LINEARE ALGEBRA 1

Wolfgang Soergel

23. März 2018

Inhaltsverzeichnis

1 Gleichungssysteme und Vektorräume **5**
1.1 Lösen linearer Gleichungssysteme 5
1.2 Vektorräume 14
1.3 Endliche Produkte von Mengen 18
1.4 Ordnungen auf Mengen* 22
1.5 Untervektorräume 25
1.6 Lineare Unabhängigkeit und Basen 28
1.7 Dimension eines Vektorraums 33
1.8 Austauschsatz von Steinitz* 39
1.9 Auswahlaxiom und Zorn'sches Lemma* 40

2 Lineare Abbildungen **47**
2.1 Homomorphismen und Isomorphismen 47
2.2 Dimensionsformel für lineare Abbildungen 51
2.3 Räume von linearen Abbildungen 55
2.4 Lineare Abbildungen $K^n \to K^m$ und Matrizen 59
2.5 Einige Eigenschaften von Matrizen 67
2.6 Ergänzungen zu linearen Abbildungen* 72

3 Räume mit und ohne Koordinaten **74**
3.1 Affine Räume und affine Abbildungen 74
3.2 Affine Teilräume 78
3.3 Affine Räume und ihre Geraden 82
3.4 Baryzentrische Koordinaten* 85
3.5 Abstrakte lineare Abbildungen und Matrizen 90
3.6 Möbiusfunktion* 95
3.7 Dualräume und transponierte Abbildungen 96

4 Zahlen **106**
4.1 Der Körper der komplexen Zahlen 106
4.2 Konstruktion der natürlichen Zahlen* 114
4.3 Untergruppen der Gruppe der ganzen Zahlen 120
4.4 Primfaktorzerlegung 122

5 Ringe und Polynome **128**
5.1 Ringe 128
5.2 Restklassenringe des Rings der ganzen Zahlen 131
5.3 Polynome 139
5.4 Polynome als Funktionen* 149

5.5 Äquivalenzrelationen 153
5.6 Quotientenkörper und Partialbruchzerlegung 156
5.7 Quaternionen* 162

6 Determinanten und Eigenwerte **166**
6.1 Das Signum einer Permutation 166
6.2 Die Determinante und ihre Bedeutung 170
6.3 Charakterisierung der Determinante 176
6.4 Rechenregeln für Determinanten 180
6.5 Algebraische Orientierung 185
6.6 Eigenwerte und Eigenvektoren 190

7 Geometrische Ergänzungen* **200**
7.1 Affine Inzidenzebenen 200
7.2 Projektive Räume 212
7.3 Projektive Inzidenzebenen 215
7.4 Lineare Konvexgeometrie 223

8 Danksagung **239**

9 Die Vorlesung LA1 im Wintersemester 14/15 **240**

Literaturverzeichnis **244**

Index **245**

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.

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.

1.1 Lösen linearer Gleichungssysteme

1.1.1. Ich erinnere aus [GR] 3.4.2 die Definition eines Körpers.

Definition 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, 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 $K \backslash \{0_K\}$ ist unter der Multiplikation ihrerseits eine Gruppe, die **multiplikative Gruppe** des Körpers;
3. Es gilt das **Distributivgesetz**

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

Fordert man hier nicht die Kommutativität der Multiplikation und fordert zusätzlich das „Distributivgesetz für die Multiplikation von rechts“ $(b + c) \cdot a = (b \cdot a) + (c \cdot a) \quad \forall a, b, c \in K$, so heißt unsere Struktur ein **Schiefkörper**.

1.1.3. 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 Fälle denke, Elemente eines allgemeinen Körpers K auch oft als „Zahlen“ bezeichnen. Gegeben seien n Gleichungen in m Unbekannten alias **Variablen** $x_1, \ldots, x_m$ von der Gestalt

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

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,

$$
\begin{aligned}
x_1 + 3x_2 &= 1 \\
2x_1 + 2x_2 + x_3 &= 2 \\
4x_1 + 6x_2 + x_3 &= 8
\end{aligned}
$$

Ein lineares Gleichungssystem mit drei Gleichungen und drei Unbekannten.

$$
\begin{aligned}
2y - 17z &= 0 \\
4x + 22y + z &= 0
\end{aligned}
$$

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.

$$
0x = 1
$$

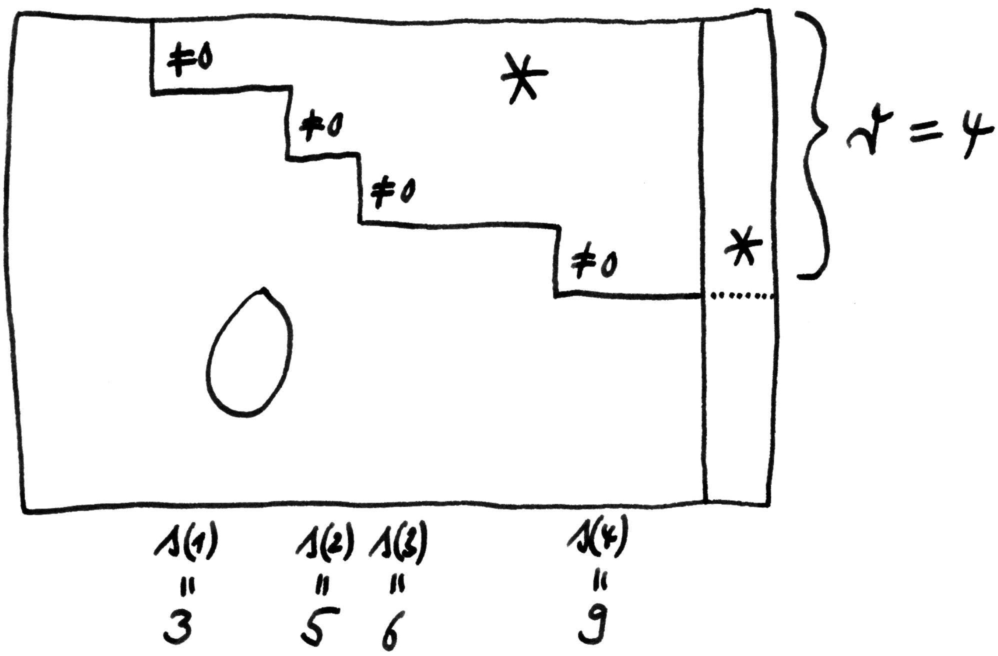
Ein inhomogenes lineares Gleichungssystem mit einer Gleichung und einer Unbekannten und leerer Lösungsmenge.

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 wie $x_1x_2x_3$ vorkommen. Die a_{ij} heißen in diesem und ähnlichen Zusammenhängen **Koeffizienten** von lateinisch „coefficere" 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 1.3.7 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, der sogenannten **Lösungsmenge** L unseres Gleichungssystems.

1.1.4. 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 entsteht, indem man alle b_i zu Null setzt, heißt das zugehörige **homogenisierte** Gleichungssystem.

Bemerkung 1.1.5 (**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, aber das hätte unser Gleichungssystem dann auch wieder 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 eine Computer zu programmieren. Beim Programmieren eines Computers muß die Eindeutigkeit der Anweisungen die oberste Priorität sein, beim Schreiben und Erklären für Menschen kommt es eher auf die Übersichtlichkeit an und bei Mehrdeutigkeiten kann man erwarten, daß die aus dem Kontext heraus aufgelöst werden können 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.

1.1.6. 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:



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. 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.

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 $1 \leq s(1) < s(2) < \ldots < s(r) \leq m$ 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 $\mu \geq s(i)$.

1.1.7. Es ist üblich und erspart viel 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**

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

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.

1.1.8 (**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 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.

1.1.9 (**Lösungsmenge bei Zeilenstufenform**). Die Lösungsmenge eines linearen Gleichungssystems in Zeilenstufenform ist schnell bestimmt: Ist eine der Zahlen $b_{r+1}, \ldots, b_n$ nicht Null, so besitzt es gar keine Lösung. Gilt dahingegen $b_{r+1} =$

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

$$\Big\downarrow$$

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

$$\Big\downarrow$$

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

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.

$\ldots = b_n = 0$, können wir Zahlen x_μ für μ verschieden von den Spaltenindizes $s(1), \ldots, s(r)$ der Stufen beliebig vorgeben und finden für jede solche Vorgabe der Reihe nach eindeutig bestimmte Zahlen $x_{s(r)}, x_{s(r-1)}, \ldots, x_{s(1)}$ derart, daß das entstehende m-Tupel $(x_1, \ldots, x_m)$ eine Lösung unseres Gleichungssystems ist.

1.1.10. Eine Abbildung der Produktmenge $\{1, \ldots, n\} \times \{1, \ldots, m\}$ 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 dieses Datum 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. Die Menge aller $(n \times m)$-Matrizen mit Koeffizienten in einer Menge Z notieren wir

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

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

Ergänzung 1.1.11 (**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" hervorzugehen. 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 6.2.1 ein.

Satz 1.1.12 (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 $c = (c_1, \ldots, c_m)$ eine Lösung unseres linearen Gleichungssystems und $d = (d_1, \ldots, d_m)$ eine Lösung des homogenisierten Systems, so ist offensichtlich die komponentenweise Summe $c \dotplus d = (c_1 + d_1, \ldots, c_m + d_m)$ eine Lösung des ursprünglichen Systems. Ist andererseits $c' = (c'_1, \ldots, c'_m)$ eine weitere Lösung unseres linearen Gleichungssystems, so ist offensichtlich die komponentenweise Differenz $d = (c'_1 - c_1, \ldots, c'_m - c_m)$ eine Lösung des homogenisierten

Systems, für die gilt $c' = c \dot{+} d$ mit unserer komponentenweisen Addition $\dot{+}$ aus [GR] 1.2.7. □

1.1.13 (**Unabhängigkeit der Stufenzahl vom Lösungsweg**). Die vorstehenden Überlegungen zeigen, wie man die Lösungsmenge jedes linearen Gleichungssystems bestimmen kann. Man erhält dabei nach 1.1.9 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" $j \neq s(1), \ldots, s(r)$ 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 $(x_{j+1}, x_{j+2}, \ldots, x_m)$, das zu einer Lösung $(x_1, x_2, \ldots, x_m)$ ergänzbar ist, nur ein x_j derart, daß auch $(x_j, x_{j+1}, x_{j+2}, \ldots, x_m)$ zu einer Lösung $(x_1, x_2, \ldots, x_m)$ ergänzbar ist? Genau dann lautet die Antwort „ja", wenn in der j-ten Spalte eine neue Stufe beginnt.

1.1.14 (**Unabhängigkeit der Stufenzahl von der Variablenreihung**). Sicher könnten wir auch vor dem Anwenden des Gauß-Algorithmus zuerst unsere Variablen umnummerieren alias die Spalten unserer Koeffizientenmatrix vertauschen. Wir erhielten wieder eine Bijektion eines K^u 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 willkürlich vertauschen, bevor wir den Gauß-Algorithmus durchführen? Die Antwort lautet wieder „Ja", aber hierzu ist mir kein ganz elementares Argument mehr eingefallen. Darüber 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 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.

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

$$\Downarrow$$

$$\left(\begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 0 & -4 & 1 & 0 \end{array}\right) \quad \rightsquigarrow \quad \begin{array}{l} x_3 \text{ freier Parameter,} \\ x_2 = x_3/4 \\ x_1 = 1 - (3/4)x_3 \end{array}$$

Ein lineares Gleichungssystem mit zwei Gleichungen und drei Unbekannten, dessen Lösungsmenge nach unser allgemeinen Theorie für jedes x_3 genau einen Punkt (x_1, x_2, x_3) enthält, 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 Lösung lautet $(1 - (3/4)\lambda, \lambda/4, \lambda)$ für variables λ.

1.2 Vektorräume

Definition 1.2.1. Ein **Vektorraum** V **über einem Körper** K ist ein Paar bestehend aus einer abelschen Gruppe $V = (V, \dot{+})$ und einer Abbildung

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

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

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

Wie bei der Axiomatik eines Körpers [GR] 3.4.2 heißen die ersten beiden Gesetze die **Distributivgesetze**. In Analogie zu der Sprechweise bei Mengen mit Verknüpfung heißt das dritte Gesetz das **Assoziativgesetz**.

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 [LA2] 1.1.14 einführen und das aus zwei Vektoren einen Skalar macht. Ich habe oben aus didaktischen Gründen die Addition von Vektoren $\dot{+}$ 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 λ, μ und alle Vektoren $\vec{v}, \vec{w}$ gelten möge

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

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 setzen $\lambda\vec{v} = \vec{0}$ für alle $\lambda \in K$ und $\vec{v} \in V$.

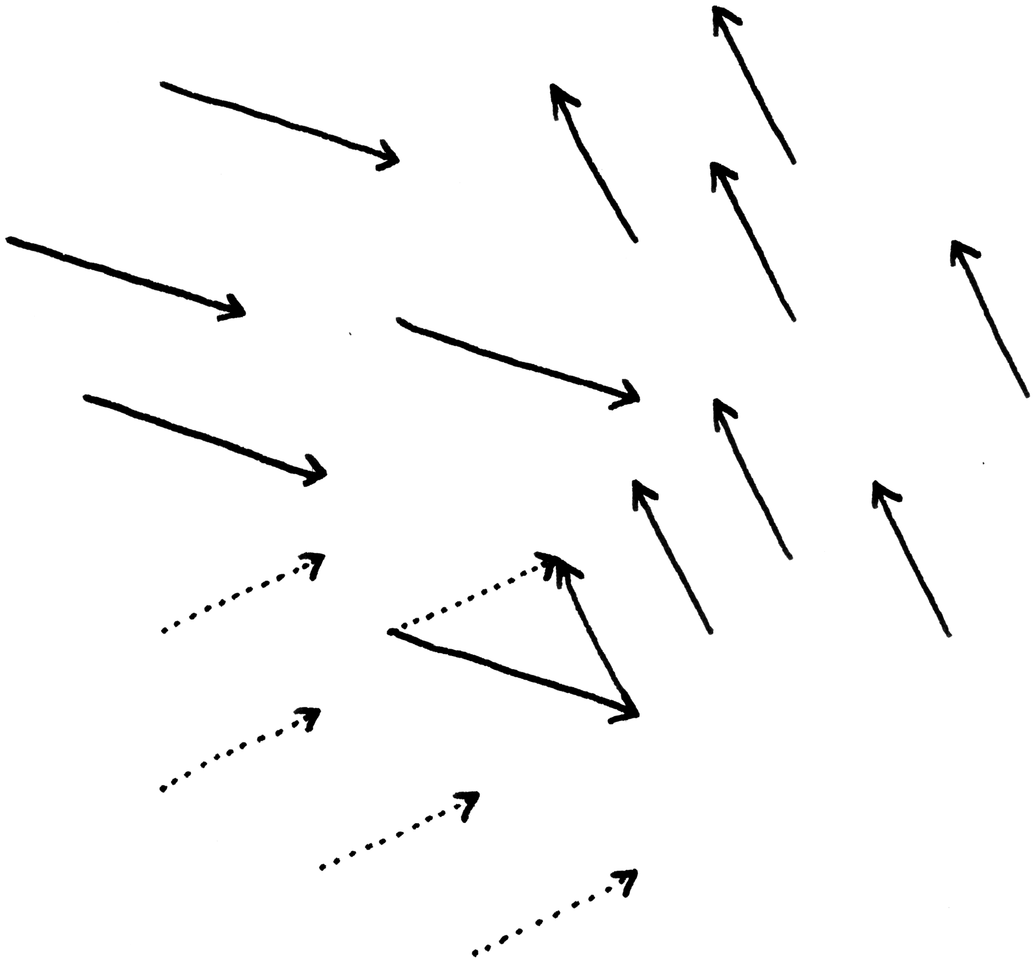
Beispiel 1.2.3 (**Die schmutzige Anschauung**). Ich stelle mir als Vektorraum gerne wie in [GR] 1.2.5 ausgeführt die Menge V der Parallelverschiebungen der schmutzigen Ebene oder auch die Menge V der Parallelverschiebungen des schmutzigen Raums der Anschauung vor, mit der „Hintereinanderausführung“ als 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 basierende aseptisch steril perfekte Mathematik zu schmutzig ist, um als echtes Beispiel durchzugehen.

Ergänzung 1.2.4. Ich rede hier bewußt vom „Raum der Anschauung“ und nicht vom „Anschauungsraum“, da ich mir letztere Bezeichnung für das in [LA2] 2.3.16 erklärte Gebilde der Mengenlehre vorbehalten will, das zwar den Raum der Anschauung modellieren soll, das ich aber doch sprachlich von diesem absetzen will. 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 1.2.5 (**Funktionenräume als Vektorräume**). Gegeben eine Menge X und ein Körper K ist die Menge $\operatorname{Ens}(X, K)$ aller Abbildungen von $X \to K$ 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. Insbesondere erhält so auch die Menge $\operatorname{Mat}(n \times m; K)$ aller $(n \times m)$-Matrizen mit Einträgen in einem Körper K aus 1.1.10 die Struktur eines K-Vektorraums.

Beispiel 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 $\dot{+}$ und der komponentenweisen Multiplikation mit Skalaren versehen.

Ergänzung 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 dazu, daß



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

man „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 1.2.8 (**Ursprung der Terminologie**). Die Bezeichnung „Vektor“ kommt von lateinisch „vehere“ für „fahren, transportieren“. Sie rührt von unserem Beispiel [GR] 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 Grundkörpers.

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 $0_K\vec{v} = (0_K + 0_K)\vec{v} = 0_K\vec{v} \dot{+} 0_K\vec{v}$ und Subtraktion von $0_K\vec{v}$ alias Addition seines Negativen $-0_K\vec{v}$ auf beiden Seiten liefert $\vec{0} = 0_K\vec{v}$.

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 $\vec{v} \dot{+} (-1_K)\vec{v} = 1_K\vec{v} \dot{+} (-1_K)\vec{v} = (1_K + (-1_K))\vec{v} = 0_K\vec{v} = \vec{0}$. Damit ist $(-1_K)\vec{v}$ in der Tat das additive Inverse von $\vec{v}$.

Beispiele 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 1.2.12. Gegeben ein Körper K wird jede einelementige Menge V vermittels 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 einfach für die verschiedensten Dinge herhalten.

Beispiel 1.2.13. Die additive Gruppe $\mathbb{R}$ der reellen Zahlen ist in offensichtlicher Weise ein $\mathbb{Q}$-Vektorraum. Ist allgemeiner $\varphi : K \to L$ ein Körperhomomorphismus, so wird die additive Gruppe L ein K-Vektorraum vermittels der Multiplikation mit Skalaren $\lambda a := \varphi(\lambda)a$.

Übungen

Übung 1.2.14 (**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 1.2.15. 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 [GR] 3.4.12 stets $n_K\vec{v} = n\vec{v}$ oder ausgeschrieben in unserer Notation [GR] 3.2.10 für iterierte Verknüpfungen $(n^+1_K)\vec{v} = n^+\vec{v}$. Hinweis: Die Fälle $n = 0$ und $n = (-1)$ dieser Aussage wurden im übrigen bereits in 1.2.9 und 1.2.10 besprochen.

Ergänzende Übung 1.2.16. Für eine vorgegebene abelsche Gruppe $(V, +)$ gibt es höchstens eine Abbildung $\mathbb{Q} \times V \to V$ derart, daß sie mit dieser Abbildung als Multiplikation mit Skalaren ein $\mathbb{Q}$-Vektorraum wird.

Ergänzende Übung 1.2.17. 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 [GR] 3.2.18.

Übung 1.2.18. Gegeben eine Menge X und ein Körper K und ein K-Vektorraum V ist auch die Menge $\mathrm{Ens}(X, V)$ aller Abbildungen $X \to V$ 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 1.2.5.

Ergänzende Übung 1.2.19. Ist $\varphi : L \to K$ 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.

1.3 Endliche Produkte von Mengen

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 jedoch auch für mehr Mengen $X_1, \ldots, X_n$ das kartesische Produkt

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

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 $(x_1, \ldots, x_n)$. Die Mengen X_i heißen die **Faktoren** unseres kartesischen Produkts.

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

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

$$\begin{array}{rccc} \mathrm{pr}_i: & X_1 \times \ldots \times X_n & \to & X_i \\ & (x_1, \ldots, x_n) & \mapsto & x_i \end{array}$$

Wir erhalten dann für jede weitere Menge Z eine Bijektion

$$\begin{array}{ccc} \mathrm{Ens}(Z, X_1 \times \ldots \times X_n) & \stackrel{\sim}{\to} & \mathrm{Ens}(Z, X_1) \times \ldots \times \mathrm{Ens}(Z, X_n) \\ f & \mapsto & (\mathrm{pr}_1 \circ f, \ldots, \mathrm{pr}_n \circ f) \end{array}$$

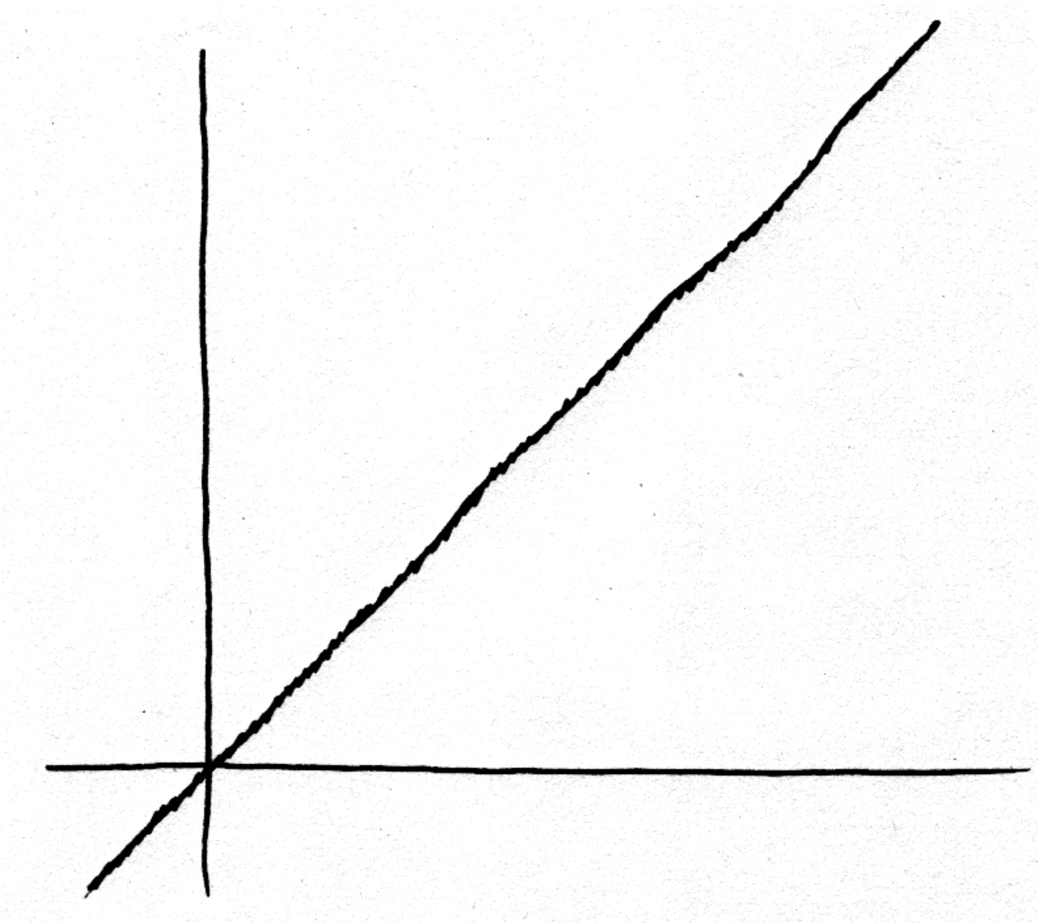
zwischen Abbildungen in das Produkt und Tupeln von Abbildungen in seine Faktoren. Die Umkehrung dieser **kanonischen Bijektion** notieren wir sozusagen gar nicht: Gegeben Abbildungen $f_i : Z \to X_i$ notieren wir die Abbildung $f : Z \to X_1 \times \ldots \times X_n$ von Z in das kartesische Produkt der X_i gegeben durch die Vorschrift $z \mapsto (f_1(z), \ldots, f_n(z))$ schlicht $f = (f_1, \ldots, f_n)$. In der exponentiellen Schreibweise geschrieben liest sich unsere Bijektion ganz suggestiv als eine Bijektion $(X_1 \times \ldots \times X_n)^Z \stackrel{\sim}{\to} X_1^Z \times \ldots \times X_n^Z$. Besonders wichtig ist die **diagonale Einbettung** oder **Diagonale**

$$\begin{array}{rccc} \Delta := \Delta_X := (\mathrm{id}, \mathrm{id}): & X & \to & X \times X \\ & x & \mapsto & (x, x) \end{array}$$

Ergänzung 1.3.4 (**Abbildungen zwischen kartesischen Produkten**). Ist ein weiteres Produkt von der Form $Y = Y_1 \times \ldots \times Y_n$ gegeben sowie Abbildungen $f_i : X_i \to Y_i$, so können wir auch die Abbildung

$$\begin{array}{ccc} X_1 \times \ldots \times X_n & \to & Y_1 \times \ldots \times Y_n \\ (x_1, \ldots, x_n) & \mapsto & (f_1(x_1), \ldots, f_n(x_n)) \end{array}$$

erklären. Wir notieren diese Abbildung $f_1 \times \cdots \times f_n$. Man beachte jedoch, daß keineswegs alle Abbildungen $X_1 \times \ldots \times X_n \to Y_1 \times \cdots \times Y_n$ von dieser Form sind. Man beachte allgemeiner, daß eine Abbildung $f : X_1 \times \ldots \times X_n \to Z$ von einem kartesischen Produkt in eine beliebige Menge Z sich keineswegs in ähnlicher Weise aus Abbildungen $X_i \to Z$ zusammensetzen läßt, wie das bei Abbildungen von einer beliebigen Menge in ein kartesisches Produkt gelingt.



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

Ergänzung 1.3.5 (**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 pr_X, pr_Y und 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 beiden fraglichen Tripelprodukte schlicht als gleich anzusehen.

1.3.6 (**Einelementige Mengen**). In derselben Weise sprechen auch mit einem bestimmten Artikel von „der" einelementigen Menge. Wir notieren sie manchmal 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 einpunktigen Menge notieren wir gerne $*$, also in Formeln

$$\mathrm{ens} = \{*\}$$

1.3.7 (**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 $X^0 = \mathrm{ens}$, 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 1.3.8 (**Der Vektorraum der n-Tupel**). Einige Beispiele für Vektorräume wurden bereits in [GR] 1.2 diskutiert. Besonders wichtig ist das Beispiel des Vektorraums

$$V = K^n$$

über einem vorgegebenen Körper K. Hier verwenden wir die Notation 1.3.7, 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

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

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

für $\lambda, v_1, \ldots, v_n, w_1, \ldots, w_n \in K$. 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 $v_1, v_2, \ldots, v_n$ und versehe sie nicht mit Pfeilen, da sie ja Elemente des Grundkörpers sind. Wenn irgendwo einmal $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ 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 auch aufgegeben haben werde, muß der Leser aus dem Kontext erschließen, was im Einzelfall jeweils gemeint ist.

Übungen

Übung 1.3.9. Gegeben ein Körper K und K-Vektorräume $V_1, \ldots, V_n$ können wir das kartesische Produkt $V_1 \times \ldots \times V_n$ zu einem K-Vektorraum machen, indem wir die Addition sowie die Multiplikation mit Skalaren komponentenweise definieren. In Formeln sieht das dann so aus wie 1.3.8, 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

$$V_1 \oplus \ldots \oplus V_n$$

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

1.4 Ordnungen auf Mengen*

1.4.1. Bei den Inhalten dieses Abschnitts hoffe ich, daß sie rechtzeitig in der Analysis besprochen werden, so daß dieser Abschnitt in der linearen Algebra übersprungen werden kann. Ich habe ihn aus [AN1] 1.3 kopiert.

Definition 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 auch eine **partielle Ordnung** oder **Halbordnung** oder auch einfach nur eine **Ordnung** genau dann, wenn für alle $x, y, z \in X$ gilt:

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

Auf Englisch benutzt man für eine partiell geordnete Menge alias „partially ordered set" auch oft die Abkürzung **poset**. Eine Ordnungsrelation heißt eine **Anordnung** oder eine **totale Ordnung** oder auch eine **lineare Ordnung** genau dann, wenn wir zusätzlich haben

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

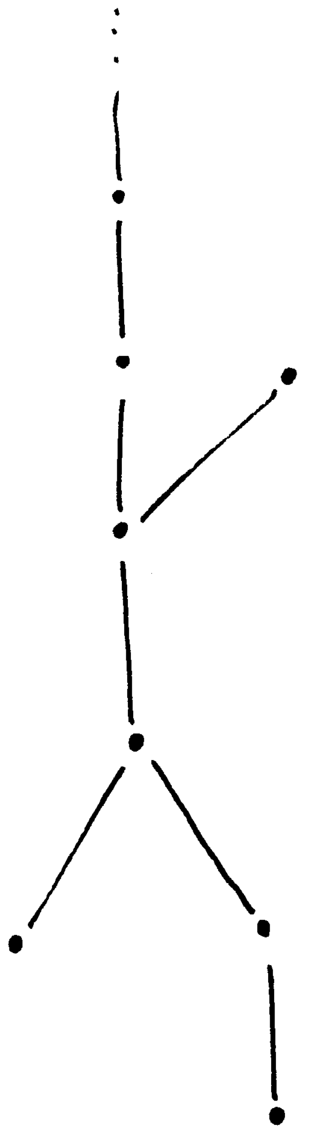
1.4.3 (**Diskussion der Terminologie**). Es gilt, im folgenden sorgfältig zu unterscheiden zwischen einer Ordnung und einer Anordnung.

Ergänzung 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 [GR] 2.3.2 spezielle Relationen. Noch allgemeiner betrachtet man auch für $n \geq 0$ und Mengen $X_1, \ldots, X_n$ Teilmengen $R \subset X_1 \times \ldots \times X_n$ und nennt sie n-stellige Relationen, aber das ist für uns vorerst noch nicht relevant.

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 $(x \leq y$ und $x \neq y)$ ab mit $x < y$ und ebenso $(x \geq y$ und $x \neq y)$ mit $x > y$. Auf jeder angeordneten Menge definieren wir Verknüpfungen $\max$ und $\min$ in offensichtlicher Verallgemeinerung von [GR] 3.1.3.

Definition 1.4.6. Sei $(Y, \leq)$ eine partiell geordnete Menge.

1. Ein Element $g \in Y$ heißt ein **größtes Element von** Y genau dann, wenn gilt $g \geq y \quad \forall y \in Y$. Ein Element $g \in Y$ heißt ein **maximales Element von** Y genau dann, wenn es kein $y \in Y$ gibt mit $y > g$.



Eine partiell geordnete 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 anderers genau dann, wenn es von diesem „durch einen aufsteigenden Weg erreicht werden kann“.

2. Ein Element $k \in Y$ heißt ein **kleinstes Element von** Y genau dann, wenn gilt $k \leq y \quad \forall y \in Y$. Ein Element $k \in Y$ heißt ein **minimales Element von** Y genau dann, wenn es kein $y \in Y$ gibt mit $y < k$.

1.4.7. Jede partiell geordnete 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 partiell geordnete Menge ein größtes beziehungsweise ein kleinstes Element, so ist dies auch ihr einziges maximales beziehungsweise minimales Element. Sonst kann es jedoch maximale beziehungsweise minimale Elemente in großer Zahl geben, zumindest dann, wenn unsere Ordnungsrelation keine Anordnung ist.

1.4.8. Gegeben geordnete Mengen $(X, \leq)$ und $(Y, \leq)$ versteht man unter einem **Homomorphismus von geordneten Mengen** oder gleichbedeutend einer **monoton wachsenden Abbildung** eine Abbildung $\phi : X \to Y$ mit $x \leq z \Rightarrow \phi(x) \leq \phi(z)$. Wie immer erklärt man einen Isomorphismus als einen Homomorphismus ϕ mit der Eigenschaft, daß es einen Homomorphismus ψ 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.

1.5 Untervektorräume

Definition 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 $\lambda \vec{u} \in U$.

1.5.2. Statt zu fordern, daß unsere Teilmenge den Nullvektor enthält, reicht es wegen 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 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 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.

1.5.4 (**Lösungsmengen als Untervektorräume**). Unter einem homogenen linearen Gleichungssystem über einem gegebenen Körper K versteht man, wie in 1.1.4 besprochen, ein System von Gleichungen der Gestalt

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

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

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 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.

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 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 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*

$$\langle T \rangle = \langle T \rangle_K \subset V$$

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

1.5.8. Ein Ausdruck der Gestalt $\alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r$ heißt eine **Linearkombination** der Vektoren $\vec{v}_1, \ldots, \vec{v}_r$. Hierbei sind nur endliche Summen erlaubt. Der kleinste T umfassende Untervektorraum $\langle T \rangle \subset V$ heißt der **von T erzeugte Untervektorraum** 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 1.5.9. Andere übliche Notationen für den von einer Teilmenge T eines Vektorraums erzeugten Untervektorraum sind $\operatorname{span}(T)$ und $\operatorname{lin}(T)$.

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. □

Definition 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 1.5.11 (**Erzeugnis in der schmutzigen Anschauung**). Ich erinnere an unsere Identifikation 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.

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

Definition 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

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

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.

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 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 1.5.15. Sei K ein Körper. Man zeige, daß der K-Vektorraum K genau zwei Untervektorräume besitzt.

Ergänzende Übung 1.5.16. Eine Teilmenge eines Vektorraums heißt ganz allgemein eine **Hyperebene** oder präziser **lineare Hyperebene** genau dann, 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 1.5.17. Gegeben ein Vektorraum über dem Körper mit zwei Elementen ist jede Untergruppe bereits ein Untervektorraum.

Übung 1.5.18. Sei V ein Vektorraum mit zwei Untervektorräumen U, W. Ist $U \cup W$ ein Untervektorraum, so gilt $U \subset W$ oder $W \subset U$.

1.6 Lineare Unabhängigkeit und Basen

Definition 1.6.1. Eine Teilmenge L eines Vektorraums V heißt **linear unabhängig**, wenn für paarweise verschiedene Vektoren $\vec{v}_1, \ldots, \vec{v}_r \in L$ und beliebige Skalare $\alpha_1, \ldots, \alpha_r \in K$ aus $\alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r = \vec{0}$ bereits folgt $\alpha_1 = \ldots = \alpha_r = 0$.

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 in der leeren Menge läßt er sich noch als die leere Linearkombination schreiben.

Definition 1.6.3. Eine Teilmenge L eines Vektorraums V heißt **linear abhängig**, wenn sie nicht linear unabhängig ist, wenn es also ausgeschrieben paarweise verschiedene Vektoren $\vec{v}_1, \ldots, \vec{v}_r \in L$ und Skalare $\alpha_1, \ldots, \alpha_r \in K$ gibt derart, daß nicht alle α_i Null sind und dennoch gilt $\alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r = \vec{0}$.

Beispiel 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 1.2.14.

Beispiel 1.6.5. Denken wir uns wie in 1.5.6 den schmutzigen Raum der Anschauung mit einem ausgezeichneten Urspung als reellen Vektorraum, so sind drei Vektoren linear unabhängig genau dann, wenn sie nicht „zusammen mit unserem Ursprung in einer anschaulichen Ebene liegen“.

Definition 1.6.6. Eine **Basis eines Vektorraums** ist ein linear unabhängiges Erzeugendensystem.

Beispiel 1.6.7. Denken wir uns wie in 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.

1.6.8. Gegeben Mengen A und I bezeichnet man eine Abbildung $I \to A$ 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 zugedacht hat. Im Fall $I = \emptyset$ spricht man von der **leeren Familie** von Elementen von A.

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 $i(1), \ldots, i(r) \in I$ und beliebige Skalare $\alpha_1, \ldots, \alpha_r \in K$ aus $\alpha_1\vec{v}_{i(1)} + \ldots + \alpha_r\vec{v}_{i(r)} = \vec{0}$ bereits folgt $\alpha_1 = \ldots = \alpha_r = 0$. 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**.

1.6.10. Besonders oft werden wir später Basen betrachten, die durch eine Menge der Gestalt $\{1, \ldots, n\}$ mit $n \in \mathbb{N}$ indiziert sind. Hier ist dann der wesentliche Unterschied zu einer Basis im Sinne von 1.6.6, daß wir zusätzlich festlegen, welcher Basisvektor der Erste, welcher der Zweite und so weiter sein soll. In der Terminologie aus 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 1.6.11. Seien K ein Körper und $n \in \mathbb{N}$. Wir betrachten in unserem Vektorraum K^n der n-Tupel die Vektoren

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

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

Satz 1.6.12 (über Linearkombinationen von Basiselementen). *Seien V ein Vektorraum V über einem Körper K und seien $\vec{v}_1, \ldots, \vec{v}_r \in V$ Vektoren. Genau dann ist die Familie der $\vec{v}_i$ eine Basis von V, wenn das Auswerten von Linearkombinationen eine Bijektion $\Phi : K^r \xrightarrow{\sim} V$, $(\alpha_1, \ldots, \alpha_r) \mapsto \alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r$ liefert.*

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

Beweis. Ausführlicher gilt für unsere Abbildung Φ sogar:

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

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

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

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. □

Satz 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.*

1.6.15. Die Begriffe minimal und maximal sind hier zu verstehen im Sinne von 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 **unverkürzbaren Erzeugendensystem** und einer **unverlängerbaren linear unabhängigen Teilmenge**. Ein nicht unverkürzbares Erzeugendensystem nennen wir folgerichtig ein **verkürzbares Erzeugendensystem** und eine nicht unverlängerbare linear unabhängige Teilmenge entsprechend eine **verlängerbare linear unabhängige Teilmenge**.

1.6.16 (**Existenz von Basen**). Unsere Minimalcharakterisierung 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 1.9.15.

Beweis. (1⇔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 $\lambda_1 \vec{v}_1 + \ldots + \lambda_r \vec{v}_r = \vec{0}$ mit $r \geq 1$, mit den $\vec{v}_i \in E$ paarweise verschieden und mit allen $\lambda_i \neq 0$, aus der wir folgern

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

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

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

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

(1⇔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 $\vec{v} \in V \backslash \langle L \rangle$ 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. □

Satz 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 $L \subset E$, 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.*

1.6.18. Die Begriffe minimal und maximal sind hier genau wie in 1.6.14 zu verstehen im Sinne von 1.4.6 in Bezug auf Inklusionen zwischen Teilmengen, nicht etwa in Bezug auf die Zahl der Elemente.

Beweis. (1) Wäre E keine Basis, so gäbe es zwischen seinen Vektoren eine nichttriviale Relation $\lambda_1 \vec{v}_1 + \ldots + \lambda_r \vec{v}_r = \vec{0}$ 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 $E \backslash L$ und kann als Linearkombination der anderen Elemente von E geschrieben werden. Dann aber ist $E \backslash \{\vec{v}_i\}$ 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. $\square$

Ergänzung 1.6.19. 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 $m_1, \ldots, m_r \in L$ und beliebige ganze Zahlen $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$ aus $\alpha_1 m_1 + \ldots + \alpha_r m_r = 0$ bereits folgt $\alpha_1 = \ldots = \alpha_r = 0$. 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 ist, und mit $\{2\}$ eine maximale linear unabhängige Teilmenge, die kein Erzeugendensystem ist.

Übungen

Übung 1.6.20. Eine zweielementige Teilmenge eines Vektorraums ist linear unabhängig genau dann, wenn keiner ihrer beiden Vektoren ein Vielfaches des anderen ist.

Übung 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.

1.7 Dimension eines Vektorraums

Satz 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*

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

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 1.8.3 in größerer Allgemeinheit diskutiert wird. Man benötigt dazu den „Austauschsatz von Steinitz" 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.

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

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

Alle Lösungen des „vertikal geschriebenen" homogenen linearen Gleichungssystems

$$\begin{array}{cccc} x_1 a_{11} & x_1 a_{21} & \ldots & x_1 a_{m1} \\ + & + & & + \\ \vdots & \vdots & \cdots & \vdots \\ + & + & & + \\ x_n a_{1n} & x_n a_{2n} & \cdots & x_n a_{mn} \\ = & = & & = \\ 0 & 0 & \cdots & 0 \end{array}$$

sind dann Tupel $(x_1, \ldots, x_n) \in K^n$ mit $x_1\vec{v}_1 + \ldots + x_n\vec{v}_n = 0$. Gilt $n > m$, so hat unser Gleichungssystem weniger Gleichungen hat als Unbekannte. Also liefert der Gauß-Algorithmus 1.1.8 dafür mindestens eine von Null verschiedene Lösung $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. Dann kann die Familie der Vektoren $\vec{v}_i$ aber nicht linear unabhängig sein. □

Korollar 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 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 1.9.15.

Beweis. Nach der Maximalcharakterisierung 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 1.7.1 kann man M auch tatsächlich zu einer maximalen linear unabhängigen Teilmenge von $M \cup E$ vergrößern. □

Korollar 1.7.5 (Kardinalitäten von Basen). *Jeder endlich erzeugte Vektorraum besitzt eine endliche Basis, und je zwei seiner Basen haben gleich viele Elemente.*

Vorschau 1.7.6. In [AL] 5.3.4 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 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 1.7.1 außerdem stets $|B| \leq |B'| \leq |B|$. □

Definition 1.7.7. Die Kardinalität einer und nach 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 [AL] 5.3.4 besprochen.

Ergänzung 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. Ich kann nur hoffen, daß der Leser aus dem Kontext erschließen kann, welcher Dimensionsbegriff im Einzelfall jeweils gemeint ist.

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 1.6.11 des Vektorraums K^n genau n Elemente und das zeigt

$$\dim_K K^n = n$$

Korollar 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 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 $|L| = |B|$ mithin L eine unverlängerbare linear unabhängige Teilmenge und damit nach der Maximalcharakterisierung 1.6.14 eine Basis sein. Im Fall $|B| = |E|$ muß E in derselben Weise ein unverkürzbares Erzeugendensystem und damit nach der Minimalcharakterisierung 1.6.14 eine Basis sein. □

Korollar 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 beliebigen Vektorraums, so behaupten wir mithin $\dim U \leq \dim V$ und behaupten zusätzlich, daß aus $\dim U = \dim V < \infty$ folgt $U = V$. Ist V nicht endlich erzeugt, so ist nichts zu zeigen. Ist V endlich erzeugt, so gibt es nach der Hauptabschätzung 1.7.10 in U eine unverlängerbare linear unabhängige Teilmenge, und jede derartige Teilmenge hat höchstens $\dim V$ Elemente. Jede derartige Teilmenge ist aber nach der Maximalcharakterisierung 1.6.14 notwendig eine Basis von U und das zeigt $\dim U \leq \dim V$. Gilt hier Gleichheit und ist V endlichdimensional, so ist wieder nach der Hauptabschätzung 1.7.10 jede Basis von U auch eine Basis von V und das zeigt $U = V$. □

Satz 1.7.12 (Dimensionssatz). *Gegeben ein Vektorraum V und darin Teilräume $U, W \subset V$ gilt*

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

1.7.13. Wir verwenden hier die 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 2.2.10 noch ein zweites Mal als Korollar der Dimensionsformel für lineare Abbildungen.

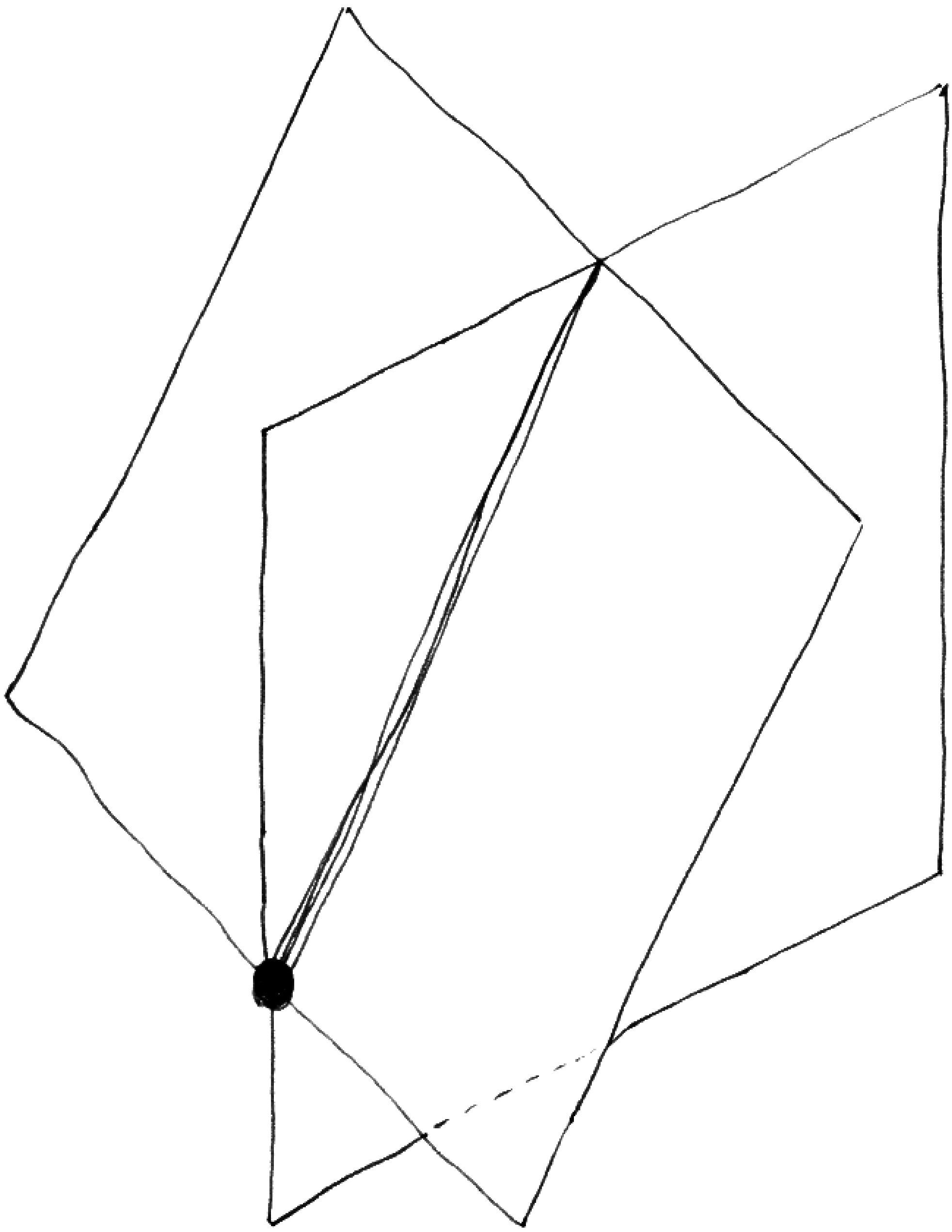


Illustration zum Dimensionssatz nach 1.7.14: Zwei verschiedene Ebenen im Raum, die beide einen ausgezeichneten festen Punkt enthalten, schneiden sich in einer Geraden.

Beispiel 1.7.14. Denken wir uns wie in 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 $s_1, \ldots, s_d$ von $U \cap W$ und ergänzen sie erst durch $u_1, \ldots, u_r \in U$ zu einer Basis von U und dann weiter durch $w_1, \ldots, w_t \in W$ zu einer Basis von $U + W$. Wir haben gewonnen, wenn wir zeigen können, daß bei derartigen Wahlen bereits $s_1, \ldots, s_d, w_1, \ldots, w_t$ eine Basis von W ist. Dazu reicht es zu zeigen, daß diese Menge W erzeugt. Sicher können wir jedes $w \in W$ schreiben als Linearkombination

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

Dabei gilt jedoch offensichtlich $\lambda_1 u_1 + \ldots + \lambda_r u_r \in W \cap U$. 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 $\lambda_1 = \ldots = \lambda_r = 0$, aber das ist für unseren Beweis schon gar nicht mehr von Belang. □

Übungen

Übung 1.7.15. Man zeige, daß jeder eindimensionale Vektorraum genau zwei Untervektorräume besitzt.

Übung 1.7.16. Gegeben K-Vektorräume V und W mit Basen $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$ 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 $V_1, \ldots, V_n$ gilt allgemeiner für die Dimension ihres kartesischen Produkts die Formel

$$\dim(V_1 \oplus \ldots \oplus V_n) = \dim(V_1) + \ldots + \dim(V_n)$$

Ergänzende Übung 1.7.17. Wir erinnern die Körper $\mathbb{R} \subset \mathbb{C}$ aus [GR] 3.4.15. 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 $\dim_{\mathbb{R}} V^{\mathbb{R}} = 2 \dim_{\mathbb{C}} V$.

1.8 Austauschsatz von Steinitz*

1.8.1. Einen anderen Zugang zur Hauptabschätzung der linearen Algebra 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 [AL] 5.3.5 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 meines Erachtens 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 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 $(E \backslash \varphi(L)) \cup L$ ein Erzeugendensystem von V ist.*

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 [AL] 5.3.5 skizziert.

Beweis. Der Austauschsatz folgt leicht induktiv aus dem Austauschlemma 1.8.4, das wir im Anschluß beweisen: Dies Lemma erlaubt uns nämlich, die Elemente von L der Reihe nach in E hineinzutauschen. □

Lemma 1.8.4 (Austauschlemma von Steinitz). *Seien V ein Vektorraum und darin $E \supset M$ ein Erzeugendensystem mit einer linear unabhängigen Teilmenge. Ist $\vec{w} \in V \backslash M$ ein Vektor außerhalb von M derart, daß auch $M \cup \{\vec{w}\}$ linear unabhängig ist, so gibt es $\vec{e} \in E \backslash M$ derart, daß auch $(E \backslash \vec{e}) \cup \{\vec{w}\}$ 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

$$\vec{w} = \lambda_1 \vec{e}_1 + \ldots + \lambda_r \vec{e}_r$$

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

$$\vec{e}_1 = \lambda_1^{-1}(\vec{w} - \lambda_2\vec{e}_2 - \ldots - \lambda_r\vec{e}_r)$$

und sehen so, daß auch $(E \backslash \vec{e}_1) \cup \{\vec{w}\}$ ein Erzeugendenystem ist. □

1.9 Auswahlaxiom und Zorn'sches Lemma*

Lemma 1.9.1 (Auswahlaxiom). *Für jede surjektive Abbildung $f : X \twoheadrightarrow Y$ von Mengen existiert ein* **Rechtsinverses** *alias ein* **Schnitt** *alias eine Abbildung $g : Y \to X$ mit $f \circ g = \mathrm{id}_Y$.*

1.9.2. 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 von 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 rührt die Bezeichnung unseres Lemmas als „Axiom". Wir werden das Auswahlaxiom hier für die Herleitung des „Zorn'schen Lemmas" 1.9.8 benötigen, von dem man sogar zeigen kann, daß es zum Auswahlaxiom äquivalent ist.

Lemma 1.9.3 (Auswahlaxiom, Variante). *Gegeben eine Menge X gibt es stets eine Abbildung $a : \mathcal{P}(X) \backslash \emptyset \to X$ mit $a(T) \in T \ \forall T \in \mathcal{P}(X)$.*

1.9.4. 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**.

1.9.5. 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 $X_0, X_1, \ldots$ nichtleerer Teilmengen einer Menge X eine Folge von Elementen $x_0, x_1, \ldots$ gibt mit $x_i \in X_i \ \forall i$, mag man das „Folgenauswahlaxiom" nennen. Es wird häufig ohne viel Nachfragen schon zu Beginn der ersten Grundvorlesung zur Analysis verwendet, zum Beispiel beim Nachweis, daß jede folgenstetige Funktion das ε-δ-Kriterium erfüllt.

1.9.6. 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 $Y \to \mathcal{P}(X)$. Sie induziert eine Surjektion $Y \twoheadrightarrow \mathcal{P}(X)\backslash\emptyset$, und verknüpfen wir einen Schnitt dieser Surjektion mit der Projektion auf die erste Koordinate $(x, T) \mapsto x$, so erhalten wir eine Auswahlfunktion $\mathcal{P}(X)\backslash\emptyset \to X$.

1.9.7. Wir benutzen im folgenden die Begrifflichkeit aus 1.4 und erinnern an einige Begriffe im Zusammenhang mit partiell geordneten Mengen, deren genaue Bedeutung für das Folgende wesentlich ist. Wir nennen ein Element x einer partiell geordneten Menge X **maximal** genau dann, wenn es keine Elemente oberhalb von x gibt. Wir nennen x das **größte Element** von X genau dann, wenn alle anderen Elemente von X unterhalb von x liegen. Es kann also in einer partiell geordneten 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.

Lemma 1.9.8 (Zorn'sches Lemma). *Sei $(X, \leq)$ eine partiell geordnete Menge. Besitzt jede total geordnete Teilmenge $Y \subset X$ eine obere Schranke in X, so gibt es in unserer partiell geordneten Menge X mindestens ein maximales Element.*

1.9.9. Unter einer total geordneten Teilmenge einer partiell geordneten Menge verstehen wir eine Teilmenge, in der je zwei Elemente vergleichbar sind. Wir bezeichnen derartige Teilmengen im folgenden meist als **Ketten**. Eine partiell geordnete Menge, in der jede Kette eine obere Schranke besitzt, nennt man **induktiv geordnet**. Eine induktiv geordnete Menge ist insbesondere nie leer, denn die leere Menge ist ja auch eine Kette und besitzt folglich eine obere Schranke. Es reicht nicht aus, im Zorn'schen Lemma nur die Existenz einer oberen Schranke für jede monoton wachsende Folge zu fordern, vergleiche 1.9.13.

1.9.10. Wir werden das Zorn'sche Lemma im Anschluß an die Formulierung des „Fixpunktsatzes von Bourbaki" 1.9.18 mithilfe des Auswahlaxioms 1.9.3 auf diesen Fixpunktsatz zurückführen, für den wir dann einen vom Auswahlaxiom unabhängigen Beweis geben. Zunächst will ich jedoch zur besseren Motivation noch einige Folgerungen aus dem Zorn'schen Lemma besprechen.

1.9.11. 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 1.9.12. *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.*

1.9.13. Hier verwenden wir die Konvention 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 partiell geordnete 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. □

1.9.14. Ich schicke dem Beweis des Zorn'schen Lemmas eine typische Anwendung voraus. Der Beweis des Zorn'schen Lemmas selber ist für diese Vorlesung nicht mehr relevant.

Satz 1.9.15 (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 $M \subset B \subset E$.*

1.9.16. 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 $\mathrm{Ens}(\mathbb{N}, K)$ 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 $M \subset A \subset E$, geordnet 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 vorhergehenen Korollar 1.9.12 gibt es damit ein maximales Element von $\mathcal{X}$ alias eine linear 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 1.6.17 eine Basis von V sein. □

1.9.17. Eine partiell geordnete Menge, in der jede Kette T sogar eine *kleinste* obere Schranke besitzt, nennt man **streng induktiv geordnet**. Für jede Teilmenge T einer partiell geordneten Menge S kann es natürlich nicht mehr als eine kleinste obere Schranke geben, und falls sie existiert, heißt wie in der Analysis das **Supremum** von T in S und wird bezeichnet mit $\sup T$. Wir führen das Zorn'sche Lemma mithilfe des Auswahlaxioms zurück auf den folgenden Satz, den wir dann im Anschluß beweisen.

Satz 1.9.18 (Fixpunktsatz von Bourbaki). *Ist $(S, \leq)$ eine streng induktiv geordnete Menge, so besitzt jede Abbildung $f : S \to S$ mit der Eigenschaft $f(s) \geq s \; \forall s \in S$ mindestens einen Fixpunkt.*

1.9.19. Wir werden diesen Satz zeigen, ohne das Auswahlaxiom zu verwenden. Genauer werden wir sogar einen vollständig kanonischen Fixpunkt konstruieren als das „größte Element des kleinsten Turms“. Zuvor folgern wir jedoch noch aus dem Fixpunktsatz das Zorn'sche Lemma, und bei diesem Schritt brauchen wir das Auswahlaxiom 1.9.3.

Herleitung des Zorn'schen Lemmas 1.9.8 aus dem Fixpunktsatz 1.9.18. Sei X unsere partiell geordnete Menge. Wir betrachten das System $\mathcal{S} \subset \mathcal{P}(X)$ aller Ketten von X. Sicher ist $\mathcal{S}$ partiell geordnet vermittels der Inklusion. Unser $\mathcal{S}$ ist auf diese Weise sogar streng induktiv geordnet, das Supremum über ein total geordnetes System $\mathcal{T} \subset \mathcal{S}$ von Ketten ist einfach ihre Vereinigung $\sup \mathcal{T} = \bigcup_{K\in\mathcal{T}} K$. Wir definieren nun eine Abbildung $f : \mathcal{S} \to \mathcal{S}$ durch die Vorschrift

$$f(K) := \begin{cases} K \cup \{x\} & \text{falls } x \notin K \text{ existiert derart, daß } K \cup \{x\} \text{ eine Kette ist;} \\ K & \text{sonst.} \end{cases}$$

Hier verwenden wir das Auswahlaxiom, um für alle fraglichen K jeweils unter allen möglichen x Eines auszuwählen. Jetzt hat die Abbildung f nach dem Satz von Bourbaki 1.9.18 einen Fixpunkt, es gibt also eine maximale Kette $K_{\max} \subset X$. Eine obere Schranke einer solchen maximalen Kette $K_{\max}$ ist dann notwendig ein maximales Element von X. □

1.9.20. Die obere Schranke von $K_{\max}$ vom Schluß des vorhergehenden Beweises ist sogar eindeutig bestimmt und kann beschrieben werden als das größte Element von $K_{\max}$. Das interessiert aber schon gar nicht mehr.

Beweis des Fixpunktsatzes von Bourbaki 1.9.18. Die Menge S besitzt notwendig ein kleinstes Element $k \in S$, nämlich das Supremum der leeren Menge, die ja stets eine Kette ist. Die folgende Definition vereinbaren wir nur behelfsmäßig für die Zwecke dieses Beweises, danach darf sie wieder vergessen werden.

Definition 1.9.21. Sei S eine streng induktiv geordnete Menge und $f : S \to S$ eine Abbildung mit $f(s) \geq s$ für alle $s \in S$. Eine Teilmenge $T \subset S$ heißt ein **Turm** oder präziser ein **Turm in Bezug auf** f, wenn gilt

1. Das kleinste Element k von S gehört zu T;
2. Aus $t \in T$ folgt $f(t) \in T$;
3. Ist $K \subset T$ eine Kette, so gehört auch $\sup K$ zu T.

1.9.22. Es reicht, einen Turm T zu finden, der auch eine Kette ist, denn dann ist $\sup T$ das größte Element von T und damit ein Fixpunkt von f. Der Schnitt über alle Türme in S ist offensichtlich der bezüglich Inklusion kleinste Turm von S, wir nennen ihn R. Wir behaupten nun, daß dieser kleinste Turm R eine Kette ist.

Ergänzung 1.9.23. 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, dann auch $f(k), f^2(k), f^3(k)\dots$ Wird diese Folge stabil, etwa bei $f^n(k) = f^{n+1}(k)$, so ist diese endliche Menge der kleinste Turm. Wird sie nicht stabil, 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 stabil, 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 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 zum Ziel führen. Stattdessen vereinbaren wir eine weitere Sprechweise.

Definition 1.9.24. Ein Element unseres kleinsten Turms $c \in R$ heißt **eng**, wenn für alle $a \in R$ gilt $(a < c) \Rightarrow (f(a) \leq c)$.

Ergänzung 1.9.25. Anschaulich mag man sich unsere partiell geordnete 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. Ein enges Element 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.

Lemma 1.9.26. *Gegeben ein enges Element c unseres kleinsten Turms R gilt für jedes weitere Element unseres kleinsten Turms $x \in R$ mindestens eine der beiden Ungleichungen $x \leq c$ oder $f(c) \leq x$.*

Beweis. Es reicht zu zeigen, daß die Menge $R_c = \{x \in R \mid \text{Es gilt entweder } x \leq c \text{ oder } f(c) \leq x\}$ ein Turm ist. Sicher gilt $k \in R_c$. Ist $K \subset R_c$ eine Kette, so gehört offensichtlich auch $\sup K$ zu R_c. Wir müssen also nur noch zeigen, daß R_c stabil ist unter f, und das folgt mühelos aus unserer Definition eines engen Elements c. □

Lemma 1.9.27. *Jedes Element unseres kleinsten Turms R ist eng.*

Beweis. Es reicht zu zeigen, daß die Menge E der engen Elemente von R ein Turm ist. Sicher gilt $k \in E$. Um zu zeigen, daß E stabil ist unter f, bemerken wir, daß für c eng aus $a < f(c)$ schon folgt $a \leq c$ nach Lemma 1.9.26. Es bleibt zu zeigen, daß für jede Kette $K \subset E$ auch ihr Supremum $b = \sup K$ zu E gehört. Sei also $a \in R$ und $a < b$. Es gilt zu zeigen $f(a) \leq b$. Wenn wir haben $a < c$ für ein $c \in K$, so folgt wegen c eng sofort $f(a) \leq c \leq b$. Wenn nicht, so gilt notwendig $a \geq c$ für alle $c \in K$ und folglich $a \geq b$ im Widerspruch zur Annahme. □

Jetzt führen wir den Beweis des Fixpunktsatzes von Bourbaki zu Ende. In der Tat zeigt ja Lemma 1.9.27 zusammen mit seinem Vorgänger Lemma 1.9.26 sofort, daß der kleinste Turm R total geordnet ist. Also ist R sowohl ein Turm als auch eine Kette und $\sup R$ ist ein Fixpunkt von f. □

Übungen

Übung 1.9.28. Man zeige, daß es auf jeder Menge eine Anordnung gibt.

