wird. In der Tat, repräsentieren  $(S, \varphi)$  und  $(T, \psi)$  zwei derartige Strukturen, so muß die Identität auf  $X$  verträglich sein sowohl als Morphismus  $(X, S, \varphi) \rightarrow (X, T, \psi)$  als auch als Morphismus in die Gegenrichtung und daraus folgt leicht, daß diese beiden Daten dieselbe Struktur repräsentieren. Wir nennen sie die **induzierte Struktur** oder die **initiale Struktur** auf  $X$ .

*Beispiel 4.7.3.11.* Sei  $\mathfrak{U}$  ein Mengensystem. Im Fall der  $\mathfrak{U}$ -Mengen mit  $(\mathfrak{U}\text{Top}, v)$ -Struktur alias topologischen Räume aus  $\mathfrak{U}$  heißt unsere induzierte Struktur die Initialtopologie und im Fall der Einbettung einer Teilmenge auch die induzierte Topologie oder Spurtopologie oder Teilraumtopologie. In dieser Situation gibt es stets eine initiale Struktur.

*Beispiele 4.7.3.12.* Sei  $\mathfrak{U}$  ein Mengensystem. Im Fall des Vergessens der Verknüpfung  $v : \mathfrak{U}\text{Grp} \rightarrow \mathfrak{U}\text{Ens}$  existiert eine induzierte Struktur genau für diejenigen Abbildungen, die injektiv sind und deren Bild eine Untergruppe ist. Die induzierte Struktur ist dann die induzierte Gruppenstruktur. Eine Teilmenge  $X \subset Y$  einer Menge  $Y$  mit  $(\mathcal{S}, v)$ -Struktur nennt man ganz allgemein ein  $(\mathcal{S}, v)$ -**Unterobjekt**, wenn sie eine induzierte Struktur besitzt. Beispiele sind Untergruppen, Untervektorräume, affine Teilräume, Unterringe und so weiter.

4.7.3.13. Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$  ist auch  $v^{\text{opp}} : \mathcal{S}^{\text{opp}} \rightarrow \mathcal{C}^{\text{opp}}$  ein treuer Funktor und wir erhalten in der offensichtlichen Weise einen Isomorphismus von Kategorien

$$(\mathcal{C}_{(\mathcal{S}, v)})^{\text{opp}} \xrightarrow{\sim} \mathcal{C}_{(\mathcal{S}^{\text{opp}}, v^{\text{opp}})}^{\text{opp}}$$

Morphismen  $f : X \rightarrow Y$  in  $\mathcal{C}_{(\mathcal{S}, v)}$  mit  $f^\circ$  initial in Bezug auf die jeweiligen  $(\mathcal{S}^{\text{opp}}, v^{\text{opp}})$ -Strukturen nennen wir **final**. Ausgeschrieben bedeutet das, daß für jedes weitere Objekt  $Z \in \mathcal{C}_{(\mathcal{S}, v)}$  gilt

$$\mathcal{C}_{(\mathcal{S}, v)}(Y, Z) = \{g \in \mathcal{C}(Y, Z) \mid gf \in \mathcal{C}_{(\mathcal{S}, v)}(X, Z)\}$$

Finale Morphismen heißen oft **Quotienten**. Es ist klar, daß jede Verknüpfung finaler Morphismen final ist und daß eine Verknüpfung von zwei Morphismen in  $\mathcal{C}_{(\mathcal{S}, v)}$  nur dann final sein kann, wenn der zweite final ist. Einen Morphismus in  $\mathcal{S}$  nennen wir  $v$ -**final**, wenn er unter  $v$  einen  $(\mathcal{S}, v)$ -finalen Morphismus induziert.

**4.7.3.14.** Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$  und ein Morphismus  $f : X \rightarrow Y$  in  $\mathcal{C}$  und eine  $(\mathcal{S}, v)$ -Struktur auf  $X$  gibt es höchstens eine  $(\mathcal{S}, v)$ -Struktur auf  $Y$  derart, daß  $f$  final wird. Wir nennen sie die **koinduzierte Struktur** oder die **finale Struktur** auf  $Y$ .

**Beispiel 4.7.3.15.** Sei  $\mathfrak{U}$  ein Mengensystem. Im Fall der  $\mathfrak{U}$ -Mengen mit  $(\mathfrak{U}\text{Top}, v)$ -Struktur alias topologischen Räume heißt unsere koinduzierte Struktur die Finaltopologie und insbesondere im Fall von surjektiven Abbildungen auch die Quotiententopologie.

**Beispiele 4.7.3.16.** Sei  $\mathfrak{U}$  ein Mengensystem. Im Fall des Vergessens der Verknüpfung  $v : \mathfrak{U}\text{Grp} \rightarrow \mathfrak{U}\text{Ens}$  existiert eine koinduzierte Struktur genau für diejenigen Abbildungen von einer Gruppe in eine Menge, die faktorisieren in einen surjektiven Gruppenhomomorphismus gefolgt von einer Bijektion, und die koinduzierte Struktur ist die von einer und jeder derartigen Bijektion induzierte Gruppenstruktur.

**Vorschau 4.7.3.17.** In ?? und ?? führen wir allgemeiner „gesamthaft initiale“ und „gesamthaft finale“ Familien ein.

## Übungen

**Übung 4.7.3.18.** Gegeben ein treuer Funktor  $v : \mathcal{S} \rightarrow \mathcal{C}$ , der zusätzlich konservativ ist, kann die Identität auf einem Objekt  $X \in \mathcal{C}$  nicht für zwei unterschiedliche  $(\mathcal{S}, v)$ -Strukturen  $(S, \varphi)$  und  $(T, \psi)$  auf  $X$  ein Morphismus  $(X, S, \varphi) \rightarrow (X, T, \psi)$  sein.

## 4.7.4 Transformationen

**4.7.4.1.** Bis hierher hat sich unsere Theorie noch in leidlich vertrauten Bahnen bewegt: Wir haben eben eine neue Art von Strukturen erklärt, die Kategorien, und dazwischen strukturerhaltende Abbildungen alias Morphismen betrachtet, die Funktoren. Insoweit paßt alles noch in den strukturellen Rahmen, an den man in

der linearen Algebra durch das Studium von Vektorräumen und linearen Abbildungen oder Gruppen und Gruppenhomomorphismen gewöhnt worden ist. Das Neue bei der Kategorientheorie ist nun, daß es auch „Morphismen zwischen Morphismen“ gibt. Sie heißen „Transformationen von Funktoren“ und sind das Thema dieses Abschnitts.

**Definition 4.7.4.2.** Seien  $\mathcal{A}, \mathcal{B}$  Kategorien und  $F, G : \mathcal{A} \rightarrow \mathcal{B}$  Funktoren. Eine **Transformation**  $\tau : F \Rightarrow G$  ist eine Vorschrift, die jedem Objekt  $X \in \mathcal{A}$  einen Morphismus  $\tau_X \in \mathcal{B}(FX, GX)$  zuordnet derart, daß für jeden Morphismus  $f : X \rightarrow Y$  in  $\mathcal{A}$  das Rechteck

$$\begin{array}{ccc} FX & \xrightarrow{\tau_X} & GX \\ Ff \downarrow & & \downarrow Gf \\ FY & \xrightarrow{\tau_Y} & GY \end{array}$$

in  $\mathcal{B}$  kommutiert. In Formeln meint das die Gleichheit  $(Gf) \circ \tau_X = \tau_Y \circ (Ff)$  in der Morphismenmenge  $\mathcal{B}(FX, GY)$ . Ob ein Doppelpfeil eine Transformation von Funktoren oder vielmehr eine Implikation meint, muß der Leser aus dem Kontext erschließen. Sind alle  $\tau_X$  Isomorphismen, so nenne ich  $\tau$  eine **Isotransformation** und notiere sie  $\tilde{\Rightarrow}$ , aber diese Terminologie ist nicht gebräuchlich. In der Literatur spricht man eher von einem **Isomorphismus von Funktoren** oder auch von einer **Äquivalenz von Funktoren**. Gibt es zwischen zwei Funktoren eine Isotransformation, so heißen sie **isomorph**.

**4.7.4.3 (Diskussion der Doppelpfeil-Notation).** Ich finde die Notation von Transformationen durch Doppelpfeile didaktisch hilfreich in derselben Weise wie die Notation  $\vec{v}$  für Vektoren am Anfang der linearen Algebra. Andererseits werden wir sie nicht konsequent durchhalten können und das ist auch nicht sinnvoll, denn wie in 4.7.4.12 erklärt können auch die Transformationen als Morphismen einer Kategorie aufgefaßt werden, der „Funktorkategorie“.

**4.7.4.4 (Diskussion der Terminologie).** In der Literatur heißen unsere Transformationen meist „natürliche Transformationen“. Diese Terminologie schien mir jedoch unnötig umständlich und entspricht auch nicht meinem Sprachempfinden: Ich möchte zum Beispiel unter der „natürlichen“ Transformation des Identitätsfunktors auf der Kategorie aller  $\mathbb{R}$ -Vektorräume in den Bidualraumfunktor gerne die in 4.7.4.9 gegebene Transformation verstehen, die zwar keineswegs die einzige Transformation zwischen diesen Funktoren ist, aber vielleicht schon die „natürlicheste“.

**Beispiel 4.7.4.5 (Die Länge als Transformation).** Ich betrachte den Vergißfunktor und den Längengeradenfunktor 4.7.2.4 von der Kategorie der euklidischen Vektorräume in die Kategorie der reellen Vektorräume. Schalten wir noch einen

weiteren Vergißfunktor nach, so werden sie zu Funktoren  $\text{Euk} \rightarrow \text{Ens}$ . Unsere in 4.1.5.12 erklärten Längenabbildungen  $\| \|_V : V \rightarrow \mathbb{L}(V)$  bilden dann in ihrer Gesamtheit eine Transformation  $\text{verg} \Rightarrow \mathbb{L}$  zwischen Funktoren  $\text{Euk} \rightarrow \text{Ens}$ . Ob ich nämlich erst einen Vektor mittels eines Homomorphismus von euklidischen Vektorräumen in einen weiteren euklidischen Vektorraum abbilde und dann seine Länge in Bezug auf den Bildraum nehme, oder erst seine Länge nehme und diese mittels des auf den Längengeraden induzierten Homomorphismus zu einer Länge in Bezug auf den Bildraum mache, es kommt beidesmal dasselbe heraus.

**Beispiel 4.7.4.6 (Winkelmaße als Transformationen).** Wir betrachten den Funktor  $W : \text{KongEb} \rightarrow \text{Grp}$ , der jeder Kongruenzebene  $(E, K)$  ihre Winkelgruppe  $W(E) := \vec{K}^+$  zuordnet, also die Gruppe ihrer orientierungserhaltenden Richtungskongruenzen. Unsere Winkelmaße aus 4.1.8.1 können wir auffassen als Transformationen

$$\text{or}_{\mathbb{R}} \circ \text{Richt} \Rightarrow W$$

von Funktoren  $\text{KongEb} \rightarrow \text{Grp}$  alias „natürliche“ Gruppenhomomorphismen  $\text{or}_{\mathbb{R}}(\vec{E}) \rightarrow W(E)$  von der Orientierungsgerade in die Winkelgruppe.

4.7.4.7. Winkelmaße sind etwas grundsätzlich anderes als Einheiten. Ein Winkelmaß in einer Kongruenzebene anzugeben bedeutet, ein Winkelmaß in allen Kongruenzebenen anzugeben. Eine Längeneinheit in einer Kongruenzebene anzugeben bedeutet dagegen keineswegs, eine Längeneinheit in allen Kongruenzebenen anzugeben.

**Beispiel 4.7.4.8 (Das kanonische Skalarprodukt als Transformation).** Unsere kanonischen Skalarprodukte  $\langle , \rangle_V : V \otimes V \rightarrow \mathbb{L}(V)^{\otimes 2}$  für euklidische Vektorräume aus 4.6.4.6 bilden in ihrer Gesamtheit eine Transformation

$$\text{verg}^{\otimes 2} \Rightarrow \mathbb{L}^{\otimes 2}$$

zwischen Funktoren  $\text{Euk} \rightarrow \text{Mod}_{\mathbb{R}}$  von der Kategorie der euklidischen Vektorräume in die Kategorie der  $\mathbb{R}$ -Vektorräume.

**Beispiel 4.7.4.9 (Evaluation als Transformation).** Gegeben ein Körper  $K$  bezeichne  $B : \text{Mod}_K \rightarrow \text{Mod}_K$  den **Bidualraumfunktor**, der jedem  $K$ -Vektorraum  $V$  seinen Bidualraum  $BV := V^{\top\top}$  zuordnet. So bilden die Evaluationsabbildungen  $\text{ev}_V : V \rightarrow V^{\top\top}, v \mapsto (f \mapsto f(v))$  in ihrer Gesamtheit eine Transformation

$$\text{ev} : \text{Id} \Rightarrow B$$

und eine Isotransformation zwischen den Restriktionen dieser Funktoren auf die Kategorie der endlichdimensionalen  $K$ -Vektorräume, vergleiche 3.2.9.26. Oft formalisiert man Situationen dieser Art nicht bis ins Letzte aus und spricht von **kanonischen Abbildungen** beziehungsweise **kanonischen Isomorphismen**, wenn

bei formalerer Betrachtung Abbildungen  $\tau_X : FX \rightarrow GX$  oder Isomorphismen  $\tau_X : FX \xrightarrow{\sim} GX$  gemeint sind, die in ihrer Gesamtheit eine Transformation beziehungsweise Isotransformation von Funktoren  $\tau : F \Rightarrow G$  bilden.

**Beispiel 4.7.4.10 (Dualraum und Transponieren).** Seien  $K$  ein Körper und  $D : \text{Mod}_K \rightarrow \text{Mod}_K^{\text{opp}}$  der **Dualraumfunktor**, der jedem Raum seinen Dualraum zuordnet. Sei weiter  $\text{Mat}_K$  die Matrixkategorie aus 4.7.1.7 und  $T : \text{Mat}_K \rightarrow \text{Mat}_K^{\text{opp}}$  der Funktor, der die Objekte festhält und Matrizen transponiert. Sei schließlich  $R : \text{Mat}_K \rightarrow \text{Mod}_K$  unser Realisierungsfunktor  $n \mapsto K^n$  aus 4.7.2.2 und bezeichne  $R^{\text{opp}}$  den entsprechenden Funktor zwischen den jeweils opponierten Kategorien. So erhalten wir eine Isotransformation

$$\tau : R^{\text{opp}}T \xrightarrow{\sim} DR$$

durch die Vorschrift, die jeder natürlichen Zahl alias jedem Objekt  $n \in \text{Mat}_K$  den offensichtlichen Isomorphismus  $\tau_n : K^n \xrightarrow{\sim} (K^n)^\top$  zuordnet. Es kann hilfreich sein, durch Doppelpfeile in Diagrammen von Kategorien und Funktoren klarzumachen, zwischen welchen Funktoren eine Transformation gemeint ist. So wäre etwa in diesem Beispiel unser  $\tau$  ein möglicher Doppelpfeil im Diagramm

$$\begin{array}{ccc} \text{Mat}_K & \xrightarrow{T} & \text{Mat}_K^{\text{opp}} \\ R \downarrow & \swarrow \tau \sim & \downarrow R^{\text{opp}} \\ \text{Mod}_K & \xrightarrow{D} & \text{Mod}_K^{\text{opp}} \end{array}$$

**Beispiel 4.7.4.11 (Tensor und Hom).** Die natürlichen Abbildungen

$$\text{can} : V^\top \otimes_K W \rightarrow \text{Hom}_K(V, W)$$

aus 4.6.1.21 für  $K$ -Vektorräume  $V, W$  liefern eine Transformation zwischen den durch diese Vorschriften gegebenen Funktoren

$$\text{Mod}_K^{\text{opp}} \times \text{Mod}_K \rightarrow \text{Mod}_K$$

**4.7.4.12 (Kategorien von Funktoren).** Sind  $\tau : F \Rightarrow G$  und  $\sigma : G \Rightarrow H$  Transformationen, so ist auch  $\sigma \circ \tau : F \Rightarrow H$  gegeben durch  $(\sigma \circ \tau)_X := \sigma_X \circ \tau_X$  für jedes Objekt  $X$  der Ausgangskategorie von  $F$  eine Transformation. Des weiteren gibt es für jeden Funktor  $F$  die **identische Transformation**  $\text{id} = \text{id}_F$  von besagtem Funktor zu sich selber, gegeben durch  $(\text{id}_F)_X := \text{id}_{FX}$  für jedes Objekt  $X$  der Ausgangskategorie unseres Funktors. Sind  $\mathcal{A}, \mathcal{B}$  Kategorien, so bilden die Funktoren  $\mathcal{A} \rightarrow \mathcal{B}$  sogar selbst eine Kategorie, mit Funktoren als Objekten und Transformationen als Morphismen und der eben erklärten Verknüpfung von Transformationen als Verknüpfung von Morphismen. Ich verwende für diese **Funktorkategorie** verschiedene Notationen. Erst einmal dieselbe Notation  $\text{Cat}(\mathcal{A}, \mathcal{B})$  wie

für die Menge der Objekte, dann die Notation  $\underline{\text{Cat}}(\mathcal{A}, \mathcal{B})$  wenn es darum geht, die Zusatzstruktur als Kategorie zu betonen, weiter die Notation  $(\mathcal{A} \Rightarrow \mathcal{B})$ , weil es sich um einen Spezialfall von „internem Hom“ erweisen wird, und als besonders kurze Form die exponentielle Notation  $\mathcal{B}^{\mathcal{A}}$ , so daß etwa für Funktoren  $F, G : \mathcal{A} \rightarrow \mathcal{B}$  die Menge der Transformationen

$$\text{Cat}(\mathcal{A}, \mathcal{B})(F, G) = \mathcal{B}^{\mathcal{A}}(F, G)$$

notiert werden kann. Wenn die Kategorien selber durch größere Ausdrücke gegeben werden, sind für die Menge der Transformationen auch abkürzende Notationen wie etwa  $\text{Trans}(F, G)$  sinnvoll und üblich. Unsere Isotransformationen sind genau die Isomorphismen der Funktorkategorie.

*Ergänzung 4.7.4.13 (Exponentialgesetz für Kategorien).* Man zeige, daß man für je drei Kategorien  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  eine Bijektion

$$\text{Cat}(\mathcal{A}, \underline{\text{Cat}}(\mathcal{B}, \mathcal{C})) \xrightarrow{\sim} \text{Cat}(\mathcal{A} \times \mathcal{B}, \mathcal{C})$$

erhält durch die Vorschrift  $F \mapsto \tilde{F}$  mit  $\tilde{F}(A, B) = (F(A))(B)$  auf Objekten und eine vom Leser zu spezifizierende Vorschrift auf Morphismen. Man baut diese auch leicht zu einem Isomorphismus von Kategorien aus, und das folgt alternativ auch aus allgemeinen Aussagen zu „internem Hom“, wie sie etwa in ?? diskutiert werden.

*Beispiel 4.7.4.14.* Seien  $F, G : \mathcal{A} \rightarrow \mathcal{B}$  Funktoren und  $\tau : F \Rightarrow G$  eine Transformation. Gegeben ein weiterer Funktor  $H : \mathcal{B} \rightarrow \mathcal{C}$  erhalten wir in offensichtlicher Weise eine Transformation  $H\tau : HF \Rightarrow HG$ . Gegeben ein weiterer Funktor  $K : \mathcal{D} \rightarrow \mathcal{A}$  erhalten wir in offensichtlicher Weise ebenso eine Transformation  $\tau K : FK \Rightarrow GK$ . Offensichtlich liefern diese Konstruktionen ihrerseits Funktoren  $\text{Cat}(\mathcal{A}, \mathcal{B}) \rightarrow \text{Cat}(\mathcal{A}, \mathcal{C})$  und  $\text{Cat}(\mathcal{A}, \mathcal{B}) \rightarrow \text{Cat}(\mathcal{D}, \mathcal{B})$  zwischen den entsprechenden Funktorkategorien, die wir als das **Nachschalten von  $H$**  beziehungsweise **Vorschalten von  $K$**  bezeichnen.

**4.7.4.15 (Schwierigkeiten der Notation).** Die Notationen  $\tau K$  und  $H\tau$  führen leicht zu Verwirrung, sobald nicht aus der Art der Symbole heraus klar ist, welche Symbole Funktoren und welche Transformationen darstellen. Ich kenne keine generelle Lösung für diese Schwierigkeiten der Notation. In diesem Abschnitt habe ich versucht, eine gewisse Übersichtlichkeit dadurch zu erreichen, daß ich systematisch lateinische Großbuchstaben für Funktoren und kleine griechische Buchstaben für Transformationen verwende.

## Übungen

*Übung 4.7.4.16.* Gegeben ein Körper  $K$  zeige man, daß der Funktor  $\text{Modf}_K^\times \rightarrow \text{Modf}_K^\times$  von der Isomorphiekategorie der endlichdimensionalen  $K$ -Vektorräume

zu sich selber, der jedem Raum seinen Dualraum zuordnet und jedem Isomorphismus die Inverse der transponierten Abbildung  $\varphi \mapsto (\varphi^\top)^{-1}$ , nicht isomorph ist zum Identitätsfunktor. Hinweis: Man passe im Fall des Körpers mit zwei Elementen besonders gut auf.

*Übung 4.7.4.17.* Seien  $K$  ein Körper und  $\text{Id} : \text{Mod}_K \rightarrow \text{Mod}_K$  der Identitätsfunktor. Man bestimme alle Transformationen von diesem Funktor zu sich selber. Ebenso bestimme man alle Transformationen von diesem Funktor zum Bidualraumfunktor.

*Übung 4.7.4.18.* Sind zwei Funktoren isomorph und ist der eine eine Äquivalenz von Kategorien, so auch der andere.

*Übung 4.7.4.19.* Man diskutiere, inwiefern die in 4.6.5.3 für jeden Vektorraum  $V$  konstruierten kanonischen Isomorphismen  $(\bigwedge^r V)^\top \xrightarrow{\sim} \text{Alt}^r(V)$  eine Isotransformation bilden. Idem für die in 4.6.5.9 für jeden endlichdimensionalen Vektorraum  $V$  konstruierten kanonischen Isomorphismen  $\bigwedge^r(V^\top) \xrightarrow{\sim} \text{Alt}^r(V)$ .

*Übung 4.7.4.20.* Gegeben ein Monoid  $G$  heißt eine Abbildung  $\phi : X \rightarrow Y$  von  $G$ -Mengen **äquivariant**, wenn gilt  $\phi(gx) = g\phi(x)$  für alle  $g \in G$  und  $x \in X$ . Die  $G$ -Mengen mit den äquivarianten Abbildungen als Morphismen bilden dann eine Kategorie, für die ich die beiden Notationen  $G\text{-Ens} = \text{Ens}_{G\backslash}$  verwende. Bilden wir zu unserem Monoid  $G$  die Ein-Objekt-Kategorie  $[G]$ , so liefert der hoffentlich offensichtliche Funktor einen Isomorphismus von Kategorien

$$G\text{-Ens} \xrightarrow{\sim} \text{Cat}([G], \text{Ens})$$

*Ergänzende Übung 4.7.4.21 (Komplexifizierung einer Reellifizierung).* Wir erhalten eine Isotransformation zwischen Funktoren  $\text{Mod}_{\mathbb{C}} \rightarrow \text{Mod}_{\mathbb{C}}$  vermittels der Abbildungen  $i_V : \mathbb{C} \otimes_{\mathbb{R}} V \xrightarrow{\sim} V \oplus \bar{V}$  gegeben durch  $\alpha \otimes v \mapsto (\alpha v, \alpha \bar{v})$  in den Notationen 4.1.12.33. Die inverse Isotransformation wird beschrieben durch die Abbildungsvorschrift

$$(v, \bar{w}) \mapsto (1/2) \otimes (v + w) - (i/2) \otimes (iv - iw)$$

Im übrigen bildet unser Isomorphismus oben den Eigenraum  $\text{Eig}(1 \otimes i | \mathbb{C} \otimes_{\mathbb{R}} V; i)$  isomorph auf  $V$  ab und den Eigenraum  $\text{Eig}(1 \otimes i | \mathbb{C} \otimes_{\mathbb{R}} V; -i)$  isomorph auf  $\bar{V}$ . Der schiefflineare Automorphismus  $\alpha \otimes v \mapsto \bar{\alpha} \otimes v$  von  $\mathbb{C} \otimes_{\mathbb{R}} V$  schließlich entspricht unter unserem Isomorphismus dem schiefflinearen Automorphismus  $(v, \bar{w}) \mapsto (w, \bar{v})$  von  $V \oplus \bar{V}$ .

