Beispiele für Gruppen, Körper und Vektorräume

Jendrik Stelzner

25. Dezember 2015

Vorwort

Inhaltsverzeichnis

1. Definitionen und Notationen

1.1. Gruppen

Definition 1.1. *Eine* Gruppe *ist ein Paar $(G, \cdot)$ bestehend aus einer Menge G und einer binären Verknüpfung $\cdot\colon G \times G \to G$, $(g, h) \mapsto g \cdot h$, die die folgenden Bedingungen erfüllt:*

i) Die Verknüpfung $\cdot$ ist assoziativ, d.h. für alle $g_1, g_2, g_3 \in G$ ist $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

ii) Es gibt ein neutrales Element *$e \in G$, d.h. $e \cdot g = g \cdot e = g$ für alle $g \in G$.*

iii) Für jedes Element $g \in G$ gibt es ein inverses Element *$h \in G$, d.h. $g \cdot h = h \cdot g = e$.*

Die Gruppe $(G, \cdot)$ heißt abelsch[1]*, bzw.* kommutativ*, falls $g \cdot h = h \cdot g$ für alle $g, h \in G$.*

Bemerkung 1.2. Es sei $(G, \cdot)$ eine Gruppe.

1. Wegen der Assoziativität von $\cdot$ ist das Produkt $g_1 \cdots g_n$ für alle $n \geq 1$ und $g_1, \ldots, g_n \in G$ wohldefiniert.

2. Je zwei neutrale Element $e, e' \in G$ sind gleich, da $e = e \cdot e' = e'$. Man spricht daher von *dem* neutralen Element von G.

3. Für jedes $g \in G$ sind je zwei inverse Elemente h, h' von g gleich, da

$$h = h \cdot e = h \cdot g \cdot h' = e \cdot h' = h'.$$

   Man spricht daher von *dem* inversen Element von g und schreibt g^{-1} für dieses.

4. Es genügt zu fordern, dass es ein linksneutrales Element $e \in G$ gibt, d.h. dass $e \cdot g = g$ für alle $g \in G$, und dass jedes $g \in G$ ein linksinverses Element $h \in G$ gibt, d.h. dass $h \cdot g = e$. Es folgt dann, dann e auch rechtsneutral ist (d.h. $g \cdot e = g$ für alle $g \in G$) und ein linksinverses Element $h \in G$ von g auch schon rechtsinvers ist (d.h. $g \cdot h = e$).

5. Für jedes $g \in G$ ist $g^{-1} \cdot g = g \cdot g^{-1} = e$ also g das Inverse zu g^{-1}, und somit $g = (g^{-1})^{-1}$.

6. Für alle $g, h \in G$ ist $(h^{-1} \cdot g^{-1}) \cdot (g \cdot h) = h^{-1} \cdot g^{-1} \cdot g \cdot h = h^{-1} \cdot e \cdot h = h^{-1} \cdot h = e$, also $h^{-1} \cdot g^{-1}$ das (Links)inverse zu $g \cdot h$ und somit $h^{-1} \cdot g^{-1} = (g \cdot h)^{-1}$.

7. Ist $(G, \cdot)$ abelsch, so schreibt man die Verknüpfung häufig nicht *multiplikativ* (d.h. als $\cdot$), sondern *additiv* (d.h. als $+$).

[1] Benannt nach dem norwegischen Mathematiker Niels Henrik Abel.

8. Schreibt man eine Gruppe $(G, \cdot)$ multiplikativ, so bezeichnet man das neutrale Element häufig mit 1 statt e. Man schreibt auch gh statt $g \cdot h$. Für alle $g \in G$ und $n \in \mathbb{Z}$ schreibt man abkürzend

$$g^n \coloneqq \begin{cases} \underbrace{g \cdots g}_{n \text{ viele}} & \text{falls } n \geq 1 \\ 1 & \text{falls } n = 0 \\ (g^{-}1)^{-n} & \text{falls } n \leq -1. \end{cases}$$

Es gilt dann $g^n \cdot g^m = g^{n+m}$ für alle $g \in G$ und $n, m \in \mathbb{Z}$, sowie $g^0 = 1$ und auch $(g^n)^{-1} = (g^{-1})^n = g^{-n}$ für alle $g \in G$ und $n \in \mathbb{Z}$.

9. Schreibt man eine abelsche Gruppe $(A, +)$ additiv, so bezeichnet man das neutrale Element mit 0 und das neutrale Element von $a \in A$ als $-a$. Für alle $a \in A$ und $n \in \mathbb{Z}$ schreibt man dann abkürzend

$$na \coloneqq n \cdot a \coloneqq \begin{cases} \underbrace{a + \cdots + a}_{n \text{ viele}} & \text{falls } n \geq 1 \\ 0 & \text{falls } n = 0 \\ (-n) \cdot (-a) & \text{falls } n \leq -1. \end{cases}$$

Es gilt dann $n \cdot a + m \cdot a = (n+m) \cdot a$ für alle $a \in A$ und $n, m \in \mathbb{Z}$, $n \cdot (a+b) = n \cdot a + n \cdot b$ für alle $n \in \mathbb{Z}$ und $a, b \in A$, sowie $0 \cdot a = 0$ und $-(n \cdot a) = n \cdot (-a) = (-n) \cdot a$ für alle $a \in A$ und $n \in \mathbb{Z}$.

10. Obwohl eine Gruppe, per Definition, ein Paar $(G, \cdot)$, bzw. $(G, +)$ ist, nennt man die Verknüpfung $\cdot$ häufig nicht explizit. Statt von einer Gruppe $(G, \cdot)$, bzw. $(G, +)$, spricht man also nur von einer Gruppe G.

Definition 1.3. *Es sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt* Untergruppe *falls die folgenden Bedingungen erfüllt sind:*

i) $e \in H$ für das neutrale Element $e \in G$.

ii) Für alle $h_1, h_2 \in H$ ist auch $h_1 h_2 \in H$.

iii) Für alle $h \in H$ ist auch $h^{-1} \in H$.

Bemerkung 1.4. Es sei G eine Gruppe.

1. Statt zu fordern, dass $e \in H$, genügt es zu fordern, dass $H \neq 0$, dass es also irgendein $h \in G$ gibt mit $h \in H$. Dann ist nämlich auch $h^{-1} \in H$ und deshalb auch $e = h \cdot h^{-1} \in H$.

2. Ist $H \subseteq G$ eine Untergruppe, so ist auch $(H, \cdot)$ eine Gruppe. Das neutrale Element in H stimmt mit dem neutralen Element in G überein und für jedes $h \in H$ entspricht das inverse Element in H dem inversen Element in G.

3. Ist G abelsch, so ist auch H abelsch.

4. Ist $H \subseteq G$ eine Untergruppe und $K \subseteq H$ eine Untergruppe (der Gruppe $(H, \cdot)$), so ist auch $K \subseteq G$ eine Untergruppe.

5. Eine Teilmenge $H \subseteq G$ ist genau dann eine Untergruppe, wenn $H \neq \emptyset$ (bzw. äquivalent $e \in H$) und $h_1 h_2^{-1} \in H$ für alle $h_1, h_2 \in H$.

Definition 1.5. *Es seien G und H zwei Gruppen. Eine Abbildung $\varphi\colon G \to H$ heißt* Gruppenhomomorphismus*, falls*

$$\varphi(xy) = \varphi(x)\varphi(y) \quad \textit{für alle } x, y \in G.$$

Ist φ injektiv, so heißt φ Gruppenmonomorphismus*; ist φ surjektiv, so heißt φ* Gruppenepimorphismus*; und ist φ bijektiv, so heißt φ* Gruppenisomorphismus*. Ist $G = H$, so heißt φ* Gruppenendomorphismus*; ist φ zusätzlich bijektiv, so heißt φ Gruppenautomorphismus.*

	allgemein	$G = H$
allgemein	homo	endo
injektiv	mono	
surjektiv	epi	
bijektiv	iso	auto

Bemerkung 1.6. 1. Für jede Gruppe G ist $\mathrm{id}_G\colon G \to G$ ein ein Gruppenautomorphismus.

2. Sind G_1, G_2 und G_3 Gruppen und $\varphi\colon G_1 \to G_2$ und $\psi\colon G_2 \to G_3$ Gruppenhomomorphismen, so ist auch die Verknüpfung $\psi \circ \varphi$ ein Gruppenhomomorphismus, denn für alle $x, y \in G_1$ ist

$$\begin{aligned}(\psi \circ \varphi)(x\dot{y}) = \psi(\varphi(x \cdot y)) &= \psi(\varphi(x) \cdot \varphi(y)) \\ &= \psi(\varphi(x)) \cdot \psi(\varphi(y)) = (\psi \circ \varphi)(x) \cdot (\psi \circ \varphi)(y).\end{aligned}$$

3. Sind G und H Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus, so ist $\varphi(1) = 1$, denn
$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$$
und durch Multiplikation mit $\varphi(1)$ ergibt sich, dass $1 = \varphi(1)$.

4. Sind G und H Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus, so ist $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$, da
$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(1) = 1$$
und $\varphi(g^{-1})$ somit das inverse Element zu $\varphi(g)$ ist.

5. Sind G und H Gruppen und ist $\varphi\colon G \to H$ ein Gruppenhomomorphismus, so ist allgemeiner $\varphi(g^n) = \varphi(g)^n$ für alle $n \in \mathbb{Z}$. Für $n \geq 0$ ist nämlich
$$\varphi(g^n) = \varphi(g \cdots g) = \varphi(g) \cdots \varphi(g) = \varphi(g)^n,$$
und für $n \leq 0$ ist deshalb ebenfalls
$$\varphi(g^n) = \varphi\left(\left(g^{-1}\right)^{-n}\right) = \varphi\left(g^{-1}\right)^{-n} = \left(\varphi(g)^{-1}\right)^{-n} = \varphi(g)^n.$$

6. Sind G und H abelsche Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus, so schreibt sich die vorherigen Beobachtung also $\varphi(n \cdot g) = n \cdot \varphi(g)$ für alle $n \in \mathbb{Z}$ und $g \in G$.

7. Sind G und H Gruppen und ist $\varphi\colon G \to H$ ein Gruppenisomorphismus (also ein Gruppenhomomorphismus und bijektiv), so ist auch $\varphi^{-1}\colon H \to G$ ein Gruppenisomorphismus, da für alle $x, y \in H$

$$\begin{aligned}\varphi^{-1}(x \cdot y) &= \varphi^{-1}(\varphi(\varphi^{-1}(x)) \cdot \varphi(\varphi^{-1}(y))) \\ &= \varphi^{-1}(\varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y))) = \varphi^{-1}(x) \cdot \varphi^{-1}(y).\end{aligned}$$

8. Sind G_1 und G_2 zwei Gruppen, $\varphi\colon G_1 \to G_2$ ein Gruppenhomomorphismus und $H \subseteq G_1$ eine Untergruppe, so ist auch die Einschränkung

$$\varphi|_H\colon H \to G_2, h \mapsto \varphi(h)$$

ein Gruppenhomomorphismus, denn ist $\varphi(xy) = \varphi(x)\varphi(y)$ für alle $x, y \in G_1$, so gilt dies insbesondere für alle $x, y \in H$.

Definition 1.7. *Zwei Gruppen G und H heißen* isomorph, *falls es einen Gruppenisomorphismus $\varphi\colon G \to H$ gibt. (Dann ist auch $\varphi^{-1}\colon H \to G$ ein Gruppenisomorphismus). Man schreibt dann $G \cong H$.*

Bemerkung 1.8. Isomorphie von Gruppen lässt sich als Äquivalenzrelation sehen: Ist G eine Gruppe, so ist $G \cong G$, da die Identität $\mathrm{id}_G\colon G \to G$ ein Gruppenisomorphismus ist. Das zeigt die Reflexivität von $\cong$.

Sind G und H Gruppen mit $G \cong H$, d.h. gibt es einen Isomorphismus $\varphi\colon G \to H$, so ist auch $\varphi^{-1}\colon H \to G$ ein Gruppenisomorphismus, also $H \cong G$. Das zeigt, dass $\cong$ symmetrisch ist.

Sind G, H und K Gruppen mit $G \cong H$ und $H \cong K$, d.h. gibt es Gruppenisomorphismen $\varphi\colon G \to H$ und $\psi\colon H \to K$, so ist auch die Verknüpfung $\psi\colon \varphi$ bijektiv und ein Gruppenhomomorphismus, also ein Gruppenisomorphismus. Also ist dann $G \cong K$, was die Transitivität von $\cong$ zeigt.

1.2. Körper

Definition 1.9. *Ein Körper ist ein Tupel $(K, +, \cdot)$ bestehend aus einer Menge K und zwei binären Verknüpfungen, einer* Addition $+\colon K \times K \to K, (x, y) \mapsto x + y$ *und einer* Multiplikation $\cdot\colon K \to K, (x, y) \mapsto x \cdot y$*, so dass die folgenden Bedingungen erfüllt sind:*

i) $(K, +)$ *ist eine abelsche Gruppe.*

ii) Die Multiplikation $\cdot$ erfüllt die folgenden Bedingungen:

a) $\cdot$ ist assoziativ.

b) $\cdot$ ist kommutativ.

c) Es gibt ein Einselement $1 \in K$*, d.h.* $1 \cdot x = x$ *für alle* $x \in K$*, und es gilt* $1 \neq 0$*.*

d) Für jedes Element $x \in K$ *mit* $x \neq 0$ *gibt es ein multiplikativ inverses Element* $y \in K$*, d.h.* $x \cdot y = 1$*.*

iii) Es gilt die Distributivität von $+$ *und* $\cdot$*, d.h. für alle* $x, y, z \in K$ *ist*

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

Bemerkung 1.10. 1. Die zweite Bedingung in der Definition lässt sich dadurch ersetzen, dass $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist. Dann muss bei der Distributivität allerdings zusätzlich gefordert werden, dass auch $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ für alle $x, y, z \in K$.

2. Die hier angegebene Definition hat den Vorteil, dass sie kürzer zu überprüfen ist.

3. In der hier angegebenen Definition fordert man, dass $1 \neq 0$, da die Menge $\{0\}$ zusammen mit der Addition $0 + 0 = 0$ und $0 \cdot 0 = 0$ sonst einen Körper bilden würde (was man nicht möchte).

Bemerkung 1.11. 1. Man bezeichnet einen Körper meistens nur mit K statt mit $(K, +, \cdot)$, d.h. man nennt die Addition und Multiplikation nicht explizit. Das neutrale Element bezüglich der Addition wird mit 0 bezeichnet, das neutrale Element der Multiplikation mit 1.

2. Man rechnet „Punkt vor Strich“, d.h. für alle $x, y, z \in K$ ist

$$x + y \cdot z \coloneqq x + (y \cdot z).$$

3. In einem Körper K gelten die gewöhnlichen Rechenregeln, beispielsweise die folgenden:

   a) Für alle $x \in K$ ist $0 \cdot x = 0$, denn

   $$0 \cdot x = (0 + 0) \cdot x = (0 \cdot x) + (0 \cdot x),$$

   woraus sich die Gleichung durch Addition mit $-(0 \cdot x)$ ergibt. Da $1 \neq 0$ ist 0 insbesondere nicht multiplikativ invertierbar.

   b) Für alle $x \in K$ ist $-x = (-1) \cdot x$, da

   $$x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0 \cdot x = 0.$$

   c) Für alle $x, y \neq 0$ ist auch $x \cdot y \neq 0$ mit $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$. Es ist nämlich

   $$(x \cdot y) \cdot (x^{-1} \cdot y^{-1}) = x \cdot x^{-1} \cdot y \cdot y^{-1} = 1 \cdot 1 = 1,$$

   und 0 ist nicht multiplikativ invertierbar.

   d) Für alle $x \neq 0$ ist $(-x)^{-1} = -(x^{-1})$. Da $(-1) \cdot (-1) = -(-1) = 1$ ist nämlich $-1 = (-1)^{-1}$ und somit

   $$\begin{aligned} x^{-1} + (-x)^{-1}) &= x^{-1} + ((-1) \cdot x)^{-1} = x^{-1} + (-1)^{-1} \cdot x^{-1} \\ &= x^{-1} + (-1) \cdot x^{-1} = x^{-1} - x^{-1} = 0. \end{aligned}$$

4. Man bezeichnet die Gruppe $(K, +)$ als die *additive Gruppe* von K. Man schreibt abkürzend $K^\times := K \setminus \{0\}$; aus den obigen Rechenregeln folgt, dass $K^\times$ zusammen mit der Multiplikation des Körpers eine Gruppe bildet. Diese Gruppe $(K^\times, \cdot)$ wird als die *multiplikative Gruppe* von K bezeichnet.

5. In der Definition eines Körpers lässt sich der Begriff einer Gruppe umgehen, indem man die darin versteckten Bedingungen alle explizit angibt: Ein Körper ist dann definiert als ein Tupel $(K, +, \cdot)$ bestehend aus einer Menge K und zwei binären Verknüpfungen $+$ und $\cdot$ auf K, so dass die folgenden Bedingungen erfüllt sind:
   i) $+$ ist assoziativ, d.h. $x + (y + z) = (x + y) + z$ für alle $x, y, z \in K$.
   ii) $+$ ist kommutativ, d.h. $x + y = y + x$ für alle $x, y \in K$.
   iii) Es gibt ein additiv neutrales Element $0 \in K$, d.h. $x + 0 = x$ für alle $x \in K$.
   iv) Es gibt für jedes $x \in K$ ein additiv inverses Element $y \in K$, d.h. $x + y = 0$.
   v) $\cdot$ ist assoziativ, d.h. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ für alle $x, y, z \in K$.
   vi) $\cdot$ ist kommutativ, d.h. für alle $x, y \in K$ ist $x \cdot y = y \cdot x$.
   vii) Es gibt ein multiplikatives neutrales Element $1 \in K \setminus \{0\}$, d.h. $x \cdot 1 = x$ für alle $x \in K$, und $1 \neq 0$.
   viii) Für jedes $x \in K \setminus \{0\}$ gibt es ein multiplikativ inverses Element $y \in K$, d.h. $x \cdot y = 1$.
   ix) $+$ ist distributiv bezüglich $\cdot$, d.h. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ für alle $x, y, z \in K$.

Definition 1.12. *Es sei L ein Körper. Eine Teilmenge $K \subseteq L$ heißt* Unterkörper, *falls die folgenden Bedingungen erfüllt sind:*

i) K ist eine Untergruppe der additiven Gruppe von L (es ist also $0 \in K$, für alle $x, y \in K$ ist auch $x + y \in K$, und für alle $x \in K$ ist auch $-x \in K$).

ii) Es ist $1 \in K$, für alle $x, y \in K$ ist $x \cdot y \in K$, und für jedes $x \in K$ mit $x \neq 0$ ist auch $x^{-1} \in K$.