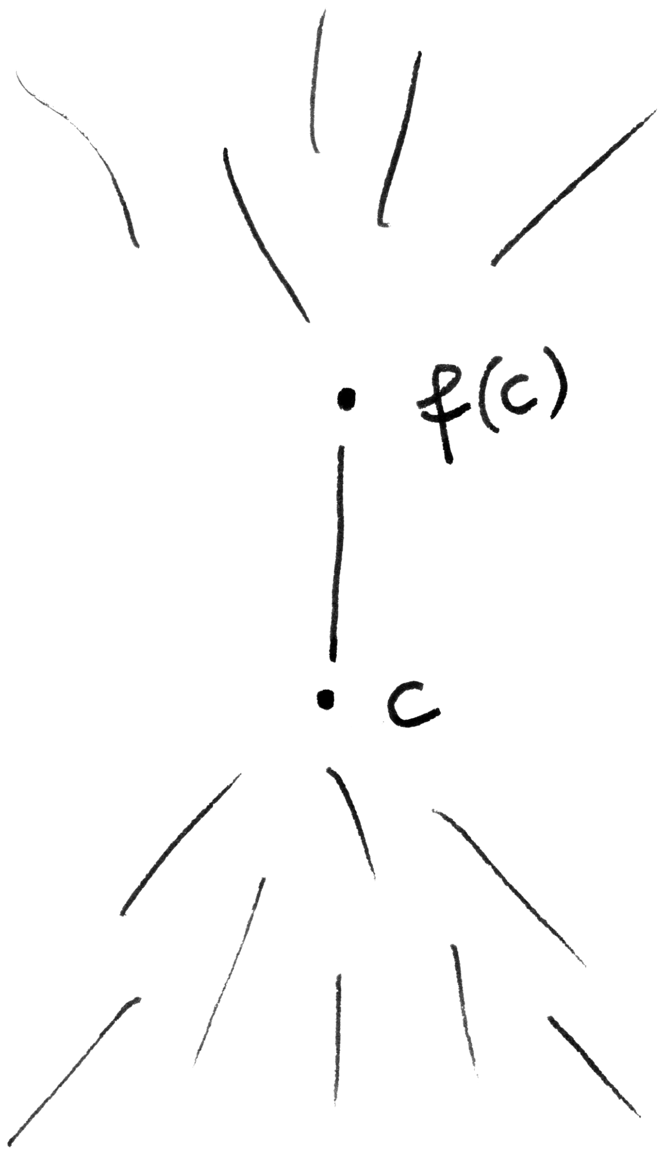


Illustration zu 1.9.26 im Fall, daß unser enges Element des kleinsten Turms $c \in R$ kein Fixpunkt von f ist. Die partielle Ordnung wird hier vage durch Striche angedeutet, die von kleineren zu größeren Elementen aufsteigen.

2 Lineare Abbildungen

2.1 Homomorphismen und Isomorphismen

Definition 2.1.1. Seien V, W Vektorräume über einem Körper K. Eine Abbildung $f : V \to W$ heißt **linear** oder genauer K**-linear**, wenn für alle $\vec{v}, \vec{w} \in V$ und $\lambda \in K$ gilt

$$\begin{array}{rcl} f(\vec{v} + \vec{w}) & = & f(\vec{v}) + f(\vec{w}) \\ f(\lambda \vec{v}) & = & \lambda f(\vec{v}) \end{array}$$

Eine lineare Abbildung heißt auch ein **Homomorphismus von** K**-Vektorräumen**.

Definition 2.1.2. Eine lineare Abbildung ϕ heißt ein **Isomorphismus von Vektorräumen**, wenn es eine lineare Abbildung ψ 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.

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 $\mathrm{Aut}_K(V)$.

2.1.4. Jede lineare Abbildung bildet den Nullvektor auf den Nullvektor ab, denn für $f : V \to W$ 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 $f : V \to W$ linear gilt

$$f(\lambda_1 \vec{v}_1 + \ldots + \lambda_n \vec{v}_n) = \lambda_1 f(\vec{v}_1) + \ldots + \lambda_n f(\vec{v}_n)$$

für beliebige $\lambda_i \in K$ und $\vec{v}_i \in V$.

Didaktische Anmerkung 2.1.5. Ich denke, an dieser Stelle mag auch der Abschnitt [GR] 3.3 über Homomorphismen von Magmas und Monoiden und Gruppen besprochen werden, ergänzt um Homomorphismen von Körpern. Besser wäre es aber, diesen Abschnittschon früher zu besprechen. Dann kann man hier an [GR] 3.3.6 erinnern, wonach sogar überhaupt jeder Gruppenhomomorphismus das neutrale Element auf das neutrale Element werfen muß.

2.1.6 (**Herkunft der Terminologie**). Die Herkunft eines Teils dieser Terminologie haben wir bereits in [GR] 3.3.8 diskutiert. „Linear“ heißen unsere Abbildungen vermutlich, weil im Fall $\mathbb{R}$-linearer Abbildungen $f : \mathbb{R} \to \mathbb{R}$ ihre Graphen Geraden alias gerade Linien sind. Allerdings sind auch allgemeiner die Graphen der Funktionen $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$ 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 „$\varepsilon\nu\delta o\nu$“ für deutsch „drinnen“, und das Wort „Automorphismus“ von „$\alpha\upsilon\tau o\varsigma$“ für deutsch „selbst“.

Beispiele 2.1.7. Die Projektionen auf die Faktoren $\mathrm{pr}_i : K^n \to K$ sind linear. Die Abbildung $K^2 \to K$ 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 $K \to V$ gegeben durch $\lambda \mapsto \lambda\vec{v}$ linear. Jede lineare Abbildung von K in einen K-Vektorraum ist von dieser Gestalt. Das Quadrieren $K \to K$ ist nicht linear, es sei denn, K ist ein Körper mit zwei Elementen, so daß es mit der Identität zusammenfällt.

Beispiele 2.1.8. Gegeben Vektorräume V, W sind die Projektionsabbildungen $\mathrm{pr}_V : (V \oplus W) \to V$ und $\mathrm{pr}_W : (V \oplus W) \to W$ linear. Dasselbe gilt allgemeiner für die Projektionen $\mathrm{pr}_i : V_1 \oplus \ldots \oplus V_n \to V_i$. Ebenso sind die **kanonischen Injektionen** $\mathrm{in}_V : V \to (V \oplus W)$, $v \mapsto (v, 0)$ und $\mathrm{in}_W : W \to (V \oplus W)$, $w \mapsto (0, w)$ linear und dasselbe gilt allgemeiner für die analog definierten Injektionen $\mathrm{in}_i : V_i \to V_1 \oplus \ldots \oplus V_n$.

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 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 $B = (\vec{v}_1, \ldots, \vec{v}_n)$ aus n Vektoren, so liefert die Vorschrift $(\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1\vec{v}_1 + \ldots + \lambda_n\vec{v}_n$ etwa nach 1.6.12 einen Vektorraumisomorphismus $K^n \xrightarrow{\sim} V$. □

2.1.11 (**Stufenzahl nach Durchführen des Gauß-Algorithmus**). Nun können wir auch unsere Ausgangsfrage 1.1.14 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 $x_{s(1)}, x_{s(2)}, \ldots, x_{s(r)}$ aus einem m-Tupel $(x_1, \ldots, x_m) \in L$. 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 2.1.12. Ein Punkt, der unter einer Abbildung auf sich selbst abgebildet wird, heißt ein **Fixpunkt** besagter Abbildung. Gegeben eine Abbildung $f : X \to X$ 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 $f \in \operatorname{End} V$ bildet die Menge der von f festgehaltenen Vektoren alias aller **Fixvektoren von** f stets einen Untervektorraum $V^f \subset V$.

Übung 2.1.13. Jede Verknüpfung von Vektorraumhomomorphismen ist wieder ein Vektorraumhomomorphismus. Sind also in Formeln $g : U \to V$ und $f : V \to W$ Vektorraumhomomorphismen, so ist auch $f \circ g : U \to W$ ein Vektorraumhomomorphismus.

Übung 2.1.14. Gegeben ein surjektiver Vektorraumhomomorphismus $g : U \twoheadrightarrow V$ und eine Abbildung $f : V \to W$ in einen weiteren Vektorraum ist f genau dann linear, wenn die Verknüpfung $f \circ g : U \to W$ linear ist. Gegeben ein injektiver Vektorraumhomomorphismus $f : V \hookrightarrow W$ und eine Abbildung $g : U \twoheadrightarrow V$ von einen weiteren Vektorraum nach V ist g genau dann linear, wenn die Verknüpfung $f \circ g : U \to W$ linear ist. Hinweis: [GR] 3.3.35.

Übung 2.1.15. Ist $f : V \to W$ ein bijektiver Vektorraumisomorphismus, so ist auch die Umkehrabbildung $f^{-1} : W \to V$ ein Vektorraumhomomorphismus und f ist folglich ein Isomorphismus.

Übung 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

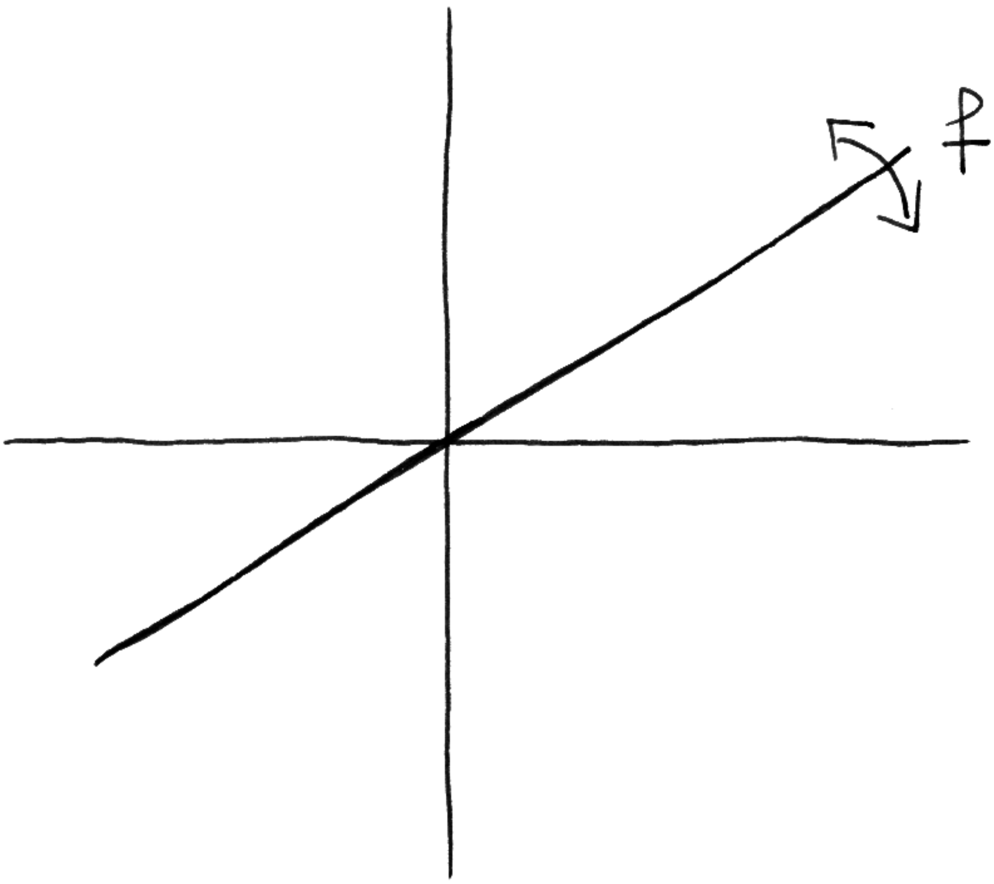


Illustration zu Übung 2.1.12, nach der die Fixpunktmenge jedes Endomorphismus eines Vektorraums ein Untervektorraum ist. Zum Beispiel ist die Spiegelung an einer Ursprungsgerade eine lineare Abbildung und ihre Fixpunktmenge ist in der Tat ein Untervektorraum, nämlich besagte Ursprungsgerade.

des $\mathbb{R}^3$ werden unter der Spiegelung $(x, y, z) \mapsto (x, y, -z)$ in sich selber überführt?

Ergänzende Übung 2.1.17. Eine Gruppe, in der jedes Element sein eigenes Inverses ist, kann nach 1.2.17 auf genau eine Weise mit der Struktur eines Vektorraums über dem Körper mit zwei Elementen versehen werden. Ein Beispiel ist unsere Gruppe aus [GR] 3.2.18 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 2.1.18. Eine Abbildung $f : V \to W$ von Vektorräumen ist genau dann linear, wenn ihr Graph $\Gamma(f) \subset V \times W$ ein Untervektorraum des Produkts ist.

2.2 Dimensionsformel für lineare Abbildungen

Lemma 2.2.1. *Das Bild eines Untervektorraums unter einer linearen Abbildung ist ein Untervektorraum. Das Urbild eines Untervektorraums unter einer linearen Abbildung ist ein Untervektorraum.*

Beweis. 1. Sei $f : V \to W$ unsere lineare Abbildung. Sei $U \subset V$ ein Untervektorraum. Wir müssen zeigen, daß auch $f(U) \subset V$ ein Untervektorraum ist. Da f ein Homomorphismus der zugrundeliegenden additiven Gruppen ist, ist $f(U)$ schon mal eine additive Untergruppe von W nach [GR] 3.3.22. 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 $f : V \to W$ 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 [GR] 3.3.22. 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. $\square$

2.2.2. Das **Bild** einer linearen Abbildung $f : V \to W$ alias die Teilmenge $(\operatorname{im} f) := f(V) \subset W$ ist nach 2.2.1 ein Untervektorraum von W.

2.2.3. Das Urbild des Nullvektors unter einer linearen Abbildung $f : V \to W$ 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 2.2.1 ein Untervektorraum von V. Wir hatten ihn in [GR] 3.3.20 sogar bereits für beliebige Gruppenhomomorphismen eingeführt.

Lemma 2.2.4 (Verschwindender Kern bedeutet Injektivität). *Eine lineare Abbildung $f : V \to W$ ist injektiv genau dann, wenn ihr Kern Null ist.*

Beweis. Das sollten sie in Übung [GR] 3.3.20 bereits für beliebige Gruppenhomomorphismen zeigen. Hier geben wir das Argument nocheinmal 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. □

Satz 2.2.5. *Für jede lineare Abbildung $f : V \to W$ 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 dem Korollar 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 2.2.6. Alternativ kann man auch mit Übung 2.2.13 argumentieren. □

Lemma 2.2.6. *Sei $f : V \to W$ eine lineare Abbildung. Ist A eine Basis ihres Kerns, B eine Basis ihres Bildes und $g : B \to V$ eine Wahl von Urbildern unserer Basis des Bildes, so ist $g(B) \cup A$ eine Basis von V.*

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 $f(\vec{v}) = \lambda_1 \vec{w}_1 + \ldots + \lambda_r \vec{w}_r$ mit $\vec{w}_i \in B$. Offensichtlich liegt dann $\vec{v} - \lambda_1 g(\vec{w}_1) - \ldots - \lambda_r g(\vec{w}_r)$ 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

$$\lambda_1 g(\vec{w}_1) + \ldots + \lambda_r g(\vec{w}_r) + \mu_1 \vec{v}_1 + \ldots + \mu_s \vec{v}_s = 0$$

mit den $\vec{v}_i \in A$ und $\vec{w}_j \in B$ paarweise verschieden. Wenden wir f an, so folgt $\lambda_1 \vec{w}_1 + \ldots + \lambda_r \vec{w}_r = 0$ und damit $\lambda_1 = \ldots = \lambda_r = 0$ wegen der linearen Unabhängigkeit der $\vec{w}_i$. Setzen wir diese Erkenntnis in die ursprüngliche Gleichung ein, so folgt weiter $\mu_1 = \ldots = \mu_s = 0$ wegen der linearen Unabhängigkeit der Vektoren $\vec{v}_j$. □

Korollar 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 $f : V \to W$ unsere lineare Abbildung. Im ersten Fall folgt erst $\ker f = 0$ und dann $\dim(\operatorname{im} f) = \dim V = \dim W$ aus der Dimensionsformel und so $\operatorname{im} f = W$ mit 1.7.11. Im zweiten Fall folgt erst $\ker f = 0$ aus der Dimensionsformel und dann die Injektivität aus 2.2.4. □

2.2.9. Gegeben ein Vektorraum V und Teilräume $U, W \subset V$ setzen wir

$$U + W := \{v \in V \mid \text{Es gibt } u \in U \text{ und } w \in W \text{ mit } v = u + w\}$$

unter Verwendung unserer allgemeinen Notationskonvention aus [GR] 3.1.3. Offensichtlich ist $U + W$ wieder ein Teilraum von V.

Korollar 2.2.10 (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 1.7.12 sozusagen zu Fuß bewiesen. Mit unserer Dimensionsformel 2.2.5 können wir nun noch einen alternativen Beweis geben. Betrachtet man nämlich die lineare Abbildung

$$f : U \oplus W \to V$$

gegeben durch $f(u, w) = u + w$, so gilt $(\operatorname{im} f) = U + W$ und die Abbildung $d \mapsto (d, -d)$ definiert einen Isomorphismus $(U \cap W) \xrightarrow{\sim} \ker f$. Die Formel 1.7.16 für die Dimension der direkten Summe in Verbindung mit der Dimensionsformel liefert so

$$\dim U + \dim W = \dim(U \oplus W) = \dim(U \cap W) + \dim(U + W) \qquad \square$$

Definition 2.2.11. Zwei Untervektorräume U, W eines Vektorraums V heißen **komplementär**, wenn die Addition eine Bijektion

$$U \times W \xrightarrow{\sim} V$$

liefert. Nach 2.3.12 ist diese Abbildung dann unter Verwendung der in 1.3.9 eingeführten Notation 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**.

2.2.12 (**Vektorraumkomplement und Komplementmenge**). Man unterscheide 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 [LA2] 8.6.13 als Ausprägungen von „Koprodukten“ erweisen, und das ist zumindest eine gewisse Rechtfertigung für die vermutlich etwas verwirrende Terminologie.

Übungen

Übung 2.2.13. Sei $f : V \to W$ 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 2.2.14. Man zeige: Zwei Untervektorräume U, W eines Vektorraums V sind komplementär genau dann, wenn gilt $V = U + W$ und $U \cap W = 0$.

Übung 2.2.15. 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: 1.7.16.

Übung 2.2.16. Der Kern einer von Null verschiedenen linearen Abbildung in den Grundkörper ist stets eine Hyperebene im Sinne von 1.5.16.

Ergänzende Übung 2.2.17. Sei $\varphi : V \to V$ ein Endomorphismus eines endlichdimensionalen Vektorraums. Man zeige, daß $\ker(\varphi^2) = \ker \varphi$ gleichbedeutend ist zu $+ : \ker \varphi \oplus \operatorname{im} \varphi \stackrel{\sim}{\to} V$.

Ergänzende Übung 2.2.18. 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 Teilräumen. Gegeben ein Vektorraum V liefert genauer die Abbildung $f \mapsto (\operatorname{im} f, \ker f)$ eine Bijektion

$$\{f \in \operatorname{End} V \mid f^2 = f\} \stackrel{\sim}{\to} \left\{ (I, J) \in \mathcal{P}(V)^2 \,\middle|\, \begin{array}{c} I, J \subset V \text{ sind Teilräume} \\ \text{und als solche komplementär} \end{array} \right\}$$

Für die Umkehrabbildung unserer Bijektion sagt man, sie ordne unserem Paar (I, J) komplementärer Teilräume die **Projektion von** V **auf** I **längs** J zu.

Übung 2.2.19. 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.

2.3 Räume von linearen Abbildungen

2.3.1. Seien V, W Vektorräume über einem Körper K. Die Menge aller Homomorphismen von V nach W notieren wir

$$\mathrm{Hom}_K(V, W) = \mathrm{Hom}(V, W) \subset \mathrm{Ens}(V, W)$$

Lemma 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*

$$\mathrm{Hom}_K(V, W) \xrightarrow{\sim} \mathrm{Ens}(B, W)$$

Jede lineare Abbildung ist also in Worten festgelegt und festlegbar durch ihre Werte auf einer Basis.

Beweis im Fall einer endlichen Basis. Seien $f, g : V \to W$ linear. Gilt $f(\vec{v}) = g(\vec{v})$ für alle $\vec{v} \in B$, so folgt $f(\lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r) = g(\lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r)$ für alle $\lambda_1, \ldots, \lambda_r \in K$ und $\vec{v}_1, \ldots, \vec{v}_r \in B$ 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 $g : B \to W$ gegeben, so können wir sie zu einer linearen Abbildung $\tilde{g} : V \to W$ ausdehnen wie folgt: Jeder Vektor $\vec{v} \in V$ läßt sich ja nach 1.6.12 eindeutig als Linearkombination der Basisvektoren schreiben, etwa $\vec{v} = \lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r$ mit paarweise verschiedenen $\vec{v}_i \in B$. Wir können nun schlicht $\tilde{g}$ definieren durch die Vorschrift

$$\tilde{g}(\vec{v}) := \lambda_1 g(\vec{v}_1) + \ldots + \lambda_r g(\vec{v}_r)$$

Man sieht leicht, daß dann $\tilde{g}$ linear ist und aud der Basis zu g einschränkt. $\square$

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".

2.3.4 (**Freie Vektorräume und ihre universelle Eigenschaft**). Seien X eine Menge und K ein Körper. Die Menge $\mathrm{Ens}(X, K)$ aller Abbildungen $f : X \to K$ 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

$$K\langle X\rangle \subset \mathrm{Ens}(X, K)$$

Dieser Vektorraum $K\langle X\rangle$ heißt der **freie Vektorraum über der Menge** X. Gegeben $x \in X$ bezeichne $\delta_x : X \to K$ die Abbildung mit $\delta_x(x) = 1$ und $\delta_x(y) = 0$ für $y \neq x$. So ist die sogenannte **kanonische Einbettung** $\mathrm{can} : X \to K\langle X\rangle$ gegeben durch $x \mapsto \delta_x$ offensichlich eine Basis im Sinne einer Familie von $K\langle X\rangle$. Weiter liefert für jeden K-Vektorraum V das Vorschalten der kanonischen Einbettung can eine Bijektion

$$(\circ\, \mathrm{can}) : \mathrm{Hom}_K(K\langle X\rangle, V) \tilde{\to} \mathrm{Ens}(X, V)$$

In der Tat kann man in diesem Fall eine Umkehrabbildung leicht angeben durch die Vorschrift $\phi \mapsto \Phi$ mit

$$\Phi : a \mapsto \sum_{\{x \mid a(x) \neq 0\}} a(x)\phi(x)$$

Wir sagen dann auch, die lineare Abbildung $\Phi : K\langle X\rangle \to V$ entstehe aus der Abbildung $\phi : X \to V$ durch **lineare Fortsetzung**.

2.3.5 (**Notationen bei freien Vektorräumen**). Ein Element $a \in K\langle X\rangle$ des freien Vektorraums über einer Menge X fassen wir als „formale Linearkombination von Elementen von X" auf und notieren es statt $\sum_{\{x \mid a(x) \neq 0\}} a(x)\delta_x$ 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 Φ einer Abbildung $\phi : X \to V$ beschrieben durch die hoffentlich suggestivere Formel

$$\Phi : \sum_{x \in X} a_x x \quad \mapsto \quad \sum_{x \in X} a_x \phi(x)$$

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 $X = \{x_1, \ldots, x_n\}$ schreiben wir statt dem etwas umständlichen $K\langle\{x_1, \ldots, x_n\}\rangle$ auch abkürzend $K\langle x_1, \ldots, x_n\rangle$. 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 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 $\phi : I \to V$, $i \mapsto \vec{v}_i$ nach 2.3.4 entstehende lineare Abbildung ist ein Isomorphismus $\Phi : K\langle I\rangle \xrightarrow{\sim} V$.*

Beweis. Ausführlicher gilt sogar:

$$\begin{array}{lcll} (\vec{v}_i)_{i\in I} \text{ ist Erzeugendensystem} & \Leftrightarrow & \Phi \text{ ist eine Surjektion} & K\langle I\rangle \twoheadrightarrow V \\ (\vec{v}_i)_{i\in I} \text{ ist linear unabhängig} & \Leftrightarrow & \Phi \text{ ist eine Injektion} & K\langle I\rangle \hookrightarrow V \\ (\vec{v}_i)_{i\in I} \text{ ist eine Basis} & \Leftrightarrow & \Phi \text{ ist eine Bijektion} & K\langle I\rangle \xrightarrow{\sim} V \end{array}$$

Der Beweis ist mutatis mutandis derselbe wie im in 1.6.12 behandelten Fall einer endlichen Familie, mit einigen Vereinfachungen, die die bereits entwickelte Theorie ermöglicht. Das Bild von Φ ist offensichtlich der von unserer Familie erzeugte Untervektorraum. Andererseits ist Φ nach 2.2.4 genau dann injektiv, wenn gilt $\ker(\Phi) = 0$. Diese Bedingung bedeutet aber nach unseren Definitionen genau die lineare Unabhängigkeit unserer Familie. □

Beweis von Lemma 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 2.3.6 einen Isomorphismus $\Phi : K\langle B\rangle \xrightarrow{\sim} V$. Wir erhalten so für jeden weiteren K-Vektorraum Bijektionen

$$\mathrm{Hom}_K(V, W) \xrightarrow{\sim} \mathrm{Hom}_K(K\langle B\rangle, W) \xrightarrow{\sim} \mathrm{Ens}(B, W)$$

durch Vorschalten von Φ und can. Deren Verknüpfung alias das Vorschalten der Einbettung $B \hookrightarrow V$ ist also auch eine Bijektion, und das war genau die Behauptung. □

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 2.3.8. Seien U, V, W Vektorräume über einem Körper K. Eine Abbildung $F : U \times V \to W$ 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

$$\begin{array}{rcl} F(u + a, v) & = & F(u, v) + F(a, v) \\ F(\lambda u, v) & = & \lambda F(u, v) \end{array}$$

$$\begin{array}{rcl} F(u, v + b) & = & F(u, v) + F(u, b) \\ F(u, \mu v) & = & \mu F(u, v) \end{array}$$

für alle $\lambda, \mu \in K$ und $u, a \in U$ und $v, b \in V$. Die Menge aller solchen bilinearen Abbildungen notieren wir

$$\mathrm{Hom}_K^{(2)}(U \times V, W) \subset \mathrm{Ens}(U \times V, W)$$

Diese Notation befriedigt mich unter formalen Aspekten nicht vollständig, da das Symbol $\times$ auf der linken Seite nicht als kartesisches Produkt, sondern vielmehr als ein Trenner aufzufassen ist. Ich habe sie dennoch gewählt in der Hoffnung, daß sie sich leichter merken und lesen läßt als eine unter formalen Aspekten bessere Notation wie zum Beispiel $\mathrm{Hom}_K^{(2)}(U, V; W)$. Eine bilineare Abbildung $V \times V \to K$ in den Grundkörper heißt eine **Bilinearform auf** V.

Übungen

Übung 2.3.9. Seien U, V, W Vektorräume und $A \subset U$ sowie $B \subset V$ jeweils Basen. So liefert die Einschränkung eine Bijektion

$$\mathrm{Hom}_K^{(2)}(U \times V, W) \xrightarrow{\sim} \mathrm{Ens}(A \times B, W)$$

In Worten ist also eine bilineare Abbildung festgelegt und festlegbar durch ihre Werte auf Paaren von Basisvektoren. Hinweis: Man orientiere sich am Beweis von 2.3.2.

Ergänzende Übung 2.3.10. Sei $(X, \leq)$ eine partiell geordnete Menge und K ein Körper. Seien für alle $x \in X$ Abbildungen $f_x : X \to K$ 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 $\mathrm{Ens}(X, K)$ aller Abbildungen von X nach K.

Weiterführende Übung 2.3.11. Man zeige, daß für eine unendliche Menge X weder der Vektorraum $\mathrm{Ens}(X, K)$ noch der freie Vektorraum $K\langle X \rangle$ über X endlich erzeugt sind.

Übung 2.3.12 (**Homomorphismen aus direkten Summen**). Man zeige: Gegeben Vektorräume $V_1, \ldots, V_n, W$ und lineare Abbildungen $f_i : V_i \to W$ erhalten wir auch eine lineare Abbildung $f : V_1 \oplus \ldots \oplus V_n \to W$ durch die Vorschrift $f(v_1, \ldots, v_n) = f_1(v_1) + \ldots + f_n(v_n)$. Auf diese Weise ergibt sich sogar einen Isomorphismus

$$\mathrm{Hom}(V_1, W) \oplus \ldots \oplus \mathrm{Hom}(V_n, W) \xrightarrow{\sim} \mathrm{Hom}(V_1 \oplus \ldots \oplus V_n, W)$$

Die Umkehrabbildung können wir in der Form $f \mapsto (f \circ \mathrm{in}_i)_i$ schreiben.

Übung 2.3.13 (**Homomorphismen in Produkte**). Man zeige: Gegeben Vektorräume $V, W_1, \ldots, W_n$ und lineare Abbildungen $g_i : V \to W_i$ erhalten wir auch eine lineare Abbildung $g : V \to W_1 \oplus \ldots \oplus W_n$ durch die Vorschrift $g(v) = (g_1(v), \ldots, g_n(v))$. Auf diese Weise ergibt sich sogar einen Isomorphismus

$$\operatorname{Hom}(V, W_1) \oplus \ldots \oplus \operatorname{Hom}(V, W_n) \xrightarrow{\sim} \operatorname{Hom}(V, W_1 \oplus \ldots \oplus W_n)$$

Die Umkehrabbildung können wir in der Form $f \mapsto (\operatorname{pr}_i \circ f)_i$ schreiben.

Übung 2.3.14 (**Der Hom-Raum und seine Dimension**). Seien V, W Vektorräume über einem Körper K. Man zeige, daß $\operatorname{Hom}_K(V, W)$ ein Untervektorraum der Menge $\operatorname{Ens}(V, W)$ aller Abbildungen von V nach W mit ihrer Vektorraumstruktur aus 2.3.4 ist. Man zeige für die Dimension von $\operatorname{Hom}_K(V, W)$ die Formel

$$\dim \operatorname{Hom}_K(V, W) = (\dim V)(\dim W)$$

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: 2.3.2.

Übung 2.3.15. Man zeige, daß für je drei Vektorräume U, V, W über einem Körper die Verknüpfung von linearen Abbildungen $\operatorname{Hom}(U, V) \times \operatorname{Hom}(V, W) \to \operatorname{Hom}(U, W)$ bilinear ist. Hier sind unsere Homomorphismenräume zu verstehen mit ihrer in 2.3.14 erklärten Vektorraumstruktur.

Übung 2.3.16 (**Exponentialgesetz für lineare Abbildungen**). Gegeben Vektorräume U, V, W über einem Körper induziert die Identifikation $\operatorname{Ens}(U \times V, W) \xrightarrow{\sim} \operatorname{Ens}(U, \operatorname{Ens}(V, W))$ aus dem Exponentialgesetz [GR] 2.3.34 einen Isomorphismus

$$\operatorname{Hom}^{(2)}(U \times V, W) \xrightarrow{\sim} \operatorname{Hom}(U, \operatorname{Hom}(V, W))$$

zwischen dem Raum der bilinearen Abbildungen $U \times V \to W$ und dem Raum der linearen Abbildungen $U \to \operatorname{Hom}(V, W)$.

2.4 Lineare Abbildungen $K^n \to K^m$ und Matrizen

Satz 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 $K^n \to K^m$ und der Menge der K-wertigen Matrizen mit m Zeilen und n Spalten*

$$\begin{array}{rccc} \mathrm{M}: & \operatorname{Hom}_K(K^n, K^m) & \xrightarrow{\sim} & \operatorname{Mat}(m \times n; K) \\ & f & \mapsto & [f] \end{array}$$

durch die Vorschrift, die jeder linearen Abbildung f ihre **darstellende Matrix** $\mathrm{M}(f) := [f]$ *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*

$$[f] := (f(\mathrm{e}_1) | f(\mathrm{e}_2) | \ldots | f(\mathrm{e}_n))$$

Beweis. Das folgt unmittelbar aus unserer Erkenntnis 2.3.2, daß eine lineare Abbildung festgelegt wird durch ihre Werte auf den Vektoren einer Basis, die ihrerseits beliebig vorgegeben werden können. □

Beispiel 2.4.2. Die Matrix der Identität auf K^n ist die **Einheitsmatrix**

$$\mathrm{I} = \mathrm{I}_n := [\mathrm{id}] = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

mit Einträgen $\mathrm{I}_{i,j} = \delta_{i,j}$ 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“ $f : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_m)$ gerade

$$[f] = \begin{pmatrix} 1 & & 0 & & 0 \ldots 0 \\ & \ddots & & & \\ & & \ddots & & \\ & 0 & & 1 & 0 \ldots 0 \end{pmatrix}$$

Die Matrix des „Vertauschens der Koordinaten“ $g : K^2 \to K^2$, $(x, y) \mapsto (y, x)$ schließlich ist

$$[g] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Definition 2.4.3. Gegeben natürliche Zahlen $m, n, l \in \mathbb{N}$ und ein Körper K und Matrizen $A \in \mathrm{Mat}(n \times m; K), B \in \mathrm{Mat}(m \times l; K)$ definieren wir ihr **Produkt** $A \circ B = AB \in \mathrm{Mat}(n \times l; K)$ 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

$$\begin{pmatrix} 1 & 2 \\ 2 & 0 \\ 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 0 & 2 & 2 & 0 \\ 1 & 7 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 16 & 14 & 12 \\ 0 & 4 & 4 & 0 \\ 3 & 29 & 26 & 18 \end{pmatrix}$$

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 vermittels der Rechnung $4 = 2 \cdot 2 + 0 \cdot 6$.

die Produktmatrix auch ausführlicher $AB = A \circ B$. Die **Matrixmultiplikation** liefert eine Abbildung

$$\begin{array}{ccc} \mathrm{Mat}(n \times m; K) \times \mathrm{Mat}(m \times l; K) & \to & \mathrm{Mat}(n \times l; K) \\ (A \quad , \quad B) & \mapsto & AB \end{array}$$

2.4.4. In der Terminologie aus 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.

Satz 2.4.5 (Verknüpfen von Abbildungen und Matrixprodukt). *Gegeben lineare Abbildungen $g : K^l \to K^m$ und $f : K^m \to K^n$ 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

$$\begin{array}{rcccl} g(\vec{w}_k) & = & (b_{*k}) & = & \vec{v}_1 b_{1k} + \ldots + \vec{v}_m b_{mk} \\ f(\vec{v}_j) & = & (a_{*j}) & = & \vec{u}_1 a_{1j} + \ldots + \vec{u}_n a_{nj} \end{array}$$

und folgern

$$\begin{array}{rcl} (f \circ g)(\vec{w}_k) & = & f(\vec{v}_1 b_{1k} + \ldots + \vec{v}_m b_{mk}) \\ & = & f(\vec{v}_1) b_{1k} + \ldots + f(\vec{v}_m) b_{mk} \\ & = & \sum_{j=1}^m f(\vec{v}_j) b_{jk} \\ & = & \sum_{j=1}^m \left(\sum_{i=1}^n \vec{u}_i a_{ij}\right) b_{jk} \\ & = & \sum_{i=1}^n \vec{u}_i \left(\sum_{j=1}^m a_{ij} b_{jk}\right) \end{array}$$

Andererseits sind ja die Einträge (c_{ik}) der Matrix $[f \circ g]$ gerade definiert durch die Identität $(f \circ g)(\vec{w}_k) = \vec{u}_1 c_{1k} + \ldots + \vec{u}_n c_{nk}$, und durch einen Koeffizientenvergleich folgt für die Einträge c_{ik} von $[f \circ g]$ wie gewünscht $c_{ik} = \sum_{j=1}^m a_{ij} b_{jk}$. □

Proposition 2.4.6 (Rechnen mit Matrizen). *Für die Matrixmultiplikation gelten die folgenden Rechenregeln:*

$$\begin{array}{rcl} (A+A')B & = & AB + A'B \\ A(B+B') & = & AB + AB' \\ \mathrm{I}B & = & B \\ A\mathrm{I} & = & A \\ (AB)C & = & A(BC) \end{array}$$

für beliebige $k, l, m, n \in \mathbb{N}$ *und* $A, A' \in \mathrm{Mat}(n \times m; K)$*,* $B, B' \in \mathrm{Mat}(m \times l; K)$*,* $C \in \mathrm{Mat}(l \times k; K)$ *und* $\mathrm{I} = \mathrm{I}_m$ *die* $(m \times m)$*-Einheitsmatrix.*

Erster Beweis. Stures Rechnen, ich führe nur zwei Teile beispielhaft aus. Wir haben $(A\mathrm{I})_{ij} = \sum_k A_{ik}\mathrm{I}_{kj} = \sum_k A_{ik}\delta_{kj} = A_{ij}$ und das zeigt $A\mathrm{I} = A$. Für die nächste Rechnung verwende ich einmal andere Notationen und nehme $\kappa, \lambda, \mu, \nu$ als Laufindizes. Dann haben wir

$$\begin{array}{rcl} ((AB)C)_{\nu\kappa} & = & \sum_{\lambda=1}^{l} (AB)_{\nu\lambda} C_{\lambda\kappa} \\ & = & \sum_{\lambda=1}^{l} \left(\sum_{\mu=1}^{m} A_{\nu\mu} B_{\mu\lambda} \right) C_{\lambda\kappa} \\ & = & \sum_{\lambda,\mu=1}^{l,m} A_{\nu\mu} B_{\mu\lambda} C_{\lambda\kappa} \\ (A(BC))_{\nu\kappa} & = & \sum_{\mu=1}^{m} A_{\nu\mu} (BC)_{\mu\kappa} \\ & = & \sum_{\mu=1}^{m} A_{\nu\mu} \left(\sum_{\lambda=1}^{l} B_{\mu\lambda} C_{\lambda\kappa} \right) \\ & = & \sum_{\mu,\lambda=1}^{m,l} A_{\nu\mu} B_{\mu\lambda} C_{\lambda\kappa} \end{array}$$

und das zeigt $(AB)C = A(BC)$. □

Zweiter Beweis. Wir können unsere Rechenregeln für Matrizen auch mit 2.4.1 und 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 2.4.1, finden mit 2.4.5 sofort

$$\begin{array}{rcl} (AB)C & = & ([a] \circ [b]) \circ [c] = [a \circ b] \circ [c] = [(a \circ b) \circ c] \\ A(BC) & = & [a] \circ ([b] \circ [c]) = [a] \circ [b \circ c] = [a \circ (b \circ c)] \end{array}$$

und die Behauptung ergibt sich aus der für die Verknüpfung von Abbildungen offensichtlichen Identität $(a \circ b) \circ c = a \circ (b \circ c)$. □

2.4.7 (**Lineare Abbildungen** $K^m \to K^n$ **als Matrixmultiplikationen**). Mit dem Formalismus der Matrixmultiplikation können wir auch die Umkehrung unserer

Bijektion $\operatorname{Hom}_K(K^m, K^n) \xrightarrow{\sim} \operatorname{Mat}(n \times m; K)$, $f \mapsto [f]$ aus 2.4.1, bei der jeder linearen Abbildung ihre darstellende Matrix zugeordnet wird, elegant beschreiben. Dazu müssen wir nur die Elemente von K^m bzw. K^n als Spaltenvektoren auffassen und einer Matrix $A \in \operatorname{Mat}(n \times m; K)$ die durch Matrixmultiplikation gegebene Abbildung $(A\circ) : \operatorname{Mat}(m \times 1; K) \to \operatorname{Mat}(n \times 1; K)$ alias

$$(A\circ) : K^m \to K^n$$

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 $K^m \to K^n$ und Matrizen eh so in Fleisch und Blut übergehen, daß man unterschiedslos A schreiben und damit beides gleichzeitig meinen kann.

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 $\operatorname{Hom}(K, V) \xrightarrow{\sim} V$. Deren Umkehrabbildung kann explizit beschrieben werden als die Abbildung

$$V \xrightarrow{\sim} \operatorname{Hom}(K, V)$$

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 $[\cdot\vec{v}]$ von $(\cdot\vec{v}) : K \to K^m$ 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 $f : V \to W$ linear, so gilt auch ganz allgemein sicher $f \circ (\cdot\vec{v}) = (\cdot f(\vec{v}))$, denn diese beiden linearen Abbildungen $K \to W$ 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 2.4.7 nocheinmal die Identität

$$[f] \circ [\vec{v}] = [f(\vec{v})]$$

von Spaltenvektoren, diesmal aber als Konsequenz unseres Satzes 2.4.5 über die Matrix einer Verknüpfung.

Ergänzung 2.4.9. Gegeben eine Matrix $A \in \operatorname{Mat}(n \times m; K)$ definiert man die **transponierte Matrix** $A^\top \in \operatorname{Mat}(m \times n; K)$ 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 ${}^tA$.

$$\begin{pmatrix} 1 & 4 & 7 & 3 \\ 2 & 2 & 0 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 2 \\ 4 & 2 \\ 7 & 0 \\ 3 & 0 \end{pmatrix}$$

Die transponierte Matrix erhält man durch eine „Spiegelung an der Hauptdiagonalen“.

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 davormultiplizieren 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 einen durchlaufenden Text ungeschickt, Spaltenvektoren auch als solche zu schreiben. Da fügen 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 $(x_1, \ldots, x_n)^\top$. Oft schreibe ich aber auch einfach $(x_1, \ldots, x_n)$ und der Leser muß aus dem Kontext erschließen, was genau gemeint ist, wenn es denn darauf überhaupt ankommen sollte.

2.4.11. Vielleicht ist eine alternative Notation besser, in der $(x_1, \ldots, x_n)$ im Zweifelsfall einen Spaltenvektor meint und $(x_1|\ldots|x_n)$ stets einen Zeilenvektor? Im vorliegenden Text wir diese Konvention jedenfalls nicht durchgehalten.

Ergänzung 2.4.12 (**Homomorphismen zwischen direkten Summen**). Gegeben Vektorräume $V_1, \ldots, V_m$ und $W_1, \ldots, W_n$ über einem Körper k liefern die Identifikationen 2.3.12 und 2.3.13 zusammen eine natürliche Identifikation

$$\begin{array}{ccc} \mathrm{Hom}(V_1 \oplus \ldots \oplus V_m, W_1 \oplus \ldots \oplus W_n) & \stackrel{\sim}{\to} & \prod_{i,j} \mathrm{Hom}(V_j, W_i) \\ f & \mapsto & (\mathrm{pr}_i \circ f \circ \mathrm{in}_j)_{ij} \end{array}$$

Wir werden die Elemente einer endlichen direkten Summe oft als Spaltenvetoren 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 $f_{11}, f_{21}, \ldots, f_{n1}$ als erster Spalte, $f_{12}, f_{22}, \ldots, f_{n2}$ 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 $g : U_1 \oplus \ldots \oplus U_l \to V_1 \oplus \ldots \oplus V_m$ die Matrix der $g_{jk} = \mathrm{pr}_j \circ g \circ \mathrm{in}_k : U_k \to V_j$, so entspricht der Verknüpfung $f \circ g$ die Matrix mit Einträgen

$$\left(\sum_j f_{ij} \circ g_{jk} \right) : U_k \to W_i$$

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 2.4.13. Man zeige, daß die Abbildung M aus 2.4.1 sogar ein Vektorraumisomorphismus ist für die Vektorraumstruktur 2.3.14 auf dem Raum der Homomorphismen und die Vektorraumstruktur 1.2.18 auf der Menge der Matrizen.

Übung 2.4.14. Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Spiegelung $(x, y) \mapsto (x, -y)$. Man zeige, daß die linearen Abbildungen $g : \mathbb{R}^2 \to \mathbb{R}^2$ mit der Eigenschaft $fg = gf$ einen Untervektorraum des Homomorphismenraums $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2)$ bilden und gebe eine Basis dieses Untervektorraums des Homomorphismenraums an.

Übung 2.4.15. Man zeige für das Produkt transponierter Matrizen die Formel

$$(AB)^\top = B^\top A^\top$$

2.5 Einige Eigenschaften von Matrizen

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

$$\mathrm{Mat}(n; K) := \mathrm{Mat}(n \times n; K)$$

notieren. Die invertierbaren Elemente dieses Monoids heißen die **invertierbaren** oder gleichbedeutend auch die **regulären** $(n \times n)$**-Matrizen**. In Formeln heißt eine quadratische Matrix $A \in \mathrm{Mat}(n; K)$ also invertierbar genau dann, wenn es eine Matrix $B \in \mathrm{Mat}(n; K)$ gibt mit $AB = \mathrm{I} = BA$. 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

$$\mathrm{GL}(n; K) := \mathrm{Mat}(n; K)^\times$$

in Anlehnung an die englische Bezeichnung **general linear group**.

Lemma 2.5.2 (Invertierbarkeit a priori nicht quadratischer Matrizen). *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n; K)$ eine nicht notwendig quadratische Matrix.*

1. *Gilt $n \geq m$ und gibt es $B \in \mathrm{Mat}(n \times m; K)$ mit $BA = \mathrm{I}$, so gilt $n = m$ und A ist invertierbar;*

2. *Gilt $n \leq m$ und gibt es $B \in \mathrm{Mat}(n \times m; K)$ mit $AB = \mathrm{I}$, so gilt $n = m$ und A ist invertierbar.*

Beweis. Gibt es B mit $BA = \mathrm{I}$, 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 $AB = \mathrm{I}$, 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. □

2.5.3 (**Lineare Gleichungssysteme und Matrixalgebra**). Ein lineares Gleichungssystem

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

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 $(A\circ) : K^m \to K^n$. Die Lösung des homogenisierten Systems ist genau der Kern dieser linearen Abbildung, und die Erkenntnis 1.1.12, 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 3.2.14 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 λ-fachen der j-ten Zeile zur i-ten Zeile entsteht, in Matrixschreibweise dargestellt werden als

$$(\mathrm{I} + \lambda E_{ij})Ax = (\mathrm{I} + \lambda E_{ij})b$$

Wegen $(\mathrm{I} - \lambda E_{ij})(\mathrm{I} + \lambda E_{ij}) = \mathrm{I}$ 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 $P_{ij}P_{ij} = \mathrm{I}$ hat es offensichtlich dieselbe Lösungsmenge wie das ursprüngliche System.

2.5.4. Man lasse sich durch die terminologische Inkonhärenz nicht verwirren: E_{ij} und P_{ij} sind an dieser Stelle Matrizen, nicht wie vorher Einträge von Matrizen.

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 2.5.6 (**Diskussion der Terminologie**). Es herrscht in der Literatur keine Einigkeit in der Frage, was genau unter einer Elementarmatrix zu verstehen sein soll. Manche Quellen bezeichnen zusätzlich zu unseren Elementarmatrizen auch noch die Permutationsmatrizen P_{ij} als Elementarmatrizen, andere Quellen insbesondere in der „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 [LA2] 1.3.4 gehören.

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 auch eine Matrix in **Smith-Normalform**.

Satz 2.5.8 (**Transformation auf Smith-Normalform**). *Für jede Matrix $A \in \mathrm{Mat}(n \times m; K)$ mit Einträgen in einem Körper 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 2.5.9. In 3.5.11 geben wir einen noch alternativen eigenständigen Beweis. □

Proposition 2.5.9 (**Transformation auf Smith-Normalform, Variante**). *Für jede Matrix $A \in \mathrm{Mat}(n \times m; K)$ mit Einträgen in einem Körper K gibt es invertierbare Elementarmatrizen $S_1, \ldots, S_n, T_1, \ldots, T_m$ derart, daß $S_n \ldots S_1 A$ Zeilenstufenform hat und $S_n \ldots S_1 A T_1 \ldots T_m$ 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

$$P_{ij} = \mathrm{diag}(1, \ldots, 1, -1, 1, \ldots, 1)(\mathrm{I} + E_{ij})(\mathrm{I} - E_{ji})(\mathrm{I} + E_{ij})$$

Hier soll die (-1) an der j-ten Stelle stehen und $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ 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. □

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Eine Matrix in Smith-Normalform

Korollar 2.5.10. *Jede quadratische Matrix mit Einträgen in einem Körper läßt sich als ein Produkt von Elementarmatrizen darstellen.*

Ergänzung 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 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 $\operatorname{diag}(1, \dots, 1, 0, \dots, 0)$ 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

$$A = S_1^{-1} \dots S_n^{-1} D_1 \dots D_r T_m^{-1} \dots T_1^{-1} \qquad \square$$

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 $(A|\mathrm{I})$ 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

$$(S_t \dots S_2 S_1 A | S_t \dots S_2 S_1 \mathrm{I})$$

und wenn dann gilt $S_t \dots S_2 S_1 A = \mathrm{I}$, so folgt $S_t \dots S_2 S_1 \mathrm{I} = S_t \dots S_2 S_1 = A^{-1}$. Dasselbe Verfahren funktioniert auch, wenn wir statt mit Zeilen- mit Spaltenumformungen arbeiten. Es ist nur nicht erlaubt, diese zu mischen, denn aus $S_t \dots S_1 A T_1 \dots T_r = \mathrm{I}$ folgt keineswegs $S_t \dots S_1 T_1 \dots T_r = A^{-1}$.

Definition 2.5.13. Gegeben eine Matrix $A \in \operatorname{Mat}(n \times m; K)$ 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 2.5.14. *Für jede Matrix stimmen Zeilenrang und Spaltenrang überein, in Formeln gilt also* $\operatorname{rk}(A) = \operatorname{rk}(A^\top)$.

2.5.15. Diese gemeinsame Zahl heißt dann der **Rang** oder auf englisch **rank** unserer Matrix und wird $\operatorname{rk} A$ 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 $A \in \operatorname{Mat}(n \times m; K)$ kann interpretiert werden als die Dimension des Bildes von

$$(A\circ) : K^m \to K^n$$

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 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. □

Definition 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 von Null verschiedene Abbildungen endlichen Ranges.

Übungen

Übung 2.5.17. Gegeben lineare Abbildungen $f : U \to V$ und $g : V \to W$ 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 2.5.18. Man gebe eine ganzzahlige (3×3)-Matrix vom Rang Zwei ohne Eintrag Null an, bei der je zwei Spalten linear unabhängig sind.

Übung 2.5.19. Eine quadratische Block-obere Dreiecksmatrix ist invertierbar genau dann, wenn alle Blöcke auf der Diagonalen invertierbar sind. Hinweis: 2.4.12.

Ergänzende Übung 2.5.20. Die Automorphismengruppe eines zweidimensionalen Vektorraums über einem zweielementigen Körper ist isomorph zur Gruppe der Permutationen von drei Elementen, in Formeln $\operatorname{GL}(2; \mathbb{F}_2) \cong \mathcal{S}_3$.

Ergänzende Übung 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 $\begin{pmatrix} \mathrm{I} & 0 \\ 0 & W_{22}^{-1} \end{pmatrix}$ und dann mit $\begin{pmatrix} \mathrm{I} & 0 \\ -W_{21} & \mathrm{I} \end{pmatrix}$.

2.6 Ergänzungen zu linearen Abbildungen*

Satz 2.6.1. *In einem Vektorraum besitzt jeder Untervektorraum ein Komplement.*

Beweis. Seien $V \supset U$ unser Raum mit seinem Untervektorraum. Ist unser Raum V endlich erzeugt, so ist auch U endlich erzeugt nach 1.7.11. Wir finden nach 1.6.16 eine Basis L von U und können sie nach 1.7.3 zu einer Basis B von V ergänzen. Das Erzeugnis des Komplements $B \backslash L$ 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 1.9.15 ersetzen. □

Proposition 2.6.2. *1. Für jede injektive lineare Abbildung $f : V \hookrightarrow W$ existiert ein* **Linksinverses**, *als da heißt, eine lineare Abbildung $g : W \to V$ mit $g \circ f = \mathrm{id}_V$;*

2. Für jede surjektive lineare Abbildung $f : V \twoheadrightarrow W$ existiert ein **Rechtsinverses**, *als da heißt, eine lineare Abbildung $g : W \to V$ mit $f \circ g = \mathrm{id}_W$.*

Beweis. Der Beweis beider Aussagen benötigt im unendlichdimensionalen Fall das Zorn'sche Lemma. Um Teil 1 zu zeigen, wählen wir mit 2.6.1 ein Komplement $U \subset W$ von $f(V)$ und definieren $g : W \to V$ durch die Vorschrift $g(u + f(v)) = v \; \forall u \in U, v \in V$: Das ist erlaubt, da nach unsern 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. □

Übungen

Übung 2.6.3. Jede lineare Abbildung von einem Untervektorraum U eines Vektorraums V in einen weiteren Vektorraum $f : U \to W$ läßt sich zu einer linearen Abbildung $\tilde{f} : V \to W$ auf den ganzen Raum V fortsetzen. Hinweis: 2.6.2.

3 Räume mit und ohne Koordinaten

3.1 Affine Räume und affine Abbildungen

Definition 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 $\vec{E} \subset \mathrm{Ens}^{\times} E$ der Gruppe der Permutationen von E sowie einer Abbildung $a : K \times \vec{E} \to \vec{E}$ 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 $a : K \times \vec{E} \to \vec{E}$ 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 die **Translationen** oder **Richtungsvektoren** unseres affinen Raums. Den Vektorraum $\vec{E}$ selbst nennen wir den **Richtungsraum** unseres affinen Raums. Das Resultat der Operation von $\vec{v} \in \vec{E}$ auf $p \in E$ notieren wir $\vec{v} + p := \vec{v}(p)$ und manchmal auch $p + \vec{v}$.

3.1.2 (**Diskussion der Notation und Terminologie**). Die Notation des Richtungsraums mit einem Pfeil steht in Konflikt zu unserer Notation aus [AN2] 6.3.7, nach der mit Pfeilen versehene Mannigfaltigkeiten orientierte Mannigfaltigkeiten andeuten sollen. Was im Einzelfall jeweils gemeint ist, muß der Leser aus dem Kontext erschließen. Die leere Menge kann in unseren Konventionen nie ein affiner Raum sein. Es gibt hier jedoch auch andere Konventionen. Unser Richtungsraum wird in manchen Quellen auch der **Differenzraum** genannt. Vielfach findet man 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 vorgegebenen Vektorraum vermeidet und den Raum unserer Anschauung meines Erachtens besser modelliert.

3.1.3. Unter der **Dimension** eines affinen Raums verstehen wir die Dimension seines Richtungsraums. Einen affinen Raum über dem Körper $\mathbb{R}$ der reellen Zahlen nenne ich auch einen **reellen affinen Raum** oder kurz **reellen Raum**.

3.1.4. 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**.

3.1.5 (**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 $p, q \in E$ definieren wir

$$p - q$$

als denjenigen Richtungsvektor $\vec{u} \in \vec{E}$ mit $p = \vec{u} + q$. In Schulbüchern verwendet man oft Großbuchstaben $A, B, C, \ldots$ für die Punkte eines affinen Raums und verwendet die Notation $\overrightarrow{AB}$ für den Richtungsvektor, der A nach B schiebt und den wir hier $B - A$ notieren. Vielleicht ist es eine gute Idee, zu Anfang statt $p - q$ lieber $p \leftarrow q$ zu schreiben.

3.1.6 (**Vektorräume als affine Räume**). Jeder Vektorraum V kann als ein 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 $V \hookrightarrow \mathrm{Ens}^{\times}(V)$, $v \mapsto (v+)$ 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

$$\mathrm{trans} : V \xrightarrow{\sim} \vec{V}$$

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 3.1.7 (**Der schmutzige Raum unserer Anschauung als affiner Raum**). Es scheint mir besonders sinnfällig, den „Raum unserer Anschauung" mathematisch als einen dreidimensionalen reellen affinen Raum

$$\mathbb{E}$$

zu modellieren. Dieses Modell werden wir in [LA2] 2.3.16 noch um die Vorgabe einer ausgezeichneten „Bewegungsgruppe" und einer ausgezeichneten „Orientierung" erweitern und so den „Anschauungsraum" formal als ein Gebilde der Mengenlehre definieren. Die endgültige Definition muß aber noch auf die Einführung der fehlenden Begriffe warten. Der Buchstabe $\mathbb{E}$ soll an das französische Wort „éspace" für „Raum" erinnern. Unser „Raum unserer Anschauung" heißt manchmal auch der „Raum der klassischen Mechanik". Manche Punkte dieses Raums können wir uns direkt als Kirchturmspitzen, Zimmerecken und dergleichen denken, die Übrigen gilt es sich vorzustellen. Die „affinen Geraden" sollen unseren

Sichtlinien entsprechen. 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 denkt man sich dann 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 [AN1] 2.2.15 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 oder allgemeineren Teilkörpern des Körpers der reellen Zahlen. Überspitzt könnte man sagen, daß man im Gegensatz zu früher, als die mathematische Modellierung der Ebene mithilfe der euklidischen Axiome an den Anfang gestellt wurde, seit dem Anfang des 20.-ten Jahrhunderts mit der Modellierung der Gerade beginnt, in der Gestalt unserer Axiomatik für den Körper der reellen Zahlen [AN1] 1.5.

Beispiel 3.1.8. 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 3.1.9. Die schmutzige Menge aller **Zeitpunkte der klassischen Mechanik** mag man mathematisch als einen eindimensionalen reellen affinen Raum

$$\mathbb{T}$$

modellieren. Dieses Modell werden wir in 6.5.10 noch durch die Vorgabe einer ausgezeichneten „Orientierung" erweitern und so die „Zeit" formal als ein Gebilde der Mengenlehre definieren. Der Buchstabe $\mathbb{T}$ soll an das lateinische Wort „tempus" für „Zeit" erinnern. Eine mögliche Translation in diesem Raum 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 $\mathbb{T} \to \mathbb{E}$ oder genauer, da Fliegen ja sterblich sind, durch die Abbildung einer geeigneten Teilmenge $I \subset \mathbb{T}$ nach $\mathbb{E}$ beschreiben.

Beispiel 3.1.10. Ein Vektor des Homomorphismenraums $\mathrm{Hom}(\vec{\mathbb{T}}, \vec{\mathbb{E}})$ im Sinne von 2.3.14 modelliert, was man in der Physik eine **vektorielle Geschwindigkeit** nennt.

Definition 3.1.11. Eine Abbildung $\varphi : E \to F$ zwischen affinen Räumen über demselben Körper heißt eine **affine Abbildung**, wenn es eine lineare Abbildung zwischen den zugehörigen Richtungsräumen $\vec{\varphi} : \vec{E} \to \vec{F}$ gibt mit

$$\varphi(p) - \varphi(q) = \vec{\varphi}(p - q) \ \ \forall p, q \in E$$

Diese lineare Abbildung $\vec{\varphi}$ ist dann durch φ eindeutig bestimmt und heißt der **lineare Anteil** oder **Richtungsanteil** $\mathrm{Richt}(\varphi) := \vec{\varphi}$ unserer affinen Abbildung. Eine bijektive affine Abbildung heißt ein **Isomorphismus von affinen Räumen**. Ein Isomorphismus von einem affinen Raum auf sich selbst heißt ein **Automorphismus** von besagtem affinen Raum. Die Menge aller affinen Abbildungen von einem affinen Raum E in einen weiteren affinen Raum F über demselben Grundkörper K notieren wir

$$\mathrm{Aff}(E, F) = \mathrm{Aff}_K(E, F)$$

Beispiel 3.1.12. Eine Abbildung $\varphi : V \to W$ zwischen Vektorräumen ist affin als Abbildung zwischen den dazu gebildeten affinen Räumen genau dann, wenn es eine lineare Abbildung $\vec{\varphi} : V \to W$ und einen Punkt $w \in W$ gibt mit

$$\varphi(v) = w + \vec{\varphi}(v)$$

für alle $v \in V$. Jede affine Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ hat also die Gestalt $v \mapsto Av + b$ für $A \in \mathrm{Mat}(m \times n; \mathbb{R})$ und $b \in \mathbb{R}^m$. Dabei ist $A = [\vec{\varphi}]$ die Matrix des Richtungsanteils und $b = \varphi(0)$ das Bild des Ursprungs.

Beispiel 3.1.13 (**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. Im reellen Fall sind im Graphenbild aus der Schule die affinen Abbildungen $\mathbb{R} \to \mathbb{R}$ genau diejenigen Abbildungen, deren Graph eine Gerade ist, und die auf der Schule leider meist als „lineare Abbildungen“ bezeichnet werden.

Übungen

Übung 3.1.14. 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 3.1.15. Eine Abbildung $\varphi : E \to F$ zwischen affinen Räumen ist genau dann affin, wenn es einen Punkt $p \in E$ und eine lineare Abbildung $\vec{\varphi} : \vec{E} \to \vec{F}$ zwischen den zugehörigen Richtungsräumen gibt mit

$$\varphi(p + \vec{v}) = \varphi(p) + \vec{\varphi}(v) \ \ \forall \vec{v} \in \vec{E}$$

Übung 3.1.16 (**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

$$\vec{E} = \{\varphi \in \mathrm{Aff}(E, E) \mid \vec{\varphi} = \mathrm{id}_{\vec{E}}\}$$

Übung 3.1.17 (**Affine Abbildungen mit verschwindendem linearen 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

$$\{\varphi \in \mathrm{Aff}(E, F) \mid \vec{\varphi} = 0\} = \{\varphi \in \mathrm{Ens}(E, F) \mid \varphi \text{ ist konstant}\}$$

Übung 3.1.18. Gegeben ein affiner Raum E und ein Punkt $p \in E$ zeige man, daß die Abbildung $E \to E$ gegeben durch $p + \vec{v} \mapsto p - \vec{v}$ affin ist. Sie heißt die **Punktspiegelung an** p. Allgemeiner zeige man, daß für alle Skalare λ aus dem Grundkörper die Abbildung $E \to E$ gegeben durch $p + \vec{v} \mapsto p + \lambda\vec{v}$ affin ist. Sie heißt die **Streckung** oder auch **Homothetie mit Zentrum** p **um den Faktor** λ.

Übung 3.1.19. Beschreiben Sie in schmutzigen Worten affine Abbildungen $\mathbb{T} \to \mathbb{E}$ des affinen Raums der Zeiten in den Anschauungsraum. Natürlich ist das keine mathematische Übung im eigentlichen Sinne!

Übung 3.1.20 (**Produkt affiner Räume**). Man zeige: Gegeben affine Räume $X_1, \ldots, X_n$ gibt es auf ihrem kartesischen Produkt $X_1 \times \ldots \times X_n$ genau eine Struktur als affiner Raum derart, daß alle Projektionen pr_i affin sind. Des weiteren liefern dann die linearen Anteile der Projektionen mit 2.3.13 einen Isomorphismus zwischen dem Richtungsraum des Produkts und dem Produkt der Richtungsräume der Faktoren.

Beispiel 3.1.21. Bezeichnet $\mathbb{E}$ den Raum unserer Anschauung, so mag man jede mögliche Konstellation von Erde und Mond als einen Punkt von $\mathbb{E} \times \mathbb{E}$ modellieren.

3.2 Affine Teilräume

3.2.1. Nach der reinen Lehre sollte eine Teilmenge eines affinen Raums ein „affiner Teilraum“ heißen genau dann, wenn sie so mit der Struktur eines affinen Raums versehen werden kann, daß die Einbettung eine affine Abbildung wird. Da diese Definition jedoch für Anwendungen erst aufgeschlüsselt werden muß, nehmen wir als unsere Definition gleich die aufgeschlüsselte Fassung und überlassen dem Leser den Nachweis der Äquivalenz zur Definition aus der reinen Lehre als Übung 3.2.16.