*Ergänzende Übung 4.7.4.22.* Wir erhalten eine Isotransformation zwischen Funktoren  $\text{Mod}_{\mathbb{C}} \rightarrow \text{Mod}_{\mathbb{C}}^{\text{opp}}$  vermittels der Abbildungen  $\bar{V}^\top \xrightarrow{\sim} \bar{V}^\top$  gegeben durch  $\bar{\varphi} \mapsto \bar{c} \circ \varphi$  in den Notationen 4.1.12.33, mit  $\bar{c} : \mathbb{C} \rightarrow \mathbb{C}$  der komplexen Konjugation. Diese Identifikation scheint mir so kanonisch, daß ich auch oft  $\bar{\varphi}$  statt  $\bar{c} \circ \varphi$  schreiben werde.

*Ergänzung 4.7.4.23 (Dualraum und Restriktion der Skalare).* Gegeben ein komplexer Vektorraum  $V$  erklären wir einen natürlichen Isomorphismus

$$\text{res}_{\mathbb{C}}^{\mathbb{R}}(V^\top) \xrightarrow{\sim} (\text{res}_{\mathbb{C}}^{\mathbb{R}} V)^\top$$

zwischen der Reellifizierung seines Dualraums und dem Dualraum seiner Reellifizierung durch die Vorschrift  $\lambda \mapsto 2\text{Re}\lambda$ . Es kommutiert dann das Diagramm

$$\begin{array}{ccccc} \mathbb{C} \otimes_{\mathbb{R}} \text{res}_{\mathbb{C}}^{\mathbb{R}}(V^\top) & \xrightarrow{\sim} & \mathbb{C} \otimes_{\mathbb{R}} (\text{res}_{\mathbb{C}}^{\mathbb{R}} V)^\top & \xrightarrow{\sim} & (\mathbb{C} \otimes_{\mathbb{R}} \text{res}_{\mathbb{C}}^{\mathbb{R}} V)^\top \\ i_{V^\top} \downarrow \wr & & & & \wr i_V^\top \\ V^\top \oplus \overline{V^\top} & \xrightarrow{\sim} & V^\top \oplus \overline{V^\top} & & \end{array}$$

Hier kommen die Vertikalen von 4.7.4.21 her, unten ist die von 4.7.4.22 gelieferte Abbildung  $(\lambda, \bar{\mu}) \mapsto (\lambda, \bar{c} \circ \mu)$  gemeint mit  $\bar{c} : \mathbb{C} \rightarrow \mathbb{C}$  der komplexen Konjugation, und in der oberen Horizontale die Abbildung, die aus obiger Identifikation  $\text{res}_{\mathbb{C}}^{\mathbb{R}}(V^\top) \xrightarrow{\sim} (\text{res}_{\mathbb{C}}^{\mathbb{R}} V)^\top$  unter der Komplexifikation entsteht, gefolgt von der Identifikation  $(W^\top)_{\mathbb{C}} \xrightarrow{\sim} (W_{\mathbb{C}})^\top$  aus 4.6.1.42. Der Faktor 2 zu Beginn scheint mir nicht nur angemessen, da er obiges Diagramm zum Kommutieren bringt, sondern auch, da man allgemeiner für jede „endliche separable Körpererweiterung“ vermutlicherweise einen natürlichen Isomorphismus  $\text{res}_K^k(V^\top) \xrightarrow{\sim} (\text{res}_K^k V)^\top$  erklärt durch die Vorschrift  $\lambda \mapsto S_K^k \circ \lambda$  mit  $S_K^k : K \rightarrow k$  der Spur aus ??.

*Ergänzende Übung 4.7.4.24.* Gegeben ein Körper  $K$  erhalten wir eine Isotransformation von Funktoren  $\text{Mod}_K \times \text{Mod}_K \rightarrow \text{Mod}_K$  vermittels der durch das Dachprodukt gegebenen Abbildungen

$$\bigoplus_{i+j=k} \bigwedge^i V \otimes \bigwedge^j W \xrightarrow{\sim} \bigwedge^k (V \oplus W)$$

Zusammen mit Übung 4.7.4.21 erhalten wir insbesondere Isotransformationen von Funktoren  $\text{Mod}_{\mathbb{C}} \rightarrow \text{Mod}_{\mathbb{C}}$  alias für komplexe Vektorräume  $V$  kanonische Isomorphismen  $\bigoplus_{i+j=k} \bigwedge^i V \otimes \bigwedge^j \overline{V} \xrightarrow{\sim} \bigwedge^k (\mathbb{C} \otimes_{\mathbb{R}} V)$ .

*Ergänzende Übung 4.7.4.25.* Gegeben Funktoren  $F, F' : \mathcal{A} \rightarrow \mathcal{B}$  und  $G, G' : \mathcal{B} \rightarrow \mathcal{C}$  sowie Transformationen  $\alpha : F \Rightarrow F'$  und  $\beta : G \Rightarrow G'$  gilt die Gleichheit  $\beta F' \circ G\alpha = G'\alpha \circ \beta F$  von Transformationen  $GF \Rightarrow G'F'$ . Wir notieren diese Transformation auch  $\alpha * \beta : GF \Rightarrow G'F'$  und nennen sie die **Juxtaposition** unserer beiden Transformationen. Unsere Identität ist auch gleichbedeutend zu der Aussage, daß das Nachschalten einen Funktor  $\text{Cat}(\mathcal{B}, \mathcal{C}) \rightarrow \text{Cat}(\mathcal{B}^{\mathcal{A}}, \mathcal{C}^{\mathcal{A}})$  liefert, oder auch in ausführlicherer Notation das Vorschalten einen Funktor

$$\text{Cat}(\mathcal{A}, \mathcal{B}) \rightarrow \text{Cat}(\text{Cat}(\mathcal{B}, \mathcal{C}), \text{Cat}(\mathcal{A}, \mathcal{C}))$$

*Übung 4.7.4.26.* Man zeige: Ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  ist genau dann eine Äquivalenz von Kategorien, wenn es eine Äquivalenz von Kategorien in die Gegenrichtung  $G : \mathcal{B} \rightarrow \mathcal{A}$  gibt nebst einer Isotransformation  $\tau : \text{Id}_{\mathcal{A}} \xrightarrow{\sim} GF$ . Die Äquivalenz  $G$  oder genauer das Paar  $(G, \tau)$  heißt dann ein **quasiinverser Funktor zu  $F$** . Man zeige weiter: Zu jedem Paar  $(G, \tau)$  wie eben gibt es genau eine Isotransformation  $\eta : FG \xrightarrow{\sim} \text{Id}_{\mathcal{A}}$  mit  $(\eta F) \circ (F\tau) = \text{id}_F$ .

*Übung 4.7.4.27.* Man zeige: Genau dann ist ein Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  eine Äquivalenz von Kategorien, wenn es einen Funktor  $G : \mathcal{B} \rightarrow \mathcal{A}$  gibt derart, daß  $FG$  isomorph ist zum Identitätsfunktor auf  $\mathcal{B}$  und  $GF$  isomorph zum Identitätsfunktor auf  $\mathcal{A}$ .

*Übung 4.7.4.28.* Man zeige: Gegeben eine Äquivalenz von Kategorien  $F : \mathcal{A} \xrightarrow{\sim} \mathcal{B}$  und ein Funktor  $G : \mathcal{B} \rightarrow \mathcal{A}$  nebst einer Isotransformation  $\tau : FG \xrightarrow{\sim} \text{Id}_{\mathcal{A}}$  ist auch  $G$  eine Äquivalenz von Kategorien und  $(G, \tau)$  quasiinvers zu  $F$ .

*Übung 4.7.4.29 (Äquivalenzen von Funktorkategorien).* Sind  $\mathcal{A}, \mathcal{B}$  Kategorien und ist  $K : \mathcal{A}' \xrightarrow{\sim} \mathcal{A}$  eine Äquivalenz von Kategorien, so liefert das Vorschalten von  $K$  eine Äquivalenz von Funktorkategorien

$$\text{Cat}(\mathcal{A}, \mathcal{B}) \xrightarrow{\sim} \text{Cat}(\mathcal{A}', \mathcal{B})$$

Ist ähnlich  $H : \mathcal{B} \xrightarrow{\sim} \mathcal{B}'$  eine Äquivalenz von Kategorien, so liefert das Nachschalten von  $H$  eine Äquivalenz von Funktorkategorien

$$\text{Cat}(\mathcal{A}, \mathcal{B}) \xrightarrow{\sim} \text{Cat}(\mathcal{A}, \mathcal{B}')$$

## 4.7.5 Natürliche Konstruktionen in der Geometrie

**4.7.5.1 (Kanonische Skalarprodukte als Transformationen).** Wir interessieren uns nun für die Kategorie  $\text{Euk}$  der euklidischen Vektorräume und für Funktoren

$$\text{Euk} \rightarrow \text{Mod}_{\mathbb{R}}$$

Beispiele sind das Vergessen der euklidischen Struktur verg oder das Bilden der Längengerade  $\mathbb{L}$  oder Tensorpotenzen dieser Funktoren wie etwa  $\text{verg}^{\otimes r}$  oder  $\mathbb{L}^{\otimes r}$ . Unsere kanonischen Skalarprodukte sind Transformationen

$$\text{verg}^{\otimes 2} \Rightarrow \mathbb{L}^{\otimes 2}$$

von Funktoren alias Morphismen in der Funktorkategorie  $\text{Cat}(\text{Euk}, \text{Mod}_{\mathbb{R}})$ .

**4.7.5.2 (Kanonische Skalarprodukte brauchen Einheiten).** Wir betrachten den konstanten Funktor  $C_{\mathbb{R}} : \text{Euk} \rightarrow \text{Mod}_{\mathbb{R}}$ , der jedem euklidischen Vektorraum den

reellen Vektorraum  $\mathbb{R}$  zuordnet und jeder euklidischen linearen Abbildung die Identität. Wir zeigen, daß es außer der Nulltransformation keine Transformation

$$\text{verg}^{\otimes 2} \Rightarrow C_{\mathbb{R}}$$

gibt. In der Tat ist die Multiplikation mit jeder reellen Zahl  $\lambda \neq 0$  für jeden euklidischen Vektorraum  $V$  eine euklidische Abbildung  $(\lambda \cdot) : V \rightarrow V$  und jede bilineare Abbildung  $\eta : V \times V \rightarrow C_{\mathbb{R}}$  mit  $\eta(v, w) = \eta(\lambda v, \lambda w) \forall \lambda \in \mathbb{R}^\times$  ist offensichtlich Null. Salopp gesprochen gibt es also „kein kanonisches Skalarprodukt auf euklidischen Räumen mit Werten in den reellen Zahlen“.

**4.7.5.3 (Kanonische Spatprodukte als Transformation).** Nun halten wir  $n \in \mathbb{N}_{>0}$  fest und interessieren uns für die Kategorie  $\text{Euk}_n$  der  $n$ -dimensionalen euklidischen Vektorräume und die Funktorkategorie  $\text{Cat}(\text{Euk}_n, \text{Mod}_{\mathbb{R}})$ . Zu dieser Funktorkategorie gehören etwa die Funktoren  $\text{verg}^{\otimes n} : V \mapsto V^{\otimes n}$  und  $\text{or}_{\mathbb{R}} \otimes \mathbb{L}^{\otimes n} : V \mapsto \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)^{\otimes n}$  und eine Transformation  $\tau : \text{verg}^{\otimes n} \Rightarrow \text{or}_{\mathbb{R}} \otimes \mathbb{L}^{\otimes n}$  wird gegeben wird durch die Gesamtheit der in 4.6.4.3 konstruierten linearen Abbildungen  $\tau_V : V^{\otimes n} \rightarrow \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)^{\otimes n}$  und im Fall  $n = 3$  speziell durch unsere kanonischen Spatprodukte

$$\langle , , \rangle : V^{\otimes 3} \rightarrow \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)^{\otimes 3}$$

Man überzeugt sich unschwer, daß wir auf diese Weise sogar für jedes  $n$  eine Isotransformation  $\tau : \bigwedge^n \text{verg} \Rightarrow \text{or}_{\mathbb{R}} \otimes \mathbb{L}^{\otimes n}$  erhalten.

**4.7.5.4 (Kanonische Kreuzprodukte als Transformation).** Das Kreuzprodukt ist eine Transformation  $\times : \text{verg}^{\otimes 2} \Rightarrow \text{verg} \otimes \text{or}_{\mathbb{R}} \otimes \mathbb{L}$  alias ein Morphismus in der Funktorkategorie  $\text{Cat}(\text{Euk}_3, \text{Mod}_{\mathbb{R}})$ , der gegeben wird durch die in 4.6.4.9 konstruierten Morphismen

$$\times : V \otimes V \rightarrow V \otimes \text{or}_{\mathbb{R}}(V) \otimes \mathbb{L}(V)$$

**4.7.5.5 (Klassifikationsfragen und Gruppenhomomorphismen).** Um die Funktorkategorie  $\text{Cat}(\text{Euk}_n, \text{Mod}_{\mathbb{R}})$  für vorgegebenes  $n$  besser zu verstehen, mag man von der Erkenntnis ausgehen, daß in der Kategorie  $\text{Euk}_n$  der  $n$ -dimensionalen euklidischen Vektorräume je zwei Objekte isomorph sind und nach 4.7.2.31 folglich der Einbettungsfunktor eine Äquivalenz

$$[\text{Euk}(\mathbb{R}^n)] \xrightarrow{\sim} \text{Euk}_n$$

ist. Die Automorphismengruppe des  $\mathbb{R}^n$  mit seiner Standardstruktur als euklidischer Raum ist nun die Gruppe  $\text{GO}(n) := \mathbb{R}^\times \text{O}(n) = \text{Euk}(\mathbb{R}^n)$  aller seiner **linearen Ähnlichkeiten**. Wir können so unsere Äquivalenz von oben umschreiben zu einer Äquivalenz  $[\text{GO}(n)] \xrightarrow{\sim} \text{Euk}_n$ . Bezeichnet andererseits  $\text{Mod}_{\mathbb{R}}^{d-\dim}$  die

Kategorie der  $d$ -dimensionalen reellen Vektorräume, so erhalten wir ebenso eine Äquivalenz  $[\mathrm{Mat}_{\mathbb{R}}(d)] \xrightarrow{\sim} \mathrm{Mod}_{\mathbb{R}}^{d\text{-dim}}$ . Weil nach 4.7.4.29 Äquivalenzen von Kategorien Äquivalenzen von Funktorkategorien induzieren, erhalten wir so Äquivalenzen von Kategorien

$$\mathrm{Cat}(\mathrm{Euk}_n, \mathrm{Mod}_{\mathbb{R}}^{d\text{-dim}}) \xrightarrow{\sim} \mathrm{Cat}([\mathrm{GO}(n)], \mathrm{Mod}_{\mathbb{R}}^{d\text{-dim}}) \xleftarrow{\sim} \mathrm{Cat}([\mathrm{GO}(n)], [\mathrm{Mat}_{\mathbb{R}}(d)])$$

und damit nach 4.7.2.28 Bijektionen zwischen den jeweiligen Mengen von Isomorphieklassen. Objekte von  $\mathrm{Cat}([\mathrm{GO}(n)], [\mathrm{Mat}_{\mathbb{R}}(d)])$  sind nun Monoidhomomorphismen  $\mathrm{GO}(n) \rightarrow \mathrm{Mat}_{\mathbb{R}}(d)$  alias Gruppenhomomorphismen  $\mathrm{GO}(n) \rightarrow \mathrm{GL}(d; \mathbb{R})$ , und zwei solche Gruppenhomomorphismen  $\phi, \psi$  sind isomorphe Objekte genau dann, wenn es  $A \in \mathrm{GL}(d; \mathbb{R})$  gibt mit  $(\mathrm{int} A) \circ \phi = \psi$ . So erkennen wir zum Beispiel, daß Funktoren, die jedem  $n$ -dimensionalen euklidischen Vektorraum einen eindimensionalen Vektorraum zuordnen, klassifiziert werden durch die Menge aller Gruppenhomomorphismen  $\mathrm{GO}(n) \rightarrow \mathbb{R}^{\times}$ . Die folgende Tabelle gibt einige Beispiele für solche Funktoren in die Kategorie der eindimensionalen reellen Vektorräume und die zugehörigen Gruppenhomomorphismen.

| Funktoren           | $\mathrm{Euk}_n \rightarrow \mathrm{Mod}_{\mathbb{R}}^{1\text{-dim}}$ | Morphismen   | $\mathrm{GO}(n) \rightarrow \mathbb{R}^{\times}$ |
|---------------------|---|--------------|--|
| konstanter Funktor  | $C_{\mathbb{R}}$  | konstanter   | 1  |
| Maximalpotenz       | $\wedge^n$  | Determinante | $\det$   |
| Orientierungsgerade | $\mathrm{or}_{\mathbb{R}}$  |              | $\det /  \det $                                  |
| Längengerade        | $\mathbb{L}$  |              | $\sqrt[n]{ \det }$                               |

## Übungen

*Ergänzende Übung 4.7.5.6.* Gibt es für zweidimensionale euklidische Vektorräume  $V$  nichttriviale natürliche Gruppenhomomorphismen  $\mathrm{or}_{\mathbb{R}}(V) \rightarrow \mathrm{O}(V)$  von der Orientierungsgerade in die orthogonale Gruppe?

### 4.7.6 Köcher\*

4.7.6.1. Der Begriff einer Transformation ist in noch größerer Allgemeinheit natürlich und sinnvoll, wie hier kurz skizziert werden soll.

**Definition 4.7.6.2.** Ein **Köcher** ist ein Datum  $\mathcal{Q} = (P, E, a, e)$  bestehend aus zwei Mengen  $P, E$  und zwei Abbildungen  $a, e : P \rightarrow E$ . Wir nennen die Elemente von  $E$  die **Ecken** oder auch **Punkte** des Köchers und die Elemente von  $P$  seine **Pfeile**. Für einen Pfeil  $\vec{p} \in P$  nennen wir  $a(\vec{p})$  seinen **Anfangspunkt** und  $e(\vec{p})$

seinen **Endpunkt**. Ein **Morphismus**  $F$  von unserem Köcher in einen weiteren Köcher  $(P', E', a', e')$  ist ein Paar bestehend aus einer Abbildung  $F : P \rightarrow P'$  und einer Abbildung  $F : E \rightarrow E'$  derart, daß gilt  $Fa = a'F$  und  $Fe = e'F$ . Wir erhalten so die Kategorie der Köcher

Car

Ähnlich wie bei Kategorien schreiben wir auch gerne abkürzend  $\mathcal{Q}$  für die Eckenmenge eines Köchers  $\mathcal{Q} = (P, E, a, e)$  und  $\mathcal{Q}(x, y)$  für die Menge der Pfeile mit Anfangspunkt  $x$  und Endpunkt  $y$ .

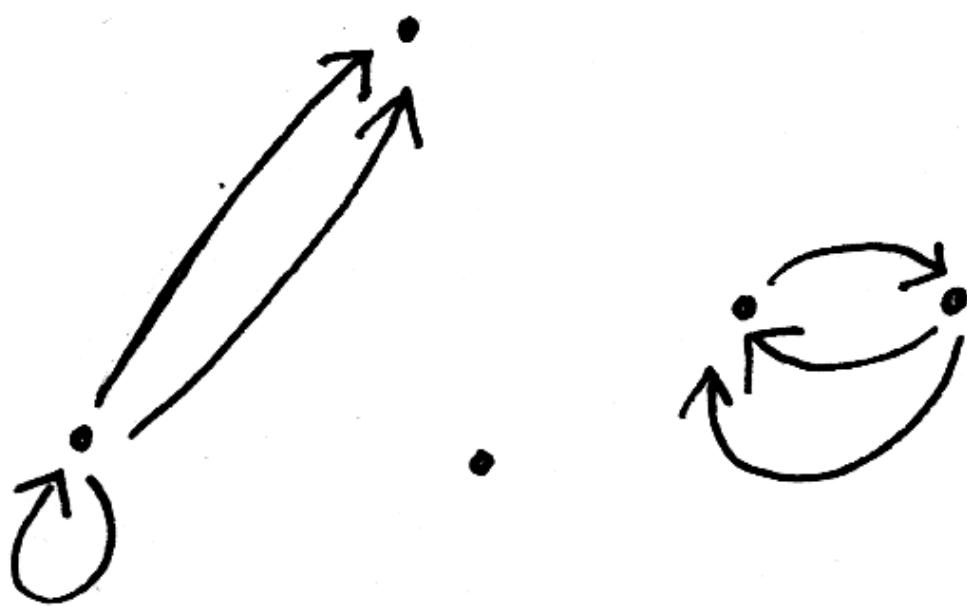
4.7.6.3. Auf Englisch sagt man **quiver**, auf Französisch **carquois**. Auf Englisch heißen die Ecken **vertices** und die Pfeile **arrows** oder **edges**.

4.7.6.4. Jede Kategorie liefert einen Köcher, mit den Objekten als Ecken und den Morphismen als Pfeilen. Zu jeder Menge  $\Omega$  bilden wir den **Ein-Punkt-Köcher**  $[\Omega]$ , mit nur einem Punkt  $*$  und für jedes  $\omega \in \Omega$  einem Pfeil von diesem Punkt zu sich selbst. Ein Köcher heißt **endlich**, wenn er nur endlich viele Punkte und Pfeile hat. Manche Autoren nennen einen Köcher auch ein **Diagrammschema**. Ein Köchermorphismus von einem Köcher in eine Kategorie heißt eine **Darstellung unseres Köchers** in besagter Kategorie oder auch eine **Realisierung unseres Diagrammschemas** in besagter Kategorie oder, wenn wir auf das zugrundeliegende Diagrammschema nicht Bezug nehmen wollen, ein **Diagramm** in besagter Kategorie.

*Ergänzung 4.7.6.5.* Bezeichne  $\Rightarrow$  die Kategorie mit zwei Objekten Pf, Ec und vier Morphismen, von denen Zwei die Identitäten sind und Zwei von Pf nach Ec gehen und „Anfang“ und „Ziel“ heißen mögen. Dann kann die Kategorie der Köcher verstanden werden als die Funktorkategorie  $\text{Cat}(\Rightarrow, \text{Ens})$ .

*Ergänzung 4.7.6.6.* Eine **Verknüpfung auf einem Köcher**  $\mathcal{Q}$  ist eine Sammlung von Abbildungen  $\mathcal{Q}(x, y) \times \mathcal{Q}(y, z) \rightarrow \mathcal{Q}(x, z)$  für alle  $x, y, z \in \mathcal{Q}$ . Einen Köcher mit Verknüpfung nennen wir auch einen **Magmaoid**. Ein **Morphismus von Magmaoiden** ist ein Köchermorphismus, der mit den jeweiligen Verknüpfungen verträglich ist. Eine Kategorie ist in dieser Terminologie Magmaoid, das noch zusätzliche Eigenschaften hat, die man „Assoziativität“ und „Existenz von Identitätspfeilen“ nennen mag und die wir zur Bedingung **unitärassoziativ** zusammenfassen.