Bemerkung 1.13. 1. Ist L ein Körper und $K \subseteq L$ ein Unterkörper, so ist $(K, +, \cdot)$ ebenfalls ein Körper. Es gilt $0_K = 0_L$ und $1_K = 1_L$ und für jedes $x \in K^\times$ stimmen die inversen Element in K und L überein.

2. Ist L ein Körper und $K \subseteq L$ ein Unterkörper, so ist $K \subseteq L$ eine additive Untergruppe und $K^\times \subseteq L^\times$ eine multiplikative Untergruppe.

3. Ist L ein Körper, $K \subseteq L$ ein Unterkörper und $K' \subseteq K$ ein Unterkörper (von K), so ist $K' \subseteq L$ ein Unterkörper.

Definition 1.14. *Es seien K und L zwei Körper. Eine Abbildung $\phi\colon K \to L$ heißt* Körperhomomorphismus, *falls*

i) $\phi(x + y) = \phi(x) + \phi(y)$ für alle $x, y \in K$

ii) $\phi(xy) = \phi(x)\phi(y)$ für alle $x, y \in K$, und

iii) $\phi(1) = 1$.

Ist ϕ bijektiv, so ist ϕ ein Körperisomorphismus. *Ist $K = L$ und ϕ bijektiv, so ist ϕ ein* Körperautomorphismus.

Bemerkung 1.15. 1. Für jeden Körper K ist die Identität $\mathrm{id}_K \colon K \to K$ ein Körperautomorphismus.

2. Sind K_1, K_2 und K_3 Körper und $\phi \colon K_1 \to K_2$ und $\psi \colon K_2 \to K_3$ Körperhomomorphismen, so ist auch $\psi \circ \phi \colon K_1 \to K_3$ ein Körperhomomorphismus: Für alle $x, y \in K_1$ ist

$$\begin{aligned}(\psi \circ \phi)(x + y) = \psi(\phi(x + y)) &= \psi(\phi(x) + \phi(y)) \\ &= \psi(\phi(x)) + \psi(\phi(y)) = (\psi \circ \phi)(x) + (\psi \circ \phi)(y)\end{aligned}$$

und

$$\begin{aligned}(\psi \circ \phi)(x \cdot y) = \psi(\phi(x \cdot y)) &= \psi(\phi(x) \cdot \phi(y)) \\ &= \psi(\phi(x)) \cdot \psi(\phi(y)) = (\psi \circ \phi)(x) \cdot (\psi \circ \phi)(y),\end{aligned}$$

und es gilt

$$(\psi \circ \phi)(1) = \psi(\phi(1)) = \psi(1) = 1.$$

3. Sind K und L Körper und ist $\phi \colon K \to L$ ein Körperhomomorphismus, so ist ϕ insbesondere ein Gruppenhomomorphismus zwischen den unterliegenden abelschen Gruppen $(K, +)$ und $(L, +)$. Daher ist insbesondere

$$\phi(n \cdot x) = n \cdot \phi(x) \quad \text{für alle } n \in \mathbb{Z} \text{ und } x \in K.$$

4. Sind K und L Körper und ist $\phi \colon K \to L$ ein Körperisomorphismus, so ist auch die Umkehrabbildung $\phi^{-1} \colon L \to K$ ein Körperisomorphismus: ϕ ist bijektiv und für alle $x, y \in L$ ist

$$\begin{aligned}\phi^{-1}(x + y) &= \phi^{-1}(\phi(\phi^{-1}(x)) + \phi(\phi^{-1}(y))) \\ &= \phi^{-1}(\phi(\phi^{-1}(x) + \phi^{-1}(y)) = \phi^{-1}(x) + \phi^{-1}(y)\end{aligned}$$

und

$$\begin{aligned}\phi^{-1}(x \cdot y) &= \phi^{-1}(\phi(\phi^{-1}(x)) \cdot \phi(\phi^{-1}(y))) \\ &= \phi^{-1}(\phi(\phi^{-1}(x) \cdot \phi^{-1}(y))) = \phi^{-1}(x) \cdot \phi^{-1}(y),\end{aligned}$$

sowie auch

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

5. Sind K und L Körper und ist $\phi \colon K \to L$ ein Körperhomomorphismus, so ist ϕ ein Gruppenhomomorphismus von $(K, +)$ nach $(L, +)$, da $\phi(x + y) = \phi(x) + \phi(y)$ für alle $x, y \in K$.

   Insbesondere ist daher $\phi(0) = 0$ und $\phi(-x) = -\phi(x)$ für alle $x \in K$.

6. Sind K und L Körper und ist $\phi\colon K \to L$ ein Körperhomomorphismus, so ist $\phi(x) \neq 0$ für alle $x \in K \setminus \{0\}$ sowie $\phi(x^{-1}) = \phi(x)^{-1}$ für alle $x \in K \setminus \{0\}$: Da

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

ist $\phi(x)$ invertierbar, also $\phi(x) \neq 0$, und $\phi(x^{-1})$ das Inverse von $\phi(x)$, also $\phi(x^{-1}) = \phi(x)^{-1}$.

Da $\phi(x) \neq 0$ für alle $x \neq 0$ ist $\phi(K^\times) \subseteq L^\times$. Da außerdem $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ für alle $x, y \in K$, und somit insbesondere für alle $x, y \in K^\times$, induziert ϕ durch Einschränkung einen Gruppenhomomorphismus $\phi|_{K^\times}\colon K^\times \to L^\times, x \mapsto \phi(x)$.

7. Körperhomomorphismen sind injektiv, d.h. sind K und L Körper und ist $\phi\colon K \to L$ ein Körperhomomorphismus, so ist ϕ injektiv: Sind $x, y \in K$ mit $x \neq y$, so ist $x - y \neq 0$ und somit $\phi(x - y) \neq 0$. Da $\phi(x) - \phi(y) = \phi(x - y) \neq 0$ ist $\phi(x) \neq \phi(y)$.

   Da Körperhomomorphismen stets injektiv sind, spricht man nicht von Körperepimorphismen oder Körpermonomorphismen: Jeder Körperhomomorphismus wäre ein Körpermonomorphismus und jeder Körperepimorphismus wäre bereits ein Körperisomorphismus.

Definition 1.16. *Zwei Körper K und L sind* isomorph*, falls es einen Körperisomorphismus $\phi\colon K \to L$ gibt. (Dann ist auch $\phi^{-1}\colon L \to K$ ein Körperisomorphismus.) Man schreibt dann $K \cong L$.*

Bemerkung 1.17. Komplett analog zu Bemerkung 1.8 lässt sich auch die Isomorphie von Körpern als Äquivalenzrelation verstehen.

1.3. Vektorräume

Definition 1.18. *Ein K-Vektorraum ist ein Tripel $(K, V, \cdot)$ bestehend aus einem Körper K, einer abelschen Gruppe V und einer Verknüpfung $\cdot K \times V \to V$, $(\lambda, v) \mapsto \lambda \cdot v$, die die folgenden Bedingungen erfüllt:*

i) $\lambda \cdot (v + w) = (\lambda \cdot v) + (\lambda \cdot w)$ *für alle* $\lambda \in K$ *und* $v, w \in V$.

ii) $(\lambda + \mu) \cdot v = (\lambda \cdot v) + (\mu \cdot v)$ *für alle* $\lambda, \mu \in K$ *und* $v \in V$.

iii) $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$ *für alle* $\lambda, \mu \in K$ *und* $v \in V$.

iv) $1 \cdot v = v$ *für alle* $v \in V$.

Die Elemente $v \in V$ nennt man Vektoren *und die Elemente $\lambda \in K$ nennt man* Skalare*. Die Verknüpfung $\cdot$ heißt* Skalarmultiplikation*.*

Bemerkung 1.19. 1. Man schreibt die Skalarmultiplikation auch also λv statt $\lambda \cdot v$.

2. Man rechnet „Punkt vor Strich“, d.h. es ist

$$\lambda \cdot v + w \coloneqq (\lambda \cdot v) + w \quad \text{für alle } \lambda \in K \text{ und } v, w \in V.$$

3. Es ist wichtig, zu verstehen, dass man zwar Elemente des Körpers miteinander multiplizieren kann und auch Elemente aus dem Körper mit Elementen aus dem Vektorraum, dass man aber nicht Elemente aus dem Vektorraum miteinander multiplizieren kann. Produkte der Form $v \cdot w$ mit $v, w \in V$ ergeben für einen K-Vektorraum V im Allgemeinen also keinen Sinn.

4. Aus den gegebenen Axiomen eines K-Vektorraums V folgen noch weiter Rechenregeln, wie etwa die folgenden:
   a) $0 \cdot v = 0$ für alle $v \in V$ (die 0 auf der linken Seite ist die des Körpers, die 0 auf der rechten Seite die des Vektorraums). Es ist nämlich
   $$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v,$$
   woraus sich die Aussage durch Subtraktion von $0 \cdot x$ von beiden Seiten der Gleichungskette ergibt.
   b) Für alle $\lambda \in K$ ist $\lambda \cdot 0 = 0$. Es ist nämlich
   $$\lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 + \lambda \cdot 0,$$
   woraus sich die Aussage durch Subtraktion von $\lambda \cdot 0$ von beiden Seiten der Gleichungkette ergibt.
   c) Sind andererseits $\lambda \in K$ und $v \in V$ mit $\lambda \neq 0$ und $v \neq 0$, so ist auch $\lambda \cdot v \neq 0$. Andernfalls wäre nämlich
   $$v = 1 \cdot v = \lambda^{-1} \cdot \lambda \cdot v == \lambda^{-1} \cdot 0 = 0.$$
   d) $(-1) \cdot v = -v$ für alle $v \in V$. Da nämlich
   $$v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = 0$$
   ist $(-1) \cdot v$ das additiv Inverse zu v.
   e) Allgemeiner gilt $(-\lambda) \cdot v = -(\lambda \cdot v)$ für alle $\lambda \in K$ und $v \in V$. Der Beweis verläuft analog zum Fall $\lambda = 1$: Es ist
   $$\lambda \cdot v + (-\lambda) \cdot v = (\lambda + (-\lambda)) \cdot v = 0 \cdot v = 0,$$
   also ist $(-\lambda) \cdot v$ das additiv Inverse zu $\lambda \cdot v$.

Definition 1.20. *Eine Teilmenge $U \subseteq V$ eines K-Vektorraums V heißt* Untervektorraum *falls*

i) $0 \in U$,

ii) für alle $u, v \in U$ ist auch $u + v \in V$,

iii) für alle $u \in U$ und $\lambda \in K$ ist auch $\lambda \cdot v \in U$.

Bemerkung 1.21. 1. Ist $U \subseteq V$ ein Untervektorraum, so ist U insbesondere eine abelsche Untergruppe, denn für alle $u \in U$ ist auch $-u = (-1) \cdot u \in U$, und dass $0 \in U$ und U unter der Addition abgeschlossen ist, ist gegeben.

2. Für einen K-Vektorraum V und Untervektorraum $U \subseteq V$ ist $(U, K, \cdot)$ ebenfalls ein K-Vektorraum. Da U eine additive Untergruppe von V ist, stimmt das Nullelement in U mit dem in V überein, und für jedes $u \in U$ stimmt das additiv Inverse Element in U mit dem in V überein.

3. Ist W ein K-Vektorraum, $V \subseteq W$ ein Untervektorraum und $U \subseteq V$ ein Untervektorraum (also U ein Untervektorraum von V), so ist auch $U \subseteq W$ ein Untervektorraum.

Definition 1.22. *Sind V und W zwei K-Vektorräume, so ist eine Abbildung $f\colon V \to W$ ein* Vektorraumhomomorphismus*, bzw.* linear*, falls*

i) $f(v_1 + v_2) = f(v_1) + f(v_2)$ *für alle* $v_1, v_2 \in V$ *und*

ii) $f(\lambda v) = \lambda f(v)$ *für alle* $\lambda \in K$ *und* $v \in V$.

Ist f injektiv, so ist f ein Vektorraummonomorphismus*. Ist f surjektiv, so eist f ein* Vektorraumepimorphismus*. Ist f bijektiv, so ist f ein* Vektorraumisomorphismus*. Ist $V = W$, so ist f ein* Vektorraumendomorphismus*. Ist $V = W$ und f bijektiv, so ist f ein* Vektorraumautomorphismus*.*

Bemerkung 1.23. 1. Man spricht auch abkürzend nur von Homomorphismen, Monomorphismen, Epimorphismen, Isomorphismen, Endomorphismen und Automorphismen.

2. Für jeden Vektorraum V ist die Identität $\mathrm{id}_V : V \to V$ ein Automorphismus.

3. Sind V_1, V_2 und V_3 K-Vektorräume und $f\colon V_1 \to V_2$ und $g\colon V_2 \to V_3$ linear, so ist auch $g \circ f\colon V_1 \to V_3$ linear, da für alle $x, y \in V_1$

$$\begin{aligned}(g \circ f)(x + y) = g(f(x + y)) &= g(f(x) + g(y)) \\ &= g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y),\end{aligned}$$

und für alle $\lambda \in K$ und $v \in V$

$$(g \circ f)(\lambda v) = g(f(\lambda v)) = g(\lambda f(v)) = \lambda g(f(v)) = \lambda (g \circ f)(v).$$

4. Sind V und W K-Vektorräume und ist $f\colon V \to W$ linear, so ist f inbesondere ein Gruppenhomomorphismus zwischen den unterliegenden abelschen Gruppen $(V, +)$ und $(W, +)$. Deshalb ist insbesondere

$$f(n \cdot v) = n \cdot f(v) \quad \text{für alle } n \in \mathbb{Z} \text{ und } v \in V.$$

5. Sind V und W K-Vektorräume und ist $f\colon V \to W$ ein Isomorphismus, so ist auch $f^{-1}\colon W \to V$ ein Isomorphismus: f^{-1} ist bijektiv, für alle $x, y \in W$ ist

$$\begin{aligned}f^{-1}(x + y) &= f^{-1}(f(f^{-1}(x)) + f(f^{-1}(y))) \\ &= f^{-1}(f(f^{-1}(x) + f^{-1}(y)) = f^{-1}(x) + f^{-1}(y)\end{aligned}$$

und für alle $\lambda \in K$ und $x \in W$ ist

$$f^{-1}(\lambda x) = f^{-1}(\lambda f(f^{-1}(x))) = f^{-1}(f(\lambda f^{-1}(x))) = \lambda f^{-1}(x).$$

Definition 1.24. *Zwei K-Vektorräume V und W heißen* isomorph, *falls es einen Isomorphismus $f\colon V \to W$ gibt. (Dann ist auch $f^{-1}\colon W \to V$ ein Isomorphismus.) Man schreibt dann $V \cong W$.*

Bemerkung 1.25. Analog zu Bemerkung 1.8 lässt sich auch die Isomorphie von K-Vektorräumen als Äquivalenzrelation auffassen.

1.4. Mengentheoretische Grundbegriffe und Notationen

1.4.1. Allgemeine Notationen und Begriffe

Definition 1.26. *Es sei I eine Indexmenge und für jedes $i \in I$ sei A_i eine Menge. Dann ist die* Vereinigung $\bigcup_{i\in I} A_i$ *definiert als*

$$\bigcup_{i\in I} A_i = \{x \mid \text{es gibt ein } i \in I \text{ mit } x \in A_i\}.$$

Der Schnitt $\bigcap_{i\in I} A_i$ *ist definiert als*

$$\bigcap_{i\in I} A_i = \{x \mid \text{für alle } i \in I \text{ ist } x \in A_i\}.$$

Für Mengen $A_1, \dots, A_n$ ist

$$A_1 \cup \cdots \cup A_n \coloneqq \bigcup_{i\in\{1,\cdots,n\}} A_i. \quad \text{und} \quad A_1 \cap \cdots \cap A_n \coloneqq \bigcap_{i\in\{1,\cdots,n\}} A_i.$$

Definition 1.27. *Für Mengen A und B ist die Differenz $A \setminus B$ als*

$$A \setminus B\{a \in A \mid a \notin B\}$$

definiert. Die symmetrische Differenz $A \triangle B$ ist als

$$A \triangle B = (A \cup B) \setminus (A \cap B)$$

definiert.

Definition 1.28. *Ist A eine fixierte (!) Menge und $S \subseteq A$ eine Teilmenge, so ist das* Komplement *S^C als*

$$S^C \coloneqq A \setminus S = \{a \in A \mid a \notin S\}$$

definiert.

Bemerkung 1.29. 1. Die Notation des Komplementes ergibt nur für Teilmengen $S \subseteq A$ einer fest fixierten Grundmenge A Sinn, und hängt A ab!

2. Ist $S \subseteq A$ eine Teilmenge, so ist $(S^C)^C = S$ und $S \cap S^C = \emptyset$. (S^C ist die größte Teilmenge von A, die S trivial schneidet, d.h. ist $T \subseteq A$ eine Teilmenge mit $T \cap S = \emptyset$, so ist $T \subseteq S^C$.)

3. Sind $S, T \subseteq A$ Teilmengen, so ist

$$S \setminus T = \{s \in S \mid s \notin T\} = \{s \in S \mid s \in T^C\} = S \cap T^C.$$

Bemerkung 1.30. Ist A eine Menge und A_i, $i \in I$ eine Kollektion von Teilmengen $A_i \subseteq A$, so gelten die *De Morgansche Regeln*

$$\left(\bigcup_{i\in I} A_i\right)^C = \bigcap_{i\in I} A_i^C \quad \text{und} \quad \left(\bigcap_{i\in I} A_i\right)^C = \bigcup_{i\in I} A_i^C.$$

Für jedes $a \in A$ gilt nämlich

$$a \in \left(\bigcup_{i\in I} A_i\right)^C \iff a \notin \bigcup_{i\in I} A_i \iff \text{es gibt kein } i \in I \text{ mit } a \in A_i$$
$$\iff \text{für jedes } i \in I \text{ ist } a \notin A_i \iff \text{für jedes } i \in I \text{ ist } a \in A_i^C \iff a \in \bigcap_{i\in I} A_i^C,$$

was die erste Regel zeigt. Die zweite Regel ergibt sich aus der ersten, da

$$\left(\bigcap_{i\in I} A_i\right)^C = \left(\bigcap_{i\in I} (A_i^C)^C\right)^C = \left(\left(\bigcup_{i\in I} A_i^C\right)^C\right)^C = \bigcup_{i\in I} A_i^C.$$

Bemerkung 1.31. Sind A_i, $i \in I$ und B_i, $i \in I$ zwei Kollektionen von Mengen, so ist

$$\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in I} B_j\right) = \bigcup_{i,j\in I} (A_i \cap B_j),$$

denn es ist

$$x \in \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in I} B_j\right) \iff x \bigcup_{i\in I} A_i \text{ und } \bigcup_{j\in I} B_j$$
$$\iff \text{es gibt } i, j \in I \text{ mit } x \in A_i \text{ und } x \in B_j \iff \text{es gibt } i, j \in I \text{ mit } x \in A_i \cap B_j$$
$$\iff x \in \bigcup_{i,j\in I} (A_i \cap B_j).$$

Es ist daher auch

$$\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in I} B_j\right) = \bigcap_{i,j\in I} (A_i \cup B_j),$$

denn es ist

$$\left(\bigcup_{i\in I} A_i^C\right) \cap \left(\bigcup_{j\in I} B_j^C\right) = \bigcup_{i,j\in I} (A_i^C \cap B_j^C),$$

wodurch sich durch Anwendung des Komplements auf beiden Seiten und den De Morganschen Regeln die behauptete Gleichung ergibt.