Definition 3.2.2. Eine Teilmenge $F \subset E$ eines affinen Raums heißt ein **affiner Teilraum**, wenn es einen Punkt $p \in E$ und einen Untervektorraum $W \subset \vec{E}$ gibt mit

$$F = p + W$$

Die durch Restriktion gegebene Abbildung $W \to \operatorname{Ens}^{\times} F$ ist dann eine Injektion und wir erklären wir auf F die Struktur eines affinen Raums, indem wir als Richtungsraum $\vec{F}$ das Bild von W in $\operatorname{Ens}^{\times} F$ nehmen und diese abelsche Gruppe mit derjenigen Struktur eines K-Vektorraums versehen, für die Restriktion $W \xrightarrow{\sim} \vec{F}$ ein Vektorraumisomorphismus ist.

Beispiel 3.2.3. Die affinen Teilräume 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, und der ganze $\mathbb{R}^3$.

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.

3.2.5. Ein nichtleerer Schnitt von affinen Teilräumen eines affinen Raums ist stets wieder ein affiner Teilraum, und der Richtungsraum des Schnitts ist der Schnitt der Richtungsräume, zumindest wenn wir alle diese Richtungsräume wie in 3.2.10 als Teilmengen des Richtungsraums unseres ursprünglichen Raums betrachten.

Definition 3.2.6. Gegeben eine nichtleere Teilmenge $T \neq \emptyset$ eines affinen Raums gibt es nach 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 Teilmenge, die ihn erzeugt.

3.2.7 (**Explizite Beschreibung affiner Erzeugnisse**). Man mag den von einer nichtleeren Teilmenge T eines affinen Raums E erzeugten affinen Teilraum auch beschreiben als

$$\langle T \rangle_{\text{aff}} = T + \langle p - q \mid p, q \in T \rangle$$

In Worten nehme man also den Untervektorraum des Richtungsraums von $\vec{E}$, der von allen zwei Punkte unserer Teilmenge ineinander überführenden Vektoren erzeugt wird, und lasse seine Vektoren auf Punkte unserer Teilmenge los: Alle Punkt, die man so erhalten kann, bilden einen affinen Teilraum, da ja offensichtlich gilt $T + \langle p - q \mid p, q \in T \rangle = t + \langle p - q \mid p, q \in T \rangle$ für alle $t \in T$.

3.2.8 (**Anschauliche Interpretation linearer Gleichungssysteme**). Wählen wir im Anschauungsraum $\mathbb{E}$ einen festen Punkt p als **Ursprung** und eine 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 $\mathbb{E} \to \mathbb{R}$, 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 veranschaulichen 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 Gerade 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.

3.2.9. Eine Teilmenge eines affinen Raums heißt eine **Hyperebene** oder genauer eine **affine Hyperebene**, wenn sie ein echter affiner Teilraum ist, dessen Richtungsraum im Sinne von 1.5.16 eine lineare Hyperebene im Richtungsraum unseres ursprünglichen affinen Raums ist.

3.2.10. Gegeben ein affiner Raum E mit einem affinen Teilraum $F \subset E$ verwenden wir von nun an das Symbol $\vec{F}$ auch für denjenigen Untervektorraum von $\vec{E}$, den wir als das Bild des Richtungsraums $\vec{F}$ von F unter dem linearen Anteil der Einbettung erhalten.

Definition 3.2.11. Zwei affine Teilräume $T, S \subset E$ eines affinen Raums E heißen **parallel**, wenn im Richtungsraum $\vec{E}$ gilt $\vec{T} \subset \vec{S}$ oder $\vec{S} \subset \vec{T}$.

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 bis auf das Detail, daß mit unserer Definition auch ein Enthaltensein als Parallelität gilt. Allerdings hat sie den Nachteil, daß ein Punkt zu jedem weiteren Teilraum parallel ist, was meinem Sprachempfinden eigentlich zuwiderläuft.

Ergänzung 3.2.13. Der Begriff „parallel“ kommt aus dem Griechischen und heißt „nebeneinander“.

Übungen

Übung 3.2.14 (**Fasern linearer Abbildungen**). Gegeben eine lineare Abbildung $f : V \to W$ 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 3.2.15 (**Urbilder affiner Teilräume**). Ist $f : V \to W$ 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 3.2.14.

Ergänzende Übung 3.2.16. Sei E ein affiner Raum. Genau dann ist eine Teilmenge $F \subset E$ ein affiner Teilraum im Sinne von 3.2.2, wenn F eine Struktur als affiner Raum $(F, \vec{F}, b)$ besitzt derart, daß die Einbettung eine affine Abbildung ist. Die fragliche affine Struktur auf F ist dadurch dann eindeutig bestimmt.

Übung 3.2.17. 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 3.2.18. 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 3.2.19. Der von einer nichtleeren endlichen Teilmenge T eines affinen Raums erzeugte Teilraum hat höchstens die Dimension $|T| - 1$.

Übung 3.2.20 (**Dimension eines affinen Erzeugnisses**). Gegeben zwei endlichdimensionale affine Teilräume 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 3.2.21 (**Kodimension eines Schnitts**). Ist E ein endlichdimensionaler affiner Raum und vereinbaren wir die Notation $\operatorname{codim}(A \subset E) := \dim E - \dim A$ für die Dimensionsdifferenz, die sogenannte **Kodimension von** A **in** E, so gilt unter der Annahme $A \cap B \neq \emptyset$ die Abschätzung

$$\operatorname{codim}((A \cap B) \subset E) \leq \operatorname{codim}(A \subset E) + \operatorname{codim}(B \subset E)$$

Die Kodimension des Schnitts ist also höchstens die Summe der Kodimensionen der sich schneidenden Teilräume.

Vorschau 3.2.22. In der kommutativen Algebra [KAG] 4.8.12 können Sie lernen, wie man diese Abschätzung für die Kodimension eines Schnitts auf Nullstellenmengen polynomialer Gleichungssysteme verallgemeinern kann, wenn der Grundkörper algebraisch abgeschlossen ist.

Übung 3.2.23. Eine Abbildung $f : E \to F$ von affinen Räumen ist genau dann affin, wenn ihr Graph $\Gamma(f) \subset E \times F$ ein affiner Teilraum des Produkts unserer beiden Räume im Sinne von 3.1.20 ist.

3.3 Affine Räume und ihre Geraden

Satz 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 unter unserer Abbildung wieder eine Gerade ist.*

3.3.2. Dieselbe Charakterisierung gilt allgemeiner über jedem Grundkörper, dessen einziger Körperautomorphismus die Identität ist. Wir diskutieren mehr dazu in 3.3.5.

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 3.3.1 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 3.3.1 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 Bezeichung 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 3.3.4. *Eine injektive Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ mit $\Phi(0) = 0$, unter der das Bild jeder affinen Geraden wieder eine affine Gerade ist, muß linear sein.*

Beweis. Halten wir eine geeignete lineare Abbildung dahinter, so erkennen wir mit 2.3.2, daß wir ohne Beschränkung der Allgemeinheit annehmen dürfen, daß unser Φ die Vektoren e_1 und e_2 der Standardbasis festhält. Unter dieser Zusatzannahme zeigen wir nun, daß Φ sogar die Identität ist. Zunächst gibt es sicher Abbildungen $\psi_1, \psi_2 : \mathbb{R} \to \mathbb{R}$ mit $\Phi(a\mathrm{e}_i) = \psi_i(a)\,\mathrm{e}_i$. Da wir Φ injektiv angenommen haben, müssen unter Φ parallele alias sich nicht schneidende Geraden parallel bleiben. Die Gerade durch $a\mathrm{e}_1$ und $a\mathrm{e}_2$ für $a \neq 0, 1$ ist parallel zu der durch e_1 und e_2, also ist für $a \neq 0, 1$ auch die Gerade durch $\Phi(a\mathrm{e}_1) = \psi_1(a)\,\mathrm{e}_1$ und $\Phi(a\mathrm{e}_2) = \psi_2(a)\,\mathrm{e}_2$ parallel zu der durch $\Phi(\mathrm{e}_1) = \mathrm{e}_1$ und $\Phi(\mathrm{e}_2) = \mathrm{e}_2$. 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

$$\Phi(\mathrm{e}_1 + a\,\mathrm{e}_2) \quad = \quad \mathrm{e}_1 + \psi(a)\,\mathrm{e}_2$$

im Fall $a \neq 0$ wegen der linearen Unabhängigkeit und im Fall $a = 0$ wegen $\psi(0) = 0$. Weiter folgern wir die beiden Gleichungen

$$\begin{array}{rcl} \Phi(\mathrm{e}_1 + (a+b)\,\mathrm{e}_2) & = & \mathrm{e}_1 + \psi(a+b)\,\mathrm{e}_2 \\ \Phi(\mathrm{e}_1 + a\,\mathrm{e}_2 + b\,\mathrm{e}_2) & = & \mathrm{e}_1 + \psi(a)\,\mathrm{e}_2 + \psi(b)\,\mathrm{e}_2 \end{array}$$

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 e_1 und $a\mathrm{e}_2$ parallel ist zu der durch $b\mathrm{e}_1$ und $ab\mathrm{e}_2$ folgt auch $\psi(ab) = \psi(a)\psi(b)$ 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 [AN1] 1.5.3 oder besser [AN1] 1.5.18 die Identität der einzige Körperhomomorphismus $\psi : \mathbb{R} \to \mathbb{R}$ ist, folgt $\psi = \mathrm{id}$. Da wie bereits erwähnt gilt $\Phi(v + w) = \Phi(v) + \Phi(w)$ falls v und w linear unabhängig sind, folgt sofort $\Phi = \mathrm{id}$. □

Um nun Satz 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 Φ. Gegeben $v, w \in E$ linear unabhängig kann offensichtlich die von v und w aufgespannt 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 Φ. Da Φ Geraden auf Geraden abbildet, folgt $\Phi(\langle v, w\rangle) = \langle \Phi(v), \Phi(w)\rangle$. Von der mithin von Φ 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 $\Phi(u+u_1) = \Phi(u)+\Phi(u_1)$ und $\Phi(\lambda u) = \lambda\Phi(u)$ für alle $u, u_1 \in \langle v, w\rangle$ und $\lambda \in \mathbb{R}$. Da aber in einem Vektorraum der Dimension mindestens Zwei je zwei Vektoren u, u_1 in einem gemeinsamen zweidimensionalen Teilraum liegen, zeigt das bereits die Linearität von Φ selbst. □

Ergänzung 3.3.5. Geht man den Beweis von Lemma 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 Φ 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 Φ „linear bis auf einen Körperisomorphismus".

Ergänzung 3.3.6 (**Von der Geometrie zur Algebra**). Geht man den Beweis von Satz 3.3.1 im Lichte von 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 7.1 besprochen. In dieser Weise lassen sich dann die Körperaxiome [GR] 3.4.2 sogar geometrisch rechtfertigen.

3.4 Baryzentrische Koordinaten*

3.4.1. Gegeben ein Körper K, ein affiner Raum E über K, Punkte $e_1, \ldots, e_n \in E$ und Skalare $\lambda_1, \ldots, \lambda_n \in K$ mit $\lambda_1 + \ldots + \lambda_n \neq 0$ definiert man den **Schwerpunkt** s **der** e_i **mit den Gewichten** λ_i durch die Bedingung

$$\lambda_1(e_1 - s) + \ldots + \lambda_n(e_n - s) = \vec{0}$$

Daß höchstens ein Punkt $s \in E$ diese Bedingung erfüllen kann, folgt daraus, daß für jedes weitere s', das unsere Bedingung erfüllt, gelten muß

$$(\lambda_1 + \ldots + \lambda_n)(s - s') = \vec{0}$$

Daß es überhaupt ein s gibt, das unsere Bedingung erfüllt, erkennt man, indem man einen beliebigen Punkt $p \in E$ wählt und $\lambda = \lambda_1 + \ldots + \lambda_n$ setzt und den Punkt

$$s = p + \frac{\lambda_1}{\lambda}(e_1 - p) + \ldots + \frac{\lambda_n}{\lambda}(e_n - p)$$

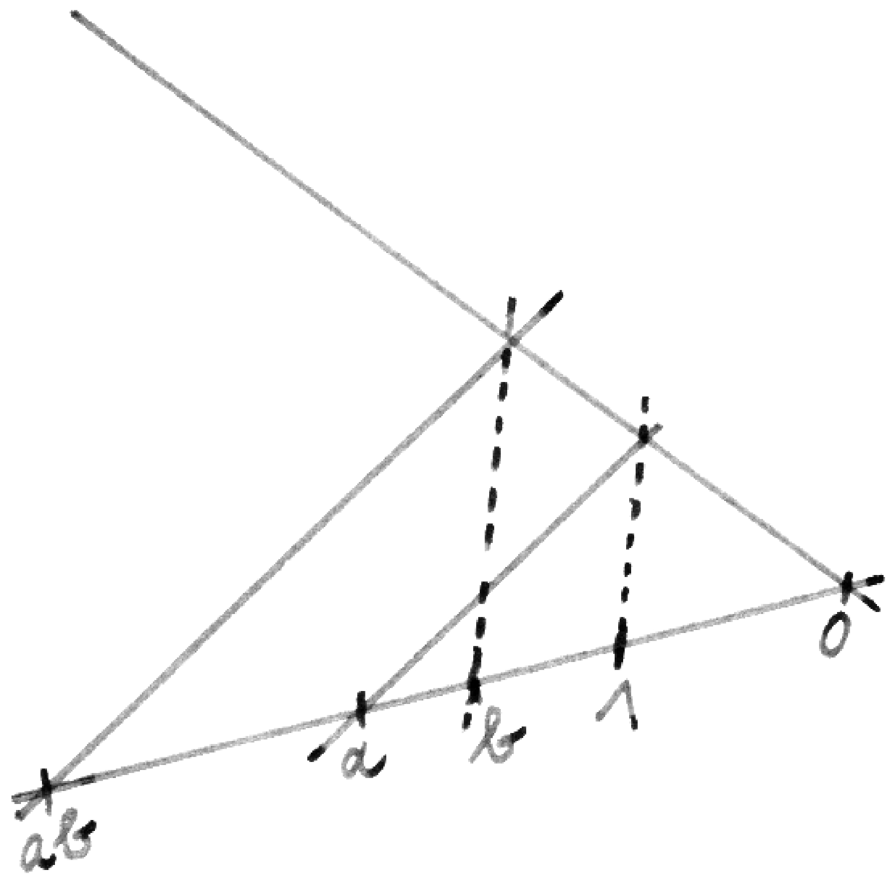
betrachtet. Für diesen Punkt $s \in E$ gilt ja

$$\lambda(s - p) = \lambda_1(e_1 - p) + \ldots + \lambda_n(e_n - p)$$

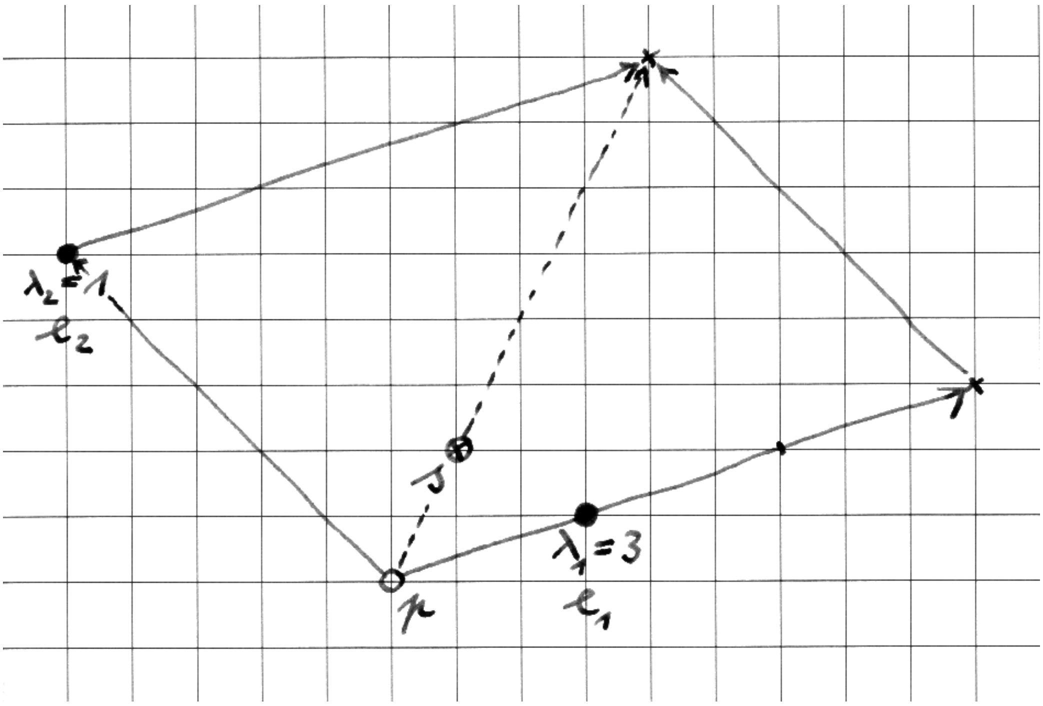
und daraus folgt dann leicht

$$\vec{0} = \lambda_1(e_1 - s) + \ldots + \lambda_n(e_n - s)$$

Ergänzung 3.4.2. Eine Teilmenge eines affinen Raums heißt **affin unabhängig**, wenn sich keiner ihrer Punkte als gewichteter Schwerpunkt von endlich vielen anderen ihrer Punkte schreiben läßt.



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.



Zwei fette Punkte der Gewichte 3 und 1 und ihr Schwerpunkt s nebst seiner Bestimmung mithilfe eines beliebigen weiteren Punktes p.

Definition 3.4.3. Gegeben Punkte p, q in einem affinen Raum E über einem angeordneten Körper schreiben wir

$$[p, q] := \{p + t(q - p) \mid 0 \leq t \leq 1\}$$

und nennen diese Menge im Fall $p \neq q$ das die Punkte p und q verbindende **Geradensegment**.

Definition 3.4.4. Eine Teilmenge eines affinen Raums über einem angeordneten Körper heißt **konvex** genau dann, wenn sie mit je zwei Punkten auch das ganze diese verbindende Geradensegment enthält.

Definition 3.4.5. 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 können sie etwa konstruieren als den Schnitt aller konvexen Teilmengen, die T umfassen. Wir verwenden für die konvexe Hülle von T die Notation

$$\operatorname{konv}(T)$$

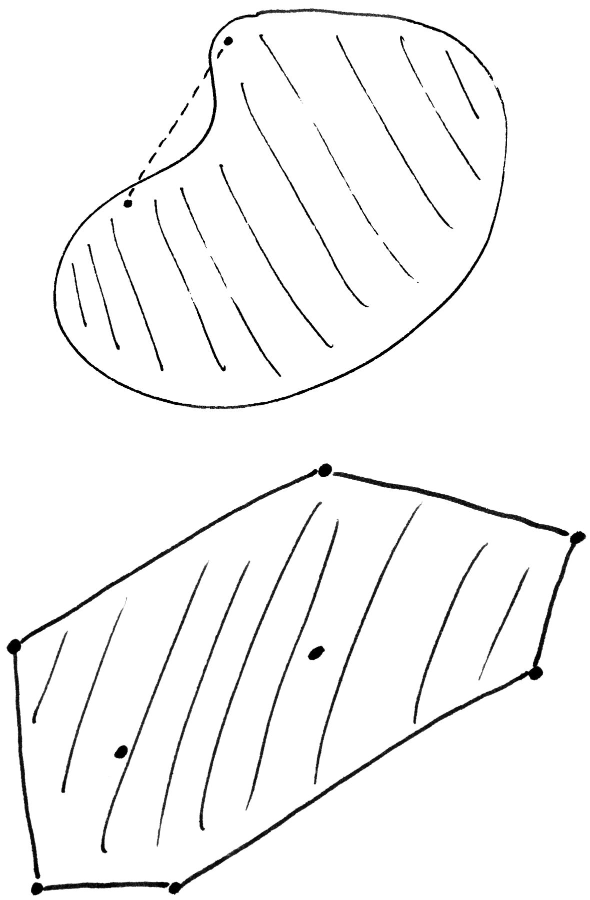
Beispiel 3.4.6. Gegeben zwei Punkte in einem affinen Raum über einem angeordneten Körper ist ihre konvexe Hülle genau das verbindende Geradensegment, in Formeln $[p, q] = \operatorname{konv}(p, q)$.

Übungen

Übung 3.4.7. Ist E ein n-dimensionaler affiner Raum und $e_0, \ldots, e_n$ ein Erzeugendensystem von E, so gibt es für jeden Punkt $s \in E$ genau ein Tupel von Gewichten $(\lambda_0, \ldots, \lambda_n) \in K^{n+1}$ so daß gilt $\lambda_0 + \ldots + \lambda_n = 1$ und daß s der Schwerpunkt der e_i mit den Gewichten λ_i ist. Die λ_i heißen dann die **baryzentrischen Koordinaten von s in Bezug auf die** e_i, nach griechisch „$\beta\alpha\rho\upsilon\varsigma$“ für „schwer“.

Ergänzende Übung 3.4.8. Der von einer nichtleeren Menge von Punkten eines affinen Raums erzeugte affine Teilraum kann auch beschrieben werden als die Menge aller Schwerpunkte zu endlichen mit Gewichten versehenen Teilmengen unserer Menge.

Ergänzende Übung 3.4.9. 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 endlichen mit positiven Gewichten versehenen Teilmengen von T.



Eine nicht konvexe Teilmenge der Ebene und eine endliche Teilmenge der Ebene, dargestellt durch fette Punkte, mit ihrer konvexen Hülle, dargestellt als schraffierter Bereich.

3.5 Abstrakte lineare Abbildungen und Matrizen

3.5.1. 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 3.5.2 (Abstrakte lineare Abbildungen und Matrizen). *Seien K ein Körper und V, W Vektorräume über K mit angeordneten Basen $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$ und $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$. Ordnen wir jeder linearen Abbildung $f : V \to W$ die* **darstellende Matrix** *${}_{\mathcal{B}}[f]_{\mathcal{A}}$ zu mit Einträgen a_{ij}, die durch die Identitäten $f(\vec{v}_j) = a_{1j}\vec{w}_1 + \ldots + a_{nj}\vec{w}_n$ gegeben werden, so erhalten wir eine Bijektion, ja sogar einen Vektorraumisomorphismus*

$$\begin{array}{rccc} \mathrm{M}_{\mathcal{B}}^{\mathcal{A}} : & \mathrm{Hom}_K(V, W) & \stackrel{\sim}{\to} & \mathrm{Mat}(n \times m; K) \\ & f & \mapsto & {}_{\mathcal{B}}[f]_{\mathcal{A}} \end{array}$$

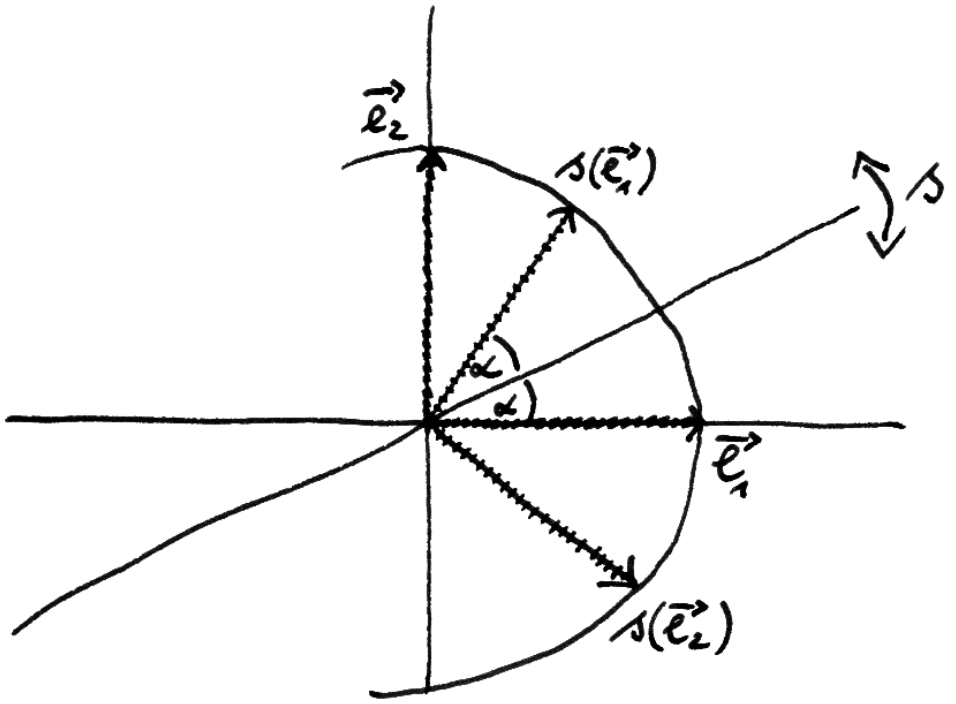
3.5.3. Wir nennen $\mathrm{M}_{\mathcal{B}}^{\mathcal{A}}(f) = {}_{\mathcal{B}}[f]_{\mathcal{A}}$ die **darstellende Matrix der Abbildung f in Bezug auf die Basen $\mathcal{A}$ und $\mathcal{B}$**. In Worten ausgedrückt stehen in ihren Spalten die Koordinaten der Bilder der Vektoren der Basis $\mathcal{A}$ des Ausgangsraums in Bezug auf die Basis $\mathcal{B}$ des Zielraums. Beliebt ist statt ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ und $\mathrm{M}_{\mathcal{B}}^{\mathcal{A}}(f)$ auch die ausführlichere Notation $\mathrm{Mat}_{\mathcal{B}}^{\mathcal{A}}(f)$. Die Matrix einer linearen Abbildung $f : K^m \to K^n$ in Bezug auf die jeweiligen Standardbasen $\mathcal{S}(m)$, $\mathcal{S}(n)$ nach 1.6.11 ist genau unsere darstellende Matrix $[f]$ aus 2.4.1, in Formeln gilt also

$$[f] = {}_{\mathcal{S}(n)}[f]_{\mathcal{S}(m)}$$

Wir vereinbaren allgemeiner, daß wir bei unserer Notation Standardbasen hinfort auch weglassen dürfen. Für eine lineare Abbildung $f : K^m \to W$ schreiben wir also abkürzend ${}_{\mathcal{B}}[f]_{\mathcal{S}(m)} = {}_{\mathcal{B}}[f]$ und für eine lineare Abbildung $f : V \to K^n$ entsprechend ${}_{\mathcal{S}(n)}[f]_{\mathcal{A}} = [f]_{\mathcal{A}}$.

Ergänzung 3.5.4. 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 $s : \mathbb{R}^2 \to \mathbb{R}^2$ 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 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 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

$$\begin{array}{ccccc} \mathrm{Hom}_K(V, W) & \xrightarrow{\sim} & \mathrm{Hom}_K(K^m, K^n) & \xrightarrow{\sim} & \mathrm{Mat}(n \times m; K) \\ f & \mapsto & \Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}} & & \end{array}$$

mit unserer Abbildung : $g \mapsto [g]$ aus 2.4.1 rechts, die eben jeder Abbildung $g : K^m \to K^n$ ihre darstellende Matrix zuordnet. □

Satz 3.5.5 (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 $f : U \to V$ und $g : V \to W$ ist die darstellende Matrix der Verknüpfung das Produkt der darstellenden Matrizen, in Formeln*

$$_{\mathcal{C}}[g \circ f]_{\mathcal{A}} = {}_{\mathcal{C}}[g]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}}$$

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 2.4.5 behandelten Spezialfall. □

Zweiter Beweis. Wir könnten auch expliziter vorgehen und den Beweis von 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 $\mathcal{A}, \mathcal{B}, \mathcal{C}$. □

Definition 3.5.6. Gegeben ein endlichdimensionaler Vektorraum V mit einer angeordneten Basis $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_n)$ notieren wir die Inverse unserer Bijektion $\Phi_{\mathcal{A}} : K^n \xrightarrow{\sim} V$, $(\lambda_1, \ldots, \lambda_n)^\top \mapsto \lambda_1 \vec{v}_1 + \ldots + \lambda_n \vec{v}_n$ 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 3.5.7 (Darstellung des Bildes eines Vektors). *Gegeben endlichdimensionale Räume V, W mit angeordneten Basen $\mathcal{A}, \mathcal{B}$ und eine lineare Abbildung $f : V \to W$ 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 $[\Phi_{\mathcal{B}}^{-1}(f(v))] = [(\Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}})] \circ [\Phi_{\mathcal{A}}^{-1} v]$ behauptet, die aus 2.4.7 folgt. □

Ergänzung 3.5.8. Betrachtet man zu einem beliebigen Vektor $v \in V$ die lineare Abbildung $(\cdot v) : K \to V$, $\lambda \mapsto \lambda v$, und bezeichnet mit $\mathcal{S}(1)$ die Standardbasis $(1) = (\mathrm{e}_1)$ 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 3.5.7 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 3.5.5 über die darstellende Matrix einer Verknüpfung.

Definition 3.5.9. Gegeben zwei angeordnete Basen $\mathcal{A} = (v_1, \ldots, v_n)$ und $\mathcal{B} = (w_1, \ldots, w_n)$ eines Vektorraums V nennt man die darstellende Matrix der Identität

$$ {}_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}} $$

in diesen Basen die **Basiswechselmatrix**. Ihre Einträge a_{ij} werden per definitionem gegeben durch die Gleichungen $v_j = \sum_{i=1}^{n} a_{ij} w_i$.

3.5.10 (**Änderung der darstellenden Matrix bei Basiswechsel**). Offensichtlich ist ${}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{A}} = I$ die Einheitsmatrix. Nach 3.5.5 ist damit die Basiswechselmatrix ${}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ invers zur Basiswechselmatrix in der Gegenrichtung ${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$, in Formeln ${}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}^{-1} = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$. Haben wir nun eine lineare Abbildung $f : V \to W$ und angeordnete Basen $\mathcal{A}, \mathcal{B}$ von V und angeordnete Basen $\mathcal{C}, \mathcal{D}$ von W, so folgt aus 3.5.5 die Identität ${}_{\mathcal{D}}[f]_{\mathcal{B}} = {}_{\mathcal{D}}[\mathrm{id}_W]_{\mathcal{C}} \circ {}_{\mathcal{C}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{B}}$. Sind noch spezieller $\mathcal{A}, \mathcal{B}$ zwei angeordnete Basen ein- und desselben Vektorraums V und ist $f : V \to V$ ein Endomorphismus von V, so erhalten wir unmittelbar die Identität ${}_{\mathcal{B}}[f]_{\mathcal{B}} = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ alias

$$ N = T^{-1} M T $$

für $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}$ und $M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$ die darstellenden Matrizen bezüglich unserer beiden Basen und $T = {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ die Basiswechselmatrix.

Satz 3.5.11 (Smith-Normalform). *Gegeben eine lineare Abbildung zwischen endlichdimensionalen Vektorräumen $f : V \to W$ 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 2.2.6: Wir wählen zunächst eine angeordnete Basis $(w_1, \ldots, w_r)$ des Bildes von f, dazu Urbilder $v_1, \ldots, v_r$ in V, ergänzen diese durch eine angeordnete Basis des Kerns von f zu einer angeordneten Basis $\mathcal{A} = (v_1, \ldots, v_n)$ von V, und ergänzen unsere angeordnete Basis des Bildes zu einer angeordneten Basis $\mathcal{B} = (w_1, \ldots, w_m)$ von W. In diesen Basen hat dann die Matrix von f offensichtlich die behauptete Gestalt. □

Definition 3.5.12. 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

$$\operatorname{tr}(A)$$

Vorschau 3.5.13. Eine vielleicht natürlichere Definition der Spur wird in [LA2] 7.4.33 erklärt. Im Rahmen der Analysis werden wir die Spur in [AN2] 1.5.9 als das Differential der Determinante an der Einheitsmatrix wiedersehen.

Übungen

Übung 3.5.14. Gegeben ein K-Vektorraum V mit einer angeordneten Basis $\mathcal{A} = (v_1, \ldots, v_n)$ liefert die Zuordnung, die jeder weiteren angeordneten Basis $\mathcal{B}$ die Basiswechselmatrix von $\mathcal{A}$ nach $\mathcal{B}$ zuordnet, eine Bijektion

$$\begin{array}{ccc} \{\text{angeordnete Basen von } V\} & \stackrel{\sim}{\to} & \mathrm{GL}(n; K) \\ \mathcal{B} & \mapsto & {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \end{array}$$

Ergänzende Übung 3.5.15. Ein Endomorphismus $f : V \to V$ eines Vektorraums heißt **nilpotent**, wenn es $d \in \mathbb{N}$ gibt mit $f^d = 0$. Sei $f : V \to V$ 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 $\ker(f) \subset \ldots \subset \ker(f^{d-1}) \subset \ker(f^d) = V$, 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 [LA2] 4.4.2 zeigen.

Übung 3.5.16. Man zeige $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ wann immer A eine $(m \times n)$-Matrix ist und B eine $(n \times m)$-Matrix. Man folgere daraus weiter die Identität $\operatorname{tr}(BAB^{-1}) = \operatorname{tr}(A)$ 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**

$$\operatorname{tr}(f) = \operatorname{tr}(f|V) = \operatorname{tr}_K(f|V)$$

zuordnen als die Spur seiner Matrix in Bezug auf eine und jede Basis. Gegeben endlichdimensionale Vektorräume V, W und lineare Abbildungen $f : V \to W$ und $g : W \to V$ zeige man auch $\operatorname{tr}(fg) = \operatorname{tr}(gf)$.

Ergänzende Übung 3.5.17. Leser, die schon mit dem Inhalt des Abschnitts 4.1 über komplexe Zahlen vertraut sind, mögen zeigen: Ist $f : V \to V$ ein Endomorphismus eines endlichdimensionalen $\mathbb{C}$-Vektorraums, so gilt für seine Spur auf dem zugrundeliegenden reellen Vektorraum $\operatorname{tr}_{\mathbb{R}}(f|V) = 2 \operatorname{Re} \operatorname{tr}_{\mathbb{C}}(f|V)$.

Ergänzende Übung 3.5.18. Ist L ein endlichdimensionaler K-Vektorraum und $A : L \to L$ eine K-lineare Abbildung, so gilt

$$\operatorname{tr}((A\circ)| \operatorname{End}_K L) = (\dim_K L) \operatorname{tr}(A|L)$$

Ergänzung 3.5.19. Gegeben ein Endomorphismus f von endlichem Rang eines Vektorraums V erklärt man die **Spur**

$$\operatorname{tr} f = \operatorname{tr}(f|V)$$

von f als die Spur der Verknüpfung $\operatorname{im} f \hookrightarrow V \twoheadrightarrow \operatorname{im} f$ im Sinne unserer Definition 3.5.16 für die Spur eines Endomorphismus eines endlichdimensionalen Vektorraums. Aus 3.5.16 folgt unmittelbar, daß diese Definition im Fall eines endlichdimensionalen Raums V dieselbe Spur liefert wie unsere ursprüngliche auf den endlichdimensionalen Fall beschränkte Definition 3.5.12.

Ergänzende Übung 3.5.20. Sind V, W Vektorräume und $f : V \to W$ sowie $g : W \to V$ lineare Abbildungen und ist eine unserer Abbildungen von endlichem Rang, so gilt $\operatorname{tr}(fg) = \operatorname{tr}(gf)$. Hinweis: Der endlichdimensionale Fall kann nach 3.5.16 vorausgesetzt werden.

Ergänzende Übung 3.5.21. Gegeben ein Endomorphismus f von endlichem Rang eines Vektorraums mit der Eigenschaft $f^2 = af$ für ein Element a des Grundkörpers gilt stets $\operatorname{tr}(f) = a \dim(\operatorname{im} f)$. Hinweis: 2.2.18.

Übung 3.5.22. 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.

3.6 Möbiusfunktion*

3.6.1. Gegeben $(X, \leq)$ eine endliche partiell geordnete 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 $x_1, x_2, \ldots, x_n$ 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 partiell geordneten Menge

$$\begin{array}{rccc} \mu : & X & \to & \mathbb{Z} \\ & y & \mapsto & (A^{-1})_{k,y} \end{array}$$

Sie wird demnach charakterisiert duch 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 partiell geordnete Menge X, die man aufzählen kann als $x_1, x_2, \ldots$ mit $x_i \leq x_j \Rightarrow i \leq j$.

3.6.2. Ist $X = \mathbb{N} = \{0, 1, 2, \ldots\}$ mit der üblichen Ordnung, so haben wir $\mu(0) = 1, \mu(1) = -1$ und $\mu(n) = 0$ für $n \geq 2$. Ist $X = \mathbb{N}_{\geq 1} = \{1, 2, \ldots\}$ mit der durch das Teilen gegebenen Ordung $a \leq b \Leftrightarrow a|b$, 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 3.6.3 (**Kehrwerte der Riemann'schen ζ-Funktion**). Mit μ der Möbiusfunktion der Zahlentheorie zeige man, daß für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$ die Inversen der Werte der Riemann'schen ζ-Funktion geschrieben werden können als

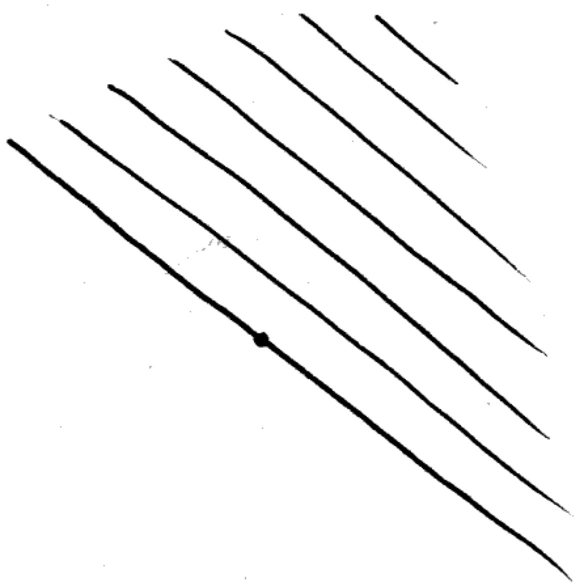
$$\frac{1}{\zeta(s)} = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$$

Übung 3.6.4. Man bestimme die Inverse der $(n \times n)$-Matrix gegeben durch $a_{ij} = 1$ für $i \leq j$ und $a_{ij} = 0$ für $i > j$.

3.7 Dualräume und transponierte Abbildungen

Definition 3.7.1. Gegeben ein Körper K und ein K-Vektorraum V nennt man eine lineare Abbildung $V \to K$ eine **Linearform auf** V oder einen **Kovektor**. Die Menge aller solchen Linearformen bildet nach 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.

3.7.2 (**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.

3.7.3. 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 3.7.4 (**Frequenzenraum als Dualraum des Raums der Zeitspannen**). Denken wir uns die Gesamtheit aller Zeitspannen als reellen Vektorraum, so können wir uns den Dualraum dieses Vektorraums denken als die Gesamtheit aller „Frequenzen" oder vielleicht besser aller möglichen „Drehgeschwindigkeiten von Drehungen um eine feste Achse". Zeichnen wir genauer einen Drehsinn als positiv aus, so entpräche 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.

3.7.5 (**Koordinatenfunktionen zu einer Basis**). Gegeben ein Vektorraum V und eine Basis $\mathcal{B} \subset V$ erhalten wir im Dualraum $V^\top$ eine linear unabhängige Familie von Linearformen $(b^\top)_{b\in\mathcal{B}}$, indem wir $b^\top = b^\top_{\mathcal{B}} : V \to K$ erklären durch

$$b^\top(c) = \delta_{bc} \; \forall c \in \mathcal{B}$$

Die Linearformen $b^\top$ heißen die **Koordinatenfunktionen** oder kurz **Koordinaten** zu unserer Basis $\mathcal{B}$. Vielfach werden sie auch b^* notiert. Ist etwa $V = \mathbb{R}^n$ und $\mathcal{B} = \mathcal{S}(n) = (\vec{\mathrm{e}}_1, \ldots, \vec{\mathrm{e}}_n)$ die Standardbasis, so wird $\vec{\mathrm{e}}_i^\top : \mathbb{R}^n \to \mathbb{R}$ die „Projektion auf die i-te Koordinate" $\vec{\mathrm{e}}_i^\top = \mathrm{pr}_i : (x_1, \ldots, x_n) \mapsto x_i$, die man oft auch einfach $x_i : \mathbb{R}^n \to \mathbb{R}$ 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 $\mathcal{B}$.

Beispiel 3.7.6 (**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 durchaus so sehen, insbesondere wenn man den kanonischen Isomorphismus $\mathrm{Mat}(1 \times n; K) \xrightarrow{\sim} \mathrm{Hom}(K^n, K)$ aus 2.4.7 soweit verinnerlicht hat, daß man beide Seiten schlicht als gleich ansieht.

Beispiel 3.7.7 (**Dualraum des Richtungsraums zum Raum der Anschauung**). Denken wir uns wie in 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 vermittels 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, und 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 [LA2] 2.3 mathematisch modellieren werden. Auf allgemeinen Vektorräumen stehen uns keine orthogonalen Projektionen zur Verfügung und der Dualraum kann dann nicht mehr so leicht mit dem Ausgangsraum identifiziert werden.

3.7.8. Gegeben ein k-Vektorraum V haben wir stets eine kanonische bilineare Abbildung $V \times V^\top \to k$, die **Auswertungsabbildung**, auch genannt die **kanonische Paarung** von Vektoren mit Kovektoren.

3.7.9 (**Dimension des Dualraums**). Gegeben ein endlichdimensionaler Vektorraum stimmt seine Dimension mit der Dimension seines Dualraums überein, in Formeln

$$\dim V^\top = \dim V$$

In der Tat, ist $B \subset V$ eine Basis, so liefert nach 2.3.2 das Einschränken von Abbildungen eine Bijektion $\dim V^\top \stackrel{\sim}{\to} \mathrm{Ens}(B, K)$, der man leicht ansieht, daß sie sogar ein Vektorraumisomorphismus sein muß.

3.7.10. Für jeden endlichdimensionalen Vektorraum V hat der Dualraum nach 3.7.9 dieselbe Dimension wie V selber. Ist also $\mathcal{B}$ eine angeordnete Basis von V, so ist $\mathcal{B}^\top := (b^\top)_{b \in \mathcal{B}}$ als linear unabhängige Familie der richtigen Kardinalität eine angeordnete Basis des Dualraums $V^\top$. Man nennt dann $\mathcal{B}^\top$ die **duale Basis** zur Basis $\mathcal{B}$. Insbesondere besteht die duale Basis zur Standardbasis des $\mathbb{R}^n$ genau aus den üblichen Koordinatenfunktionen, in Formeln $\mathcal{S}(n)^\top = (\mathrm{pr}_i)_{i=1}^n$.

Beispiel 3.7.11. Wir kehren nocheinmal zu unserem Beispiel 3.7.4 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 3.7.12 (**Dualräume unendlichdimensionaler Vektorräume**). Im Fall eines unendlichdimensionalen Vektorraums ist wieder nach 2.3.14 auch sein Dualraum unendlichdimensional, aber dessen Dimension ist „noch unendlicher" als die Dimension des Ausgangsraums in einem Sinne, der in [AL] 5.3.14 präzisiert wird.

Definition 3.7.13. Gegeben eine K-linare Abbildung $f : V \to W$ erklären wir die **duale** oder auch **transponierte Abbildung**

$$f^\top : W^\top \to V^\top$$

als das „Vorschalten von f", in Formeln $f^\top(\lambda) := \lambda \circ f : V \to K$ für jede Linearform $\lambda : W \to K$.

3.7.14. Man beachte, daß die duale Abbildung „in die umgekehrte Richtung" geht. Oft wird die duale Abbildung auch $f^* : W^* \to V^*$ notiert. Nicht selten schreibt man auch ein kleines t als Index oben links und notiert die duale alias transponierte Abbildung ${}^t f$.

3.7.15 (**Verknüpfung und Transponieren**). Sicher gilt stets $\mathrm{id}_V^\top = \mathrm{id}_{V^\top} : V^\top \to V^\top$. Man prüft auch leicht für eine Verknüpfung $f \circ g$ von linearen Abbildungen die Identität

$$(f \circ g)^\top = g^\top \circ f^\top$$

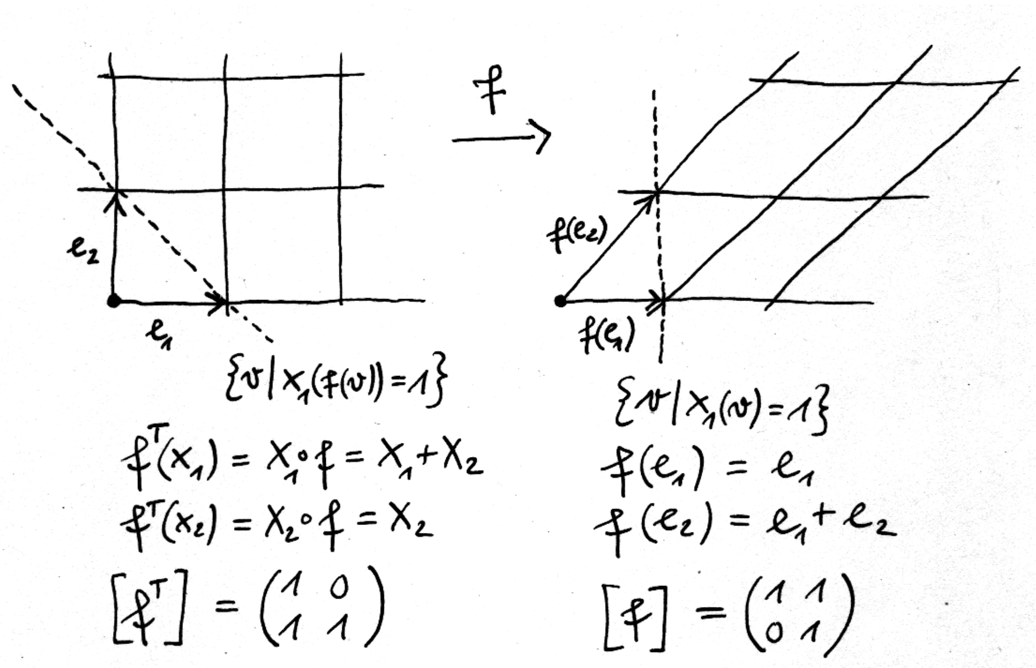
In der Tat bedeutet das Vorschalten von $f \circ g$ nichts anderes, als erst f und dann g vorzuschalten.

Proposition 3.7.16 (Matrix der dualen Abbildung). *Gegeben eine lineare Abbildung $f : V \to W$ von endlichdimensionalen Vektorräumen mit angeordneten Basen $\mathcal{A}, \mathcal{B}$ ist die darstellende Matrix der dualen Abbildung $f^\top : W^\top \to V^\top$ bezüglich der dualen Basen $\mathcal{B}^\top, \mathcal{A}^\top$ gerade Transponierte der Matrix von f, in Formeln*

$$_{\mathcal{A}^\top}[f^\top]_{\mathcal{B}^\top} = ({}_{\mathcal{B}}[f]_{\mathcal{A}})^\top$$

3.7.17. Diese Identität ist der Grund dafür, daß ich für den Dualraum vorzugsweise die Notation mit einem hochgestellten $\top$ verwenden will.

Beweis. Seien etwa $\mathcal{A} = (v_1, \ldots, v_n)$ und $\mathcal{B} = (w_1, \ldots, w_n)$. 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



Eine lineare Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$, deren Matrix in einer Basis $\mathrm{e}_1, \mathrm{e}_2$, und die Matrix der dualen Abbildung auf der dualen Basis alias der Effekt des Vorschaltens unserer Abbildung auf den Koordinatenfunktionen $x_1, x_2 : \mathbb{R}^2 \to \mathbb{R}$.

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. □

3.7.18 (**Auswerten als Matrixmultiplikation**). Sei V ein endlichdimensionaler Vektorraum mit einer angeordneten Basis $\mathcal{A}$. Eine Linearform $\lambda \in V^\top$ wird als lineare Abbildung $\lambda : V \to k$ beschrieben durch eine Zeilenmatrix $[\lambda]_{\mathcal{A}} = {}_{\mathcal{S}(1)}[\lambda]_{\mathcal{A}}$. Für das Auswerten unserer Linearform λ 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 (1×1)-Matrizen. Erinnern wir dann noch für $v \in V$ an die lineare Abbildung $(\cdot v) : K \to V$ 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 3.5.5 für die Matrix der Verknüpfung zweier linearer Abbildungen.

3.7.19 (**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, das λ auf der linken Seite nicht transponiert zu sehen. Dieser Anschein von Inkonsistenz kommt dadurch zustande, daß wir in unserer Formel links λ 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 $(\cdot\lambda) : k \to V^\top$ bis auf die offensichtliche Identifikation $k \xrightarrow{\sim} k^\top$ genau die transponierte Abbildung zu $\lambda : V \to k$ 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 3.7.16 für die Matrix der dualen Abbildung, indem wir die linke Seite obiger Formel in dieser Weise umformen und ihre rechte Seite ausschreiben zu $\left({}_{\mathcal{S}(1)}[\lambda]_{\mathcal{A}}\right)^\top$.

Beispiel 3.7.20 (**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 λ 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 $[f] = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$und $f(\vec{\mathrm{e}}_1) = \vec{\mathrm{e}}_1, f(\vec{\mathrm{e}}_2) = \vec{\mathrm{e}}_1 + \vec{\mathrm{e}}_2$. Offensichtlich bleibt die y-Koordinate eines Punktes unter solch einer Scherung unverändert, $(f^\top)^{-1}(\vec{\mathrm{e}}_2^\top) = \vec{\mathrm{e}}_2^\top$, und die x-Koordinate des Urbildpunkts entspricht der Differenz zwischen x-Koordinate und y-Koordinate des Bildpunkts, $(f^\top)^{-1}(\vec{\mathrm{e}}_1^\top) = \vec{\mathrm{e}}_1^\top - \vec{\mathrm{e}}_2^\top$. Das entspricht auch unseren Formeln, nach denen $f^\top$ bezüglich der Basis $(\vec{\mathrm{e}}_1^\top, \vec{\mathrm{e}}_2^\top)$ dargestellt wird durch die transponierte Matrix $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$, 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.

3.7.21 (**Anschauung für den Transport von Linearformen**). Eine von Null verschiedene Linearform $\lambda : V \to K$ 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 einigermasen 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 3.7.22. 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**

$$\mathrm{ev} = \mathrm{ev}_V : V \hookrightarrow V^{\top\top}$$

als die Vorschrift, die jedem Vektor $v \in V$ das „Evaluieren auf v" zuordnet. In Formeln ist $\mathrm{ev}(v) \in V^{\top\top}$ also definiert als die lineare Abbildung $\mathrm{ev}(v) : V^\top \to K$ mit $\lambda \mapsto \lambda(v)$.

3.7.23 (**Injektivität der kanonischen Abbildung**). Die Injektivität der kanonischen Abbildung $V \to V^{\top\top}$ 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 2.6.3 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 1.9.15. 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.

3.7.24 (**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.

3.7.25. Gegeben Mengen X, Y, Z, W und Abbildungen $f : X \to Y$ und $g : X \to Z$ und $h : Y \to W$ und $l : Z \to W$ mit $h \circ f = l \circ g$ sagt man auch, man habe ein **kommutatives Rechteck**

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "g"'] & Y \arrow[d, "h"] \\ Z \arrow[r, "l"] & W \end{tikzcd}$$

Ich finde diese Darstellung sehr viel übersichtlicher.

3.7.26 (**Kanonische Einbettung und bitransponierte Abbildung**). Gegeben eine lineare Abbildung $f : V \to W$ kommutiert das Rechteck

$$\begin{tikzcd} V \arrow[r, "\mathrm{ev}_V"] \arrow[d, "f"'] & V^{\top\top} \arrow[d, "f^{\top\top}"] \\ W \arrow[r, "\mathrm{ev}_W"] & W^{\top\top} \end{tikzcd}$$

In Worten ausgedrückt gilt mithin die Identität $\mathrm{ev}_W \circ f = f^{\top\top} \circ \mathrm{ev}_V$ von Abbildungen $V \to W^{\top\top}$. Um das zu sehen, muß man nur für alle $v \in V$ die Identität $f^{\top\top}(\mathrm{ev}_V(v)) = \mathrm{ev}_W(f(v))$ 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

$$(f^{\top\top}(\mathrm{ev}_V(v)))(\lambda) = (\mathrm{ev}_W(f(v)))(\lambda)$$

alias $((\mathrm{ev}_V\, v) \circ f^{\top})(\lambda) = \lambda(f(v))$ alias $(\mathrm{ev}_V\, v)(\lambda \circ f) = \lambda(f(v))$. Das ist jedoch klar.

3.7.27 (**Diskussion der Terminologie**). Meines Erachtens ist es diese letzte Erkenntnis 3.7.26, 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 [LA2] 8.3.6 mit der dort eingeführten

Begrifflichkeit die obige Erkenntnis dahingehend aussprechen können, daß für jeden Körper K die Evaluationsabbildungen eine „Isotransformation des Identitätsfunktors auf der Kategorie der endlichdimensionalen K-Vektorräume zum Bidualraumfunktor“ bilden.

3.7.28. 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 3.7.29. Seien K ein Körper und V ein K-Vektorraum. Eine endliche Familie von Linearformen $f_1, \ldots, f_n \in V^\top$ ist linear unabhängig genau dann, wenn sie eine Surjektion $(f_1, \ldots, f_n) : V \twoheadrightarrow K^n$ liefert.

Übung 3.7.30. Gegeben Vektorräume V, W liefern die transponierten Abbildungen zu den kanonischen Injektionen nach 2.1.8 auf den Dualräumen einen Isomorphismus $(\mathrm{in}_V^\top, \mathrm{in}_W^\top) : (V \oplus W)^\top \xrightarrow{\sim} V^\top \oplus W^\top$. Analoges gilt für allgemeinere endliche Summen.

Übung 3.7.31. 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 $\mathrm{ev}_V : V \xrightarrow{\sim} V^{\top\top}$ jede Basis B ihrer Bidualen entspricht, in Formeln

$$\mathrm{ev}_V(b) = (b^\top)^\top \quad \forall b \in B$$

Ergänzende Übung 3.7.32. Man zeige: Gegeben ein Vektorraum V ist die Verknüpfung

$$V^\top \xrightarrow{\mathrm{ev}_{V^\top}} V^{\top\top\top} \xrightarrow{\mathrm{ev}_V^\top} V^\top$$

der Auswertungsabbildung zum Dualraum von V mit der Transponierten der Auswertungsabbildung von V die Identität auf dem Dualraum von V. Hinweis: [GR] 2.3.46 mag helfen. Vom höheren Standpunkt [TF] 4.4.10 hängt das damit zusammen, daß „der Dualraumfunktor sein eigener Adjungierter ist“.

Übung 3.7.33. Sei K ein Körper. Wir erhalten Isomorphismen $\mathrm{Mat}(n \times m; K) \xrightarrow{\sim} \mathrm{Mat}(m \times n; K)^\top$ durch die Vorschrift $A \mapsto (B \mapsto \mathrm{tr}(AB))$.

4 Zahlen

4.1 Der Körper der komplexen Zahlen

4.1.1. Viele mathematische Zusammenhänge werden bei einer Behandlung im Rahmen der sogenannten „komplexen Zahlen" besonders transparent. Ich denke hier etwa an die Integration rationaler Funktionen [AN1] 4.10, die Normalform orthogonaler Matrizen [LA2] 1.8.3 oder die Lösung der Schwingungsgleichung [AN1] 9.3.1. 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 den abstrakten Begriff eines Körpers [GR] 3.4.2. 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.

4.1.2. 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 [AN1] 3.4. Die hier gegebene Konstruktion der komplexen Zahlen als Menge aller Matrizen zu Drehstreckungen der Ebene paßt unter didaktischen Aspekten ganz gut, weil gleichzeitig der Zusammenhang zwischen Matrizen und linearen Abbildungen angewandt und eingeübt werden kann.

Satz 4.1.3 (**Charakterisierung der komplexen Zahlen**).

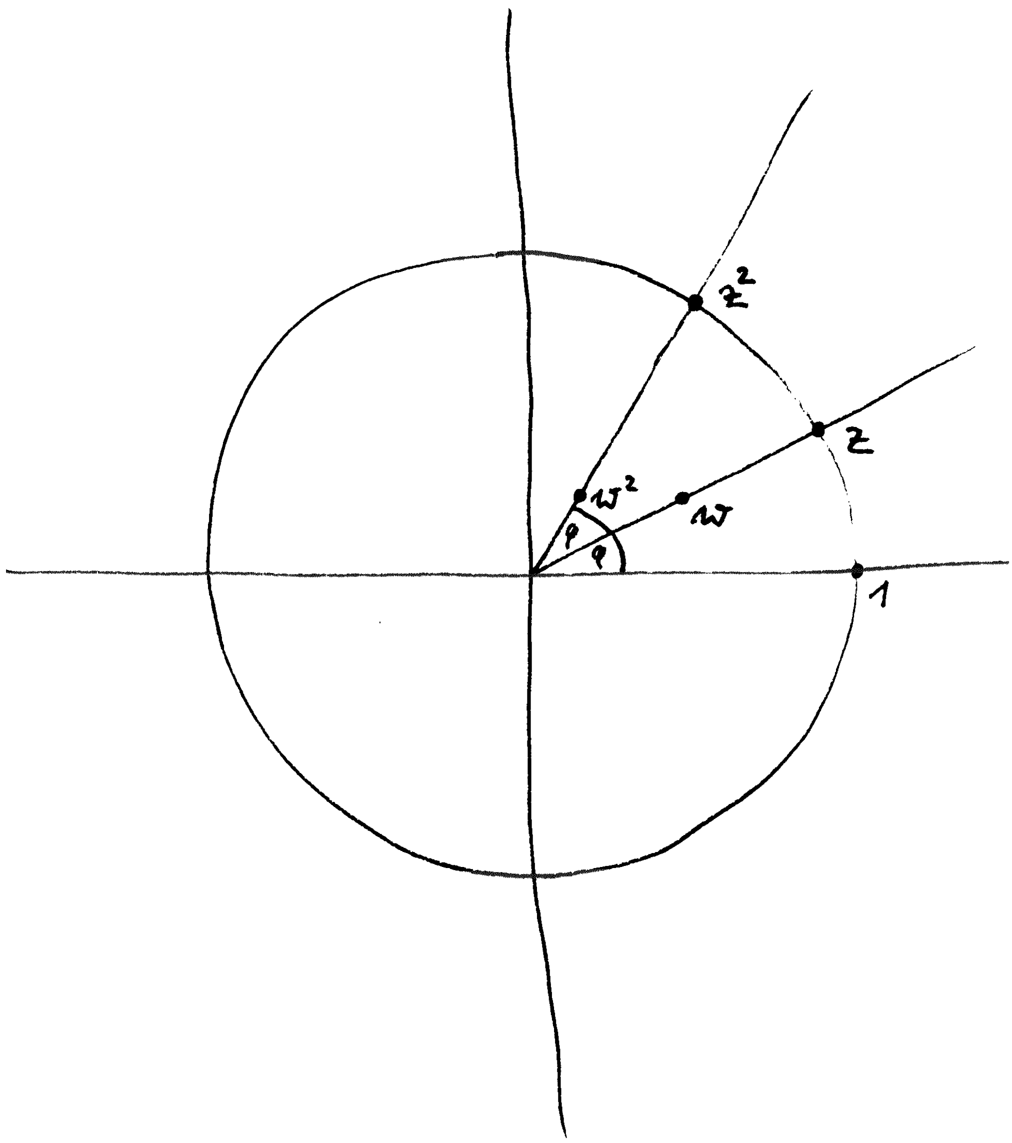
1. *Es gibt Tripel*

$$(\mathbb{C}, \mathrm{i}, \kappa)$$

bestehend aus einem Körper $\mathbb{C}$*, einem Element* $\mathrm{i} \in \mathbb{C}$ *und einem Körperhomomorphismus* $\kappa : \mathbb{R} \to \mathbb{C}$ *derart, daß gilt* $\mathrm{i}^2 = -1$ *und daß* i *und* 1 *eine* $\mathbb{R}$*-Basis von* $\mathbb{C}$ *bilden, für die durch* $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$*,* $(a, z) \mapsto \kappa(a)z$ *auf* $\mathbb{C}$ *gegebene Struktur als* $\mathbb{R}$*-Vektorraum;*

2. *Derartige Tripel sind im Wesentlichen eindeutig bestimmt. Ist genauer gesagt* $(\mathbb{C}', \mathrm{i}', \kappa')$ *ein weiteres derartiges Tripel, so gibt es genau einen Körperisomorphismus* $\varphi : \mathbb{C} \xrightarrow{\sim} \mathbb{C}'$ *mit* $\varphi : \mathrm{i} \mapsto \mathrm{i}'$ *und* $\varphi \circ \kappa = \kappa'$*.*

Definition 4.1.4. Wir wählen für den weiteren Verlauf der Vorlesung ein festes Tripel $(\mathbb{C}, \mathrm{i}, \kappa)$ der im Satz beschriebenen Art. Wegen der im zweiten Teil des Satzes formulierten „Eindeutigkeit bis auf eindeutigen Isomorphismus" erlauben



Anschauung für das Quadrieren komplexer Zahlen in ihrer anschaulichen Interpretation als Punkte der komplexen Zahlenebene wir uns weiter 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 vermittels κ als Teilmenge von $\mathbb{C}$ aufzufassen.

Ergänzung 4.1.5 (**Zur Eindeutigkeit der komplexen Zahlen**). Man beachte, daß $\mathbb{C}$ als Körper ohne weitere Daten keineswegs eindeutig ist bis auf eindeutigen Isomorphismus, in krassem Gegensatz zum Körper der reellen Zahlen [AN1] 1.5.18. Genauer gibt es überabzählbar viele Körperisomorphismen $\mathbb{C} \xrightarrow{\sim} \mathbb{C}$ und auch überabzählbar viele nicht-bijektive Körperhomomorphismen $\mathbb{C} \to \mathbb{C}$ und auch überabzählbar viele Körperhomomorphismen $\mathbb{R} \to \mathbb{C}$, wie etwa in [KAG] 4.5.15 ausgeführt wird. Zeichnet man jedoch einen Körperhomomorphismus $\kappa : \mathbb{R} \to \mathbb{C}$ 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 [AN1] 7.4.14, so wird κ seinerseits durch diese Topologie festgelegt als der einzige im Sinne von [AN1] 6.6.6 „stetige“ Körperhomomorphismen $\mathbb{R} \to \mathbb{C}$, und es gibt in Bezug auf unsere Topologie nur genau zwei „stetige“ Körperhomomorphismen $\mathbb{C} \to \mathbb{C}$, die Identität und die sogenannte „komplexe Konjugation“, die wir bald kennenlernen werden.