**Definition 4.7.6.7.** Seien  $\mathcal{Q}$  ein Köcher,  $\mathcal{B}$  eine Kategorie und  $F, G : \mathcal{Q} \rightarrow \mathcal{B}$  Köchermorphismen. Eine **Transformation**  $\tau : F \Rightarrow G$  ist eine Vorschrift, die jeder Ecke  $x \in \mathcal{Q}$  einen Morphismus  $\tau_x \in \mathcal{B}(F(x), G(x))$  zuordnet derart, daß



Veranschaulichung eines endlichen Köchers mit 5 Ecken und 6 Pfeilen.

für jeden Pfeil  $\vec{p} : x \rightarrow y$  in unserem Köcher  $\mathcal{Q}$  das Diagramm

$$\begin{array}{ccc} F(x) & \xrightarrow{\tau_x} & G(x) \\ F(\vec{p}) \downarrow & & \downarrow G(\vec{p}) \\ F(y) & \xrightarrow{\tau_y} & G(y) \end{array}$$

in unserer Kategorie  $\mathcal{B}$  kommutiert. Sind alle  $\tau_x$  Isomorphismen, so heißt  $\tau$  eine **Isotransformation**. Die Menge aller Transformationen bezeichnen wir mit  $\text{Car}(\mathcal{Q}, \mathcal{B})(F, G)$  oder  $\text{Trans}_{\mathcal{Q} \rightarrow \mathcal{B}}(F, G)$  oder abkürzend mit  $\text{Trans}_{\mathcal{Q}}(F, G)$  oder auch nur mit  $\text{Trans}(F, G)$ .

4.7.6.8. Wie in 4.7.4.12 die Funktoren bilden für jeden Köcher  $\mathcal{Q}$  und jede Kategorie  $\mathcal{C}$  die Köchermorphismen  $\mathcal{Q} \rightarrow \mathcal{C}$  die Objekte einer Kategorie  $\text{Car}(\mathcal{Q}, \mathcal{C})$  mit Transformationen als Morphismen.

*Beispiel 4.7.6.9.* Seien  $K$  ein Körper und  $\downarrow$  der Köcher mit zwei Punkten und einem Pfeil vom einen zum anderen. Die Isomorphieklassen in der Kategorie von Köchermorphismen  $\text{Car}(\downarrow, \text{Modf}_K)$  werden durch die Theorie der Smith-Normalform 3.2.5.7 bestimmt: Die Dimensionen der beiden beteiligten Vektorräume sowie der Rang der linearen Abbildung legen eine Darstellung dieses Köchers in endlichdimensionalen Vektorräumen bereits bis auf Isomorphie eindeutig fest.

*Beispiel 4.7.6.10.* Seien  $K$  ein Körper und  $\circlearrowleft$  der Köcher mit einem Punkt und einem Pfeil von diesem Punkt zu sich selber. Die Isomorphieklassen in der Kategorie  $\text{Car}(\circlearrowleft, \text{Modf}_K)$  werden zumindest im Fall eines algebraisch abgeschlossenen Körpers  $K$  bestimmt durch die Theorie der Jordan'schen Normalform 4.3.4.5.

## Übungen

*Übung 4.7.6.11.* Seien  $\mathcal{A}, \mathcal{A}'$  Köcher und  $\mathcal{B}, \mathcal{B}'$  Kategorien. Ist  $K : \mathcal{A}' \xrightarrow{\sim} \mathcal{A}$  ein Isomorphismus von Köchern, so liefert das Vorschalten von  $K$  einen Isomorphismus von Kategorien

$$\text{Car}(\mathcal{A}, \mathcal{B}) \xrightarrow{\sim} \text{Car}(\mathcal{A}', \mathcal{B})$$

Ist ähnlich  $H : \mathcal{B} \xrightarrow{\sim} \mathcal{B}'$  eine Äquivalenz von Kategorien, so liefert das Nachschalten von  $H$  eine Äquivalenz von Kategorien

$$\text{Car}(\mathcal{A}, \mathcal{B}) \xrightarrow{\sim} \text{Car}(\mathcal{A}, \mathcal{B}')$$

*Übung 4.7.6.12.* Seien  $\mathcal{C}$  und  $\mathcal{Q}$  Köcher und  $F : \mathcal{C} \rightarrow \mathcal{Q}$  ein Köchermorphismus, der für je zwei Ecken  $x, y \in \mathcal{C}$  eine Surjektion  $\mathcal{C}(x, y) \twoheadrightarrow \mathcal{Q}(x, y)$  induziert. Gegeben eine Verknüpfung auf  $\mathcal{C}$  gibt es höchstens eine Verknüpfung auf  $\mathcal{Q}$  derart, daß

$F$  ein Morphismus von Magmaiden wird. Wenn es solch eine Verknüpfung gibt, heißt unser Köchermorphismus **angepaßt an die Verknüpfung** und die fragliche Verknüpfung auf  $\mathcal{Q}$  die **auf  $\mathcal{Q}$  koinduzierte Verknüpfung**. Ist unser Magmaoid  $\mathcal{C}$  eine Kategorie, so auch der Köcher  $\mathcal{Q}$  mit der koinduzierten Verknüpfung.

### 4.7.7 Produkte und Koprodukte in Kategorien

**Definition 4.7.7.1.** Seien  $\mathcal{C}$  eine Kategorie und  $X, Y$  Objekte von  $\mathcal{C}$ . Ein **Produkt** von  $X$  und  $Y$  ist ein Datum  $(P, p, q)$  bestehend aus (1) einem Objekt  $P \in \mathcal{C}$  und (2) Morphismen  $p : P \rightarrow X$  und  $q : P \rightarrow Y$ , den sogenannten **Projektionen**, derart daß gilt: Ist  $Z \in \mathcal{C}$  ein Objekt und sind  $a : Z \rightarrow X$ ,  $b : Z \rightarrow Y$  Morphismen, so gibt es genau einen Morphismus  $c : Z \rightarrow P$  mit  $p \circ c = a$  und  $q \circ c = b$ . Wir notieren diesen Morphismus dann  $c = (a, b)$  oder, ganz pedantisch und wenn wir ihn von den Morphismen aus einem Koprodukt absetzen wollen, als Spalte  $c = (a, b)^\top$ .

*Beispiele 4.7.7.2.* In der Kategorie der Mengen ist das sogenannte kartesische Produkt  $P = X \times Y$  mit  $p, q$  den üblichen Projektionsabbildungen ein Produkt von  $X$  und  $Y$ . Analoges gilt in der Kategorie der Vektorräume, der Gruppen, der Ringe, der Monoide, der abelschen Gruppen, und vielen weiteren Strukturen der Bauart „Menge mit ausgezeichneten Verknüpfungen und speziellen Elementen“.

**4.7.7.3 (Eindeutigkeit von Produkten).** Produkte in Kategorien sind im wesentlichen eindeutig, falls sie existieren. Sind genauer  $(P, p, q)$  und  $(\tilde{P}, \tilde{p}, \tilde{q})$  zwei mögliche Produkte der Objekte  $X$  und  $Y$ , so gibt es aufgrund der universellen Eigenschaft von  $P$  genau ein  $c : \tilde{P} \rightarrow P$  mit  $p \circ c = \tilde{p}$  und  $q \circ c = \tilde{q}$  und ebenso genau ein  $d : P \rightarrow \tilde{P}$  mit  $\tilde{p} \circ d = p$  und  $\tilde{q} \circ d = q$ . Weiter gibt es auch genau ein  $f : P \rightarrow \tilde{P}$  mit  $p \circ f = \tilde{p}$  und  $q \circ f = \tilde{q}$ , und da sowohl  $f = \text{id}$  als auch  $f = c \circ d$  diese Bedingung erfüllen, folgt  $c \circ d = \text{id}$ . Ebenso erhalten wir  $d \circ c = \text{id}$ , mithin sind  $c$  und  $d$  zueinander inverse Isomorphismen. Aufgrund dieser Eindeutigkeit sprechen wir ab jetzt meist von *dem* Produkt und notieren es

$$(X \times Y, \text{pr}_X, \text{pr}_Y)$$

oder auch noch ausführlicher  $X \times^{\mathcal{C}} Y$ . Morphismen in das Produkt schreiben wir auch  $(a, b)$ . Sind schließlich Morphismen  $f : X \rightarrow X'$ ,  $g : Y \rightarrow Y'$  gegeben und existieren die Produkte  $X \times Y$  und  $X' \times Y'$ , so benutzen wir die Abkürzung  $(f \circ \text{pr}_X, g \circ \text{pr}_Y) = f \times g$  und nennen diesen Morphismus den **Produktmorphmus**

$$f \times g : X \times Y \rightarrow X' \times Y'$$

**Definition 4.7.7.4.** Sei  $F : \mathcal{A} \rightarrow \mathcal{B}$  ein Funktor. Sind in  $\mathcal{A}$  Morphismen  $p : P \rightarrow X$  und  $q : P \rightarrow Y$  gegeben, so erhalten wir Morphismen  $Fp : FP \rightarrow FX$  und

$Fq : FP \rightarrow FY$  in  $\mathcal{B}$ . Wenn das Produkt  $FX \times FY$  existiert, erhalten wir so auch einen Morphismus  $(Fp, Fq) : FP \rightarrow FX \times FY$ . Wenn schließlich auch das Produkt  $X \times Y$  existiert, so erhalten wir, indem wir es als unser  $P$  nehmen, in unserer ausführlichen Notation einen natürlichen Morphismus

$$F(X \times^{\mathcal{A}} Y) \rightarrow FX \times^{\mathcal{B}} FY$$

4.7.7.5. Der Morphismus von eben muß im allgemeinen kein Isomorphismus sein. Im Fall des Vergißfunktors von Vektorräumen über einem vorgegebenen Körper zu Mengen ist er jedoch stets ein Isomorphismus von Mengen alias eine bijektive Abbildung.

4.7.7.6. Produkte können auch für allgemeine Familien von Objekten ein- und derselben Kategorie erklärt werden, wie im folgenden ausgeführt werden soll. Wir besprechen dies Konzept zunächst im Fall der Kategorie der Mengen.

4.7.7.7 (**Produkte von Mengen, Variante**). Allgemeiner als in 3.1.3.1 diskutiert kann man auch für eine beliebige Familie von Mengen  $(X_i)_{i \in I}$  eine neue Menge bilden als die Menge aller Tupel  $(x_i)_{i \in I}$  mit  $x_i \in X_i$  für alle  $i \in I$ . Diese **Produktmenge** notiert man

$$\prod_{i \in I} X_i$$

und die Projektionsabbildungen werden mit  $\text{pr}_j : \prod_{i \in I} X_i \rightarrow X_j$  oder ähnlich bezeichnet. Wieder können wir für beliebige Abbildungen  $f_i : Z \rightarrow X_i$  eine Abbildung  $f = (f_i)_{i \in I} : Z \rightarrow \prod_{i \in I} X_i$  definieren durch die Vorschrift  $f(z) = (f_i(z))_{i \in I}$  und jede Abbildung von einer Menge  $Z$  in ein Produkt ist von dieser Form mit  $f_i = \text{pr}_i \circ f$ . In Formeln ausgedrückt liefert das Nachschalten der Projektionen also für jede Menge  $Z$  eine Bijektion

$$\begin{array}{ccc} \text{Ens}(Z, \prod_{i \in I} X_i) & \xrightarrow{\sim} & \prod_{i \in I} \text{Ens}(Z, X_i) \\ f & \mapsto & (\text{pr}_i \circ f) \end{array}$$

**Definition 4.7.7.8.** Seien  $\mathcal{C}$  eine Kategorie und  $(X_i)_{i \in I}$  eine Familie von Objekten von  $\mathcal{C}$ . Ein **Produkt** der  $X_i$  ist ein Datum  $(P, (p_i)_{i \in I})$  bestehend aus (1) einem Objekt  $P \in \mathcal{C}$  und (2) Morphismen  $p_i : P \rightarrow X_i$ , den sogenannten **Projektionen**, derart daß gilt: Ist  $Y \in \mathcal{C}$  ein Objekt und sind  $q_i : Y \rightarrow X_i$  Morphismen, so gibt es genau einen Morphismus  $q : Y \rightarrow P$  mit  $p_i \circ q = q_i \forall i \in I$ . Wir notieren diesen Morphismus dann  $q = (q_i)_{i \in I}$  oder ganz pedantisch auch schon mal  $q = (q_i)_{i \in I}^\top$ .

*Beispiele 4.7.7.9.* In der Kategorie der Mengen ist  $P = \prod_{i \in I} X_i$  mit  $p_i$  den üblichen Projektionsabbildungen ein Produkt der  $X_i$ . Produkte in der Kategorie der Vektorräume diskutieren wir in 4.7.8.4.

**Beispiel 4.7.7.10 (Nichtexistenz übergroßer Produkte in  $\mathfrak{U}\text{Ens}$ ).** Wählen wir ein Mengensystem  $\mathfrak{U}$  und betrachten präziser die Kategorie  $\mathfrak{U}\text{Ens}$  der Mengen aus  $\mathfrak{U}$ , so wird es im allgemeinen beliebige durch eine Menge  $I$  indizierte Produkte in  $\mathfrak{U}\text{Ens}$  nicht geben. Enthält zum Beispiel  $\mathfrak{U}$  eine Menge  $Z$  mit mindestens zwei Elementen, so überlegt man sich leicht, daß etwa ein Produkt  $\prod_{i \in \mathfrak{U}} Z$  in  $\mathfrak{U}\text{Ens}$  nicht existieren kann.

**Beispiel 4.7.7.11 (Nichtexistenz übergroßer Produkte im allgemeinen).** Ist allgemein  $\mathcal{C}$  eine Kategorie und  $I := \bigsqcup_{X, Y \in \mathcal{C}} \mathcal{C}(X, Y)$  die Menge der Morphismen von  $\mathcal{C}$  und gibt es Objekte  $Z, W$  mit mindestens zwei Morphismen  $|\mathcal{C}(Z, W)| \geq 2$ , so kann das Produkt  $P := \prod_{i \in I} W$  in  $\mathcal{C}$  nicht existieren, da wir  $|\mathcal{C}(Z, P)| \geq |\mathcal{P}(I)|$  hätten und die Kardinalität der Menge aller Morphismen in ganz  $\mathcal{C}$  nach Annahme  $|I|$  ist und da stets gilt  $|I| < |\mathcal{P}(I)|$ .

**4.7.7.12 (Eindeutigkeit von Produkten, Variante).** Produkte in Kategorien sind im wesentlichen eindeutig, falls sie existieren. Sind genauer  $(P, (p_i))$  und  $(\tilde{P}, (\tilde{p}_i))$  zwei mögliche Produkte der Objekte  $X_i$ , so gibt es aufgrund der universellen Eigenschaft von  $P$  genau ein  $\tilde{p} : \tilde{P} \rightarrow P$  mit  $p_i \circ \tilde{p} = \tilde{p}_i$  und ebenso genau ein  $p : P \rightarrow \tilde{P}$  mit  $\tilde{p}_i \circ p = p_i$ . Weiter gibt es auch genau ein  $f : P \rightarrow P$  mit  $p_i \circ f = p_i$ , und da sowohl  $f = \text{id}$  als auch  $f = \tilde{p} \circ p$  diese Bedingung erfüllen, folgt  $\tilde{p} \circ p = \text{id}$ . Ebenso erhalten wir  $p \circ \tilde{p} = \text{id}$ , mithin sind  $p$  und  $\tilde{p}$  zueinander inverse Isomorphismen. Aufgrund dieser Eindeutigkeit sprechen wir ab jetzt meist von *dem* Produkt und notieren es

$$\left( \prod_{i \in I} X_i, (\text{pr}_i)_{i \in I} \right)$$

oder  $\prod^{\mathcal{C}}$ , wenn wir auch noch die Kategorie  $\mathcal{C}$  spezifizieren wollen, oder im Fall endlicher angeordneter Familien  $X_1 \times \dots \times X_n$  und benutzen für die Projektionen manchmal auch die Notation  $\text{pr}_{X_i}$ . Morphismen in das Produkt schreiben wir im Fall endlicher angeordneter Familien auch  $(q_1, \dots, q_n)$  oder ganz pedantisch als Spalte  $(q_1, \dots, q_n)^{\top}$ .

**4.7.7.13 (Umindizierung).** Die Frage der Abhängigkeit eines Produkts von der Wahl der Indexmenge ist subtiler als es auf den ersten Blick scheinen mag. Natürlich liefert jede Umindizierung mittels einer Bijektion zwischen der Indexmenge und einer weiteren Menge einen ausgezeichneten Isomorphismus zwischen den jeweiligen Produkten. Jedoch liefert die Umindizierung mittels einer Permutation der Indexmenge im allgemeinen nicht die Identität auf dem jeweiligen Produkt.

**4.7.7.14 (Produkte über leere Familien).** Das Produkt über eine leere Familie von Mengen erklärt man als „die“ einpunktige Menge. Damit wird das Bilden von Produkten von Mengen „assoziativ“ in der Weise, daß wir bei einer Familie

$(I_j)_{j \in J}$  von Indexmengen mit disjunkter Vereinigung  $I = \bigsqcup_j I_j$  stets eine kanonische Bijektion

$$\prod_{i \in I} X_i \xrightarrow{\sim} \prod_{j \in J} \left( \prod_{i \in I_j} X_i \right)$$

haben. Das Produkt über eine leere Familie in einer beliebigen Kategorie  $\mathcal{C}$  verstehen wir analog als „das“ finale Objekt, da dann die offensichtliche Abbildung auch in diesem Fall Bijektionen  $\mathcal{C}(Y, \prod_{i \in I} X_i) \xrightarrow{\sim} \prod_{i \in I} \mathcal{C}(Y, X_i)$  liefert. Wenn wir sagen, eine Kategorie **habe endliche Produkte**, so meinen wir stets implizit, daß auch die Existenz eines finalen Objekts mit gefordert sein soll.

4.7.7.15. Produkte in der opponierten Kategorie heißen „Koprodukte“. Im folgenden schreiben wir das aus.

**Definition 4.7.7.16.** Sei  $\mathcal{C}$  eine Kategorie und  $(X_i)_{i \in I}$  eine Familie von Objekten aus  $\mathcal{C}$ . Ein **Koprodukt** der  $X_i$  ist ein Datum  $(K, (\text{in}_i)_{i \in I})$  bestehend aus einem Objekt  $K \in \mathcal{C}$  und Morphismen  $\text{in}_i : X_i \rightarrow K$  derart, daß gilt: Ist  $Z \in \mathcal{C}$  ein Objekt und sind  $f_i : X_i \rightarrow Z$  Morphismen, so gibt es genau einen Morphismus  $f : K \rightarrow Z$  mit  $f \circ \text{in}_i = f_i \forall i \in I$ . Wir notieren diesen Morphismus dann auch  $(f_i)_{i \in I}$  und hoffen, daß der Leser aus dem Kontext erschließen kann, wann damit ein Morphismus aus einem Koprodukt und wann ein Morphismus in ein Produkt gemeint ist. Wenn es drauf ankommt, mag ein Morphismus in ein Produkt eben als Spalte mit einem hochgestellten  $\top$  notiert werden und ein Morphismus aus einem Koprodukt als Zeile. Wir notieren Koprodukte  $\bigsqcup_{i \in I} X_i$  oder ausführlicher  $\bigsqcup_{i \in I}^{\mathcal{C}} X_i$  und bei endlich vielen Faktoren auch  $X_1 \sqcup \dots \sqcup X_n$ . Ein leeres Koprodukt ist dasselbe wie ein initiales Objekt.

**Beispiel 4.7.7.17 (Disjunkte Vereinigungen von Mengen).** Das Koprodukt in der Kategorie der Mengen über eine beliebige Familie  $(X_i)_{i \in I}$  von Mengen heißt ihre **disjunkte Vereinigung**

$$\bigsqcup_{i \in I} X_i := \bigcup_{i \in I} (X_i \times \{i\})$$

Das Anhängen der Indizes auf der rechten Seite ist hier nur eine Vorsichtsmaßnahme für den Fall, daß unsere Mengen nicht disjunkt gewesen sein sollten. Jede derartige disjunkte Vereinigung ist versehen mit Inklusionsabbildungen  $\text{in}_j : X_j \rightarrow \bigsqcup_{i \in I} X_i$ . Weiter können wir für beliebige Abbildungen  $f_i : X_i \rightarrow Z$  in eine Menge  $Z$  die Abbildung  $f : \bigsqcup_{i \in I} X_i \rightarrow Z$  bilden durch die Vorschrift  $f(x) = f_i(x)$  für  $x \in X_i$ , und jede Abbildung der disjunkteten Vereinigung in eine Menge  $Z$  ist von dieser Form mit  $f_i = f \circ \text{in}_i$ . In Formeln ausgedrückt liefert das Vorschalten der Injektionen also für jede Menge  $Z$  eine Bijektion

$$\begin{aligned} \text{Ens}(\bigsqcup_{i \in I} X_i, Z) &\xrightarrow{\sim} \prod_{i \in I} \text{Ens}(X_i, Z) \\ f &\mapsto (f \circ \text{in}_i) \end{aligned}$$

Die disjunkte Vereinigung von endlich vielen Mengen  $X_1, \dots, X_n$  notieren wir auch  $X_1 \sqcup \dots \sqcup X_n$ .

**4.7.7.18 (Notationen für disjunkte Vereinigungen).** Gegeben eine Menge  $X$  und darin eine Familie  $(X_i)_{i \in I}$  von Teilmengen schreiben wir statt  $\bigcup_{i \in I} X_i$  auch  $\bigsqcup_{i \in I} X_i$ , wenn wir zusätzlich andeuten wollen, daß unsere Teilmengen paarweise disjunkt sind. In der Tat ist die Eigenschaft, paarweise disjunkt zu sein, ja gleichbedeutend dazu, daß die offensichtliche Abbildung  $\bigsqcup_{i \in I} X_i \rightarrow X$  eine Bijektion  $\bigsqcup_{i \in I} X_i \xrightarrow{\sim} \bigcup_{i \in I} X_i$  liefert. In derselben Weise verwenden wir bei endlich vielen Teilmengen  $X_1, \dots, X_n$  einer gegebenen Menge die Notation  $X_1 \sqcup \dots \sqcup X_n$ . In der Literatur werden statt  $\sqcup$  alternativ auch die Symbole  $\uplus$  und  $\uplus$  verwendet.

*Vorschau* 4.7.7.19. Das Koprodukt in der Kategorie der Vektorräume über einem vorgegebenen Körper heißt auch die „direkte Summe“ und wird in 4.7.8.4 besprochen.

4.7.7.20. Wie in 4.7.7.4 im Fall von zwei Faktoren besprochen erhalten wir für einen Funktor  $F : \mathcal{A} \rightarrow \mathcal{B}$  und eine Familie  $(X_i)_{i \in I}$  von Objekten von  $\mathcal{A}$ , wenn Produkte der  $X_i$  und der  $FX_i$  existieren, einen natürlichen Morphismus

$$F\left(\bigsqcup X_i\right) \rightarrow \bigsqcup FX_i$$

Ist er „stets“ ein Isomorphismus, so sagen wir metasprachlich, der Funktor  $F$  sei **verträglich mit beliebigen Produkten**. Gilt das nur für Produkte endlicher Familien, so sagen wir, unser Funktor sei **verträglich mit endlichen Produkten**. Bereits die Verträglichkeit mit endlichen Produkten schließt die Eigenschaft mit ein, daß finale Objekte auf finale Objekte abgebildet werden. Dual erklären wir die Verträglichkeit mit beliebigen beziehungsweise endlichen Koprodukten.

*Beispiel* 4.7.7.21. Sei  $K$  ein Körper. Der vergeßliche Funktor  $v : \text{Mod}_K \rightarrow \text{Ens}$  ist verträglich mit beliebigen Produkten, aber nicht mit beliebigen, nicht einmal mit endlichen, ja noch nicht einmal mit dem leeren Koprodukt. Mehr dazu diskutieren wir im folgenden Abschnitt 4.7.8.

*Vorschau* 4.7.7.22. Für die algebraisch Gebildeten unter Ihnen sei bemerkt, daß in der Kategorie Kring der kommutativen Ringe das Tensorprodukt über  $\mathbb{Z}$  im Sinne von ?? ein Koprodukt ist, sofern die Multiplikation auf  $A \otimes B$  durch  $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$  erklärt wird und die kanonischen Morphismen durch  $a \mapsto a \otimes 1$  und  $b \mapsto 1 \otimes b$ .

## Übungen

*Übung* 4.7.7.23. Man präzisiere und zeige die „Assoziativität“ von Produkten, die die Formel  $(X \times Y) \times Z \cong X \times (Y \times Z)$  andeutet.