1.4.2. Produkte und Potenzen

Für Mengen $A_1, \dots, A_n$ wird das Produkt $A_1 \times \cdots \times A_n$ für gewöhnlich als

$$A_1 \times \cdots \times A_n = \{(a_1, \dots a_n) \mid a_1 \in A_1, \dots a_n, \in A_n\}$$

definiert, wobei $(a_1, \cdots, a_n)$ ein geordnetes Tupel ist. Für eine Menge A und $n \in \mathbb{N}$, $n \geq 1$ wird die Potenz A^n dann als

$$A^n \coloneqq \underbrace{A \times \cdots \times A}_{n \text{ viele}} = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in A\}$$

definiert. Wir geben hier eine formale Konstruktion von beliebig großen (bzw. mengengroßen) Produkten und Potenzen an.

Definition 1.32. *Es sei I ein Indexmenge und für jedes $i \in I$ sei A_i eine Menge. Dann ist das* Produkt $\prod_{i \in I} A_i$ *definiert als*

$$\prod_{i \in I} A_i = \left\{ f \colon I \to \bigcup_{i \in I} A_i \;\middle|\; f(i) \in A_i \text{ für alle } i \in I \right\}$$

und ein Element $f \in \prod_{i \in I} A_i$ wird als Tupel $(f(i))_{i \in I}$ *geschrieben. Für eine Menge A und Indexmenge I ist die* Potenz A^I *definiert als*

$$A^I \coloneqq \prod_{i \in I} A = \{f \colon I \to A\}.$$

Bemerkung 1.33. 1. Mithilfe der Tupelschreibweise ist

$$\prod_{i \in I} A_i = \{(f(i))_{i \in I} \mid f(i) \in A_i \text{ für alle } i \in I\}$$

sowie

$$A^I = \{(f(i))_{i \in I} \mid f(i) \in A \text{ für alle } i \in I\}.$$

Schreibt man zusätzlich f_i statt $f(i)$ (wie man es etwa von Folgen gewöhnt ist), so ist

$$\prod_{i \in I} A_i = \{(f_i)_{i \in I} \mid f_i \in A_i \text{ für alle } i \in I\}$$

und

$$A^I = \{(f_i)_{i \in I} \mid f_i \in A \text{ für alle } i \in I\}.$$

2. Schreiben wir im Folgenden $\prod_{i \in I} A_i$ oder A^I, so verstehen wir dies in erster Linie. Die obige Definition von Tupeln als Funktionen dient für uns nur als mengentheoretische Implementation des Ganzen.

   Möchten wir tatsächlich die Menge der Funktionen zwischen zwei Mengen X und Y betrachten, so schreiben wir hierfür im Folgenden

$$\mathrm{Abb}(X, Y) \coloneqq \{f \colon X \to Y\}.$$

Sofern es uns nützlich erscheint, werden wir Gleichheit $\mathrm{Abb}(I, X)$ und X^I aber nutzen, um uns doppelte Rechnungen zu ersparen. So werden wir Beispiele angeben, die über Produkte zustande kommen (etwa Produkte von Gruppen und Produkte von Vektorräumen), und aus diese ohne weiteren Rechenaufwand auch Beispiele von Abbildungsräumen (Abbildungen in eine Gruppe und Abbildungen in einen Vektorraum) erhalten.

1.5. Folgen und Matrizen

Definition 1.34. *Es sei X eine Menge. Eine* Folge *auf X ist eine Funktion $a\colon \mathbb{N} \to X$. Die Folge a wird als Tupel $a = (a_n)_{n\in\mathbb{N}}$ geschrieben, wobei $a_n = a(n)$ für alle $n \in \mathbb{N}$. Die Element a_n mit $n \in \mathbb{N}$ werden* Einträge *von $(a_n)_{n\in\mathbb{N}} \in K$ genannt. Es sei*

$$\begin{aligned}\ell(X) &\coloneqq \mathrm{Abb}(\mathbb{N}, X) = \{a\colon \mathbb{N} \to X\}\\ &= \{(a_n)_{n\in\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ ist eine Folge auf } X\}\\ &= \{(a_n)_{n\in\mathbb{N}} \mid a_n \in X \text{ für alle } n \in \mathbb{N}\}.\end{aligned}$$

Definition 1.35. *Es seien $m, n \in \mathbb{N}$ und X ein Menge. Eine $(m \times n)$-*Matrix *mit* Einträgen *in X ist eine Abbildung $A\colon \{1,\dots,m\} \times \{1,\dots,n\} \to X$. Die Matrix A wird als Tupel*

$$(A_{ij})_{(i,j)\in\{1,\dots,m\}\times\{1,\dots,n\}} = (A_{ij})_{\substack{i=1,\dots,m\\ j=1,\dots,n}}$$

geschrieben, wobei $A_{ij} = A((i,j)) \in X$ für alle $(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}$ also alle $1 \le i \le m$ und $1 \le j \le n$. A wird auch als ein rechteckiges Schema

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1n}\\ \vdots & \ddots & \vdots\\ A_{m1} & \cdots & A_{mn}\end{pmatrix}$$

geschrieben. Die Menge der $(m \times n)$-Matrizen mit Einträgen in X wird mit

$$\mathrm{Mat}(m \times n, X) = \left\{ \begin{pmatrix} A_{11} & \cdots & A_{1n}\\ \vdots & \ddots & \vdots\\ A_{m1} & \cdots & A_{mn}\end{pmatrix} \,\middle|\, A_{ij} \in X \text{ für alle } 1 \le i \le m \text{ und } 1 \le j \le n \right\}$$

bezeichnet.

Definition 1.36. *Es sei K ein Körper. Es seien $l, m, n \in \mathbb{N}$, sowie $A \in \mathrm{Mat}(l \times m, K)$ und $B \in \mathrm{Mat}(m \times n, K)$. Das Produkt $A \cdot B \in \mathrm{Mat}(l \times n, K)$ ist als*

$$(A \cdot B)_{ik} = \sum_{j=1}^{m} A_{ij}B_{jk} \quad \text{für alle } 1 \le i \le l \text{ und } 1 \le k \le m$$

definiert.

Bemerkung 1.37. Das Matrixprodukt ist assoziativ, d.h. für alle $p, q, r, s \in \mathbb{N}$ und Matrizen $A \in \mathrm{Mat}(p \times q, K)$, $B \in \mathrm{Mat}(q \times r, K)$ und $C \in \mathrm{Mat}(r \times s, K)$ ist $A \cdot (B \cdot C) = (A \cdot B) \cdot C$, denn für alle $1 \leq i \leq p$ und $1 \leq l \leq s$ ist

$$\begin{aligned}(A \cdot (B \cdot C))_{il} &= \sum_{j=1}^{q} A_{ij}(B \cdot C)_{jl} = \sum_{j=1}^{q} A_{ij} \sum_{k=1}^{r} B_{jk}C_{kl} = \sum_{j=1}^{q}\sum_{k=1}^{r} A_{ij}B_{jk}C_{kl} \\ &= \sum_{k=1}^{r}\sum_{j=1}^{q} A_{ij}B_{jk}C_{kl} = \sum_{k=1}^{r}\left(\sum_{j=1}^{q} A_{ij}B_{jk}\right)C_{kl} = \sum_{k=1}^{r}(A \cdot B)_{ik}C_{kl} \\ &= ((A \cdot B) \cdot C)_{il}.\end{aligned}$$

Bemerkung 1.38. Wir werden im Folgenden auf die Definition von Folgen und Matrizen als Abbildungen $\mathbb{N} \to X$, bzw. $\{1, \ldots, m\} \times \{1, \ldots, n\} \to X$ zurückkommen, um aus Beispielen von Abbildungsräumen (Abbildungen in eine Gruppe, Abbildungen in einen Vektorraum) Aussagen über Folgen und Matrizen zu erhalten.

2. Beispiele für Gruppen

2.1. Verschiedene kleinere Beispiele

1. Ist $G = \{x\}$ eine einelementige Menge, so gibt es auf G eine eindeutige Gruppenstruktur, gegeben durch $x \cdot x = x$. Man bezeichnet diese als die *triviale Gruppe*.

2. Ist G eine Gruppe, so ist $\{1\} \subseteq G$ eine Untergruppe. Man bezeichnet diese als die *triviale Untergruppe*.

3. Die reellen Zahlen $\mathbb{R}$ bilden zusammen mit der üblichen Addition $+$ eine abelsche Gruppe: Die Assoziativität und Kommutativität der Addition sind bekannt. $0 \in \mathbb{R}$ ist das neutrale Element bezüglich der Addition, da $x + 0 = 0 + x = x$ für alle $x \in \mathbb{R}$. Für $x \in \mathbb{R}$ ist $-x \in \mathbb{R}$ das inverse Element, da $x + (-x) = (-x) + x = 0$.

4. Nach analoger Argumentation bilden die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$ und die komplexen Zahlen $\mathbb{C}$ zusammen mit der gewöhnlichen Addition $+$ jeweils eine abelsche Gruppe. Wir erhalten eine Kette von Untergruppen $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

5. Die natürlichen Zahlen $\mathbb{N}$ bilden zusammen mit der üblichen Addition keine Gruppe: Andernfalls wäre $0 \in \mathbb{N}$ das neutrale Element, da $0 + n = n + 0 = n$ für alle $n \in \mathbb{N}$. Da es aber kein $n \in \mathbb{N}$ mit $n + 1 = 0$ gibt, besäße $1 \in \mathbb{N}$ dann kein inverses Element.

6. Die Menge $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ bildet zusammen mit der üblichen Multiplikation $\cdot$ eine abelsche Gruppe: Die Assoziativität und Kommutativität der Multiplikation sind bekannt. $1 \in \mathbb{R}^\times$ ist das neutrale Element bezüglich der Multiplikation, da $1 \cdot x = x \cdot 1 = x$ für alle $x \in \mathbb{R}^\times$. Für $x \in \mathbb{R}^\times$ ist $1/x \in \mathbb{R}^\times$ das multiplikativ Inverse, da $x \cdot (1/x) = (1/x) \cdot x = 1$.

7. Analog ergibt sich, dass $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ und $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ zusammen mit der üblichen Multiplikation abelsche Gruppen bilden. Wir erhalten somit eine Kette von Untergruppen $\mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times$.

8. Die ganzen Zahlen $\mathbb{Z}$ bilden zusammen mit der üblichen Multiplikation keine Gruppe: Da $1 \cdot n = n \cdot 1 = n$ für alle $n \in \mathbb{Z}$ wäre 1 das neutrale Element bezüglich der Multiplikation. Da es aber kein $n \in \mathbb{Z}$ mit $n \cdot 2 = 1$ gibt, besäße $2 \in \mathbb{Z}$ kein multiplikativ inverses Element.

9. Ist K ein Körper, so ist K bezüglich der Addition eine abelsche Gruppe und $K^\times = K \setminus \{0\}$ zusammen mit der Multiplikation eine abelsche Gruppe.

10. Es sei $\mathbb{R}_+ \coloneqq \{x \in \mathbb{R} \mid x > 0\} \subseteq \mathbb{R}^\times$ die Menge der positiven reellen Zahlen. Es ist $1 \in \mathbb{R}_+$, für alle $x, y \in \mathbb{R}_+$ ist auch $x \cdot y \in \mathbb{R}_+$, und für jedes $x \in \mathbb{R}_+$ ist auch $1/x \in \mathbb{R}_+$. Also ist $\mathbb{R}_+ \subseteq \mathbb{R}^\times$ eine Untergruppe. Insbesondere ist also $\mathbb{R}_+$ zusammen mit der üblichen Multiplikation eine abelsche Gruppe.

11. Die Menge der negativen reellen Zahlen $\mathbb{R}_- := \{x \in \mathbb{R} \mid x < 0\}$ ist zusammen mit der üblichen Multiplikation keine Gruppe, da zwa, $-1 \in \mathbb{R}_-$, aber $(-1) \cdot (-1) = 1 \notin \mathbb{R}_-$.

12. Für $x, y \in \mathbb{R}_-$ sei $x * y := -xy$. Wir zeigen, dass $\mathbb{R}_-$ zusammen mit $*$ eine abelsche Gruppe bildet:

    Für $x, y \in \mathbb{R}_-$ ist $x, y < 0$, also $xy > 0$ und somit $-xy < 0$. Also ist die Verknüpfung $\mathbb{R}_- \times \mathbb{R}_- \to \mathbb{R}_-$, $(x, y) \mapsto x * y$ wohldefiniert.

    Für alle $x, y, z \in \mathbb{R}_-$ ist

    $$\begin{aligned}(x * y) * z &= (-xy) * z = -((-xy)z) \\ &= xyz = -(x(-yz)) = x * (-yz) = x * (y * z),\end{aligned}$$

    also ist $*$ assoziativ. Für alle $x, y \in \mathbb{R}_-$ ist

    $$x * y = -xy = -yx = y * x$$

    also ist $*$ kommutativ. Für alle $x \in \mathbb{R}_-$ ist $(-1) * x = -((-1)x) = x$, also ist -1 ein neutrales Element bezüglich $*$. Für $x \in \mathbb{R}_-$ ist $x * (1/x) = -(x \cdot (1/x)) = -1$, also ist $1/x$ bezüglich $*$ invers zu x.

    Ingesamt zeigt dies, dass $(\mathbb{R}_-, *)$ eine abelsche Gruppe ist.

13. Für alle $n \in \mathbb{N}$, $n \geq 1$ ist $\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}$ zusammen mit der *eintragsweisen Addition*

    $$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

    eine abelsche Gruppe:

    Für alle $(x_1, \ldots, x_n), (y_1, \ldots, y_n), (z_1, \ldots, z_n) \in \mathbb{R}^n$ ist

    $$\begin{aligned}&(x_1, \ldots, x_n) + ((y_1, \ldots, y_n) + (z_1, \ldots, z_n)) \\ =\,&(x_1, \ldots, x_n) + (y_1 + z_1, \ldots, y_n + z_n) \\ =\,&(x_1 + y_1 + z_1, \ldots, x_n + y_n + z_n) \\ =\,&(x_1 + y_1, \ldots, x_n + y_n) + (z_1, \ldots, z_n) \\ =\,&((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) + (z_1, \ldots, z_n),\end{aligned}$$

    also ist die Addition assoziativ.

    Für alle $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{R}^n$ ist

    $$\begin{aligned}(x_1, \ldots, y_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n) \\ &= (y_1 + x_1, \ldots, y_n + x_n) = (y_1, \ldots, y_n) + (x_1, \ldots, x_n),\end{aligned}$$

    also ist die Addition tatsächlich kommutativ.

    Für jedes $(x_1, \ldots, x_n) \in \mathbb{R}^n$ ist

    $$(0, \ldots, 0) + (x_1, \ldots, x_n) = (0 + x_1, \ldots, 0 + x_n) = (x_1, \ldots, x_n),$$

also ist $(0,\dots,0) \in \mathbb{R}^n$ neutral bezüglich der Addition.

Für jedes $(x_1,\dots,x_n) \in \mathbb{R}^n$ ist

$$(-x_1,\dots,-x_n) + (x_1,\dots,x_n) = (-x_1+x_1,\dots,-x_n+x_n) = (0,\dots,0),$$

also ist $(-x_1,\dots,-x_n)$ invers zu $(x_1,\dots,x_n)$ bezüglich der Addition.

Ingesamt zeigt dies, dass $(\mathbb{R}^n,+)$ eine abelsche Gruppe ist.

14. Analog ergibt sich, dass $\mathbb{Z}^n$, $\mathbb{Q}^n$ und $\mathbb{C}^n$ zusammen mit der eintragsweisen Addition jeweils Gruppen bilden. Es ergibt sich damit eine Kette von Untergruppen $\mathbb{Z}^n \subseteq \mathbb{Q}^n \subseteq \mathbb{R}^n \subseteq \mathbb{C}^n$.

15. Ist allgemeiner K ein Körper, so ist K^n mit der eintragsweisen Addition eine abelsche Gruppe.

16. Für zwei reelle Zahlen $a,b \in \mathbb{R}$ ist das *arithmetische* Mittel als $a \oplus b = (a+b)/2$ definiert. Die reellen Zahlen $\mathbb{R}$ bilden zusammen mit dem arithmetischen Mittel $\oplus$ *keine* Gruppe: Für alle $a,b,c \in \mathbb{R}$ ist

$$a \oplus (b \oplus c) = a \oplus \frac{b+c}{2} = \frac{a}{2} + \frac{b+c}{4} = \frac{2a+b+c}{4}$$

und

$$(a \oplus b) \oplus c = \frac{a+b}{2} \oplus c = \frac{a+b}{4} + \frac{c}{2} = \frac{a+b+2c}{4},$$

für $a = 1$, $b = 0$ and $c = 2$ ist daher $a \oplus (b \oplus c) = 1$ und $(a \oplus b) \oplus c = 5/4$, also $a \oplus (b \oplus c) \neq (a \oplus b) \oplus c$. Also ist das arithmetische Mittel nicht assoziativ.