4.1.6. Ich hoffe, Sie werden bald merken, daß viele Fragestellungen sich bei Verwendung dieser sogenannt 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 4.1.7. Für feinere Untersuchungen finde ich es praktisch, auch Paare (K, κ) zu betrachten, die aus einem Körper K nebst einem Körperhomomorphismus $\kappa : \mathbb{R} \to K$ 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 **vergeßlichen 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 $z = a + b\,\mathrm{i}$ mit $a, b \in \mathbb{R}$. Die Addition und Multiplikation in $\mathbb{C}$ haben in dieser Notation die Gestalt

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

und 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 [GR] 3.4.14 durchgeführt haben. Alternativ kann man die im ersten Teil behauptete Existenz mit mehr Kenntnissen in linearer Algebra und weniger Rechnung auch wie folgt einsehen: Man betrachte die Menge $\mathbb{C}$ aller reellen (2×2)-Matrizen der Gestalt

$$\mathbb{C} := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\} \subset \mathrm{Mat}(2; \mathbb{R})$$

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 [GR] 3.4.2 und erhält so einen Körper $\mathbb{C}$. Die Drehung um einen rechten Winkel oder vielmehr ihre Matrix

$$\mathrm{i} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

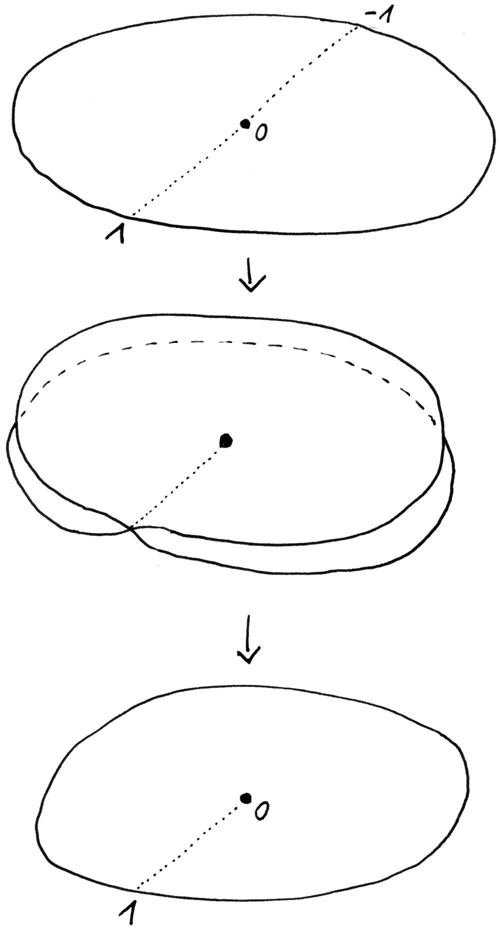
hat natürlich die Eigenschaft $\mathrm{i}^2 = -1$, und die Abbildung $\kappa : \mathbb{R} \to \mathbb{C}$ gegeben durch $\kappa : a \mapsto \mathrm{diag}(a, a)$ ist ein Körperhomomorphismus derart, daß das Tripel $(\mathbb{C}, \mathrm{i}, \kappa)$ die geforderten Eigenschaften besitzt. □

4.1.8. Es ist allgemein üblich, komplexe Zahlen mit z zu bezeichnen und als $z = x + y\,\mathrm{i}$ zu schreiben mit $x, y \in \mathbb{R}$. Man mag sich die komplexe Zahl $z = x + y\,\mathrm{i}$ 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 $(w+) : \mathbb{C} \to \mathbb{C}$, $z \mapsto w + z$ anschaulich die Verschiebung um den Vektor w. Die Multiplikationsabbildung $(w\cdot) : \mathbb{C} \to \mathbb{C}$, $z \mapsto wz$ dahingegen bedeutet anschaulich diejenige Drehstreckung, die $(1, 0)$ in w überführt.

4.1.9. Gegeben eine komplexe Zahl $z = x + y\,\mathrm{i}$ nennt man x ihren **Realteil** $\mathrm{Re}\, z := x$ und y ihren **Imaginärteil** $\mathrm{Im}\, z := y$. Wir haben damit zwei Funktionen

$$\mathrm{Re}, \mathrm{Im} : \mathbb{C} \to \mathbb{R}$$

definiert und es gilt $z = \mathrm{Re}\, z + \mathrm{i}\, \mathrm{Im}\, z$ für alle $z \in \mathbb{C}$. Man definiert weiter die **Norm** $|z|$ einer komplexen Zahl $z = x + y\,\mathrm{i} \in \mathbb{C}$ 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 [AN1] 1.4.5, in Formeln $|x| = |x|$. In der Anschauung der komplexen Zahlenebene bedeutet die Norm einer komplexen Zahl ihren Abstand vom Ursprung.



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 ε, 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.

4.1.10 (**Diskussion der Terminologie**). Bei rechtem Lichte besehen scheint mir an dieser Terminologie absonderlich, daß der Imaginärteil einer komplexen Zahl damit eine reelle Zahl ist, aber so hat es sich nun einmal eingebürgert.

4.1.11. 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 $z = x + y\,\mathrm{i} \in \mathbb{C}$ die **konjugierte komplexe Zahl** $\bar{z} = x - y\,\mathrm{i} \in \mathbb{C}$ einführt. Im Bild der komplexen Zahlenebene bedeutet das komplexe Konjugieren anschaulich die Spiegelung an der reellen Achse. Nun prüft man durch explizite Rechnung unschwer die Formeln

$$\begin{array}{rcl} \overline{z+w} & = & \bar{z} + \bar{w} \\ \overline{z \cdot w} & = & \bar{z} \cdot \bar{w} \\ |z|^2 & = & z\bar{z} \end{array}$$

Dann rechnet man einfach

$$|zw|^2 = zw\overline{zw} = z\bar{z}w\bar{w} = |z|^2|w|^2$$

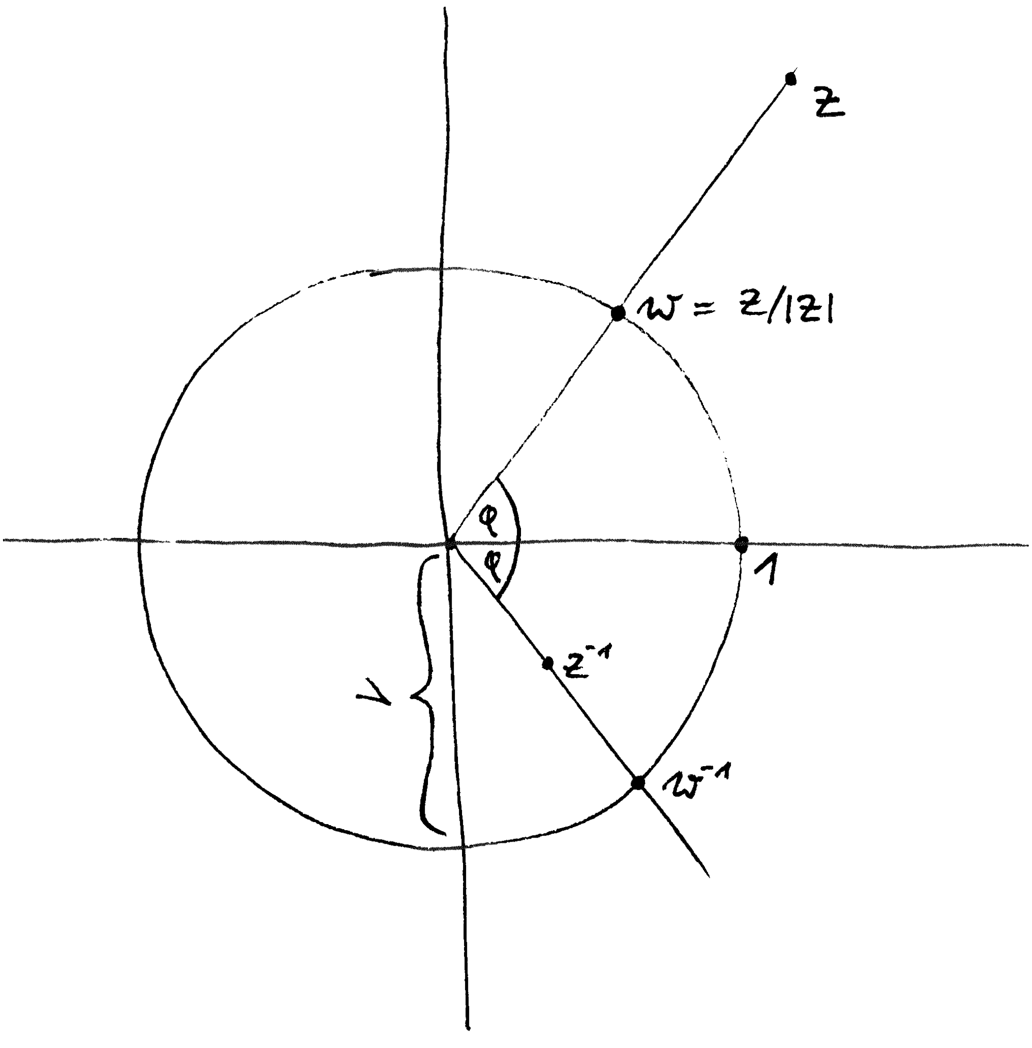
In der Terminologie aus [GR] 3.4.13 ist $z \mapsto \bar{z}$ ein Körperisomorphismus $\mathbb{C} \to \mathbb{C}$. Offensichtlich gilt auch $\bar{\bar{z}} = z$ und ebenso offensichtlich gilt $|z| = |\bar{z}|$.

4.1.12. 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 $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ definieren. Deren Gleichheit kann nach 2.3.9 auf Basen geprüft werden. Es reicht also, sie für $z, w \in \{1, \mathrm{i}\}$ nachzuweisen, und das ist schnell getan.

4.1.13. Wir können den Realteil und den Imaginärteil von $z \in \mathbb{C}$ mithilfe der konjugierten komplexen Zahl ausdrücken als

$$\operatorname{Re} z = \frac{z + \bar{z}}{2} \qquad \operatorname{Im} z = \frac{z - \bar{z}}{2\,\mathrm{i}}$$

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**.



Anschauung für das Invertieren komplexer Zahlen

4.1.14. Für unsere Norm komplexer Zahlen aus 4.1.9 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**

$$|z + w| \leq |z| + |w|$$

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 4.1.15. 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 [AN1] 3.4.

Übungen

Übung 4.1.16. Man bestimme Real- und Imaginärteil einer Quadratwurzel von i. Man bestimme Real- und Imaginärteil einer Quadratwurzel von $1 + \mathrm{i}$.

Übung 4.1.17. Gegeben eine von Null verschiedene komplexe Zahl $z = x + \mathrm{i}\,y$ 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 4.1.18. Gegeben eine komplexe Zahl $z \neq -1$ vom Betrag $|z| = 1$ zeige man, daß sie genau eine Wurzel w mit positivem Realteil hat und daß diese gegeben wird durch $w = a/|a|$ für $a = (1 + z)/2$. Können Sie auch die geometrische Bedeutung dieser Formel erklären? Man folgere, daß gegeben $\varepsilon > 0$ beliebig jedes Element von S^1 eine Potenz eines Elements z mit Realteil $\operatorname{Re}(z) > 1 - \varepsilon$ ist.

Übung 4.1.19. 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 ∞. 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.

4.2 Konstruktion der natürlichen Zahlen*

4.2.1. 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 Mengenlehre, wir nennen es das **Unendlichkeitsaxiom**.

4.2.2. 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 die Vereinigung einer endlichen Menge mit einer einelementigen Menge wieder endlich ist.

Ergänzung 4.2.3 (**Maximale Elemente endlicher Mengen**). Jede nichtleere endliche partiell geordnete Menge $(E, \leq)$ besitzt mindestens ein maximales Element. Es könnte gut sein, daß wir diese Erkenntnis bereits als intuitiv klar verwendet haben, aber das war noch vor der Formalisierung des Begriffs einer endlichen Menge. Formal können wir durch Widerspruch argumentieren. In der Tat könnten wir andernfalls eine Abbildung $f : E \to E$ finden, die jedem Element ein echt größeres Element zuordnet. Halten wir dann $a \in E$ fest, so erhielten wir eine injektive aber nicht surjektive Abbildung von $\{x \in E \mid x \geq a\}$ zu sich selbst, und dieser Widerspruch zeigt die Behauptung.

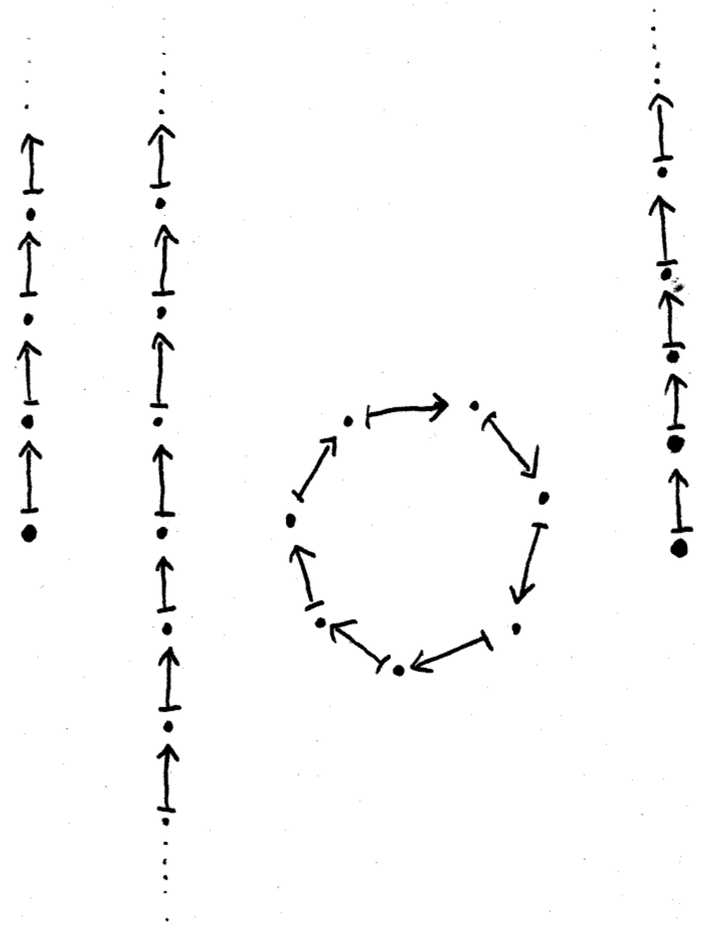
Satz 4.2.4 (**Die natürlichen Zahlen**).

1. *Es gibt ein Paar (N, S) bestehend aus einer Menge N und einer injektiven aber nicht surjektiven Abbildung $S : N \hookrightarrow N$ derart, daß jede S-stabile Teilmenge $M \subset N$, die nicht im Bild von S enthalten ist, bereits ganz N sein muß. In Formeln fordern wir für Teilmengen $M \subset N$ also $(S(M) \subset M \not\subset S(N)) \Rightarrow M = N$;*

2. *Für solch ein Paar (N, S) gibt es genau ein Element $o \in N$, das nicht im Bild von S liegt. Ist dann (X, x, f) ein beliebiges Tripel bestehend aus einer Menge X, einem Element $x \in X$ und einer Abbildung $f : X \to X$, so gibt es genau eine Abbildung $\psi : N \to X$ mit $\psi(o) = x$ und $\psi S = f\psi$;*

3. *Ein Paar (N, S) wie im ersten Teil ist im Wesentlichen eindeutig bestimmt. Ist präziser (N', S') ein weiteres derartiges Paar, so gibt es genau eine Bijektion $\varphi : N \xrightarrow{\sim} N'$ mit $S'\varphi = \varphi S$.*

4.2.5. 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“. Weiter verwenden wir für das eindeutig bestimmte Element o aus Teil 2, das kein Nachfolger ist, die Notation



Versuch der graphischen Darstellung einer Menge N mit einer injektiven aber nicht surjektiven Abbildung S in sich selbst. Ich hoffe, daß so anschaulich wird, warum unter den beiden zusätzlichen Voraussetzungen (1) „S nicht surjektiv“ und (2) „jede S-stabile Teilmenge $M \subset N$, die nicht im Bild von S enthalten ist, ist bereits ganz N“ jede mögliche Lösung wie der Strang ganz rechts aussehen muß.

0 und die Bezeichnung **Null** und für die Werte der Abbildung ψ aus Teil 2 die Notation $f^n(x) := \psi(n)$. Wir nennen f^n das **n-fach iterierte Anwenden von f**.

4.2.6. 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 [AL] 5.2.2.

Beweis. 1. Nach dem Unendlichkeitsaxiom 4.2.1 finden wir eine Menge A nebst einer injektiven Abbildung $S : A \to A$ und einem Element $o \in A \backslash S(A)$. 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, und damit $N = \{o\} \cup S(N)$, da die andere Inklusion eh klar ist. Für jede echte Teilmenge $M \subsetneq N$ mit $S(M) \subset M$ folgt nun erst $o \notin M$ und dann $M \subset S(N)$. Damit haben wir bereits ein mögliches Paar (N, S) gefunden.

2. Daß bei einem derartigen Paar das Komplement $N \backslash S(N)$ genau aus einem einzigen Punkt bestehen muß, scheint mir offensichtlich. Gegeben (X, x, f) wie oben betrachten wir nun zunächst 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 Γ 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 Γ entfernen, im Widerspruch zur Minimalität von Γ. Ist ähnlich $m \in M$, so zeigen wir in derselben Weise $S(m) \in M$. Also gilt $M = N$ und Γ ist der Graph einer Funktion $f : N \to X$ mit den gewünschten Eigenschaften. Finden wir eine weitere Funktion mit den gewünschten Eigenschaften, so ist deren Graph auch ein mögliches G und wir folgern erst $G \supset \Gamma$ und dann $G = \Gamma$.

3. Gegeben ein zweites Paar (N', S') wie in Teil 1 gibt es auch genau ein Element $o' \in N'$, das nicht im Bild von S' liegt. Für jede Bijektion $\varphi : N \xrightarrow{\sim} N'$ mit $S'\varphi = \varphi S$ gilt also $\varphi : o \mapsto o'$ und damit folgt die Eindeutigkeit unserer Bijektion aus Teil 2. Andererseits folgt aus Teil 2 auch die Existenz einer Abbildung $\psi : N \to N'$ mit $S'\psi = \psi S$ und $\psi : o \mapsto o'$, und wir haben gewonnen, wenn wir zeigen können, daß ψ eine Bijektion ist. Wieder nach Teil 2 gibt es aber auch eine Abbildung $\phi : N' \to N$ mit $S\phi = \phi S'$ und $\phi : o' \mapsto o$. Nocheinmal nach Teil 2, diesmal der Eindeutigkeitsaussage, gilt $\psi\phi = \mathrm{id}$ und $\phi\psi = \mathrm{id}$. Also ist unser ψ in der Tat eine Bijektion. □

4.2.7. Gegeben eine Menge X und zwei Abbildungen $\psi, \phi : \mathbb{N} \to X$ mit $\psi(0) = \phi(0)$ und $(\psi(b) = \phi(b)) \Rightarrow (\psi(Sb) = \phi(Sb))$ folgt $\psi = \phi$. Diese Umformulierung der Eindeutigkeitsaussage aus 4.2.4 heißt auch das **Prinzip der vollständigen Induktion**.

Satz 4.2.8 (Addition natürlicher Zahlen). *Für die Menge der natürlichen Zahlen mit Nachfolgerabbildung* $(\mathbb{N}, S)$ *aus 4.2.5 gilt:*

1. *Es gibt genau eine Verknüpfung* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a, b) \mapsto a + b$ *mit der Eigenschaft* $0 + b = b$ *und* $Sa + b = S(a + b)$ *für alle* $a, b \in \mathbb{N}$. *Wir nennen sie die* **Addition***;*

2. *Gegeben eine Menge* X, *eine Abbildung* $f : X \to X$ *und ein Element* $x \in X$ *gilt für alle* $m, n \in \mathbb{N}$ *die Identität* $f^n(f^m(x)) = f^{n+m}(x)$*;*

3. *Unsere Verknüpfung* $+$ *auf* $\mathbb{N}$ *ist kommutativ;*

4. *Mit der Verknüpfung* $+$ *wird* $\mathbb{N}$ *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. 1. Um die Existenz und Eindeutigkeit unserer Verknüpfung zu zeigen, wenden wir 4.2.4 an auf $(X, x, f) = (\mathbb{N}, b, S)$. In der Notation aus 4.2.5 können und müssen wir also unsere Verknüpfung erklären durch die Formel $a + b := S^a(b)$.

2. Das folgt leicht durch Induktion über n.

3. Zunächst zeigen wir $a + 0 = a$ mit vollständiger Induktion über a. Ebenso folgern wir $a + Sb = S(a + b)$ mit vollständiger Induktion über a, denn für $a = 0$ ist die Aussage klar und wir haben $Sa + Sb = S(a + Sb) = S(S(a + b)) = S(Sa + b)$ nach der Definition der Addition für die erste und letzte Gleichung und Induktionsannahme für die mittlere Gleichung. Jetzt folgt $a + b = b + a$ mit vollständiger Induktion über a. Für $a = 0$ haben wir das schon gezeigt, und dann finden wir mit unseren Vorüberlegungen $Sa + b = S(a + b) = S(b + a) = b + Sa$.

4. Die Assoziativität $(a + b) + c = a + (b + c)$ ist äquivalent zur Behauptung $S^{a+b}(c) = S^a(S^b(c))$ und folgt damit aus dem zweiten Teil. 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 $(a+) : \mathbb{N} \to \mathbb{N}$ liegt, und dann folgt auch $b = 0$ nach der Kürzungsregel. $\square$

4.2.9 (**Iterierte Verknüpfung**). Gegeben ein Magma $(M, \top)$ und Elemente $a, b \in M$ und $n \in \mathbb{N}$ können wir durch iteriertes Anwenden $(a\top)^n b$ bilden und es folgt $(a\top)^n((a\top)^m b) = (a\top)^{n+m} b$. Ist unser Magma ein Monoid, so setzen wir $n^\top a := (a\top)^n e_M$ und folgern erst induktiv $(a\top)^n(b) = (n^\top a)\top b$ für alle n und dann $(n + m)^\top a = (n^\top a)\top(m^\top a)$ für alle m, n.

Satz 4.2.10 (Anordnung auf den natürlichen Zahlen). *Sei* $(\mathbb{N}, S)$ *die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus* 4.2.5 *und Addition aus* 4.2.8*. 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 4.2.8 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 $A = \emptyset$. □

Satz 4.2.11 (Multiplikation natürlicher Zahlen). *Sei* $(\mathbb{N}, S)$ *die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus* 4.2.5 *und bezeichne* $+$ *ihre Addition aus* 4.2.8*. Mit der durch iterierte Addition gegebenen Verknüpfung* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$*,* $(n, b) \mapsto nb = n \cdot b := n^{+}b$ *wird* $\mathbb{N}$ *ein kommutatives Monoid mit neutralem Element* $1 := S0$ *und es gilt das Distributivgesetz* $a(b + c) = ab + ac$ *für alle* $a, b, c \in \mathbb{N}$*.*

4.2.12. Diese Verknüpfung heißt die **Multiplikation** von natürlichen Zahlen.

Beweis. Übung. □

Satz 4.2.13 (Iteriertes Anwenden und Multiplikation). *Gegeben eine Menge* X*, eine Abbildung* $f : X \to X$ *und ein Element* $x \in X$ *gilt für alle* $m, n \in \mathbb{N}$ *die Identität*

$$(f^n)^m(x) = f^{nm}(x)$$

Beweis. Vollständige Induktion über m. □

Satz 4.2.14 (Teilen mit Rest). *Sei* $(\mathbb{N}, S)$ *die Menge der natürlichen Zahlen mit Nachfolgerabbildung und Addition, Multiplikation und Anordnung wie in* 4.2.11 *und* 4.2.10*. 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. □

Satz 4.2.15 (Potenzieren natürlicher Zahlen). *Sei* $(\mathbb{N}, S)$ *die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus* 4.2.5 *und ihrer Addition aus* 4.2.8 *und Multiplikation aus* 4.2.11*. So gelten für die durch iterierte Multiplikation erklärte Verknüpfung* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$*,* $(a, b) \mapsto a^b := b^{\times}a$ *die Regeln* $a^{b+c} = a^b a^c$ *und* $(ab)^c = a^c b^c$ *und* $a^{bc} = (a^b)^c$ *für alle* $a, b, c \in \mathbb{N}$*.*

Beweis. Übung. $\square$

4.2.16. 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 $a_0, a_1, \ldots, a_r \in \{0, 1, \ldots, 9\}$ die **Dezimaldarstellung**

$$a_r \ldots a_1 a_0 = a_r z^r + \ldots + a_1 z^1 + a_0 z^0$$

So erhalten wir insbesondere für unsere natürliche Zahl Zehn die Dezimaldarstellung $z = 10 = 1z^1 + 0z^0$. 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.

4.2.17 (**Zahldarstellungen**). Gegeben eine beliebige natürliche Zahl $b > 1$ hat jede natürliche Zahl n genau eine Darstellung der Form

$$n = a_r b^r + \ldots + a_1 b^1 + a_0 b^0$$

mit $a_0, a_1, \ldots, a_r \in \{0, 1, \ldots, b-1\}$ 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 $a_r \ldots a_0$ als Darstellung der Zahl n interpretieren. Wir sagen dann auch, sie **stelle n im b-adischen System dar**. Das 10-adische Sytem heißt das **Dezimalsystem** und man spricht dann auch von der **Dezimaldarstellung** einer natürlichen Zahl. Bei $b \leq 10$ wählt man als Ziffern meist die ersten b üblichen Ziffern des Dezimalsystems. Das 2-adische Sytem heißt das **Dualsystem** und man spricht dann auch von der **Binärdarstellung** einer natürlichen Zahl. So wäre 1010 die Darstellung im Dualsystem der Zahl, die im Dezimalsystem $2^3 + 2^1 = 10$ geschrieben würde und die wir Zehn nennen. Gebräuchlich sind auch Darstellungen im 16-adischen Sytem alias **Hexadezimalsystem** mit den Ziffern $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}$. Etwa wäre FF die Darstellung im Hexadezimalsystem der Zahl, die im Dezimalsystem $15 \cdot 16 + 15 = 16^2 - 1 = 255$ geschrieben würde.

Übungen

Übung 4.2.18. Man zeige, daß gilt $S(a) \neq a$ für alle $a \in \mathbb{N}$.

Übung 4.2.19. Man führe die Beweise von Einigen der Sätze 4.2.11, 4.2.15, 4.2.10 und 4.2.14 aus.

Übung 4.2.20. 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 [AL] 5.2.3, obwohl wir es natürlich schon oft verwendet haben und weiter verwenden müssen. Der Beweis ist nicht schwer, aber alles zu seiner Zeit.

Übung 4.2.21. Gegeben eine endliche Menge X und eine Abbildung $f : X \to X$ 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 $f : X \to X$ eine Abbildung, so gibt es $y \in X$ und $r \geq 1$ mit $f^r(y) = y$.

Übung 4.2.22. Gegeben eine Menge X und eine Abbildung $f : \mathbb{N} \times X \to X$ und ein Element $a \in X$ gibt es genau eine Folge $\mathbb{N} \to X$, $n \mapsto x_n$ mit $x_0 = a$ und $x_{n+1} = f(n, x_n)\ \forall n \in \mathbb{N}$.

4.3 Untergruppen der Gruppe der ganzen Zahlen

Definition 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 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 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 $\mathrm{Aut}(V) \subset \mathrm{Ens}^\times(V)$ der Gruppe aller Permutationen der zugrundeliegenden Menge.

Satz 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*

$$\mathbb{N} \xrightarrow{\sim} \{H \subset \mathbb{Z} \mid H \textit{ ist Untergruppe von } \mathbb{Z}\}$$

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. □

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 $\langle a_1, \ldots, a_n \rangle$ statt $\langle \{a_1, \ldots, a_n\} \rangle$. 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 einzigem 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.

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 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 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 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 4.3.10. Sei G eine Gruppe und $\varphi : G \to G$ ein Gruppenhomomorphismus. Man zeige: Gilt für ein $n \in \mathbb{N}$ die Geichheit $\ker \varphi^n = \ker \varphi^{n+1}$, so folgt $\ker \varphi^n = \ker \varphi^{n+1} = \ker \varphi^{n+2} = \ldots$

Übung 4.3.11. Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so gilt die Formel $|G| = |\operatorname{im} \varphi| \cdot |\ker \varphi|$. Man bemerke, daß diese Formel im Fall linearer Abbildungen von Vektorräumen über endlichen Körpern äquivalent ist zur Dimensionsformel.

4.4 Primfaktorzerlegung

Definition 4.4.1. Eine **Primzahl** ist eine natürliche Zahl ≥ 2, die sich nicht als das Produkt von zwei echt kleineren natürlichen Zahlen erhalten läßt.

Beispiel 4.4.2. Die Primzahlen unterhalb von 50 sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

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, d.h. 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" heißt auf lateinisch „Primus" und auf griechisch ähnlich und es könnte sein, daß die Bezeichnung „Primzahl" daher rührt.

Satz 4.4.4 (Existenz einer Primfaktorzerlegung). *Jede natürliche Zahl $n \geq 2$ kann als ein Produkt von Primzahlen $n = p_1 p_2 \ldots p_r$ dargestellt werden.*

4.4.5. Der Satz gilt in unserer Terminologie auch für die Zahl $n = 1$, die eben durch das „leere Produkt" mit $r = 0$ dargestellt wird. Ebenso gilt er für jede Primzahl p, die dabei als Produkt von einem Faktor mit $r = 1$ als $p = p_1$ zu verstehen ist.

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. □

Satz 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 4.4.4 eine Primfaktorzerlegung besitzen, aber keine unserer endlich vielen Primzahlen käme als Primfaktor in Frage. □

Ergänzung 4.4.7 ((2016)). Noch offen ist die Frage, ob es auch unendlich viele **Primzahlzwillinge** gibt, d.h. 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 ≤ 246 gibt.

Satz 4.4.8 (**Eindeutigkeit der Primfaktorzerlegung**). *Die Darstellung einer natürlichen Zahl $n \geq 1$ als ein Produkt von Primzahlen $n = p_1 p_2 \ldots p_r$ ist eindeutig bis auf die Reihenfolge der Faktoren. Nehmen wir zusätzlich $p_1 \leq p_2 \leq \ldots \leq p_r$ an, so ist unsere Darstellung mithin eindeutig.*

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 dazuzugehören, so wäre der vorhergehende Satz in dieser Formulierung falsch. In obigem Satz ist $r \geq 0$ zu verstehen, 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 4.4.15 endlich bewiesen werden kann. □

Definition 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 $a|b$ genau dann, wenn es $c \in \mathbb{Z}$ gibt mit $ac = b$.

Definition 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** genau dann, wenn sie außer ± 1 keine gemeinsamen Teiler besitzen. Insbesondere sind also $a = 0$ und $b = 0$ nicht teilerfremd.

Satz 4.4.12 (**über den größten gemeinsamen Teiler**). *Sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ nicht beide Null, so 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.

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 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. $(d$ teilt a und $b) \Rightarrow (d$ teilt $\hat{c})$.

Daraus folgt aber sofort, daß $\hat{c}$ der größte gemeinsame Teiler von a und b ist, und damit folgt dann der Satz. □

4.4.14 (**Notation für größte gemeinsame Teiler**). Gegeben $a_1, \ldots, a_n \in \mathbb{Z}$ können wir mit der Notation 4.3.5 kürzer schreiben

$$a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = \langle a_1, \ldots, a_n \rangle$$

Üblich ist hier auch die Notation $(a_1, \ldots, a_n)$, die jedoch oft auch n-Tupel von ganzen Zahlen bezeichnet, also Elemente von $\mathbb{Z}^n$, und in der Analysis im Fall $n = 2$ 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 4.4.15 (von Euklid). *Teilt eine Primzahl ein Produkt von zwei ganzen Zahlen, so teilt sie einen der Faktoren.*

4.4.16 (**Diskussion der Terminologie**). Dies Lemma findet sich bereits in Euklid's Elementen in Buch VII als Proposition 30.

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 [AL] 2.4.8 sehen, daß etwa in $\mathbb{Z}[\sqrt{-5}]$ 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 ± 1 und $\pm p$. Der größte gemeinsame Teiler von p und a kann aber nicht p sein und muß folglich 1 sein. Nach 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. □

Beweis der Eindeutigkeit der Primfaktorzerlegung 4.4.8. Zunächst sei bemerkt, daß aus Lemma 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 $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ 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. □

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 $5 = \operatorname{ggT}(10, 15)$ 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 $5 = \operatorname{ggT}(15, 145)$ 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 4.4.19 (**ABC-Vermutung**). Gegeben eine positive natürliche Zahl n bezeichne $\operatorname{rad}(n)$ 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

$$c > (\operatorname{rad}(abc))^{1+\varepsilon}$$

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 (2016) 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 $c \geq \operatorname{rad}(abc)$. Diese sind jedoch bereits vergleichsweise selten, so gibt es etwa nur 120 mögliche Tripel mit $c < 10000$.

Übungen

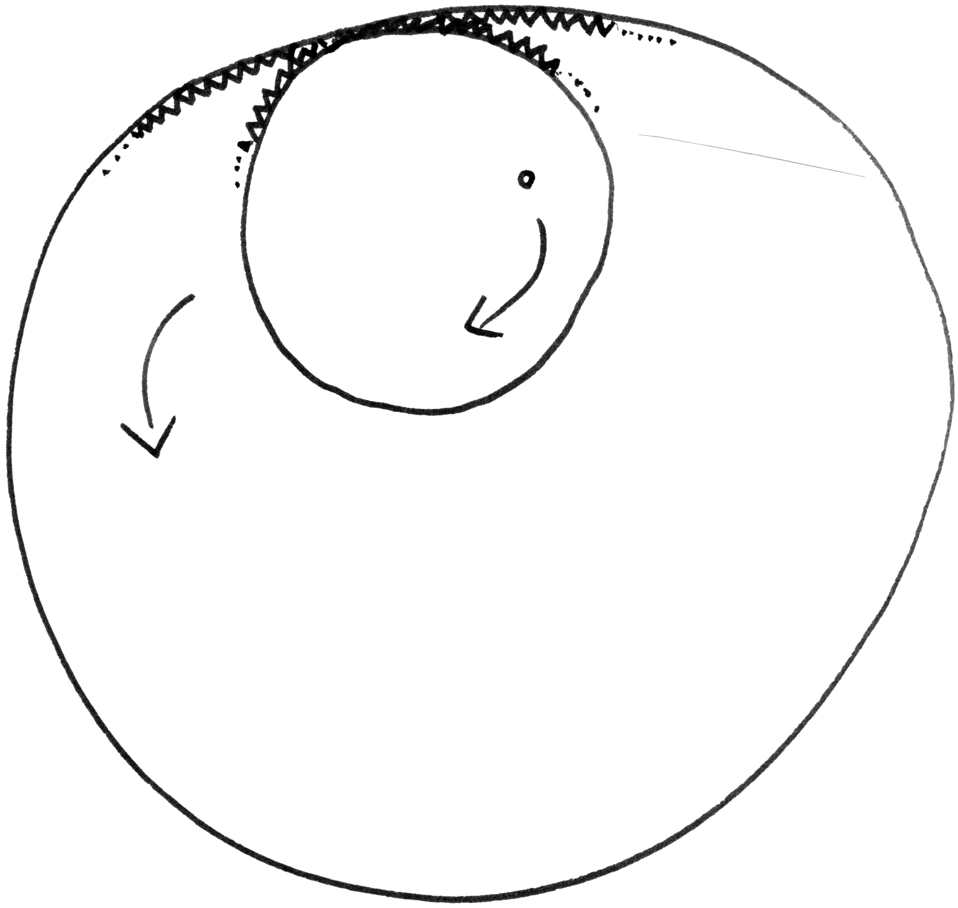
Übung 4.4.20. Man berechne den größten gemeinsamen Teiler von 3456 und 436 und eine Darstellung desselben als ganzzahlige Linearkombination unserer beiden Zahlen.

Übung 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 $\operatorname{kgV}(a, b)$. Man zeige in dieser Notation die Formel $\operatorname{kgV}(a, b) \operatorname{ggT}(a, b) = ab$.

Ergänzende Übung 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 man das Zahnrad auf dem inneren Zahnkranz umlaufen, bevor solch eine Figur fertig gemalt ist?

Ergänzende Übung 4.4.23. Berechnen Sie, wieviele verschiedene Strophen das schöne Lied hat, dessen erste Strophe lautet:

> Tomatensalat Tomatensala Tooo-
> -matensalat Tomatensaaaaaaaa-
> -lat Tomatensalat Tomatensalat
> Tomatensalat Tomatensaaaaaaa-



Der Spirograph aus Übung 4.4.22

5 Ringe und Polynome

5.1 Ringe

Definition 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 [GR] 3.1.17, 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 heißt, für alle $a, b, c \in R$ gilt

$$\begin{array}{rcl} a \cdot (b + c) & = & (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c & = & (a \cdot c) + (b \cdot c) \end{array}$$

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 [GR] 3.1.16. Ein Ring, dessen Multiplikation kommutativ ist, heißt ein **kommutativer Ring** und bei uns in unüblicher Verkürzung ein **Kring**.

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 in der Form $a(b + c) = ab + ac$ geschrieben werden kann.

Beispiel 5.1.3. Die ganzen Zahlen $\mathbb{Z}$ bilden mit der üblichen Multiplikation und Addition nach 5.5.10 einen kommutativen Ring.

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 geschlossenener Körperschaften verwendet. So gibt es etwa den „Ring deutscher Makler“ oder den „Ring deutscher Bergingenieure“.

5.1.5 (**Diskussion der Terminologie**). Eine Struktur wie in der vorhergehenden Definition, bei der nur die Existenz eines Einselements nicht gefordert wird, bezeichnen wir im Vorgriff auf [KAG] 1.9.7 als eine **assoziative $\mathbb{Z}$-Algebra** oder kurz **$\mathbb{Z}$-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 5.1.6. Allgemeiner als in 3.5.15 erklärt heißt 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 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 $\mathrm{Ens}(X, R)$ 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 $\mathrm{Mat}(n; R)$ 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

$$\mathrm{End}\, A$$

und nennt ihn den **Endomorphismenring der abelschen Gruppe** A. Ähnlich bilden auch die Endomorphismen eines Vektorraums V über einem Körper k einen Ring $\mathrm{End}_k V$, den sogenannten **Endomorphismenring von** V. Oft notiert man auch den Endomorphismenring eines Vektorraums abkürzend $\mathrm{End}\, V$ 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 $\mathrm{End}_{\mathbb{Z}} A$ aus Gründen, die erst in [KAG] 1.3.3 erklärt werden. Ich verwende für diesen Ring zur Vermeidung von Indizes lieber die Notation $\mathrm{End}_{\mathbb{Z}} A = \mathrm{Ab}\, A$, die sich aus den allgemeinen kategorientheoretischen Konventionen [LA2] 8.1.5 ergibt.

Definition 5.1.8. Eine Abbildung $\varphi : R \to S$ 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

$$\mathrm{Ring}(R, S)$$

Ergänzung 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 5.1.10. *Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$, in Formeln* $|\operatorname{Ring}(\mathbb{Z}, R)| = 1$.

Beweis. Nach [GR] 3.3.29 gibt es genau einen Gruppenhomomorphismus von additiven Gruppen $\varphi : \mathbb{Z} \to R$, 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 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. □

5.1.11 (**Ganze Zahlen und allgemeine Ringe**). Gegeben ein Ring R notieren wir den Ringhomomorphismus $\mathbb{Z} \to R$ aus 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 $nr = n_R r = r n_R$, wobei nr in Bezug auf die Struktur von R als additive abelsche Gruppe verstehen, also $nr = n^+ r = r + r \ldots + r$ mit n Summanden falls $n \geq 1$ und so weiter, wie in der Tabelle [GR] 3.2.12 und in [GR] 3.2.10 ausgeführt wird. Unsere Gleichung $nr = n_R r = r n_R$ bedeutet dann hinwiederum, daß es auf den Unterschied zwischen n_R und n meist gar nicht ankommt. Deshalb führt es auch selten zu Mißvertändnissen, wenn wir statt n_R nur kurz n schreiben.

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 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 [GR] 3.3.26, ist Q mit der koinduzierten Addition und Multiplikation auch wieder ein Ring.

Ergänzende Übung 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 5.1.15. Man zeige, daß in jedem Ring R gilt $0a = 0 \quad \forall a \in R$; $-a = (-1)a \quad \forall a \in R$; $(-1)(-1) = 1$; $(-a)(-b) = ab \quad \forall a, b \in R$.

Übung 5.1.16. Gegeben eine Überdeckung einer endlichen Menge X durch Teilmengen $X = X_1 \cup \ldots \cup X_n$ zeige man die **Einschluß-Ausschluß-Formel**

$$0 = \sum_{I \subset \{1,\ldots,n\}} (-1)^{|I|} \left|\bigcap\nolimits_{i \in I} X_i\right|$$

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 χ_i bezeichnen und im Ring der $\mathbb{Z}$-wertigen Funktionen auf X das Produkt $(1-\chi_1)\ldots(1-\chi_n)$ ausmultiplizieren.

5.2 Restklassenringe des Rings der ganzen Zahlen

Definition 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 **Repräsentantensystem** für die Menge der Linksnebenklassen.

Vorschau 5.2.2. Diese Konstruktion wird in [LA2] 5.1.2 noch sehr viel ausführlicher diskutiert werden.

Beispiel 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

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

Da in dieser Aufzählung keine Nebenklassen mehrfach genannt werden, ist die Teilmenge $\{0, 1, \ldots, m-1\}$ also ein Repräsentantensystem für die Menge von Nebenklassen $\mathbb{Z}/m\mathbb{Z}$. Ein anderes Repräsentantensystem wäre $\{1, \ldots, m\}$, ein Drittes $\{1, \ldots, m-1, 7m\}$.

Satz 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 $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ mit $a \mapsto \bar{a}$ ein Ringhomomorphismus ist.*

5.2.5. Das ist dann natürlich die Struktur als Quotientenring im Sinne unserer Übung 5.1.13.

Beweis. Daß es höchstens eine derartige Ringstruktur gibt, es eh klar. Zu zeigen bleibt nur deren Existenz. Nach [GR] 3.1.3 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 5.1.13. □

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 5.1.11 eh schon vereinbart hatten.

Beispiel 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 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 $\{\bar{0}, \bar{1}, \ldots, \overline{11}\}$ und wir haben $\overline{11} + \bar{5} = \overline{16} = \bar{4}$ alias „5 Stunden nach 11 Uhr ist es 4 Uhr". Weiter haben wir in $\mathbb{Z}/12\mathbb{Z}$ etwa auch $\bar{3} \cdot \bar{8} = \overline{24} = \bar{0}$. In einem Ring kann es also durchaus passieren, daß ein Produkt von zwei von Null verschiedenen Faktoren Null ist.

Vorschau 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 [FT1] 5.2.1, 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 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 definitionem 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. □

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.

Definition 5.2.12. 1. Gegeben ein Kring 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 $ad = b$;

2. Jedes Element eines Krings ist ein Teiler der Null. Ein Element a eines Rings R heißt ein **Nullteiler von** R, wenn es $d \in R\backslash 0$ gibt mit $ad = 0$ oder $da = 0$. Die Null ist insbesondere genau dann ein Nullteiler, wenn unser Ring nicht der Nullring ist;

3. Ein Ring heißt **nullteilerfrei**, wenn er außer der Null keine Nullteiler besitzt, wenn also das Produkt von je zwei von Null verschiedenen Elementen auch wieder von Null verschieden ist;

4. Ein Ring heißt ein **Integritätsbereich**, wenn er nullteilerfrei und außerdem nicht der Nullring ist.

5.2.13 (**Diskussion der Terminologie**). Manche Autoren fordern von nullteilerfreien Ringen zusätzlich, daß sie nicht der Nullring sein dürfen, benutzen also dieses Wort als Synonym für „Integritätsbereich“. Alle Elemente eines Krings teilen die Null. Deshalb ist es üblich, die Bezeichnung „Nullteiler“ wie in obiger Definition zu beschränken auf Elemente, die „die Null in nicht-trivialer Weise teilen“ in dem Sinne, daß sie eben von einem von Null verschiedenen Element zu Null multipliziert werden können. Daß damit auch die Null in jedem von Null verschiedenen Ring ein Nullteiler ist, nehmen wir in Kauf, um weitere Fallunterscheidungen zu vermeiden.

Beispiel 5.2.14. Die Nullteiler in $\mathbb{Z}/12\mathbb{Z}$ sind $0, 2, 3, 4, 6, 8, 9, 10$.

5.2.15 (**Kürzen in Ringen**). Sei R ein Ring. Ist $a \in R$ kein Nullteiler, so folgt aus $ax = ay$ schon $x = y$. In der Tat haben wir nämlich $ax = ay \;\Rightarrow\; a(x - y) = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$.

Definition 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 [GR] 3.2.2, 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 [GR] 3.2.12 mit $R^\times$ bezeichnet.

Beispiel 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 $\mathbb{Q}^\times = \mathbb{Q}\backslash 0$.

5.2.18. Eine Einheit eines Krings teilt alle Elemente unseres Krings und ist sogar dasselbe wie ein Teiler der Eins. Eine Einheit $a \in R^\times$ eines Rings R kann dahingegen nie ein Nullteiler sein, denn gibt es $x \in R$ mit $xa = 1$, so folgt aus $ac = 0$ bereits $xac = 1c = c = 0$.

Definition 5.2.19. Zwei Elemente eines Krings heißen **teilerfremd**, wenn sie außer Einheiten keine gemeinsamen Teiler haben.

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.

5.2.21 (**Nichtnullteiler endlicher Ringe**). In einem endlichen Ring R sind die Einheiten genau die Nichtnullteiler. In der Tat, ist $a \in R$ kein Nullteiler, so ist die Multiplikation mit a nach 5.2.15 eine Injektion $(a\cdot) : R \hookrightarrow R$. Ist aber R endlich, so muß sie auch eine Bijektion sein und es gibt folglich $b \in R$ mit $ab = 1$. Ebenso finden wir $c \in R$ mit $ca = 1$ und dann folgt leicht $b = c$.

Beispiel 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.

5.2.23 (**Ursprung der Terminologie**). A priori meint eine Einheit in der Physik das, was ein Mathematiker eine Basis eines eindimensionalen Vektorraums nennen würde. So wäre etwa die Sekunde s eine Basis des reellen Vektorraums $\vec{\mathbb{T}}$ aller Zeitspannen aus 3.1.9. 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 rührt dann wohl auch die Terminologie.

5.2.24. Ein Körper kann in dieser Begrifflichkeit definiert werden als ein Kring, der nicht der Nullring ist und in dem jedes von Null verschiedene Element eine Einheit ist.

Proposition 5.2.25 (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 Nullteiler. Damit kann $\mathbb{Z}/m\mathbb{Z}$ kein Körper sein, da Einheiten nach 5.2.18 nie

Nullteiler sein können. Ist dahingegen $m = p$ eine Primzahl, so folgt aus dem Satz von Euklid 4.4.15, daß $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei ist. Dann aber sind nach 5.2.21 alle seine von Null verschiedenen Elemente Einheiten und $\mathbb{Z}/p\mathbb{Z}$ ist folglich ein Körper. □

5.2.26 (**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 [AL] 3.1.6 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 Primzahlpotenz q im Index als Bezeichnung für „den endlichen Körper mit q Elementen", den wir erst in [AL] 3.7.1 kennenlernen werden, und der weder als Ring noch als abelsche Gruppe isomorph ist zu $\mathbb{Z}/q\mathbb{Z}$.

Ergänzung 5.2.27. Ich bespreche kurz das **Verfahren von Diffie-Hellman** zum öffentlichen Vereinbaren geheimer Schlüssel. Wir betrachten dazu das des 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 5.2.28. 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 5.2.29. Gegeben ein Ring R gibt es nach 5.1.10 genau einen Ringhomomorphismus $\mathbb{Z} \to R$. Dessen Kern alias das Urbild der Null ist nach [GR] 3.3.22 eine Untergruppe von $\mathbb{Z}$ und hat nach 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 $m = \operatorname{char} R$.

5.2.30 (**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 $1 + 1 + \ldots + 1 = 0$ mit einer positiven Zahl von Summanden links. Kriegen wir da überhaupt nie Null heraus, so ist die Charakteristik Null, wir haben also etwa $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$. Gilt bereits $1 = 0$, so ist die Charakteristik 1 und wir haben den Nullring vor uns. Für $p \in \mathbb{N}$ gilt allgemein $\operatorname{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

5.2.31 (**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 5.2.32. Im Körper $\mathbb{F}_7$ ist (-1) kein Quadrat, wie man durch Ausprobieren leicht feststellen kann. Einen Körper mit 49 Elementen kann man deshalb nach [GR] 3.4.15 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 5.2.33. Gegeben eine abelsche Gruppe V und ein Körper K induziert die kanonische Identifikation $\mathrm{Ens}(K \times V, V) \xrightarrow{\sim} \mathrm{Ens}(K, \mathrm{Ens}(V, V))$ aus [GR] 2.3.34 eine Bijektion

$$\left\{ \begin{array}{c} \text{Strukturen als } K\text{-Vektorraum} \\ \text{auf der abelschen Gruppe } V \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Ringhomomorphismen} \\ K \to \mathrm{Ab}\, V \end{array} \right\}$$

Wir verwenden hier unsere alternative Notation $\mathrm{Ab}\, V$ für den Endomorphismenring der abelschen Gruppe V, um jede Verwechslung mit dem Endomorphismenring als Vektorraum auszuschließen.

Übung 5.2.34. Man finde das multiplikative Inverse der Nebenklasse von 22 im Körper $\mathbb{F}_{31}$. Hinweis: Euklidischer Algorithmus.

Ergänzende Übung 5.2.35. Man konstruiere einen Körper mit 49 Elementen und einen Körper mit 25 Elementen. Hinweis: [GR] 3.4.14 und [GR] 3.4.15.

Ergänzende Übung 5.2.36. Sei R ein Kring, dessen Charakteristik eine Primzahl p ist, für den es also einen Ringhomomorphismus $\mathbb{Z}/p\mathbb{Z} \to R$ gibt. Man zeige, daß dann der sogenannte **Frobenius-Homomorphismus** $F : R \to R$, $a \mapsto a^p$ ein Ringhomomorphismus von R in sich selber ist. Hinweis: Man verwende, daß die binomische Formel [GR] 3.4.9 offensichtlich in jedem Kring gilt, ja sogar für je zwei Elemente a, b eines beliebigen Rings mit $ab = ba$.

Ergänzende Übung 5.2.37. 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 5.2.38. Eine natürliche Zahl ist durch 11 teilbar genau dann, wenn ihre „alternierende Quersumme“ durch 11 teilbar ist.

Ergänzende Übung 5.2.39. Eine natürliche Zahl, die kongruent zu sieben ist modulo acht, kann nicht eine Summe von drei Quadraten sein.

Ergänzende Übung 5.2.40. Eine Zahl mit einer Dezimaldarstellung der Gestalt $abcabc$ wie zum Beispiel 349349 ist stets durch 7 teilbar.

Ergänzende Übung 5.2.41. 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 5.2.42. Jeder Ringhomomorphismus macht Einheiten zu Einheiten. Jeder Ringhomomorphismus von einem Körper in einen vom Nullring verschiedenen Ring ist injektiv.

Übung 5.2.43. 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 5.2.44. Wieviele Untervektorräume hat ein zweidimensionaler Vektorraum über einem Körper mit fünf Elementen? Wieviele angeordnete Basen?

Ergänzende Übung 5.2.45. Gegeben ein Vektorraum über einem endlichen Primkörper sind seine Untervektorräume genau die Untergruppen der zugrundeliegenden abelschen Gruppe.

Ergänzende Übung 5.2.46. Man zeige: In jedem endlichen Körper ist das Produkt aller von Null verschiedenen Elemente (-1). Hinweis: Man zeige zunächst, daß nur die Elemente ± 1 ihre eigenen Inversen sind. Als Spezialfall erhält man $(p-1)! \equiv -1 \pmod p$ 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 5.2.47. 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: 4.4.12.

Übung 5.2.48. Man zeige für Binomialkoeffizienten im Körper $\mathbb{F}_p$ die Identität $\binom{p-1}{i} = (-1)^i$.

5.3 Polynome

5.3.1. Ist K ein Ring, so bildet die Menge $K[X]$ aller „formalen Ausdrücke" der Gestalt $a_n X^n + \ldots + a_1 X + a_0$ mit $a_i \in K$ unter der offensichtlichen Addition und Multiplikation einen Ring, den **Polynomring über K in einer Variablen** X, und wir haben eine offensichtliche Einbettung $\operatorname{can} : K \hookrightarrow K[X]$. Die Herkunft der Bezeichnung diskutieren wir in [AN1] 2.3.9. Die a_ν heißen in diesem Zusammenhang die **Koeffizienten** unseres Polynoms, genauer heißt a_ν der **Koeffizient von** X^ν. 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 5.3.2. Sei K ein Ring. Wir bezeichnen mit $K[X]$ die Menge aller Abbildungen $\varphi : \mathbb{N} \to K$, die nur an endlich vielen Stellen von Null verschiedene

Werte annehmen, und definieren auf $K[X]$ eine Addition und eine Multiplikation durch die Regeln

$$\begin{array}{rcl}(\varphi + \psi)(n) & := & \varphi(n) + \psi(n) \\ (\varphi \cdot \psi)(n) & := & \sum_{i+j=n} \varphi(i)\psi(j)\end{array}$$

Mit diesen Verknüpfungen wird $K[X]$ ein Ring, der **Polynomring über** K. Ordnen wir jedem $a \in K$ die Abbildung $\mathbb{N} \to K$ zu, die bei 0 den Wert a annimmt und sonst den Wert Null, so erhalten wir eine Einbettung, ja einen injektiven Ringhomomorphismus

$$\mathrm{can} : K \hookrightarrow K[X]$$

Wir notieren ihn schlicht $a \mapsto a$ und nennen die Polynome im Bild dieser Einbettung **konstante Polynome**. Bezeichnen wir weiter mit X die Abbildung $\mathbb{N} \to K$, die bei 1 den Wert 1 annimmt und sonst nur den Wert Null, so können wir jede Abbildung $\varphi \in K[X]$ 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 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.

5.3.4. Die wichtigste Eigenschaft eines Polynomrings ist, daß man „für die Variable etwas einsetzen darf“. Das wollen wir nun formal aufschreiben.

Proposition 5.3.5 (**Einsetzen in Polynome**). *Seien K ein Kring und $b \in K$ ein Element. So gibt es genau einen Ringhomomorphismus*

$$\mathrm{E}_b : K[X] \to K$$

mit $\mathrm{E}_b(X) = b$ und $\mathrm{E}_b \circ \mathrm{can} = \mathrm{id}_K$. Wir nennen E_b den **Einsetzungshomomorphismus zu** b*.*

Beweis. Dieser eindeutig bestimmte Ringhomomorphismus E_b ist eben gegeben durch die Vorschrift $\mathrm{E}_b(a_n X^n + \ldots + a_1 X + a_0) = a_n b^n + \ldots + a_1 b + a_0$. $\square$

5.3.6. Es ist üblich, das Bild unter dem Einsetzungshomomorphismus E_b eines Polynoms $P \in K[X]$ abzukürzen als

$$P(b) := \mathrm{E}_b(P)$$

5.3.7. Unsere übliche Darstellung einer Zahl in Ziffernschreibweise 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 $7X^3 + 2X^2 + 5X + 8$.

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 $bc = cb$.

Proposition 5.3.9 (Einsetzen in Polynome, Variante). *Seien $\varphi : K \to R$ ein Ringhomomorphismus und $b \in R$ ein Element derart, daß b für alle $a \in K$ mit $\varphi(a)$ kommutiert. So gibt es genau einen Ringhomomorphismus*

$$\mathrm{E}_{\varphi,b} = \mathrm{E}_b : K[X] \to R$$

mit $\mathrm{E}_b(X) = b$ und $\mathrm{E}_b \circ \mathrm{can} = \varphi$. Wir nennen $\mathrm{E}_{\varphi,b}$ den **Einsetzungshomomorphismus zu b über φ**.

Beweis. Dieser eindeutig bestimmte Ringhomomorphismus E_b ist gegeben durch die Vorschrift $\mathrm{E}_b(a_n X^n + \ldots + a_1 X + a_0) := \varphi(a_n)b^n + \ldots + \varphi(a_1)b + \varphi(a_0)$. □

5.3.10. Es ist auch in dieser Allgemeinheit üblich, das Bild unter dem Einsetzungshomomorphismus $\mathrm{E}_{\varphi,b}$ eines Polynoms $P \in K[X]$ abzukürzen als

$$P(b) := \mathrm{E}_{\varphi,b}(P)$$

So schreiben wir im Fall eines Krings K zum Beispiel $P(A)$ für die Matrix, die beim Einsetzen einer quadratischen Matrix $A \in \mathrm{Mat}(n; K)$ in das Polynom P ensteht. In diesem Fall hätten wir $R = \mathrm{Mat}(n; K)$ und φ wäre der Ringhomomorphismus, der jedem $a \in K$ das a-fache der Einheitsmatrix zuordnet.

5.3.11 (**Wechsel der Koeffizienten**). Ist $\varphi : K \to S$ ein Ringhomomorphismus, so erhalten wir einen Ringhomomorphismus $\varphi = \varphi_{[X]} : K[X] \to S[X]$ der zugehörigen Polynomringe durch das „Anwenden von φ auf die Koeffizienten“. Formal können wir ihn als das „Einsetzen von X für X über φ“ beschreiben, also als den Ringhomomorphismus $\varphi_{[X]} = \mathrm{E}_{\varphi,X}$.

Definition 5.3.12. Seien K ein Kring und $P \in K[X]$ ein Polynom. Ein Element $a \in K$ heißt eine **Nullstelle** oder auch eine **Wurzel** von P, wenn gilt $P(a) = 0$.

Definition 5.3.13. Sei K ein Ring. Jedem Polynom $P \in K[X]$ ordnen wir seinen **Grad** $\operatorname{grad} P \in \mathbb{N} \sqcup \{-\infty\}$ (englisch **degree**, französisch **degré**) zu durch die Vorschrift

$$\begin{array}{ll} \operatorname{grad} P = n & \text{für } P = a_n X^n + \ldots + a_1 X + a_0 \text{ mit } a_n \neq 0; \\ \operatorname{grad} P = -\infty & \text{für } P \text{ das Nullpolynom.} \end{array}$$

Für ein von Null verschiedenes Polynom $P = a_n X^n + \ldots + a_1 X + a_0$ mit $n = \operatorname{grad} P$ nennt man $a_n \in K \backslash 0$ seinen **Leitkoeffizienten**. Den Leitkoeffizienten des Nullpolynoms definieren wir als die Null von K. 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 5.3.14 (Grad eines Produkts). *Ist K ein nullteilerfreier Ring, so ist auch der Polynomring $K[X]$ nullteilerfrei und der Grad eines Produkts ist die Summe der Grade der Faktoren, in Formeln*

$$\operatorname{grad}(PQ) = \operatorname{grad} P + \operatorname{grad} Q$$

Beweis. Ist K nullteilerfrei, so ist offensichtlich der Leitkoeffizient von PQ das Produkt der Leitkoeffizienten von P und von Q. □

Lemma 5.3.15 (Polynomdivision mit Rest). *Sei K ein Ring. Gegeben Polynome $P, Q \in K[X]$ mit Q normiert gibt es eindeutig bestimmte Polynome A, R mit $P = AQ + R$ und $\operatorname{grad} R \leq (\operatorname{grad} Q) - 1$.*

Beispiel 5.3.16. Die Polynomdivision mit Rest des Polynoms $X^4 + 2X^2$ durch $X^2 + 2X + 1$ liefert

$$\begin{array}{rcl} X^4 + 2X^2 &=& X^2(X^2 + 2X + 1) - 2X^3 + X^2 \\ &=& X^2(X^2 + 2X + 1) - 2X(X^2 + 2X + 1) + 5X^2 + 2X \\ &=& (X^2 - 2X + 5)(X^2 + 2X + 1) - 8X - 5 \end{array}$$

Beweis. Ich habe mir bei der Formulierung des Lemmas Mühe gegeben, daß es auch im Fall des Nullrings $K = 0$ richtig ist, wenn wir $-\infty - 1 = -\infty$ verstehen. Für den Beweis dürfen wir damit annehmen, daß K nicht der Nullring ist. Wir suchen ein Polynom A mit $\operatorname{grad}(P - AQ)$ kleinstmöglich. Gälte dennoch $\operatorname{grad}(P - AQ) \geq (\operatorname{grad}(Q))$, sagen wir $P - AQ = aX^r + \ldots + c$ mit $a \neq 0$ und $r > d = \operatorname{grad}(Q)$, so hätte $P - (A + aX^{r-d})Q$ echt kleineren Grad als R, im Widerspruch zur Wahl von A. Das zeigt die Existenz. Für den Nachweis der Eindeutigkeit gehen wir aus von einer weiteren Gleichung $P = A'Q + R'$ mit $\operatorname{grad} R' < d$. Es folgt zunächst $(A - A')Q = R' - R$ und wegen der offensichtlichen Formel für den Grad des Produkts eines beliebigen Polynoms mit einem normierten Polynom weiter $A - A' = 0$ und dann auch $R' - R = 0$. □

Korollar 5.3.17 (Abspalten von Linearfaktoren bei Nullstellen). *Sei K ein Kring und $P \in K[X]$ ein Polynom. Genau dann ist $\lambda \in K$ eine Nullstelle des Polynoms P, wenn das Polynom $(X - \lambda)$ das Polynom P teilt.*

Beweis. Nach Lemma 5.3.15 über die Division mit Rest finden wir ein Polynom $A \in K[X]$ und eine Konstante $b \in K$ mit $P = A(X - \lambda) + b$. Einsetzen von λ für X liefert dann $b = 0$. □

5.3.18. Der im Sinne von 5.3.13 lineare Faktor $(X - \lambda)$ unseres Polynoms heißt auch ein **Linearfaktor**, daher der Name des Korollars.

Satz 5.3.19 (Zahl der Nullstellen eines Polynoms). *Ist K ein Körper oder allgemeiner ein kommutativer Integritätsbereich, so hat ein von Null verschiedenes Polynom $P \in K[X]$ höchstens $\operatorname{grad} P$ Nullstellen in K.*

Beweis. Ist $\lambda \in K$ eine Nullstelle, so finden wir nach 5.3.17 eine Darstellung $P = A(X - \lambda)$ mit $\operatorname{grad} A = \operatorname{grad} P - 1$. Eine von λ verschiedene Nullstelle von P ist für K nullteilerfrei notwendig eine Nullstelle von A und der Satz folgt mit Induktion. □

Beispiel 5.3.20. In einem Körper K oder allgemeiner einem kommutativen Integritätsbereich 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 5.3.21. Die Kommutativität ist hierbei wesentlich. In 5.7.4 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 $\pm\,\mathrm{i}$, $\pm\,\mathrm{j}$, $\pm\,\mathrm{k}$ und nicht ganz so offensichtlich [ML] 1.6.9 sogar unendlich viele Lösungen.