*Übung 4.7.7.24.* Man zeige, daß in der Kategorie der kommutativen Monoide das Produkt  $M \times N$  zusammen mit  $\text{in}_1 : M \rightarrow M \times N$ ,  $m \mapsto (m, 0)$  und  $\text{in}_2 : N \rightarrow M \times N$ ,  $n \mapsto (0, n)$  ein Koprodukt ist.

### 4.7.8 Produkte und Summen von Vektorräumen\*

**Definition 4.7.8.1.** Gegeben eine Familie  $(V_i)_{i \in I}$  von Vektorräumen über einem Körper  $K$  bilden wir zwei neue  $K$ -Vektorräume, ihr **Produkt**  $\prod_{i \in I} V_i$  und ihre **direkte Summe** oder kurz **Summe**  $\bigoplus_{i \in I} V_i$  durch die Regeln

$$\begin{aligned}\prod_{i \in I} V_i &:= \{(v_i)_{i \in I} \mid v_i \in V_i\} \\ \bigoplus_{i \in I} V_i &:= \{(v_i)_{i \in I} \mid v_i \in V_i \text{ und nur endlich viele } v_i \text{ sind nicht null}\}\end{aligned}$$

Die Vektorraumstruktur ist dabei komponentenweise zu verstehen. Dieselben Konstruktionen sind auch im Fall von Gruppen sinnvoll, wenn wir „null“ als das jeweilige neutrale Element verstehen, und wir werden beide Konstruktionen auch in diesem Kontext verwenden.

4.7.8.2. Für eine endliche Familie von Gruppen oder Vektorräumen  $V_1, \dots, V_s$  stimmen die direkte Summe und das Produkt überein. Wir benutzen dann alternativ die beiden Notationen

$$V_1 \oplus \dots \oplus V_s = V_1 \times \dots \times V_s$$

Wir zeigen im folgenden, daß die direkte Summe ein Koprodukt in der Kategorie der Vektorräume ist. Die allgemeine Notation  $\sqcup$  für Koprodukte benutzen wir für Vektorräume aber nur ungern und verwenden sie in konkreten Situationen vorzugsweise für das Koprodukt von Mengen alias deren disjunkte Vereinigung.

*Beispiel 4.7.8.3 (Summe und Produkt konstanter Familien).* Im Fall der konstanten Familie  $(K)_{x \in X}$  erhalten wir einen Isomorphismus des freien Vektorraums über  $X$  im Sinne von 3.2.3.4 mit unserer direkten Summe

$$K\langle X \rangle \xrightarrow{\sim} \bigoplus_{x \in X} K$$

vermittels der Abbildungsvorschrift  $\sum_{x \in X} a_x x \mapsto (a_x)_{x \in X}$ . Auch im Fall einer allgemeineren konstanten Familie  $(V)_{x \in X}$  erhalten wir einen Vektorraumisomorphismus

$$\text{Ens}(X, V) \xrightarrow{\sim} \prod_{x \in X} V$$

vermittels der Abbildungsvorschrift  $f \mapsto (f(x))_{x \in X}$ .

**4.7.8.4 (Universelle Eigenschaften von Summe und Produkt).** Das Produkt beziehungsweise die Summe haben im Fall von Vektorräumen oder allgemeiner von abelschen Gruppen die folgenden Eigenschaften: Die offensichtlichen Einbettungen und Projektionen sind Homomorphismen

$$\text{in}_i : V_i \hookrightarrow \bigoplus_{i \in I} V_i \quad \text{beziehungsweise} \quad \text{pr}_i : \prod_{i \in I} V_i \twoheadrightarrow V_i$$

und ist  $V$  ein weiterer  $K$ -Vektorraum, so induzieren die durch Vorschalten der  $\text{in}_i$  beziehungsweise Nachschalten der  $\text{pr}_i$  gegebenen Abbildungen Bijektionen, ja sogar Isomorphismen

$$\begin{aligned} \text{Hom}_K\left(\bigoplus_{i \in I} V_i, V\right) &\xrightarrow{\sim} \prod_{i \in I} \text{Hom}_K(V_i, V) \\ f &\mapsto (f \circ \text{in}_i)_{i \in I} \\ \text{Hom}_K\left(V, \prod_{i \in I} V_i\right) &\xrightarrow{\sim} \prod_{i \in I} \text{Hom}_K(V, V_i) \\ f &\mapsto (\text{pr}_i \circ f)_{i \in I} \end{aligned}$$

Im Fall nichtabelscher Gruppen ist nur die Zweite dieser Abbildungen eine Bijektion. Ich gebe zu, daß das Symbol  $\text{in}_i$  nun in zweierlei Bedeutung verwendet wird: Einmal bei Mengen für die Einbettung in eine disjunkte Vereinigung und ein andermal bei Vektorräumen für die Einbettung in eine direkte Summe. Was jeweils gemeint ist, muß aus dem Kontext erschlossen werden. Betrachten wir im Fall des ersten Isomorphismus speziell den Fall  $V = K$ , so erhalten wir einen Isomorphismus zwischen dem Dualraum einer direkten Summe und dem Produkt der Dualräume der Summanden.

**4.7.8.5.** Gegeben eine Familie  $(V_i)_{i \in I}$  von Untervektorräumen eines Vektorraums  $V$  bezeichnet man den von ihrer Vereinigung erzeugten Untervektorraum auch als ihre **Summe** und notiert ihn  $\sum_{i \in I} V_i$ . Diese Summe kann auch interpretiert werden als das Bild des natürlichen Homomorphismus  $\bigoplus_{i \in I} V_i \rightarrow V$  von der direkten Summe nach  $V$ . Ist dieser Homomorphismus injektiv, so sagen wir, die **Summe der Untervektorräume  $V_i$  sei direkt**.

**4.7.8.6.** Untervektorräume  $V_1, V_2$  eines Vektorraums  $V$  sind komplementär als Untervektorräume genau dann, wenn die durch die Einbettungen gegebene lineare Abbildung aus ihrem Koprodukt in der Kategorie der Vektorräume alias ihrer direkten Summe ein Isomorphismus  $V_1 \sqcup V_2 = V_1 \oplus V_2 \xrightarrow{\sim} V$  ist. Da Koprodukte eh nur wohlbestimmt sind bis auf eindeutigen Isomorphismus, schreiben wir im Fall komplementärer Untervektorräume auch abkürzend  $V_1 \oplus V_2 = V$ .

## Übungen

*Ergänzende Übung 4.7.8.7 (Basis einer direkten Summe).* Ist  $(V_i)_{i \in I}$  eine Familie von Vektorräumen und  $B_i \subset V_i$  jeweils eine Basis, so ist die Vereinigung

$\bigcup_{i \in I} \text{in}_i(B_i)$  der Bilder ihrer Basen eine Basis der direkten Summe  $\bigoplus_{i \in I} V_i$ . Diese Basis ist auch in offensichtlicher Bijektion zur disjunkten Vereinigung von Basen  $\bigsqcup_{i \in I} B_i$ .

*Ergänzende Übung 4.7.8.8.* Man zeige, daß für jeden Endomorphismus  $f$  eines Vektorraums  $V$  über einem Körper  $K$  die Einbettungen der Haupträume eine Injektion

$$\bigoplus_{\lambda \in K} \text{Hau}(f; \lambda) \hookrightarrow V$$

liefern. Der Hauptraum  $\text{Hau}(f; \lambda)$  ist hier im Fall, daß  $\lambda$  kein Eigenwert von  $f$  ist, als der Nullraum zu verstehen.

*Ergänzende Übung 4.7.8.9.* Ich erinnere daran, daß ein Endomorphismus eines Vektorraums nach 3.6.6.15 diagonalisierbar heißt, wenn unser Vektorraum von den Eigenvektoren des besagten Endomorphismus erzeugt wird. Man zeige, daß ein Endomorphismus  $f$  eines Vektorraums  $V$  über einem Körper  $K$  genau dann diagonalisierbar ist, wenn  $V$  in die Summe seiner Eigenräume zerfällt, in Formeln

$$\bigoplus_{\lambda \in K} \text{Eig}(f; \lambda) \xrightarrow{\sim} V$$

wobei der Eigenraum  $\text{Eig}(f; \lambda)$  in dem Fall, daß  $\lambda$  kein Eigenwert ist, als der Nullraum zu verstehen ist.

*Ergänzende Übung 4.7.8.10.* Seien  $V$  ein Vektorraum und  $T \subset \text{End } V$  ein endlichdimensionaler Untervektorraum seines Endomorphismenraums, der aus diagonalisierbaren und paarweise kommutierenden Endomorphismen besteht. So besitzt  $V$  unter  $T$  eine **simultane Eigenraumzerlegung**

$$V = \bigoplus_{\lambda \in T^*} V_\lambda$$

in die **simultanen Eigenräume**  $V_\lambda := \{v \in V \mid xv = \lambda(x)v \ \forall x \in T\}$ . Hinweis: Sei  $x_0, \dots, x_n$  eine Basis von  $T$ . Da  $x_0$  diagonalisierbar ist, zerfällt  $V$  in Eigenräume unter  $x_0$ . Da die  $x_i$  für  $i \geq 1$  mit  $x_0$  kommutieren, stabilisieren sie dessen Eigenräume. Nach 3.6.6.19 sind die  $x_i$  auch auf diesen Eigenräumen diagonalisierbar. Eine Induktion beendet den Beweis.

*Ergänzende Übung 4.7.8.11.* Gegeben ein Vektorraum  $V$  und eine Familie von Vektorräumen  $(W_i)_{i \in I}$  liefert die kanonische Abbildung stets einen Isomorphismus

$$V \otimes \left( \bigoplus W_i \right) \xrightarrow{\sim} \bigoplus (V \otimes W_i)$$

Analoges gilt für den anderen Tensorfaktor. Für jeden  $K$ -Vektorraum  $V$  ist in anderen Worten der Funktor  $V \otimes : \text{Mod}_K \rightarrow \text{Mod}_K$  verträglich mit beliebigen Koproduktten.

*Ergänzende Übung 4.7.8.12.* Gegeben ein Vektorraum  $V$  und eine Familie von Vektorräumen  $(W_i)_{i \in I}$  liefert die kanonische Abbildung stets eine Injektion

$$V \otimes \left( \bigsqcup W_i \right) \hookrightarrow \bigsqcup (V \otimes W_i)$$

Sie ist jedoch im allgemeinen kein Isomorphismus. Genauer ist sie nur dann ein Isomorphismus, wenn entweder  $V$  endlichdimensional ist oder wenn nur für endlich viele  $i$  der zugehörige Vektorraum  $W_i$  von Null verschieden ist. Diese Übung sagt insbesondere, daß für jeden  $K$ -Vektorraum  $V$  der Funktor  $V \otimes : \text{Mod}_K \rightarrow \text{Mod}_K$  mit endlichen Produkten verträglich ist, und daß für jeden endlichdimensionalen  $K$ -Vektorraum  $V$  der Funktor  $V \otimes : \text{Mod}_K \rightarrow \text{Mod}_K$  mit beliebigen Produkten verträglich ist. Hinweis: Man folgere aus 4.6.1.21 die Injektivität der Komposition  $V \otimes W \rightarrow V^{\top\top} \otimes W \rightarrow \text{Hom}(V^{\top}, W)$  und bette beide Seiten verträglich ein in  $\bigsqcup \text{Hom}(V^{\top}, W_i) \xrightarrow{\sim} \text{Hom}(V^{\top}, \bigsqcup W_i)$ .

### 4.7.9 Algebren\*

4.7.9.1. Sei  $K$  ein Körper. Ganz allgemein bezeichnet man einen  $K$ -Vektorraum  $A$  mit einer bilinearen Verknüpfung  $A \times A \rightarrow A$  als eine  **$K$ -Algebra** und versteht unter einem **Algebrenhomomorphismus** in eine weitere  $K$ -Algebra eine  $K$ -lineare Abbildung, die mit den jeweiligen Verknüpfungen verträglich ist. Gegeben zwei  $K$ -Algebren  $A, B$  bezeichnen wir mit  $\text{Alg}_K(A, B)$  die Menge der Algebrenhomomorphismen von  $A$  nach  $B$ .

4.7.9.2. Ist die Verknüpfung einer Algebra assoziativ, so spricht man von einer **assoziativen Algebra**. Üblich ist in diesem Zusammenhang die Konvention, daß man eine Algebra stets als assoziativ versteht, wenn aus dem Kontext nichts anderes hervorgeht. Gibt es für diese Verknüpfung ein neutrales Element, so spricht man von einer **unitären Algebra** und nennt das fragliche Element das **Eins-Element**. Eine Algebra ist also genau dann assoziativ und unitär, wenn die grundeliegende Menge mit der Vektorraum-Addition als Addition und der bilinearen Verknüpfung als Multiplikation ein Ring ist. Ich schlage deshalb vor, derartige Algebren **Ringalgebren** und im Fall, daß sie auch noch kommutativ sind, **Kringalgebren** zu nennen. Unter einem **Homomorphismus von Ringalgebren** verstehen wir einen Algebrenhomomorphismus, der auch ein Ringhomomorphismus ist. Wir können diese Abbildungen sowohl charakterisieren als Algebrenhomomorphismen, die das Einselement auf das Einselement werfen, als auch als Ringhomomorphismen, die über dem Grundkörper linear sind. Wir vereinbaren für die Menge der Ringalgebrenhomomorphismen von einer  $K$ -Ringalgebra  $A$  in eine  $K$ -Ringalgebra  $B$  die Notation  $\text{Ralg}_K(A, B)$ . Sind beide beteiligten Algebren sogar Kringalgebren, so schreiben wir für diese Menge auch  $\text{Kralg}_K(A, B)$ .

*Beispiel 4.7.9.3.* Sei  $K$  ein Körper. Der Polynomring  $K[X]$  ist eine  $K$ -Ringalgebra, ja eine  $K$ -Kringalgebra. Dasselbe gilt für Polynomringe in mehreren Variablen. Gegeben ein  $K$ -Vektorraum  $V$  ist der Endomorphismenring  $\text{End } V$  eine  $K$ -Ringalgebra. Dasselbe gilt für die Matrizenringe  $\text{Mat}(n; K)$ . Eine weder assoziative noch unitäre Algebra wäre etwa  $\text{Mat}(n; K)$  mit der bilinearen Verknüpfung  $(A, B) \mapsto [A, B] := AB - BA$ . Der Vektorraum  $\text{Mat}(n; K)$  mit dieser Verknüpfung gehört zu einem speziellen Typ von Algebren, den sogenannten „Lie-Algebren“. Mit dieser Struktur heißt er auf englisch die „general linear Lie-algebra“ und wird  $\mathfrak{gl}(n; K)$  notiert. Die Lie-Algebren spielen eine zentrale Rolle beim Studium von abgeschlossenen Untergruppen der  $\text{GL}(n; \mathbb{R})$  und ganz allgemein beim Studium von „kontinuierlicher Symmetrie“.

**4.7.9.4 (Diskussion der Terminologie).** Für den Begriff einer Algebra sind in der Literatur leider auch viele andere Konventionen gebräuchlich, bei denen mehr oder weniger der oben explizit aufgeführten zusätzlichen Eigenschaften bereits für eine Algebra implizit mit gefordert werden.

**4.7.9.5.** Eine **Unteralgebra** einer Algebra ist ein unter der Verknüpfung stabiler Untervektorraum. Eine **Unterringalgebra** einer Ringalgebra ist ein unter der Verknüpfung stabiler Untervektorraum, der das Eins-Element enthält. Beide Begriffsbildungen ordnen sich der allgemeinen Begriffsbildung 4.7.3.12 eines Unterobjekts unter.

**4.7.9.6.** Sei  $V$  ein Vektorraum. Die direkte Summe

$$\bigwedge V = \bigoplus_{r \geq 0} \bigwedge^r V$$

der äußeren Potenzen von  $V$  wird mit dem „bilinear erweiterten“ Dachprodukt aufgrund der Assoziativität des Dachprodukts eine Ringalgebra mit Eins-Element  $1 \in K = \bigwedge^0 V$ . Sie heißt die **äußere Algebra** oder auch **Graßmann-Algebra** des Vektorraums  $V$ . Die übliche Identifikation  $V \xrightarrow{\sim} \bigwedge^1 V$  notieren wir kurzerhand  $v \mapsto v$  und behandeln sie auch sprachlich als Gleichheit. Gegeben  $v \in V$  gilt in  $\bigwedge^2 V$  wegen  $v \otimes v \in J_2$  natürlich  $v \wedge v = 0$ . Mit 3.6.3.2 folgt daraus in der Graßmann-Algebra die Identität

$$v \wedge w = -w \wedge v \quad \forall v, w \in V$$

Gegeben eine lineare Abbildung  $f : V \rightarrow W$  liefern die auf den äußeren Potenzen induzierten Abbildungen  $\bigwedge^r f : \bigwedge^r V \rightarrow \bigwedge^r W$  in ihrer Gesamtheit einen Ringhomomorphismus

$$\bigwedge f : \bigwedge V \rightarrow \bigwedge W$$

Natürlich gilt auch  $\bigwedge(f \circ g) = (\bigwedge f) \circ (\bigwedge g)$  und  $\bigwedge(\text{id}) = \text{id}$ .

*Ergänzung 4.7.9.7.* Sei  $V$  ein Vektorraum über einem Körper  $K$ . Eine weitere Ringalgebra, die man jedem  $K$ -Vektorraum in natürlicher Weise zuordnen kann, ist die sogenannte **Tensoralgebra**  $T_K V$  über  $V$ . Sie ist definiert als

$$T(V) = T_K V = \text{Ten}_K V := \bigoplus_{r \geq 0} V^{\otimes r} = K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \dots$$

mit der  $K$ -bilinear Multiplikation „Zusammentensorieren“, die festgelegt wird durch die Vorschrift  $(v_1 \otimes \dots \otimes v_r) \cdot (w_1 \otimes \dots \otimes w_t) := (v_1 \otimes \dots \otimes v_r \otimes w_1 \otimes \dots \otimes w_t)$ . Für die  $K$ -lineare Einbettung  $\tau : V \hookrightarrow T_K V$  des zweiten Summanden gilt dabei die folgende universelle Eigenschaft: Ist  $A$  eine  $K$ -Ringalgebra und  $\varphi : V \rightarrow A$  eine  $K$ -lineare Abbildung, so gibt es genau einen Homomorphismus von  $K$ -Ringalgebren  $\hat{\varphi} : T_K V \rightarrow A$  mit  $\varphi = \hat{\varphi} \circ \tau$ , im Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\tau} & T_K V \\ & \searrow \varphi & \downarrow \exists! \hat{\varphi} \\ & & A \end{array}$$

In der Tat sieht man leicht, daß die Vorschrift  $\hat{\varphi}(v_1 \otimes \dots \otimes v_r) := \varphi(v_1) \dots \varphi(v_r)$  das einzige mögliche  $\hat{\varphi}$  liefert. In wieder anderen Worten liefert also das Vorschalten der kanonischen Einbettung für jede  $K$ -Ringalgebra  $A$  eine Bijektion

$$\text{Ralg}_K(TV, A) \xrightarrow{\circ \tau} \text{Hom}_K(V, A)$$

Ist  $(x_\lambda)_{\lambda \in \Lambda}$  eine Basis von  $V$ , so bilden nach 4.6.1.4 die „nichtkommutierenden Monome in den  $x_\lambda$ “ alias die Tensoren  $x_{\lambda(1)} \otimes \dots \otimes x_{\lambda(r)}$  für beliebige  $r \in \mathbb{N}$  und beliebige Abbildungen  $\lambda : \{1, 2, \dots, r\} \rightarrow \Lambda$  eine  $K$ -Basis der Tensoralgebra  $TV$ . Das „leere Monom“ mit  $r = 0$  steht dabei für das Einselement. In diesem Sinne kann man die Tensoralgebra also salopp gesprochen auch als einen „Polynomring in nichtkommutierenden Variablen“ auffassen. Mehr dazu wird in ?? erklärt.

*Vorschau 4.7.9.8.* Es gibt noch eine dritte Ringalgebra, die man jedem Vektorraum  $V$  in natürlicher Weise zuordnen kann. Diese sogenannte „symmetrische Algebra“  $SV$  diskutieren wir in ?? In ?? diskutieren wir auch die Beschreibung der Graßmann-Algebra vom höheren Standpunkt als „Quotient der Tensoralgebra  $TV$  nach dem von allen  $v \otimes v$  mit  $v \in V$  erzeugten Ideal“.

## Übungen

*Ergänzende Übung 4.7.9.9.* Sei  $K$  ein Körper. Man zeige, daß in der Kategorie der  $K$ -Kringalgebren das Tensorprodukt ein Koprodukt ist, sofern die Multiplikation

auf  $A \otimes B$  durch  $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$  erklärt wird und die kanonischen Morphismen durch  $a \mapsto a \otimes 1$  und  $b \mapsto 1 \otimes b$ . Man zeige weiter, daß die analoge Aussage in der Kategorie der  $K$ -Ringalgebren nicht richtig ist.

*Ergänzende Übung 4.7.9.10.* Sei  $K$  ein Körper. Man zeige, daß der auf Objekten durch  $X \mapsto \text{Ens}(X, K)$  gegebene Funktor

$$\{\text{Endliche Mengen}\} \rightarrow \{K\text{-Kringalgebren}\}^{\text{opp}}$$

verträglich ist mit endlichen Produkten.

#### 4.7.10 Yoneda-Lemma\*

4.7.10.1. Einen Funktor von einer Kategorie  $\mathcal{C}$  in eine Kategorie von Mengen nennen wir kurz einen **Mengenfunktor auf  $\mathcal{C}$** . Gegeben ein Mengensystem  $\mathfrak{U}$  und eine  $\mathfrak{U}$ -Kategorie bildet die Menge aller Funktoren  $\mathcal{C} \rightarrow \mathfrak{U}\text{Ens}$  mit Transformationen als Morphismen eine Kategorie  $\text{Cat}(\mathcal{C}, \mathfrak{U}\text{Ens})$ . Jedes Objekt  $X \in \mathcal{C}$  liefert einen derartigen Mengenfunktor  $\check{X} = X^\vee$  gegeben durch  $\check{X} : A \mapsto \mathcal{C}(X, A)$ .

**Proposition 4.7.10.2 (Yoneda-Lemma).** *Seien  $\mathfrak{U}$  ein Mengensystem,  $\mathcal{C}$  eine  $\mathfrak{U}$ -Kategorie,  $X \in \mathcal{C}$  ein Objekt und  $F : \mathcal{C} \rightarrow \mathfrak{U}\text{Ens}$  ein Mengenfunktor auf  $\mathcal{C}$ . So liefert die Abbildungsvorschrift  $\tau \mapsto \tau_X(\text{id}_X)$  eine Bijektion*

$$\text{Cat}(\mathcal{C}, \mathfrak{U}\text{Ens})(\check{X}, F) \xrightarrow{\sim} F(X)$$

zwischen der Menge aller Transformationen  $\check{X} \Rightarrow F$  und der Menge  $F(X)$ .

*Vorschau 4.7.10.3.* Sie mögen als Übung 4.7.10.16 zeigen, inwiefern diese Bijektionen natürlich sind in  $X$  und  $F$ .

4.7.10.4. Die zur Kategorie dieser Mengenfunktoren auf  $\mathcal{C}$  opponierte Kategorie

$$\mathcal{C}^\vee = \mathcal{C}_{\mathfrak{U}}^\vee := \text{Cat}(\mathcal{C}, \mathfrak{U}\text{Ens})^{\text{opp}}$$

kann man als eine „Vervollständigung“ von  $\mathcal{C}$  interpretieren. In der Tat liest sich unser Yoneda-Lemma in dieser Notation als eine Bijektion  $\mathcal{C}^\vee(F, \check{X}) \xrightarrow{\sim} F(X)$ . Spezialisieren wir zu  $F = \check{Y}$ , so erhalten wir eine Bijektion  $\mathcal{C}^\vee(\check{Y}, \check{X}) \xrightarrow{\sim} \mathcal{C}(Y, X)$ , von der man leicht zeigt, daß sie zur offensichtlichen Abbildung  $\mathcal{C}(Y, X) \rightarrow \mathcal{C}^\vee(\check{Y}, \check{X})$  invers ist. So folgt, daß die Vorschrift  $X \mapsto \check{X}$  einen volltreuen Funktor  $\mathcal{C} \xrightarrow{\sim} \mathcal{C}^\vee$  induziert, die **Yoneda-Einbettung**. Im weiteren lassen wir das Mengensystem  $\mathfrak{U}$  wieder in den Hintergrund treten und ignorieren es meist in unserer Notation.