17. Für je zwei Teilmengen $A, B \subseteq \mathbb{R}$ sei

$$A \boxplus B \coloneqq \{a+b \mid a \in A, b \in B\}.$$

Wir untersuchen, ob die Potenzmeneg $\mathcal{P}(\mathbb{R}) = \{A \mid A \subseteq \mathbb{R}\}$ zusammen mit der obigen Verknüpfung eine (abelsche) Gruppe bildet:

Für $A,B,C \in \mathcal{P}(\mathbb{R})$ ist

$$\begin{aligned} A \boxplus (B \boxplus C) &= \{a+d \mid a \in A, d \in B \boxplus C\} \\ &= \{a+d \mid a \in A, d \in \{b+c \mid b \in B, c \in C\}\} \\ &= \{a+b+c \mid a \in A, b \in B, c \in C\} \\ &= \{d+c \mid d \in \{a+b \mid a \in A, b \in B\}, c \in C\} \\ &= \{d+c \mid d \in A \boxplus B, c \in C\} = (A \boxplus B) \boxplus C, \end{aligned}$$

also ist $\boxplus$ assoziativ. Da für alle $A,B \in \mathcal{P}(\mathbb{R})$

$$A \boxplus B = \{a+b \mid a \in A, b \in B\} = \{b+a \mid b \in B, a \in A\} = B \boxplus A.$$

ist $\boxplus$ auch kommutativ. Die Teilmenge $\{0\} \subseteq \mathbb{R}$ ist neutral bezüglich $\boxplus$, denn für alle $A \in \mathcal{P}(\mathbb{R})$ ist

$$A \boxplus \{0\} = \{a + b \mid a \in A, b \in \{0\}\} = \{a + 0 \mid a \in A\} = \{a \mid a \in A\} = A.$$

Es fehlt nur noch, dass jedes $A \in \mathcal{P}(X)$ ein inverses Element $B \in \mathcal{P}(X)$ bezüglich $\boxplus$ besitzt, d.h. dass $A \boxplus (-A) = \{0\}$. Da aber beispielsweise

$$\emptyset \boxplus \emptyset = \{a + b \mid a \in \emptyset, b \in \emptyset\} = \emptyset$$

besitzt $\emptyset \in \mathcal{P}(X)$ kein Inverses. Also definiert $\boxplus$ *keine* Gruppenstruktur auf $\mathcal{P}(X)$.

18. Für ein fixiertes $c \in \mathbb{R}$ definieren wir eine binäre Verknüpfung $+_c$ auf $\mathbb{R}$ durch

$$x +_c y \coloneqq x + y - c \quad \text{für alle } x, y \in \mathbb{R}.$$

Wir überprüfen, ob $\mathbb{R}$ zusammen mit $+_c$ eine (abelsche) Gruppe bildet: Für alle $x, y, z \in \mathbb{R}$ ist

$$\begin{aligned} x +_c (y +_c z) &= x +_c +(y + z - c) = x + y + z - 2c \\ &= (x + y - c) + z - c = (x + y - c) +_c z = (x +_c y) +_c z, \end{aligned}$$

also ist $+_c$ assoziativ. Für alle $x, y \in \mathbb{R}$ ist auch

$$x +_c y = x + y - c = y + x - c = y +_c x,$$

also ist $+_c$ kommutativ. Für alle $x, e \in \mathbb{R}$ ist

$$x = x +_c e = x + e - c \Leftrightarrow e = c,$$

also ist c neutral bezüglich $+_c$. Für $x, y \in \mathbb{R}$ ist

$$c = x +_c y = x + y - c \Leftrightarrow y = 2c - x,$$

also ist $2c - x$ invers zu x bezüglich $+_c$. Ingesamt zeigt dies, dass $\mathbb{R}$ zusammen mit $+_c$ eine abelsche Gruppe bildet. (Für $c = 0$ erhalten wir die additive Gruppe von $\mathbb{R}$.)

19. Als Verallgemeinerung des obigen Beispiels ergibt sich für eine beliebige abelsche Gruppe A und ein beliebiges Element $c \in A$, dass die Verknüpfung $+_c$ mit

$$a +_c b \coloneqq a + b - c \quad \text{für alle } a, b \in A$$

auf der unterliegenden Menge von A eine (neue) Gruppenstruktur definiert. Diese Verknüpfung $+_c$ stimmt genau dann mit der ursprünglichen Addition $+$ überein, wenn $c = 0$ (denn $0 + 0 = 0$ und $0 +_c 0 = -c$.

20. Für $n, m \in \mathbb{N}$ sei $n * m \coloneqq n^m$ (wobei $0^0 = 1$). Dann bildet $\mathbb{N}$ zusammen mit $*$ keine Gruppe, da etwa

$$2 * (3 * 2) = 2^{(3^2)} = 2^9 \neq 2^6 = (2^3)^2 = (2 * 3) * 2.$$

21. Für $x, y \in \mathbb{R}$ sei $x \vee y = \max\{x, y\}$. Wir überprüfen, ob $\mathbb{R}$ zusammen mit $\vee$ eine (abelsche) Gruppe bildet:

    Für alle $x, y, z \in \mathbb{R}$ ist

    $$\begin{aligned} x \vee (y \vee z) &= x \vee \max\{y, z\} = \max\{x, \max\{y, z\}\} = \max\{x, y, z\} \\ &= \max\{\max\{x, y\}, z\} = \max\{x, y\} \vee z = (x \vee y) \vee z, \end{aligned}$$

    also ist $\vee$ assoziativ. Für alle $x, y \in \mathbb{R}$ ist

    $$x \vee y = \max\{x, y\} = \max\{y, z\} = y \vee x,$$

    also ist $\vee$ auch kommutativ. Wäre $e \in \mathbb{R}$ neutral bezüglich $\vee$, so wäre

    $$x = x \vee e = \max\{x, e\} \quad \text{für alle } x \in \mathbb{R}.$$

    Somit wäre $e \leq x$ für alle $x \in \mathbb{R}$; es gibt aber keine reelle Zahl, die diese Bedingung erfüllt. Also ist $\mathbb{R}$ zusammen mit $\vee$ keine Gruppe.

22. Es sei $R = \mathbb{R} \cup \{-\infty\} = [-\infty, \infty)$. Wir untersuchen, ob R zusammen mit der Verknüpfung $\vee$ mit

    $$x \vee y = \max\{x, y\} \quad \text{für alle } x, y \in R$$

    eine abelsche Gruppe bildet: Wie bereits im vorherigen Beispiel ergibt sich, dass $\vee$ assoziativ und kommutativ ist. Da

    $$x \vee -\infty = \max\{x, -\infty\} = x \quad \text{für alle } x \in R$$

    ist $-\infty$ neutral bezüglich $\vee$. Es gilt nur noch zu überprüfen, ob $x \in R$ ein Inverses bezüglich $\vee$ besitzt: Ist bereits $x \in \mathbb{R}$, so ist

    $$x \vee y = \max\{x, y\} \geq x > -\infty \quad \text{für alle } y \in R,$$

    weshalb x kein Inverses bezüglich $\vee$ besitzt. Also ist R keine Gruppe bezüglich $\vee$.

2.2. Gruppen mit zwei Elementen

Wir wollen in diesem Abschnitt erläutern, wieso es quasi nur eine Gruppe mit zwei Elementen gibt. Konkret zeigen wir, dass es für zweielementige Gruppen G und H einen eindeutigen Isomorphismus $\varphi\colon G \to H$ gibt.

Ist G eine zweielementige Gruppe, so ist $G = \{e, \alpha\}$, wobei e das neutrale Element von G bezeichnet und $\alpha \neq e$. Es muss $\alpha^{-1} = \alpha$; ansonsten wäre nämlich $\alpha^{-1} = e$ und somit $\alpha = (\alpha^{-1})^{-1} = e^{-1} = e$. Da $\alpha = \alpha^{-1}$ ist $\alpha^2 = e$. Die Multplikation auf G ist damit eindeutig bestimmt, da $e \cdot e = \alpha \cdot \alpha = e$ und $e \cdot \alpha = \alpha \cdot e = \alpha$.

Dies zeigt, dass es auf einer zweielementigen Menge nur eine Gruppenstruktur geben kann. Inbesondere sollten daher je zwei zweielementige Gruppen „gleich“ sein. Diese intuitive Idee von Gleichheit lässt sich mithilfe des Idee der eindeutigen Isomorphie konkretisieren:

Sind G und H zwei zweielementige Gruppen, so gibt es eindeutige Elemente $\alpha \in G$ und $\beta \in H$ mit $\alpha \neq e_G$ und $\beta \neq e_H$, wobei e_G das neutrale Element von G bezeichnet und e_H das neutrale Element von H. Nach der obigen Diskussion ist $\alpha^2 = e_G$ und $\beta^2 = e_H$.

Die Abbildung

$$\varphi\colon G \to H, \quad \text{mit} \quad \varphi(e_G) = e_H \quad \text{und} \quad \varphi(\alpha) = \beta$$

ist bijektiv. Sie ist ein Gruppenisomorphismus, da

$$\begin{aligned}
\varphi(e_G \cdot e_G) &= \varphi(e_G) = e_H = e_H \cdot e_H = \varphi(e_G) \cdot \varphi(e_G),\\
\varphi(e_G \cdot \alpha) &= \varphi(\alpha) = \beta = e_H \cdot \beta = \varphi(e_G) \cdot \varphi(\alpha),\\
\varphi(\alpha \cdot e_G) &= \varphi(\alpha) = \beta = \beta \cdot e_H = \varphi(\alpha) \cdot \varphi(e_G),\\
\varphi(\alpha \cdot \alpha) &= \varphi(e_G) = e_H = \beta \cdot \beta = \varphi(\beta) \cdot \varphi(\beta).
\end{aligned}$$

Also sind G und H isomorph.

Ist $\psi\colon G \to H$ ein Gruppenisomorphismus, so muss bereits $\varphi = \psi$: Da ψ ein Gruppenhomomorphismus ist, muss $\psi(e_G) = e_H$. Da ψ injektiv ist, muss außerdem $\psi(\alpha) \neq \psi(e_G) = e_H$, also $\psi(\alpha) = \beta$. Also ist φ bereits der eindeutige Gruppenisomorphismus $G \to H$. Man sagt, dass G und H *eindeutig isomorph* sind.

2.3. Untergruppen bezüglich Gruppenhomomorphismen

Es seien G und H Gruppen und es sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus.

2.3.1. Der Kern eines Gruppenhomomorphismus

Definition 2.1. *Der* Kern *von φ ist*

$$\ker(\varphi) \coloneqq \{g \in G \mid \varphi(g) = 1\}.$$

Wir zeigen, dass $\ker(\varphi)$ eine Untergruppe von G ist: Da $\varphi(1) = 1$ ist $1 \in \ker(\varphi)$. Sind $x, y \in \ker(\varphi)$, so ist $\varphi(x) = \varphi(y) = 1$ und deshalb

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = 1 \cdot 1 = 1,$$

also auch $x \cdot y \in \ker(\varphi)$. Ist $x \in \ker(\varphi)$, so ist $\varphi(x) = 1$ und deshalb

$$\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1,$$

also auch $x^{-1} \in \ker(\varphi)$. Ingesamt zeigt dies, dass $\ker(\varphi)$ eine Untergruppe von G ist.

Bemerkung 2.2. Es gilt, dass φ genau dann injektiv ist, falls $\ker(\varphi) = \{1\}$, falls also der Kern möglichst klein ist:

Ist φ injektiv und $x \in \ker(\varphi)$ so ist $\varphi(x) = 1 = \varphi(1)$, wegen der Injektivität von φ also $x = 1$. Somit ist dann $\ker(\varphi) = \{1\}$.

Ist $\ker(\varphi) = \{1\}$ und sind $x, y \in G$ mit $\varphi(x) = \varphi(y)$, so ist

$$\varphi(x \cdot y^{-1}) = \varphi(x) \cdot \varphi(y^{-1}) = \varphi(x) \cdot \varphi(y)^{-1} = \varphi(x) \cdot \varphi(x)^{-1} = 1,$$

und deshalb $x \cdot y^{-1} \in \ker(\varphi) = \{1\}$. Da $x \cdot y^{-1} = 1$ ergibt sich durch Multiplikation mit y von rechts, dass $x = y$. Also ist φ injektiv.

2.3.2. Das Bild eines Gruppenhomomorphismus

Wir zeigen, dass das Bild

$$\mathrm{im}(\varphi) = \varphi(G) = \{\varphi(g) \mid g \in G\}$$

eine Untergruppe von H ist: Da $1 = \varphi(1)$ ist $1 \in \mathrm{im}(\varphi)$. Sind $x, y \in \mathrm{im}(\varphi)$, so gibt es $x', y' \in G$ mit $\varphi(x') = x$ und $\varphi(y') = y$. Damit ist

$$x \cdot y = \varphi(x') \cdot \varphi(y') = \varphi(x' \cdot y'),$$

also auch $x \cdot y \in \mathrm{im}(\varphi)$. Ist $x \in \mathrm{im}(\varphi)$, so gibt es $x' \in G$ mit $\varphi(x') = x$. Da damit

$$x^{-1} = \varphi(x')^{-1} = \varphi((x')^{-1})$$

ist auch $x^{-1} \in \mathrm{im}(\varphi)$. Ingesamt zeigt dies, dass $\mathrm{im}(\varphi)$ ein Untergruppe von H ist.

Ist G abelsch, so ist es auch $\mathrm{im}(\varphi)$: Sind nämlich $x, y \in \mathrm{im}(\varphi)$, so gibt es $x', y' \in G$ mit $x = \varphi(x')$ und $y = \varphi(y')$, weshalb

$$x \cdot y = \varphi(x') \cdot \varphi(y') = \varphi(x' \cdot y') = \varphi(y' \cdot x') = \varphi(y') \cdot \varphi(x') = y \cdot x.$$

2.3.3. Bilder von Untergruppen

Es sei $K \subseteq G$ eine Untergruppe. Wir zeigen, dass das Bild von K unter φ, also

$$\varphi(K) = \{\varphi(k) \mid k \in K\},$$

eine Untergruppe von H ist: Da $1 \in K$ ist $1 = \varphi(1) \in H$. Sind $x, y \in \varphi(K)$ so gibt es $x', y' \in K$ mit $\varphi(x') = x$ und $\varphi(y') = y$. Da K ein Untergruppe ist, ist auch $x' \cdot y' \in K$. Da außerdem

$$x \cdot y = \varphi(x') \cdot \varphi(y') = \varphi(x' \cdot y')$$

ist dann auch $x \cdot y \in \varphi(K)$. Ist $x \in \varphi(K)$, so gibt es $x' \in K$ mit $\varphi(x') = x$. Da K eine Untergruppe ist, ist auch $(x')^{-1} \in K$. Da außerdem

$$x^{-1} = \varphi(x')^{-1} = \varphi((x')^{-1})$$

ist dann auch $x^{-1} \in \varphi(K)$. Ingesamt zeigt dies, dass $\varphi(K)$ eine Untergruppe von K ist.

Ist K abelsch, so ist es auch $\varphi(K)$: Für $x, y \in \mathrm{im}(\varphi)$ gibt es nämlich $x', y' \in K$ mit $x = \varphi(x')$ und $y = \varphi(y')$, weshalb

$$x \cdot y = \varphi(x') \cdot \varphi(y') = \varphi(x' \cdot y') = \varphi(y' \cdot x') = \varphi(y') \cdot \varphi(x') = y \cdot x.$$

Bemerkung 2.3. Es fällt auf, dass der Beweis, dass $\varphi(K)$ ein Untergruppe ist, analog zu dem Beweis verläuft, dass $\mathrm{im}(\varphi)$ eine Untegruppe ist. Dies ist kein Zufall: Da φ ein Gruppenhomomorphismus ist, ist auch die Einschränkung $\varphi|_K \colon K \to H$ ein Gruppenhomomorphismus. Daraus folgt direkt, dass $\varphi(K) = \mathrm{im}(\varphi|_K)$ eine Untergruppe von H ist.

2.3.4. Urbilder von Untergruppen

Es sei $K \subseteq H$ eine Untergruppe. Wir zeigen, dass das Urbild von K unter φ, also

$$\varphi^{-1}(K) = \{x \in G_1 \mid \varphi(x) \in K\},$$

eine Untergruppe von G ist: Da K eine Untergruppe ist, ist $\varphi(1) = 1 \in K$. Also ist $1 \in \varphi^{-1}(K)$. Sind $x, y \in \varphi^{-1}(K)$, so ist $\varphi(x), \varphi(y) \in K$. Da K eine Untergruppe ist, ist damit auch $\varphi(xy) = \varphi(x)\varphi(y) \in K$, also $xy \in \varphi^{-1}(K)$. Ist $x \in \varphi^{-1}(K)$, so ist $\varphi(x) \in K$. Da K eine Untergruppe ist, ist damit auch $\varphi(x^{-1}) = \varphi(x)^{-1} \in K$, also $x^{-1} \in \varphi^{-1}(K)$. Insgesamt zeigt dies, dass $\varphi^{-1}(K)$ eine Untergruppe von G ist.

Bemerkung 2.4. Indem man $K = \{1\}$ wählt, erhält man auch so einen neuen Beweis, dass

$$\varphi^{-1}(K) = \varphi^{-1}(\{1\}) = \{x \in G \mid \varphi(x) \in \{1\}\} = \{x \in G \mid \varphi(x) = 1\} = \ker(\varphi)$$

eine Untergruppe von G ist.

2.4. Schnitte und Vereinigungen von Untergruppen

Es sei G eine Gruppe.

2.4.1. Schnitte von Untergruppen

Es sei I eine Indexmenge und für jedes $i \in I$ sei $H_i \subseteq G$ eine Untergruppe. Wir zeigen, dass dann auch der Schnitt $\bigcap_{i \in I} H_i \subseteq G$ eine Untergruppe ist:

Da H_i für jedes $i \in I$ eine Untergruppe ist, ist $1 \in H_i$ für jedes $i \in I$, und somit auch $1 \in \bigcap_{i \in I} H_i$.

Sind $x, y \in \bigcap_{i \in I} H_i$, so ist $x, y \in H_i$ für jedes $i \in I$. Damit ist auch $x \cdot y \in H_i$ für alle $i \in I$, da H_i für jedes $i \in I$ eine Untergruppe ist. Also ist auch $x \cdot y \in \bigcap_{i \in I} H_i$.

Ist $x \in \bigcap_{i \in I} H_i$, so ist $x \in H_i$ für alle $i \in I$. Da H_i für alle $i \in I$ eine Untergruppe ist, ist damit auch $x^{-1} \in H_i$ für jedes $i \in I$. Also ist auch $x^{-1} \in \bigcap_{i \in I} H_i$.

Insgesamt zeigt dies, dass auch $\bigcap_{i \in I} H_i$ eine Untergruppe von G ist.