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** λ oder auch ihre **Ordnung**. Das Nullpolynom hat insbesondere an jeder Stelle eine Nullstelle mit der Vielfachheit ∞ und gar keine Nullstelle bei λ ist dasselbe wie eine „Nullstelle der Vielfachheit Null“. Durch Abspalten von Nullstellen wie in 5.3.17 zeigt man, daß im Fall eines Körpers oder allgemeiner eines kommutativen Integritätsbereichs auch die Zahl der mit ihren Vielfachheiten gezählten Nullstellen eines von Null verschiedenen Polynoms beschränkt ist durch seinen Grad.

Definition 5.3.23. Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom $P \in K[X]\backslash K$ mit Koeffizienten in unserem Körper K auch eine Nullstelle in unserem Körper K hat.

Beispiel 5.3.24. Der Körper $K = \mathbb{R}$ ist nicht algebraisch abgeschlossen, denn das Polynom $X^2 + 1$ hat keine reelle Nullstelle.

Vorschau 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 [AN1] 7.2.1, einen sehr eleganten mit den Methoden der Funktionentheorie in [FT1] 2.1.8, und einen mehr algebraischen Beweis, bei dem die Analysis nur über den Zwischenwertsatz eingeht, in [AL] 4.3.8. Mir gefällt der noch wieder andere Beweis mit den Mitteln der Topologie [TF] 1.7.13 am besten, da er meine Anschauung am meisten anspricht. Er wird in analytischer Verkleidung bereits in [AN2] 5.7.18 vorgeführt. Eine heuristische Begründung wird in nebenstehendem Bild vorgeführt.

Satz 5.3.26. *Ist K ein algebraisch abgeschlossener Körper, so hat jedes von Null verschiedene Polynom $P \in K[X]\backslash 0$ eine* **Zerlegung in Linearfaktoren** *der Gestalt*

$$P = c(X - \lambda_1) \dots (X - \lambda_n)$$

mit $n \geq 0$, $c \in K^\times$ und $\lambda_1, \dots, \lambda_n \in K$, und diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.

5.3.27. Gegeben eine Nullstelle μ von P ist in diesem Fall die Zahl der Indizes i mit $\lambda_i = \mu$ die Vielfachheit der Nullstelle μ. In der Sprache der Multimengen aus [GR] 2.3.37 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 der Multimenge ${}_\mu\{\lambda_1, \dots, \lambda_n\}$ das Polynom $(X - \lambda_1) \dots (X - \lambda_n)$ zuordnen.

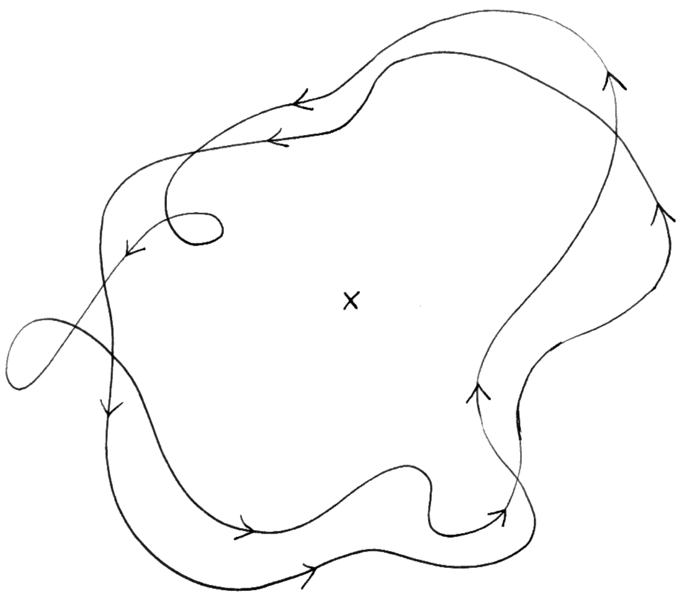
Beweis. Ist P ein konstantes Polynom, so ist nichts zu zeigen. Ist P nicht konstant, so gibt es nach Annahme eine Nullstelle $\lambda \in K$ von P und wir finden genau ein Polynom $\tilde{P}$ mit $P = (X - \lambda)\tilde{P}$. Der Satz folgt durch vollständige Induktion über den Grad von P. □

Korollar 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 stabil ist unter der komplexen Konjugation, müssen sich seine mit ihren Vielfachheiten genommenen komplexen Nullstellen so durchnummerieren 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 stabil sind unter der komplexen Konjugation, haben jedoch keine reellen Nullstellen. □



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 [AN2] 5.7.21 oder besser [TF] 1.7.13 werden wir diese Heuristik zu einem formalen Beweis ausbauen.

5.3.29 (**Polynomringe in mehreren Variablen**). Ähnlich wie den Polynomring in einer Variablen 5.3.2 konstruiert man auch Polynomringe in mehr Variablen über einem gegebenen Grundring K. Ist die Zahl der Variablen endlich, so kann man induktiv definieren

$$K[X_1, \ldots, X_n] = (K[X_1, \ldots, X_{n-1}])[X_n]$$

Man kann aber auch für eine beliebige Menge I den Polynomring $K[X_i]_{i \in I}$ 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.

Übungen

Übung 5.3.30. Welche Matrix entsteht beim Einsetzen der quadratischen Matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in das Polynom $X^2 + 1$?

Ergänzende Übung 5.3.31. Man zeige, daß jede Nullstelle $\alpha \in \mathbb{C}$ eines normierten Polynoms mit komplexen Koeffizienten $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ die Abschätzung $|\alpha| \leq 1 + |a_{n-1}| + \ldots + |a_0|$ erfüllt. Hinweis: Sonst gilt erst $|\alpha| > 1$ und dann $|\alpha|^n > |a_{n-1}\alpha^{n-1}| + \ldots + |a_0|$. 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.

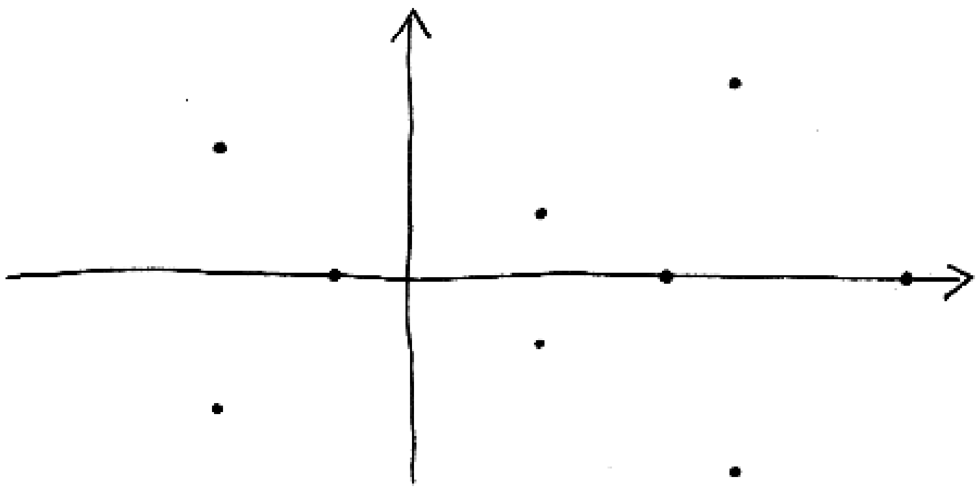
Übung 5.3.32. Ist $P \in \mathbb{R}[X]$ ein Polynom mit reellen Koeffizienten und $\mu \in \mathbb{C}$ eine komplexe Zahl, so gilt $P(\mu) = 0 \Rightarrow P(\bar{\mu}) = 0$. Ist also eine komplexe Zahl Nullstelle eines Polynoms mit reellen Koeffizienten, so ist auch die konjugiert komplexe Zahl eine Nullstelle desselben Polynoms.

Ergänzende Übung 5.3.33. Seien k, K kommutative Ringe, $i : k \to K$ ein Ringhomomorphismus und $i : k[X] \to K[X]$ 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 5.3.34. 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 5.3.35. 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 5.3.36. Man zerlege das Polynom $X^4 + 2$ in $\mathbb{R}[X]$ in der in 5.3.28 beschriebenen Weise in ein Produkt quadratischer Faktoren ohne Nullstelle.



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 5.3.32.

Ergänzende Übung 5.3.37. Ein reelles Polynom hat bei $\lambda \in \mathbb{R}$ eine mehrfache Nullstelle genau dann, wenn auch seine Ableitung bei λ verschwindet.

Ergänzende Übung 5.3.38. 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 5.3.39. 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 5.3.40. Gegeben ein Ring K bilden auch die **formalen Potenzreihen mit Koeffizienten in** K der Gestalt $\sum_{n\geq 0} a_n X^n$ mit $a_n \in K$ einen Ring, der meist $K[\![X]\!]$ notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß seine Einheiten genau diejenigen Potenzreihen sind, deren konstanter Term eine Einheit in K ist, in Formeln

$$K[\![X]\!]^\times = K^\times + XK[\![X]\!]$$

Man verallgemeinere die Definition und Beschreibung der Einheiten auf Potenzreihenringe $K[\![X_1, \ldots, X_n]\!]$ in mehreren Variablen und konstruiere einen Ringisomorphismus

$$(K[\![X_1, \ldots, X_n]\!])[\![X_{n+1}]\!] \xrightarrow{\sim} K[\![X_1, \ldots, X_n, X_{n+1}]\!]$$

Allgemeiner sei $f = \sum_{n\geq 0} a_n X^n \in K[\![X]\!]$ eine formale Potenzreihe, für die mindestens ein Koeffizient eine Einheit ist. Man zeige, daß es dann genau eine Einheit $g \in K[\![X]\!]^\times$ gibt derart, daß fg ein normiertes Polynom ist. Man zeige genauer: Ist m minimal mit $a_m \in K^\times$, so gibt es $g \in K[\![X]\!]^\times$ mit fg normiert vom Grad m. Diese Aussage ist ein formales Analogon des **Weierstraß'schen Vorbereitungssatzes** insbesondere im Fall, daß K selbst ein formaler Potenzreihenring in mehreren Variablen ist.

Ergänzende Übung 5.3.41. Gegeben ein Ring K bilden auch die **formalen Laurentreihen mit Koeffizienten in** K der Gestalt $\sum_{n\geq -N} a_n X^n$ mit $a_n \in K$ und $N \in \mathbb{N}$ einen Ring, der meist $K(\!(X)\!)$ notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß im Fall $K \neq 0$ 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 K ist, in Formeln

$$K(\!(X)\!)^\times = \bigcup_{n\in\mathbb{Z}} X^n K[\![X]\!]^\times$$

Insbesondere ist im Fall eines Körpers K auch $K(\!(X)\!)$ ein Körper.

Ergänzung 5.3.42. Wir verwenden hier die Terminologie, nach der bei *formalen* Laurentreihen im Gegensatz zu den ursprünglichen Laurentreihen der Funktionentheorie nur endlich viele Terme mit negativen Exponenten erlaubt sind.

5.4 Polynome als Funktionen*

Lemma 5.4.1 (Interpolation durch Polynome). *Seien K ein Körper und $x_0, \ldots, x_n \in K$ paarweise verschiedene* **Stützstellen** *und $y_0, \ldots, y_n \in K$ beliebig vorgegebene Werte. So gibt es genau ein Polynom $P \in K[X]$ vom Grad $\leq n$ mit $P(x_0) = y_0, \ldots, P(x_n) = y_n$.*

Beweis. Zunächst ist sicher $(X - x_1) \ldots (X - x_n) =: A_0(X)$ ein Polynom vom Grad n, das bei $x_1, \ldots, x_n$ 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 $x_1, \ldots, x_n$ verschwindet. In derselben Weise konstruieren wir auch Polynome $L_1(X), \ldots, L_n(X)$ und erhalten ein mögliches Interpolationspolynom als

$$P(X) = y_0 L_0(X) + \ldots + y_n L_n(X) = \sum_{i=0}^{n} y_i \frac{\prod_{j \neq i}(X - x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

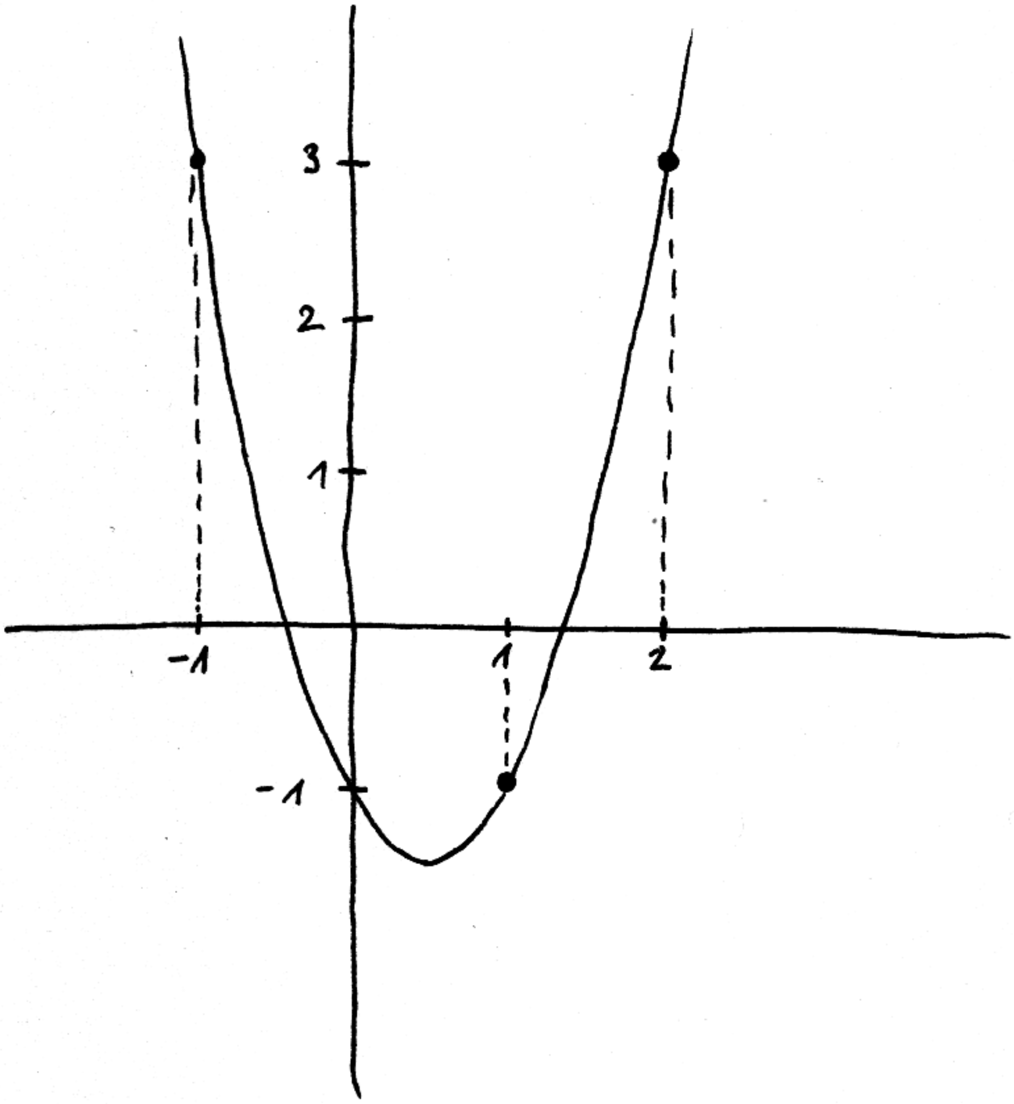
Das zeigt die Existenz. Ist Q eine weitere Lösung derselben Interpolationsaufgabe vom Grad $\leq n$, so ist $P - Q$ ein Polynom vom Grad $\leq n$ mit $n + 1$ Nullstellen, eben bei den Stützstellen $x_0, \ldots, x_n$. Wegen 5.3.19 muß dann aber $P - Q$ das Nullpolynom sein, und das zeigt die Eindeutigkeit. □

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 $f \in K[X_1, \ldots, X_n]$ die Funktion $\tilde{f} : K^n \to K$, $(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)$ zuordnen. Wir erhalten so einen Ringhomomorphismus

$$K[X_1, \ldots, X_n] \to \operatorname{Ens}(K^n, K)$$

Dieser Homomorphismus ist im Allgemeinen weder injektiv noch surjektiv. Schon für $n = 1$, $K = \mathbb{R}$ läßt sich ja keineswegs jede Abbildung $\mathbb{R} \to \mathbb{R}$ 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 $K[X_1, \ldots, X_n]$ in den endlichdimensionalen K-Vektorraum $\operatorname{Ens}(K^n, K)$ unmöglich injektiv sein. Wir haben jedoch den folgenden Satz.

Satz 5.4.3 (Polynome als Funktionen). *1. Ist K ein unendlicher Körper, ja allgemeiner ein unendlicher nullteilerfreier Kring, so ist für alle $n \in \mathbb{N}$ die Auswertungsabbildung eine Injektion $K[X_1, \ldots, X_n] \hookrightarrow \operatorname{Ens}(K^n, K)$;*



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.

2. *Ist K ein endlicher Körper, so ist für alle $n \in \mathbb{N}$ die Auswertungsabbildung eine Surjektion $K[X_1, \ldots, X_n] \twoheadrightarrow \operatorname{Ens}(K^n, K)$. Den Kern dieser Surjektion beschreibt Übung [LA2] 5.3.19.*

Beweis. 1. Durch Induktion über n. Der Fall $n = 0$ ist eh klar. Für $n = 1$ folgt die Behauptung aus der Erkenntnis, das jedes von Null verschiedene Polynom in $K[X]$ nur endlich viele Nullstellen in K haben kann. Der Kern der Abbildung

$$K[X] \to \operatorname{Ens}(K, K)$$

besteht also nur aus dem Nullpolynom. Für den Induktionsschritt setzen wir $X_n = Y$ und schreiben unser Polynom in der Gestalt

$$P = a_d Y^d + \ldots + a_1 Y + a_0$$

mit $a_i \in K[X_1, \ldots, X_{n-1}]$. Halten wir $(x_1, \ldots, x_{n-1}) = x \in K^{n-1}$ fest, so ist $a_d(x)Y^d + \ldots + a_1(x)Y + a_0(x) \in K[Y]$ das Nullpolynom nach dem Fall $n = 1$. Also verschwinden $a_d(x), \ldots, a_1(x), a_0(x)$ für alle $x \in K^{n-1}$, mit Induktion sind somit alle a_i schon das Nullpolynom und wir haben $P = 0$.

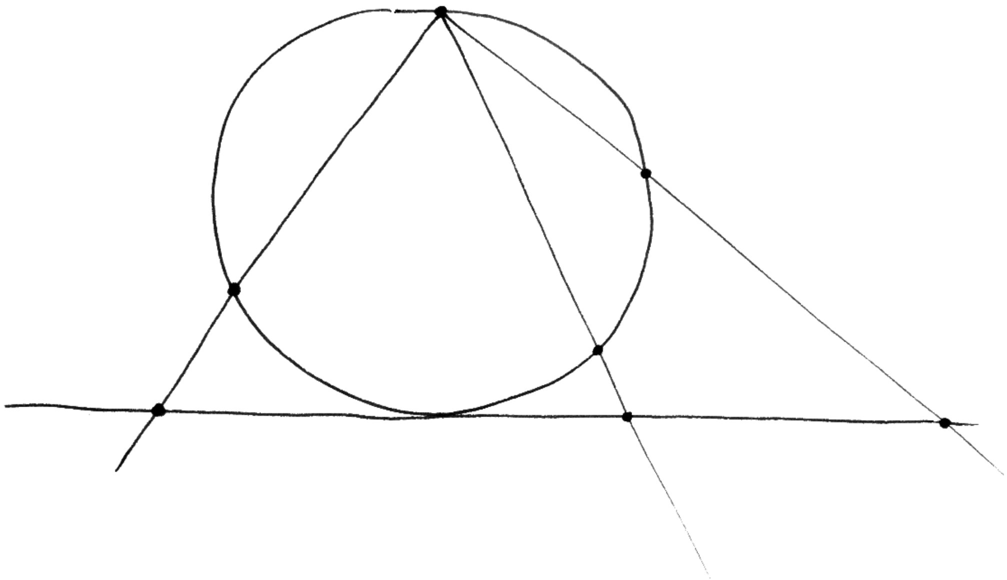
2. Das bleibt dem Leser überlassen. Man mag sich beim Beweis an 5.4.1 orientieren. Wir folgern in [AL] 2.3.7 eine allgemeinere Aussage aus dem abstrakten chinesischen Restsatz. □

Übungen

Ergänzende Übung 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 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 der, bis auf einen Skalar eindeutig bestimmten, 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 $H_1, \ldots, H_n \subset K^d$, so wird es vom Produkt der linearen Gleichungen unserer Hyperebenen geteilt.

Ergänzende Übung 5.4.6 (**Pythagoreische Zahlen**). Man zeige: Stellen wir eine Lampe oben auf den Einheitskreis und bilden jeden von $(0, 1)$ verschiedenen



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 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.

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.

Ergänzung 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 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 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 **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 numerisches Polynom sein muß und daß das $(d!)$-fache seines Leitkoeffizienten mithin eine ganze Zahl sein muß.

Ergänzende Übung 5.4.9. Man zeige, daß die Menge der Polynome 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 5.4.8.

5.5 Äquivalenzrelationen

5.5.1. Unter einer **Relation** R auf einer Menge X verstehen wir wie in 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 5.5.2. Eine Relation $R \subset X \times X$ auf einer Menge X heißt eine **Äquivalenzrelation** genau dann, wenn für alle Elemente $x, y, z \in X$ gilt:

1. **Transitivität:** $(xRy$ und $yRz) \Rightarrow xRz$;
2. **Symmetrie:** $xRy \Leftrightarrow yRx$;
3. **Reflexivität:** xRx.

5.5.3. 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 $X \neq \emptyset$.

5.5.4. 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. $A(x) \cap A(y) \neq \emptyset$.

5.5.5. 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 $\mathrm{can} : X \to (X/\sim)$, $x \mapsto A(x)$. Diese kanonische Abbildung ist eine Surjektion und ihre Fasern sind genau die Äquivalenzklassen unserer Äquivalenzrelation.

5.5.6. Ist $f : X \to Z$ eine Abbildung mit $x \sim y \Rightarrow f(x) = f(y)$, so gibt es nach der universellen Eigenschaft von Surjektionen [GR] 2.3.29 genau eine Abbildung $\bar{f} : (X/\sim) \to Z$ mit $f = \bar{f} \circ \mathrm{can}$. Wir zitieren diese Eigenschaft manchmal als die **universelle Eigenschaft des Raums der Äquivalenzklassen**. Sagt man, eine Abbildung $g : (X/\sim) \to Z$ sei **wohldefiniert** durch eine Abbildung $f : X \to Z$, so ist gemeint, daß f die Eigenschaft $x \sim y \Rightarrow f(x) = f(y)$ hat und daß man $g = \bar{f}$ setzt.

Beispiel 5.5.7 (**Restklassen als Äquivalenzklassen**). Gegeben eine ganze Zahl $m \in \mathbb{Z}$ ist unser „kongruent modulo m" aus 5.2.4 eine Äquivalenzrelation $\sim$ auf $\mathbb{Z}$ und die zugehörigen Äquivalenzklassen sind genau unsere Restklassen von dort, so daß wir also $(\mathbb{Z}/\sim) = \mathbb{Z}/m\mathbb{Z}$ erhalten.

Ergänzung 5.5.8. Sind $R \subset X \times X$ und $S \subset Y \times Y$ Äquivalenzrelationen, so auch das Bild von $(R \times S) \subset (X \times X) \times (Y \times Y)$ unter der durch Vertauschen der mittleren Einträge gegebenen Identifikation $(X \times X) \times (Y \times Y) \xrightarrow{\sim} (X \times Y) \times (X \times Y)$. Wir notieren diese Äquivalenzrelation auf dem Produkt kurz $R \times S$.

Ergänzung 5.5.9. 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 $x = x_0, x_1, \ldots, x_n = y$ von X mit $x_\nu R x_{\nu-1}$ oder $x_{\nu-1} R x_\nu$ für alle ν mit $1 \leq \nu \leq n$. Wir nennen T auch die **von der Relation** R **erzeugte Äquivalenzrelation auf** X. Denken wir uns etwa X als die „Menge aller Tiere" und R als die Relation „könnten 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.

Übungen

Übung 5.5.10 (**Konstruktion von** $(\mathbb{Z}, +)$ **aus** $(\mathbb{N}, +)$). Gegeben eine kommutative nichtleere Halbgruppe $(M, +)$ erklärt man ihre **einhüllende Gruppe** $\bar{M}$ wie folgt: Man geht aus von der Menge $M \times M$ und erklärt darauf eine Relation durch die Vorschrift

$$(x, y) \sim (a, b) \Leftrightarrow (\exists c \in M \text{ mit } x + b + c = y + a + c)$$

Man zeige, daß sie eine Äquivalenzrelation ist, und daß die komponentenweise Verknüpfung auf $M \times M$ eine Verknüpfung auf der Menge der Äquivalenzklassen $\bar{M} := M \times M/\sim$ induziert. Man zeige weiter, daß mit dieser Verknüpfung $\bar{M}$ eine abelsche Gruppe wird. Man zeige weiter, daß die Abbildung $\operatorname{can} : M \to \bar{M}$, $a \mapsto [x, x + a]$ dann unabhängig von der Wahl von $x \in M$ und ein Halbgruppenhomomorphismus ist. Man zeige, daß can genau dann injektiv ist, wenn M die „Kürzungsregel" $(a + c = b + c) \Rightarrow (a = b)$ erfüllt. Gegeben eine Gruppe G zeige man schließlich, daß das Vorschalten von $\operatorname{can} : M \to \bar{M}$ eine Bijektion

$$\operatorname{Grp}(\bar{M}, G) \xrightarrow{\sim} \operatorname{Halb}(M, G)$$

liefert. Ist M ein Monoid, so ist unser $M \to \bar{M}$ sogar ein Monoidhomomorphismus. Zum Beispiel kann man die obige Konstruktion verwenden, um aus dem

Monoid $(\mathbb{N}, +)$ oder der Halbgruppe $(\mathbb{N}_{\geq 1}, +)$ die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen $\tilde{\mathbb{N}} =: \mathbb{Z}$ zu bilden. Aufgrund der Kürzungsregel 4.2.8 ist die kanonische Abbildung in diesem Fall eine Injektion $\mathbb{N} \hookrightarrow \mathbb{Z}$. Aus [AN1] 1.5.6 folgt dann schließlich, daß sich unsere Multiplikation auf $\mathbb{N}$ aus 4.2.11 auf eine und nur eine Weise zu einer kommutativen und über $+$ distributiven Multiplikation auf $\mathbb{Z}$ fortsetzen läßt.

Ergänzende Übung 5.5.11. Ist G eine Gruppe und $H \subset G \times G$ eine Untergruppe, die die Diagonale umfaßt, so ist H eine Äquivalenzrelation.

5.6 Quotientenkörper und Partialbruchzerlegung

5.6.1. 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 5.6.2. Gegeben ein kommutativer Integritätsbereich R konstruieren wir seinen **Quotientenkörper**

$$\operatorname{Quot}(R)$$

wie folgt: Wir betrachten die Menge $R \times (R \backslash 0)$ 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 $\operatorname{Quot}(R)$ und die Äquivalenzklasse von (a, s) mit $\frac{a}{s}$ oder a/s. Dann definieren wir auf $\operatorname{Quot}(R)$ 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 $\operatorname{Quot}(R)$ zu einem Körper machen und daß die Abbildung $\operatorname{can} : R \to \operatorname{Quot}(R)$, $r \mapsto r/1$ ein injektiver Ringhomomorphismus ist. Er heißt die **kanonische Einbettung** unseres Integritätsbereichs in seinen Quotientenkörper.

Ergänzung 5.6.3. Auf Englisch bezeichnet man den Quotientenkörper als **fraction field** und auf Französisch als **corps de fractions**. Dort verwendet man folgerichtig statt unserer Notation $\operatorname{Quot}(R)$ die Notation $\operatorname{Frac}(R)$. Die noch allgemeinere Konstruktion der „Lokalisierung" lernen wir erst in [KAG] 3.3.4 kennen.

Beispiel 5.6.4. Der Körper der rationalen Zahlen $\mathbb{Q}$ wird formal definiert als der Quotientenkörper des Rings der ganzen Zahlen, in Formeln

$$\mathbb{Q} := \operatorname{Quot} \mathbb{Z}$$

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 5.6.5 (**Universelle Eigenschaft des Quotientenkörpers**). *Sei R ein kommutativer Integritätsbereich. Ist $\varphi : R \to A$ ein Ringhomomorphismus, unter dem jedes von Null verschiedene Element von R auf eine Einheit von A abgebildet wird, so faktorisiert φ eindeutig über* $\operatorname{Quot} R$*, es gibt also in Formeln genau einen Ringhomomorphismus $\tilde{\varphi} : \operatorname{Quot} R \to A$ mit $\varphi(r) = \tilde{\varphi}(r/1)\ \forall r \in R$.*

Beweis. Für jedes mögliche $\tilde{\varphi}$ muß gelten $\tilde{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$, und das zeigt bereits die Eindeutigkeit von $\tilde{\varphi}$. Um auch seine Existenz zu zeigen, betrachten wir die Abbildung $\hat{\varphi} : R \times (R \backslash 0) \to A$ gegeben durch $\hat{\varphi}(r, s) = \varphi(r)\varphi(s)^{-1}$ und prüfen, daß sie konstant ist auf Äquivalenzklassen. Dann muß sie nach 5.5.5 eine wohlbestimmte Abbildung $\operatorname{Quot} R \to A$ induzieren, von der der Leser leicht selbst prüfen wird, daß sie ein Ringhomomorphismus ist. □

5.6.6 (**Brüche mit kontrollierten Nennern**). Gegeben ein kommutativer Integritätsbereich R und eine Teilmenge $S \subset R \backslash 0$ betrachten wir im Quotientenkörper von R den Teilring

$$S^{-1}R := \{(r/s) \in \operatorname{Quot} R \mid s \text{ ist Produkt von Elementen von } S\}$$

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 $\varphi : R \to A$ ein Ringhomomorphismus, unter dem jedes Element von S auf eine Einheit von A abgebildet wird, so faktorisiert φ mit demselben Beweis wie zuvor eindeutig über $S^{-1}R$, es gibt also in Formeln genau einen Ringhomomorphismus $\tilde{\varphi} : S^{-1}R \to A$ mit $\varphi(r) = \tilde{\varphi}(r/1)\ \forall r \in R$.

Beispiel 5.6.7 (**Auswerten rationaler Funktionen**). Ist K ein Körper, so bezeichnet man den Quotientenkörper des Polynomrings mit $K(X) := \operatorname{Quot} K[X]$ 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 verstehen 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 λ 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 λ keine Nullstelle hat. Auf diesem Teilring ist das Auswerten bei λ nach 5.6.6 ein wohlbestimmter Ringhomomorphismus $K[X]_\lambda \to K$, 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. 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 ∞ zuweisen soll, so erhält man für jeden unendlichen Körper K sogar eine wohlbestimmte Injektion $K(X) \hookrightarrow \operatorname{Ens}(K, K \sqcup \{\infty\})$.

Ergänzung 5.6.8. Es ist sogar richtig, daß jede rationale Funktion eine eindeutige maximal gekürzte Darstellung mit normiertem Nenner hat. Um das einzusehen, benötigt man jedoch ein Analogon der eindeutigen Primfaktorzerlegung für Polynomringe, das wir erst in [AL] 2.4.24 zeigen.

5.6.9. Wir erinnern aus 5.3.40 und 5.3.41 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 5.6.5 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 5.6.10. 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 5.6.11 (Partialbruchzerlegung). *Ist K ein algebraisch abgeschlossener Körper, so 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 $1 \in K(X)$.

5.6.12. 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 7.2.2 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.

5.6.13. Ist K ein algebraisch abgeschlossener Körper, so sind die Polstellen eines Elements $f \in K(X)$ im Sinne von 5.6.7 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 5.6.14. 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 [AL] 3.7.17 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 in spe, 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 5.6.6 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. $\square$

5.6.15 (**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 5.6.16. Wir bestimmen von $(X^4 + 2X^2)/(X^2 + 2X + 1)$ die Partialbruchzerlegung. Die Polynomdivision haben wir bereits in 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

$$\frac{X^4 + 2X^2}{X^2 + 2X + 1} = X^2 - 2X + 5 - \frac{8}{X + 1} + \frac{3}{(X + 1)^2}$$

5.6.17 (**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 [GR] 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 5.6.11 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 5.6.9 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 [GR] 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 5.6.18. Man zeige: Besitzt ein kommutativer Integritätsbereich R eine Anordnung $\leq$, unter der er im Sinne von [AN1] 1.4.2 ein angeordneter Ring wird, so besitzt sein Quotientenkörper $\operatorname{Quot} R$ genau eine Struktur als angeordneter Körper, für die die kanonische Einbettung $R \hookrightarrow \operatorname{Quot} R$ mit der Anordnung verträglich alias monoton wachsend ist. Speziell erhalten wir so die übliche Anordnung auf $\mathbb{Q} = \operatorname{Quot} \mathbb{Z}$.

Ergänzende Übung 5.6.19. 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 $f : K \to K \sqcup \{\infty\}$ auf, so entspricht $(1/f)$ der Abbildung $a \mapsto f(a)^{-1}$, wenn wir $0^{-1} = \infty$ und $\infty^{-1} = 0$ vereinbaren.

Übung 5.6.20. 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 $n = \max(\operatorname{grad} g, \operatorname{grad} h)$ Stellen für $f = g/h$ eine unkürzbare Darstellung als Quotient zweier Polynome. In anderen Worten haben unter $f : D(f) \to K$ fast alle Punkte $a \in K$ genau n Urbilder.

Übung 5.6.21. 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 $a_n \to \infty$ und $P(a_n) \in \mathbb{Z}$ für alle n, so ist P bereits ein Polynom $P \in \mathbb{Q}[X]$.

Übung 5.6.22. Sei K ein Köper 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 5.6.23. 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 [AN1] 5.1.19 explizit angegeben werden, aber das sieht man leichter mit den Methoden der Analysis.

Übung 5.6.24. Man bestimme die Partialbruchzerlegung von $1/(1+X^4)$ in $\mathbb{C}(X)$.

Übung 5.6.25. 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 5.6.26. Man bearbeite nocheinmal die Übungen [GR] 1.2.10 und [GR] 1.2.11.

Übung 5.6.27 (**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 jedes $g \in K(Y) \backslash K$ zum Definitionsbereich von f und wir setzen

$$f \circ g := f(g)$$

Man zeige, daß die K-linearen Körperhomomorphismen $\varphi : K(X) \to K(Y)$ alle die Gestalt $\varphi : f \mapsto f \circ g$ haben für $g = \varphi(X) \in K(Y) \backslash K$. Sind f und g beide nicht konstant, so ist auch $f \circ g$ nicht konstant. Gegeben $f, g, h \in K(X) \backslash K$ zeige man die Assoziativität $(f \circ g) \circ h = f \circ (g \circ h)$. Unsere Abbildung $K(X) \to \operatorname{Ens}(K, K \sqcup \{\infty\}$ kann zu einer Abbildung $K(X) \to \operatorname{Ens}(K \sqcup \{\infty\})$ 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 ∞ falls der Grad von P größer ist als der von Q, und 0 falls er kleiner ist. So erhalten wir einen Monoidhomomorphismus $(K(X), \circ) \to (\operatorname{Ens}(K \sqcup \{\infty\}), \circ)$, der im Fall eines unendlichen Körpers K injektiv ist.

5.7 Quaternionen*

5.7.1. Dieser Abschnitt ist für den Rest der Vorlesung unerheblich. Allerdings gehören die Quaternionen in meinen Augen zur mathematischen Allgemeinbildung.

Definition 5.7.2. 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 5.7.3 (**Quaternionen**). *Es gibt Fünftupel* $(\mathbb{H}, \mathrm{i}, \mathrm{j}, \mathrm{k}, \kappa)$ *bestehend aus einem Ring* $\mathbb{H}$*, Elementen* $\mathrm{i}, \mathrm{j}, \mathrm{k} \in \mathbb{H}$ *und einem Ringhomomorphismus* $\kappa : \mathbb{R} \to \mathbb{H}$ *derart, daß gilt*

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$$

und $\kappa(a)q = q\kappa(a)\ \forall a \in \mathbb{R},\ q \in \mathbb{H}$ *und daß* $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ *eine Basis von* $\mathbb{H}$ *bilden für die durch die Vorschrift* $\mathbb{R} \times \mathbb{H} \to \mathbb{H}$, $(a, q) \mapsto \kappa(a)q$ *auf* $\mathbb{H}$ *gegebene Struktur als* $\mathbb{R}$*-Vektorraum. Des weiteren ist in einem derartigem Fünftupel der Ring* $\mathbb{H}$ *ein Schiefkörper.*

5.7.4. 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 $\mathrm{i}\,\mathrm{j} = \mathrm{k}$ und durch Invertieren beider Seiten weiter $\mathrm{j}\,\mathrm{i} = -\,\mathrm{k}$. Von da ausgehend erhalten wir unmittelbar die Formeln

$$\mathrm{i}\,\mathrm{j} = \mathrm{k} = -\,\mathrm{j}\,\mathrm{i}, \quad \mathrm{j}\,\mathrm{k} = \mathrm{i} = -\,\mathrm{k}\,\mathrm{j}, \quad \mathrm{k}\,\mathrm{i} = \mathrm{j} = -\,\mathrm{i}\,\mathrm{k},$$

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

$$q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$$

mit wohlbestimmten $a, b, c, d \in \mathbb{R}$. Die Abbildung $\mathbb{C} \hookrightarrow \mathbb{H}$ mit $a + b\mathrm{i}_{\mathbb{C}} \mapsto a + b\mathrm{i}$ 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 [AL] 3.12.2 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.

5.7.5. Auch die Abbildungen $\mathbb{C} \to \mathbb{H}$ mit $a+b\mathrm{i}_{\mathbb{C}} \mapsto a+b\mathrm{j}$ oder mit $a+b\mathrm{i}_{\mathbb{C}} \mapsto a+b\mathrm{k}$ 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 $\mathbb{C} \to \mathbb{H}$ gibt.

5.7.6. 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 $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$ & cut it on a stone of this bridge“.

Beweis. Bezeichne $\mathbb{H}$ die Menge aller komplexen (2×2)-Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -y \\ \bar{y} & \bar{z} \end{pmatrix} \middle| z, y \in \mathbb{C} \right\} \subset \operatorname{Mat}(2; \mathbb{C})$$

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 $z \mapsto \operatorname{diag}(z, \bar{z})$. Das Bilden der konjugierten transponierten Matrix definiert einen Antiautomorphismus $q \mapsto \bar{q}$ von $\mathbb{H}$, in Formeln $\overline{qw} = \bar{w}\bar{q}$, 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 $1_{\mathbb{C}}$, $\mathrm{i}_{\mathbb{C}}$ und den Matrizen $1 = \operatorname{diag}(1_{\mathbb{C}}, 1_{\mathbb{C}})$, $\mathrm{i} = \operatorname{diag}(\mathrm{i}_{\mathbb{C}}, -\mathrm{i}_{\mathbb{C}})$. Unser $\mathbb{H}$ hat dann über $\mathbb{R}$ die Basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ mit $\mathrm{i} := \operatorname{diag}(\mathrm{i}_{\mathbb{C}}, -\mathrm{i}_{\mathbb{C}})$ und

$$\mathrm{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } \mathrm{k} := \begin{pmatrix} 0 & \mathrm{i}_{\mathbb{C}} \\ \mathrm{i}_{\mathbb{C}} & 0 \end{pmatrix}$$

und es gilt

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1 \qquad \square$$

5.7.7. Jede zyklische Vertauschung von $\mathrm{i}, \mathrm{j}, \mathrm{k}$ liefert einen Automorphismus der Quaternionen. Die Konjugation $q \mapsto \bar{q}$ aus der im Beweis gegebenen Konstruktion hat in der Basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ die Gestalt

$$\overline{a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}} = a - b\,\mathrm{i} - c\,\mathrm{j} - d\,\mathrm{k}$$

und hat wie bereits erwähnt die Eigenschaft $\overline{qw} = \bar{w}\bar{q}$. Gegeben ein Quaternion $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ nennt man $a = (q + \bar{q})/2$ seinen **Realteil** und schreibt $a = \operatorname{Re}(q)$. Für $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ 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 (2×2)-Matrizen mit Determinante Eins. Darin enthalten ist die Untergruppe der acht Quaternionen $\{\pm 1, \pm\mathrm{i}, \pm\mathrm{j}, \pm\mathrm{k}\}$, die sogenannte **Quaternionengruppe**, von deren Multiplikationstabelle Hamilton bei seiner Konstruktion ausgegangen war.

Vorschau 5.7.8. Gegeben ein Kring R mitsamt einem selbstinversen Ringhomomorphismus $R \to R$, $r \mapsto \bar{r}$ und einem Element $v \in R$ mit $\bar{v} = v$ bildet allgemeiner die Menge aller (2×2)-Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & vy \\ \bar{y} & \bar{z} \end{pmatrix} \middle| z, y \in R \right\} \subset \operatorname{Mat}(2; R)$$

einen Teilring des Matrizenrings. Derartige Ringe heißen **Quaternionenringe**.

5.7.9. Es gibt außer der Identität nur einen $\mathbb{R}$-linearen Körperhomomorphismus $\mathbb{C} \to \mathbb{C}$, nämlich die komplexe Konjugation. Im Fall der Quaternionen liefert dahingegen jede von Null verschiedene Quaternion $q \in \mathbb{H}^\times$ einen $\mathbb{R}$-linearen Ringhomomorphismus $\operatorname{int} q : \mathbb{H} \to \mathbb{H}$, $w \mapsto qwq^{-1}$, und $\operatorname{int} q = \operatorname{int} q'$ impliziert bereits $\mathbb{R}q = \mathbb{R}q'$.

Übungen

Übung 5.7.10. Man zeige, daß es für jedes Quaternion q mit Realteil $\operatorname{Re} q = 0$ und Betrag $|q| = 1$ einen $\mathbb{R}$-linearen Ringhomomorphismus $\mathbb{C} \to \mathbb{H}$ gibt mit $\mathrm{i}_\mathbb{C} \mapsto q$.

Ergänzende Übung 5.7.11. 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-Quadrate-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 $23 = 3^2 + 3^2 + 2^2 + 1^2$.

6 Determinanten und Eigenwerte

6.1 Das Signum einer Permutation

6.1.1. Wir beginnen hier mit dem Studium der sogenannten „symmetrischen Gruppen“. Mehr dazu können Sie später in [AL] 1.5 lernen.

Definition 6.1.2. Die Gruppe aller Permutationen alias bijektiven Selbstabbildungen der Menge $\{1, 2, \ldots, n\}$ notieren wir

$$\mathcal{S}_n := \mathrm{Ens}^{\times}\{1, 2, \ldots, n\}$$

Sie heißt auch die **n-te symmetrische Gruppe**. Nach [GR] 2.3.36 hat diese Gruppe $|\mathcal{S}_n| = n!$ Elemente. Viele Autoren verwenden statt $\mathcal{S}_n$ auch die alternative Notation Σ_n. Eine Permutation, die zwei Elemente unserer Menge vertauscht und alle anderen Elemente festhält, heißt eine **Transposition**.

Definition 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

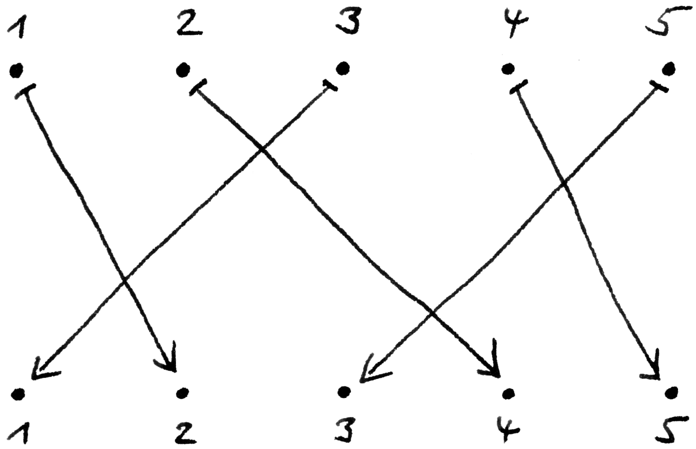
$$\mathrm{sgn}(\sigma) = (-1)^{l(\sigma)}$$

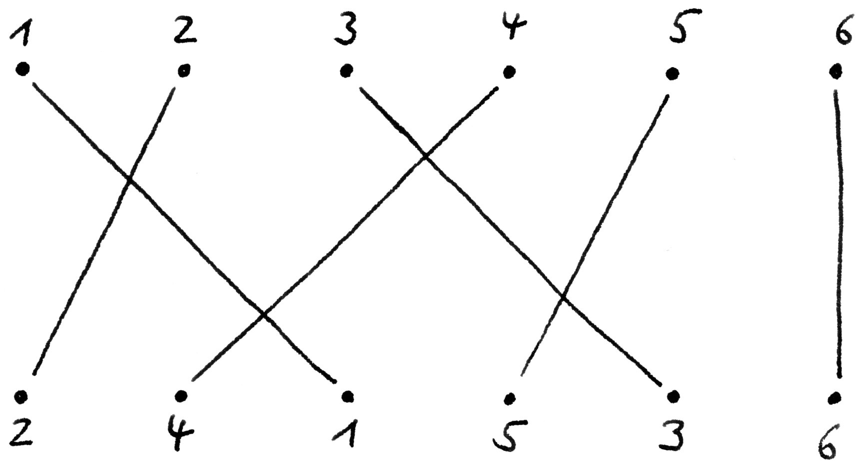
Eine Permutation mit Signum $+1$ alias gerader Länge heißt eine **gerade Permutation**, eine Permutation mit Signum -1 alias ungerader Länge eine **ungerade Permutation**.

Beispiel 6.1.4. Die Identität von $\mathcal{S}_n$ ist jeweils die einzige Permutation der Länge Null. Die Transposition, die die Zahlen i und j vertauscht, hat die Länge $2|i - j| - 1$, wie auch nebenstehendes Bild sofort zeigt, und ist also insbesondere stets ungerade.

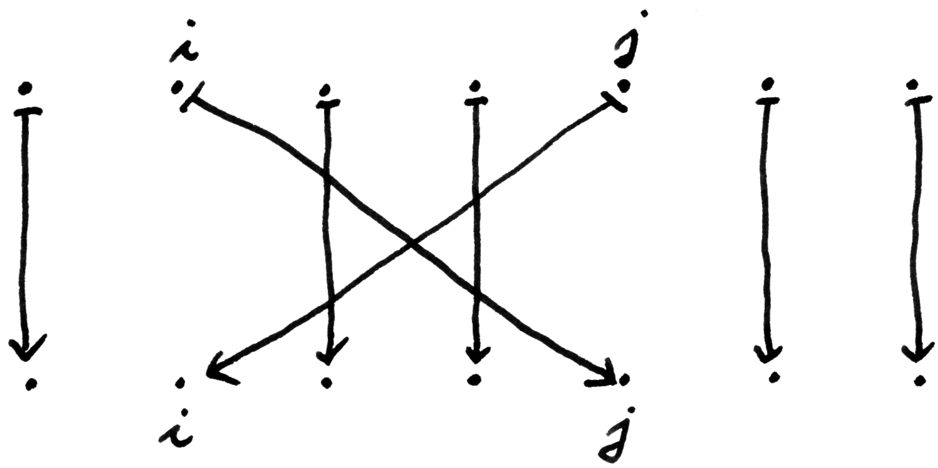
Lemma 6.1.5 (Multiplikativität des Signums). *Für jede natürliche Zahl n ist unser Signum ein Gruppenhomomorphismus $\mathrm{sgn} : \mathcal{S}_n \to \{1, -1\}$ von der symmetrischen Gruppe $\mathcal{S}_n$ in die zweielementige Gruppe der Vorzeichen, in Formeln gilt also*

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau) \quad \forall \sigma, \tau \in \mathcal{S}_n$$





Diese Bilder illustrieren zwei mögliche Anschauungen für die Länge einer Permutation, in diesem Fall der Permutation $\sigma \in \mathcal{S}_6$ 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 Verbindungslinien“. Der Leser sei ermutigt, sich auch die Produktformel für das Signum 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.

Erster Beweis. Wir vereinbaren speziell für diesen Beweis für das Vorzeichen einer von Null verschiedenen ganzen Zahl $a \in \mathbb{Z}\backslash 0$ die Notation $[a] := a/|a| \in \{1, -1\}$. Damit können wir das Signum einer Permutation σ dann auch schreiben als

$$\operatorname{sgn}(\sigma) = \prod_{i<j} [\sigma(j) - \sigma(i)]$$

Für eine beliebige weitere Permutation τ 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 τ auch die $\{\tau(j), \tau(i)\}$ für $i < j$ genau die zweielementigen Teilmengen von $\{1, \ldots, n\}$ durchlaufen, gilt für eine beliebige weitere Permutation τ 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 $\mathbb{Z}[X_1, \ldots, X_n]$ aus 5.3.29. Für jede Permutation $\sigma \in \mathcal{S}_n$ erklären wir für diesen Ring einen Ringhomomorphismus $\sigma : \mathbb{Z}[X_1, \ldots, X_n] \to \mathbb{Z}[X_1, \ldots, X_n]$ 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 6.1.6. Für jedes n bilden die geraden Permutationen als Kern eines Gruppenhomomorphismus nach [GR] 3.3.20 eine Untergruppe von $\mathcal{S}_n$. Diese Gruppe heißt die **alternierende Gruppe** und wird A_n notiert.

Übungen

Übung 6.1.7. Die Permutation $\sigma \in \mathcal{S}_n$, die i ganz nach vorne schiebt ohne die Reihenfolge der übrigen Elemente zu ändern, hat $(i-1)$ Fehlstände und folglich das Signum $\operatorname{sgn}(\sigma) = (-1)^{i-1}$.

Übung 6.1.8. Jede Permutation einer endlichen angeordneten Menge läßt sich darstellen als eine Verknüpfung von Transpositionen benachbarter Elemente.

Ergänzende Übung 6.1.9. Ist T eine endliche Menge, so gibt es genau einen Gruppenhomomorphismus

$$\operatorname{sign} : \operatorname{Ens}^\times(T) \to \{1, -1\}$$

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 $\operatorname{sign} = \operatorname{sgn}$ 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 6.1.10. Die symmetrische Gruppe $\mathcal{S}_n$ wird erzeugt von der Transposition τ 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 $\mathcal{S}_5$ wird sogar erzeugt von der „zyklischen Vertauschung“ und einer beliebigen weiteren Transposition τ. Mutige zeigen stärker: Die symmetrische Gruppe $\mathcal{S}_p$ für eine beliebige Primzahl p wird erzeugt von der „zyklischen Vertauschung“ und einer beliebigen weiteren Transposition τ.

Übung 6.1.11. Man gebe einen Gruppenisomorphismus $\mathcal{S}_3 \xrightarrow{\sim} \operatorname{GL}(2; \mathbb{F}_2)$ an.

Übung 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 $\mathcal{S}_4$ die drei Doppeltranspositionen zusammen mit dem neutralen Element eine Untergruppe bilden, die isomorph ist zur Klein'schen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6.2 Die Determinante und ihre Bedeutung

Definition 6.2.1. Sei K ein Kring und $n \in \mathbb{N}$. Die **Determinante** ist die Abbildung $\det : \operatorname{Mat}(n; K) \to K$ von den quadratischen Matrizen mit Einträgen in unserem Kring in besagten Kring selbst, die gegeben wird durch die Vorschrift

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \quad \mapsto \quad \det A := \sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

Summiert wird über alle Permutationen von n und der Vorfaktor $\operatorname{sgn}(\sigma)$ meint das Signum der Permutation σ nach 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.

6.2.2 (**Herkunft der Terminologie**). Wie wir in 6.4.2 sehen werden, bestimmt alias determiniert die Determinante, ob ein quadratisches lineares Gleichungssystem eindeutig lösbar ist. Daher rührt die Terminologie.

Beispiele 6.2.3. Wir erhalten etwa

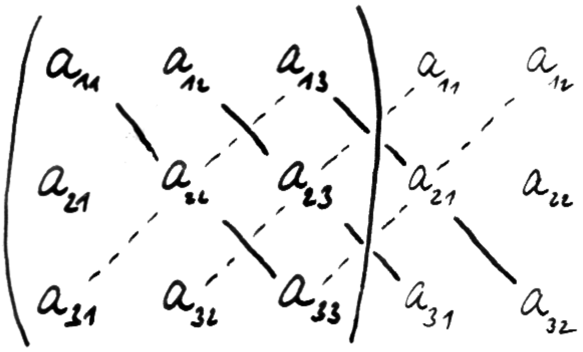
$$\begin{aligned} \det(a) &= a \\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= ad - cb \\ \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= \begin{array}{l} a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12} \end{array} \end{aligned}$$

Im Fall der (3×3)-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 6.3.9, wie man in diesen Fällen geschickter vorgehen kann.

Beispiel 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 σ mit $\sigma(i) \leq i$ für alle i, folglich trägt im Fall einer oberen Dreiecksmatrix in der Leibniz-Formel nur der Summand mit $\sigma = \mathrm{id}$ zur Determinante bei. Dasselbe gilt für untere Dreiecksmatrizen.

Lemma 6.2.5. *Die Determinante einer Matrix ändert sich nicht beim Transponieren, in Formeln*

$$\det A^\top = \det A$$



Um die Determinante einer (3×3)-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 (4×4)-Matrizen liefert aber die analoge Regel nicht mehr die Determinante!

Beweis. Per definitionem gilt $\det A^\top = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$. Ist nun $\tau = \sigma^{-1}$ die inverse Permutation, so haben wir $\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)$ 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

$$\det A^\top = \sum_{\tau \in \mathcal{S}_n} \operatorname{sgn}(\tau) a_{1\tau(1)} \dots a_{n\tau(n)} \qquad \square$$

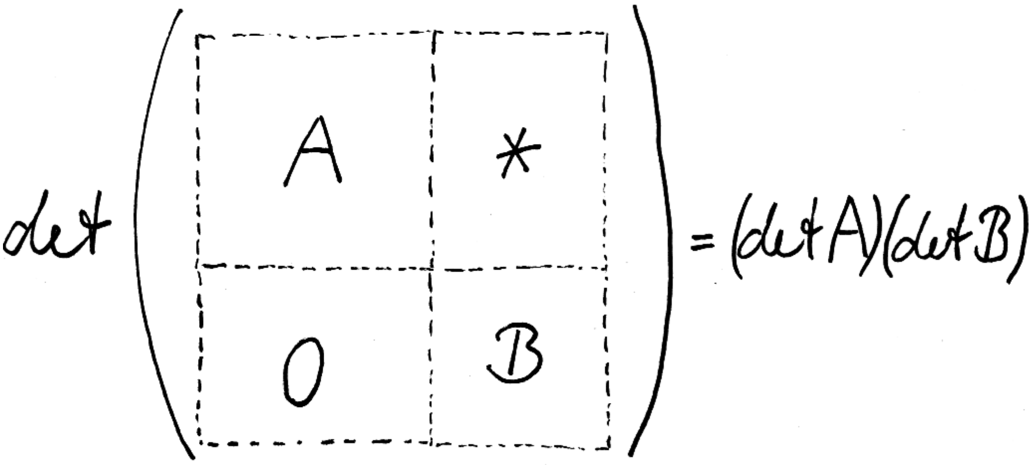
6.2.6 (**Schmutzige Anschauung: Betrag der Determinante und Volumen**). Vor der weiteren Entwicklung der Theorie will ich nun zunächst die anschauliche Bedeutung der Determinante einer Matrix mit reellen Einträgen diskutieren. Ich beginne mit der anschaulichen Bedeutung des Betrags der Determinante und beschränke mich dazu erst einmal auf den Fall $n = 2$. Hoffentlich ist anschaulich klar, daß jede lineare Abbildung $L : \mathbb{R}^2 \to \mathbb{R}^2$ 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 $\operatorname{vol}(U)$ die Fläche $\operatorname{vol}(LU) = c(L)\operatorname{vol}(U)$ hat“. Formal zeigt das die Transformationsformel [AN3] 1.10.1, 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“ $c : \operatorname{Mat}(2; \mathbb{R}) \to \mathbb{R}_{\geq 0}$ 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 $c(\operatorname{diag}(a, 1)) = c(\operatorname{diag}(1, a)) = |a|$;
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 2.5.10 jede Matrix als Produkt von Elementarmatrizen darstellen läßt, kann es höchstens eine Abbildung $c : \operatorname{Mat}(2; \mathbb{R}) \to \mathbb{R}_{\geq 0}$ geben, die diese drei Eigenschaften hat. In 6.4.1 werden wir für unsere Determinante die „Multiplikationsformel“ $\det(LM) = \det(L)\det(M)$ zeigen, und zusammen mit unserer Formel 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 Betrag der Determinante von reellen (2×2)-Matrizen. In höheren Dimensionen liefert dieselbe



Die Determinante einer block-oberen Dreiecksmatrix ist, wie Sie in Übung 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.

Argumentation analoge Resultate, insbesondere kann der Betrag der Determinante einer (3×3)-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 6.4.2 zeigen.

6.2.7 (**Schmutzige Anschauung: Determinantenvorzeichen und Drehsinn**). Das Vorzeichen der Determinante einer invertierbaren reellen (2×2)-Matrix zeigt anschaulich gesprochen an, „ob die dadurch gegebene lineare Selbstabbildung der Ebene $\mathbb{R}^2$ den Drehsinn erhält oder umkehrt". Diese Erkenntnis wird vielleicht am ehesten durch die Aussage [AN2] 5.5.16 formalisiert, nach der die „Wegzusammenhangskomponente des neutralen Elements" in der $\mathrm{GL}(n; \mathbb{R})$ genau aus allen Matrizen mit positiver Determinante besteht. Im Fall allgemeiner angeordneter Körper wird diese anschauliche Erkenntnis ihrerseits unsere Definition 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 $\varepsilon : \mathrm{GL}(2; \mathbb{R}) \to \{1, -1\}$ 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 $\varepsilon(\mathrm{diag}(a, 1)) = \varepsilon(\mathrm{diag}(1, a)) = a/|a|$;

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 2.5.10 jede invertierbare Matrix als Produkt von invertierbaren Elementarmatrizen darstellen läßt, kann es höchstens eine Abbildung $\varepsilon : \mathrm{GL}(2; \mathbb{R}) \to \{1, -1\}$ geben, die diese drei Eigenschaften hat. In 6.4.1 werden wir die „Multiplikationsformel“ $\det(LM) = \det(L)\det(M)$ für unsere Determinante zeigen, und zusammen mit unserer Formel 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 beendet unsere heuristische Argumentation für die Stichhaltigkeit der Anschauung $\det M/|\det M| = \varepsilon(L)$ für das Vorzeichen der Determinante von invertierbaren (2×2)-Matrizen. In höheren Dimensionen liefert eine analoge Argumentation analoge Resultate. So zeigt etwa das Vorzeichen der Determinante einer invertierbaren Abbildung $L : \mathbb{R}^3 \to \mathbb{R}^3$ an, ob sie die „Händigkeit“ erhält oder vielmehr „Rechtsgewinde und Linksgewinde vertauscht“.

Ergänzung 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 $180°$-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 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 6.2.4.

Übung 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.

6.3 Charakterisierung der Determinante

Definition 6.3.1. Seien V, U Vektorräume über einem Körper K. Eine bilineare Abbildung $F : V \times V \to U$ heißt **symmetrisch**, wenn gilt

$$F(v, w) = F(w, v) \quad \forall v, w \in V$$

Eine bilineare Abbildung $F : V \times V \to U$ heißt **alternierend**, wenn gilt

$$F(v, v) = 0 \quad \forall v \in V$$

6.3.2 (**Herkunft der Bezeichnung „alternierend“**). Gegeben eine bilineare Abbildung $F : V \times V \to U$ mit der Eigenschaft $F(v,v) = 0 \quad \forall v \in V$, die also im Sinne unserer Definition 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 $F(v,w) = -F(w,v)\ \forall v,w \in V$, 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 $\operatorname{char} K \neq 2$, so folgt daraus auch wieder $F(v,v) = 0$.

6.3.3. Man mag eine bilineare Abbildung $F : V \times V \to U$ **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 6.3.4. Seien $V_1, \ldots, V_n, W$ Vektorräume über einem Körper K. Eine Abbildung $F : V_1 \times \ldots \times V_n \to W$ heißt **multilinear** genau dann, wenn für alle j und alle für $i \neq j$ beliebig aber fest gewählten $v_i \in V_i$ die Abbildung $V_j \to W$, $v_j \mapsto F(v_1, \ldots, v_j, \ldots, v_n)$ linear ist. Für die Menge aller derartigen multilinearen Abbildungen verwenden wir die Notation

$$\operatorname{Hom}^{(n)}(V_1 \times V_2 \times \ldots \times V_n, W)$$

Im Fall $n = 2$ erhalten wir unsere bilinearen Abbildungen aus 2.3.8, im Fall $n = 1$ unsere linearen Abbildungen. Im Fall $n = 0$ verwenden wir die Notation $\operatorname{Hom}^{(0)}(\{*\}, W)$ für die Menge aller 0-multilinearen Abbildungen vom leeren Produkt nach W alias aller beliebigen Abbildungen von der einelementigen Menge $\operatorname{ens} = \{*\}$ nach W. Das Auswerten bei $*$ liefert damit eine Bijektion $\operatorname{Hom}^{(0)}(\{*\}, W) \xrightarrow{\sim} W$. Wir werden sie in der Notation oft so behandeln, als seien diese Mengen schlicht gleich.

Definition 6.3.5. Seien V, W Vektorräume über einem Körper K. Eine multilineare Abbildung $F : V \times \ldots \times V \to W$ heißt **alternierend** genau dann, wenn sie auf jedem n-Tupel verschwindet, in dem zwei Einträge übereinstimmen, wenn also in Formeln gilt

$$(\exists i \neq j \text{ mit } v_i = v_j) \quad \Rightarrow \quad F(v_1, \ldots, v_i, \ldots, v_j, \ldots v_n) = 0$$

Wir verwenden für den Raum aller derartigen alternierenden multilinearen Abbildungen die Notation $\mathrm{Alt}^n(V, W)$. Ist $W = K$ der Grundkörper, so sprechen wir von **Multilinearformen** und verwenden die abkürzende Notation $\mathrm{Alt}^n(V) := \mathrm{Alt}^n(V, K)$.