4.7.10.5 (**Diskussion der Notation**). Die hier verwendeten Notationen  $\mathcal{C}^\vee$  und das in 4.7.10.11 eingeführte  $\mathcal{C}^\wedge$  sind genau umgekehrt wie in [KS90]. Dafür stimmt die Notation  $\mathcal{C}^\wedge$  dann mit der in [Gro72] verwendeten Notation überein, und auch die Autoren von [KS90] verwenden in [KS00] letztere Notation, die mit der unseren übereinstimmt.

4.7.10.6 (**Das Yoneda-Lemma im Fall einer Einobjektkategorie**). Im Spezialfall einer Einobjektkategorie  $\mathcal{C} = [G]$  ist das Yoneda-Lemma besonders leicht einzusehen: Es besagt dann im Lichte von 4.7.4.20, daß die äquivarianten Abbildungen von einem Monoid  $G$  in eine beliebige  $G$ -Menge  $F$  festgelegt sind und festgelegt werden können durch das Bild des neutralen Elements.

*Beweis.* Wir konstruieren zunächst eine Abbildung in die andere Richtung. Für beliebiges  $a \in F(X)$  betrachten wir dazu die Abbildungen

$$\begin{aligned}\tau_Y : \mathcal{C}(X, Y) &\rightarrow F(Y) \\ f &\mapsto (Ff)(a)\end{aligned}$$

Man prüft ohne Schwierigkeiten, daß sie eine Transformation  $\tau : \check{X} \Rightarrow F$  bilden, die wir mit  $\hat{\tau}(a)$  bezeichnen. Jetzt gilt es nur noch zu zeigen, daß die Abbildung  $a \mapsto \hat{\tau}(a)$  invers ist zu unserer Abbildung  $\tau \mapsto \hat{\tau}(\tau) := \tau_X(\text{id}_X)$  aus der Proposition. Dafür müssen wir also prüfen, daß gilt  $a = \hat{\tau}(\hat{\tau}(a))$  für alle  $a \in F(X)$  und  $\tau = \hat{\tau}(\hat{\tau}(\tau))$  für alle Transformationen  $\tau : \check{X} \Rightarrow F$ . Das überlassen wir dem Leser.  $\square$

**Definition 4.7.10.7.** 1. Diejenigen Mengenfunktoren auf  $\mathcal{C}$ , die isomorph sind zu Mengenfunktoren im Bild von  $\mathcal{C} \rightarrow \mathcal{C}^\vee$ , heißen **darstellbare Funktoren**.

2. Ist genauer ein Mengenfunktor  $F : \mathcal{C} \rightarrow \text{Ens}$  isomorph zu  $\check{X} = \mathcal{C}(X, )$  für ein  $X \in \mathcal{C}$ , so sagen wir, der **Funktor  $F$  werde dargestellt durch das Objekt  $X$** .
3. Ist noch genauer  $F : \mathcal{C} \rightarrow \text{Ens}$  ein Mengenfunktor und  $X \in \mathcal{C}$  ein Objekt und  $a \in F(X)$  ein Element, das unter der Bijektion aus dem Yoneda-Lemma einer Isotransformation  $\mathcal{C}(X, ) \xrightarrow{\sim} F$  entspricht, so sagen wir, der **Funktor  $F$  werde strikt dargestellt durch das Paar  $(X, a)$** . Ausgeschrieben bedeutet das, daß die Vorschrift  $f \mapsto (Ff)(a)$  für alle  $Y \in \mathcal{C}$  eine Bijektion  $\mathcal{C}(X, Y) \xrightarrow{\sim} F(Y)$  liefert. Oft lassen wir das „strikt“ aber auch weg.

*Beispiel 4.7.10.8.* Der Vergißfunktor  $\text{Mod}_K \rightarrow \text{Ens}$  von den  $K$ -Vektorräumen in die Mengen wird dargestellt durch das Paar  $(K, 1)$  oder auch durch jeden anderen eindimensionalen Vektorraum zusammen mit einem beliebigen von Null verschiedenen Element.

*Beispiel 4.7.10.9.* Der Vergißfunktor  $\text{Grp} \rightarrow \text{Ens}$  von den Gruppen in die Mengen wird strikt dargestellt durch das Paar  $(\mathbb{Z}, 1)$  oder auch durch jedes andere Paar  $(Z, e)$  bestehend aus einer unendlich zyklischen Gruppe und einem Erzeuger derselben.

*Beispiel 4.7.10.10 (Das Tensorprodukt als Darstellung eines Funktors).* Seien  $K$  ein Körper und  $V, W$  zwei  $K$ -Vektorräume. Der Funktor der bilinearen Abbildungen  $\text{Mod}_K \rightarrow \text{Ens}$ ,  $L \mapsto \text{Hom}_K^{(2)}(V \times W, L)$  wird strikt dargestellt durch das Paar  $(V \otimes W, \tau)$  mit  $\tau : V \times W \rightarrow V \otimes W$  der kanonischen bilinearen Abbildung aus 4.6.1.2. Diese Aussage ist eine Umformulierung der universellen Eigenschaft des Tensorprodukts aus 4.6.1.1.

4.7.10.11. In derselben Weise kann man für jede  $\mathfrak{U}$ -Kategorie  $\mathcal{C}$  auch die Kategorie

$$\mathcal{C}^\wedge = \mathcal{C}_{\mathfrak{U}}^\wedge := \text{Cat}(\mathcal{C}^{\text{opp}}, \mathfrak{U}\text{Ens})$$

aller kontravarianten Funktoren  $\mathcal{C} \rightarrow \mathfrak{U}\text{Ens}$  betrachten und erhält mit  $X \mapsto \mathcal{C}(-, X)$  eine volltreue Einbettung  $\mathcal{C} \hookrightarrow \mathcal{C}^\wedge$ , die **Ko-Yoneda-Einbettung**. Wieder heißen die Funktoren im Bild dieser Einbettung **darstellbare Funktoren** oder, wenn wir es ganz genau nehmen wollen, **kodarstellbare Funktoren**. Die Objekte von  $\mathcal{C}^\wedge$  werden Sie später vielleicht einmal unter der Bezeichnung als „menigenwertige Prägarben auf  $\mathcal{C}$ “ wiedertreffen. Notieren wir wieder zu  $X \in \mathcal{C}$  mit  $\hat{X} \in \mathcal{C}^\wedge$  den zugehörigen Funktor  $\hat{X} : A \mapsto \mathcal{C}(A, X)$ , so liefert diesmal das Auswerten auf  $\text{id}_X$  eine Bijektion  $\mathcal{C}^\wedge(\hat{X}, F) \xrightarrow{\sim} F(X)$ .

4.7.10.12. Gegeben eine Kategorie  $\mathcal{C}$  kann man leicht explizite Isomorphismen von Kategorien  $(\mathcal{C}^\vee)^{\text{opp}} \xrightarrow{\sim} (\mathcal{C}^{\text{opp}})^\wedge$  und  $(\mathcal{C}^\wedge)^{\text{opp}} \xrightarrow{\sim} (\mathcal{C}^{\text{opp}})^\vee$  angeben. In diesem Sinne sind unsere beiden Konzepte zueinander dual.

*Vorschau 4.7.10.13.* Gegeben eine Kategorie  $\mathcal{C}$  ist die volltreue Einbettung  $\mathcal{C} \hookrightarrow \mathcal{C}^\wedge$  verträglich mit Produkten, wann immer diese in  $\mathcal{C}$  existieren. Ebenso ist die volltreue Einbettung  $\mathcal{C} \hookrightarrow \mathcal{C}^\vee$  verträglich mit Koprodukten, wann immer diese in  $\mathcal{C}$  existieren. Mehr dazu wird in ?? diskutiert.

*Vorschau 4.7.10.14.* Ein Zugang zu der von Grothendieck konstruierten Kategorie der **Schemata** ist es, diese Kategorie zu realisieren als volle Unterkategorie der Kategorie  $\text{Kring}^\vee$ , die wir erhalten, wenn wir die Kategorie der kommutativen Ringe mit der nötigen Sorgfalt bei Fragen der Mengenlehre in der oben erklärten Weise vervollständigen. Der affine Raum der Dimension  $n$  wird dann zum Beispiel definiert als der Funktor, der jedem kommutativen Ring  $R$  die Menge  $R^n$  zuordnet, und der projektive Raum der Dimension  $n$  als der Funktor, der jedem kommutativen Ring  $R$  die Menge derjenigen direkten Summanden  $D$  des  $R$ -Moduls  $R^{n+1}$  zuordnet, die „vom Rang Eins“ sind in dem Sinne, daß „bei jedem Primideal  $\mathfrak{p} \subset R$  ihre Lokalisierung  $D_{\mathfrak{p}}$  ein freier  $R_{\mathfrak{p}}$ -Modul vom Rang Eins

ist“. Man kann mit Schemata so effizient und geometrisch arbeiten, daß sie mittlerweile zum eigentlichen Arbeitspferd der sogenannten „algebraischen Geometrie“ geworden sind.

### Übungen

*Übung 4.7.10.15 (Yoneda-Einbettungen und Exponentialgesetz).* Das Exponentialgesetz 4.7.4.13 spezialisiert zu Bijektionen

$$\text{Cat}(\mathcal{C}^{\text{opp}}, \text{Cat}(\mathcal{C}, \text{Ens})) \xrightarrow{\sim} \text{Cat}(\mathcal{C}^{\text{opp}} \times \mathcal{C}, \text{Ens}) \xleftarrow{\sim} \text{Cat}(\mathcal{C}, \text{Cat}(\mathcal{C}^{\text{opp}}, \text{Ens}))$$

In der Mitte betrachten wir nun den Mengenfunktor  $\text{Mor}_{\mathcal{C}} : (X, Y) \mapsto \mathcal{C}(X, Y)$  der Morphismen. Man prüfe, daß er rechts der Koyonedaeinbettung  $\mathcal{C} \hookrightarrow \mathcal{C}^{\wedge}$  aus 4.7.10.11 entspricht und links dem Opponierten der Yonedaeinbettung  $\mathcal{C} \hookrightarrow \mathcal{C}^{\vee}$ .

*Übung 4.7.10.16 (Natürlichkeit im Yoneda-Lemma).* Man zeige, daß für jede Kategorie  $\mathcal{C}$  die Bijektionen des Yoneda-Lemmas 4.7.10.2 eine Isotransformation zwischen den beiden Wegen im Diagramm

$$\begin{array}{ccc} \text{Cat}(\mathcal{C}, \text{Ens})^{\text{opp}} \times \text{Cat}(\mathcal{C}, \text{Ens}) & \rightarrow & \text{Ens} \\ \uparrow & & \| \\ \mathcal{C} \times \text{Cat}(\mathcal{C}, \text{Ens}) & \rightarrow & \text{Ens} \end{array}$$

liefern, also zwischen den beiden Funktoren  $\mathcal{C} \times \text{Cat}(\mathcal{C}, \text{Ens})$ , die durch  $(X, F) \mapsto \text{Cat}(\mathcal{C}, \text{Ens})(\check{X}, F)$  und  $(X, F) \mapsto F(X)$  gegeben werden. Insbesondere liefern sie dann auch eine Isotransformation zwischen den Funktoren  $\mathcal{C} \times \mathcal{C}^{\text{opp}} \rightarrow \text{Ens}$  gegeben durch  $(X, Y) \mapsto \text{Cat}(\mathcal{C}, \text{Ens})(\check{X}, \check{Y})$  und  $(X, Y) \mapsto \check{Y}(X) = \mathcal{C}(Y, X)$  und wir sehen so ein weiteres Mal, daß  $X \mapsto \check{X}$  eine volltreue Einbettung  $\mathcal{C}^{\text{opp}} \hookrightarrow \text{Cat}(\mathcal{C}, \text{Ens})$  ist.

*Übung 4.7.10.17 (Eindeutigkeit darstellender Objekte).* Wird ein Mengenfunktor  $F : \mathcal{C} \rightarrow \text{Ens}$  strikt dargestellt durch das Paar  $(X, a)$  und durch das Paar  $(Y, b)$ , so gibt es genau einen Isomorphismus  $i : X \xrightarrow{\sim} Y$  mit der Eigenschaft  $F(i) : a \mapsto b$ .

*Übung 4.7.10.18.* Welche Mengenfunktoren werden durch finale und initiale Objekte dargestellt oder kodargestellt?

*Übung 4.7.10.19.* Seien  $K$  ein Körper,  $V$  ein  $K$ -Vektorraum, und  $U \subset V$  ein Teilraum. Welchen Mengenfunktor stellt der Quotient  $V/U$  dar?

*Übung 4.7.10.20.* Seien  $K$  ein Körper,  $V$  ein  $K$ -Vektorraum. Welchen Mengenfunktor stellt die Tensoralgebra dar?

*Ergänzende Übung 4.7.10.21.* Welchen Mengenfunktor stellt das Produkt im Sinne von 4.7.10.7 dar?

*Ergänzende Übung 4.7.10.22.* Seien  $K$  ein endlicher Körper und  $\text{Mat}_K$  die Matrixkategorie aus 4.7.1.7 und  $\mathfrak{U}$  ein Mengensystem derart, daß  $\text{Mat}_K$  eine  $\mathfrak{U}$ -Kategorie ist. Wir betrachten die Yonedaeinbettung

$$\text{Mat}_K \xhookrightarrow{\sim} \text{Cat}(\text{Mat}_K^{\text{opp}}, \mathfrak{U}\text{Ens})$$

Gilt  $X \in \mathfrak{U} \Rightarrow |X| < \infty$ , so induziert sie eine Äquivalenz von  $\text{Mat}_K$  mit der vollen Unterkategorie aller mit endlichen Produkten verträglichen Funktoren rechts. Gibt es zwar unendliche, aber keine überabzählbaren Mengen  $X \in \mathfrak{U}$ , so ist die volle Unterkategorie aller mit endlichen Produkten verträglichen Funktoren aus  $\text{Cat}(\text{Mat}_K^{\text{opp}}, \mathfrak{U}\text{Ens})$  äquivalent zur Kategorie aller abzählbaren  $K$ -Vektorräume. Analoge Aussagen gelten für andere Kardinalitäten und mutatis mutandis auch für unendliche Körper.

### 4.7.11 Universen\*

4.7.11.1. Um diese Leitplanken zur Vermeidung logischer Abstürze zu beschreiben, erfinde ich das Wort **Mengel** als zusammenfassende Bezeichnung für Mengen und Elemente von Mengen, die ja in unserer Terminologie selbst wieder Mengen sein dürfen, aber eben nicht sein müssen. Diese Terminologie ist allerdings nicht gebräuchlich.

*Ergänzung 4.7.11.2.* Baut man die Mengenlehre im Rahmen der Logik systematisch auf, vergleiche etwa [Ebb94], so verwendet man statt unserem „Mengel“ schlicht das Wort **Menge**. Aufgrund der Vereinbarung, daß zwei Mengen gleich sind genau dann, wenn sie dieselben Elemente haben, kann es dann nur eine einzige Menge geben, die kein Element hat. Man notiert sie  $\emptyset$ .

**Definition 4.7.11.3.** Ein **Universum** ist eine Menge  $\mathfrak{U}$  mit den folgenden Eigenschaften:

1.  $x \in M$  und  $M \in \mathfrak{U}$  implizieren zusammen  $x \in \mathfrak{U}$ ;
2.  $x \in \mathfrak{U} \Rightarrow \{x\} \in \mathfrak{U}$ ;
3.  $A \in \mathfrak{U} \Rightarrow \mathcal{P}(A) \in \mathfrak{U}$ ;
4. Gegeben  $I \in \mathfrak{U}$  und eine Abbildung  $f : I \rightarrow \mathfrak{U}$  gilt  $(\bigcup_{i \in I} f(i)) \in \mathfrak{U}$ .

*Ergänzung 4.7.11.4 (Diskussion der Terminologie).* Diese Definition steht fast genauso bei Grothendieck [Gro72, Exposé I]. Abweichend will Grothendieck nur die leere Menge nicht als Universum zulassen und fordert statt unserer zweiten Bedingung scheinbar stärker  $x, y \in \mathfrak{U} \Rightarrow \{x, y\} \in \mathfrak{U}$ . Da jedoch für jedes nicht-leere Universum gilt  $\emptyset \in \mathfrak{U}$  und folglich  $\{\emptyset\} \in \mathfrak{U}$  und  $\{\emptyset, \{\emptyset\}\} \in \mathfrak{U}$ , ergibt sich das wegen  $\{x, y\} = \{x\} \cup \{y\}$  aus dem letzten Axiom, angewandt auf die Abbildung  $f : \{\emptyset, \{\emptyset\}\} \rightarrow \mathfrak{U}$  mit  $f(\emptyset) = \{x\}$  und  $f(\{\emptyset\}) = \{y\}$ .

**4.7.11.5 (Elemente eines Universums versus Teilmengen eines Universums).** Gegeben ein Universum  $\mathfrak{U}$  gilt es genau zu unterscheiden zwischen Mengeln  $x \in \mathfrak{U}$ , die Elemente des Universums sind, die also in unserer Terminologie 2.1.2.3 zu unserem Universum gehören, und Mengeln  $M \subset \mathfrak{U}$ , die nur Teilmengen des Universums sind. Nach dem ersten Axiom ist jedes Element eines Universums, wenn es denn eine Menge ist, auch eine Teilmenge besagten Universums, aber das Umgekehrte gilt nicht. Die Formel  $M := \{x \in \mathfrak{U} \mid x \notin x\}$  definiert dann eine Teilmenge  $M \subset \mathfrak{U}$ , die kein Element von  $\mathfrak{U}$  zu sein braucht, und die Formel  $A := \{M \subset \mathfrak{U} \mid M \notin M\}$  definiert eine Menge  $A$ , die keine Teilmenge von  $\mathfrak{U}$  zu sein braucht, so daß keine dieser beiden Formeln auf den in 2.1.3.9 beschriebenen Widerspruch führt.

**4.7.11.6 (Stabilitäten eines Universums).** Wenn wir mit Kuratowski  $(x, y) := \{x, \{y\}\}$  setzen, erhalten wir sofort  $x, y \in \mathfrak{U} \Rightarrow (x, y) \in \mathfrak{U}$ . Das Produkt von je zwei Mengen, die Elemente unseres Universums sind, ist auch selbst Element unseres Universums, zum Beispiel indem wir die Vereinigung erst über alle  $x \in X$  und dann über alle  $y \in Y$  der Mengen  $\{(x, y)\}$  bilden. Weiter ist mit je zwei Mengen  $X, Y \in \mathfrak{U}$  auch die Menge der Abbildungen  $\text{Ens}(X, Y)$  Element von  $\mathfrak{U}$  und dasselbe gilt für jedes Produkt  $\prod_{i \in I} X_i$  mit  $I \in \mathfrak{U}$  und  $X_i \in \mathfrak{U}$  für alle  $i \in I$ . Ebenso folgt, daß jede Teilmenge eines Elements unseres Universums wieder ein Element unseres Universums ist.

**4.7.11.7.** Gegeben  $M \in \mathfrak{U}$  ein Element eines Universums haben wir stets  $M \subset \mathfrak{U}$ . Es kann also keine injektive Abbildung  $\mathfrak{U} \hookrightarrow M$  geben, denn dann müßte es eine injektive Abbildung  $\mathcal{P}(M) \hookrightarrow M$  geben und die gibt es nicht. Die Kardinalität eines Universums ist also stets echt größer als die Kardinalität eines jeden seiner Elemente.

**4.7.11.8 (Existenz von Universen).** Die Annahme, daß jede Menge Element eines Universums ist, müssen wir der Mengenlehre als zusätzliches Axiom hinzufügen. Es scheint nicht auf Widersprüche zu führen, hat aber die bemerkenswerte Konsequenz, daß es zu jeder Menge ein kleinstes Universum gibt, zu dem sie als Element gehört, eben den Schnitt aller Universen, zu denen sie als Element gehört. Insbesondere ist natürlich auch jedes Universum Element eines Universums. Gegeben ein Körper  $k$  und ein Universum  $\mathfrak{U}$  mit  $k \in \mathfrak{U}$  können wir dann auf der Kategorie  $k\text{-}\mathfrak{U}\text{Mod}$  der  $k$ -Vektorräume, deren zugrundeliegende Menge zu  $\mathfrak{U}$  gehört, in der Tat den Dualraumfunktor erklären.

**4.7.11.9.** Das kleinste Universum, das die leere Menge als Element enthält, besteht aus endlichen Mengen.

## 4.8 Danksagung

Für Korrekturen und Verbesserungen danke ich Ulrich Derenthal, Patrick Säring, Rolf-Dieter Frank, ...

## 4.9 Die Vorlesung LA2 im Sommersemester 2015

Es handelte sich um eine vierstündige Vorlesung, also  $4 \times 45$  Minuten Vorlesung, mit 2 Stunden Übungen.

- 21.4 Gram-Schmidt, Iwasawa-Zerlegung (keine Cholesky-Zerlegung). Isometrien affiner euklidischer Räume, Anschauung besprochen, Beweis der eindeutigen Zerlegung in Translation und Isometrie mit Fixpunkt steht noch aus.
- 23.4 Beweis der eindeutigen Zerlegung einer Isometrie in Translation und Isometrie mit Fixpunkt. Winkel und orientierte Winkel, Winkelsumme im Dreieck. Kreuzprodukt. Beweis nicht ganz fertig, Bedingung alternierend vergessen!
- 28.4 Kreuzprodukt mit Existenz und Eindeutigkeit, Spatprodukt, anschauliche Bedeutung. Hauptachsentransformation, adjungierte Abbildungen, Eindeutigkeit und Existenz des Adjungierten. Spektralsatz noch ohne Beweis, auch noch keine selbstadjungierten Abbildungen.
- 30.4 Selbstadjungierte Abbildungen, Spektralsatz, Polarzerlegung. Kein Spektralsatz für normale Abbildungen. Hermitesche Matrizen.
- 5.5 Fundamentalmatrix einer Bilinearform, Verhalten unter Basiswechsel. Symmetrische Bilinearformen und quadratische Formen. Klassifikationsfragen. Klassifikation ebener quadratischer Formen über  $\mathbb{R}$  und  $\mathbb{C}$  vorgestellt, noch nicht bewiesen.
- 7.5 Existenz einer Orthogonalbasis, Rang und Ausartungsraum, Trägheitssatz von Sylvester, Hurwitz-Kriterium.
- 12.5 Satz über Hauptachsentransformationen (Variante) und Singulärwertzerlegung. Alternierende Bilinearformen und deren Klassifikation.
- 19.5 Direktheit der Summe von Haupträumen, Fittingzerlegung, Dimension der Haupträume, Hauptraumzerlegung. Jordan-Zerlegung, nur Beweis der Existenz.
- 21.5 Eindeutigkeit der Jordan-Zerlegung und Funktionalität. Bezug zu linearen Systemen von Differentialgleichungen mit konstanten Koeffizienten. Normalform für nilpotente Endomorphismen. Jordan'sche Normalform im Fall eines algebraisch abgeschlossenen Grundkörpers.