2.4.2. Vereinigung von Untergruppen

Vereinigungen von Untergruppen sind nicht notwendigerweise wieder Untergruppen: Wir zeigen, dass für zwei Untergruppen $H_1, H_2 \subseteq G$ die Vereinigung $H_1 \cup H_2$ genau dann eine Untergruppe ist, wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$:

Ist $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$, so ist $H_1 \cup H_2 = H_2$ oder $H_1 \cup H_2 = H_1$, also $H_1 \cup H_2$ ebenfalls eine Untergruppe.

Es sei andererseits $H_1 \cup H_2$ wieder eine Untergruppe. Angenommen, es ist weder $H_1 \subseteq H_2$ noch $H_2 \subseteq H_1$. Dann gibt es $h_1 \in H_1$ mit $h_1 \notin H_2$ und $h_2 \in H_2$ mit $h_2 \notin H_1$. Da $h_1, h_2 \in H_1 \cup H_2$, und $H_1 \cup H_2$ nach Annahme eine Untergruppe ist, ist auch $h_1 h_2 \in H_1 \cup H_2$. Also ist $h_1 h_2 \in H_1$ oder $h_1 h_2 \in H_2$.

Ist $h_1h_2 \in H_1$, so ist auch $h_2 = h_1^{-1}h_1h_2 \in H_1$, was der Annahme $h_2 \notin H_1$ widerspricht. Ist andererseits $h_1h_2 \in H_2$, so ist $h_1 = h_1h_2h_2^{-1} \in H_2$, was der Annahme $h_1 \notin H_1 \cup H_2$.

Dieser Widerspruch zeigt, dass bereits $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$ gelten muss, wenn die Vereinigung $H_1 \cup H_2$ ebenfalls eine Untergruppe ist.

Beispiel(e). Durch direktes Nachrechnen ergibt sich, dass sowohl $H_1 \coloneqq \{(x,0) \mid x \in \mathbb{R}\}$ als auch $H_2 \coloneqq \{(0,y) \mid y \in \mathbb{R}\}$ je eine additive Untergruppe von $\mathbb{R}^2$ ist. (Eine abstrakte Alternative zum Nachrechnen: Die beiden Abbildungen $\iota_1 \colon \mathbb{R} \to \mathbb{R}^2, x \mapsto (x,0)$ und $\iota_2 \colon \mathbb{R} \to \mathbb{R}^2, y \mapsto (0,y)$ sind Gruppenhomomorphismen. Also sind $H_1 = \mathrm{im}(\iota_1)$ und $H_2 = \mathrm{im}(\iota_2)$ Untergruppen.) Da aber weder $H_1 \subseteq H_2$ (da $(1,0) \in H_1$ aber $(1,0) \notin H_2$) noch $H_2 \subseteq H_1$ (da $(0,1) \in H_2$ aber $(0,1) \notin H_1$), ist $H_1 \cup H_2$ keine Untergruppe von $\mathbb{R}^2$.

2.4.3. Aufsteigende Vereinigungen von Untergruppen

Für jedes $n \in \mathbb{N}$ sei $H_n \subseteq G$ eine Untergruppe, so dass $H_n \subseteq H_m$ falls $n \leq m$, d.h. wir haben eine aufsteigende Kette

$$H_0 \subseteq H_1 \subseteq H_2 \subseteq H_3 \subseteq \cdots \subseteq G$$

von Untergruppen. Wir zeigen, dass dann die Vereinigung $\bigcup_{n\in\mathbb{N}} H_n$ ebenfalls eine Untergruppe von G ist:

Es ist $1 \in H_0 \subseteq \bigcup_{n\in\mathbb{N}} H_n$, da H_0 eine Untergruppe ist. Ist $x \in \bigcup_{n\in\mathbb{N}} H_n$, so gibt es ein $m \in \mathbb{N}$ mit $x \in H_m$. Da H_m eine Untergruppe ist, ist auch $x^{-1} \in H_m \subseteq \bigcup_{n\in\mathbb{N}} H_n$.

Für $x, y \in \bigcup_{n\in\mathbb{N}} H_n$ gibt es $m_1, m_2 \in \mathbb{N}$ mit $x \in H_{m_1}$ und $y \in H_{m_2}$. Da $m_1 \leq m_2$ oder $m_2 \leq m_1$ ist $H_{m_1} \subseteq H_{m_2}$ oder $H_{m_2} \subseteq H_{m_1}$. Wir betrachten o.B.d.A. den Fall, dass $m_1 \leq m_2$, also $H_{m_1} \subseteq H_{m_2}$. Da $x \in H_{m_1} \subseteq H_{m_2}$ und $y \in H_{m_2}$, und H_{m_2} eine Untergruppe ist, ist auch $x \cdot y \in H_{m_2} \subseteq \bigcup_{n\in\mathbb{N}} H_n$.

Insgesamt zeigt dies, dass $\bigcup_{n\in\mathbb{N}} H_n$ eine Untergruppe von G ist.

Bemerkung 2.5. 1. Allgmeiner gilt: Ist $(I, \subseteq)$ eine total, bzw. linear geordnete Menge, und $H_i \subseteq G$ für jedes $i \in I$ eine Untergruppe, so dass $H_i \subseteq H_j$ für alle $i, j \in I$ mit $i \leq j$, so ist die aufsteigende Vereinigung $\bigcup_{i\in I} H_i \subseteq G$ eine Untergruppe. Der Beweis verläuft analog obigen Sonderfall $(\mathbb{N}, \leq)$.

2. Noch allgemeiner: Es sei $(I, \subseteq)$ eine *gerichtete Menge*, d.h. eine partiell geordnete Menge, so dass es für alle $i, j \in I$ ein $k \in I$ mit $i \leq k$ und $j \leq k$ gibt. Für jedes $i \in I$ sei $H_i \subseteq G$ eine Untergruppe, so dass $H_i \subseteq H_j$ für alle $i, j \in I$ mit $i \leq j$. Dann ist auch die Vereinigung $\bigcup_{i\in I} H_i$ wieder eine Untergruppe. Der Beweis hierfür verläuft ähnlich zu dem Beweis für total geordnete Mengen.

2.5. Untergruppen von $\mathbb{C}^\times$

2.5.1. Der Einheitskreis S^1

Der Betrag einer komplexen Zahl $z = x + iy \in \mathbb{C}$ ist definiert als

$$|z| \coloneqq \sqrt{x^2 + y^2} = \sqrt{z\overline{z}}.$$

Für alle $z_1, z_2 \in \mathbb{C}$ ist

$$|z_1 z_2| = \sqrt{z_1 z_2 \overline{z_1 z_2}} = \sqrt{z_1 \overline{z_1} z_2 \overline{z_2}} = \sqrt{z_1 \overline{z_1}} \sqrt{z_2 \overline{z_2}} = |z_1||z_2|$$

und es ist $|1| = \sqrt{1 \cdot \overline{1}} = \sqrt{1 \cdot 1} = \sqrt{1} = 1$.

Definition 2.6. *Der* Einheitskreis *ist definiert als*

$$S^1 \coloneqq \{z \in \mathbb{C} \mid |z| = 1\}.$$

Wir zeigen, dass S^1 eine Untergruppe von $\mathbb{C}^\times$ ist: Ist $z \in \mathbb{C}$, so ist $0 \neq 1 = |z| = \sqrt{z\overline{z}}$, also $z \neq 0$ und somit $z \in \mathbb{C}^\times$. Also ist $S^1 \subseteq \mathbb{C}^\times$ eine Teilmenge.

Da $|1| = 1$ ist $1 \in S^1$. Für $z_1, z_2 \in S^1$ ist $|z_1| = |z_2| = 1$, also auch

$$|z_1 z_2| = |z_1||z_2| = 1 \cdot 1 = 1,$$

und somit $z_1 z_2 \in S^1$. Für $z \in S^1$ ist $|z| = 1$. Daher ist auch

$$1 = |1| = |z z^{-1}| = |z||z^{-1}| = 1 \cdot |z^{-1}| = |z^{-1}|$$

und deshalb $z^{-1} \in S^1$.

Das zeigt, dass S^1 ein Untergruppe von $\mathbb{C}^\times$ ist.

Bemerkung 2.7. Die Aussage lässt sich auch abstrakter zeigen: Da $|z_1 z_2| = |z_1| \cdot |z_2|$ für alle $z_1, z_2 \in \mathbb{C}$, und $|z| > 0$ für alle $z \neq 0$, ist die Abbildung $b\colon \mathbb{C}^\times \to \mathbb{R}_+$, $z \mapsto |z|$ ein Gruppenhomomorphismus. Daher ist

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} = \{z \in \mathbb{C}^\times \mid |z| = 1\} = \{z \in \mathbb{C}^\times \mid b(z) = 1\} = \ker(b)$$

eine Untergruppe.

2.5.2. n-te Einheitswurzeln

Es sei K ein Körper und $n \in \mathbb{N}$, $n \geq 1$. Ein Element $x \in K$ heißt *n-te Einheitswurzel* falls $x^n = 1$. Wir zeigen, dass

$$W_n(K) \coloneqq \{x \in K \mid x^n = 1\}$$

eine Untergruppe von $K^\times$ ist: Da $1^n = 1$ ist $1 \in W_n(K)$. Sind $x, y \in W_n(K)$ so ist $x^n = 1$ und $y^n = 1$, also auch $(xy)^n = x^n y^n = 1 \cdot 1 = 1$ und deshalb $xy \in W_n(K)$. Für $x \in W_n(K)$ ist $x^n = 1$, also

$$(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$$

und deshalb $x \in W_n(K)$.

Ingesamt zeigt dies, dass $W_n(K)$ eine Untergruppe von $\mathbb{C}^\times$ ist.

Bemerkung 2.8. Da $x^n \neq 0$ für alle $x \neq 0$ und $(xy)^n = x^n y^n$ für alle $x, y \in K$ ist die Abbildung $p_n\colon \mathbb{C}^\times \to \mathbb{C}^\times$, $z \mapsto z^n$ ein Gruppenhomomorphismus. Daher folgt, dass

$$W_n(K) = \{x \in K \mid x^n = 1\} = \{x \in K^\times \mid x^n = 1\} = \{x \in K^\times \mid p_n(x) = 1\} = \ker(p_n)$$

eine Untergruppe ist.

Für $K = \mathbb{R}$ ist beispielsweise

$$W_n(\mathbb{R}) = \begin{cases} \{-1, 1\} & \text{falls } n \text{ ungerade ist,} \\ \{1\} & \text{falls } n \text{ ungerade ist.} \end{cases}$$

Für $K = \mathbb{C}$ und $z \in W_n(\mathbb{C})$ ist $|z| \in \mathbb{R}$ mit $|z| \geq 0$ und $|z|^n = |z^n| = |1| = 1$. Es muss also $|z| = 1$ und somit $z \in S^1$. Also ist $W_n(\mathbb{C})$ bereits eine Untergruppe von S^1. Es stellt sich heraus, dass $W_n(\mathbb{C})$ aus n Elementen besteht, die gleichmäßig auf dem Einheitskreis S^1 verteilt sind.

2.6. Klassifikation der Untergruppen von $\mathbb{Z}$

In diesem Abschnitt bestimmen wir die Untergruppen von $\mathbb{Z}$ (d.h. von $(\mathbb{Z}, +)$, wobei $+$ die gewöhnliche Addition bezeichnet). Als Anwendung dieser Klassifikation führen wir die Charakteristik eines Körpers ein.

2.6.1. Die Klassifikation selbst

Für jedes $n \in \mathbb{N}$ sei

$$n\mathbb{Z} \coloneqq \{nk \mid k \in \mathbb{Z}\} = \{a \in \mathbb{Z} \mid a \text{ ist durch } n \text{ teilbar.}$$

Wir zeigen zuänchst, dass $n\mathbb{Z}$ für jedes $n \in \mathbb{N}$ eine Untergruppe definiert:

Es ist $0 = n \cdot 0 \in \mathbb{Z}$. Sind $x, y \in n\mathbb{Z}$, so gibt es $k, l \in \mathbb{Z}$ mit $x = nk$ und $y = nl$. Da damit $x + y = nk + nl = n(k + l)$ ist auch $x + y \in n\mathbb{Z}$. Ist $x \in n\mathbb{Z}$, so gibt es $k \in \mathbb{Z}$ mit $x = nk$. Da damit $-x = -nk = n(-k)$ ist auch $-x \in \mathbb{Z}$. Das zeigt, dass $n\mathbb{Z}$ eine Untergruppe ist.

Bemerkung 2.9. Ein weniger rechenlastiger Beweis besteht darin, dass $\varphi_n : \mathbb{Z} \to \mathbb{Z}, k \mapsto nk$ ein Gruppenhomomorphismus ist, da $\varphi_n(k + l) = n(k + l) = nk + nl = \varphi_n(k) + \varphi_n(l)$ für alle $k, l \in \mathbb{Z}$, und deshalb

$$\text{im}(\varphi_n) = \{\varphi_n(k) \mid k \in \mathbb{Z}\} = \{nk \mid k \in \mathbb{Z}\} = n\mathbb{Z}$$

eine Untergruppe von $\mathbb{Z}$ ist.

Wir zeigen nun, dass jede Untergruppe $H \subseteq \mathbb{Z}$ von der Form $H = n\mathbb{Z}$ für ein eindeutiges $n \in \mathbb{N}$ ist: Ist $H = \{0\}$, so gilt die Aussage mit $n = 0$. Wir betrachten daher den Fall, dass $\{0\} \subsetneq H$. Dann gibt es ein $m \in H$ mit $m > 0$, also ist $\{m \in H \mid m > 0\} \neq 0$. Da jede nichtleere Teilmenge von $\mathbb{N}$ ein minimales Element besitzt, existiert $n \coloneqq \min\{m \in H \mid m > 0\}$.

Da $n \in H$ ist auch $n\mathbb{Z} \subseteq H$: Für alle $k \in \mathbb{N}$, $k \geq 1$ ist $nk = \sum_{i=1}^{k} n \in H$, es ist $n \cdot 0 = 0 \in H$ und für alle $k \in \mathbb{N}$ mit $k \leq -1$ ist wegen $n(-k) \in H$ auch $nk = -n(-k) \in H$.

Wir zeigen nun, dass bereits $H = n\mathbb{Z}$. Angenommen, es gibt $m \in H$ mit $m \notin n\mathbb{Z}$. Dann gibt es eindeutige $k, l \in \mathbb{Z}$ mit $m = nk + l$, wobei $0 \leq l < n$. Da $m \notin n\mathbb{Z}$ ist $l \neq 0$, also $0 < l < n$. Da $m \in H$ ist dann aber auch $l = m - nk \in H$. Da $0 < l < n$ steht dies im Widerspruch zur Definition von $n = \min\{m' \in H \mid m' > 0\}$.

Das zeigt, dass $H = n\mathbb{Z}$ mit $n \in \mathbb{N}$. Die Eindeutigkeit von n folgt daraus, dass sich n aus H bestimmen lässt durch $n = \min\{m \in H \mid m > 0\}$.

Ingesamt zeigt dies, dass es eine Bijektion

$$\mathbb{N} \to \{H \subseteq \mathbb{Z} \mid H \text{ ist eine Untergruppe}\}, n \mapsto n\mathbb{Z}$$

gibt.

2.6.2. Anwendung: Die Charakteristik eines Körpers

Ist K eine Körper, so ist die Abbildung $\varphi_K : \mathbb{Z} \to K, n \mapsto n \cdot 1$ ein Gruppenhomomorphismus von $\mathbb{Z}$ in die unterliegende additive Gruppe von K. Also ist $\ker(\varphi_K) = \{m \in \mathbb{Z} \mid m \cdot 1 = 0\}$ eine Untergruppe. Nach der obigen Klassifikation gibt es ein eindeutiges $n \in \mathbb{Z}$ mit $\ker(\varphi_K) = n\mathbb{Z}$. Man bezeichnet n als die *Charakteristik* von K, und schreibt $\mathrm{char}K$ für diese. Es ist also

$$\mathrm{char}(K) = \begin{cases} \min\{m > 0 \mid m \cdot 1 = 0\} & \text{falls es ein } m > 0 \text{ with } m \cdot 1 = 0 \text{ gibt} \\ 0 & \text{sonst.} \end{cases}$$

Beispiel(e). Für $K = \mathbb{Q}$ ist $\varphi_{\mathbb{Q}}$ injektiv, also $\ker(\varphi_K) = \{0\}$ und somit $\mathrm{char}K = 0$. Gleiches gilt für $K = \mathbb{R}$ und $K = \mathbb{C}$.

Ist $p > 0$ prim, so gilt für den in 3.5 konstruierten Körper $\mathbb{F}_p$, dass $\ker(\varphi_{\mathbb{F}_p}) = p\mathbb{Z}$ und somit $\mathrm{char}(\mathbb{F}_p) = p$.

Bemerkung 2.10. 1. Für einen Körper L und Unterkörper $K \subseteq L$ ist $\ker(\varphi_L) = \ker(\varphi_K)$ und somit $\mathrm{char}(K) = \mathrm{char}(L)$.

2. Ist K ein Körper so ist entweder $\mathrm{char}(K) = 0$, oder $\mathrm{char}(K) > 0$ eine Primzahl. Ist nämlich $n := \mathrm{char}(K) \neq 0$, so ist $n \cdot 1 = 0$. Ist n keine Primzahl, so gibt es $a, b \in \mathbb{N}$ mit $0 < a, b < n$ und $a \cdot b = n$. Da

$$(a \cdot 1) \cdot (b \cdot 1) = (a \cdot b) \cdot 1 = n \cdot 1 = 0$$

und K ein Körper ist, muss bereits $a \cdot 1 = 0$ oder $b \cdot 1 = 0$. Da $0 < a, b < n$ steht dies im Widerspruch dazu, dass $n = \min\{m > 0 \mid m \cdot 1 = 0\}$.

2.7. Die symmetrische Gruppen $S(X)$ und S_n und Untergruppen

2.7.1. Die symmetrische Gruppe $S(X)$

Es sei X eine beliebige Menge und $S(X) := \{\sigma : X \to X \mid \sigma \text{ ist bijektiv}\}$. Für beliebige $\sigma_1, \sigma_2 \in S(X)$ ist auch $\sigma_1 \circ \sigma_2 : X \to X$ bijektiv, also $\sigma_1 \circ \sigma_2 \in S(X)$.

Wir zeigen, dass $(S(X), \circ)$ eine Gruppe ist: Die Assoziativität von $\circ$ folgt direkt aus der allgemeinen Assoziativität der Funktionskomposition.