6.3.6. Sei $F : V \times \ldots \times V \to W$ eine alternierende multilineare Abbildung. Mit 6.3.2 folgt, daß sich das Vorzeichen von F ändert, wann immer man zwei Einträge vertauscht, in Formeln

$$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -F(v_1, \ldots, v_j, n \ldots, v_i, \ldots, v_n)$$

Im Fall eines Grundkörpers einer von Zwei verschiedenen Charakteristik erhält man wieder mit 6.3.2 auch die umgekehrte Implikation.

Satz 6.3.7 (Charakterisierung der Determinante). *Ist K ein Körper, so ist die Determinante die einzige Abbildung* $\det : \mathrm{Mat}(n; K) \to K$, *die multilinear und alternierend ist als Funktion der n Spaltenvektoren und die der Einheitsmatrix die Eins zuordnet.*

Beweis. Daß unsere in 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 $a_{1\sigma(1)} \ldots a_{n\sigma(n)} = a_{1\tau\sigma(1)} \ldots a_{n\tau\sigma(n)}$ und $\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\tau\sigma)$, 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 $d : \mathrm{Mat}(n; K) \to K$ mit den besagten Eigenschaften gibt. Nach 6.3.10 ist nun eine multilineare Abbildung festgelegt und festlegbar durch ihre Werte auf Tupeln von Basisvektoren. Insbesondere kennen wir aber unsere multilineare Abbildung d bereits, wenn wir ihre Werte

$$d(\mathrm{e}_{\sigma(1)} | \ldots | \mathrm{e}_{\sigma(n)})$$

kennen für alle Abbildungen $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Ist d zusätzlich alternierend, so gilt $d(\mathrm{e}_{\sigma(1)} | \ldots | \mathrm{e}_{\sigma(n)}) = 0$, falls σ nicht injektiv ist, und für jede Transposition τ haben wir $d(\mathrm{e}_{\sigma\tau(1)} | \ldots | \mathrm{e}_{\sigma\tau(n)}) = -d(\mathrm{e}_{\sigma(1)} | \ldots | \mathrm{e}_{\sigma(n)})$. Da nach 6.1.8 die Transpositionen die symmetrische Gruppe erzeugen, folgt daraus

$$d(\mathrm{e}_{\sigma(1)} | \ldots | \mathrm{e}_{\sigma(n)}) = \begin{cases} \mathrm{sgn}(\sigma) d(\mathrm{e}_1 | \ldots | \mathrm{e}_n) & \sigma \in \mathcal{S}_n; \\ 0 & \text{sonst.} \end{cases}$$

Erfüllt d dann auch noch unsere Bedingung $d(\mathrm{e}_1 | \ldots | \mathrm{e}_n) = 1$ für die Determinante der Einheitsmatrix, so folgt sofort $d = \det$. $\square$

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 $d : \mathrm{Mat}(n; K) \to K$, die multilinear und alternierend ist als Funktion der n Spaltenvektoren, die Formel

$$d = d(\mathrm{e}_1 | \ldots | \mathrm{e}_n) \det$$

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.

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 6.3.7 ja nicht, und vertauschen wir zwei Zeilen, so ändert sich nur ihr Vorzeichen. Bei einer Matrix in Zeilenstufenform ist dann nach 6.2.4 die Determinante schlicht das Produkt der Diagonaleinträge.

Übungen

Übung 6.3.10. Gegeben Vektorräume $V_1, V_2, \ldots, V_n, W$ über einem festen Körper bezeichne $\mathrm{Hom}^{(n)}(V_1 \times V_2 \times \ldots \times V_n, W)$ die Menge aller multilinearen Abbildungen $V_1 \times V_2 \times \ldots \times V_n \to W$. Man zeige: Ist $B_i \subset V_i$ jeweils eine Basis, so liefert die Restriktion eine Bijektion

$$\mathrm{Hom}^{(n)}(V_1 \times \ldots \times V_n, W) \xrightarrow{\sim} \mathrm{Ens}(B_1 \times \ldots \times B_n, W)$$

Jede multilineare Abbildung ist also festgelegt und festlegbar durch die Bilder von Tupeln von Basisvektoren. Den Spezialfall $n = 1$ kennen wir bereits aus 2.3.2, den Spezialfall $n = 2$ aus 2.3.9, im Fall $n = 0$ ist die Aussage eh tautologisch.

Übung 6.3.11. Gegeben ein Körper K und ein K-Vektorraum der endlichen Dimension $\dim V = n \geq 0$ ist der Raum der alternierenden multilinearen Abbildungen $V^n \to K$ eindimensional.

Übung 6.3.12 (**Multiverknüpfung multilinearer Abbildungen**). Man zeige: Gegeben ein Körper K und natürliche Zahlen $n \geq 0$ und $m(1), \ldots, m(n) \geq 0$ und K-Vektorräume $W, V_1, \ldots, V_n, U_{1,1}, \ldots U_{1,m(1)}, \ldots, U_{n,m(n)}$ und multilineare Abbildungen $f : V_1 \times \ldots \times V_n \to W$ sowie $g_i : U_{i,1} \times \ldots \times U_{i,m(i)} \to V_i$ ist auch die Abbildung $f \circ (g_1 \times \ldots \times g_n)$ vom Produkt der $U_{i,j}$ nach W multilinear. Oder nein, das ist scheußlich auszuschreiben: Man behandle nur den Fall $n = 3$, $m(1) = m(2) = 2$, $m(3) = 0$.

6.4 Rechenregeln für Determinanten

Satz 6.4.1 (Multiplikativität der Determinante). *Sei K ein Kring. Gegeben quadratische Matrizen $A, B \in \mathrm{Mat}(n; K)$ gilt*

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

Erster Beweis. Wir notieren $\mathcal{T}_n := \mathrm{Ens}(\{1, \ldots, n\})$ die Menge aller Abbildungen $\kappa : \{1, \ldots, n\} \to \{1, \ldots, n\}$ und rechnen

$$\begin{aligned}
\det(AB) &= \textstyle\sum_\sigma \mathrm{sgn}(\sigma) \prod_i (AB)_{i\sigma(i)} \\
&= \textstyle\sum_\sigma \mathrm{sgn}(\sigma) \prod_i \sum_j a_{ij} b_{j\sigma(i)} \\
&= \textstyle\sum_{\sigma \in \mathcal{S}_n,\, \kappa \in \mathcal{T}_n} \mathrm{sgn}(\sigma) a_{1\kappa(1)} b_{\kappa(1)\sigma(1)} \ldots a_{n\kappa(n)} b_{\kappa(n)\sigma(n)} \\
&= \textstyle\sum_{\kappa \in \mathcal{T}_n} a_{1\kappa(1)} \ldots a_{n\kappa(n)} \sum_{\sigma \in \mathcal{S}_n} \mathrm{sgn}(\sigma) b_{\kappa(1)\sigma(1)} \ldots b_{\kappa(n)\sigma(n)} \\
&= \textstyle\sum_{\kappa \in \mathcal{T}_n} a_{1\kappa(1)} \ldots a_{n\kappa(n)} \det(B_\kappa)
\end{aligned}$$

wo B_κ diejenige Matrix bezeichnet, deren Zeilen der Reihe nach die Zeilen mit den Indizes $\kappa(1), \ldots, \kappa(n)$ der Matrix B sind. Aus 6.3.7 folgt aber $\det B_\kappa = 0$ falls $\kappa \notin \mathcal{S}_n$ und $(\det B_\kappa) = \mathrm{sgn}(\kappa)(\det B)$ falls $\kappa \in \mathcal{S}_n$. Damit erhalten wir dann $\det(AB) = (\det A)(\det B)$ wie gewünscht. □

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 2.5.10 jede Matrix ein Produkt von Elementarmatrizen ist. □

Dritter Beweis im Körperfall. Man hält die Matrix A fest und betrachtet die beiden Abbildungen $\mathrm{Mat}(n; K) \to K$ 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 6.3.8 folgt damit unmittelbar, daß unsere beiden Abbildungen übereinstimmen. □

Vierter Beweis im Körperfall. Im Rahmen der allgemeinen Theorie der Multilinearformen geben wir einen alternativen Beweis in [AN2] 6.1.16 sowie ähnlich aber in einem noch größeren Rahmen in [LA2] 7.8.14. □

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. □

Satz 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 $A \in \mathrm{Mat}(n; K)$ also

$$\det A \neq 0 \quad \Leftrightarrow \quad A \text{ invertierbar}$$

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 $a_{*1} = \lambda_2 a_{*2} + \ldots + \lambda_n a_{*n}$. Dann folgt mit den Eigenschaften multilinear und alternierend jedoch

$$\begin{aligned}
\det A &= \det(\lambda_2 a_{*2} + \ldots + \lambda_n a_{*n} | a_{*2} | \ldots | a_{*n}) \\
&= \lambda_2 \det(a_{*2} | a_{*2} | \ldots | a_{*n}) \ + \ldots + \ \lambda_n \det(a_{*n} | a_{*2} | \ldots | a_{*n}) \\
&= \lambda_2 0 + \ldots + \lambda_n 0 \\
&= 0
\end{aligned}$$

Damit ist auch die andere Implikation $\Rightarrow$ gezeigt. □

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 3.5.10 gilt für einen Endomorphismus $f : V \to V$ 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 $T = {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ 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 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**

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

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

$$a_{*1} = a_{11}\mathrm{e}_1 + \ldots + a_{n1}\mathrm{e}_n$$

Die Multilinearität der Determinante liefert sofort die erste Gleichung der Gleichungskette

$$\det A = \sum_{i=1}^{n} a_{i1} \det(\mathrm{e}_i|a_{*2}|\dots|a_{*n}) = \sum_{i=1}^{n} a_{i1}(-1)^{i-1} \det A\langle i, 1\rangle$$

Die zweite Gleichung sehen wir ein, indem wir in der Matrix $(\mathrm{e}_i|a_{*2}|\dots a_{*n})$ die i-te Zeile ganz nach oben schieben, ohne die Reihenfolge der übrigen Zeilen zu ändern, um dann die Formel 6.2.9 für die Determinante von Block-oberen-Dreiecksmatrizen anzuwenden. □

Satz 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* $A^\sharp_{ij} = (-1)^{i+j} \det A\langle j,i\rangle$ *für* $A\langle j,i\rangle$ *die entsprechende Streichmatrix nach 6.4.4, so gilt*

$$A \circ A^\sharp = (\det A) \cdot I$$

6.4.7 (**Diskussion der Terminologie**). Diese adjunkte Matrix ist nicht zu verwechseln mit der adjungierten Abbildung aus [LA2] 1.9.5, 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.

6.4.8. Meist versteht man unter der **Cramer'schen Regel** die Formel

$$x_i = \frac{\det(a_{*1}|\ldots|b_*|\ldots|a_{*n})}{\det(a_{*1}|\ldots|a_{*i}|\ldots|a_{*n})}$$

für die Lösung des Gleichungssystems $x_1 a_{*1} + \ldots + x_i a_{*i} \ldots + x_n a_{*n} = b_*$, 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 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. □

Korollar 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.*

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 polynomialen Einträgen, wenn ihre Determinante ein von Null verschiedenes konstantes Polynom ist.

Beweis. Sei K unser Kring. Gegeben Matrizen $A, B \in \mathrm{Mat}(n; K)$ 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 6.4.6 die Formel $B = (\det A)^{-1} A^\sharp$ eine Matrix $B \in \mathrm{Mat}(n; K)$ mit $AB = I$. Indem wir dies Argument auf die transponierte Matrix anwenden und das Resultat wieder transponieren, finden wir auch $C \in \mathrm{Mat}(n; K)$ mit $CA = I$. Durch Multiplizieren der zweiten Gleichung mit B von rechts folgt sofort $B = C$, folglich ist A in der Tat invertierbar in $\mathrm{Mat}(n; K)$ im Sinne von [GR] 3.2.2. □

Übungen

Übung 6.4.11. Gegeben Endomorphismen f, g eines endlichdimensionalen Vektorraums gilt $\det(fg) = (\det f)(\det g)$.

Ergänzende Übung 6.4.12. Man zeige die Formel für die **van-der-Monde-Determinante**

$$\det \begin{pmatrix} 1 & X_0 & X_0^2 & \dots & X_0^n \\ \vdots & & & & \vdots \\ 1 & X_n & X_n^2 & \dots & X_n^n \end{pmatrix} = \prod_{0 \le j < i \le n} (X_i - X_j)$$

Hinweis: Ich empfehle, vom Nullstellensatz für Hyperebenen 5.4.5 und dem Fall des Grundkörpers $\mathbb{Q}$ auszugehen.

Übung 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 $\mathrm{Mat}(m \times n; K)$ sind genau diejenigen Matrizen, bei denen alle r-Minoren verschwinden.

Ergänzende Übung 6.4.14. Jeder komplexe Vektorraum V kann auch als reeller Vektorraum aufgefaßt werden. Man zeige im endlichdimensionalen Fall die Formel $\det_{\mathbb{R}}(f|V) = |\det_{\mathbb{C}}(f|V)|^2$.

Ergänzende Übung 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

$$\det B = \det\left(\sum_{\sigma\in\mathcal{S}_n} \operatorname{sgn}(\sigma) A_{1\sigma(1)} \dots A_{n\sigma(n)}\right)$$

Hinweis: Ist A_{11} die Einheitsmatrix, so folgt die Behauptung durch Nullen der ersten Blockspalte und Induktion. Ist $\det A_{11}$ ein Nichtnullteiler unseres Krings R, 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 kein Nullteiler ist. Nachher setze man dann $X = 0$.

Übung 6.4.16 (**Determinante geeignet geblockter Matrizen, Variante**). Man zeige dieselbe Formel wie in 6.4.15 auch für den Fall, daß die Matrizen A_{ij} alle obere Dreiecksmatrizen sind. Hinweis: Wir betrachten diejenige Abbildung

$$f : \{1, \dots, mn\} \to \{1, \dots, m\}$$

die verträglich ist mit der Restklassenabbildung beider Mengen auf $\mathbb{Z}/m\mathbb{Z}$, und beachten, daß für eine Permutation $\sigma \in \mathcal{S}_{mn}$ mit $f(\sigma(i)) \leq f(i)\ \forall i$ notwendig Gleichheit gilt für alle i.

Ergänzende Übung 6.4.17 (**Satz von Hensel**). Seien K ein Körper und $\varphi : \mathrm{GL}(n; K) \to K^\times$ ein Gruppenhomomorphismus. Man zeige, daß es einen Gruppenhomomorphismus $\alpha : K^\times \to K^\times$ 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 $CAC^{-1} = B$.

6.5 Algebraische Orientierung

6.5.1. Wir verwandeln unsere anschauliche Interpretation 6.2.7 des Vorzeichens der Determinante nun 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 6.5.2. Eine **Orientierung** eines endlichdimensionalen Vektorraums V über einem angeordneten Körper ist eine Vorschrift ε, 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

$$\varepsilon(\mathcal{A})\varepsilon(\mathcal{B}) = \operatorname{sign}(\det {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}})$$

Das Vorzeichen $\varepsilon(\mathcal{A})$ nennen wir dann die **Orientierung der angeordneten Basis** $\mathcal{A}$ unseres orientierten Vektorraums. Eine angeordnete Basis der Orientierung $+1$ in einem orientierten Vektorraum nennen wir eine **positiv orientierte Basis** oder auch einfach nur eine **orientierte Basis**, angeordnete Basis der Orientierung -1 eine **negativ orientierte Basis**. Sprechen wir von der **durch eine angeordnete Basis gegebene Orientierung**, so meinen wir diejenige Orientierung, die besagter Basis das Vorzeichen $+1$ zuordnet. Ein Isomorphismus von orientierten endlichdimensionalen Vektorräumen heißt **orientierungserhaltend**, wenn er die Orientierung von angeordneten Basen erhält. Andernfalls heißt er **orientierungsumkehrend**. Gegeben ein angeordneter Körper K bezeichnen wir diejenige Orientierung des K^n als die **Standardorientierung**, die der Standardbasis das Vorzeichen $+1$ zuordnet.

Definition 6.5.3. Unter einer **Orientierung eines endlichdimensionalen affinen Raums** über einem angeordneten Körper verstehen wir eine Orientierung seines Richtungsraums. Ein Automorphismus eines endlichdimensionalen affinen Raums heißt **orientierungserhaltend** beziehungsweise **orientierungsumkehrend**, wenn sein linearer Anteil die fragliche Eigenschaft hat.

Vorschau 6.5.4. In der Topologie werden wir für endlichdimensionale reelle affine Räume eine „topologische Orientierung“ als einen Erzeuger der kompakten Kohomologie erklären. In diesem Kontext nennen wir den hier eingeführten Begriff dann eine „algebraische Orientierung“.

6.5.5. Jeder endlichdimensionale Raum über einem angeordneten Körper besitzt genau zwei Orientierungen. Das gilt insbesondere auch für jeden einpunktigen Raum: Hier verwenden wir unsere Konvention, nach der der einzige Endomorphismus des Nullvektorraums die Determinante 1 hat. Der Nullvektorraum hat eine einzige angeordnete Basis, nämlich die leere Menge mit ihrer einzigen Anordnung, und eine Orientierung des Nullvektorraums zu wählen bedeutet schlicht, das Vorzeichen auszusuchen, das dieser Basis zugeordnet werden soll.

6.5.6. Gegeben ein endlichdimensionaler Vektorraum V über einem angeordneten Körper erklären wir seine **Orientierungsmenge**

$$\operatorname{or}(V)$$

als die zweielementige Menge seiner beiden Orientierungen nach 6.5.2. Jeder Vektorraumisomorphismus $f : V \xrightarrow{\sim} W$ liefert eine Bijektion $\operatorname{or}(f) : \operatorname{or}(V) \xrightarrow{\sim} \operatorname{or}(W)$ vermittels der von f zwischen den Mengen der angeordneten Basen beider Räume induzierten Bijektion. Es gilt dann $\operatorname{or}(f \circ g) = \operatorname{or}(f) \circ \operatorname{or}(g)$ und $\operatorname{or}(\mathrm{id}) = \mathrm{id}$. Weiter gilt für jeden Automorphismus $f : V \xrightarrow{\sim} V$ offensichtlich

$$\operatorname{or}(f) = \mathrm{id}_{\operatorname{or}(V)} \;\Leftrightarrow\; (\det f) > 0$$

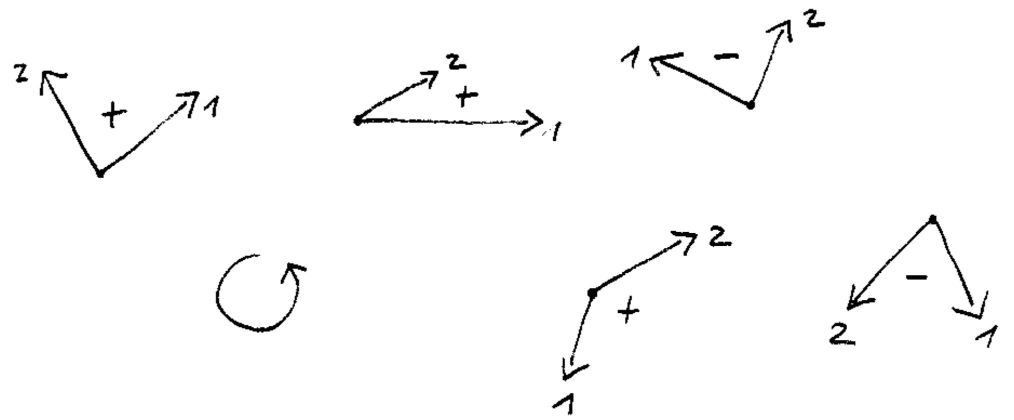
In Worten sind also die orientierungserhaltenden Automorphismen genau die mit positiver Determinante und entsprechend die orientierungsumkehrenden Automorphismen genau die mit negativer Determinante.

Bemerkung 6.5.7 (**Diskussion der Terminologie**). In der Literatur findet man vielfach eine Variante der Definition, bei der eine Orientierung eines reellen Vektorraums als eine Äquivalenzklasse von Basen unter einer geeigneten Äquivalenzrelation erklärt wird. Diese Definition liefert dasselbe in allen Fällen mit Ausnahme des Nullraums. In diesem Fall scheint mir die hier gegebene Definition, die auch dem Nullraum zwei verschiedene Orientierungen erlaubt, das sinnvollere Konzept zu liefern.

Beispiel 6.5.8. Eine Orientierung einer reellen Gerade anzugeben bedeutet anschaulich, auf dieser Gerade eine „Richtung" auszuwählen, eben die Richtung, in die diejenigen Vektoren zeigen, die positiv orientierte Basen ihres Richtungsraums bilden. Wir nennen diese Vektoren dann auch kurzerhand **positiv orientierte Vektoren** oder noch kürzer **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 **nichtnegativen Vektoren**. In [TF] 1.8.5 werden wir einen Drehsinn formal definieren als die „Auswahl eines Erzeugers der Fundamentalgruppe vom Komplement des Ursprungs". Man kann dann trefflich darüber streiten, wie natürlich die hier skizzierte Identifikation zwischen Drehsinn und Orientierung wirklich ist und ob nicht die entgegengesetzte Identifikation genauso natürlich wäre, aber alles zu seiner Zeit.

Beispiel 6.5.9 (**Die schmutzige Anschauung**). Denken wir uns die Tafelebene als einen zweidimensionalen reellen affinen Raum, so dürfen wir uns eine Orientierung der Tafelebene 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 Tafelebene 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.

Definition 6.5.10. Wir fixieren von nun an ein für allemal einen eindimensionalen



Angeordnete Basen des Raums der Richtungsvektoren der Papierebene mit den Vorzeichen, die der Orientierung „im Gegenuhrzeigersinn“ entsprechen orientierten reellen affinen Raum

$$\mathbb{T}$$

und nennen ihn die **mathematische Zeit** oder kurz **Zeit**.

6.5.11 (**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** $\mathrm{s} \in \vec{\mathbb{T}}$.

6.5.12 (**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.

6.5.13 (**Orientierung des Dualraums**). Jede Orientierung auf einem Vektorraum induziert eine Orientierung auf seinem Dualraum vermittels der Vorschrift, daß die Duale einer orientierten Basis eine orientierte Basis des Dualraums sein soll. Die Elemente des positiven Teils $\vec{\mathbb{T}}^{\top}_{>0}$ des Dualraums des Raums $\vec{\mathbb{T}}$ der Zeitspannen mag man **Frequenzen** nennen. Eine solche Frequenz ist etwa der einzige Vektor $\mathrm{s}^{\top}$ der dualen Basis zur orientierten Basis der Sekunde $\mathrm{s} \in \vec{\mathbb{T}}$. Statt $\mathrm{s}^{\top}$ schreibt man meist s^{-1} oder Hz und nennt diese Frequenz ein **Hertz** nach dem Physiker Heinrich Rudolf Hertz.

Vorschau 6.5.14 (**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 [AN2] 5.5.12 des Raums aller angeordneten Basen liegen. Man kann sich davon etwa mithilfe der Iwasawa-Zerlegung [LA2] 1.8.9 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 [AN2] 5.5.16 zeigen. Der in meinen Augen natürlichste Zugang zu diesem Resultat verwendet Methoden der Topologie und wird in [TM] **??** diskutiert.

Übungen

Ergänzende Übung 6.5.15. Gegeben eine lineare Abbildung $f : V \to W$ endlichdimensionaler Vektorräume über einem angeordneten Körper gibt es genau eine Abbildung $\operatorname{or}(\ker f) \times \operatorname{or}(\operatorname{im} f) \to \operatorname{or}(V)$, $(\varepsilon, \eta) \mapsto \varepsilon\eta$ mit der Eigenschaft, daß gegeben eine angeordnete Basis $\mathcal{A}$ des Kerns und eine angeordnete Basis $\mathcal{B}$ des Bildes und $\tilde{\mathcal{B}}$ eine Wahl von Urbildern letzterer Basisvektoren in V für die durch Hintereinanderschreiben erhaltene angeordnete Basis $(\mathcal{A}, \tilde{\mathcal{B}})$ von V gilt $(\varepsilon\eta)(\mathcal{A}, \tilde{\mathcal{B}}) = \varepsilon(\mathcal{A})\eta(\mathcal{B})$.

6.6 Eigenwerte und Eigenvektoren

Definition 6.6.1. Sei $f : V \to V$ 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

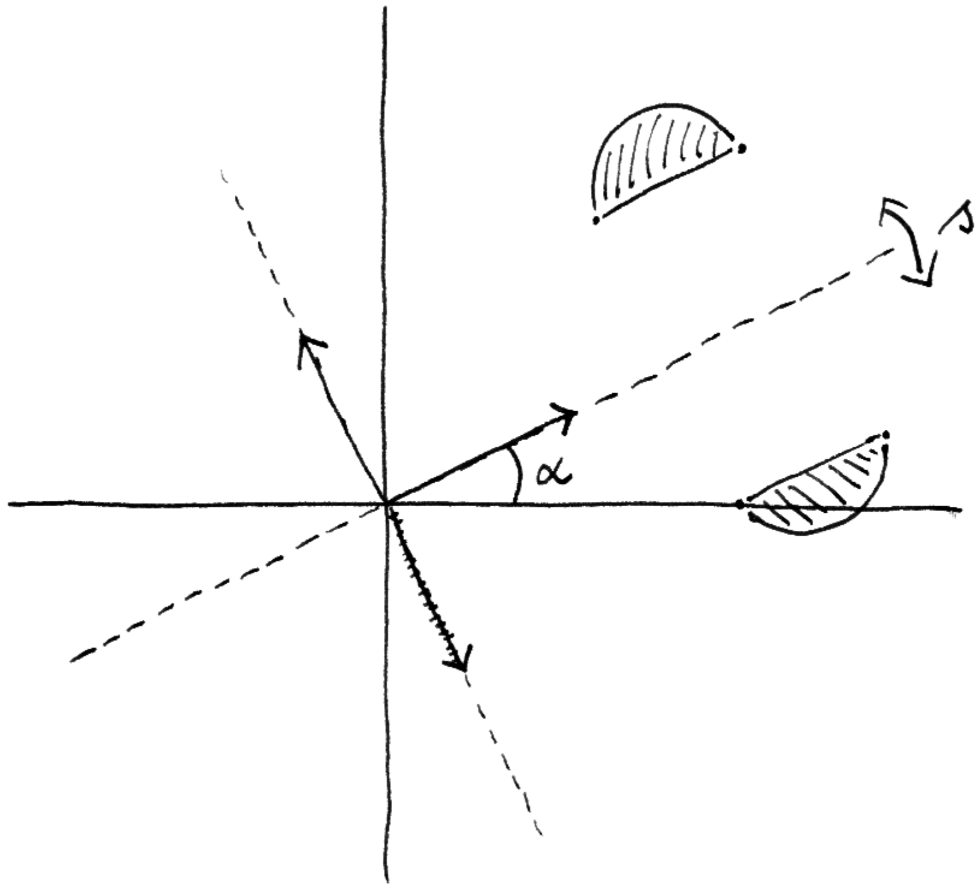
$$f(v) = \lambda v$$

Jeder derartige von Null verschiedene Vektor heißt ein **Eigenvektor von** f **zum Eigenwert** λ. Die Menge aller Eigenvektoren zum Eigenwert λ bildet zusammen mit dem Nullvektor einen Untervektorraum von V, den **Eigenraum von** f **zum Eigenwert** λ.

Beispiel 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 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 polynomialen Funktionen, ist der einzige Eigenwert die Null und die zugehörigen Eigenvektoren sind genau die von Null verschiedenen konstanten Polynome.

Satz 6.6.4 (**Existenz von Eigenwerten**). *Jeder Endomorphismus eines von Null verschiedenen endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper besitzt einen Eigenwert.*



Die anschauliche Spiegelung s an der gestrichelt einegezeichneten Achse ist eine lineare Abbildung $s : \mathbb{R}^2 \to \mathbb{R}^2$ mit den Eigenwerten ± 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 3.5 die Matrix

$$A = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

mit charakteristischem Polynom
$\chi_A(T) = (T - \cos 2\alpha)(T + \cos 2\alpha) - \sin^2 2\alpha = T^2 - 1.$

6.6.5. Auf dem $\mathbb{C}$-Vektorraum $\mathbb{C}[T]$ der Polynome besitzt der Endomorphimus „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 $0°$ und $180°$ verschiedenen Winkel 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 6.6.9.

Definition 6.6.6. Seien K ein Körper und $A \in \mathrm{Mat}(n; K)$ eine quadratische Matrix mit Koeffizienten in K. Bezeichne $\mathrm{I} \in \mathrm{Mat}(n; K)$ die Einheitsmatrix. Das Polynom $\det(A - T\mathrm{I})$ aus dem Polynomring $K[T]$ heißt das **charakteristische Polynom der Matrix** A. Es wird mit einem griechischen χ notiert in der Form

$$\chi_A(T) := \det(A - T\mathrm{I})$$

Satz 6.6.7 (Eigenwerte und charakteristisches Polynom). *Seien K ein Körper und $A \in \mathrm{Mat}(n; K)$ eine quadratische Matrix mit Koeffizienten in K. So sind die Eigenwerte des durch unsere Matrix gegebenen Homomorphismus $A : K^n \to K^n$ genau die Nullstellen ihres charakteristischen Polynoms χ_A.*

Beweis. Bezeichnet $\mathrm{I} \in \mathrm{Mat}(n; K)$ die Einheitsmatrix, so haben wir für $\lambda \in K$ die Äquivalenzen

$$\begin{array}{rcl} (\lambda \text{ ist Eigenwert von } A) & \Leftrightarrow & \exists v \neq 0 \text{ mit } Av = \lambda v \\ & \Leftrightarrow & \exists v \neq 0 \text{ mit } (A - \lambda \mathrm{I})v = 0 \\ & \Leftrightarrow & \ker(A - \lambda \mathrm{I}) \neq 0 \\ & \Leftrightarrow & \det(A - \lambda \mathrm{I}) = 0 \\ & \Leftrightarrow & \chi_A(\lambda) = 0 \end{array}$$

□

6.6.8. Es ist üblich, bei charakteristischen Polynomen die Variable mit λ zu bezeichnen. Ich werde dieser Konvention von hier an meist folgen.

6.6.9. Sei K ein Körper und $f : V \to V$ ein Endomorphismus eines endlichdimensionalen K-Vektorraums. Mit demselben Argument wie in 6.4.3 sehen wir, daß bezüglich jeder angeordneten Basis von V die darstellende Matrix von f dasselbe charakteristische Polynom hat, in Formeln $\det({}_{\mathcal{B}}[f]_{\mathcal{B}} - \lambda \,\mathrm{id}) = \det({}_{\mathcal{A}}[f]_{\mathcal{A}} - \lambda \,\mathrm{id})$ für je zwei angeordnete Basen $\mathcal{A}$ und $\mathcal{B}$ von V. Dies Polynom notieren wir dann

$$\chi_f = \chi_f(\lambda) = \mathrm{char}(f|V)$$

und nennen es das **charakteristische Polynom des Endomorphismus** f. Die Eigenwerte von f sind nach 6.6.6 genau die Nullstellen des charakteristischen Polynoms χ_f von f.

Beweis von Satz 6.6.4. Satz 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 6.6.9 auch bereits der gesuchte Eigenwert. □

6.6.10. Das charakteristische Polynom einer Block-oberen-Dreiecksmatrix ist nach 6.2.9 das Produkt der charakteristischen Polynome ihrer Blöcke auf der Diagonalen.

Proposition 6.6.11 (Trigonalisierbarkeit). *Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums $f : V \to V$ 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* **trigonalisierbar***;*

2. *Das charakteristische Polynom χ_f von f zerfällt bereits im Polynomring $K[\lambda]$ vollständig in Linearfaktoren.*

Beweis. $1 \Rightarrow 2$ ist klar nach unserer Formel 6.2.4 für die Determinante einer oberen Dreiecksmatrix: Hat ${}_{\mathcal{B}}[f]_{\mathcal{B}}$ obere Dreiecksgestalt mit Diagonaleinträgen $\lambda_1, \ldots, \lambda_n$, so haben wir ja $\chi_f(\lambda) = (\lambda_1 - \lambda) \ldots (\lambda_n - \lambda)$. 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 λ_1 von χ_A und dann nach 6.6.7 ein $c_1 \in K^n \backslash 0$ mit $Ac_1 = \lambda_1 c_1$. Ergänzen wir c_1 durch $c_2, \ldots, c_n$ zu einer Basis von K^n und betrachten die Matrix $C = (c_1 | \ldots | c_n)$, 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 6.2.9 zur Determinante von Block-oberen-Dreiecksmatrizen haben wir dann $\chi_H = (\lambda_2 - \lambda) \ldots (\lambda_n - \lambda)$ und per Induktion finden wir $F \in \mathrm{GL}(n-1; K)$ mit $F^{-1}HF$ von oberer Dreiecksgestalt. Bilden wir nun $\tilde{F} = \operatorname{diag}(1, F)$, 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. □

Proposition 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 $A \in \operatorname{Mat}(n; K)$ nilpotent genau dann, wenn gilt $\chi_A(\lambda) = (-\lambda)^n$.*

Beweis. Ist unsere Matrix nilpotent, so ist sie nach 3.5.15 konjugiert zu einer oberen Dreiecksmatrix mit Nullen auf der Diagonalen und unsere Behauptung folgt aus 6.6.10. Besteht umgekehrt das charakteristische Polynom nur aus dem Leitterm, so existiert nach 6.6.11 oder zumindest seinem Beweis eine invertierbare Matrix $B \in \operatorname{GL}(n; K)$ mit $B^{-1}AB$ von oberer Dreiecksgestalt mit Nullen auf der Diagonale. Daraus folgt jedoch unmittelbar erst $(B^{-1}AB)^n = 0$ und dann $A^n = 0$. □

Ergänzung 6.6.13. Alternative Argumente für die Rückrichtung beim Beweis der Proposition liefern der Satz von Cayley-Hamilton 6.6.20 und der Satz über die Hauptraumzerlegung [LA2] 4.2.13.

Definition 6.6.14. Seien K ein Körper und $n \in \mathbb{N}$. Eine quadratische Matrix $A \in \operatorname{Mat}(n; K)$ heißt **diagonalisierbar**, wenn es eine invertierbare Matrix $S \in \operatorname{GL}(n; K)$ gibt mit $S^{-1}AS = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ diagonal.

Definition 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 $\mathcal{B} = (v_1, \ldots, v_n)$ besitzt, für die die Matrix unserer Abbildung Diagonalgestalt hat, in Formeln ${}_{\mathcal{B}}[f]_{\mathcal{B}} = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. In der Tat bedeutet das ja gerade $f(v_i) = \lambda_i v_i$.

6.6.16 (**Diagonalisierbare Endomorphismen und ihre Matrizen**). Sei K ein Körper und $n \in \mathbb{N}$. Der durch Multiplikation mit einer Matrix $A \in \operatorname{Mat}(n; K)$ gegebene Endomorphismus des K^n ist genau dann diagonalisierbar, wenn die Matrix A diagonalisierbar ist. In der Tat, genau dann ist $v_1, \ldots, v_n$ eine Basis des K^n aus Eigenvektoren $Av_i = \lambda_i v_i$, wenn die Matrix $S = (v_1 | \ldots | v_n)$ mit den v_i in den Spalten invertierbar ist mit $S^{-1}AS = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ diagonal.

Beispiel 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 6.6.18 (Lineare Unabhängigkeit von Eigenvektoren). *Sei f ein Endomorphismus eines Vektorraums und seien $v_1, \ldots, v_n$ Eigenvektoren von f zu paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_n$. So sind unsere Eigenvektoren linear unabhängig.*

Beweis. Der Endomorphismus $(f - \lambda_2 \operatorname{id}) \ldots (f - \lambda_n \operatorname{id})$ macht $v_2, \ldots, v_n$ zu Null, nicht aber v_1. Gegeben $x_1, \ldots, x_n \in K$ mit $x_1 v_1 + \ldots + x_n v_n = 0$ folgt demnach durch Anwenden unseres Endomorphismus $x_1 = 0$. Ebenso zeigt man $x_2 = \ldots = x_n = 0$. □

Variante des Beweises. Durch Widerspruch. Sei sonst $v_1, v_2, \ldots, v_n$ ein Gegenbeispiel mit der kleinstmöglichen Anzahl von Vektoren. So gilt sicher $n \geq 2$ und gegeben eine lineare Abhängigkeit $x_1 v_1 + \ldots + x_n v_n = 0$ müssen alle x_i verschieden sein von Null. Dann aber folgte durch Anwenden von $(f - \lambda_1 \operatorname{id})$ die lineare Abhängigkeit der Vektoren $v_2, \ldots, v_n$ im Widerspruch zu unserer Annahme. □

Lemma 6.6.19 (Restriktion diagonalisierbarer Endomorphismen). *Die Restriktion eines diagonalisierbaren Endomorphismus auf einen unter besagtem Endomorphismus stabilen Teilraum ist stets wieder diagonalisierbar.*

Beweis. Sei $f : V \to V$ unser Endomorphismus und $W \subset V$ ein unter f stabiler Teilraum. Gegeben $v \in W$ haben wir nach Annahme eine Darstellung $v = v_1 + \ldots + v_n$ mit $v_i \in V$ Eigenvektoren zu paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_n \in K$. Dann gilt wegen $(f - \lambda_i \operatorname{id}) v_i = 0$ aber

$$(f - \lambda_2 \operatorname{id}) \ldots (f - \lambda_n \operatorname{id}) v = (\lambda_1 - \lambda_2) \ldots (\lambda_1 - \lambda_n) v_1 \in W$$

und folglich $v_1 \in W$. Ebenso zeigt man auch $v_2, \ldots, v_n \in W$. Mithin wird auch W von Eigenvektoren erzeugt. □

Satz 6.6.20 (Cayley-Hamilton). *Setzt man eine quadratische Matrix in ihr eigenes charakteristisches Polynom ein, so erhält man die Nullmatrix.*

Bemerkung 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 [KAG] 1.8.15 angedeutet.

Beweis mit dem Fundamentalsatz der Algebra. Wir beginnen mit dem Fall einer komplexen Matrix E. Nach 6.6.11 ist sie trigonalisierbar. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß sie bereits obere Dreiecksgestalt hat. Sind dann $\lambda_1, \ldots, \lambda_n$ ihre Diagonaleinträge und betrachten wir die von den ersten

$$\left(\left(\begin{array}{ccc|ccc|ccc}
1 & & & 2 & & & 3 & & \\
 & 1 & & & 2 & & & 3 & \\
 & & 1 & & & 2 & & & 3 \\
\hline
0 & & & 5 & & & 4 & & \\
 & 0 & & & 5 & & & 4 & \\
 & & 0 & & & 5 & & & 4 \\
\hline
7 & & & 8 & & & 6 & & \\
 & 7 & & & 8 & & & 6 & \\
 & & 7 & & & 8 & & & 6
\end{array}\right) - \left(\begin{array}{ccc|ccc|ccc}
1 & 0 & 7 & & & & & & \\
2 & 5 & 8 & & & & & & \\
3 & 4 & 6 & & & & & & \\
\hline
 & & & 1 & 0 & 7 & & & \\
 & & & 2 & 5 & 8 & & & \\
 & & & 3 & 4 & 6 & & & \\
\hline
 & & & & & & 1 & 0 & 7 \\
 & & & & & & 2 & 5 & 8 \\
 & & & & & & 3 & 4 & 6
\end{array}\right)\right)\left(\begin{array}{c}
1 \\ 0 \\ 0 \\ \hline 0 \\ 1 \\ 0 \\ \hline 0 \\ 0 \\ 1
\end{array}\right) = 0$$

$(F - fE)(\mathrm{e}_1^\top, \ldots, \mathrm{e}_n^\top)^\top = 0$ am Beispiel einer Matrix F mit drei Zeilen und Spalten. Alle nicht ausgeschriebenen Einträge der obigen Matrizen sind als Null zu verstehen.

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 5.4.3 ist es also schon selbst das Nullpolynom und der Satz folgt. □

Beweis ohne den Fundamentalsatz der Algebra. Gegeben eine quadratische Matrix A mit Koeffizienten in einem Kring gibt es nach 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

$$A^\sharp A = (\det A) \cdot E$$

für E die Einheitsmatrix. Nehmen wir speziell den Kring $K[t]$ und die Matrix $A = F - tE$ für eine vorgegebene Matrix $F \in \mathrm{Mat}(n; K)$, so erhalten wir in $\mathrm{Mat}(n; K[t])$ die Gleichung

$$A^\sharp (F - tE) = \chi_F(t) \cdot E$$

Bezeichne nun $f : K^n \to K^n$ 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 $K[t] \to \mathrm{End}_K K^n$ mit $t \mapsto f$ an, so erhalten wir in $\mathrm{Mat}(n; \mathrm{End}_K K^n)$ alias $\mathrm{Mat}(n^2; K)$ die Gleichung

$$A^\sharp (F - fE) = \chi_F(f) \cdot E$$

Betrachten wir nun die Standardbasis $\mathrm{e}_1, \ldots, \mathrm{e}_n$ aus Spaltenvektoren des K^n und wenden beide Seiten dieser Gleichung an auf den Vektor $(\mathrm{e}_1^\top, \ldots, \mathrm{e}_n^\top)^\top$, aufgefaßt als Spaltenvektor in K^{n^2}, so ergibt auf der linken Seite schon die Multiplikation mit $(F - fE)$ den Nullvektor, denn bei

$$(F - fE)(\mathrm{e}_1^\top, \ldots, \mathrm{e}_n^\top)^\top$$

steht im i-ten Block von K^{n^2} genau $F_{i1}\,\mathrm{e}_1 + \ldots + F_{in}\,\mathrm{e}_n - f(\mathrm{e}_i) = 0$. Also wird die rechte Seite auch Null und es folgt $\chi_F(f)\,\mathrm{e}_1 = \ldots = \chi_F(f)\,\mathrm{e}_n = 0$. Hier ist zwar χ_F a priori das charakteristische Polynom der zu einer Matrix von f transponierten Matrix, aber das stimmt nach 6.2.5 mit dem charakteristischen Polynom von f überein. □

Proposition* 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 $P(f) = 0$. 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 λ_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 6.6.18, ist damit $f|_E$ diagonalisierbar und v eine Summe von Eigenvektoren von f. Die Proposition folgt. □

Übungen

Übung 6.6.23. Seien K ein Körper und $A \in \mathrm{Mat}(n; K)$ eine quadratische Matrix mit Koeffizienten in K. Man zeige, daß das charakteristische Polynom von A die Gestalt

$$\chi_A(T) = (-T)^n + \mathrm{tr}(A)(-T)^{n-1} + \dots + \det(A)$$

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.

Ergänzende Übung 6.6.24. 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.

Übung 6.6.25. 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 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 $(a\cdot) : K \to K$ und deren Eigenwerte.

Ergänzende Übung 6.6.27 (**Simultane Trigonalisierbarkeit**). Man zeige: 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 Dreiecksgestalt haben. Hinweis: **??**.

Ergänzende Übung 6.6.28. 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 6.6.29. Sei ein diagonalisierbarer Endomorphismus eines vierdimensionalen Vektorraums gegeben, dessen Eigenwerte paarweise verschieden sind. Wieviele unter unserem Endomorphismus stabile Untervektorräume besitzt unser Vektorraum?

Übung 6.6.30 (**Endomorphismen, deren Quadrat die Identität ist**). Sei V ein Vektorraum über einem Körper einer von Zwei verschiedenen Charakteristik und $r : V \to V$ eine lineare Abbildung mit $r^2 = \mathrm{id}_V$. So ist r diagonalisierbar und alle seine Eigenwerte sind ± 1. Fordern wir zusätzlich $\dim V = 2$ und $r \neq \mathrm{id}_V$, 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 6.6.31 (**Jordanform für** (2×2)**-Matrizen**). Sei K ein algebraisch abgeschlossener Körper. Man zeige, daß es für jede quadratische Matrix $A \in \mathrm{Mat}(2; K)$ eine invertierbare Matrix $P \in \mathrm{GL}(2; K)$ 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 6.6.32. Gegeben zwei quadratische Matrizen A, B derselben Größe gilt $\chi_{AB} = \chi_{BA}$. Hinweis: Man erinnere beim Beweis der Multiplikativität der Determinante 6.4.1 das Argument zur Herleitung des Falls eines beliebigen Krings aus dem Körperfall.

7 Geometrische Ergänzungen*

7.1 Affine Inzidenzebenen

Definition 7.1.1. Eine Menge X von sogenannten „Punkten" mit einem System von Teilmengen $G \subset \mathcal{P}(X)$, dessen Elemente $g \in G$ wir „Geraden" nennen, heißt eine **affine Inzidenzebene** oder genauer eine **konkrete affine Inzidenzebene**, wenn gilt:

1. Gegeben $x, y \in X$ mit $x \neq y$ gibt es genau ein $g \in G$ mit $x, y \in g$ alias: Durch je zwei verschiedene Punkte geht genau eine Gerade. Wir notieren sie $\overline{xy}$;

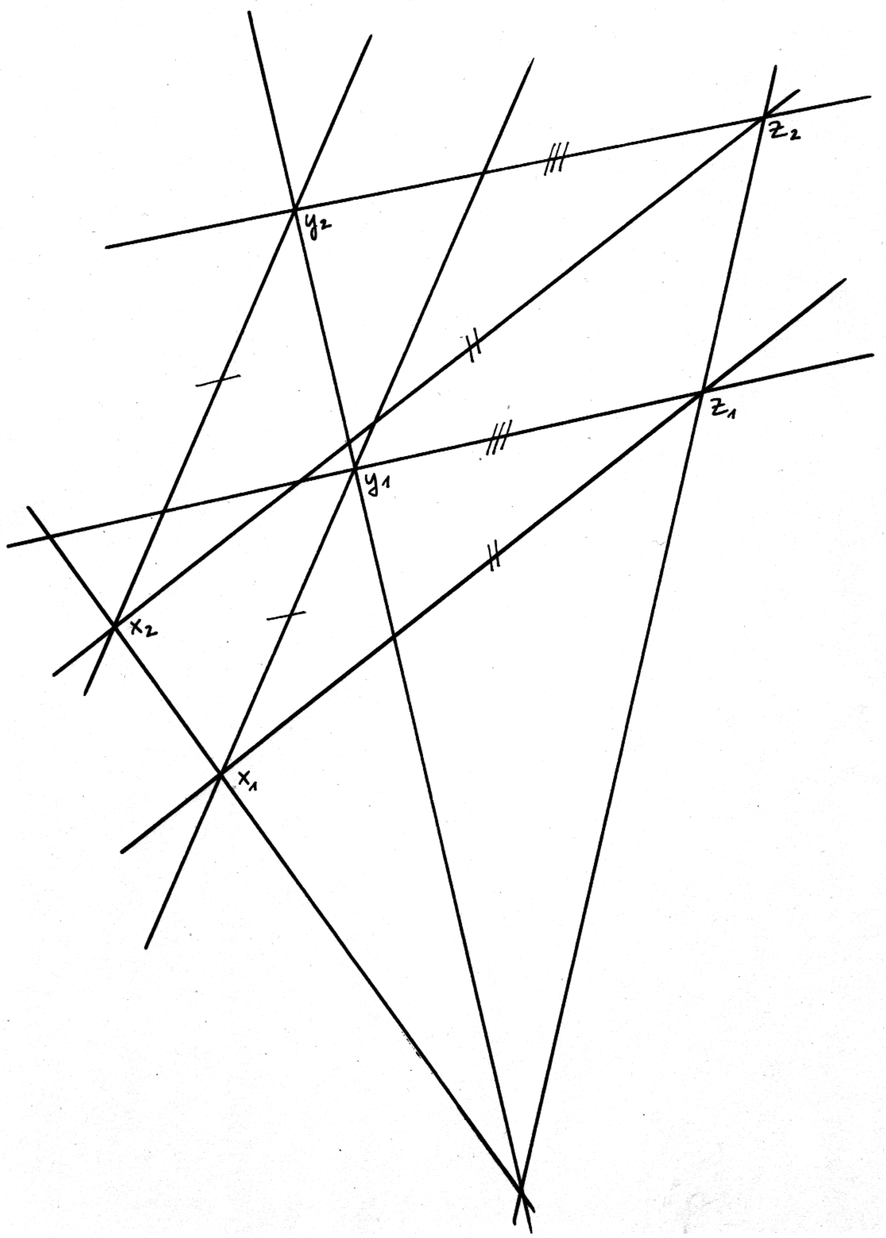
2. Gegeben $g \in G$ und $x \in X \backslash g$ gibt es genau ein $h \in G$ mit $x \in h$ und $h \cap g = \emptyset$ alias: Gegeben eine Gerade und ein Punkt außerhalb besagter Gerade gibt es genau eine Gerade durch besagten Punkt, die besagte Gerade nicht schneidet. Geraden, die sich nicht schneiden, nennt man in diesem Kontext **parallel**;

3. Es gibt $x, y, z \in X$ paarweise verschieden derart, daß kein $g \in G$ sie alle enthält alias: Es gibt drei Punkte, die nicht auf ein- und derselben Geraden liegen. Man sagt dann auch, die Punkte seien nicht **kolinear** und spricht von einem **Dreieck**.

Beispiel 7.1.2. Jeder zweidimensionale affine Raum X über einem Körper K mit $G \subset \mathcal{P}(X)$ der Menge der affinen Geraden in X bildet eine affine Inzidenzebene. Analoges gilt, wenn K nur ein Schiefkörper ist: Dann ist die Menge von Punkten $X := K^2$ mit Geraden allen Teilmengen der Gestalt $g := p + Kv$ für $p, v \in K^2$ und $v \neq (0, 0)$ eine affine Inzidenzebene, wie der Leser leicht selbst wird zeigen können. Wir nennen diese Struktur die **affine Inzidenzebene über dem Schiefkörper** K.

Beispiel 7.1.3. Im Fall des Körpers mit zwei Elementen besteht die zugehörige affine Ebene aus vier Punkten und ihre Geraden sind alle zweielementigen Teilmengen, so daß es insgesamt genau sechs Geraden gibt. Man überlegt sich leicht, daß jede affine Inzidenzebene, in der es eine Gerade mit nur einer einzigen Parallele gibt, zu dieser vierelementigen Inzidenzebene isomorph sein muß.

7.1.4. Sei (X, G) eine affine Inzidenzebene. Wir überlegen uns, daß die Relation „gleich oder parallel" eine Äquivalenzrelation auf G im Sinne von 5.5.2 sein muß, die wir im folgenden $\|$ notieren. In der Tat, haben zwei Parallelen zu einer gegebenen Geraden einen Schnittpunkt, so müssen sie beide die eindeutig bestimmte Parallele durch diesen Schnittpunkt sein.



Skizze zur affinen Desargues-Eigenschaft

Definition 7.1.5. Wir sagen, eine affine Inzidenzebene habe die **affine Desargues-Eigenschaft**, wenn gegeben drei paarweise verschiedene Geraden g_1, g_2, g_3 mit einem gemeinsamen Punkt z und für $i \in \{1, 2, 3\}$ Punkte $x_i, y_i \in g_i \backslash z$ stets gilt

$$(\overline{x_1x_2} \parallel \overline{y_1y_2} \text{ und } \overline{x_2x_3} \parallel \overline{y_2y_3}) \Rightarrow \overline{x_1x_3} \parallel \overline{y_1y_3}$$

Definition 7.1.6. Ein **Isomorphismus von affinen Inzidenzebenen** ist eine Bijektion der zugrundeliegenden Punktmengen, die eine Bijektion zwischen den jeweiligen Mengen von Geraden induziert. Zwei affine Inzidenzebenen heißen **isomorph**, wenn es zwischen ihnen einen Isomorphismus gibt.

Satz 7.1.7 (Desargues-Eigenschaft und Koordinatisierung). *Eine affine Inzidenzebene hat genau dann die affine Desargues-Eigenschaft, wenn sie isomorph ist zur affinen Ebene K^2 über einem Schiefkörper K.*

7.1.8. Dieser Satz ist in meinen Augen eine besonders schöne Illustration der innigen Beziehung zwischen Geometrie und Algebra. Wir schicken dem Beweis ein Lemma voraus.

Lemma 7.1.9. *Sei X eine affine Inzidenzebene mit der affinen Desargue-Eigenschaft. Gegeben drei paarweise verschiedene parallele Geraden g_i und Punkte $x_i, y_i \in g_i$ gilt dann*

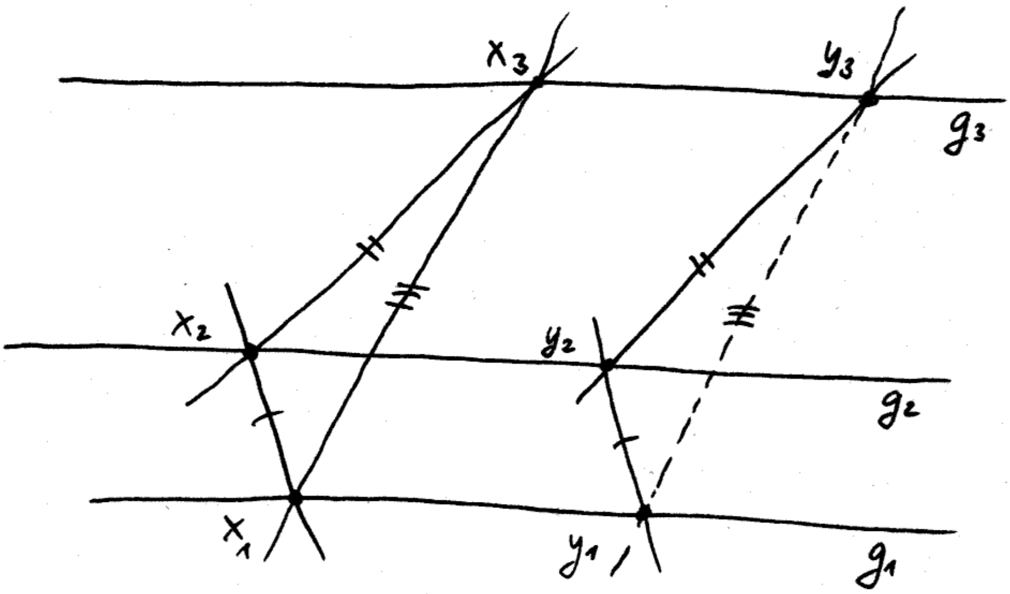
$$(\overline{x_1x_2} \parallel \overline{y_1y_2} \textit{ und } \overline{x_2x_3} \parallel \overline{y_2y_3}) \Rightarrow \overline{x_1x_3} \parallel \overline{y_1y_3}$$

Vorschau 7.1.10. Die Aussage des Lemmas kann als ein Analogon der affinen Desargues-Eigenschaft verstanden werden, bei der der Punkt z ein „unendlich ferner Punkt" ist. Im folgenden Abschnitt werden wir diese Intuition zu einer präzisen Aussage machen.

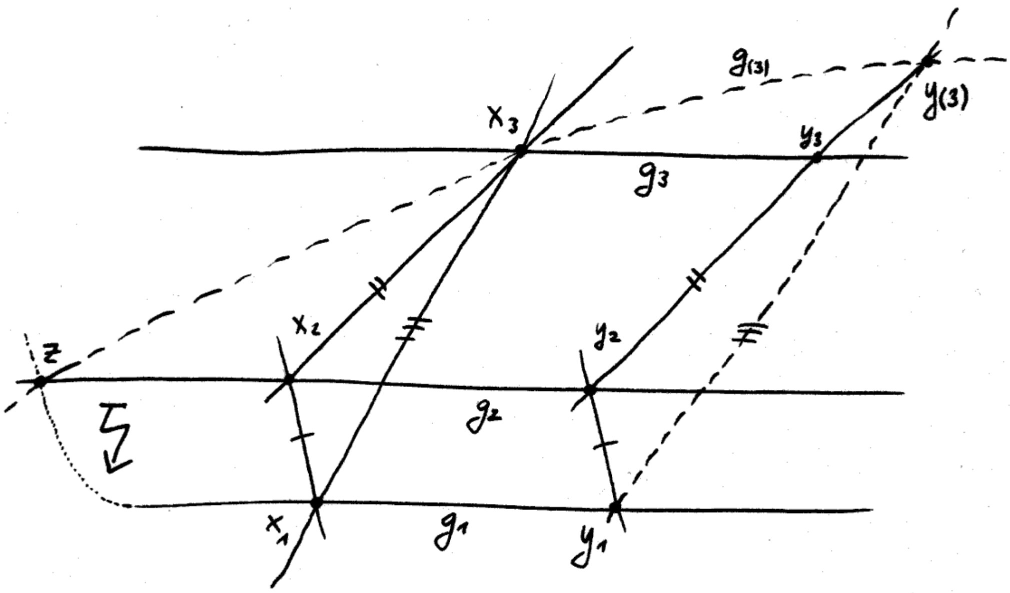
Beweis. Sind die x_i kolinear, so ist das eh klar. Anderfalls können wir $y_{(3)}$ erklären durch $\overline{x_1x_3} \| \overline{y_1y_{(3)}}$ und $y_{(3)} \in \overline{y_2y_3}$. Die Gerade $g_{(3)} := \overline{x_3y_{(3)}}$ schneidet dann g_2 in einem Punkt z, und dann müßte g_1 auch durch z gehen im Widerspruch zu unseren Annahmen. □

Beweis des Koordinatisierungssatzes 7.1.7. Im folgenden Beweis bleibt für den Leser Vieles auszuführen, das jedoch im einzelnen keine Schwierigkeiten bieten sollte. Als erste Aufgabe sei es dem Leser überlassen, zu zeigen, daß eine affine Inzidenzebene über einem Schiefkörper stets die affine Desargues-Eigenschaft hat. Um die Gegenrichtung zu zeigen, gehen wir in mehreren Schritten vor.