- 2.6 Nebenklassen von Untergruppen, Satz von Lagrange; Normalteiler, Faktorgruppe, universelle Eigenschaft, Isomorphiesatz, Noether'scher Isomorphiesatz noch ohne Beweis.
- 9.6 Beweis des Noether'schen Isomorphiesatzes. Zyklische Gruppen, Gruppen von Primzahlordnung, Kleiner Fermat, Chinesischer Restsatz, RSA-Verfahren;
- 11.6 Beide Klassifikationen endlich erzeugter abelscher Gruppen und ihre Beziehung, aber noch ohne Beweis. Zerlegung endlicher abelscher Gruppen in ihre Primtorsionsanteile. Elementarteilersatz. Noch nicht: Untergruppen endlich erzeugter abelscher Gruppen sind endlich erzeugt.
- 16.6 Eindeutigkeit im Elementarteilersatz. Untergruppen endlich erzeugter abelscher Gruppen sind endlich erzeugt. Endliche Gruppen von Einheitswurzeln sind zyklisch. Beweis der Klassifikation endlich erzeugter abelscher Gruppen durch Teilerfolgen. Beweis der Eindeutigkeit fast fertig.
- 18.6 Beweis der Eindeutigkeit in den Klassifikationen. Satz von Euler als Anwendung. Exakte Sequenzen. Teil des Beweises der Proposition ??: Nur Teil 2 und Beweis der Eindeutigkeit in Teil 1. Das soll erst bei Quotientenvektorräumen wieder aufgegriffen werden.
- 23.6 Gruppenoperationen auf Mengen. Definition von Fixpunkt, Stabilisator, stabiler Teilmenge, Bahn. Freie und transitive Wirkungen. Bahnzerlegung und Bahnenraum. Universelle Eigenschaft des Bahnenraums. Zahlreiche Beispiele von Gruppenwirkungen.
- 25.6 Linksoperationen versus Rechtsoperationen. Bahnformel. Konjugationsklassen. Beispiel: die Bahnformel für die Konjugationsklassen einer Gruppe. Der projektive Raum als Bahnenraum.
- 30.6 Endliche Untergruppen der Drehgruppe. Einbettung der Symmetriegruppen der platonischen Körper als Untergruppen vom Index höchstens Zwei in symmetrische Gruppen. Bild der Bahnpolordnungsabbildung. Injektivität soll in der kommenden Stunde diskutiert werden.
- 2.7 Injektivität der Bahnpolordnungsabbildung. Existenz der Ikosaedergruppe nicht gezeigt. Quotientenvektorräume, universelle Eigenschaft.
- 7.7 Exakte Sequenzen, Neunerlemma, Gram'sche Determinante.
- 9.7 Tensorprodukt, Existenz und Eindeutigkeit, Kroneckerprodukt von Matrizen, Tensor-Hom-Adjunktion.

- 14.7 Tensorprodukt mit dem Dualraum und Homomorphismen. Spur und Evaluationsmorphismus. Identität auf endlichdimensionalen Raum als Tensor.
- 14.7 Allgemeinere Tensorprodukte. Dachprodukt und äußere Potenzen. Erzeugung durch streng monotone Monome. Noch nicht deren lineare Unabhängigkeit.
- 21.7 Deren lineare Unabhängigkeit. Kategorien, Funktoren, Beispiele. Volltreue Funktoren. Noch nicht Äquivalenz von Kategorien.
- 23.7 Äquivalenz von Kategorien. Matrixkategorie äquivalent zur Kategorie endlich erzeugter Vektorräume. Äußere Potenz und Determinante. Cauchy-Binet-Formel. Transformationen. Evaluationstransformation zum Bidualraum. Natürliche Konstruktionen von Vektorräumen zu Bewegungsräumen. Kreuzprodukt und Skalarprodukt als Transformationen.

## 4.10 Die Vorlesung Elementargeometrie im SS 18

Es handelte sich um eine zweistündige Vorlesung, also wöchentlich  $2 \times 45$  Minuten Vorlesung mit wöchentlich  $2 \times 45$  Minuten Übungen. Wegen des ungeschickten Donnerstags-Termins gab es nur elf Vorlesungen. Im Modulhandbuch steht:

Die Studierenden kennen den axiomatischen und den analytischen Zugang zur Geometrie. Sie verstehen die mathematischen Grundlagen und die Inhalte des Geometriunterrichts an Gymnasien und können diese mathematikgeschichtlich einordnen.

Und als Inhalte: Axiomensysteme für die affine und die euklidische Geometrie; Der analytische Zugang zur Geometrie über Koordinaten; Nichteuklidische Geometrie – ein Modell der hyperbolischen Ebene; Projektionen und projektive Geometrie; Isometriegruppen euklidischer Räume und platonische Körper, Eulersche Polyederformel; Geometrie der Kegelschnitte. Hier nun das Tagebuch der Vorlesung.

- 19.4 Affine Inzidenzebenen ??, Desargues-Eigenschaft und Koordinatisierung ??, Verschiebungen, noch nicht deren Gruppeneigenschaft.
- 26.4 Koordinatisierung ?? fertig bewiesen, aber zum Teil auch eher skizzenhaft. Pappus angegeben und gezeigt, daß er gleichbedeutend ist zur Kommutativität eines und jedes Koordinatenschiefkörpers. Satz von Hessenberg ?? angegeben, aber nicht bewiesen. Charakterisierung ?? reeller Inzidenzebenen durch „Zwischenrelation“ nur ganz kurz angesprochen. Neues Kapitel begonnen: Definition affiner Räume und affiner Abbildungen 3.3.1. Lemma 3.3.3.4 über affine Räume und ihre Geraden steht noch aus.
- 3.5 Affine Räume und affine Abbildungen 3.3.1. Affine Teilräume 3.3.2. Charakterisierung affiner Abbildungen 3.3.3.1. Baryzentrische Koordinaten 3.3.4.2 nur ganz kurz, sollen in den Übungen weiter besprochen werden.
- 17.5 Parallel- und Zentralprojektion ?. Bilder von Geraden unter Zentralprojektionen. Umrechnung zwischen Photographien ?. Projektive Räume als Inzidenzgeometrien ?. Anschauung für die reelle projektive Ebene. Projektive Vervollständigungen affiner Räume als Inzidenzgeometrien ?. Explizite Beschreibung der Geraden. Projektive Hyperebenen und deren Schnitte mit projektiven Geraden ?. Kurz: Nach projektiver Vervollständigung sind Parallelprojektionen spezielle Zentralprojektionen und die Zentralprojektion von einer Hyperebene auf eine weitere Hyperebene verliert ihre Definitions lücken und wird eine Bijektion. ?? und ?? waren noch nicht dran.

- 7.6 Die euklidische Ebene als Kongruenzebene 4.1.1.10. Gut fertig geworden, noch Pythagoras gezeigt.
- 14.6 Winkel 4.1.7: Zweistrahlen, Orientierte und nichtorientierte Winkel, Winkelgruppe und Winkelmenge, Identifikation der Winkelgruppe mit  $U(1)$  durch Standardorientierung von  $\mathbb{C}$  und mit  $SO(2)$  durch Standardorientierung von  $\mathbb{R}^2$ , Winkelmaße, Beziehung zum Skalarprodukt, Winkelsumme im Dreieck mit Beweis. Ich war nachher nicht sicher, ob das eine Doppelstunde wert war.
- 21.6. Isometrien euklidischer Räume 4.1.10.1 und 4.1.10.9. Endliche Untergruppen der Drehgruppe, bis zur entscheidenden Gleichung

$$2 - \frac{2}{|G|} = \sum_{i=1}^r \left(1 - \frac{1}{n_i}\right)$$

gekommen, daraus aber noch nichts gefolgt.

- 28.6. Mögliche Polordnungsmengen 4.5.4.2 und platonische Körper 4.5.4.9. Euler'sche Polyederformel 4.5.5.3. Hauptachsentransformation 4.1.12.1 und ihre inhomogene Variante 4.1.12.34.
- 5.7. Fototransformationen ?? und Kollineationen ?? als Elemente der projektiven Gruppe  $PGL(3; \mathbb{R})$ . Inzidenzstrukturen, abstrakte projektive Inzidenzebenen, Punkt-Geraden-Duales einer abstrakten projektiven Inzidenzebene, Isomorphismus zwischen  $\mathbb{P}V$  und dem Punkt-Geraden-Dualen von  $\mathbb{P}(V^*)$  im Fall  $\dim V = 3$  nach ??.
- 12.7 Desargues und Pappus im Vollausbau ???. Kreispiegelungen ???. Erhalten Kreise. Appollonisches Problem ???. Möbiustransformationen ???. Deren komplexe Interpretation als komplexe projektive Gruppe  $PGL(2; \mathbb{C})$  für orientationserhaltende Möbiustransformationen und  $PGL(2; \mathbb{C})\langle\gamma\rangle$  für alle Möbiustransformationen ???.
- 19.7 Orthogonalität von verallgemeinerten Kreisen ???. Bleibt erhalten unter Möbiustransformationen. Disjunkte Kreise können in konzentrische echte Kreise Möbiustransformiert werden. Kreiskettensatz von Steiner ???. Die hyperbolische Ebene als Inzidenzgeometrie mit Zwischenrelation und ausgezeichneter Automorphismengruppe ??, ??.

# Literaturverzeichnis

- [Bae50] Reinhold Baer. Free mobility and orthogonality. *Trans. Amer. Math. Soc.*, 68:439–460, 1950.
- [Ebb94] Heinz-Dieter Ebbinghaus. *Einführung in die Mengenlehre*. Bibliographisches Institut, Mannheim, third edition, 1994.
- [Gab62] Peter Gabriel. Des catégories abéliennes. *Bull. Soc. Math. France*, 90:323–448, 1962.
- [Gro72] Alexander Grothendieck. SGA 4, volume 269, 270, 305 of *Lecture Notes in Mathematics*. Springer, 1972.
- [KS90] Masaki Kashiwara and Pierre Schapira. *Sheaves on Manifolds*, volume 292 of *Grundlehren*. Springer, 1990.
- [KS00] Masaki Kashiwara and Pierre Schapira. *Categories and Sheaves*, volume 332 of *Grundlehren*. Springer, 2000.
- [LR03] William F. Lawvere and Robert Rosebrugh. *Sets for mathematics*. Cambridge University Press, 2003.
- [Mac98] Saunders MacLane. *Categories for the working mathematician*, volume 5 of *GTM*. Springer, 1998.
- [Maz08] Barry Mazur. Mathematical platonism and its opposites. *Newsletter of the EMS*, 68:19–21, 2008.
- [Pic49] Günter Pickert. Elementare Behandlung des Helmholtzschen Raumproblems. *Math. Ann.*, 120:492–501, 1949.
- [Sch86] Alexander Schrijver. *Theory of linear and integer programming*. Wiley, 1986.
- [Wey35] Hermann Weyl. Elementare Theorie der konvexen Polyeder. *Comment. Math. Helv.*, 7:290–306, 1935. In den gesammelten Abhandlungen: Band III, S 517–533.



## Indexvorwort

Hier werden die Konventionen zum Index erläutert. Kursive Einträge bedeuten, daß ich die fragliche Terminologie oder Notation in der Literatur gefunden habe, sie aber selbst nicht verwende. Bei den Symbolen habe ich versucht, sie am Anfang des Index mehr oder weniger sinnvoll gruppiert aufzulisten. Wenn sie von ihrer Gestalt her einem Buchstaben ähneln, wie etwa das  $\cup$  dem Buchstaben u oder das  $\subset$  dem c, so liste ich sie zusätzlich auch noch unter diesem Buchstaben auf. Griechische Buchstaben führe ich unter den ihnen am ehesten entsprechenden deutschen Buchstaben auf, etwa  $\zeta$  unter z und  $\omega$  unter o.



# Index

- 0 einelementige Gruppe, 115
- Nullvektorraum, 115
- 0 neutrales Element für  $+$ , 63
- $0_K$  Null des Körpers  $K$ , 78, 101
- $0_M$  im Fall von  $(M, +)$ , 63
- natürliche Zahl, 63, 235
- 1 Nachfolger der Null, 237
- 1 neutrales Element für  $\cdot$ , 63
- $1_K$  Eins des Körpers  $K$ , 80
- $1_M$  im Fall von  $(M, \cdot)$ , 63
- $1_R$  Eins eines Rings, 255
- natürliche Zahl, 63, 241
- $2, 3, 4, 5, 6, 7, 8, 9 \in \mathbb{N}$ , 241
- $\angle$  Winkel
  - von Vektoren, 371
  - von Zweistrahlgang, 369
- $\angle$  gerichteter Winkel, 368
- | Notation bei Teilmengen, 32
- | ist Teiler von, 260
- $\neg$  Verneinung, 65
- $\square$  Beweisende, 8
- # Kardinalität, 31
- $\exists$  es existiert ein, 55
- $\forall$  für alle, 55
- $\exists!$  es existiert genau ein, 55
- $n!$  Fakultät, 12
- $\emptyset$  leere Menge, 30
- $\in$  Element von, 30
- $\notin$  nicht Element von, 30
- / Quotient, 258
- $X/G$  Bahnenraum, 507
- $X/\iota G$  Bahnenraum, 507
- $G \backslash X$  Bahnenraum, 507
- $X \setminus Y$  Differenz von Mengen, 36
- $\Leftarrow$  folgt aus, 55
- $\Leftrightarrow$  gleichbedeutend, 55
- $\Rightarrow$  Transformation, 586
- $\Rightarrow$  impliziert, 55
- $\hookrightarrow$  Injektion, 46
- $\mapsto$  wird abgebildet auf, 44
- $\rightarrow$  Abbildung, 42
- $\rightarrow$  Morphismus in Kategorie, 571
- $\rightsquigarrow$  Isotransformation, 586
- $\rightsquigarrow$  Bijektion, 46
- $\rightsquigarrow$  Isomorphismus
  - in Kategorie, 574
  - von Kategorien, 580
- $\rightleftharpoons$  Äquivalenz von Kategorien, 580
- $\rightarrowtail$  Surjektion, 46
- $\rightsquigarrow$  volltreuer Funktor, 580
- { } Mengenklammern, 30
- $\mu\{ \}$  Multimenge, 53
- || Kardinalität, 31
- $|\alpha|$  Betrag des Winkels  $\alpha$ , 369
- $(x|y)$  Notation für Paare, 36
- $K(X)$  Funktionenkörper, 282
- $\mathcal{C}(X) := \mathcal{C}(X, X)$ , 573
- $\binom{n}{k}$  Binomialkoeffizient, 13
- $R((X))$  formale Laurentreihen, 275
- $\langle T \rangle$  Untervektorraum-Erzeugnis, 125
- $\langle \lambda, v \rangle$  Auswerten einer Linearform, 197
- $\langle \vec{u}, \vec{v}, \vec{w} \rangle$  Spatprodukt, 380
- $\langle \vec{v}, \vec{w} \rangle$  Skalarprodukt, 346
- $\langle \vec{v} | \vec{w} \rangle$  Skalarprodukt, 347
- $R[X]$  Polynomring, 266
- $R[X_1, \dots, X_n]$  Polynomring, 273

- [ $M$ ] Einobjektkategorie, 573
- [ $\Omega$ ] Einpunktköcher, 595
- [ $\vec{v}, \vec{w}$ ] Vektorprodukt, 379
- [ $f$ ] Matrix von  $f$ , 160
- $k[[T]]$  formale Potenzreihen, 275
- $\mathcal{C}^\wedge$  Funktorkategorie, 611
- $X^2 = X \times X$ , 36
- $\bar{z}$  komplexe Konjugation, 83
- $\check{X}$  Funktor  $\mathcal{C}(X, \cdot)$ , 609
- $\overline{V}$  konjugierter Vektorraum, 405
- $\overline{v}$  Vektor als Element von  $\overline{V}$ , 405
- $\overrightarrow{AB}$  Richtungsvektor, 200
- $S^{-1}$  Lokalisierung
  - $S^{-1}R$  eines Integritätsbereichs, 282
- $f^{-1}$  Umkehrabbildung, 49
- $f^{-1}$  Urbild von Menge, 45
- $f^{-1}$  inverser Morphismus, 576
- $b^*$  Vektoren der dualen Basis, 190
- $f^*$  transponierte Abbildung, 192
- $f^\circ$  in opponierter Struktur
  - Menge mit Verknüpfung, 77
  - opponierter Morphismus, 578
- $T^\perp$  Orthogonalraum von  $T$ , 348, 426
- $tA$  transponierte Matrix, 165
- $tf$  transponierte Abbildung, 192
- $A^\top$  transponierte Matrix, 165
- $b^\top$  Vektoren der dualen Basis, 190
- $f^\top$  transponierte Abbildung, 192
- $X^\vee$  Funktor  $\mathcal{C}(X, \cdot)$ , 609
- $\mathcal{C}^\vee$  Funktorkategorie, 609
- = Gleichheitszeichen, 31
- =: wird definiert als, 9
- := ist definiert durch, 9
- $\perp$  orthogonal
  - in Skalarproduktraum, 347
- \* Juxtaposition, 591
- \* einziges Element von ens, 119
- o Verknüpfung
  - Matrixprodukt, 161
  - von Abbildungen, 45
  - von Morphismen, 570
- $\vee$  Trenner
  - bei Multiabbildungen, 52
  - bei multilinearen Abbildungen, 302
- $\oplus$  direkte Summe
  - $\bigoplus$  Summe von Familie, 603
  - von komplementären Untervektorräumen, 604
  - von Vektorräumen, 120
- $\otimes$  Tensorprodukt, 536
  - Differenz von Mengen, 36
- $n_K$  ganze Zahl in Körper  $K$ , 82
- $p - q$  bei affinem Raum, 200
- $V^{\mathbb{R}}$  Reellifizierung von  $V$ , 137
- $X^M$  Fixpunkte von  $M$  in  $X$ , 501
- $X^n$  für  $n$ -Tupel in  $X$ , 119
- $X^{\times n}$  für  $n$ -Tupel in  $X$ , 119
- $Y^X$ 
  - statt  $\text{Ens}(X, Y)$ , 52
- $a^k$  Potenz, 14
- $\mathcal{B}^\wedge$  Funktorkategorie, 589
- $\geq, >, \leq, <$  bei Ordnungsrelation, 121
- $\triangleleft$  Normalteiler in, 468
- $\square$  Produkt
  - in Kategorie, 600
  - von Mengen, 599
  - von Vektorräumen, 603
- $\prod$  Produkt, 64
  - von Zahlen, 12
- $\sum$  Summe
  - von Zahlen, 11
- $\wedge$  Dachprodukt, 561
  - $\bigwedge^r$  äußere Potenz, 560
  - $\bigwedge^{\max}$  maximale Potenz, 563
  - Vektorprodukt, 379
- $\cap$  Schnitt, 34
  - $\bigcap$  von Mengensystem, 126
- $\subset$  Teilmenge, 36
- $\uplus$  disjunkte Vereinigung, 602
- $\uplus$  disjunkte Vereinigung, 602
- $\cup$  Vereinigung, 34
  - $\bigcup$  von Mengensystem, 126

- Koprodukt
  - disjunkte Vereinigung, 602
- disjunkte Vereinigung
  - von Mengenfamilie, 601
  - von Teilmengen, 602
- $M^\times$  invertierbare Elemente eines Monoids  $M$ , 68
- $\mathcal{C}^\times$  Isomorphismen in  $\mathcal{C}$ , 575
- $\times$ 
  - kartesisches Produkt, 36
  - Kartesisches Produkt von Abbildungen, 117
  - Produkt von Kategorien, 579
- $\times$  Produkt
  - in Kategorie, 600
- $\mathcal{C}^\times$  Isomorphismenkategorie, 575
- ☒ äußeres Produkt
  - von Funktionen, 548
- + Verschieben von Punkt um Richtungsvektor, 199
- $a$  Negatives von  $a$ , 68
- $a - b$  bei Gruppe, 69
- ( $x|y$ ) Notation für Paare, 36
- $f|X$  Einschränkung auf  $X$ , 46
- $f|_X$  Einschränkung auf  $X$ , 46
- Ab abelsche Gruppen
  - Kategorie, 572
- Abb, 52
- Abbildung, 42
  - einwertige, 45
  - identische, 44
  - inverse, 49
  - konstante, 45
  - Projektionsabbildung, 116
  - Umkehrabbildung, 49
- ABC-Vermutung, 252
- abelsch
  - Gruppe, 66
  - Verknüpfung, 60
- abgeschlossen
- algebraisch, 270
- unter Verknüpfung, 60
- Abmonoid, 63
- Absorptionsgesetz, 85
- Abspalten von Linearfaktoren, 269
- Abständezahl, 525
- Abstand, 347, 383
- Achsenspiegelung, 365
- Acht als natürliche Zahl, 241
- Addition
  - in Ring, 255
  - natürlicher Zahlen, 238
- adjungiert
  - lineare Abbildung, 396
- adjunkte Matrix, 308
- ähnlich
  - Dreiecke, 345
  - Ähnlichkeit, 344, 359, 439
  - lineare, 593
  - Ähnlichkeitsabbildung, 359
  - lineare, 359, 437
- Äquivalenz
  - von Funktoren, 586
  - von Kategorien, 580
- Äquivalenzklasse, 244
- Äquivalenzrelation
  - auf einer Menge, 243
  - erzeugt von Relation, 245
- äquivariant, 590
- äußere Algebra, 607
- äußere Potenz, 560
- Aff Kategorie der affinen Räume, 577
- Aff affine Abbildungen, 202
- Aff $^\times$  Affinitäten, 202
- affin
  - Abbildung, 202
  - Raum, 199
  - Raum, über Vektorraum, 199
  - Teilraum, 204
- unabhängig
  - als Familie, 214

- als Teilmenge, 214
- Affinität, 202
- Alexandroff, Satz von, 439
- Alg Algebrenhomomorphismen, 606
- Alg Kategorie der Algebren, 572
- Algebra, 606
  - assoziative  $\mathbb{Z}$ -Algebra, 255
- algebraisch
  - abgeschlossen, Körper, 270
- Algebrenhomomorphismus, 256, 606
- allgemeine lineare Gruppe, 146, 168
- Alphabet, griechisches, 23
- Alt alternierende Formen, 559
- $\text{Alt}^n(V)$  alternierende Multilinearformen, 303
- $\text{Alt}^n(V, W)$  alternierende multilineare Abbildungen, 303
- Alternator, 564
- alternierend
  - bilineare Abbildung, 301
  - Matrix, 412
  - multilineare Abbildung, 302
  - Tensor, 564
- alternierende Gruppe, 294
- Amplitude, 132
- Anfangspunkt
  - von Pfeil in Köcher, 594
- anneau, 255
- Anordnung, 121
- anschaulich, 112
- antikausal, 436
- antisymmetrisch
  - bilineare Abbildung, 302
  - Relation, 121
- arrow of quiver, 595
- Artin, Vermutung von, 489
- assoziativ, 60
- Assoziativgesetz
  - bei Vektorraum, 111
- Assoziativität
  - bei Gruppenoperation, 500
- aufgespannt
  - Untervektorraum, 125
- aufsteigende Vereinigung, 144
- Ausartungsraum, 420
- Ausgangskategorie, 577
- ausgeartet
  - Bilinearform, 420
  - Paarung, 425
- Auswahlaxiom, 142
- Auswahlaxiom, Variante, 142
- Auswahlfunktion, 142
- Auswerten, 42
- Auswertungsabbildung, 54, 191
- Automorphismengruppe
  - eines Vektorraums, 146
- Automorphismus
  - einer Gruppe, 512
  - eines Vektorraums, 146
  - in Kategorie, 575
  - von affinem Raum, 202
- Bahn, 502
- Bahnenraum, 507
- Bahnformel, 511
- Bahnpolordnungsabbildung, 521
- balanciertes Produkt, 512
- baryzentrisch
  - Koordinaten, 216
- Baryzentrum, 213
- Basis, 128
  - angeordnete, 128
  - duale, 191
  - indizierte, 128
  - unverträglich orientierte, 311
  - verträglich orientierte, 311
  - von Vektorraum, 128
- Basisexistenzsatz, 130
- Basismatrix, 169
- Basispunkt, 493
- Basiswechselmatrix, 177
- bepunktete Menge, 493