Für die Identitätsfunktion $\mathrm{id}_X \colon X \to X, x \mapsto x$ ist $\mathrm{id}_X \in S(X)$, da id_X bijektiv ist. Da $\mathrm{id}_X \circ \sigma = \sigma = \sigma \circ \mathrm{id}_X$ ist id_X ein neutrales Element bezüglich $\circ$.

Ist $\sigma \in S(X)$ so ist σ bijektiv und somit invertierbar, d.h. es gibt eine (eindeutige) Abbildung $\sigma^{-1} \colon X \to X$ mit $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}_X$. Also sind σ^{-1} und σ invers zueinander bezüglich $\circ$.

Insgesamt zeigt dies, dass $(S(X), \circ)$ eine Gruppe ist.

Definition 2.11. *Ist X eine Menge, so heißt die Gruppe $(S(X), \circ)$ die* symmetrische Gruppe von X. *Ein Element $\sigma \in S(X)$ heißt* Permutation.

Bemerkung 2.12. Statt $S(X)$ schreibt man auch $\Sigma(X)$.

2.7.2. Die symmetrische Gruppe S_n

Definition 2.13. *Für $n \in \mathbb{N}$ sei $S_n := S(\{1, \dots, n\})$ die* symmetrische Gruppe auf n Elementen.

Ein Element $\sigma \in S_n$ schreibt man auch als

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Beispiel(e). Für $\sigma \in S_5$ mit $\sigma(1) = 3$ $\sigma(2) = 5, \sigma(3) = 2, \sigma(4) = 1, \sigma(5) = 4$ ist

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4. \end{pmatrix}$$

Bemerkung 2.14. Statt S_n schreibt man auch Σ_n.

Wir bemerken zunächst, dass S_n genau $n!$ viele Elemente hat, da es genau $n!$ viele Bijektionen $\{1, \dots, n\} \to \{1, \dots, n\}$ gibt: Wählt man das Bild von 1 beliebig, so gibt es für das Bild von 2 noch $n-1$ Möglichkeiten, für das Bild von 3 anschließend noch $n-2$ Möglichkeiten, usw. Damit ergeben sich insgesamt $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$ mögliche Bijektionen.

Beispiel(e). 1. Die symmetrische Gruppe S_1 besitzt nur ein Element, nämlich $\mathrm{id}_{\{1\}}$. Insbesonder ist S_1 abelsch.

2. Die symmetrische Gruppe S_2 besteht aus $2! = 2$ Elementen, nämlich

$$1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \mathrm{id}_{\{1,2\}} \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Dabei ist $\tau^2 = 1$, was der Klassifikation zweielementiger Mengen in 2.2 entspricht. Insbesondere ist S_2 abelsch.

3. Die symmetrische Gruppe S_3 besteht aus $3! = 6$ Elementen, nämlich

$$1 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right),\ \tau_{12} = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right),\ \tau_{23} = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right),\ \tau_{13} = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right),\ r = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right),\ r^2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right).$$

Dabei steht τ für „Transposition“, d.h. das Vertauschen zweier Elemente, und r für „Rotation“. Man bemerke, dass $r^3 = 1$, bzw. $r^2 = r^{-1}$, d.h. einmal nach links rotieren ist das gleich wie zweimal nach rechts rotieren.

Man bemerke, dass die Gruppe S_3 nicht abelsch ist, da etwa $r\tau_{12} = \tau_{23} \neq \tau_{13} = \tau_{12}r$.

4. Die symmetrische Gruppe S_4 besteht aus den folgenden $4! = 24$ Elementen:

$$\begin{array}{ccccc}
\left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\1&2&4&3\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\1&3&2&4\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right) \\
\left(\begin{smallmatrix}1&2&3&4\\2&1&3&4\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\2&3&1&4\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\2&3&4&1\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\2&4&1&3\end{smallmatrix}\right) \\
\left(\begin{smallmatrix}1&2&3&4\\3&1&2&4\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\3&1&4&2\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\3&2&1&4\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right) \\
\left(\begin{smallmatrix}1&2&3&4\\4&1&2&3\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\4&1&3&2\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\4&2&1&3\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\4&2&3&1\end{smallmatrix}\right) & \left(\begin{smallmatrix}1&2&3&4\\4&3&1&2\end{smallmatrix}\right)
\end{array}$$

5. Wir möchten den geneigten Leser dazu ermutigen, sich auch die Element von S_5 aufzuschreiben.

Bemerkung 2.15. Wie oben gesehen ist S_3 nicht abelsch. Allgemeiner gilt, dass S_n für $n \geq 3$ nicht abelsch ist. Ein entsprechendes Gegenbeispiel lässt sich leicht aus dem von S_3 verallgemeinern: Für $\tau, r \in S_n$ mit

$$\tau = \begin{pmatrix}1&2&3&4&\cdots&n\\2&1&3&4&\cdots&n\end{pmatrix} \quad \text{und} \quad r = \begin{pmatrix}1&2&3&4&\cdots&n\\2&3&1&4&\cdots&n\end{pmatrix}.$$

ist

$$r\tau = \begin{pmatrix}1&2&3&4&\cdots&n\\1&3&2&4&\cdots&n\end{pmatrix} \neq \begin{pmatrix}1&2&3&4\cdots&n\\3&2&1&4\cdots&n\end{pmatrix} = \tau r.$$

2.7.3. Normalisatoren $N(Y)$ und Zentralisatoren $Z(Y)$

Definition 2.16. *Es sei X eine Menge und $Y \subseteq X$ eine Teilmenge. Dann heißt*

$$N_{S(X)}(Y) \coloneqq \{\sigma \in S(X) \mid \sigma(Y) = Y\}$$

der Normalisator *von Y (in $S(X)$) und*

$$Z_{S(X)}(Y) \coloneqq \{\sigma \in S(X) \mid \sigma(y) = y \text{ für alle } y \in Y\}$$

der Zentralisator *von Y (in $S(X)$).*

Wir zeigen zunächst, dass $N_{S(X)}(Y)$ eine Untergruppe von $S(X)$ ist: Da $\mathrm{id}_X(Y) = Y$ ist $\mathrm{id}_X \in N_{S(X)}(Y)$. Sind $\sigma, \tau \in N_{S(X)}(Y)$ so ist $\sigma(Y) = Y$ und $\tau(Y) = Y$. Daher ist

$$\begin{aligned}(\sigma \circ \tau)(Y) &= \{(\sigma \circ \tau)(y) \mid y \in Y\} = \{\sigma(\tau(y)) \mid y \in Y\} \\ &= \sigma(\{\tau(y) \mid y \in Y\}) = \sigma(\tau(Y)) = \sigma(Y) = Y\end{aligned}$$

und deshalb auch $\sigma \circ \tau \in N_{S(X)}(Y)$. Ist $\sigma \in N_{S(X)}(X)$, so ist $\sigma(Y) = Y$ und deshalb

$$\begin{aligned}Y &= \mathrm{id}_X(Y) = (\sigma^{-1} \circ \sigma)(Y) = \{(\sigma^{-1} \circ \sigma)(y) \mid y \in Y\} = \{\sigma^{-1}(\sigma(y)) \mid y \in Y\} \\ &= \sigma^{-1}(\{\sigma(y) \mid y \in Y\}) = \sigma^{-1}(\sigma(Y)) = \sigma^{-1}(Y),\end{aligned}$$

also auch $\sigma^{-1} \in N_{S(X)}(Y)$.

Insgesamt zeigt dies, dass $N_{S(X)}(Y) \subseteq S(X)$ eine Untergruppe ist. Inbesondere ist daher $N_{S(X)}(Y)$ zusammen mit der Funktionskomposition $\circ$ eine Gruppe.

Nun zeigen wir, dass auch $Z_{S(X)}(Y) \subseteq S(X)$ eine Untergruppe ist: Da $\mathrm{id}_X(x) = x$ für alle $x \in X$, und damit inbesondere $\mathrm{id}_X(y) = y$ für alle $y \in Y$, ist $\mathrm{id}_X \in Z_{S(X)}(Y)$. Sind $\sigma, \tau \in Z_{S(X)}(Y)$, so ist $\sigma(y) = y$ und $\tau(y) = y$ für alle $y \in Y$ und deshalb auch

$$(\sigma \circ \tau)(y) = \sigma(\tau(y)) = \sigma(y) = y \quad \text{für alle } y \in Y.$$

Also ist auch $\sigma \circ \tau \in Z_{S(X)}(Y)$. Ist $\sigma \in Z_{S(X)}(Y)$, so ist $\sigma(y) = y$ für jedes $y \in Y$ und daher

$$\sigma^{-1}(y) = \sigma^{-1}(\sigma(y)) = y \quad \text{für alle } y \in Y.$$

Also ist auch $\sigma \in Z_{S(X)}(Y)$.

Ingesamt zeigt dies, dass $Z_{S(X)}(Y)$ eine Untergruppe von $S(X)$ ist. Deshalb ist $Z_{S(X)}(Y)$ zusammen mit der Funktionskomposition $\circ$ wieder eine Gruppe.

Für jedes $\sigma \in Z_{S(X)}(Y)$ ist auch

$$\sigma(Y) = \{\sigma(y) \mid y \in Y\} = \{y \mid y \in Y\} = Y,$$

also $\sigma \in N_{S(X)}(Y)$. Wir haben also eine Kette von Untergruppen

$$Z_{S(X)}(Y) \subseteq N_{S(X)}(Y) \subseteq S(X).$$

Beispiel(e). 1. Es sei $X = \{1, 2, 3, 4, 5\}$, also $S(X) = S_5$, und $Y = \{4, 5\}$. Dann ist

$$Z_{S_5}(\{4, 5\}) = \{\sigma \in S_5 \mid \sigma(4) = 4, \sigma(5) = 5\}.$$

Die Elemente von $Z_{S_5}(Y)$ sind also diejenigen Permutationen aus S_5, die tatächlich nur die ersten drei Element vertauschen. Diese sind

$$\left(\begin{smallmatrix}1&2&3&4&5\\1&2&3&4&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&2&3&4&5\\2&1&3&4&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&2&3&4&5\\1&3&2&4&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&2&3&4&5\\3&2&1&4&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&2&3&4&5\\2&3&1&4&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&2&3&4&5\\3&1&2&4&5\end{smallmatrix}\right).$$

Insbesondere ist deshalb $Z_{S_5}(\{4, 5\}) \cong S_3$, wobei ein möglicher (und naheliegender) Gruppenisomorphismus durch

$$\varphi\colon S_3 \longrightarrow Z_{S_5}(\{4, 5\}),$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix} \longmapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 & 5 \end{pmatrix},$$

gegeben ist. Das Inverse φ^{-1} ist gegeben durch die Einschränkung

$$\varphi^{-1}\colon S_5 \to S_3, \quad \sigma \mapsto \sigma|_{\{1,2,3\}}.$$

2. Ist allgemeiner $Y \subseteq X$, so ist die Abbildung $\varphi\colon S(X \setminus Y) \to Z_{S(X)}(Y)$ mit

$$\varphi(\sigma)(x) = \begin{cases} \sigma(x) & \text{falls } x \notin Y, \\ x & \text{falls } x \in Y, \end{cases}$$

ein Gruppenisomorphismus, und das Inverse φ^{-1} ist gegeben durch die Einschränkung

$$\varphi^{-1}\colon Z_{S(X)}(Y) \to S(X \setminus Y), \quad \sigma \mapsto \sigma|_{X \setminus Y}.$$

2.8. Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ und ihre Untergruppen

Im Folgenden sei K ein (beliebiger) Körper.

2.8.1. Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$

Definition 2.17. *Eine Matrix $S \in \mathrm{Mat}(n \times n, K)$ heißt* invertierbar*, falls es eine Matrix $T \in \mathrm{Mat}(n \times n, K)$ gibt, so dass $ST = I_n = TS$. (Hier bezeichnet $I_n \in \mathrm{Mat}(n \times n, K)$ die Einheitsmatrix.)*

Es ist $\mathrm{GL}_n(K) \coloneqq \{S \in \mathrm{Mat}(n \times n, K) \mid S \text{ ist invertierbar}\}$.

Wir zeigen, dass $\mathrm{GL}_n(K)$ zusammen mit der üblichen Matrixmultiplikation eine Gruppe bildet:

Es ist bekannt, dass Matrixmultiplikation assoziativ ist.

Sind $S_1, S_2 \in \mathrm{GL}_n(K)$ invertierbar, so gibt es $T_1, T_2 \in \mathrm{Mat}(n \times n, K)$ mit $S_1T_1 = I_n$ und $S_2T_2 = I_n$. Da

$$(S_1S_2)(T_2T_1) = S_1S_2T_2T_1 = S_1I_nT_1 = S_1T_1 = I_n$$

ist auch S_1S_2 invertierbar. Das zeigt, dass die Multiplikation $\mathrm{GL}_n(K) \times \mathrm{GL}_n(K) \to \mathrm{GL}_n(K)$, $(S_1, S_2) \mapsto S_1S_2$ wohldefiniert ist.

Da $I_nI_n = I_n$ ist I_n invertierbar, also $I_n \in \mathrm{GL}_n(K)$. Da $SI_n = I_nS = S$ für alle $S \in \mathrm{Mat}(n \times n, k)$, und somit insbesondere für alle $S \in \mathrm{GL}_n(K)$, ist I_n neutral bezüglich der Matrixmultiplikation.

Für jedes $S \in \mathrm{GL}_n(K)$ gibt es per Definition von $\mathrm{GL}_n(K)$ eine Matrix $T \in \mathrm{Mat}(n \times n, K)$ mit $ST = TS = I_n$. Aus diesen Gleichungen folgt, dass auch T invertierbar ist, also $T \in \mathrm{GL}_n(K)$, und dass T bezüglich der Matrixmultiplikation invers zu S ist.

Insgesamt zeigt dies, dass $\mathrm{GL}_n(K)$ zusammen mit der üblichen Matrixmultiplikation eine Gruppe bildet. Man bezeichnet diese als die *allgemeine lineare Gruppe* (General Linear group).

2.8.2. Die Diagonalmatrizen $\mathrm{D}_n(k)$

Definition 2.18. *Eine quadratische Matrix $D = (d_{ij})_{i,j=1,\dots,n} \in \mathrm{Mat}(n \times n, K)$ heißt* Diagonalmatrix*, falls $d_{ij} = 0$ für alle $1 \leq i \neq j \leq n$, d.h. wenn D von der Form*

$$D = \begin{pmatrix} d_{11} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_{nn} \end{pmatrix}$$

ist. Für all $\lambda_1, \dots, \lambda_n \in K$ sei abkürzend $\mathrm{diag}(\lambda_1, \dots, \lambda_n) \in \mathrm{Mat}(n \times n, K)$ *die Diagonalmatrix mit Diagonaleinträgen $\lambda_1, \dots, \lambda_n$, d.h.*

$$\mathrm{diag}(\lambda_1, \dots, \lambda_n)_{ij} = \delta_{ij}\lambda_i = \delta_{ij}\lambda_j \quad \text{für alle } 1 \leq i, j \leq n,$$

also

$$\operatorname{diag}(\lambda_1, \dots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n. \end{pmatrix}$$

Es sei

$$\mathrm{D}_n(k) \coloneqq \{D \in \mathrm{GL}_n(K) \mid D \textit{ ist eine Diagonalmatrix}\}.$$

Wir zeigen, dass $\mathrm{D}_n(k)$ zusammen mit der üblichen Matrixmultiplikation eine Gruppe bildet, indem wir zeigen, dass $\mathrm{D}_n(K)$ eine Untergruppe von $\mathrm{GL}_n(K)$ ist.

Wir wollen zunächt verstehe, wie das Produkt von Diagonalmatrizen mit anderen Matrizen aussieht. Hierfür sei $D \in \mathrm{Mat}(n \times n, K)$ eine Diagonalmatrix, $A \in \mathrm{Mat}(m \times n, K)$ sowie $B \in \mathrm{Mat}(n \times m, K)$. Es seien $\lambda_1, \dots, \lambda_n \in K$ mit $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. Für alle $1 \leq i \leq m$ und $1 \leq j \leq n$ ist

$$(AD)_{ij} = \sum_{k=1}^{n} A_{ik} D_{kj} = \lambda_j A_{ij},$$

und für alle $1 \leq i \leq n$ und $1 \leq j \leq m$ ist

$$(DB)_{ij} = \sum_{k=1}^{n} D_{ik} B_{ij} = \lambda_i B_{ij}.$$

Also ist

$$AD = \begin{pmatrix} \lambda_1 A_{11} & \cdots & \lambda_n A_{1n} \\ \lambda_1 A_{21} & \cdots & \lambda_n A_{2n} \\ \vdots & \ddots & \vdots \\ \lambda_1 A_{m1} & \cdots & \lambda_n A_{mn} \end{pmatrix} \quad \text{und} \quad DB = \begin{pmatrix} \lambda_1 B_{11} & \lambda_1 B_{12} & \cdots & \lambda_1 B_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n B_{n1} & \lambda_n B_{n2} & \cdots & \lambda_n B_{nm} \end{pmatrix}$$

Ist $D' \in \mathrm{Mat}(n \times n, K)$ eine weiter Diagonalmatrix mit Diagonaleinträgen $\mu_1, \dots, \mu_n \in K$, also $D' = \operatorname{diag}(\mu_1, \dots, \mu_n)$, so ist insbesondere

$$\begin{aligned} &\operatorname{diag}(\lambda_1, \dots, \lambda_n) \cdot \operatorname{diag}(\mu_1, \dots, \mu_n) = D \cdot D' \\ &= \begin{pmatrix} \lambda_1 D'_{11} & \cdots & \lambda_1 D'_{1n} \\ \vdots & \ddots & \vdots \\ \lambda_n D'_{n1} & \cdots & \lambda_n D'_{nn} \end{pmatrix} = \begin{pmatrix} \lambda_1 \mu_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \mu_n \end{pmatrix} \\ &= \operatorname{diag}(\lambda_1 \mu_1, \dots, \lambda_n \mu_n). \end{aligned}$$

Die Multiplikation von Diagonalmatrizen funktioniert als „eintragsweise“.

Dies zeigt zum einen, dass das Produkt von Diagonalmatrizen wieder eine Diagonalmatrix ist. Also ist $\mathrm{D}_n(k)$ unter Produkten abgeschlossen. Außerdem ist $I_n = \mathrm{diag}(1, \dots, 1) \in D_n(k)$. Es bleibt zu zeigen, dass für alle $D \in \mathrm{D}_n(k)$ auch $D^{-1} \in \mathrm{D}_n(k)$.