1. Unter einem **Parallelogramm** in einer affinen Inzidenzebene X verstehen wir ein Quadrupel von Punkten $(x_{11}, x_{12}, x_{21}, x_{22}) \in X^4$ derart, daß es Paare von



Skizze zur Aussage von Lemma 7.1.9

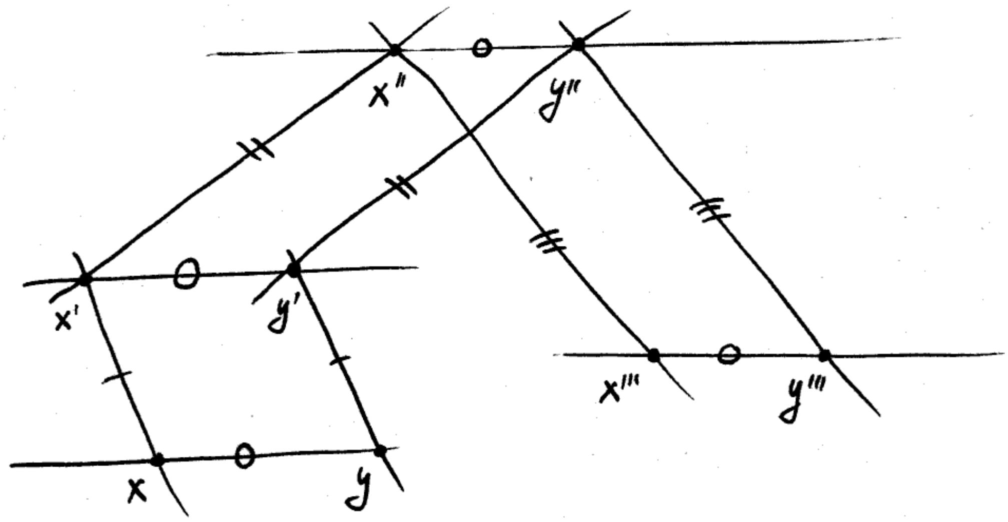


Skizze zum Beweis von Lemma 7.1.9

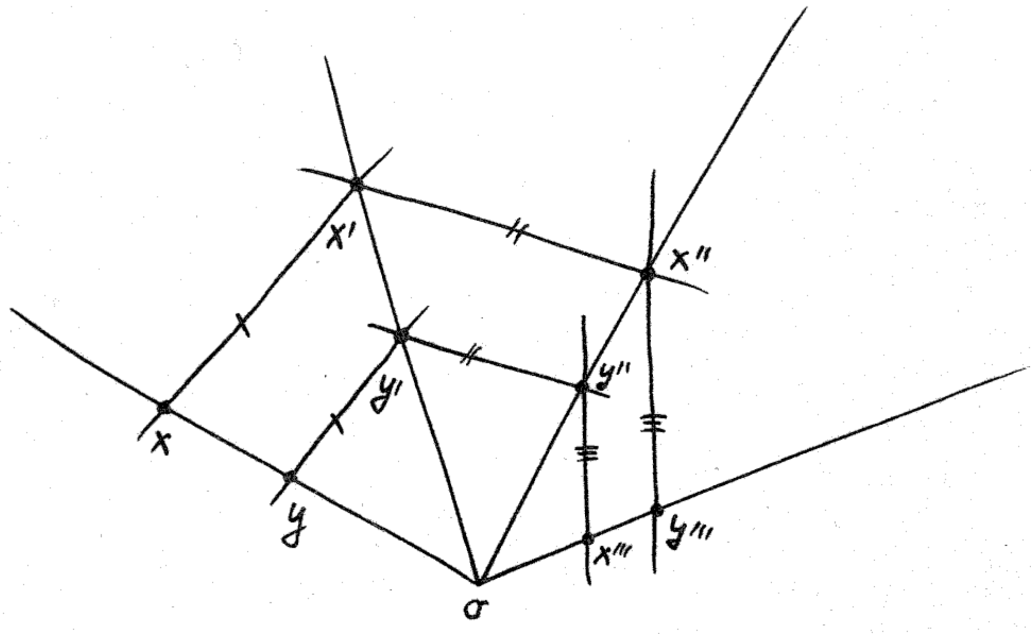
Geraden $g_1 \parallel g_2$ und $h_1 \parallel h_2$ gibt mit $h_i \nparallel g_j$ und $h_i \cap g_j = x_{ij}$. Hier verwenden wir unsere Notation $\parallel$ für „gleich oder parallel“. Gegeben eine affine Inzidenzebene X betrachten wir auf der Menge X^2 aller Punktpaare aus X die Relation $\sim$ mit $(x, y) \sim (x', y')$ genau dann, wenn unsere vier Punkte ein Parallelogramm (x, y, x', y') bilden. Diese Relation ist sicher symmetrisch und reflexiv. Bezeichne $\approx$ die davon erzeugte Äquivalenzrelation. Per definitionem gilt also $(x, y) \approx (x', y')$ genau dann, wenn es eine endliche Folge von Punktpaaren (x_i, y_i) gibt mit

$$(x, y) = (x_0, y_0) \sim \ldots \sim (x_n, y_n) = (x', y')$$

Wir überlegen uns, daß es unter Annahme der affinen Desargues-Eigenschaft im Fall $(x, y) \approx (x', y')$ auch eine derartige Folge der Länge $n \leq 2$ geben muß, und setzen dafür $g_i = \overline{x_i y_i}$. Gilt $g_i = g_{i+1}$, so folgt $(x_i, y_i) = (x_{i+1}, y_{i+1})$ und wir können unsere Folge verkürzen. Sind die Geraden g_i, g_{i+1}, g_{i+2} paarweise verschieden, so folgt aus Lemma 7.1.9 bereits $(x_i, y_i) \sim (x_{i+2}, y_{i+2})$ und wir können unsere Folge auch verkürzen. Haben wir schließlich $g_i = g_{i+2} \neq g_{i+1} = g_{i+3}$, so können wir, da der Fall der vierelementigen Ebene eh unproblematisch ist, mit 7.1.3 annehmen, daß es eine weitere Gerade g gibt mit $g \parallel g_i$ aber $g_i \neq g \neq g_{i+1}$. Es gibt dann nach Lemma 7.1.9 Punkte $x''', y''' \in g$ mit $(x_\nu, y_\nu) \sim (x''', y''')$ für $i \leq \nu \leq i + 3$ und wir können unsere Folge auch wieder verkürzen. Damit ist klar, daß wie behauptet je zwei äquivalente Paare durch eine Folge mit höchstens einem Zwischenschritt verknüpft werden können. Es folgt, daß die Äquivalenzklassen unserer Äquivalenzrelation Graphen von Abbildungen $X \to X$ sind. Die Abbildung zu einem Punktepaar (x, y) notiere ich $\overrightarrow{xy}$. Es ist klar, daß $\overrightarrow{yx}$ stets die Umkehrabbildung von $\overrightarrow{xy}$ ist. Weiter ist mit 7.1.9 klar, daß unsere Abbildungen Geraden in Geraden überführen, daß sie also Automorphismen unserer affinen Inzidenzebene sind. Und schließlich ist auch klar, daß im Fall $x \neq y$ unser $\overrightarrow{xy}$ der einzige fixpunktfreie Automorphismus φ unserer affinen Inzidenzebene ist mit $\varphi(x) = y$ und $\varphi(g) \parallel g$ für jede Gerade g. Hat nun $\overrightarrow{ub} \circ \overrightarrow{xy}$ einen Fixpunkt p, so schreiben wir $\overrightarrow{xy} = \overrightarrow{pq}$ dann ist notwendig $\overrightarrow{ub} = \overrightarrow{qp}$ die Umkehrabbildung und unsere Verknüpfung die Identität. So sehen wir, daß die Gesamtheit all unserer Abbildungen eine Gruppe von Automorphismen unserer affinen Inzidenzebene ist. Liegen $x, y, z \in X$ nicht auf einer Geraden, so folgt $\overrightarrow{xy} \circ \overrightarrow{yz} = \overrightarrow{yz} \circ \overrightarrow{xy}$ leicht aus den Definitionen. Gilt $x = y$, so ist das eh klar. Sonst wählen wir w außerhalb der besagten Geraden und haben $\overrightarrow{xy} = \overrightarrow{wy} \circ \overrightarrow{xw}$. So sehen wir, daß unsere Gruppe kommutativ sein muß. Wir schreiben ihre Verknüpfung von nun an $+$ und bezeichnen unsere Gruppe als $\vec{X}$ nennen ihre Elemente **Richtungsvektoren**. Für das weitere bemerken wir noch, daß jeder Isomorphismus $\varphi : X \xrightarrow{\sim} Y$ von affinen Desargues-Ebenen offensichtlich einen Isomorphismus $\vec{\varphi} : \vec{X} \xrightarrow{\sim} \vec{Y}$ zwischen den zugehörigen Gruppen von Richtungsvektoren induziert mit



Skizze zur Äquivalenzrelation durch iterierte Parallelogramme



Skizze zur Äquivalenzrelation durch iterierte o-Trapeze

$$\vec{\varphi} : \overrightarrow{xy} \mapsto \overrightarrow{\varphi(x)\varphi(y)}$$

2. Sei wieder X eine affine Inzidenzebene. Wir halten einen Punkt $o \in X$ willkürlich fest. Unter einem o-**Trapez** in $X \backslash o$ verstehen wir dann ein Quadrupel von Punkten $(x_{11}, x_{12}, x_{21}, x_{22}) \in X^4$ derart, daß es Geraden h_1, h_2 durch o und Geraden $g_1 \parallel g_2$ gibt mit $h_i \cap g_j = x_{ij}$. Nun betrachten wir auf der Menge $(X \backslash o)^2$ die Relation $\sim$ mit $(x, y) \sim (x', y')$ genau dann, wenn unsere vier Punkte (x, y, x', y') ein o-Trapez bilden. Diese Relation ist sicher symmetrisch und reflexiv. Bezeichne $\approx$ die davon erzeugte Äquivalenzrelation. Ähnlich wie zuvor zeigen wir, daß unter der Annahme der affinen Desargues-Eigenschaft ihre Äquivalenzklassen die Graphen von bijektiven Abbildungen $(X \backslash o) \xrightarrow{\sim} (X \backslash o)$ sind, und daß die Fortsetzungen unserer Bijektionen durch die Vorschrift $o \mapsto o$ die einzigen Automorphismen ψ unserer Inzidenzebene sind mit Fixpunkt o und $\psi(g) \parallel g$ für jede Gerade g. Diese Automorphismen bilden dann natürlich auch eine Gruppe von Automorphismen unserer affinen Ebene, die wir die **Homothetien mit Zentrum** o nennen und $\mathcal{H}_o = \mathcal{H}$ notieren.

3. Sei X eine affine Inzidenzebene mit der affinen Desargues-Eigenschaft. Gegeben eine Gerade $K \subset X$ und ein Punkt $o \in K$ ist die Abbildung $K \to \vec{X}$ gegeben durch $x \mapsto \overrightarrow{ox}$ offensichtlich eine Injektion und ihr Bild eine Untergruppe. Wir erklären eine Verknüpfung $+_o$ auf K durch die Vorschrift, daß sie unter unserer Injektion der Addition in $\vec{X}$ entsprechen soll. Mit dieser Verknüpfung wird $(K, +)$ offensichtlich eine abelsche Gruppe mit neutralem Element o. Ist $\varphi : X \xrightarrow{\sim} Y$ ein Isomorphismus von Inzidenzebenen, so ist $\varphi : K \xrightarrow{\sim} \varphi(K)$ offensichtlich ein Gruppenisomorphismus $\varphi : (K, +_o) \xrightarrow{\sim} (\varphi(K), +_{\varphi(o)})$.

4. Sei X eine affine Inzidenzebene mit der affinen Desargues-Eigenschaft. Gegeben eine Gerade $K \subset X$ und zwei Punkte $\imath \neq o$ in K liefert das Anwenden auf $\imath \in K$ offensichtlich eine Bijektion

$$\mathcal{H}_o \xrightarrow{\sim} K \backslash o$$

zwischen unserer Gruppe von Homothetien und dem Komplement des Punktes o in unserer Geraden K. Wir erklären dann eine Verknüpfung $\cdot$ auf $K \backslash o$ durch die Vorschrift, daß diese Bijektion ein Isomorphismus von Mengen mit Verknüpfung sein soll. Mit dieser Verknüpfung wird $K \backslash o$ offensichtlich eine Gruppe mit neutralem Element $\imath$. Da unsere Homothetien ψ Automorphismen unserer Inzidenzebene sind, die K stabilisieren und o festhalten, liefern sie Gruppenhomomorphismen $\psi : (K, +_o) \xrightarrow{\sim} (K, +_o)$. Es folgt

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

für alle $a, b \in K$ und $c \in K \backslash o$. Setzen wir die Multiplikation auf ganz K fort durch die Regeln $o \cdot a = o = a \cdot o \ \forall a \in K$, so folgt obige Distributivität sogar für alle $a, b, c \in K$.

5. Das in der nebenstehenden Grafik mit den Notationen $\imath = 1$ und $o = 0$ dargestellte Argument zeigt, daß andererseits auch gilt

$$(\imath + d)b = b + db$$

unter den Voraussetzungen $b \notin \{o, \imath\}$ und $d \notin \{o, -\imath\}$. Vorgegeben sind darin die rechte Gerade und die Punkte $o, \imath, b, d$. Dazu wird die linke Gerade durch o verschieden aber sonst willkürlich gewählt sowie der fette eingekringelte Punkt darauf verschieden vom Ursprung aber sonst willkürlich. Dann zeichnen wir die Geraden von diesem Punkt zu $\imath$ und b und die Parallele durch diesen Punkt zur rechten Ursprungsgeraden. Indem wir weitere Parallelen geeignet einzeichnen, konstruieren wir die Punkte db und $\imath + d$ und $(\imath + d)b$. Die Gültigkeit der Formel $(\imath + d)b = b + db$ entspricht dann der geometrischen Eigenschaft, daß die gestrichelte Gerade durch den nicht fetten eingekringelten Punkt läuft. Das aber stellt die affine Desargues-Eigenschaft sicher. Es ist nun leicht explizit zu sehen, daß unsere Identität $(\imath + d)b = b + db$ auch ohne alle Voraussetzungen gilt, und mit der Assoziativität der Multiplikation und der bereits gezeigten Distributivität für die Multiplikation von links folgt dann die Distributivität für die Multiplikation von rechts. Wir erkennen so, daß K mit unseren beiden Verknüpfungen ein Schiefkörper wird.

6. Die Wahl eines Elements $v \in X \backslash K$ induziert nun offensichtlich eine Bijektion

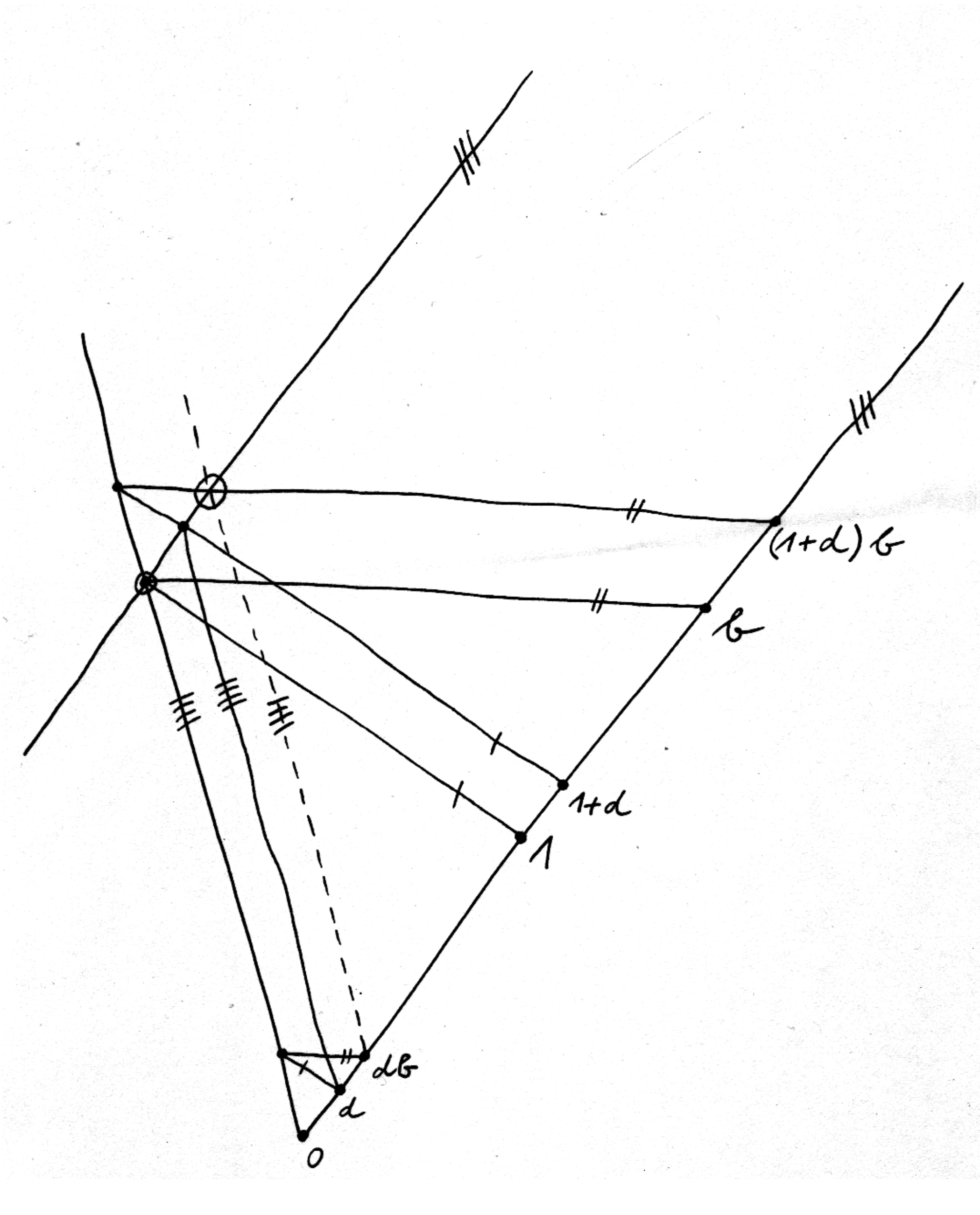
$$K^2 \xrightarrow{\sim} X$$

durch die Vorschrift, daß jedem Paar (λ, μ) der Schnittpunkt der zu K parallelen oder gleichen Geraden durch $u \cdot v$ mit der zu $\overline{ov}$ gleichen oder parallelen Geraden durch $\lambda = \lambda \cdot 1$ zugeordnet wird. Es ist dann leicht zu sehen, daß unter dieser Bijektion die Geraden von X den affinen Geraden von K^2 entsprechen. $\square$

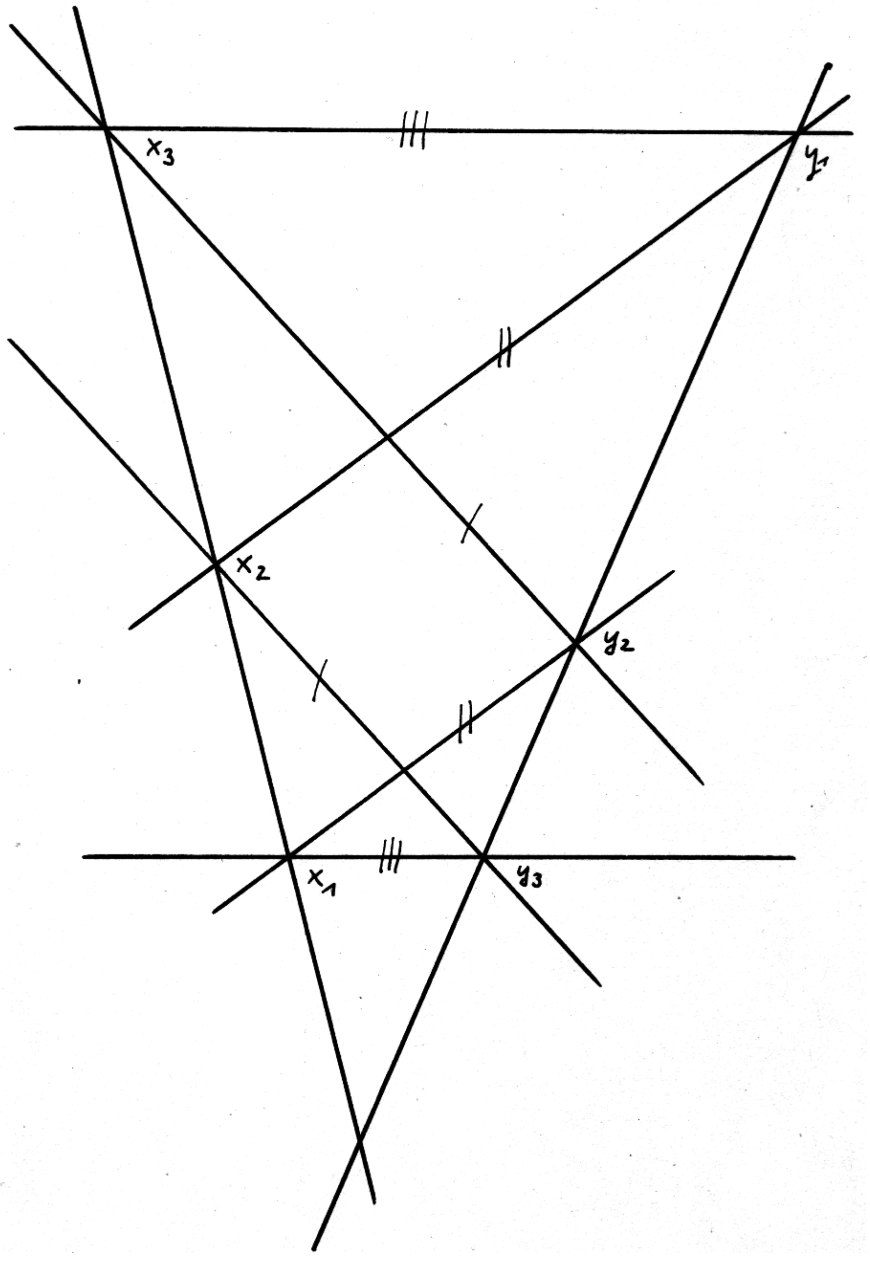
Definition 7.1.11. Wir sagen, eine affine Inzidenzebene habe die **affine Pappus-Eigenschaft**, wenn gegeben Geraden g, h und für $i \in \{1, 2, 3\}$ Punkte $x_i \in g \backslash h$ und $y_i \in h \backslash g$ stets gilt

$$(\overline{x_1 y_2} \parallel \overline{x_2 y_1} \text{ und } \overline{x_2 y_3} \parallel \overline{x_3 y_2}) \Rightarrow \overline{x_1 y_3} \parallel \overline{x_3 y_1}$$

7.1.12. Sie dürfen als Übung zeigen, daß diese Eigenschaft für beliebige Geraden bereits folgt, wenn wir sie nur für sich schneidende Geraden fordern.



Skizze zum Beweis der Koordinatisierbarkeit von Desargues-Ebenen



Skizze zur affinen Pappus-Eigenschaft.

7.1.13. Es ist nicht schwer zu sehen, daß eine affine Inzidenzebene mit der affinen Desargues-Eigenschaft genau dann die Pappus-Eigenschaft hat, wenn ihr nach 7.1.16 bis auf Isomorphismus wohlbestimmter Koordinatenschiefkörper kommutativ ist. Hierfür muß man nur die Streckfaktoren der Streckungen untersuchen, die die verschiedenen Parallelen in der Pappus-Eigenschaft ineinander überführen. Der im folgenden bewiesene Satz von Hessenberg zeigt sogar, daß die Pappus-Eigenschaft bereits die Desargues-Eigenschaft impliziert.

Satz 7.1.14 (Hessenberg). *Jede affine Inzidenzebene mit der Pappus-Eigenschaft hat auch die Desargues-Eigenschaft.*

Beweis. Gegeben eine Konstellation aus drei paarweise verschiedene Geraden g_1, g_2, g_3 mit einem gemeinsamen Punkt z und für $i \in \{1, 2, 3\}$ Punkte $x_i, y_i \in g_i \backslash z$ mit $\overline{x_1 x_2} \parallel \overline{y_1 y_2}$ und $\overline{x_2 x_3} \parallel \overline{y_2 y_3}$ gilt es, aus der Pappus-Eigenschaft

$$\overline{x_1 x_3} \parallel \overline{y_1 y_3}$$

zu folgern. Wir sagen dann, „Desargues gelte für diese Konstellation“. Wenn die x_i kolinear sind, so folgt auch ohne Pappus bereits, daß die y_i kolinear sind und damit gilt Desargues für die gegebene Konstellation. Wir dürfen also zusätzlich annehmen, daß die x_i und dann auch die y_i jeweils nicht kolinear sind. Gilt $\overline{x_1 x_3} \parallel g_2$ und $\overline{y_1 y_3} \parallel g_2$, so folgt wieder Desargues für die gegebene Konstellation auch ohne Pappus. Wir dürfen also zusätzlich auch noch annehmen, daß $\overline{y_1 y_3}$ nicht zu g_2 parallel ist. Jetzt betrachten wir die zu g_2 parallele Gerade g durch x_3 und setzen

$$p := g \cap g_1 \qquad q := g \cap \overline{y_1 y_3} \qquad \text{und} \quad r := \overline{q y_2} \cap \overline{x_2 x_3}$$

und holen das Argument dafür nach, daß auch r sinnvoll definiert ist. Wir haben nämlich $q \notin \overline{y_2 y_3}$, da die y_i nicht kolinear sind und damit andernfalls $q = y_3$ folgern würde im Widerspruch dazu, daß y_3 nicht auf g liegen kann. Damit gilt schon mal $q \neq y_2$ und $\overline{q y_2}$ ist eine wohldefinierte Gerade. Diese Gerade schließlich ist nicht parallel zu $\overline{x_2 x_3}$, da sie nicht parallel ist zu $\overline{y_2 y_3}$, da eben gilt $q \notin \overline{y_2 y_3}$. Damit ist also auch r sinnvoll definiert. Jetzt wenden wir dreimal Pappus an.

1. Wir betrachten die Geraden $\overline{rq}$ sowie g_3 und darauf die Punkte r, y_2, q sowie y_3, x_3, z. Wir bemerken $r \neq x_3$, da sonst x_3, q und y_2 kolinear wären und wir $g = g_2$ folgern könnten im Widerspruch zu $x_3 \notin g_2$. Wir haben nun $r \notin g_3$ wegen $x_2 \notin g_3$ und $y_2 \notin g_3$ nach Annahme und $q \notin g_3$, da sonst folgte $q = x_3$ und wieder x_3, q und y_2 kolinear wären, was ja nicht sein kann. Andererseits haben wir $y_3 \notin \overline{rq}$, weil die y_i nicht kolinear sind, und $x_3 \notin \overline{rq}$, weil $x_3 \neq q$, und $z \notin \overline{rq}$, weil g_2 nicht parallel ist zu $\overline{rq}$. Nun haben wir $\overline{r x_3} \parallel \overline{y_2 y_3}$ und $\overline{y_2 z} \parallel \overline{q x_3}$ und mit Pappus folgt

$$\overline{rz} \parallel \overline{q y_3}$$

2. Wir betrachten die Geraden $\overline{ry_2}$ sowie g_1 und darauf die Punkte r, q, y_2 sowie y_1, z, p. Wir haben $r \notin g_1$ wegen $\overline{rz} \parallel \overline{qy_3} = \overline{y_1y_3}$. Wir haben $q \notin g_1$, da sonst folgte $q = y_1$ und dann die y_i kolinear wären. Wir haben $y_2 \notin g_1$ nach Annahme. Wir haben weiter $z \notin \overline{ry_2}$, weil g_2 nicht parallel ist zu $\overline{ry_2} = \overline{qy_2}$. Haben wir außerdem $y_1, p \notin \overline{ry_2}$, so können wir aus $\overline{rz} \parallel \overline{qy_1}$ und $\overline{qp} \parallel \overline{y_2z}$ mit Pappus folgern
$$\overline{rp} \parallel \overline{y_2y_1}$$
Haben wir andererseits $p \in \overline{ry_2}$ oder $y_1 \in \overline{ry_2}$, so folgt $p = q = y_1$. Auch in diesem Fall haben wir jedoch $r \neq p$, da sonst gälte $r \in g$ und folglich $r = x_3$. Auch in diesem Fall ist also $\overline{rp}$ eine wohlbestimmte Gerade und wir haben sogar $\overline{rp} = \overline{y_2y_1}$ und a forteriori $\overline{rp} \parallel \overline{y_2y_1}$.

3. Wir betrachten die Geraden $\overline{x_2x_3}$ sowie g_1 und darauf die Punkte x_3, x_2, r sowie z, p, x_1. Nach Annahme gilt $x_3, x_2 \notin g_1$ und $r \notin g_1$ hatten wir bereits geprüft. Unsere Annahmen zeigen auch unmittelbar $z, x_1 \notin \overline{x_2x_3}$. Aus $p \in \overline{x_2x_3}$ schließlich folgte $p = x_3$ und das ist unmöglich wegen $x_3 \notin g_1$. Wegen $\overline{x_3p} \parallel \overline{x_2z}$ und $\overline{x_2x_1} \parallel \overline{rp}$, letzeres nach dem vorhergehenden, folgern wir mit Pappus
$$\overline{x_3x_1} \parallel \overline{rz}$$

Zusammen zeigen der erste und dritte Teil $\overline{x_3x_1} \parallel \overline{rz} \parallel \overline{qy_3} = \overline{y_1y_3}$. □

Ergänzung 7.1.15 (**Geometrische Charakterisierung reeller Ebenen**). Man kann die Forderung, daß der Koordinatenkörper einer affinen Inzidenzebene mit der affinen Pappus-Eigenschaft und a forteriori der affinen Desargues-Eigenschaft der Körper der reellen Zahlen ist, auch in geometrischer Sprache ausdrücken. Das liest sich dann wie folgt: Zunächst erklärt man eine **Doppelordnung** auf einer Menge X als eine Teilmenge $D \subset \mathcal{P}(X \times X)$, die aus zwei Anordnungen von X besteht, die zueinander opponiert sind. Dann vereinbart man, daß eine **Doppelordnung mit besten Schranken** eine Doppelordnung sein möge, in der für jede ihrer beiden Anordnungen jede nach oben beschränkte nichtleere Teilmenge $Y \subset X$ eine kleinste obere Schranke $\sup_X Y$ hat. Und dann betrachtet man affine Inzidenzebenen, in denen es möglich ist, jede Gerade so mit einer Doppelordnung mit besten Schranken zu versehen, daß jede „Parallelenidentifikation" zwischen zwei verschiedenen Geraden die Doppelordnung erhält. Unter einer „Parallelenidentifikation" verstehen wir dabei jede Bijektion zwischen unseren beiden Geraden, die entsteht, indem wir eine sie beide schneidende dritte Gerade nehmen und zwei Punkte auf unseren beiden ursprünglichen Geraden genau dann identifizieren, wenn sie beide auf derselben Parallele zu unserer dritten Gerade liegen oder beide auf unserer dritten Gerade selber. Es ist nicht schwer zu sehen, daß der Koordinatenkörper unter diesen Voraussetzungen alle die Axiome [AN1] 1.5.3 erfüllen muß, die den Körper der reellen Zahlen charakterisieren.

Übungen

Übung 7.1.16. Man zeige, daß die affinen Inzidenzebenen zu Schiefkörpern K, L genau dann isomorph sind, wenn unsere Schiefkörper isomorph sind.

Übung 7.1.17. Man zeige, daß in einer affinen Inzidenzebene jede Gerade mindestens zwei Punkte hat.

Übung 7.1.18. Man zeige, daß die Pappus-Eigenschaft für für parallele Geraden bereits folgt, wenn wir sie nur für sich schneidende Geraden fordern. Hinweis: Man mag sich am Beweis der analogen Aussage 7.1.9 in Bezug auf die Desargues-Eigenschaft orientieren.

7.2 Projektive Räume

Definition 7.2.1. Gegeben ein Körper K und ein K-Vektorraum W bezeichnen wir die Menge aller Ursprungsgeraden in W mit

$$\mathbb{P}W = \mathbb{P}_K W := \{V \subset W \mid V \text{ ist ein eindimensionaler Untervektorraum}\}$$

und nennen diese Menge den **projektiven Raum zu** W oder auch die **Projektivisierung von** W. Jeder injektive Vektorraumhomomorphismus $V \hookrightarrow W$ induziert eine Injektion $\mathbb{P}V \hookrightarrow \mathbb{P}W$ der zugehörigen Projektivisierungen.

7.2.2. Gegeben ein Körper K und ein K-Vektorraum W hat jeder Punkt des zugehörigen projektiven Raums $\mathbb{P}W$ also die Gestalt $\langle w \rangle$ für $w \in W \backslash 0$. Ist W der Nullvektorraum, so ist $\mathbb{P}W$ leer. Ist W eindimensional, so besteht $\mathbb{P}W$ aus einem einzigen Punkt. Für $n \geq 0$ heißt der projektive Raum zu K^{n+1} der **n-dimensionale projektive Raum über dem Körper** K und wir notieren ihn

$$\mathbb{P}^n K := \mathbb{P}(K^{n+1})$$

Gegeben $x_0, x_1, \ldots, x_n \in K$ nicht alle Null bezeichnen wir die Gerade durch den Ursprung und den Punkt mit den Koordinaten $x_0, x_1, \ldots, x_n$, aufgefaßt als Punkt des n-dimensionalen projektiven Raums, mit

$$\langle x_0, x_1, \ldots, x_n \rangle := \langle (x_0, x_1, \ldots, x_n) \rangle$$

Üblich sind auch die Schreibweisen $[x_0, x_1, \ldots, x_n]$ und $(x_0; x_1; \ldots; x_n)$ für diesen Punkt des projektiven Raums $\mathbb{P}^n K$. Wir erhalten eine Einbettung $K^n \hookrightarrow \mathbb{P}^n K$ vermittels der Abbildungsvorschrift $(x_1, \ldots, x_n) \mapsto \langle 1, x_1, \ldots, x_n \rangle$. Das Komplement des Bildes dieser Einbettung ist genau die Menge $\mathbb{P}^{n-1} K$ aller Geraden durch den Ursprung im Teilraum $0 \times K^n \subset K^{n+1}$, so daß wir mit einigen impliziten Identifikationen für alle $n \geq 1$ eine Zerlegung

$$\mathbb{P}^n K = K^n \sqcup \mathbb{P}^{n-1} K$$

erhalten. Im Fall $n = 1$ notieren wir diese Zerlegung meist $\mathbb{P}^1K = K \sqcup \{\infty\}$ oder reden von der **kanonischen Bijektion** $K \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{P}^1K$.

7.2.3. Unser Monoidhomomorphismus $K(X) \to \operatorname{Ens}(K \sqcup \{\infty\})$ aus 5.6.27 verwandelt sich unter obigen Identifikationen in einen Monoidhomomorphismus $K(X) \to \operatorname{Ens}(\mathbb{P}^1K)$, der in Formeln beschrieben werden kann durch die Vorschrift $f : \langle 1, x\rangle \mapsto \langle Q(x), P(x)\rangle$ für $f = P/Q$ eine Darstellung mit P und Q ohne gemeinsame Nullstelle in K oder besser, wenn man den Wert bei $\langle 0, 1\rangle$ auch korrekt erhalten will, durch $f : \langle y, x\rangle \mapsto \langle \tilde{Q}(y, x), \tilde{P}(y, x)\rangle$ für $\tilde{Q}, \tilde{P} \in K[Y, X]$ diejenigen homogenen Polynome vom gleichen Grad in zwei Variablen, die beim Einsetzen von $Y = 1$ unsere ursprünglichen Polynome liefern und bei denen der gemeinsame Grad unter diesen Bedingungen kleinstmöglich ist. Für $P(X) = X^2 + 1$ und $Q(X) = X^5 + X$ hätten wir etwa $\tilde{P}(Y, X) = X^2Y^3 + Y^5$ und $\tilde{Q}(Y, X) = X^5 + XY^4$. Die offensichtliche Operation von $\operatorname{GL}(2; K)$ auf $\mathbb{P}^1K$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \langle y, x\rangle \mapsto \langle ay + bx, cy + dx\rangle$$

kommt dann offensichtlich her von einer Operation auf $K(X)$ durch Einsetzen von $(c+dX)/(a+bX)$ für X. Man kann sich auch überlegen, daß man so alle K-linearen Körperautomorphismen von $K(X)$ erhält, daß also das Einsetzen anderer nichtkonstanter rationaler Funktionen keinen Körperautomorphismus liefert: Ist K algebraisch abgeschlossen, so folgt das daraus, daß unter $K(X) \to \operatorname{Ens}(\mathbb{P}^1K)$ andere Elemente keine Injektion liefern. Im allgemeinen gilt es, zu einem algebraischen Abschluß überzugehen, was wir erst in [AL] 3.11.5 lernen.

7.2.4. Gegeben ein affiner Raum E über einem Körper K erklärt man seine **projektive Vervollständigung** oder gleichbedeutend seinen **projektiven Abschluß** als die disjunkte Vereinigung

$$\mathbb{V}E := E \sqcup \mathbb{P}\vec{E}$$

unseres affinen Raums mit der Projektivisierung seines Richtungsraums. Anschaulich gesprochen ergänzt man also E um je einen zusätzlichen Punkt für jedes maximale System paarweise paralleler Geraden in E. Die Elemente von $\mathbb{P}\vec{E}$ heißen die **unendlich fernen Punkte** unserer projektiven Vervollständigung. Ist E eine Ebene, so heißt $\mathbb{P}\vec{E}$ die **unendlich ferne Gerade**. Ist E dreidimensional, so heißt $\mathbb{P}\vec{E}$ die **unendlich ferne Ebene**. Im allgemeinen heißt $\mathbb{P}\vec{E}$ die **unendlich ferne Hyperebene**. Jeder injektive Homomorphismus von affinen Räumen $E \hookrightarrow F$ induziert eine Injektion $\mathbb{V}E \hookrightarrow \mathbb{V}F$ der zugehörigen projektiven Vervollständigungen.

7.2.5 (**Projektive Vervollständigung als Projektivisierung**). Sei E ein affiner Raum. Wir können seine projektive Vervollständigung $\mathbb{V}E$ aus 7.2.4 wie folgt als projektiven Raum zu einem Vektorraum realisieren: Wir beginnen mit dem Raum $\operatorname{Aff}(E, K) \subset \operatorname{Ens}(E, K)$ aller affinen Abbildungen $E \to K$, einem Untervektorraum im Raum aller Abbildungen von E nach K. Den in seinem Dualraum von den Auswertungen an Punkten aufgespannten Untervektorraum nennen wir die **Linearisierung** $\operatorname{Lin}(E) \subset \operatorname{Aff}(E, K)^{\top}$ des affinen Raums E. Im endlichdimensionalen Fall ist diese Linearisierung bereits der ganze Dualraum, in Formeln $\operatorname{Lin}(E) = \operatorname{Aff}(E, K)^{\top}$. In jedem Fall erhalten wir eine Bijektion

$$(E \times K^{\times}) \sqcup \vec{E} \ \xrightarrow{\sim}\ \operatorname{Lin}(E)$$

durch die Vorschrift, die jedem Paar (e, λ) das λ-fache der Auswertung bei e zuordnet und jedem Richtungsvektor $\vec{v}$ die Linearform, die einem $\varphi \in \operatorname{Aff}(E, K)$ den Wert der konstanten Funktion $p \mapsto \varphi(p + \vec{v}) - \varphi(p)$ zuordnet. Diese Bijektion hinwiederum induziert dann offensichtlich eine Bijektion

$$\mathbb{V}E = E \sqcup \mathbb{P}\vec{E} \ \xrightarrow{\sim}\ \mathbb{P}\operatorname{Lin}(E)$$

7.2.6 (**Projektivisierung als projektive Vervollständigung**). Ist W ein Vektorraum, H ein affiner Raum und $i : H \hookrightarrow W$ eine affine Injektion, deren Bild den Ursprung nicht enthält, so kann man die Abbildung $H \to \mathbb{P}W$, $v \mapsto \langle i(v) \rangle$ zu einer Einbettung $\mathbb{V}H \hookrightarrow \mathbb{P}W$ fortsetzen, indem man jeder Gerade aus $\mathbb{P}\vec{H}$ ihr Bild in $\mathbb{P}W$ unter dem linearen Anteil $\vec{\imath}$ unserer Injektion i zuordnet. Ist hier das Bild von i eine Hyperebene $i(H) \subset W$, so liefert diese Konstruktion sogar eine Bijektion

$$\mathbb{V}H \ \xrightarrow{\sim}\ \mathbb{P}W$$

zwischen der projektiven Vervollständigung von H und der Projektivisierung von W. Ist speziell $i : K^n \hookrightarrow K^{n+1}$ das Davorscheiben einer Eins als erster Koordinate, so ist diese Abbildung die bereits in 7.2.2 besprochene Bijektion

$$K^n \sqcup \mathbb{P}^{n-1}K = K^n \sqcup \mathbb{P}(K^n) = \mathbb{V}K^n \xrightarrow{\sim} \mathbb{P}(K^{n+1}) = \mathbb{P}^n K$$

Vorschau 7.2.7. Die projektiven Räume $\mathbb{P}V$ zu endlichdimensionalen reellen oder komplexen Vektorräumen V können mit einer Topologie versehen werden durch die Vorschrift, daß eine Teilmenge offen sein soll genau dann, wenn ihr Urbild in $V \backslash 0$ offen ist. Mehr zu dieser sogenannten „Quotiententopologie" diskutieren wir in [TM] 1.11. Bereits hier sei erwähnt, daß es für diese Topologien stetige Bijektionen mit stetiger Umkehrung gibt, die $\mathbb{P}^1\mathbb{R}$ mit der Kreislinie S^1 und $\mathbb{P}^1\mathbb{C}$ mit der Kugelschale S^2 identifizieren. Deshalb heißt $\mathbb{P}^1\mathbb{C}$ auch die **Riemann'sche Zahlenkugel**. Genauer erhalten wir eine derartige Identifikation für $\mathbb{P}^1\mathbb{C}$, indem wir eine Kugelschale auf die komplexe Zahlenebene legen, eine Lampe an den höchsten Punkt P stellen und jeden Punkt der Kugelschale, der nicht gerade der höchste Punkt ist, auf seinen Schatten in der Ebene $\mathbb{C}$ abbilden, den höchsten Punkt P jedoch auf ∞. Im reellen Fall verfährt man analog.

Übungen

Ergänzende Übung 7.2.8 (**Universelle Eigenschaft der Linearisierung**). Sei ein affiner Raum E über einem Körper K. Man gebe Formeln an für die Verknüpfung auf $(E \times K^\times) \sqcup \vec{E}$, die unter der Bijektion aus 7.2.5 der Addition von Vektoren entsprechen. Man zeige weiter, daß die kanonische Abbildung $\mathrm{can} : E \to \mathrm{Lin}\, E$, die jedem Punkt $e \in E$ das Auswerten bei e zuordnet, die universelle Eigenschaft hat, daß für jeden K-Vektorraum das Vorschalten von can eine Bijektion

$$\mathrm{Hom}_K(\mathrm{Lin}\, E, V) \xrightarrow{\sim} \mathrm{Aff}_K(E, V)$$

induziert. In anderen Worten faktorisiert also jede affine Abbildung von einem affinen Raum in einen Vektorraum auf genau eine Weise über eine linare Abbildung seiner Linearisierung in besagten Vektorraum, im Diagramm

$$\begin{tikzcd} E \arrow[r] \arrow[d, "\mathrm{can}"'] & V \\ \mathrm{Lin}\, E \arrow[ur, dashed] & \end{tikzcd}$$

7.3 Projektive Inzidenzebenen

7.3.1. Durch den Übergang von affinen Inzidenzebenen zu den sogenannten „projektiven Inzidenzebenen“ entstehen neue Symmetrien, die die Eigenschaften von Desargues und Pappus zu sehr viel stärkeren Aussagen machen.

Definition 7.3.2. Eine Menge X von „Punkten“ mit einem System von Teilmengen $G \subset \mathcal{P}(X)$, genannt „Geraden“, heißt eine **projektive Inzidenzebene** oder genauer eine **konkrete projektive Inzidenzebene**, wenn gilt:

1. Gegeben $x, y \in X$ mit $x \neq y$ gibt es genau ein $g \in G$ mit $x \in g$ und $y \in g$ alias: Durch je zwei verschiedene Punkte geht genau eine Gerade. Wir notieren sie $\overline{xy}$;

2. Gegeben $g, h \in G$ mit $g \neq h$ gibt es genau ein $x \in X$ mit $x \in g$ und $x \in h$ alias: Je zwei verschiedene Geraden schneiden sich in genau einem Punkt;

3. Es gibt vier paarweise verschiedene Punkte, von denen keine drei in demselben $g \in G$ alias auf derselben Gerade liegen. Man spricht dann auch von einem **Viereck**.

Beispiel 7.3.3. Ist W ein dreidimensionaler Vektorraum über einem Körper K, so wird der projektive Raum $X := \mathbb{P}W$ eine projektive Inzidenzebene, wenn wir als Geraden alle Teilmengen der Gestalt $\mathbb{P}V$ mit $V \subset W$ einem zweidimensionalen Untervektorraum auszeichnen. Analoges gilt, wenn allgemeiner K ein Schiefkörper ist.

Beispiel 7.3.4. Ist K ein Schiefkörper, so wird die Menge

$$X := \mathbb{P}^2 K := (K^3 \backslash 0)/K^\times$$

der Bahnen unter der Rechtsmultiplikation von $K^\times$ eine projektive Inzidenzebene, wenn wir als Geraden alle Teilmengen der Gestalt $((vK+wK)\backslash 0)/K^\times$ mit $v, w \in K^3\backslash 0$ und $vK \neq wK$ auszeichnen.

Beispiel 7.3.5 (**Projektive Vervollständigung**). Gegeben eine affine Inzidenzebene (X, G) können wir eine projektive Inzidenzebene $(\mathbb{V}X, \bar{G})$ konstruieren wie folgt: Die Menge der Äquivalenzklassen unserer Äquivalenzrelation „gleich oder parallel" aus 7.1.4 notieren wir $\mathbb{S}X$ und nennen ihre Elemente, also die einzelnen Äquivalenzklassen, die **unendlich fernen Punkte von** X. Es mag verwirrend sein, daß die unendlich fernen Punkte von X keine Punkte von X sind, sondern vielmehr Mengen von Teilmengen von X, aber so ist nun einmal die Terminologie. Dann erklären wir die Menge $\mathbb{V}X$ als die disjunkte Vereinigung

$$\mathbb{V}X := X \sqcup \mathbb{S}X$$

und erklären $\bar{G} \subset \mathcal{P}(\mathbb{V}X)$, indem wir zu jedem $g \in G$ die Menge $\bar{g} := g \sqcup [g]$ mit $[g] \in \mathbb{S}X$ der Äquivalenzklasse von g bilden und dann

$$\bar{G} := \{\bar{g} \mid g \in G\} \sqcup \{\mathbb{S}X\}$$

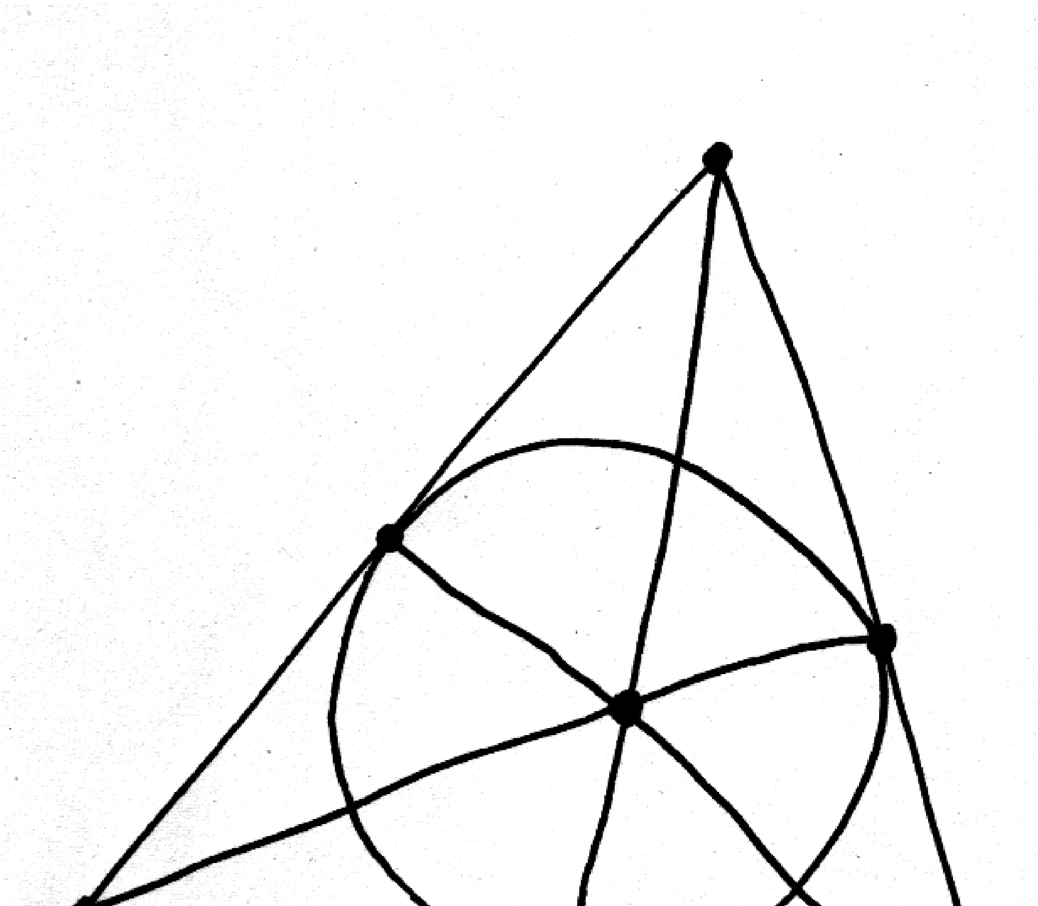
setzen. In diesem Zusammenhang heißt $\mathbb{S}X$ die **unendlich ferne Gerade**. Man sieht leicht, daß die projektive Vervollständigung einer affinen Inzidenzebene stets eine projektive Inzidenzebene ist. Umgekehrt ist auch klar, daß man stets eine affine Inzidenzebene erhält, wenn man eine projektive Gerade aus einer projektiven Inzidenzebene entfernt und als affine Geraden die Schnitte der anderen projektiven Geraden mit dem Komplement besagter projektiver Gerade erklärt.

Beispiel 7.3.6. Ist E ein zweidimensionaler affiner Raum über einem Körper K, so haben wir eine natürliche Bijektion $\mathbb{P}\vec{E} \xrightarrow{\sim} \mathbb{S}E$ zwischen der Projektivisierung seines Richtungsraums und seiner unendlich fernen Gerade. Unter der Komposition von Bijektionen

$$\mathbb{V}E = E \sqcup \mathbb{S}E \xrightarrow{\sim} E \sqcup \mathbb{P}\vec{E} \xrightarrow{\sim} \mathbb{P}\operatorname{Lin} E$$

mit dem letztem Pfeil nach 7.2.5 entsprechen dann die Geraden der im Sinne von 7.3.5 projektiv vervollständigten Inzidenzebene $\mathbb{V}E$ den Geraden der als Projektivisierung $\mathbb{P}\operatorname{Lin} E$ im Sinne von 7.3.3 der Linearisierung $\operatorname{Lin} E$ unserer affinen Ebene E konstruierten projektiven Inzidenzebene.

Skizze zum Beweis des Satzes von Hessenberg



Die projektive Ebene über dem Körper mit zwei Elementen hat sieben Punkte und sieben Geraden.

Definition 7.3.7. Eine **Inzidenzstruktur** ist ein Datum (X, G, I) bestehend aus zwei Mengen X und G und einer Teilmenge $I \subset X \times G$ alias einer Relation zwischen X und G. Statt $(x, g) \in I$ schreiben wir auch xIg. Gegeben zwei Inzidenzstrukturen (X, G, I) und (X', G', I') verstehen wir unter einem **Isomorphismus von Inzidenzstrukturen** ein Paar (φ, ψ) bestehend aus einer Bijektion $\varphi : X \xrightarrow{\sim} X'$ und einer Bijektion $\psi : G \xrightarrow{\sim} G'$ derart, daß gilt $(\varphi \times \psi)(I) = I'$.

Definition 7.3.8. Eine Inzidenzstruktur (X, G, I) heißt eine **abstrakte affine Inzidenzebene**, wenn gilt:

1. Gegeben $x, y \in X$ mit $x \neq y$ gibt es genau ein $g \in G$ mit xIg und yIg;
2. Gegeben $g \in G$ und $x \in X$ mit $(x, g) \notin I$ gibt es genau ein $h \in G$ mit xIh derart, daß es kein $y \in X$ gibt mit yIg und yIh;
3. Es gibt $x, y, z \in X$ paarweise verschieden derart, daß kein $g \in G$ existiert mit xIg und yIg und zIg.

Definition 7.3.9. Eine Inzidenzstruktur (X, G, I) heißt eine **abstrakte projektive Inzidenzebene**, wenn gilt:

1. Gegeben $x \neq y$ in X gibt es genau ein $g \in G$ mit xIg und yIg;
2. Gegeben $g \neq h$ in G gibt es genau ein $x \in X$ mit xIg und xIh;
3. Es gibt ein **Viereck** alias paarweise verschiedene $x_1, x_2, x_3, x_4 \in X$ und paarweise verschiedene $g_1, g_2, g_3, g_4 \in G$ mit $x_i I g_j$ genau dann, wenn entweder gilt $i = j$ oder $i \equiv j + 1 (\operatorname{mod} 4)$.

7.3.10 (**Abstrakte und konkrete Inzidenzebenen**). Jeder konkreten affinen Inzidenzebene (X, G) können wir eine abstrakte affine Inzidenzebene (X, G, I) zuordnen durch die Vorschrift $I := \{(x, g) \mid x \in g\}$ Man überzeugt sich auch leicht, daß jede abstrakte affine Inzidenzebene isomorph ist zu einer abstrakten affinen Inzidenzebene, die in dieser Weise von einer konkreten affinen Inzidenzebene herkommt. In diesem Sinne sind unsere beiden Begriffe also nur unwesentlich verschieden. Der Nutzen dieser beiden Begrifflichkeiten liegt allein darin, die Betonung unterschiedlicher Aspekte der Theorie zu erleichtern. Analoges gilt für projektive Inzidenzebenen.

Ergänzung 7.3.11. Jedem Paar (X, G) bestehend aus einer Menge X mitsamt einem Mengensystem $G \subset \mathcal{P}(X)$ können wir ganz allgemein die Inzidenzstruktur (X, G, I) mit $I := \{(x, g) \mid x \in g\}$ zuordnen. Jede Inzidenzstruktur (X, A, I) mit der Eigenschaft, daß gegeben $a, b \in A$ aus $(xIa \Leftrightarrow xIb)$ bereits folgt $a = b$, ist weiter isomorph zu der Inzidenzstruktur eines Paares (X, G) wie oben.

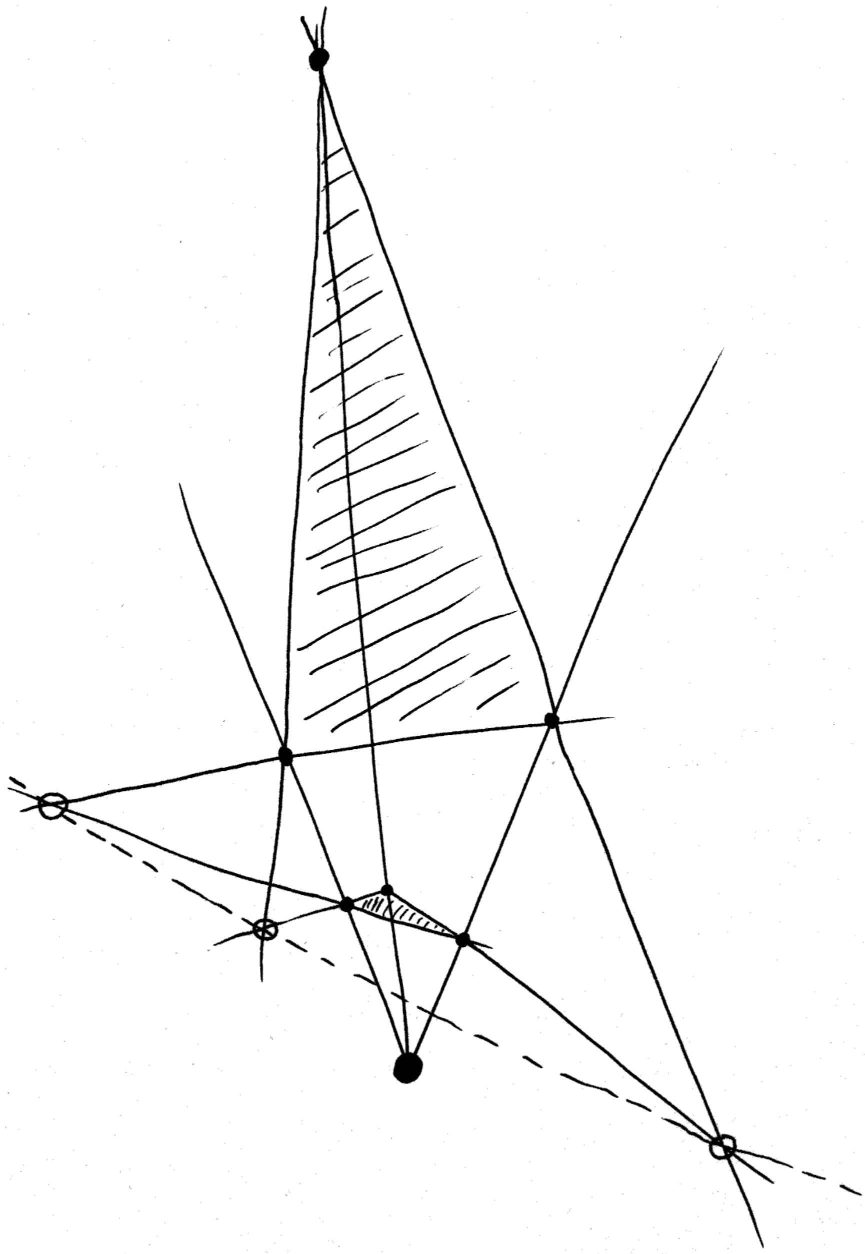
7.3.12 (**Punkt-Geraden-Symmetrie projektiver Ebenen**). Ist (X, G, I) eine abstrakte projektive Inzidenzebene, so ist offensichtlich für $\tau : X \times G \xrightarrow{\sim} G \times X$ die Vertauschung auch $(G, X, \tau(I))$ eine abstrakte projektive Inzidenzebene. Sie heißt die **duale projektive Inzidenzebene**.

Definition 7.3.13. Man sagt, eine projektive Inzidenzebene habe die **Desargues-Eigenschaft**, wenn folgendes gilt: Gegeben seien zwei dreielementige jeweils nicht kolineare Mengen von Punkten, und dazwischen eine Bijektion. Die Geraden durch je zwei Punkte eines Tripels bilden damit eine dreielementige Menge von Geraden, und wir erhalten so auch zwei dreielementige Mengen von Geraden und dazwischen eine Bijektion. Gibt es dann einen Punkt, der mit je zwei Punkten in Bijektion kolinear ist, so gibt es auch eine Gerade, die mit je zwei Geraden in Bijektion **kopunktal** ist alias einen allen Dreien gemeinsamen Punkt hat.

7.3.14. In Formeln übersetzt besagt die Desargues-Eigenschaft: Gegeben seien zwei Tripel x_1, y_1, z_1 und x_2, y_2, z_2 von jeweils nicht kolinearen Punkten. Wir setzen $\bar{x}_i := \overline{y_i z_i}$, $\bar{y}_i := \overline{z_i x_i}$ und $\bar{z}_i := \overline{x_i y_i}$ und erhalten so zwei Tripel $\bar{x}_1, \bar{y}_1, \bar{z}_1$ und $\bar{x}_2, \bar{y}_2, \bar{z}_2$ von jeweils nicht kopunktalen Geraden. Gibt es dann einen Punkt p mit (p, x_1, x_2) und (p, y_1, y_2) und (p, z_1, z_2) jeweils kolinear, so gibt es auch eine Gerade g mit $(g, \bar{x}_1, \bar{x}_2)$ und $(g, \bar{y}_1, \bar{y}_2)$ und $(g, \bar{z}_1, \bar{z}_2)$ jeweils kopunktal.

7.3.15. Verstärken wir in der Formulierung der Desargues-Eigenschaft den letzten Satz zur Forderung „Genau dann gibt es einen Punkt, der mit je zwei Punkten in Bijektion kolinear ist, wenn es eine Gerade gibt, die mit je zwei Geraden in Bijektion **kopunktal** ist“, so gilt diese a priori stärkere Eigenschaft offensichtlich für eine projektive Inzidenzebene genau dann, wenn sie für die duale projektive Inzidenzebene gilt.

7.3.16 ($\mathbb{P}^2 K$ **hat die Desargues-Eigenschaft**). Wir prüfen, daß jede projektive Ebene über einem beliebigen Schiefkörper im Sinne von 5.7.2 die Desargues-Eigenschaft hat. Wir arbeiten zunächst in einer beliebigen projektiven Inzidenzebene. Fallen Punkte in Bijektion oder Geraden in Bijektion zusammen, so ist die zugehörige Bedingung der Desargues-Eigenschaft aus trivialen Gründen erfüllt. Diese Fälle schließen wir von jetzt an aus. Damit ist der Punkt p eindeutig bestimmt und es gilt $\bar{x}_1 \cap \bar{x}_2 \neq \bar{y}_1 \cap \bar{y}_2$ und es gibt genau eine Gerade g mit $(g, \bar{x}_1, \bar{x}_2)$ und $(g, \bar{y}_1, \bar{y}_2)$ kopunktal. Es gilt zu zeigen, daß dann im Fall einer projektiven Ebene über einem Schiefkörper auch $(g, \bar{z}_1, \bar{z}_2)$ kopunktal ist. Ohne Beschränkung der Allgemeinheit dürfen wir dabei annehmen, daß g die unendlich ferne Gerade von $\mathbb{P}^2 K$ ist. Liegen nun von einem unserer beiden Tripel zwei Punkte auf der unendlich fernen Geraden, ist die zugehörige Bedingung der Desargues-Eigenschaft wieder aus trivialen Gründen erfüllt. Liegt von einem unserer beiden Tripel nur ein Punkt auf der unendlich fernen Geraden, etwa der Punkt x_1, so müssen sowohl (x_1, y_1, y_2) als auch (x_1, y_1, y_3) kolinear sein und damit müssen



Die Desargues-Eigenschaft besagt, daß die drei als hohle Kreise dargestellten Schnittpunkte stets auf einer hier gestrichelt gezeichneten Gerade liegen.

(y_1, y_2, y_3) kolinear sein im Widerspruch zu unseren Annahmen. Es reicht also, den Fall zu betrachten, daß keiner unserer Punkte $x_1, x_2, x_3, y_1, y_2, y_3$ auf der unendlich fernen Geraden liegt. Unter diesen Annahmen gilt es nun noch, die beiden Fälle $p \notin g$ und $p \in g$ zu behandeln. Der erste Fall ist der im Bild Dargestellte. In diesem Fall kann man mit einer Streckung mit Zentrum p argumentieren. Im zweiten Fall $p \in g$ argumentiert man analog mit einer Parallelverschiebung.

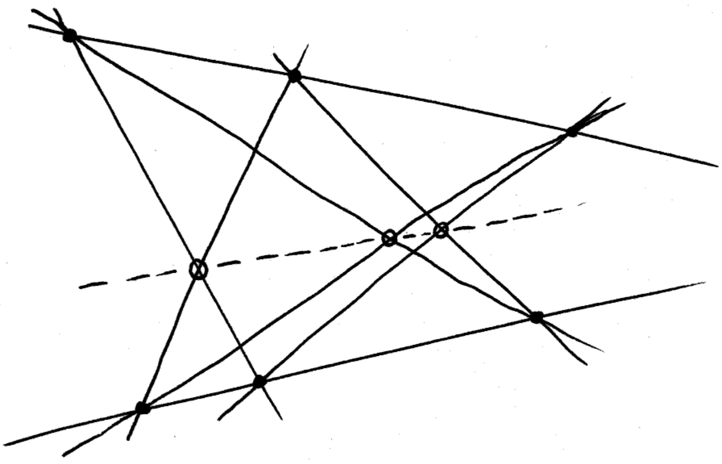
7.3.17. Hat eine projektive Inzidenzebene die Desargues-Eigenschaft, so hat die durch Weglassen einer beliebigen Gerade entstehende affine Inzidenzebene offensichtlich die affine Desargues-Eigenschaft.

Definition 7.3.18. Man sagt, eine projektive Inzidenzebene habe die **Pappus-Eigenschaft**, wenn folgendes gilt: Gegeben seien zwei kolineare Tripel von Punkten. So gibt es ein drittes kolineares Tripel von Punkten derart, daß wenn wir aus einem beliebigen unserer drei Tripel den ersten Eintrag nehmen, aus einem beliebigen anderen den zweiten Eintrag und aus dem verbleibenden Tripel den dritten Eintrag, daß wir dann stets ein kolineares Tripel erhalten.

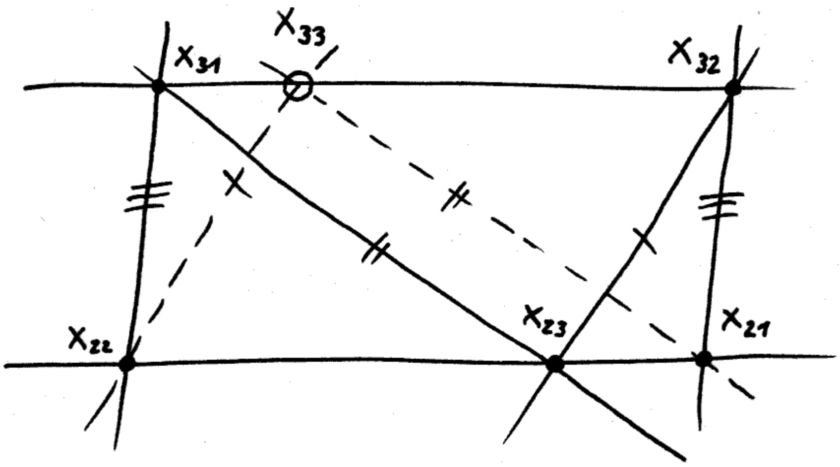
7.3.19. In Formeln soll es also für Punkte $x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}$ mit der Eigenschaft x_{i1}, x_{i2}, x_{i3} kolinear für $i = 1, 2$ stets kolineare Punkte x_{31}, x_{32}, x_{33} geben mit $x_{1\sigma(1)}, x_{2\sigma(2)}, x_{3\sigma(3)}$ kolinear für jede Permutation $\sigma \in \mathcal{S}_3$.