- Bessel'sche Ungleichung, 352
- Betrag
  - bei Quaternionen, 289
  - eines Winkels, 369
- Betragswurzel
  - aus reellem Vektorraum, 359
- Bewegung, 362, 514
- Bewegungsgruppe, 514
  - affine, 361
- Bewegungsraum, 362
- biadditiv, 472
- Bidualraum, 195
- Bierdeckelgruppe, 515
- Bijektion, 46
- bijektiv
  - Abbildung, 46
- Bil Bilinearformen, 410
- Bil( $V$ ) Bilinearformen auf  $V$ , 158
- Bild, 42
  - einer Teilmenge, 44
  - von linearer Abbildung, 151
- bilinear
  - bei Vektorräumen, 158
- Bilinearform, 158, 344
  - nichtausgeartete, 420
- Bilinearformen, 410
- Binärdarstellung, 242
- Binomialkoeffizienten, 13
- binomische Formel, 14
- Bogenmaß, 373
- Boole'sche Algebra, 84
- Brennpunkt
  - einer Ellipse, 407
- Bruchzahlen, 31
- Bruhat-Zerlegung
  - in der  $\mathrm{GL}(n; R)$ , 532
- $C_n$  Catalan-Zahl, 62
- $C_n$  zyklische Gruppe, 473
- $\mathbb{C}$  komplexe Zahlen, 181
- Car Kategorie der Köcher, 595
- Car( $\mathcal{Q}, \mathcal{C}$ ), 597
- Caratheodory, Satz von
  - im Affinen, 223
  - lineare Version, 218
- card, 31
- carquois, 595
- Cartan-Zerlegung, 401
- Cat( $\mathcal{A}, \mathcal{B}$ ), 589
- Catalan-Zahl, 62
- Cauchy
  - Satz von, 510
- Cauchy-Binet-Formel, 568
- Cauchy-Schwarz'sche Ungleichung, 350
- Cayley-Hamilton, 322
- char Charakteristik, 264
- char charakteristisches Polynom, 319
- Charakteristik
  - eines Rings, 264
- charakteristisches Polynom, 317
  - von Endomorphismus, 319
- $\chi_A$  charakteristisches Polynom, 317
- $\chi_f$  charakteristisches Polynom, 319
- Chinesischer Restsatz, 474
- Cholesky-Zerlegung, 391
- codim Kodimension
  - bei affinen Räumen, 208
  - eines Untervektorräums, 492
- cok Kokern
  - bei abelschen Gruppen, 494
- cone
  - englisch für Kegel, 227
  - strongly convex, 227
- corps, 78
- corps gauche, 288
- $\cos_a$  analytischer Cosinus, 371
- $\cos_g$  geometrischer Cosinus, 371
- Cosinus, 370
  - analytischer, 371
  - geometrischer, 371
- Cosinus-Satz, 377
- Cramer'sche Regel, 308

- $D(f)$  Definitionsbereich von  $f$ , 282
- $\Delta$  Diagonale, 117
- Dachprodukt, 561
- darstellbarer Funktor, 610, 611
- darstellende Matrix, 160, 174
- Darstellung
  - eines Köchers, 595
- de Morgan'sche Regeln, 38
- Definition, 11
- Definitionsbereich, 44, 282
- degré, 268
- degree, 268
- det Determinante
  - einer Matrix, 295
  - von Endomorphismus, 307
- $\det_K$  Determinante
  - von Endomorphismus, 307
- Determinante
  - einer Matrix, 295
  - von Endomorphismus, 307
- Dezimaldarstellung, 242
- Dezimalsystem, 242
- $\text{diag}(\lambda_1, \dots, \lambda_n)$  Diagonalmatrix, 170
- Diagonale, 117
- diagonalisierbar
  - Endomorphismus, 321
  - Matrix, 320
- Diagonalmatrix, 170
- Diagramm
  - in Kategorie, 595
- Diagrammjagd, 498
- Diagrammschema, 595
- dicke Zelle
  - in der  $\text{GL}(n; K)$ , 533
- Diedergruppe, 514
- Differenz
  - von Mengen, 36
- Differenzraum, von affinem Raum, 199
- Diffie-Hellman, 263
- Diffie-Hellman-Problem, 263
- dim Dimension eines Vektorraums, 134
- Dimension
  - eines affinen Raums, 199
  - eines Vektorraums, 134
  - physikalische, 134
- Dimensionsformel
  - für lineare Abbildungen, 152
- direkte Summe
  - von Vektorräumen, 120, 603
- disjunkt, 36
- disjunkte Vereinigung, 601
- diskret
  - Kategorie, 574
  - Logarithmus, 263
- Distributivgesetz, 255
  - bei Körper, 79, 101
  - bei Vektorraum, 111
- Divisionsring, 288
- Dodekaeder, 515
- Doppeltransposition, 295
- Drehachse, 361
  - von linearer Drehung, 361
- Drehgruppe, 516
- Drehspiegelgruppe, 366
- Drehspiegelung, 384
- Drehung, 360
  - lineare, 360
- Drehungsgruppe, 363, 366
- Drei als natürliche Zahl, 241
- Dreiecksungleichung
  - für komplexen Absolutbetrag, 185
  - in euklidischem Vektorraum, 350
- Dreispiegelungssatz, 386
- dual
  - Basis, 191
  - duale Abbildung, 192
  - dualer Kegel, 228
- Dualitätssatz
  - der linearen Optimierung, 232
- Dualraum, 188
- Dualsystem, 242
- Durchschnitt

- zweier Mengen, 34
- $E_{ij}$  Basismatrizen, 169
- $\mathbb{E}$  Anschauungsraum, 200
- Ebene
  - affine, 199, 204
  - echt
    - Teilmenge, 32
  - Ecke
    - eines Dreiecks, 376
    - von Graph, 526
    - von Köcher, 594
  - edge of quiver, 595
- Eig Eigenraum, 316, 445
- Eigenraum, 316, 445
  - von quadratischer Form
    - auf Skalarproduktraum, 415
- Eigenvektor, 316
- Eigenwert, 316
  - von quadratischer Form
    - auf Skalarproduktraum, 415
    - auf  $\mathbb{R}^n$ , 396
- Ein-Objekt-Kategorie, 573
- Einbettung, 584
  - einer Teilmenge, 46
- Einheit
  - von Ring, 261
- Einheitsmatrix, 160
- Einheitswurzel
  - eines Körpers, 485
- einhüllende Gruppe, 245
- Einpunktköcher, 595
- Eins als natürliche Zahl, 241
- Eins in  $\mathbb{N}$ , 237
- Eins-Element, 63
  - einer Algebra, 606
  - in Ring, 255
- Einschluß-Ausschluß-Formel, 257
- Einschränkung, 46
- Einsetzen, 42
- Einsetzungshomomorphismus, 267, 568
- Eintrag von Matrix, 107
- einwertige Abbildung, 45
- Element, 30
- Elementabbildung, 53
- Elementarmatrix, 170
  - spezielle, 170
- Elementarteiler, 481
- Elementarteilersatz
  - über dem Grundring  $\mathbb{Z}$ , 480
- Ellipse
  - Brennpunkt, 407
- elt Elementabbildung, 53
- $\text{em}_x$ 
  - Morphismus aus finalem Objekt, 576
- End
  - Endomorphismenring
    - von abelscher Gruppe, 256
- $\text{End}_k$ 
  - Endomorphismenring
    - von  $k$ -Vektorraum, 256
- endlich
  - Köcher, 595
  - Menge, 31, 234
- endlich erzeugbar, 125
- endlich erzeugt
  - Vektorraum, 125
- endliche Primkörper, 262
- Endomorphismen
  - in Kategorie, 573
- Endomorphismenring
  - von abelscher Gruppe, 256
  - von Vektorraum, 256
- Endomorphismus
  - von abelscher Gruppe, 256
  - von Vektorräumen, 146
- Endpunkt
  - von Pfeil in Köcher, 595
- ens einelementige Menge, 119, 576
- Ens Kategorie der Mengen, 572
- Ens( $X, Y$ ) Abbildungen  $X \rightarrow Y$ , 52

- Ens( $X, Y$ ) Abbildungsmenge, 107
- Ens( $Z$ ) Selbstabbildungen der Menge  $Z$ , 59
- Ens\* bepunktete Mengen, 572
- Ens $^\times(Z)$  Bijektionen  $Z \xrightarrow{\sim} Z$ , 68
- ensemble, 52
- Ereignisse, 434
- Erweiterung der Skalare
  - bei Vektorräumen, 546
- erzeugende Funktion
  - der Fibonacci-Folge, 285
- Erzeugendensystem, 125
  - von affinem Raum, 205
- Erzeugnis
  - in Vektorraum, 125
- erzeugt
  - Äquivalenzrelation, 245
  - affiner Teilraum, 204
  - Untergruppe, 247
  - Untervektorraum, 125
- erzeugt, endlich
  - Vektorraum, 125
- essentiell surjektiv
  - Funktör, 580
- Euk Kategorie der euklidischen Vektorräume, 577
- Euklid
  - Lemma von, 251
- euklidisch
  - Abbildung, 359
  - Ebene, 357
  - Raum, 357
  - Struktur, 357
  - Vektorraum, 347, 357
- euklidische Struktur
  - induzierte, 359
- Euler'sche Winkel, 393
- Euler, Satz von, 488
- Euler-Formel, 531
- Eulerformel, 530
- ev Evaluationspaarung, 546
- ev Auswertungsabbildung, 54
- ev Evaluation, 195
- Evaluationsabbildung, 54, 195
- Evaluationspaarung, 546
- ex Expansion der Identität, 547
- exakte Sequenz
  - von bepunkteten Mengen, 494
- Expansion der Identität, 547
- Exponent, 485
- Exponentialgesetz
  - für Mengen, 52
- F( $b$ ) Fundamentalmatrix, 410
- Faktor, 116
- Faktoren, 12
- Fakultät, 12
- Familie, 128
- Farkas, Lemma von, 220
- Farkas, Satz von, 228
- Faser
  - einer Abbildung, 45
- Fehlstand, 291
- Fermat'sche Kongruenz, 474
- festgehalten
  - Teilmenge unter Selbstabbildung, 53
  - punktwise, 53
- Fibonacci-Folge, 16
- field, 78
- fin Morphismus zum finalen Objekt, 576
- fin( $\mathcal{C}$ ) finales Objekt, 576
- final, 585
  - Objekt, 575
  - Struktur, 585
- Fitting-Zerlegung
  - von Vektorräumen, 448
- Fixator, 501, 502
  - mengenweiser, 502
  - punktwise, 502
- Fixpunkt, 149

- von Gruppenwirkung, 501
- Fixvektor, 149
- Flächengerade, 556
- Form
  - allgemein, 190
  - quadratische, 490
  - quadratische homogene, 413
- Fortsetzung
  - lineare, 156
- Frac Quotientenkörper, 281
- fraction field, 281
- frei
  - Gruppenwirkung, 502
  - Vektorraum, 156
  - Wirkung eines Monoids, 502
- Frequenz, 314
- Frobenius-Homomorphismus, 265
- Fünf als natürliche Zahl, 241
- Fundamentalmatrix, 410
- Fundamentalsatz der Algebra, 270
- Funktion
  - rationale, 282
  - Umkehrfunktion, 49
- Funktionenkörper, 282
- Funktör, 577
  - darstellbarer, 610, 611
  - kodarstellbarer, 611
  - kontravarianter, 579
  - quasiinverser, 592
- Funktorkategorie, 588
- Fußball, Satz vom, 356
- $\Gamma(f)$  Graph von  $f$ , 44
- ganze Zahlen, 30, 246
- ganzwertig
  - Polynom, 280
- Gauß-Algorithmus, 105
- gegensinnig
  - Kongruenz, 336
- general linear group, 146, 168
- geordnet
- induktiv, 139
- streng induktiv, 139
- gerade
  - Permutation, 291, 295
  - Zahl, 259
- Gerade
  - affine, 199, 204
- Geradensegment, 216
- Geschwindigkeit
  - absolute, 541
  - vektorielle, 202
- gestreckter Winkel, 370
- Gewichtsprozent, 115
- Gitter
  - $\mathbb{Z}$ -Gitter in  $\mathbb{Q}$ -Vektorraum, 489
- GL( $V$ ) allgemeine lineare Gruppe, 146
- GL( $n; K$ ) allgemeine lineare Gruppe, 168
- gleichsinnig
  - Kongruenz, 336
- Gleichungssystem, 103
  - lineares, 103
- Gleitspiegelung, 384
- GO<sub>aff</sub>( $E$ ) Ähnlichkeiten, 439
- Goldbach-Vermutung, 249
- goldener Schnitt, 18
- Gon als Winkelmaß, 373
- grad
  - Grad
    - eines Polynoms, 268
- Grad
  - bei der Winkelmessung, 373
  - eines Polynoms, 268
- Gram'sche Determinante, 425
- Gram'sche Matrix, 425
- Gram-Schmidt, 388
  - Orthogonalisierungsverfahren, 389
- Graph
  - einer Abbildung, 44
  - kombinatorischer, 526
- Graßmann-Algebra, 607

- griechisches Alphabet, 23
- größter gemeinsamer Teiler, 250
- größtes Element, 123, 138
- Grp
  - Gruppenhomomorphismen, 71
  - Grp Kategorie der Gruppen, 572
  - $\text{Grp}^\times(G)$  Automorphismen von  $G$ , 512
  - Grundkörper, 111
  - Gruppe, 65
    - einhüllende, 245
    - opponierte, 77
  - Gruppe der Einheiten, 261
  - Gruppenhomomorphismus, 71
  - Gruppentafel, 72
  - Grupoid, 574
- Halb
  - Halbgruppenhomomorphismen, 75
- halbeinfach
  - Endomorphismus, 451
- halbeinfacher Anteil
  - eines Endomorphismus, 451
- Halbgerade, 334
- Halbgruppe, 75
- Halbordnung, 121
- Halbraumfahne
  - fastvollständige, 366
  - vollständige, 366
- Hamilton'sche Zahlen, 288
- Hau Hauptraum, 445
- Hauptachse
  - von quadratischer Form
    - auf Skalarproduktraum, 415
  - von quadratischer Form
    - auf  $\mathbb{R}^n$ , 396
- Hauptminoren-Kriterium, 423
- Hauptraum, 445
- Hauptsatz
  - über lineare Ungleichungen, 218
- Hauptvektor, 445
- Helmholtz'sches Raumproblem, 367
- hermitesch, 346, 398
- Hertz, 314
- Hexadezimalsystem, 242
- Hilbert'sche Probleme
  - Nummer 18, 516
- Hilbertraum
  - endlichdimensionaler, 347
  - $\text{Hom}^{(2)}$  bilineare Abbildungen, 158
  - $\text{Hom}^{(n)}$  multilineare Abbildungen, 302
- homogen, homogenisieren
  - lineares Gleichungssystem, 103
- homogener Raum, 502
- Homomorphismus
  - von Gruppen, 71
  - von Magmas, 71
  - von Monoiden, 71
  - von Ringalgebren, 606
  - von Sequenzen, 494
  - von Vektorräumen, 146
- Homothetie, 203
- Hülle
  - konvexe, 216
  - lineare, 125
- Hurwitz-Kriterium, 423
- Hyperebene
  - affine, 206
  - lineare, 127
- i Wurzel aus  $-1$  in  $\mathbb{C}$ , 181
- I =  $I_n$  Einheitsmatrix, 160
- id, 44
- Id Identitätsfunktor, 578
- Idempotent
  - in Magma, 155
- identische Transformation, 588
- Identität auf  $X$ , 570
- Identität, 44
- Identitätsfunktor, 578
- Ikosaeder, 515
- Ikosaedergruppe, 515
- im

- Bild von Abbildung, 45
- Bild von linearer Abbildung, 151
- image, 151
- Imaginärteil
  - bei komplexen Zahlen, 183
- in, Morphismus in Koprodukt, 604
- in<sub>i</sub>
  - Injektionen bei Summen, 148
- indefinit, 422
- Index
  - einer Untergruppe, 466
  - von Bilinearform, 422
- Induktion, vollständige, 8
  - Induktionsannahme, 8
  - Induktionsbasis, 8
  - Induktionsschritt, 8
  - Induktionsvoraussetzung, 8
- induziert
  - Struktur, 584
- ini( $\mathcal{C}$ ) initiales Objekt, 576
- initial
  - Objekt, 575
  - Struktur, 584
- Injektion, 46
  - kanonische, 148
- injektiv
  - Abbildung, 46
- Inklusion, 46
- innerer Automorphismus
  - einer Gruppe, 512
- insertion homomorphism, 568
- int<sub>x</sub> Konjugation mit  $x$ , 512
- Integritätsbereich, 261
- Integritätskring, 261
- Integritätsring, 261
- interior automorphisms, 512
- Invariante
  - von Gruppenwirkung, 501
- invers
  - in Monoid, 65
  - Matrix, 168
- Morphismus, 576
- Inverse
  - Matrix, 168
- Inversion, 185
- invertierbar, 65
  - in Ring, 261
  - Matrix, 168
- Involution, 472
- Iso
  - in Kategorie, 574
- Isometrie, 382
  - partielle, 403
- Isometriesymmetrien, 529
- isometrisch, 382
  - lineare Abbildung, 428
- Isomorphismus, 382
- isomorph
  - Funktoren, 586
  - Graphen, 526
  - Gruppen, 72
  - in Kategorie, 574
  - Vektorräume, 146
- Isomorphiekasse, 575
- Isomorphiesatz, 470
  - Noether'scher, 470
- Isomorphismenkategorie, 575
- Isomorphismus, 72
  - in Kategorie, 574
  - isometrischer, 382
  - von affinen Räumen, 202
  - von Funktoren, 586
  - von Graphen, 526
  - von Kategorien, 580
  - von Kongruenzebenen, 343
  - von Sequenzen, 495
  - von Vektorräumen, 146
- Isotransformation, 586, 597
- Isotropiegruppe
  - für Standgruppe, 501
- Iwasawa-Zerlegung
  - für  $GL(n; \mathbb{C})$ , 390

- für  $\mathrm{GL}(n; \mathbb{R})$ , 390
- für  $\mathrm{SL}(n; \mathbb{C})$ , 393
- $J(r)$  nilpotenter Jordan-Block, 455
- $J(r; \lambda)$  Jordan-Block, 456
- Jacobson-Morozov, 462
- Jägerzaunformel, 296
- Jordan'sche Normalform, 458
- Jordan-Basis, 458, 463
- Jordan-Block, 458
  - nilpotenter, 455
- Jordan-Zerlegung
  - additive, 451
  - multiplikative, 454
- Juxtaposition, 591
- kanonisch
  - Abbildung, 587
  - Injectioп, 148
  - Isomorphismus, 587
- Kante
  - von Graph, 526
- Kardinalität, 31, 239
  - einer Multimenge, 53
- kartesisch
  - Produkt
    - endlich vieler Mengen, 116
    - von beliebig vielen Mengen, 599
    - von zwei Mengen, 36
- Kategorie, 570
  - $\mathfrak{U}$ -Kategorie, 581
  - diskrete, 574
- kausal, 436
- Kegel, 227
  - dualer, 228
  - spitzer, 227
- ker
  - Kern von linearer Abbildung, 152
- Kern
  - von Gruppenhomomorphismus, 76
  - von linearer Abbildung, 152
- Kette
  - in teilgeordneter Menge, 139
- kgV kleinstes gemeinsames Vielfaches, 252
- Klassifikation, 416
  - abelsche Gruppen, 479
- Klassifikationsprobleme, 575
- Klein'sche Vierergruppe, 73
- kleinstes
  - Element, 123
- kleinstes gemeinsames Vielfaches, 252
- Ko-Yoneda-Einbettung, 611
- kodarstellbarer Funktor, 611
- Kodimension
  - bei affinen Räumen, 208
  - eines Untervektorraums, 492
- Köcher, 594
  - mit Verknüpfung, 595
- Koeffizient, 103
  - von Polynom, 266
- Koeffizientenmatrix, 105
  - erweiterte, 105
- Körper, 78, 101
  - Körperhomomorphismus, 82
  - Körperisomorphismus, 82
- kofinal
  - Objekt, 575
- koinduziert
  - Struktur, 585
- Kokern
  - bei abelschen Gruppen, 494
- kollinear, 204
- kommutativ
  - Diagramm, 497
  - Rechteck, 196
  - Ring, 255
  - Verknüpfung, 60
- kommutieren, 267
  - Elemente, 60
- Komplement, 36
  - orthogonales, 349

- komplementär
  - Untervektorräume, 153
- Komplementmenge, 36
- komplex konjugiert
  - Vektorraum, 405
- komplexe Konjugation, 83
- komplexe Zahlen, 83, 181
  - vergessliche, 182
- Komplexifizierung, 547
- Komponente
  - eines Tupels, 116
- komponentenweise Verknüpfung, 59
- kongruent
  - angeordnete Dreiecke, 377
  - Dreiecke, 335
- kongruent modulo, 258
- Kongruenz, 334
- Kongruenzebene, 334
- Kongruenzgruppe
  - affine, 334
- Konjugation, 512
- Konjugationsklasse, 512
- konjugiert
  - Vektorraum, komplexer, 405
- konjugierte komplexe Zahl, 183
- konservativ
  - Funktor, 582
- konstant
  - Abbildung, 45
  - Polynom, 266
- kontravariant
  - Funktor, 579
- konv konvexe Hülle, 231
- konv( $T$ ) konvexe Hülle von  $T$ , 216
- konvex
  - in affinem Raum, 216
- konvexe Hülle, 216
- Konvexkegel, 227
  - erzeugt von, 228
  - polyedrischer, 228
- Koordinaten, 190
  - affine, 205
- Koordinatenfunktionen, 190
- Koordinatensystem
  - affines, 205
- Koprodukt, 601
- Korrespondenz, 121
- Kovektor, 188
- Kralg
  - Kategorie der Ringalgebren, 572
  - Kringalgebrenhomomorphismen, 606
- Kreis
  - verallgemeinerter, 187
- Kreisgruppe, 185
- Kreuzprodukt, 379
  - geometrisches, 558
- Kring
  - kommutativer Ring, 255
- Kring Kategorie der Kringe, 572
- Kringalgebra, 606
- Kristall
  - im Raum, 515
- Kristallklasse, 516
- Kristallsystem, 516
- Kronecker-Produkt, 542
- Kroneckerdelta, 161
- kubisch
  - Polynom, 268
- kürzbar, 60, 261
- Kürzen in Ringen, 261
- kurze exakte Sequenz, 494
- $l(\sigma)$  Länge von Permutation, 291
- Längeneinheit
  - relativistische, 438
- Länge, 360, 438
  - von Permutation, 291
- Längengerade, 360, 438
  - von euklidischem Raum, 360
- Lagrange
  - Satz von, 466
- Laspp, 575

- Laufindex, 11
- Laurententwicklung
  - algebraische, 283
- Laurentreihe
  - formale, 275
- leer
  - Familie, 128
  - Menge, 30
- Leibniz-Formel, 296
- Leitkoeffizient, 268
- Lemma, 62
- lichtartig, 436
  - kausal, 436
- lichtartige Vektoren, 418
- Lichtkegel, 418
- lin Spann, 125
- linear
  - Abbildung, 146
    - Funktion, 148
    - Polynom, 268
  - linear abhängig
    - Familie, 128
    - Teilmenge, 127
  - linear unabhängig
    - Familie, 128
    - Teilmenge, 127, 131
  - lineare Abbildung
    - schulische Konvention, 202
  - lineare Anteil, 202
  - lineare Gruppe
    - allgemeine, 146
    - spezielle, 354
  - lineare Hülle, 125
  - Linearfaktor, 269
  - Linearfaktoren
    - Zerlegung in, 270
  - Linearform, 188
  - Linearkombination, 125
  - Linksinverses, 198
    - in Kategorie, 576
  - linkskürzbar, 60, 261
  - Linksnebenklasse, 258, 464
  - linksspalten
    - Gruppenhomomorphismus, 471
    - Morphismus, 576
  - Linksteiler, 60, 260
  - Lösungsmenge, 103
  - Logarithmus
    - diskreter, 263
  - lokal endlich, 449
  - lokal nilpotent, 446
  - lokal unipotent, 454
  - Lorentzmetrik, 418
  - LR-Zerlegung, 533
  - LU-Zerlegung, 533
  - $\mu\{ \}$  Multimenge, 53
  - $M(f)$  Matrix von  $f$ , 160
  - Mackey
    - Lemma von, 425
  - Mächtigkeit, 31
  - Mag( $X, Y$ ) Homomorphismen von Magmas, 71
  - Magma, 71
  - Magmaoid, 595
  - Mat Matrixkategorie, 573
  - Mat( $n \times m; Z$ ) Matrizenmenge, 107
  - Matrix, 107
    - quadratische, 107
  - Matrixkategorie, 573
  - Matrixmultiplikation, 161
  - $\bigwedge^{\max}$  maximale äußere Potenz, 563
  - max, 121
  - maximal
    - Element, 123
  - Menge, 30
    - $M$ -Menge, 500
    - im Sinne der Logik, 613
    - leere Menge, 30
    - Potenzmenge, 33
    - Teilmenge, 32
  - Mengel, 613