Hierfür betrachten wir zunächst den Fall, dass $\lambda_i \neq 0$ für alle $1 \leq i \leq n$. Dann ist auch $D' \coloneqq \mathrm{diag}(\lambda_1^{-1}, \dots, \lambda_n^{-1})$ ein Diagonalmatrix, und es gilt

$$D \cdot D' = \mathrm{diag}(\lambda_1 \lambda_1^{-1}, \dots, \lambda_n \lambda_n^{-1}) = \mathrm{diag}(1, \dots, 1) = I_n.$$

Also ist dann $D^{-1} = D'$ ein Diagonalmatrix.

Tatsächlich muss, da D invertierbar ist, bereits $\lambda_i \neq 0$ für alle $1 \leq i \leq n$: Ansonsten gebe ein $1 \leq i \leq n$ mit $\lambda_i = 0$ und somit $D_{ij} = 0$ für alle $1 \leq j \leq n$ (für alle $1 \leq j \leq n$ mit $j \neq i$ gilt bereits $D_{ij} = 0$, da D ein Diagonalmatrix ist). Für jede Matrix $S \in \mathrm{GL}_n(K)$ wäre damit

$$(DS)_{ii} = \sum_{j=1}^{n} \underbrace{D_{ij}}_{=0} S_{ji} = 0.$$

Insbesondere wäre somit $DS \neq I_n$ für alle $S \in \mathrm{GL}_n(K)$, was im Widerspruch zu der Invertierbarkeit von D stünde.

Das zeigt, dass eine Diagonalmatrix $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ genau dann invertierbar ist, wenn $\lambda_i \neq 0$ für alle $1 \leq i \leq n$, und dann $D^{-1} = \mathrm{diag}(\lambda_1^{-1}, \dots, \lambda_n^{-1})$ ebenfalls eine Diagonalmatrix ist. Also ist $\mathrm{D}_n(k)$ ein Untergruppe von $\mathrm{GL}_n(K)$.

2.8.3. Die Skalarmatrizen $\mathrm{S}_n(K)$

Definition 2.19. *Eine quadratische Matrix $S \subseteq \mathrm{Mat}(n \times n, K)$ heißt* Skalarmatrix, *falls S eine Diagonalmatrix ist, deren Diagonaleinträge alle gleich sind, d.h. $S = \mathrm{diag}(\lambda, \dots, \lambda)$ für ein $\lambda \in K$. Es sei*

$$\mathrm{S}_n(K) \coloneqq \{S \in \mathrm{GL}(n \times n, K) \mid S \textit{ ist eine Skalarmatrix}\}.$$

Wir zeigen, dass $\mathrm{S}_n(K)$ eine Untergruppe von $\mathrm{GL}_n(K)$ ist: Es ist $I_n = \mathrm{diag}(1, \dots, 1) \in \mathrm{S}_n(K)$. Für $S, T \in \mathrm{S}_n(K)$ gibt es $\lambda, \mu \in K$ mit $S = \mathrm{diag}(\lambda, \dots, \lambda)$ und $T = \mathrm{diag}(\mu, \dots, \mu)$, weshalb auch

$$S \cdot T = \mathrm{diag}(\lambda, \dots, \lambda) \cdot \mathrm{diag}(\mu, \dots, \mu) = \mathrm{diag}(\lambda\mu, \dots, \lambda\mu) \in \mathrm{S}_n(K).$$

Außerdem ist damit auch

$$S^{-1} = \mathrm{diag}(\lambda, \dots, \lambda)^{-1} = \mathrm{diag}(\lambda^{-1}, \dots, \lambda^{-1}) \in \mathrm{S}_n(K).$$

Insgesamt zeigt dies, dass $\mathrm{S}_n(K)$ eine Untergruppe von $\mathrm{GL}_n(K)$ ist. Da Skalarmatrizen stets Diagonalmatrizen sind, ist bereits $\mathrm{S}_n(K) \subseteq \mathrm{D}_n(K)$. Wir haben also eine Kette von Untergruppen

$$\mathrm{S}_n(K) \subseteq \mathrm{D}_n(K) \subseteq \mathrm{GL}_n(K).$$

Bemerkung 2.20. Da eine Diagonalmatrix $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ genau dann invertierbar ist, wenn $\lambda_i \neq 0$ für alle $i = 1, \ldots, n$, ist eine Skalarmatrix $\mathrm{diag}(\lambda, \ldots, \lambda)$ genau dann invertierbar, wenn $\lambda \neq 0$. Bezeichnet $s(\lambda) \in \mathrm{Mat}(n \times n, K)$ die Skalarmatrix mit Diagonaleinträgen $\lambda \in K$, also $s(\lambda) = \mathrm{diag}(\lambda, \ldots, \lambda)$, so zeigen die obigen Rechnungen, dass $s(\lambda) \cdot s(\mu) = s(\lambda \cdot \mu)$ für alle $\lambda, \mu \in K$ und $s(\lambda)^{-1} = s(\lambda^{-1})$ für alle $\lambda \in K$ mit $\lambda \neq 0$. Damit ergibt sich, dass die Abbildung

$$K^\times \to \mathrm{S}_n(K), \quad \lambda \mapsto s(\lambda)$$

ein Gruppenisomorphismus ist. Also ist $\mathrm{S}_n(K) \cong K^\times$.

2.8.4. Die orthogonale Gruppe $\mathrm{O}_n(K)$

Definition 2.21. *Für $A \in \mathrm{Mat}(m \times n, K)$ ist das* Transponierte von A *definiert als die Matrix $A^T \in \mathrm{Mat}(n \times m, K)$ mit $(A^T)_{ij} = A_{ij}$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$. Es ist also*

$$A^T = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \vdots & A_{mn} \end{pmatrix}^T = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{m1} \\ A_{12} & A_{22} & \cdots & A_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{mn} \end{pmatrix}.$$

A^T entsteht also aus A durch Spiegelung der Matrix an der Hauptdiagonalen.

Bemerkung 2.22. 1. Für $A \in \mathrm{Mat}(l \times m, K)$ und $B \in \mathrm{Mat}(m \times n, K)$ ist $(AB)^T = B^T A^T$, da für alle $1 \leq i \leq n$ und $1 \leq j \leq l$

$$(B^T A^T)_{ij} = \sum_{p=1}^{m} (B^T)_{ip} (A^T)_{pj} = \sum_{p=1}^{m} B_{pi} A_{jp} = \sum_{p=1}^{m} A_{jp} B_{pi} = (AB)_{ji} = ((AB)^T)_{ij}.$$

2. Für $S \in \mathrm{GL}_n(K)$ ist auch $S^T \in \mathrm{GL}_n(K)$, mit $(S^T)^{-1} = (S^{-1})^T$, da

$$S^T (S^{-1})^T = (S^{-1} S)^T = I_n^T = I_n \quad \text{und} \quad (S^{-1})^T S^T = (S S^{-1})^T = I_n^T = I_n.$$

Für $n \in \mathbb{N}$, $n \geq 1$ sei

$$\mathrm{O}_n(K) := \{S \in \mathrm{GL}_n(K) \mid S^T S = I_n\} = \{S \in \mathrm{GL}_n(K) \mid S^{-1} = S^T\}.$$

Wir zeigen, dass $\mathrm{O}_n(K) \subseteq \mathrm{GL}_n(K)$ eine Untergruppe ist:

Da $I_n^T I_n = I_n^2 = I_n$ ist $I_n \in \mathrm{O}_n(K)$. Für $S_1, S_2 \in \mathrm{O}_n(K)$ ist $S_1^T S_1 = I_n$ und $S_2^T S_2 = I_n$, also auch

$$(S_1 S_2)^T (S_1 S_2) = S_2^T S_1^T S_1 S_2 = S_2^T I_n S_2 = S_2^T S_2 = I_n$$

und somit $S_1 S_2 \in \mathrm{O}_n(K)$. Ist $S \in \mathrm{O}_n(K)$, so ist $S^T S = I_n$. Durch Multiplikation mit $(S^T)^{-1}$ von links und S^{-1} von rechts ergibt sich daraus, dass

$$\begin{aligned} I_n = I_n^2 &= (S^T)^{-1} S^T S S^{-1} = (S^T)^{-1} (S^T S) S^{-1} \\ &= (S^T)^{-1} I_n S^{-1} = (S^T)^{-1} S^{-1} = (S^{-1})^T S^{-1}. \end{aligned}$$

Somit ist auch $S^{-1} \in \mathrm{O}_n(K)$.

Das zeigt, dass $\mathrm{O}_n(K) \subseteq \mathrm{GL}_n(K)$ eine Untergruppe ist; daher ist $\mathrm{O}_n(K)$ zusammen mit der üblichen Matrixmultiplikation eine Gruppe. Man bezeichnet diese als die *orthogonale Gruppe über K*.

Bemerkung 2.23. 1. Für $S \in \mathrm{O}_n(\mathbb{R})$ ist die Abbildung $D_S \colon \mathbb{R}^n \to \mathbb{R}^n$, $x \mapsto S \cdot x$ linear. Geometrisch gesehen sind die Abbildungen D_S mit $S \in \mathrm{O}_n(\mathbb{R})$ genau die Drehspiegelungen (d.h. Drehungen, Spiegelungen und Kombinationen) des n-dimensionalen Raumes. Die Gruppe $\mathrm{O}_n(\mathbb{R})$ spielt daher eine wichtige Rolle. Man bezeichnet sie als die *orthogonale Gruppe* und schreibt abkürzend $\mathrm{O}(n) \coloneqq \mathrm{O}_n(\mathbb{R})$.

2. Analog zur obigen Rechnung kann man zeigen, dass für eine beliebige quadratische Matrix $B \in \mathrm{Mat}(n \times n, k)$ die Menge

$$\mathrm{O}(B) \coloneqq \{S \in \mathrm{GL}_n(K) \mid S^T B S = B\}$$

eine Untergruppe von $\mathrm{GL}_n(K)$ ist. Die orthogonale Gruppe ergibt sich als der Sonderfall $\mathrm{O}_n(K) = \mathrm{O}(I_n)$.

2.8.5. Die spezielle orthogonale Gruppe $\mathrm{SO}(2)$

Es sei

$$\mathrm{SO}(2) \coloneqq \left\{ \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \,\middle|\, \varphi \in \mathbb{R} \right\}.$$

Wir zeigen, dass $\mathrm{SO}(2)$ mit der üblichen Matrixmultiplikation eine abelsche Gruppe bildet; hierfür nutzen wir die Additionstheoreme des Sinus und Kosinus: Für alle $\varphi, \psi \in \mathbb{R}$ gilt

$$\cos(\varphi + \psi) = \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)$$

und

$$\sin(\varphi + \psi) = \sin(\varphi)\cos(\psi) + \sin(\psi)\cos(\varphi).$$

Wir führen zunächst Notation ein: Für alle $\varphi \in \mathbb{R}$ sei

$$D_\varphi \coloneqq \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

Es ist also $\mathrm{SO}(2) = \{D_\varphi \mid \varphi \in \mathbb{R}\}$. Es ist $I_2 = D_0$ und für alle $\varphi, \psi \in \mathbb{R}$ ist

$$\begin{aligned} D_\varphi D_\psi &= \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} \cos(\psi) & -\sin(\psi) \\ \sin(\psi) & \cos(\psi) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi) & -\sin(\varphi)\cos(\psi) - \sin(\psi)\cos(\varphi) \\ \sin(\varphi)\cos(\psi) + \sin(\psi)\cos(\varphi) & \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\varphi+\psi) & -\sin(\varphi+\psi) \\ \sin(\varphi+\psi) & \cos(\varphi+\psi) \end{pmatrix} = D_{\varphi+\psi}. \end{aligned}$$

Für alle $\varphi \in \mathbb{R}$ ist daher

$$D_\varphi D_{-\varphi} = D_0 = I_2 \quad \text{und} \quad D_{-\varphi} D_\varphi = D_0 = I_2$$

und deshalb, also D_φ invertierbar und $D_\varphi^{-1} = D_{-\varphi}$, also

$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}^{-1} = \begin{pmatrix} \cos(-\varphi) & -\sin(-\varphi) \\ \sin(-\varphi) & \cos(-\varphi) \end{pmatrix} = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

(denn $\sin(-\varphi) = -\sin(\varphi)$ und $\cos(-\varphi) = \cos(\varphi)$).

Wir zeigen zunächst, dass $\mathrm{SO}(2) \subseteq \mathrm{GL}_2(\mathbb{R})$ eine Untergruppe ist: Es ist $I_2 = D_0 \in \mathrm{SO}(2)$. Für $S, T \in \mathrm{SO}(2)$ gibt es $\varphi, \psi \in \mathbb{R}$ mit $S = D_\varphi$ und $T = D_\psi$. Deshalb ist damit auch $ST = D_\varphi D_\psi = D_{\varphi+\psi} \in \mathrm{SO}(2)$. Für $S \in \mathrm{SO}$ gibt es $\varphi \in \mathbb{R}$ mit $S = D_\varphi$, weshalb auch $S^{-1} = D_\varphi^{-1} = D_{-\varphi} \in \mathrm{SO}(2)$.

Das zeigt, dass $\mathrm{SO}(2) \subseteq \mathrm{GL}_2(\mathbb{R})$ eine Untergruppe ist. Deshhalb ist $\mathrm{SO}(2)$ zusammen mit der üblichen Matrixmultiplikation eine Gruppe. Es gilt noch zu zeigen, dass $\mathrm{SO}(2)$ abelsch ist: Sind $S, T \in \mathrm{SO}(2)$ so gibt es $\varphi, \psi \in \mathbb{R}$ mit $S = D_\varphi$ und $T = D_\psi$. Es ist daher

$$ST = D_\varphi D_\psi = D_{\varphi+\psi} = D_{\psi+\varphi} = D_\psi D_\varphi = TS.$$

Insgesamt zeigt dies, dass $\mathrm{SO}(2)$ zusammen mit der üblichen Matrixmultiplikation eine abelsche Gruppe bildet. Man bezeichnet diese als die *spezielle orthogonale Gruppe (von Rang 2)*.

Bemerkung 2.24. Die obige Rechnung lässt sich auch abkürzen: Da $D_\varphi \cdot D_\psi = D_{\varphi+\psi}$ für alle $\varphi, \psi \in \mathbb{R}$ und D_φ für alle $\varphi \in \mathbb{R}$ invertierbar ist, also $D_\varphi \in \mathrm{GL}_2(\mathbb{R})$ für alle $\varphi \in \mathbb{R}$, ist die Abbildung

$$D \colon \mathbb{R} \to \mathrm{GL}_2(\mathbb{R}), \varphi \colon D_\varphi$$

ein wohldefinierter Gruppenhomomorphismus. Folglich ist $\mathrm{SO}(2) = \mathrm{im}(D)$ eine Untergruppe. Da $\mathbb{R}$ abelsch ist, ist es auch $\mathrm{im}(D)$

Bemerkung 2.25. 1. Wie der Name bereits andeutet, ist die spezielle orthogonale Gruppe eine Untergruppe der orthogonalen Gruppe, d.h. $\mathrm{SO}(2) \subseteq \mathrm{O}(2)$. Dies folgt daraus, dass für alle $\varphi \in \mathbb{R}$

$$\begin{aligned} D_\varphi^T D_\varphi &= \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}^T \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \\ &= \begin{pmatrix} \sin(\varphi)^2 + \cos(\varphi)^2 & 0 \\ 0 & \sin(\varphi)^2 + \cos(\varphi)^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2. \end{aligned}$$

2. Für jede Matrix $S \in \mathrm{GL}_n(K)$ ist die Abbildung $M_S \colon \mathbb{R}^2 \to \mathbb{R}^2, x \mapsto S \cdot x$ linear. Ist $S = D_\varphi$, so ist $M_S = M_{D_\varphi}$ die Drehung der Ebene $\mathbb{R}^2$ um den Winkel φ.

2.9. Die abelschen Gruppen $\mathbb{Z}/n\mathbb{Z}$

Wir fixieren ein $n \in \mathbb{N}$ mit $n \geq 1$.

2.9.1. Konstruktion

Definition 2.26. *Eine ganze Zahl $m \in \mathbb{Z}$ ist durch n teilbar, falls es ein $s \in \mathbb{Z}$ mit $m = sn$ gibt. Man schreibt dann $n \mid m$.*

Wir definieren auf $\mathbb{Z}$ eine Äquivalenzrelation durch

$$k \sim l \iff n \mid (k-l) \iff \exists s \in \mathbb{Z} : k - l = sn \iff \exists s \in \mathbb{Z} : k = l + sn$$

Es muss gezeigt werden, dass dies tatsächlich eine Äquivalenzrelation definiert.

Behauptung. *$\sim$ definiert eine Äquivalenzrelation auf $\mathbb{Z}$.*

Beweis. Für jedes $k \in \mathbb{Z}$ ist $k = k + 0 \cdot n$, also $k \sim k$. Das zeigt, dass $\sim$ reflexiv ist.

Sind $k, l \in \mathbb{Z}$ with $k \sim l$, so gibt es ein $s \in \mathbb{Z}$ mit $k = l + sn$. Dann ist $l = k - sn = k + (-s)n$ mit $-s \in \mathbb{Z}$, also auch $l \sim k$. Das zeigt, dass $\sim$ symmetrisch ist.

Sind $k_1, k_2, k_3 \in \mathbb{Z}$ mit $k_1 \sim k_2$ und $k_2 \sim k_3$, so gibt es $s, t \in \mathbb{Z}$ mit $k_1 = k_2 + sn$ und $k_2 = k_3 + tn$. Dann ist

$$k_1 = k_2 + sn = k_3 + tn + sn = k_3 + (t+s)n$$

mit $t + s \in \mathbb{Z}$, also $k_1 \sim k_3$. Das zeigt, dass $\sim$ transitiv ist.

Ingesamt zeigt dies, dass $\sim$ eine Äquivalenzrelation auf $\mathbb{Z}$ ist. □

Für $k \in \mathbb{Z}$ bezeichne im Folgenden

$$[k] = \{l \in \mathbb{Z} \mid k \sim l\}$$

die Äquivalenzklasse von $\mathbb{Z}$. Außerdem sei

$$\mathbb{Z}/n\mathbb{Z} \coloneqq \mathbb{Z}/\sim = \{[k] \mid k \in \mathbb{Z}\}$$

die Menge der Äquivalenzklassen. Wir definieren auf $\mathbb{Z}/n\mathbb{Z}$ eine binäre Verknüpfung durch

$$[k] + [l] = [k + l] \quad \text{für alle } k, l \in \mathbb{Z}. \tag{2.1}$$

Wir müssen zeigen, dass diese Verknüpfung wohldefiniert ist, d.h. nicht von den Repräsentanten k und l der Äquivalenzklassen $[k]$ und $[l]$ abhängt.