7.3.20 (**Für K kommutativ hat $\mathbb{P}^2 K$ die Pappus-Eigenschaft**). Wir prüfen, daß jede projektive Ebene über einem Körper die Pappus-Eigenschaft hat. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß mindestens eines unserer beiden Tripel, sagen wir das Erste, aus drei paarweise verschiedenen Punkten besteht, und daß dieses auf der unendlich fernen Gerade liegt. Liegt auch einer der Punkte x_{2i} des zweiten Tripels auf der unendlich fernen Geraden, so können wir unser drittes Tripel unschwer auf der unendlich fernen Geraden finden. Diesen Fall brauchen wir also auch nicht weiter zu betrachten. Dann aber sind unsere Punkte x_{31}, x_{32}, x_{33} bereits eindeutig festgelegt und liegen nicht in der unendlich fernen Geraden und es muß nur noch gezeigt werden, daß sie kolinear sind. Fallen zwei Punkte des dritten Tripels zusammen, ist das eh klar. Ist $\overline{x_{31}x_{32}}$ parallel zu einer Gerade durch x_{21}, x_{22}, x_{23}, so ist die Behauptung leicht zu sehen. Ist schließlich $\overline{x_{31}x_{32}}$ nicht parallel zu einer Gerade durch x_{21}, x_{22}, x_{23}, so dürfen wir den Schnittpunkt unserer beiden Geraden als den Ursprung eines Koordinatensystems annehmen und mit Streckungen argumentieren. Die Details seien dem Leser zur Übung überlassen.

7.3.21. Hat eine projektive Inzidenzebene die Pappus-Eigenschaft, so hat die durch Weglassen einer beliebigen Gerade entstehende affine Inzidenzebene offensichtlich die affine Pappus-Eigenschaft.



Die Pappus-Eigenschaft besagt, daß die drei als hohle Kreise dargestellten Schnittpunkte stets auf einer hier gestrichelt gezeichneten Gerade liegen.



Der Fall einer parallelen dritten Gerade beim Beweis der Pappus-Eigenschaft 7.3.20. Die unendlich fernen Punkte x_{1i} gehören zu den Parallelenscharen, von denen zwei Repräsentanten mit jeweils i Strichen gekennzeichnet sind. Zu zeigen ist, daß der Schnittpunkt x_{33} der gestrichelten Linien auf $\overline{x_{31}x_{32}}$ liegt, das als parallel zur Geraden durch die Punkte x_{2i} angenommen ist.

Übungen

Übung 7.3.22. Man zeige, daß in einer projektiven Inzidenzebene jede Gerade mindestens drei Punkte hat.

Übung 7.3.23. Man zeige ohne auf den Koordinatisierungssatz zurückzugreifen, daß eine projektive Inzidenzebene genau dann die Pappus-Eigenschaft hat, wenn die duale projektive Inzidenzebene die Pappus-Eigenschaft hat.

7.4 Lineare Konvexgeometrie

Definition 7.4.1. Sei V ein Vektorraum über einem angeordneten Körper und $E \subset V$ eine Teilmenge. Wir sagen, ein Vektor $v \in V$ **läßt sich aus E positiv linear kombinieren**, wenn er eine Darstellung

$$v = \alpha_1 e_1 + \ldots + \alpha_n e_n$$

besitzt mit $\alpha_i > 0$ und $e_i \in E$ 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.

7.4.2. 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 $\alpha_i \geq 0$ schreiben können. Wenn wir aber im folgenden von einer **positiven Linearkombination** reden, so meinen wir stets positive und nicht etwa nur nichtnegative Koeffizienten.

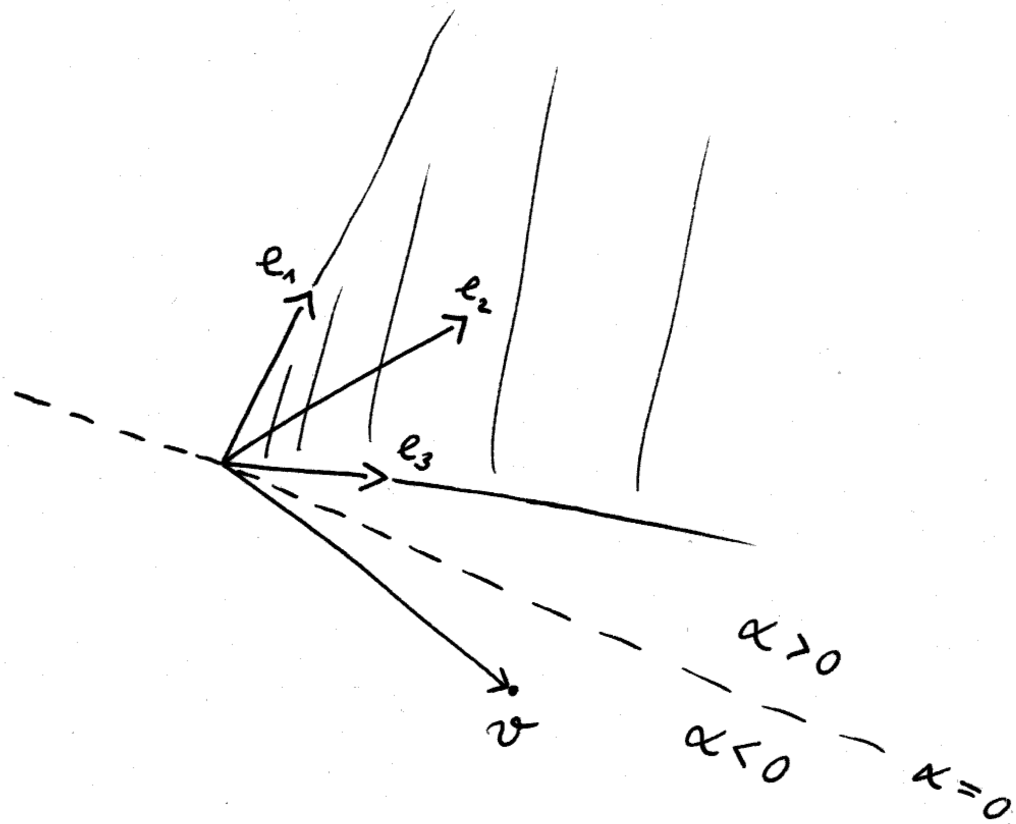
Satz 7.4.3 (Hauptsatz über lineare Ungleichungen). *Ist V ein Vektorraum über einem angeordneten Körper und $E \subset V$ eine endliche Teilmenge, so gilt für jeden Vektor $v \in V$ genau eine der beiden folgenden Aussagen:*

Entweder *der Vektor v läßt sich aus E positiv linear kombinieren,*

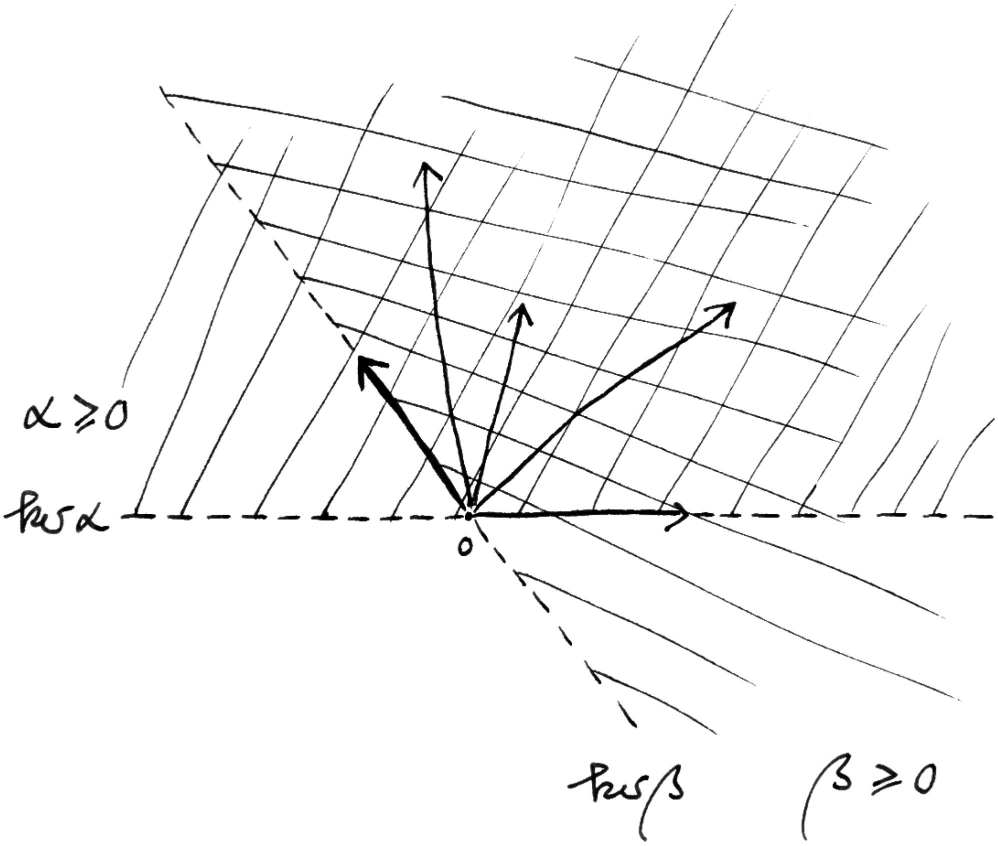
oder aber *es gibt eine Linearform $\alpha \in V^\top$ mit $\alpha(e) \geq 0 \;\; \forall e \in E$ und $\alpha(v) < 0$.*

Im ersten Fall kann v sogar positiv linear kombiniert werden aus höchstens $\dim V$ *Elementen von E. Ist E ein Erzeugendensystem von V, so kann im zweiten Fall α sogar so gewählt werden, daß* $\ker \alpha$ *von seinem Schnitt mit E erzeugt wird.*

Ergänzung 7.4.4. Ist zusätzlich ein Teilraum $W \subset V^\top$ gegeben derart, daß auf keinem Vektor von $V \backslash 0$ alle Linearformen aus W verschwinden, so können wir im zweiten Fall sogar $\alpha \in W$ finden. In der Tat gibt es ja dann für jede endliche



Eine Menge $E = \{e_1, e_2, e_3\}$ 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 abtrennen läßt.



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.

Teilmenge von V und jedes $\alpha \in V^\top$ ein $\tilde{\alpha} \in W$, das auf dieser endlichen Teilmenge dieselben Werte annimmt wie α. Ist V endlichdimensional, so muß hier natürlich bereits $W = V^\top$ gelten.

7.4.5. Der Satz und der hier gegebene Beweis stammen von Weyl [Wey35]. Im Fall des Grundkörpers $\mathbb{R}$ geht er aber 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].

7.4.6 (**Der Hauptsatz über lineare Ungleichungen in Koordinaten**). Spezialisieren wir den Satz zu $V = \mathbb{R}^n$, dessen Elemente wir als Spaltenvektoren auffassen, und besteht unsere endliche Menge E aus den m Spaltenvektoren einer Matrix $A \in \mathrm{Mat}(n \times m; \mathbb{R})$, so erhalten wir für einen Spaltenvektor $v = b = (b_1, \ldots, b_n)^\top \in \mathbb{R}^n$ aus 7.4.3 die folgende Alternative:

Entweder es gibt einen Spaltenvektor $x \in (\mathbb{R}_{\geq 0})^m$ mit $b = Ax$,

oder aber es gibt $y = (y_1, \ldots, y_n)^\top \in \mathbb{R}^n$ mit $y^\top A \in (\mathbb{R}_{\geq 0})^m$ und $y^\top b < 0$.

Unser α ist in diesem Fall der Zeilenvektor $y^\top = (y_1, \ldots, y_n)$.

7.4.7 (**Variante zum Hauptsatz über lineare Ungleichungen**). Besteht unsere endliche Menge E aus den m Spaltenvektoren einer Matrix $C \in \mathrm{Mat}(n \times m; \mathbb{R})$ und ihren Negativen sowie den Vektoren der Standardbasis, so erhalten wir aus 7.4.3 für einen Spaltenvektor $b = (b_1, \ldots, b_n)^\top \in \mathbb{R}^n$ die folgende Alternative:

Entweder es gibt einen Spaltenvektor $x \in \mathbb{R}^m$ mit $Cx \leq b$ in dem Sinne, daß diese Ungleichung in jeder Koordinate gilt,

oder aber es gibt $y = (y_1, \ldots, y_n)^\top \in (\mathbb{R}_{\geq 0})^n$ mit $y^\top C = 0$ und $y^\top b < 0$.

Beispiel 7.4.8. Man denke sich einen Ikosaeder mit einer Ecke im Urprung, und denke sich E als seine Eckenmenge. In diesem Fall hätte die Menge der positiven Linearkombinationen von Vektoren aus E die Gestalt eines eckigen Kegels mit fünf Flächen, die übrigends genau die Kerne der „extremen Stützen von E“ aus dem gleich folgenden Beweis sind.

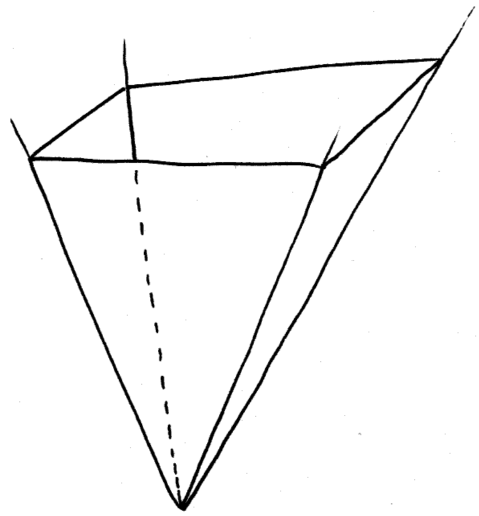
Korollar 7.4.9 (Satz von Caratheodory). *Seien $V \supset T$ ein Vektorraum endlicher Dimension über einem angeordneten Körper mit einer ausgezeichneten Teilmenge. Läßt sich ein Vektor von V aus T positiv linear kombinieren, so läßt er sich bereits aus einer Teilmenge von T mit höchstens* $\dim V$ *Elementen positiv linear kombinieren.*

Beweis. Dies Korollar folgt unmittelbar aus dem Hauptsatz über lineare Ungleichungen 7.4.3. Besonders anschaulich scheint mir die affine Variante 7.4.13 dieser Aussage. $\square$

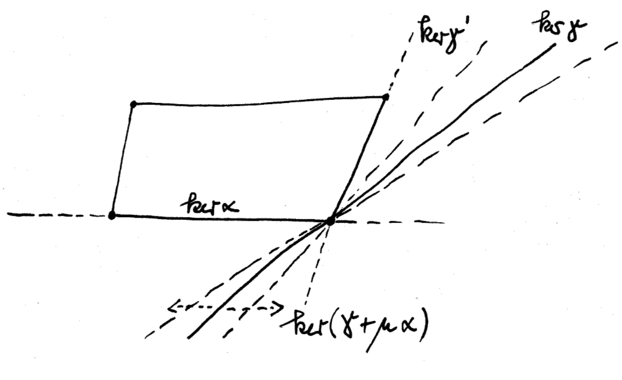
7.4.10 (**Der Fall positiver Linearkombinationen unendlicher Mengen**). Gegeben eine Gerade in der Ebene $\mathbb{R}^2$, die die Menge der Punkte mit rationalen Koordinaten $\mathbb{Q}^2$ nur im Nullpunkt trifft, betrachte man in $\mathbb{Q}^2$ einen der beiden zugehörigen Halbräume mitsamt der Null. Dieser durch den Ursprung ergänzte Halbraum ist eine konvexe Teilmenge E 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 E im allgemeinen nicht mehr richtig. Betrachten wir jedoch abgeschlossene konvexe Kegel E im Sinne von 7.4.14 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. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß V von E erzeugt wird. Eine Linearform $\alpha \in V^\top \backslash 0$ mit $\alpha(e) \geq 0 \; \forall e \in E$ nennen wir eine **Stütze** von E. Wird zusätzlich $\ker \alpha$ erzeugt von $(\ker \alpha) \cap E$, so nennen wir α eine **extreme Stütze** von E. Natürlich ist auch jedes positive Vielfache einer Stütze eine Stütze und jedes positive Vielfache einer extremen Stütze eine extreme Stütze. Wir beweisen den Satz durch Induktion über $d = \dim V$ und müssen die zweite unserer beiden ergänzenden Zusatzaussagen gleich mit beweisen, um die Induktion am Laufen zu halten. Wir unterscheiden zwei Fälle.

Fall 1: E besitzt mindestens eine extreme Stütze. Sei dann $v \in V$ gegeben mit $\alpha(v) \geq 0$ für jede extreme Stütze α. Es gilt zu zeigen, daß sich v positiv linear aus höchstens d Elementen von E kombinieren läßt. Liegt v im Kern einer der extremen Stützen, sagen wir $\alpha(v) = 0$, so ersetzen wir $E \subset V$ durch $E \cap \ker \alpha \subset \ker \alpha$ und sind fertig mit Induktion: Jede Linearform γ' auf $\ker \alpha$, die eine extreme Stütze von $E \cap \ker \alpha \subset \ker \alpha$ ist, läßt sich nämlich zu einer Linearform γ auf V ausdehnen. Die alternativen Ausdehnungen $\gamma + \mu\alpha$ müssen für hinreichend große Skalare μ Stützen von E sein, da ja α positiv ist auf allen Punkten von E außerhalb des Kerns, und wählen wir μ kleinstmöglich mit $\gamma + \mu\alpha$ Stütze von E, so erhalten wir eine Ausdehnung von γ' zu einer Linearform auf V, die selbst extreme Stütze von $E \subset V$ ist. Sind also alle extremen Stützen von $E \subset V$ nichtnegativ auf $v \in \ker \alpha$, so auch alle extremen Stützen von $E \cap \ker \alpha \subset \ker \alpha$, und unsere Induktion läuft. Liegt v bei keiner extremen Stütze im Kern, so suchen wir uns ein $e \in E$, das nicht im Kern aller extremen Stützen liegt, und wählen $\lambda \geq 0$ kleinstmöglich derart, daß die Ungleichungen $\alpha(v - \lambda e) \geq 0$ für alle extremen Stützen α weiter bestehen bleiben, aber mindestens eine, sagen wir zur extremen Stütze β, eine Gleichung $\beta(v - \lambda e) = 0$ wird. Dann zeigt dieselbe Induktion, daß sich $v - \lambda e$ positiv linear kombinieren läßt aus $d - 1$ Elementen von $E \cap \ker \beta$ und damit v aus d Elementen von E.



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 γ in $\ker \alpha$ zu einer extremen Stütze γ' verwackelt.

Fall 2: E besitzt keine extremen Stützen. Wir dürfen $V \neq 0$ annehmen und wählen unter allen $\alpha \in V^\top \backslash 0$ derart, daß $(\ker \alpha)$ von seinem Schnitt mit E erzeugt wird, ein α aus, für das die Kardinalität der Menge $E^+ = E^+(\alpha) := \{e \in E \mid \alpha(e) \geq 0\}$ maximal möglich wird. Nach Annahme finden wir dennoch ein $e^- \in E$ mit $\alpha(e^-) < 0$ und dürfen ohne Beschränkung der Allgemeinheit $\alpha(e^-) = -1$ annehmen. Dann betrachten wir die Projektion $\pi : v \mapsto v + \alpha(v)e^-$ von V auf $\ker \alpha$ längs e^-. Hätte $\pi(E^+)$ eine extreme Stütze β, so könnten wir diese durch die Vorschrift $\beta(e^-) = 0$ fortsetzen zu einer Linearform $\beta \in V^\top$ mit $\beta | E^+ \geq 0$ und $\beta(e^-) = 0$, und $\ker \beta$ wäre erzeugt von seinem Schnitt mit E, im Widerspruch zur Wahl von α. Also hat $\pi(E^+)$ keine extreme Stütze und nach Induktionsvoraussetzung läßt sich jeder Vektor aus $\ker \alpha$ positiv linear aus $\pi(E^+)$ kombinieren. Also läßt sich jedes $v \in V$ schon mal aus E linear kombinieren unter der Einschränkung, daß nur der Koeffizient vor e^- negativ sein darf. Weiter gibt es aber auch mindestens ein $e^+ \in E$ mit $\alpha(e^+) > 0$, sonst wäre ja $-\alpha$ eine extreme Stütze von E. Schreiben wir $-e^+$ in unserer eingeschränkten Weise und wenden α an, so erkennen wir, daß der Koeffizient von e^- positiv sein muß, und nach geeigneter Umformung stellen wir $-e^-$ dar als positive Linearkombination von Elementen von E^+. Damit läßt sich nun offensichtlich jeder Vektor aus V positiv linear aus E, ja sogar aus $E^+ \cup \{e^-\}$ kombinieren. Um schließlich zu zeigen, daß für solch eine Darstellung eines gegebenen Vektors v sogar d Elemente von E ausreichen, beginnen wir mit irgendeiner Darstellung $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$ als positive Linearkombination von Elementen von E. Benutzt sie mehr als d Elemente von E, so ist $(\lambda_1, \ldots, \lambda_n)$ ein Punkt aus dem Inneren des positiven Quadranten in k^n auf einer ganzen affinen Geraden von Lösungen der Gleichung $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$. Die Stelle, an der diese Gerade den positiven Quadranten verläßt, ist dann eine kürzere Darstellung von v als positive Linearkombination von Elementen von E. □

Korollar 7.4.11 (Hauptsatz über affine Ungleichungen). *Ist E eine endliche Teilmenge eines affinen Raums W über einem angeordneten Körper k, so gilt für jedes $p \in W$ genau eine der beiden folgenden Aussagen:*

1. *Der Punkt p liegt in der konvexen Hülle von E;*

2. *Es gibt eine affine Abbildung $\alpha : W \to k$ mit $\alpha(e) \geq 0 \quad \forall e \in E$ und $\alpha(p) < 0$.*

Im ersten Fall liegt p sogar bereits in der konvexen Hülle einer Teilmenge von E mit höchstens $(\dim W) + 1$ Elementen. Erzeugt E unseren affinen Raum W, so kann im zweiten Fall α sogar so gewählt werden, daß seine Nullstellenmenge von ihrem Schnitt mit E erzeugt wird.

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 7.4.12 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 E affin erzeugt wird.

7.4.12. Ist also W ein affiner Raum über einem angeordneten Körper und $E \subset W$ eine endliche Teilmenge, die unseren affinen Raum erzeugt, so ist die konvexe Hülle von E genau der Schnitt aller „abgeschlossenen Halbräume“, die E umfassen und deren „begrenzende Hyperebene“ von ihrem Schnitt mit E erzeugt wird. Diese Formulierung scheint mir der Anschauung besonders gut zugänglich. Im übrigen heißt eine Teilmenge eines affinen Raums über einem angeordneten Körper, die die konvexe Hülle einer endlichen Teilmenge ist, auch ein **Polytop**.

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 7.4.3. □

Korollar 7.4.13 (Satz von Caratheodory im Affinen). *Ist $W \supset T$ ein affiner Raum endlicher Dimension über einem angeordneten Körper mit einer ausgezeichneten Teilmenge, so liegt jeder Punkt aus der konvexen Hülle von T bereits in der konvexen Hülle einer Teilmenge von T mit höchstens $(\dim W) + 1$ Elementen.*

Beweis. Die konvexe Hülle von T ist die Vereinigung der konvexen Hüllen aller endlichen Teilmengen von T. Unser Korollar erweist sich so als unmittelbare Konsequenz aus dem vorhergehenden Hauptsatz über affine Ungleichungen 7.4.11. □

Definition 7.4.14. 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**.

7.4.15. 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 $v \in C \Rightarrow \lambda v \in C \; \forall \lambda \in k_{\geq 0}$.

7.4.16. Auf Englisch sagt man **cone** für „Kegel“ und **strongly convex cone** für „spitzer Konvexkegel“.

7.4.17. 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. Ein endlich erzeugter Konvexkegel heißt auch ein **polyedrischer Konvexkegel**.

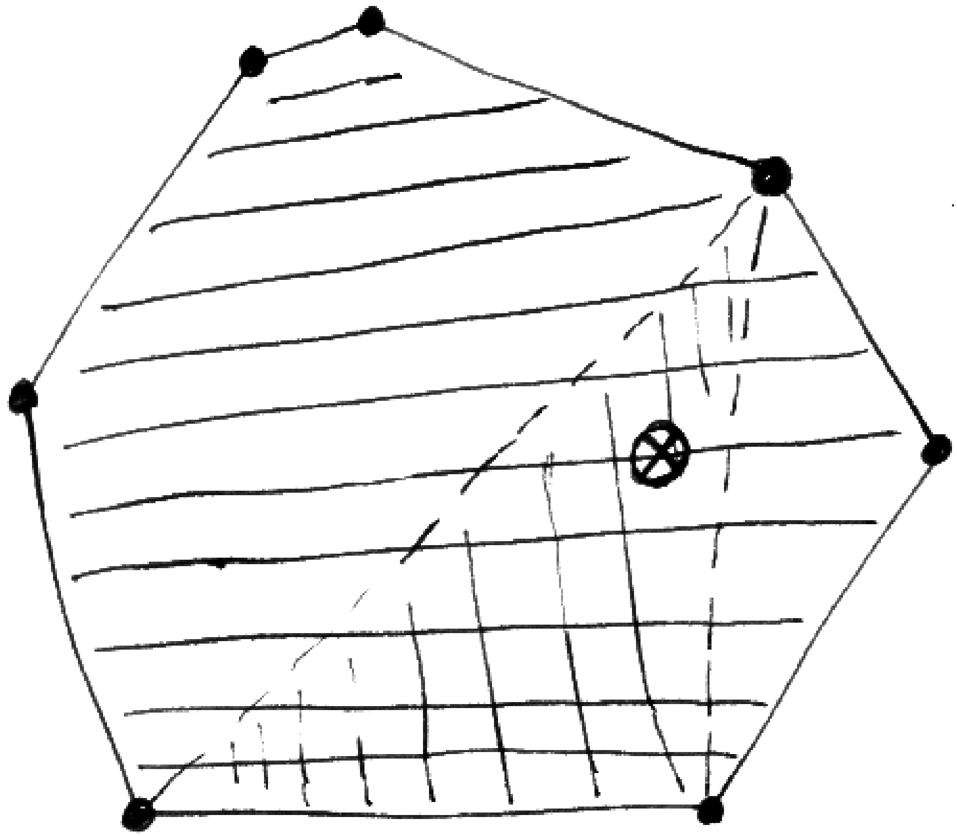


Illustration zum Satz von Caratheodory. Die konvexe Hülle der sieben fetten Punkte T ist das schraffierte Siebeneck, und jeder Punkt aus diesem Siebeneck liegt in der Tat auf einem Dreieck, dessen drei Ecken Ecken unseres Siebenecks sind.

7.4.18. Man beachte den Unterschied zwischen dem von einer Menge erzeugten Kegel und dem von derselben Menge erzeugten Konvexkegel.

Definition 7.4.19. Gegeben eine Teilmenge $E \subset V$ eines Vektorraums über einem angeordneten Körper definieren wir im Dualraum $V^\top$ unseres Vektorraums ihre **Polarenmenge** $E^\circ \subset V^\top$ durch die Vorschrift

$$E^\circ := \{\lambda \in V^\top \mid \lambda(e) \leq 1 \quad \forall e \in E\}$$

7.4.20. Die Polarenmenge eines Kegels C ist offensichtlich ein Konvexkegel und kann beschrieben werden durch die Formel

$$C^\circ = \{\lambda \in V^\top \mid \lambda(c) \leq 0 \, \forall c \in C\}$$

Die Polarenmenge eines Kegels nennt man auch den **dualen Kegel**. Daß diese Terminologie sinnvoll ist, zeigt der folgende Satz.

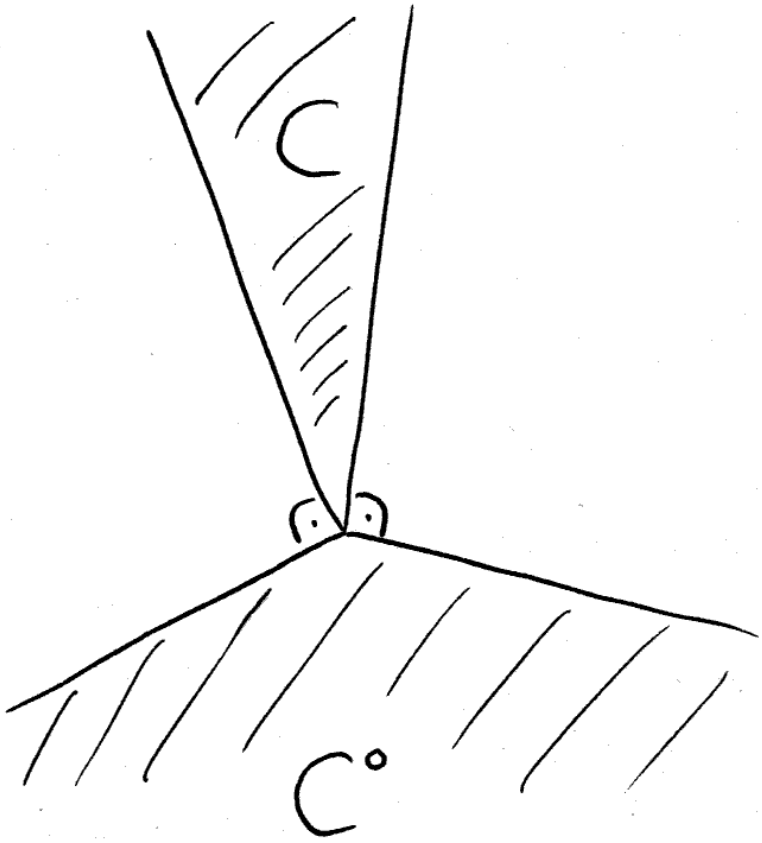
Satz 7.4.21 (von Farkas über duale Kegel). *Ist C ein endlich erzeugter Konvexkegel in einem endlichdimensionalen Vektorraum V über einem angeordneten Körper, so ist auch seine Polarenmenge $C^\circ \subset V^\top$ ein endlich erzeugter Konvexkegel und der kanonische Isomorphismus $V \xrightarrow{\sim} V^{\top\top}$ induziert eine Bijektion*

$$C \xrightarrow{\sim} C^{\circ\circ}$$

Beweis. Wir identifizieren im folgenden $V^{\top\top}$ und V vermittels des kanonischen Isomorphismus. Für jede Teilmenge $E \subset V$ gilt $E \subset E^{\circ\circ}$, und für einen endlich erzeugten Konvexkegel C haben wir nach dem Hauptsatz über lineare Ungleichungen 7.4.3 auch $C \supset C^{\circ\circ}$, mithin $C = C^{\circ\circ}$. Es bleibt nur zu zeigen, daß auch C° ein endlich erzeugter Konvexkegel ist. Wir zeigen dazu erst einmal, daß wir endlich viele Gleichungen $\lambda_1, \ldots, \lambda_r \in V^\top$ finden können mit

$$C = \{v \in V \mid \lambda_i(v) \geq 0 \quad \forall i\}$$

Sei in der Tat $E \subset C$ ein endliches Erzeugendensystem unseres Konvexkegels C. Erzeugt E schon ganz V als Vektorraum, so folgt unsere Behauptung aus dem Hauptsatz über lineare Ungleichungen 7.4.3, genauer seiner allerletzten Aussage. Andernfalls gilt es eben, geeignete Linearformen, $\lambda_1, \ldots, \lambda_s$ auf dem von C erzeugten Untervektorraum W zu wählen, diese auf V fortzusetzen, und noch genügend auf W verschwindende Linearformen hinzuzunehmen. Die Linearformen $-\lambda_1, \ldots, -\lambda_r \in V^\top$ 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° endlich erzeugt ist. □



Ein Konvexkegel und sein dualer Kegel im Richtungsraum $\vec{P}$ der Papierebene P, den wir dazu vermittels eines unter allen Kongruenzbewegungen invarianten Skalarprodukts $\langle\ ,\ \rangle$ durch $\operatorname{can} : \vec{P} \stackrel{\sim}{\rightarrow} \vec{P}^{\top}, v \mapsto \langle v,\ \rangle$ mit seinem Dualraum identifiziert haben, so daß wir erhalten

$$\operatorname{can}^{-1}(C^{\circ}) = \{v \mid \langle v, c \rangle \leq 0 \ \forall c \in C\}$$

Ein Punkt der Papierebene stellt dabei denjenigen Richtungsvektor dar, der vom „Zentrum“ unseres Bildes zum entsprechenden Punkt schiebt.

Korollar 7.4.22 (**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.*

7.4.23. Die Bedingung „endlich erzeugt“ ist hier wesentlich. Zum Beispiel wäre die Menge aller Punkt 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 E umfaßt E° eine Gerade genau dann, wenn E nicht den ganzen Raum erzeugt. Mit 7.4.21 folgt $(1) \Leftrightarrow (3)$. Die Implikation $(2) \Rightarrow (1)$ ist offensichtlich. Um schließlich $(3) \Rightarrow (2)$ zu zeigen wählen wir nach 7.4.21 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. □

Übungen

Übung 7.4.24. 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 7.4.25. Gegeben ein Konvexkegel K in einem Vektorraum über einem angeordneten Körper, der den ganzen Vektorraum erzeugt, läßt sich jede Abbildung $\varphi : K \to W$ in einen weiteren Vektorraum mit $\varphi(v + w) = \varphi(v) + \varphi(w)$ sowie $\varphi(\alpha v) = \alpha\varphi(v)$ für alle $v, w \in K$ und $\alpha > 0$ auf genau eine Weise zu einer linearen Abbildung $K \to W$ fortsetzen.

Ergänzende Übung 7.4.26 (**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 7.4.27. Gegeben eine Teilmenge E eines affinen Raums über einem angeordneten Körper k bezeichne $\operatorname{konv}(E)$ ihre konvexe Hülle. Ist E die Standardbasis des k^n und $W \subset k^n$ ein affiner Teilraum, so zeige man, daß ein Punkt p extrem ist im Schnitt $W \cap \operatorname{konv}(E)$ genau dann, wenn er für mindestens eine Teilmenge $E' \subset E$ der einzige Punkt von $W \cap \operatorname{konv}(E')$ ist.

Übung 7.4.28. 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 7.4.21 über duale Kegel

$$(C \cap D)^\circ = C^\circ + D^\circ$$

Gegeben endlich viele Linearformen $\alpha_1, \ldots, \alpha_n \in V^*$ hat insbesondere der Konvexkegel $C := \{v \mid \alpha_i(v) \geq 0 \ \forall i\}$ als dualen Kegel C° den Kegel aller negativen Linearkombinationen der α_i, in Formeln

$$C^\circ = \left\{ \sum_i x_i \alpha_i \,\middle|\, x_i \leq 0 \ \forall i \right\}$$

Übung 7.4.29 (**Starker Dualitätssatz der linearen Optimierung**). Ungleichungen zwischen Vektoren des $\mathbb{R}^n$ oder $\mathbb{R}^m$ sind im folgenden stets komponentenweise zu verstehen. Seien $A \in \operatorname{Mat}(n \times m; \mathbb{R})$ 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 $\{(x,t) \in \mathbb{R}^{m+1} \mid (c^\top | -\delta)\binom{x}{t} \leq 0\} \supset \{(x,t) \in \mathbb{R}^{m+1} \mid \left(\begin{smallmatrix} A & -b \\ 0 & -1 \end{smallmatrix}\right)\binom{x}{t} \leq 0\}$;

4. Unser d ist das Kleinste aller $\delta \in \mathbb{R}$ mit $\mathbb{R}_{\geq 0}(-c^\top | \delta) \subset \{(y^\top | \gamma)\left(\begin{smallmatrix} A & -b \\ 0 & -1 \end{smallmatrix}\right) \mid (y, \gamma) \in \mathbb{R}^{n+1}, (y, \gamma) \leq 0\}$;

5. Unser d ist das Kleinste aller $\delta \in \mathbb{R}$, für das $y \geq 0$ und $\gamma \geq 0$ existieren mit $(-c^\top | \delta) = (-y^\top A | y^\top b + \gamma)$;

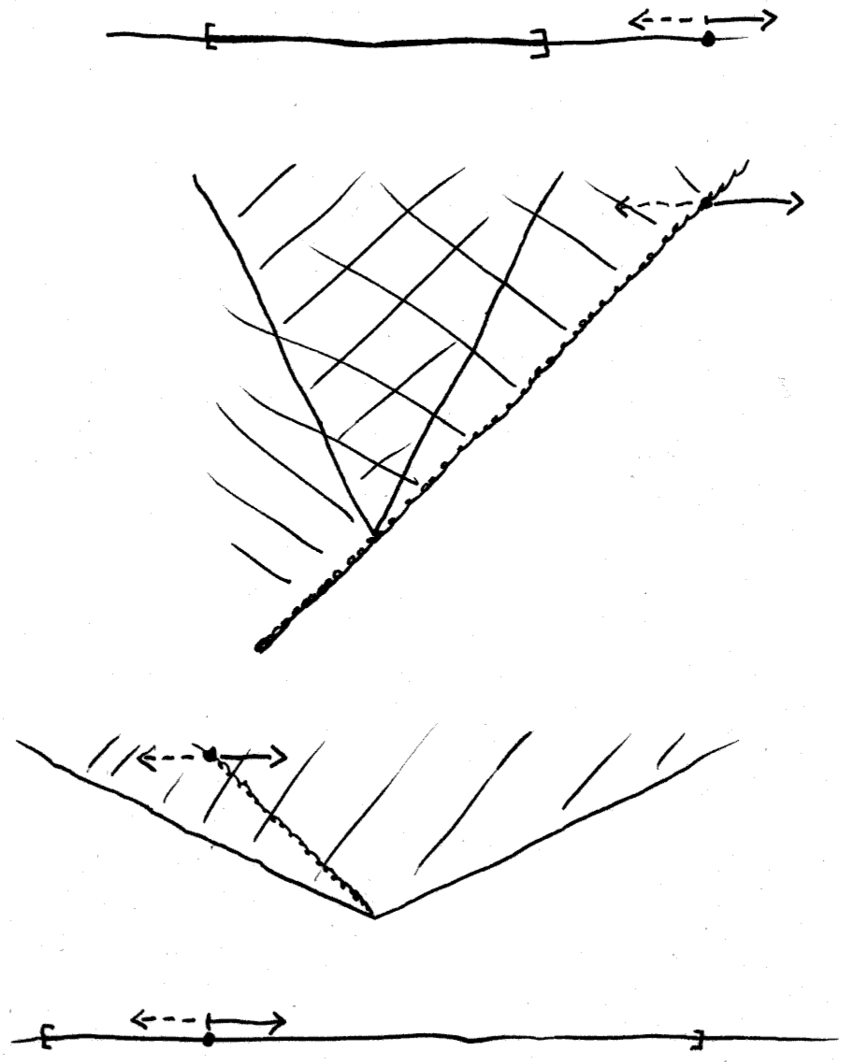


Illustration zum starken Dualitätssatz. Die Frage des Maximums wird übersetzt in eine Frage nach dem Enthaltensein von Kegeln und dualisiert durch Übergang zu den dualen Kegeln. Der duale Kegel zu einem Halbraum ist dabei ein Strahl.

6. Unser d ist das Minimum der linearen Funktion $y \mapsto y^\top b$ auf der Menge aller $y \in \mathbb{R}^n$ mit $y \geq 0$ und $c^\top = y^\top A$.

Beim Übergang zwischen 3 und 4 benötigt man Übung 7.4.28, die anderen Übergänge sind elementar. Die Äquivalenz von 1 und 6 heißt der **starke Dualitätssatz**.

8 Danksagung

Für Korrekturen und Verbesserungen danke ich Judith Bender, Anna Staron, Markus Junker, Olaf Schnürer, Bernhard Krötz. Besonders danke ich Veronika Thierfelder, deren fundamentale allgemeine Ratschläge zur Darstellung mir sehr geholfen haben. Bei der Behandlung von Fragen der Inzidenzgeometrie war mir ein Skript von Hubert Kiechle sehr hilfreich.

9 Die Vorlesung LA1 im Wintersemester 14/15

Es handelte sich um eine vierstündige Vorlesung, also 4×45 Minuten Vorlesung, mit 2 Stunden Übungen. Für die Darstellung der Grundlagen fand keine Abstimmung mit anderen Grundvorlesungen statt.

20.10 Fibonnacci-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 1.9.12, 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 $K^n \to K^m$, 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, Nullteiler, 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. Besprechung 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 invarianter Skalarprodukte noch nicht ganz fertig, Eindeutigkeit noch nicht gemacht.

29.1 Beweis der Existenz und Eindeutigkeit invarianter Skalarprodukte für Kongruenzebenen. Tensorprodukt mit eindimensionalem Raum, Längengerade, 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 Teilräume, 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, Abfaktorisieren von Wurzeln, Quotientenkörper, Partialbruchzerlegung.
10. Signum, Determinante, Multiplikationsformel, Entwicklungssatz, Cramer'sche Regel.
11. Eigenwerte, Eigenvektoren, charakteristisches Polynom, Trigonalisierbarkeit, Diagonalisierbarkeit, Cayley-Hamilton.

Literatur

[AL] *Skriptum Algebra und Zahlentheorie;*.

[AN1] *Skriptum Analysis 1;*.

[AN2] *Skriptum Analysis 2;*.

[AN3] *Skriptum Analysis 3;*.

[FT1] *Skriptum Funktionentheorie 1;*.

[GR] *Skriptum Grundlagen;*.

[KAG] *Skriptum Kommutative Algebra und Geometrie;*.

[LA2] *Skriptum Lineare Algebra 2;*.

[ML] *Skriptum Mannigfaltigkeiten und Liegruppen;*.

[Sch86] Alexander Schrijver, *Theory of linear and integer programming*, Wiley, 1986.

[TF] *Skriptum Fundamentalgruppe und Überlagerungstheorie;*.

[TM] *Skriptum Topologie und kompakte Gruppen;*.

[Wey35] Hermann Weyl, *Elementare Theorie der konvexen Polyeder*, Comment. Math. Helv. **7** (1935), 290–306, In den gesammelten Abhandlungen: Band III, S 517–533.

Index

$/$ Quotient, 131
0
  einelementige Gruppe, 17
  natürliche Zahl, 116
  Nullvektorraum, 17
$0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \in \mathbb{N}$, 119
0_K Null des Körpers K, 5
$1 = 1_R$ Eins eines Rings, 128
$K[X]$ Polynomring, 140
$K[X_1, \ldots, X_n]$ Polynomring, 146
$S^{-1}R$ Lokalisierung
  von Integritätsbereich, 157
$[f]$ Matrix von f, 59
Δ Diagonale, 19
$*$ einziges Element von ens, 21
$\bigcap$ Schnitt, 28
$\circ$
  Matrixprodukt, 62
$\langle \lambda, v \rangle$ Auswerten einer Linearform, 105
$|$ teilt, 134
$\oplus$ direkte Summe
  von Vektorräumen, 22
$\overline{xy}$ Gerade durch x und y, 215
$\overrightarrow{AB}$ Richtungsvektor, 75
$\vec{v} + p$ Verschieben von Punkt um Richtungsvektor, 74
${}^t f$ transponierte Abbildung, 100
b^* Vektoren der dualen Basis, 98
$b^\top$ Vektoren der dualen Basis, 98
f^* transponierte Abbildung, 100
$f^\top$ transponierte Abbildung, 100
$K(X)$ rationale Funktionen
  in einer Variablen X, 157
$K((X))$ formale Laurentreihen, 148
$\langle T \rangle_K = \langle T \rangle$ Untervektorraum-Erzeugnis, 27
$K[X]$ Polynomring, 140
$K[[X]]$ formale Potenzreihen, 148
$V^{\mathbb{R}}$ Reellifizierung von V, 39
$A^\top$ transponierte Matrix, 64
X^n für n-Tupel in X, 21
$X^{\times n}$ für n-Tupel in X, 21
${}^t A$ transponierte Matrix, 64
$\|$ gleich oder parallel, 200
$p - q$
  bei affinem Raum, 75
$\geq, >, \leq, <$ bei Ordnungsrelation, 23
$(x_0; x_1; \ldots; x_n)$ Punkt des $\mathbb{P}^n K$, 212
$[x_0, x_1, \ldots, x_n]$ Punkt des $\mathbb{P}^n K$, 212
$\langle x_0, x_1, \ldots, x_n \rangle$ Punkt des $\mathbb{P}^n K$, 212

$\text{Ab}\, X$
  Endomorphismenring der abelschen Gruppe X, 129
Abbildung
  Projektionsabbildung, 19
ABC-Vermutung, 125
abgeschlossen
  algebraisch, 143
Abschluß
  projektiver, 213
Abspalten von Linearfaktoren, 142
Acht als natürliche Zahl, 119
Addition
  in Ring, 128
  natürlicher Zahlen, 117
adjunkt
  Matrix, 183
Äquivalenzklasse, 154
Äquivalenzrelation
  auf einer Menge, 154
  erzeugt von Relation, 155
Aff affine Abbildungen, 77
affin
  Abbildung, **77**

Raum, **74**
Raum, über Vektorraum, **74**
Teilraum
von affinem Raum, 79
unabhängig, **85**
Algebra
$\mathbb{Z}$-Algebra, 128
algebraisch
abgeschlossen, Körper, 143
Algebrenhomomorphismen, 129
allgemeine lineare Gruppe, 47, 67
$\mathrm{Alt}^n(V)$ alternierende Multilinearformen, 178
$\mathrm{Alt}^n(V, W)$ alternierende multilineare Abbildungen, 178
alternierend
bilineare Abbildung, 176
multilineare Abbildung, 177
alternierende Gruppe, 169
anneau, 128
Anordnung, 23
anschaulich, 15
Anschauungsraum, 15
antisymmetrisch
bilineare Abbildung, 177
Relation, 23
Assoziativgesetz
bei Vektorraum, 14
aufgespannt
Untervektorraum, 27
aufsteigende Vereinigung, 42
Auswahlaxiom, 40
Auswahlaxiom, Variante, 40
Auswahlfunktion, 40
Auswertungsabbildung, 99
Automorphismengruppe
eines Vektorraums, 47
Automorphismus
eines Vektorraums, 47
von affinem Raum, 77
baryzentrische Koordinaten, 88
Basis, 30
angeordnete, 30
duale, 99
indizierte, 30
negativ orientierte, 186
orientierte, 186
positiv orientierte, 186
von Vektorraum, 29
Basisexistenzsatz, 31
Basismatrix, 68
Basiswechselmatrix, 93
Betrag
bei Quaternionen, 164
Bidualraum, 103
Bild
von linearer Abbildung, 51
bilinear
bei Vektorräumen, 57
Bilinearform, 58
Binärdarstellung, 119

$\mathbb{C}$ komplexe Zahlen, 108
Caratheodory, Satz von
im Affinen, 231
lineare Version, 226
Cayley-Hamilton, 195
χ_A charakteristisches Polynom, 192
char Charakteristik, 137
char charakteristisches Polynom, 192
Charakteristik
eines Rings, 137
charakteristisches Polynom, 192
von Endomorphismus, 192
χ_f charakteristisches Polynom, 192
codim Kodimension
bei affinen Räumen, 81
cone
englisch für Kegel, 231
strongly convex, 231
corps gauche, 162

Cramer'sche Regel, 183

$D(f)$ Definitionsbereich von f, 158
Δ Diagonale, 19
darstellende Matrix, 59, 90
Definitionsbereich, 158
degré, 141
degree, 141
Desargues-Eigenschaft
    affine, 202
    projektive, 219
$\det$ Determinante
    einer Matrix, 170
    von Endomorphismus, 182
$\det_K$ Determinante
    von Endomorphismus, 182
Determinante
    einer Matrix, 170
    von Endomorphismus, 182
Dezimaldarstellung, 119
Dezimalsystem, 119
$\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ Diagonalmatrix, 69
Diagonale, 19
diagonalisierbar
    Endomorphismus, 194
    Matrix, 194
Diagonalmatrix, 69
Differenzraum, von affinem Raum, 74
Diffie-Hellman, 136
Diffie-Hellman-Problem, 137
$\dim$ Dimension eines Vektorraums, 35
Dimension
    eines affinen Raums, **74**
    eines Vektorraums, 35
    physikalische, 35
Dimensionsformel
    für lineare Abbildungen, 52
direkte Summe
    von Vektorräumen, 22
diskret
    Logarithmus, 136

Distributivgesetz, 128
    bei Körper, 5
    bei Vektorraum, 14
Divisionsring, 162
Doppelordnung, 211
Doppeltransposition, 170
Drei als natürliche Zahl, 119
Dreieck, 200
Dreiecksungleichung
    für komplexen Absolutbetrag, 113
dual
    Basis, 99
    projektive Inzidenzebene, 219
duale Abbildung, 100
dualer Kegel, 233
Dualitätssatz
    der linearen Optimierung, 236
Dualraum, 96
Dualsystem, 119

E_{ij} Basismatrizen, 68
$\mathbb{E}$ Anschauungsraum, 75
Ebene
    affine, 74, 79
    unendlich ferne, 213
Eigenraum, 190
Eigenvektor, 190
Eigenwert, 190
Einheit
    von Ring, 134
Einheitsmatrix, 60
einhüllende Gruppe, 155
Eins als natürliche Zahl, 119
Eins-Element
    in Ring, 128
Einschluß-Ausschluß-Formel, 131
Einsetzungshomomorphismus, 140
Eintrag von Matrix, 11
Elementarmatrix, 69
    spezielle, 69
End

Endomorphismenring
von abelscher Gruppe, 129
End_k
Endomorphismenring
von k-Vektorraum, 129
endlich
Menge, 114
endlich erzeugbar, 27
endlich erzeugt
Vektorraum, 27
endliche Primkörper, 135
Endomorphismenring
von abelscher Gruppe, 129
von Vektorraum, 129
Endomorphismus
von abelscher Gruppe, 129
von Vektorräumen, 47
ens einelementige Menge, 21
erzeugende Funktion
der Fibonacci-Folge, 160
Erzeugendensystem, 27
von affinem Raum, 79
Erzeugnis
in Vektorraum, 27
erzeugt
Äquivalenzrelation, 155
affiner Teilraum, 79
Untergruppe, 121
Untervektorraum, 27
erzeugt, endlich
Vektorraum, 27
Euklid
Lemma von, 124
ev Evaluation, 103
Evaluationsabbildung, 103

Faktor, 19
Familie, 29
Farkas, Lemma von, 226
Farkas, Satz von, 233
Fehlstand, 166
Fixpunkt, 49
Fixvektor, 49
Form
allgemein, 98
Fortsetzung
lineare, 56
Frac Quotientenkörper, 156
fraction field, 156
frei
Vektorraum, 56
Frobenius-Homomorphismus, 138
Fünf als natürliche Zahl, 119
Fundamentalsatz der Algebra, 143
Funktion
rationale, 157
Funktionenkörper, 157

Gauß-Algorithmus, 7
general linear group, 47, 67
gerade
Permutation, 166, 170
Zahl, 133
Gerade
affine, 74, 79
unendlich ferne, 213, 216
Geradensegment, 88
Geschwindigkeit
vektorielle, 76
$\mathrm{GL}(V)$ allgemeine lineare Gruppe, 47
$\mathrm{GL}(n; K)$ allgemeine lineare Gruppe, 67
Gleichungssystem, 7
lineares, 7
Goldbach-Vermutung, 123
grad
Grad
eines Polynoms, 141
Grad
eines Polynoms, 141
größter gemeinsamer Teiler, 123
größtes Element, 23, 41
Grundkörper, 14

Gruppe
einhüllende, 155
Gruppe der Einheiten, 134

Halbordnung, 23
Hamilton'sche Zahlen, 163
Hauptsatz
über lineare Ungleichungen, 223
Hertz, 189
Hexadezimalsystem, 119
$\mathrm{Hom}^{(2)}$ bilineare Abbildungen, 58
$\mathrm{Hom}^{(n)}$ multilineare Abbildungen, 177
homogen, homogenisieren
lineares Gleichungssystem, 7
Homomorphismus
von Vektorräumen, 47
Homothetie, 78, 206
Hülle
lineare, 27
Hyperebene
affine, 80
lineare, 28
unendlich ferne, 213

i Wurzel aus -1 in $\mathbb{C}$, 108
$\mathrm{I} = \mathrm{I}_n$ Einheitsmatrix, 60
Idempotent
Elemente, 54
im
Bild von linearer Abbildung, 51
image, 51
Imaginärteil
bei komplexen Zahlen, 109
in_i
Injektionen bei Summen, 48
induktiv geordnet, 41
Injektion
kanonische, 48
Integritätsbereich, 134
invers
Matrix, 67
Inverse
Matrix, 67
Inversion, 111
invertierbar
in Ring, 134
Matrix, 67
Inzidenzebene
über Schiefkörper, 200
Inzidenzebene
abstrakte affine, 218
affine konkrete, 200
projektive abstrakte, 218
projektive konkrete, 215
Inzidenzstruktur, 218
isomorph
Vektorräume, 47
Isomorphismus
von affinen Räumen, 77
von Vektorräumen, 47
iteriertes Anwenden, 116

Jägerzaunformel, 171

kanonisch
Injektion, 48
kartesisch
Produkt
endlich vieler Mengen, 18
Kegel, 231
dualer, 233
spitzer, 231
ker
Kern von linearer Abbildung, 51
Kern
von linearer Abbildung, 51
Kette
in partiell geordneter Menge, 41
kgV kleinstes gemeinsames Vielfaches, 126
kleinstes
Element, 25

kleinstes gemeinsames Vielfaches, 126
Kodimension
  bei affinen Räumen, 81
Koeffizient, 7
  von Polynom, 139
Koeffizientenmatrix, 9
  erweiterte, 9
Körper, 5
kolinear, 200
kommutativ
  Rechteck, 104
kommutativer Ring, 128
kommutieren, 141
komplementär
  Untervektorräume, 53
komplexe Zahlen, 108
  vergeßliche, 108
Komponente
  eines Tupels, 19
kongruent modulo, 131
konjugierte komplexe Zahl, 111
konstant
  Polynom, 140
konv konvexe Hülle, 236
konv(T) konvexe Hülle von T, 88
konvex
  in affinem Raum, 88
konvexe Hülle, 88
Konvexkegel, 231
  polyedrischer, 231
Konvexkegell
  erzeugt von, 231
Koordinaten, 98
  affine, 80
Koordinatenfunktionen, 98
Koordinatensystem
  affines, 80
kopunktal, 219
Kovektor, 96
Kreis
  verallgemeinerter, 113
Kreisgruppe, 111
Kring
  kommutativer Ring, 128
Kroneckerdelta, 60
kubisch
  Polynom, 142
Kürzen in Ringen, 134

$l(\sigma)$ Länge von Permutation, 166
Länge
  von Permutation, 166
Laurententwicklung
  algebraische, 158
Laurentreihe
  formale, 148
leer
  Familie, 29
Leibniz-Formel, 171
Leitkoeffizient, 141
lin Spann, 27
Lin(E) Linearisierung von E, 214
linear
  Abbildung, 47
  Funktion, 48
  Polynom, 142
linear abhängig
  Familie, 30
  Teilmenge, 29
linear unabhängig
  Familie, 30
  Teilmenge, 28, 33
lineare Abbildung
  schulische Konvention, 77
lineare Anteil, 77
lineare Gruppe
  allgemeine, 47
lineare Hülle, 27
lineare Ordnung, 23
Linearfaktor, 143
Linearfaktoren
  Zerlegung in, 144

Linearform, 96
Linearisierung
  eines affinen Raums, 214
Linearkombination, 27
Linksinverses, 73
Linksnebenklasse, 131
Lösungsmenge, 7
Logarithmus
  diskreter, 136

$\mathrm{M}(f)$ Matrix von f, 59
$\mathrm{Mat}(n \times m; Z)$ Menge von Matrizen, 11
Matrix, 11
  quadratische, 11
Matrixmultiplikation, 62
max, 23
maximal
  Element, 23, 41
min, 23
minimales
  Element, 25
Minor einer Matrix, 184
Möbiusfunktion
  allgemeine, 95
  der Zahlentheorie, 96
monic polynomial, 142
multilinear, 177
Multilinearform, 178
Multiplikation
  in Ring, 128
  natürlicher Zahlen, 118

Nachfolger, 114
natürliche Zahlen, 114
negativ
  Vektor, 187
Neun als natürliche Zahl, 119
nichtnegativ
  Vektor, 187
nilpotent
  Element, 129
  Endomorphismus, 94
Norm
  einer komplexen Zahl, 109
normiert
  Polynom, 142
Null, 116
Nullring, 129
Nullstelle, 141
Nullteiler, 134
nullteilerfrei, 134
Nullvektor, 14
Nullvektorraum, 17
numerisch
  Polynom, 153

Operation
  von Grundkörper auf Vektorraum, 14
$\mathrm{or}(V)$ Orientierungsmenge
  eines Vektorraums, 186
Ordnung
  auf einer Menge, 23
  einer Nullstelle, 143
  lineare, 23
  partielle, 23
  totale, 23
Ordnungsrelation, 23
Orientierung
  von Vektorraum, 185
Orientierungsmenge
  eines Vektorraums, 186

$\mathbb{P}W$ projektiver Raum zu W, 212
$\mathbb{P}^n K$ projektiver Raum, 212
  zu Schiefkörper, 216
Paarung
  kanonische, 99
Pappus-Eigenschaft, 221
  affine, 207
parallel

affine Teilräume, 80
in affiner Inzidenzebene, 200
Partialbruchzerlegung, 159
partiell
Ordnung, 23
Polarenmenge, 233
Polstelle
von rationaler Funktion, 158
Polynom
konstantes, 140
numerisches, 153
Polynomring, 139, 140
Polytop, 231
poset, 23
positiv
Vektor, 187
positiv orientiert
Vektor, 187
Potenzmenge, 27
Potenzreihe
formale, 148
pr_i
Projektion, 19
prim
Restklasse, 133
Primfaktorzerlegung
Existenz, 122
Primkörper, 136
Primzahl, 122
Primzahlzwillinge, 123
Produkt
von Matrizen, 60
von Vektorräumen
endliches, 22
Projektion
längs Teilraum, 54
von kartesischem Produkt, 19
projektiver Raum
als Menge, 212
Projektivisierung, 212
Punkt
unendlich ferner, 213
von affinem Raum, **74**
Punktspiegelung, 78
pythagoreische Zahlentripel, 152

quadratisch
Matrix, 11, 67
Polynom, 142
Quaternionen, 163
Quaternionengruppe, 164
Quaternionenring, 164
Quersumme, 133
Quot Quotientenkörper, 156
Quotient, 131
Quotientenkörper, 156

Rang
einer linearen Abbildung, 72
einer Matrix, 71
rank, 71
rationale Funktion, 157
Raum
affiner, **74**
der Anschauung, 15
reeller, **74**
Realteil
bei komplexen Zahlen, 109
bei Quaternionen, 164
Rechtsinverses, 40, 73
redundant, 29
reell
Raum, **74**
Reellifizierung, 39
reflexiv
Relation, 23
regulär
Matrix, 67
Relation
auf einer Menge, 23, 153
zwischen zwei Mengen, 23
Repräsentant, 131, 154

Repräsentantensystem, 131, 154
Restklasse, 131
  prime, 133
Richtungsanteil, 77
Richtungsraum, **74**
  schmutziger, 15
Richtungsvektor, **74**
Richtungsvektoren, 204
Riemann'sche Zahlenkugel, 214
Ring, 128
Ring Ringhomomorphismen, 129
Ringhomomorphismus, 129
rk Rang einer Matrix, 71

S^1 Einheitskreis, 111
Σ_n symmetrische Gruppe, 166
$\mathcal{S}_n$ symmetrische Gruppe, 166
Schiefkörper, 5, 162
Schnitt, 40
  von Mengensystem, 28
Schwerpunkt, 85
Sechs als natürliche Zahl, 119
Sekunde, 189
Sieb des Eratosthenes, 122
Sieben als natürliche Zahl, 119
$\operatorname{sign}(a)$ Vorzeichen von a, 185
Signum, 170
Signum einer Permutation, 166
Skalar, 14
skew field, 162
Smith-Normalform, 69, 93
Spaltenindex, 11
Spaltenrang, 71
span Spann, 27
Spann
  in Vektorraum, 27
Spur
  einer Matrix, 94
  eines Endomorphismus, 94, 95
Standardbasis, 30
Standardorientierung, 186
Streckung, 78
Streichmatrix, 182
streng induktiv geordnet, 43
Supremum, 43
Symmetrie
  für Relation, 154
symmetrisch
  bilineare Abbildung, 176
symmetrische Gruppe, 166
System von Teilmengen, 28

$\mathbb{T}$ Zeit, 76, **189**
Teilen in Polynomringen, 142
Teiler, 123, 134
teilerfremd
  Elemente eines Krings, 135
  ganze Zahlen, 123
Teilraum, 25
Teilring, 130
teilt, 123, 134
totale Ordnung, 23
Totalität
  für Relation, 23
tr Spur alias „trace“, 94
tr Spur alias „trace“ , 94
tr_K Spur alias „trace“, 94
trace
  einer Matrix, 94
trans, 75
transitiv
  Relation, 23
Translation
  von affinem Raum, **74**
transponiert
  Abbildung
    bei Vektorräumen, 100
  Matrix, 64
Transposition, 166
trigonalisierbar, 193
Tripel, 19
Tupel

angeordnete, 19

$\bigcup$ Vereinigung, 28
Umin, 100
unendlich
ferne Ebene, 213
ferne Gerade, 213, 216
ferne Hyperebene, 213
ferner Punkt, 213, 216
Menge, 114
Unendlichkeitsaxiom, 114
ungerade
Permutation, 166, 170
Zahl, 133
Universelle Eigenschaft
des Raums der Äquivalenzklassen, 154
Untergruppe, 120
erzeugt von Teilmenge, 121
triviale, 120
Untervektorraum, 25
unverkürzbar
Erzeugendensystem, 31
unverlängerbar
linear unabhängige Teilmenge, 31

$\mathbb{V}E$ projektive Vervollständigung von E, 213
van-der-Monde-Determinante, 184
Variable
von Polynom, 139
Vektor
Element eines Vektorraums, 14
Vektorraum, 14
Vereinigung
aufsteigende, 42
von Mengensystem, 28
vergeßliche komplexe Zahlen, 108
verkürzbar
Erzeugendensystem, 31
verlängerbar
linear unabhängige Teilmenge, 31
Verschlüsselung
Diffie-Hellman, 136
Vervollständigung
projektive, 213
Vielfachheit
einer Nullstelle, 143
Vier als natürliche Zahl, 119
Viereck, 215
in der projektiven Inzidenzebene, 218
voll
Rang, 71
vollständige Induktion, 117

Weierstraß
Vorbereitungssatz, 148
Wilson
Satz von, 139
wohldefiniert, 154
Wurzel
von Polynom, 141

$\times$
Produkt von Abbildungen, 19

Zahl
gerade, 133
Hamilton'sche, 163
komplexe, 108
ungerade, 133
Zahldarstellungen, 119
Zahlenebene, 109
Zahlenkugel, Riemann'sche, 214
Zehn als natürliche Zahl, 119
Zeilenindex, 11
Zeilenrang, 71
Zeilenstufenform, 9
Zeilenvektor, 64
Zeit, 189
Zeiteinheit
nichtrelativistische, 189
Zeitpunkt, 76

Zeitspanne, 76, 189
Zorn’sches Lemma, 41
Zwei als natürliche Zahl, 119