- Mengenabbildung, 53  
Mengenfunktor, 609  
Mengenklammern, 30  
min, 59  
min, 121  
minimales  
  Element, 123  
Minor einer Matrix, 309, 481  
 $\text{Mod}_K$  Vektorräume über  $K$ , 572  
 $\text{Mod}_K(U \vee V, W)$  bilineare Abbildungen, 158  
 $\text{Modf}_K$  Vektorräume, endlich erzeugte, 580  
Modul  
  über Körper, 573  
modular  
  Verband, 154  
Möbiusfunktion  
  allgemeine, 187  
  der Zahlentheorie, 188  
mol, 262  
Mon  
  Monoidhomomorphismen, 71  
Mon Kategorie der Monoide, 572  
monic polynomial, 268  
Monoid, 63  
  additiv notiertes, 63  
  multiplikativ notiertes, 63  
Monoidhomomorphismus, 71  
 $\text{Mor}(\mathcal{C})$  Menge der Morphismen von  $\mathcal{C}$ , 571  
Morphismus  
  in Kategorie, 570  
  von euklidischen Räumen, 359  
  von Monoiden, 71  
Multiabbildung, 117  
  2-Multiabbildung, 52  
multilinear, 302  
Multilinearform, 303  
Multimatrix, 413  
Multimenge, 53  
Multinomialkoeffizient, 50  
Multiplikation  
  in Ring, 255  
Multiverknüpfung  
  von multilineareren Abbildungen, 549  
 $\mathbb{N}$  natürliche Zahlen, 30  
 $\mathbb{N}_0$ , 31  
Nachfolger, 235  
Nachschalten von Abbildung, 46  
natürliche Zahlen, 30, 234, 235  
Nebenklasse, 464  
Nebenklassengruppe, 470  
negativ  
  Vektor, 312  
negativ definit, 422  
negativ semidefinit, 422  
Negatives, 68  
Neograd, 373  
Neun als natürliche Zahl, 241  
Neunerlemma, 497  
neutrales Element, 63  
nichtausgeartet  
  Bilinearform, 420  
  Paarung, 425  
  quadratische Form, 414  
nichtkürzbar, 60, 261  
nichtnegativ  
  Vektor, 312  
nilpotent  
  Element, 256  
  Endomorphismus, 178  
  lokal, 446  
nilpotenter Anteil  
  eines Endomorphismus, 451  
Noether'scher Isomorphiesatz, 470  
Norm, 332  
  einer komplexen Zahl, 183  
  eines Vektors, 340  
normal  
  Endomorphismus, 449

- Untergruppe, 468
- Vektor, 347
- Normalteiler, 468
- normiert
  - Polynom, 268
- Null, 235
- Null-Element, 63
- Nullkegel, 437
- Nullring, 256
- Nullstelle, 268
- Nullteiler, 261
- Nullvektor, 112
- Nullvektorraum, 115
- Nullwinkel, 370
- numerisch
  - Polynom, 280
- $O(V)$  orthogonale Automorphismen, 354
- $O(n)$  orthogonale Matrizen, 355
- $O_{\text{aff}}(E)$  orthogonalaffine Gruppe, 439
- $O(V, S)$  orthogonale Gruppe, 358
- $O_{\text{aff}}(E, S)$  Gruppe der orthogonalaffinen Automorphismen, 358
- oBdA ohne Beschränkung der Allgemeinheit, 56
- Objekt einer Kategorie, 570
- oder, 54
- Oktaeder, 515
- Operation
  - eines Monoids, 500
  - triviale
    - von Gruppe, 500
  - von Grundkörper auf Vektorraum, 111
  - von Menge auf Menge, 500
- $F^{\text{opp}}$  für Funktor  $F$ , 579
- $X^{\text{opp}}$  Menge  $X$  mit opponierter Verknüpfung, 77
- opponiert
  - Gruppe, 77
  - Kategorie, 578
- Verknüpfung, 77
- $\text{or}(V)$  Orientierungsmenge eines Vektorraums, 311
- $\text{or}^{\text{alg}}$  algebraische Orientierungsmenge, 311
- orbit, 502
- $\text{ord } g$  Ordnung von  $g$ , 472
- Ord Kategorie der geordneten Mengen, 572
- Ordnung, 121
  - für Teilordnung, 121
  - einer Gruppe, 473
  - einer Nullstelle, 270
  - lineare, 121
  - partielle, 121
  - totale, 121
  - von Gruppenelement, 472
- Ordnungsrelation, 121
- Orientierung
  - von affinem Raum
    - durch Erzeugendensystem, 316
  - von Vektorraum, 310
- Orientierungsgerade
  - eines Vektorraums, 555
- Orientierungsmenge
  - algebraische, 311
  - eines Vektorraums, 311
- orthogonal, 337, 438
  - Affinität, 439
  - Automorphismus, 358
  - Komplement, 349
  - lineare Abbildung, 353
  - Matrix, 355
  - Teilräume, 349
  - Vektoren, 347
- orthogonalaffine Gruppe, 439
- Orthogonalbasis, 419
- orthogonale Gruppe, 333, 358
- orthogonale Projektion, 349
- Orthogonalraum, 348
- Orthonormalbasis, 348

- Orthonormalsystem, 348
- $\mathcal{P}(X)$  Potenzmenge, 33
- $\mathcal{P}_1(X)$  einelementige Teilmengen von  $X$ , 53
- $\prod$  Produkt, 64
  - von Zahlen, 12
- Paar
  - angeordnetes, 36
  - ungeordnetes, 53
- Paarung
  - bilineare, 425
  - kanonische, 191
  - nichtausgeartete, 425
- parallel
  - affine Teilräume, 206
- Parallelogrammregel, 339
- Partialbruchzerlegung, 283
- partiell
  - Ordnung, 121
- Partition
  - einer Menge, 505
- Pascal'sches Dreieck, 15
- Permutation, 68
- Permutationsmatrix, 173
- Pfaff'sche Determinante, 431
- Pfeile, 594
- Phase, 132
- platonisch
  - Eckenmenge, 521
  - Körper, 521
- Polarenmenge, 228
- Polarisierungsidentität, 381
- Polarzerlegung, 401
  - eines Endomorphismus, 403
- Polordnung, 518
- Polstelle
  - von rationaler Funktion, 282
- Polstellenordnung, 282
- Polyeder
  - konvexer, 227
- Polynom
  - ganzwertiges, 280
  - konstantes, 266
  - numerisches, 280
- Polynomring, 266
- Polytop
  - konvexes, 227
- poset, 121
- positiv
  - Vektor, 312
- positiv definit, 332, 421
  - Bilinearform, 344
  - Endomorphismus, 403
  - hermitesche Matrix, 401
  - symmetrische Matrix, 390
- positiv semidefinit, 421
  - Endomorphismus, 403
  - hermitesche Matrix, 401
  - symmetrische Matrix, 390
- positivlinear, 231
- Pot(X) Potenzmenge, 33
- Potenz
  - $p$ -Potenz, 479
  - in Monoid, 241
  - Primpotenz, 479
  - Primzahlpotenz, 479
- Potenzmenge, 33, 126
- Potenzreihe
  - formale, 275
- pr Projektion aus Produkt, 600
- pr, Projektion aus Produkt, 604
- $\text{pr}_X$ 
  - Projektion, 44
- $\text{pr}_i$ 
  - Projektion, 116
- Prähilbertraum, 347
- prim
  - Restklasse, 260
- Primfaktorzerlegung
  - Existenz, 249
- Primitivwurzel, 488

- Primkörper, 262
- Primpotenz, 479
- Primzahl, 248
- Primzahlpotenz, 479
  - echte, 479
- Primzahlzwillinge, 249
- prinzipaler homogener  $G$ -Raum, 502
- produit extérieur, 561
- Produkt
  - balanciertes, 512
  - in Kategorie
    - von Familie, 599
    - von zwei Objekten, 598
  - von Gruppen, 70
  - von Kategorien, 579
  - von Matrizen, 161
  - von Mengen, 599
  - von Sequenzen, 495
  - von Vektorräumen, 603
    - endliches, 120
- Produktmorphismus, 598
- Produktorientierung, 315
- Projektion
  - bei zwei Mengen, 44
  - in Kategorie, 598, 599
  - längs Teilraum, 155
  - von kartesischem Produkt, 116
- pseudoeuklidisch, 438
  - orientiert, 438
- $\text{pt} = \text{pt}(\mathcal{C})$  finales Objekt von  $\mathcal{C}$ , 576
- Punkt, 30
  - von affinem Raum, 199
  - von Köcher, 594
- Punktgruppe, 516
- Punktspiegelung, 203, 382
  - räumliche, 386
- Pythagoras, Satz von, 347
- pythagoreische Zahlentripel, 279
- $\mathbb{Q}$  rationale Zahlen, 30
- QR-Zerlegung, 390
- quadratisch
  - Matrix, 107, 168
  - Polynom, 268
- quadratische Form, 490
  - homogene, 413
  - auf  $\mathbb{R}^n$ , 394
  - inhomogene, 427
- Quantor, 55
- quasiinverser Funktor, 592
- Quaternionen, 288
- Quaternionengruppe, 289
- Quaternionenring, 289
- Quersumme, 260
- quiver, 595
- Quot Quotientenkörper, 280
- Quotient, 258, 585
  - von affinem Raum, 493
  - von Gruppe, 470
- Quotientenkörper, 280
- Quotientenorientierung, 315
- Quotientenvektorraum, 491
- Rad Radian
  - für orientierten Winkel, 374
- Radian, 373, 374
- Radikal
  - einer Bilinearform, 420
- Raleigh-Quotient, 399
- Ralg
  - Kategorie der Ringalgebren, 572
  - Ringalgebrenhomomorphismen, 606
- rang Rang einer abelschen Gruppe, 479
- Rang
  - einer abelschen Gruppe, 479
  - einer Bilinearform, 420
  - einer linearen Abbildung, 173
  - einer Matrix, 172
- rank, 172
- rationale Funktion, 282
- rationale Zahlen, 30
- Raum, 30

- affiner, **199**
- reeller, **199**
- Raum-Zeit-Punkte, 434
- raumartig
  - Vektor, 436
- Raumzeit, 434
- Realisierung
  - eines Diagrammschemas, 595
- Realisierungsfaktor, 577
- Realteil
  - bei komplexen Zahlen, 183
  - bei Quaternionen, 289
- rechter Winkel, 370
- Rechtsinverses, 142, 198
  - in Kategorie, 576
- rechtskürzbar, 60, 261
- Rechtsmenge, 508
- Rechtsnebenklasse, 464
- Rechtsoperation, 508
- rechtsspaltend
  - Gruppenhomomorphismus, 471
  - Morphismus, 576
- Rechtsteiler, 60, 260
- Rechtstorsor, 508
- redundant, 127
- reell
  - Raum, **199**
- reelle Form
  - von komplexem Vektorraum, 409
- reeller Vektorraum, 22
- Reellifizierung, 137
- reflexiv
  - Relation, 121
- regulär
  - Matrix, 168
- Relation
  - auf einer Menge, 121, 243
  - mehrstellige, 121
  - zwischen zwei Mengen, 121
- Relativitätstheorie, 434
- Repräsentant, 244, 258, 464
- Repräsentantensystem, 244, 258
- Restklasse, 258
  - prime, 260
- rg Rang einer Matrix, 172
- Richt Richtungsraum, 199
- Richtungsanteil, 202
- Richtungsraum, **199**
  - eines affinen Teilraums, 204
  - schmutziger, 112
- Richtungsvektor, **199**
- Ring, 255
- Ring Kategorie der Ringe, 572
- Ring Ringhomomorphismen, 256
- Ringalgebra, **606**
- Ringhomomorphismus, 256
- Rng Kategorie der nicht unitären Ringe, 572
- RSA-Verfahren, 477
- Russell'sches Paradoxon, 40
- $S^1$  Einheitskreis, 185
- $S^1$  versus  $U(1)$ , 185
- $\Sigma_n$  symmetrische Gruppe, 291
- $S_n$  symmetrische Gruppe, 291
- $S(n)$  Standardbasis des  $K^n$ , 129
- $\sum$  Summe
  - von Zahlen, 11
- Schema, 611
- Schiefkörper, 101, 287
- schiefflinear, 346
- schmutzig
  - für umgangssprachlich, 88
- Schnitt, 142
  - von Mengensystem, 126
  - von Morphismus, 576
  - zweier Mengen, 34
- Schwerpunkt, 213
- Sechs als natürliche Zahl, 241
- Sekunde, 314
- Selbstabbildung, 59
- selbstadjungiert, 397

- senkrecht, 337
- Sequenz
  - kurze exakte, 494
- Sesquilinearform, 346
- Sieb des Eratosthenes, 248
- Sieben als natürliche Zahl, 241
- $\text{sign}(a)$  Vorzeichen von  $a$ , 310
- Signatur, 422
- Signum, 295
- Signum einer Permutation, 291
- $\sin_a$  analytischer Sinus, 371
- $\sin_g$  geometrischer Sinus, 371
- Singulärwert
  - einer Abbildung, 424
  - einer Matrix, 424
- Singulärwertzerlegung, 424
- Sinus, 370
  - analytischer, 371
  - geometrischer, 371
- Sinus-Satz, 377
- Skalar, 111
- Skalarprodukt, 332, 344
  - auf komplexem Vektorraum, 346
  - geometrisches, 556
- Skalarproduktnorm, 347
- Skalarproduktraum, 332, 347
  - affiner, 382
- skalarproduktverträglich, 353
- skew field, 288
- $\text{SL}(V)$  spezielle lineare Gruppe, 354
- $\text{SL}(n; K)$  spezielle lineare Gruppe, 354
- Slater-Determinante, 565
- Smith-Normalform, 170, 177
- Smith-Zerlegung, 486
- $\text{SO}(V)$  spezielle orthogonale Automorphismen, 354
- $\text{SO}(n)$  spezielle orthogonale Matrizen, 355
- spaltend
  - kurze exakte Sequenz, 495
- Spaltenindex, 107
- Spaltenrang, 172
- Spaltung
  - bei Gruppen, 471
  - bei Gruppen, 471
  - von Morphismus, 576
- span Spann, 125
- Spann
  - in Vektorraum, 125
- Spat, 380
- Spatprodukt, 380
  - geometrisches, 555
- Spektralradius
  - endlichdimensionaler Fall, 453
- speziellen Relativitätstheorie, 436
- Spiegelung, 382
  - orthogonale, 361, 391
- Spingruppe, 355
- Spur
  - einer Matrix, 178
  - eines Endomorphismus, 178
  - endlichen Ranges, 179
- stabil
  - Teilmenge unter Abbildung, 446
  - Teilmenge unter Selbstabbildung, 53
  - unter aufsteigenden Vereinigungen, 144
  - unter Monoid, 502
- Stabilisator, 501, 502
- stabilisiert, 53
- Standard-Skalarprodukt, 332, 346
- Standardbasis, 129
- Standardorientierung, 311
  - der komplexen Zahlenebene, 368
  - von pseudoeuklidischer Struktur, 438
- Standardorientierung des Nullraums, 311
- Standgruppe
  - für Isotropiegruppe, 501
- Strahl, 339
- Streckung, 203
- Streichmatrix, 307

- Struktur
  - $(\mathcal{S}, v)$ -Struktur, 582
  - bilineare
    - auf reellem Vektorraum, 437
  - strukturverträglich
    - Abbildung, 437
  - $SU(V)$  spezielle unitäre Automorphismen, 354
  - $SU(n)$  spezielle unitäre Matrizen, 355
  - Summanden, 11
  - Summe
    - von Untervektorräumen, 604
    - von Vektorräumen, 603
  - Surjektion, 46
  - surjektiv
    - Abbildung, 46
  - Sylvester
    - Trägheitssatz, 422
  - Symmetrie
    - für Relation, 244
  - Symmetriebewegung, 514
  - Symmetriegruppe, 502
  - symmetrisch
    - bilineare Abbildung, 301
    - Bilinearform, 344
    - Matrix, 390
  - symmetrische Gruppe, 291
  - symplektisch
    - Vektorraumautomorphismus, 431
  - symplektische Form, 430
  - symplektischer Vektorraum, 430
  - System von Teilmengen, 126
  - $\tau = 2\pi$ , 374
  - $\mathbb{T}$  Zeit, 201, **314**
  - $T_KV$  Tensoralgebra, 608
  - Teilen in Polynomringen, 269
  - Teiler, 250, 260
  - teilerfremd
    - Elemente eines Krings, 261
    - ganze Zahlen, 250
- teilgeordnet
  - induktiv, 139
  - streng induktiv, 139
- Teilmenge, 32
  - echte, 32
- Teilordnung, 121
- Teilraum, 123
- Teilring, 257
- teilt, 250, 260
- $Ten_KV$  Tensoralgebra, 608
- Tensor
  - physikalisch, ko-kontravariant, 552, 553
  - physikalisch, kontravariant, 550, 552
  - physikalisch, kovariant, 551
- Tensoralgebra, 608
- Tensorprodukt
  - von linearen Abbildungen, 539
  - von Vektorräumen, 536
- Tetraeder, 515
- Tetraedergruppe, 514
- top einelementiger Raum, 576
- Top topologische Räume, 572
- Top\* bepunktete topologische Räume, 572
- $A_{\text{tor}}$  Torsionsuntergruppe von  $A$ , 475
- torsionsfrei
  - Gruppe, 475
- Torsionsuntergruppe, 475
- Torsor, 505
  - Rechtstorsor, 508
  - von links, 502
- Totalität
  - für Relation, 121
- tr Spur
  - $\text{tr}_K$  bei Grundkörper  $K$ , 178
  - einer Matrix, 178
  - eines Endomorphismus, 178
  - trace, deutsch Spur, 178
- Trägheitssatz
  - Sylvester'scher, 422

- trans, 200
- Trans Transformationen, 589, 597
- Transformation
  - von Funktoren, 586
  - von Köchermorphismen, 595
- transitiv
  - Gruppenwirkung, 502
  - Relation, 121
- Translation
  - von affinem Raum, 199
- transponiert
  - Abbildung
    - bei Vektorräumen, 192
    - Matrix, 165
- Transposition, 291
- treu
  - Funktor, 580
- trigonalisierbar, 319
- Tripel, 116
- trivial
  - Operation
    - von Gruppe, 500
- Tupel
  - angeordnete, 116
- Typ
  - von reeller quadratischer Form, 422
- $\sqcup$  Koprodukt, 601
- $U(V)$  unitäre Automorphismen, 354
- $U(n)$  unitäre Matrizen, 355
- $U(1)$  versus  $S^1$ , 185
- $\mathfrak{U}$ Ens Mengen  $X \in \mathfrak{U}$ , 571
- $\mathfrak{U}$ -Kategorie, 581
- $U_{\min}$ , 192
- Umkehrfunktion, 49
- $\mathfrak{U}\text{Mod}_K$ , 572
- $\mathfrak{U}\text{Mod}_K$  Vektorräume  $V \in \mathfrak{U}$ , 573
- unendlich
  - Menge, 234
- Unendlichkeitsaxiom, 234
- ungerade
- Permutation, 291, 295
- Zahl, 259
- unipotent
  - Endomorphismus, 454
  - lokal unipotent, 454
- unitär
  - lineare Abbildung, 353
  - Matrix, 355
  - Raum, 347
- unitärassoziativ, 65
- Magmaoid, 595
- Unitärassoziativität, 500
- universell
  - alternierende Abbildung, 560
  - multilineare Abbildung, 536
- Universelle Eigenschaft
  - des Raums der Äquivalenzklassen, 244
- Universum, 613
- Unter-, 73
- Unteralgebra, 607
- Untergruppe, 73, 246
  - erzeugt von Teilmenge, 247
  - triviale, 75, 247
- Unterkategorie, 575
- Untermonoid, 73
- Unterobjekt
  - $(\mathcal{S}, v)$ -Unterobjekt, 584
- Unterringalgebra, 607
- Untervektorraum, 123
- unverkürzbar
  - Erzeugendensystem, 130
- unverlängerbar
  - linear unabhängige Teilmenge, 130
- Urbild
  - von Menge, 45
- van-de-Ven-Diagramm, 36
- Vandermonde-Determinante, 309
- Variable
  - von Polynom, 266

- Vektor
  - Element eines Vektorraums, 111
- Vektorprodukt, 379
- Vektorraum, 111
  - komplex konjugierter, 405
- Verband, 85
  - modularer, 154
- Vereinigung, 34
  - aufsteigende, 144
  - von Mengensystem, 126
- vergeßliche komplexe Zahlen, 182
- Vergiß-Funktor, 579
- Verjüngung von Tensoren, 545
- Verknüpfung
  - auf einer Menge, 57
  - auf Köcher, 595
  - induzierte, 76
  - koinduzierte, 76, 598
  - komponentenweise, 59
  - von Abbildungen, 45
  - von Morphismen, 570
- Verknüpfungstafel, 58
- verkürzbar
  - Erzeugendensystem, 130
- verlängerbar
  - linear unabhängige Teilmenge, 130
- Verschlüsselung
  - Diffie-Hellman, 263
  - RSA-Verfahren, 477
- Verschraubung, 384
- vertex of quiver, 595
- verträglich
  - Orientierungen, 315
- Vielfachheit
  - einer Nullstelle, 270
- Vier als natürliche Zahl, 241
- voll
  - Funktor, 580
  - Rang, 172
  - Unterkategorie, 575
- vollständige Induktion, 235
- volltreu, Funktor, 580
- Volumenform
  - geometrische, 555
- Volumenprozent, 115
- Vorschalten von Abbildung, 46
- $\bar{W}$  Winkelmenge, 368
- $W$  Winkelgruppe, 368
- Wahrheitstafel, 59
- wedge-product, 561
- Wert, 42
- Wertebereich, 44
- Wilson
  - Satz von, 266
- Winkel, 367, 368, 371, **374**
  - echt stumpfer, 391
  - gerichteter, 368
  - gestreckter, 370
  - negativ, 367
  - positiv, 367
  - rechter, 370
- Winkelgruppe
  - abstrakte, 368
  - konkrete, 367
- Winkelmaß, 373
- Winkelmenge
  - abstrakte, 368
- Wirkung
  - eines Monoids, 500
- Witt, Satz von, 428
- wohldefiniert, 244
- Würfel, 515
  - Zeichnung, 391
- Würfelgruppe, 514
- Wurzel
  - von Polynom, 268
- Yoneda-Einbettung, 609
- $Z_n$  zyklische Gruppe, 473
- $\mathbb{Z}$  ganze Zahlen, 30, **246**
- $\mathbb{Z}_n$  zyklische Gruppe, 473

**Zahl**

- ganze, 30
- gerade, 259
- Hamilton'sche, 288
- komplexe, 181
- natürliche, 30
- rationale, 30
- ungerade, 259

Zahldarstellungen, 242

Zahlenebene, 183

Zehn als natürliche Zahl, 242

Zeilenindex, 107

Zeilenrang, 172

Zeilenstufenform, 105

Zeilenvektor, 165

Zeit, 314

zeitartig

- Vektor, 436

Zeiteinheit

- nichtrelativistische, 314
- relativistische, 438

Zeitpunkt, 201

Zeitspanne, 201, 314

Zielkategorie, 577

Zorn'sches Lemma, 143

zusammenhängend

- Graph, 526

Zusammenhangskomponente

- eines Graphen, 526

Zwei als natürliche Zahl, 241

Zweistrahl, 367

- angeordneter, 367

zyklisch

- Anordnung, 50

- Gruppe, 472