Behauptung. *Die Verknüpfung in (2.1) ist wohldefiniert.*

Beweis. Es seien $k_1, k_2, l_1, l_2 \in \mathbb{Z}$ with $k_1 \sim k_2$ und $l_1 \sim l_2$. Es muss gezeigt werden, dass $[k_1 + l_1] = [k_2 + l_2]$, also $k_1 + l_1 \sim k_2 + l_2$

Da $k_1 \sim k_2$ und $l_1 \sim l_2$ gibt es $s, t \in \mathbb{Z}$ with $k_1 = k_2 + sn$ und $l_1 = l_2 + tn$. Damit ist

$$k_1 + l_1 = k_2 + sn + l_2 + tn = k_2 + l_2 + (s+t)n,$$

also auch $k_1 + l_1 \sim k_2 + l_2$. □

Wir zeigen nun, dass $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der in (2.1) definierten binären Verknüpfung eine abelsche Gruppe bildet:

Für alle $k_1, k_2, k_3 \in \mathbb{Z}$ ist

$$([k_1]+[k_2])+[k_3] = [k_1+k_2]+[k_3] = [k_1+k_2+k_3] = [k_1]+[k_2+k_3] = [k_1]+([k_2]+[k_3]),$$

also ist die Verknüpfung assoziativ. Für alle $k, l \in \mathbb{Z}$ ist

$$[k] + [l] = [k + l] = [l + k] = [l] + [k],$$

also ist die Verknüpfung komutativ. Für jedes $k \in \mathbb{Z}$ ist

$$[0] + [k] = [0 + k] = [k],$$

also ist $[0]$ das neutrale Element bezüglich $+$. Für jedes $k \in \mathbb{Z}$ ist

$$[k] + [-k] = [k + (-k)] = [k - k] = [0],$$

also ist $[-k]$ invers zu $[k]$ bezüglich $+$. Ingesamt zeigt dies, dass $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der Addition $+$ aus (2.1) eine abelsche Gruppe bildet.

Bemerkung 2.27. Für alle $n \in \mathbb{Z}$ ist $n \cdot [k] = [n \cdot k]$ für alle $k \in \mathbb{Z}$: Für $n \geq 0$ ist nämlich

$$n \cdot [k] = \sum_{i=1}^{n} [k] = \left[\sum_{i=1}^{n} k\right] = [n \cdot k],$$

und für $n \leq 0$ ist somit

$$n \cdot [k] = -((-n) \cdot [k]) = -[(-n) \cdot k] = [-(-n) \cdot k] = [n \cdot k].$$

2.9.2. Erklärung

Wir wollen noch eine bessere Erklärung dafür geben, wie $\mathbb{Z}/n\mathbb{Z}$ aussieht und sich die Addition verhält.

Zunächst bemerken wir, dass für jedes $k \in \mathbb{Z}$

$$\begin{aligned}[k] &= \{l \in \mathbb{Z} \mid k \sim l\} = \{l \in \mathbb{Z} \mid \exists s \in \mathbb{Z} : l = k + ns\} \\ &= \{k + ns \mid s \in \mathbb{Z}\} = k + \{ns \mid s \in \mathbb{Z}\} = k + n\mathbb{Z}.\end{aligned}$$

Beispiel(e). a) Es sei $n = 2$. Dann ist $[0] = 2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ die Menge der ganzen Zahlen und $[1] = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$ die Menge der ungeraden Zahlen. Dies sind die einzigen beiden Äquivalenzklassen (da jede ganze Zahl in genau einer der beiden Äquivalenzklassen enthalten ist). Also ist

$$\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$$

und die Addition ist gegeben durch $[0] + [0] = [0]$, $[0] + [1] = [1] + [0] = [1]$ sowie $[1] + [1] = [2] = [0]$.

b) Es sei $n = 3$. Dann ist

$$\begin{aligned}[0] &= 0 + 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\} \\ [1] &= 1 + 3\mathbb{Z} = \{\dots, -5, -2, 1, 4, 7, \dots\} \\ [2] &= 2 + 3\mathbb{Z} = \{\dots, -4, -1, 2, 5, 8, \dots\}.\end{aligned}$$

Da jede ganze Zahl in genau einer dieser Äquivalenzklassen enthalten ist, ist

$$\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}.$$

Die Addition ist gegeben durch $[0] + [k] = [k] + [0] = [k]$ für alle $k \in \{0, 1, 2\}$, sowie $[1] + [1] = [2]$, $[1] + [2] = [2] + [1] = [3] = [0]$ und $[2] + [2] = [4] = [1]$.

Im Allgemeinen gilt, dass

$$\begin{aligned}[0] &= 0 + n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}, \\ [1] &= 1 + n\mathbb{Z} = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}, \\ [2] &= 2 + n\mathbb{Z} = \{\dots, -2n+2, -n+2, 2, n+2, 2n+2, \dots\}, \\ &\vdots \\ [n-1] &= (n-1) + n\mathbb{Z} = \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}.\end{aligned}$$

Da jede ganze Zahl in genau einer dieser Äquivalenzklassen vorkommt, ist

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

mit $[k] \neq [l]$ für alle $0 \leq k \neq l \leq n-1$, und die Addition ist gegeben durch

$$[k] + [l] = [(k + l) \bmod n] \quad \text{für alle } 0 \leq k, l \leq n-1.$$

Wir identifiziert daher für gewöhnlich die Repräsentanten $0, \dots, n-1$ mit den entsprechenden Äquivalenzklassen $[0], \dots, [n-1]$. Es ist also $\mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$, und bezeichnet $+$ die Addition auf $\mathbb{Z}$ und $\tilde{+}$ die Addition auf $\mathbb{Z}/n\mathbb{Z}$, so ist $k \tilde{+} l = (k + l) \bmod n$.

Bemerkung 2.28. In 2.2 haben wir bereits gesehen, dass jede zweielementige Gruppe eindeutig isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist. Allgemeiner lässt sich für jede Primzahl $p > 0$ zeigen, dass jede p-elementige Gruppe isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist (allerdings nicht eindeutig isomorph — zwischen zwei p-elementigen Gruppen gibt es genau $p - 1$ Gruppenisomorphismen).

2.10. Ausblick: Quotienten abelscher Gruppen

Als ein weiteres (abstraktes) Beispiel geben wir eine Verallgemeinerung der Konstruktion von $\mathbb{Z}/n\mathbb{Z}$ an, die für eine beliebige abelsche Gruppe A und Untergruppe $H \subseteq A$ eine *Quotientengruppe* A/H liefert.

Wir definieren auf A eine Äquivalenzrelation durch

$$x \sim y \iff x - y \in H.$$

Es muss zunächst gezeigt werden, dass dies tatsächlich eine Äquivalenzrelation definiert:

Für alle $x \in A$ ist $x - x = 0 \in H$, da H eine Untergruppe ist, also $x \sim x$, was die Reflexivität zeigt.

Für $x, y \in A$ mit $x \sim y$ ist $x - y \in H$. Da H eine Untergruppe ist, ist damit auch $y - x = -(x - y) \in H$, also $y \sim x$. Das zeigt die Symmetrie von $\sim$.

Sind $x, y, z \in A$ mit $x \sim y$ und $y \sim z$, so ist $x - y \in H$ und $y - z \in H$. Da H eine Untergruppe ist, ist damit auch $x - z = (x - y) + (y - z) \in H$, also $x \sim z$. Das zeigt die Transitivität von $\sim$.

Ingesamt zeigt dies, dass $\sim$ eine Äquivalenzrelation auf A definiert. Wir schreiben

$$A/H \coloneqq \{[x] \mid x \in A\}$$

für die Menge der Äquivalenzklassen.

Wir definieren auf A/H eine Verknüpfung durch

$$[x] + [y] = [x + y].$$

Wir müssen überprüfen, dass diese Verknüpfung wohldefiniert ist: Es seien $x, x', y, y' \in A$ mit $x \sim x'$ und $y \sim y'$. Dann ist $x - x' \in H$ und $y - y' \in H$. Da H eine Untergruppe ist, ist auch

$$(x + y) - (x' + y') = (x - x') + (y - y') \in H,$$

also $x + y \sim x' + y'$. Das zeigt die Wohldefiniertheit.

Wir zeigen, dass A/H zusammen mit $+$ eine abelsche Gruppe bildet: Die Assoziativität folgt daraus, dass für alle $x, y, z \in A$

$$[x] + ([y] + [z]) = [x] + [y + z] = [x + y + z] = [x + y] + [z] = ([x] + [y]) + [z].$$

Die Kommutativität ergibt sich daraus, dass für alle $x, y \in A$

$$[x] + [y] = [x + y] = [y + x] = [y] + [x].$$

Für die Äquivalenzklasse von 0 gilt für alle $x \in A$, dass

$$[0] + [x] = [0 + x] = [x] = [x + 0] = [x] + [0],$$

weshalb $[0]$ neutral bezüglich $+$ ist. Für jedes $x \in A$ ist

$$[x] + [-x] = [x - x] = [0] = [x - x] = [-x] + [x],$$

weshalb $[-x]$ invers zu $[x]$ bezüglich $+$ ist. Ingesamt zeigt dies, dass $(A/H, +)$ eine abelsche Gruppe ist.

Bemerkung 2.29. 1. Für $A = \mathbb{Z}$ und $H = n\mathbb{Z}$ ergibt sich die bereits bekannte Konstruktion von $\mathbb{Z}/n\mathbb{Z}$.

2. Die Äquivalenzklasse von $x \in A$ ist gegeben durch

$$\begin{aligned}[x] = \{y \in A \mid y - x \in H\} &= \{y \in A \mid y = x + h \text{ ein } h \in H\} \\ &= \{x + h \mid h \in H\} = x + \{h \mid h \in H\} = x + H.\end{aligned}$$

3. Die Addition lässt sich alternativ auch wie folgt definieren: Für beliebige Teilmengen $R, S \subseteq A$ sei
$$R + S = \{r + s \mid r \in R, s \in S\}.$$
Für alle $x, y \in A$ ist dann
$$\begin{aligned}[x] + [y] &= (x + H) + (y + H) = \{x + h \mid h \in H\} + \{y + h' \mid h' \in H\} \\ &= \{x + h + y + h' \mid h, h' \in H\} = \{(x + y) + (h + h') \mid h, h' \in H\} \\ &= \{(x + y) + h'' \mid h'' \in H\} = (x + y) + H = [x + y].\end{aligned}$$
Diese Definition der Addition hat den Vorteil, dass es keine Wohldefiniertheit zu überprüfen gilt.

2.11. Das Zentrum einer Gruppe

Definition 2.30. *Das* Zentrum *einer Gruppe G ist*
$$Z(G) \coloneqq \{g \in G \mid gh = hg \text{ für alle } h \in G\}.$$

Es sei G eine Gruppe. Wir zeigen, dass $Z(G)$ eine Untergruppe ist: Da $1 \cdot g = g = g \cdot 1$ für alle $g \in G$ ist $1 \in Z(G)$. Sind $g_1, g_2 \in G$, so ist
$$g_1 g_2 h = g_1 h g_2 = h g_1 g_2 \quad \text{für alle } h \in G,$$
und somit auch $g_1 g_2 \in Z(G)$. Ist $g \in Z(G)$, so ist
$$g^{-1} h = g^{-1} h g g^{-1} = g^{-1} g h g^{-1} = h g^{-1} \quad \text{für alle } h \in G,$$
und somit auch $g^{-1} \in Z(G)$. Insgesamt zeigt dies, dass $Z(G)$ eine Untergruppe ist.

Beispiel(e). 1. Eine Gruppe G ist genau dann abelsch, wenn $Z(G) = G$.

2. Es lässt sich zeigen, dass $Z(\mathrm{GL}_n(K)) = \mathrm{S}_n(K)$ genau die Untergruppe der Skalarmatrizen ist.

3. Da die symmetrischen Gruppen S_1 und S_2 sind abelsch ist $Z(S_1) = S_1$ und $Z(S_2) = S_2$. Für $n \geq 3$ ist S_n nicht abelsch, also $Z(S_n) \subsetneq S_n$. Es lässt sich allgemeiner zeigen, dass bereits $Z(S_n) = \{1\}$ für alle $n \geq 3$:

   Angenommen, es ist $\sigma \in Z(S_n)$ mit $\sigma \neq 1 = \mathrm{id}_{\{1,\dots,n\}}$. Dann gibt es ein $k \in \{1, \dots, n\}$ mit $\sigma(k) \neq k$. Da $n \geq 3$ gibt es ein $l \in \{1, \dots, n\}$ mit $k_0 \notin \{k, \sigma(k)\}$. Die drei Element k, $\sigma(k)$ und k_0 sind also paarweise verschieden. Es sei $\tau \in S_n$ definiert als
$$\tau(l) \coloneqq \begin{cases} k_0 & \text{für } l = \sigma(k), \\ \sigma(k) & \text{für } l = k_0, \\ l & \text{sonst.} \end{cases}$$

τ vertauscht also die beiden Elemente k_0 und $\sigma(k)$ und lässt alle anderen Element unverändert; insbesondere ist $\tau(k) = k$ Es gilt nun

$$\tau(\sigma(k)) = k_0 \neq \sigma(k) = \sigma(\tau(k)),$$

also ist $\tau \circ \sigma \neq \sigma \circ \tau$. Deshalb ist $\sigma \notin Z(S_n)$.

4. Allgemeiner lässt sich für eine beliebige Teilmenge $X \subseteq G$ einer Gruppe G der *Zentralisator* $Z_G(X) := \{g \in G \mid gh = hg \text{ für alle } h \in X\}$ betrachten; dies ist stets eine Untergruppe von G. Das Zentrum ergibt sich dann als Sonderfall für $X = G$, also $Z(G) = Z_G(G)$.

2.12. Automorphismengruppen

2.12.1. Automorphismengruppe einer Gruppe

Definition 2.31. *Ist G ein Gruppe, so heißt*

$$\mathrm{Aut}(G) := \{\varphi \colon G \to G \mid \varphi \textit{ ist ein Gruppenautomorphismus}\}$$

die Automorphismengruppe von G.

Es sei G eine Gruppe. Wir zeigen, dass $\mathrm{Aut}(G)$ zusammen mit der Funktionskomposition eine Gruppe bildet, indem wir zeigen, dass $\mathrm{Aut}(G) \subseteq S(G)$ eine Untergruppe ist. Dass $\mathrm{Aut}(G) \subseteq S(G)$ eine Teilmenge ist, folgt direkt daraus, dass Gruppenautomorphismen bijektiv sind.

Da die Identität $\mathrm{id}_G \colon G \to G$ ein Gruppenautomorphismus ist, ist $\mathrm{id}_G \in \mathrm{Aut}(G)$. Sind $\varphi, \psi \in \mathrm{Aut}(G)$, also φ und ψ bijektiv und Gruppenhomomorphismen, so ist auch die Verknüpfung $\varphi \circ \psi \colon G \to G$ bijektiv und ein Gruppenhomomorphismus, also $\varphi \circ \psi$ ein Gruppenautomorphismus, und somit $\varphi \circ \psi \in \mathrm{Aut}(G)$. Ist $\varphi \in \mathrm{Aut}(G)$, also $\varphi \colon G \to G$ ein Gruppenisomorphismus, so ist auch $\varphi^{-1} \colon G \to G$ ein Gruppenisomorphismus, und somit $\varphi^{-1} \in \mathrm{Aut}(G)$.

Ingesamt zeigt dies, dass $\mathrm{Aut}(G) \subset S(G)$ eine Untergruppe ist.

Beispiel(e). Ist G eine zweielementige Gruppe, so gibt es einen eindeutigen Isomorphismus $G \to G$; dieser ist notwendigerweise die Identität id_G. Also ist $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$ die triviale Gruppe.

Beispiel(e). Wir bestimmen $\mathrm{Aut}(\mathbb{Z})$. Wir wissen bereits, dass $\mathrm{id}_{\mathbb{Z}} \colon \mathbb{Z} \to \mathbb{Z}$ ein Gruppenautomorphismus ist. Auch $i \colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto -n$ ist ein Gruppenautomorphismus; da $i^2 = \mathrm{id}_{\mathbb{Z}}$ ist i bijektiv mit $i^{-1} = i$, und da

$$i(x + y) = -(x + y) = (-x) + (-y) = i(x) + i(y) \quad \text{für alle } x, y \in \mathbb{Z}$$

ist i ein Gruppenhomomorphismus.

Es sei nun $\varphi \colon \mathbb{Z} \to \mathbb{Z}$ ein beliebiger Gruppenhomomorphismus und $m := \varphi(n)$. Für alle $n \in \mathbb{Z}$ ist dann

$$\varphi(n) = \varphi(n \cdot 1) = n \cdot \varphi(1) = n \cdot m,$$

also ist φ durch Multiplikation mit m gegeben. Inbesonder ist deshalb $\operatorname{im}(\varphi) = n\mathbb{Z}$. Damit φ surjektiv ist, muss also $m \in \{1, +1\}$. Ist $m = 1$, so zeigt die obige Rechnung, dass $\varphi = \mathrm{id}_{\mathbb{Z}}$. Ist $m = -1$, so zeigt die obige Rechnung, dass $\varphi = i$.

Das zeigt, dass $\mathrm{id}_{\mathbb{Z}}$ und i die einzigen surjektiven Gruppenhomomorphismen $\mathbb{Z} \to \mathbb{Z}$ sind. Inbesondere sind damit $\mathrm{id}_{\mathbb{Z}}$ und i die einzigen Gruppenautomorphismen von $\mathbb{Z}$. Also ist $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}_{\mathbb{Z}}, i\}$ mit $i^2 = \mathrm{id}_{\mathbb{Z}}$. Es handelt sich bei $\mathrm{Aut}(\mathbb{Z})$ also um die zweielementige Gruppe.

Beispiel(e). Es sei $p > 0$. Wir untersuchen die Automorphismengruppe von $\mathbb{Z}/p\mathbb{Z}$. Hierfür klassifizieren wir zunächst alle Gruppenendomorphismen $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Für jedes $m \in \{0, 1, \dots, p-1\} \subseteq \mathbb{N}$ sei $\varphi_m \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $x \mapsto m \cdot x$. Für jedes $m \in \{0, \dots, p-1\}$ ist φ_m ein Gruppenhomomorphismus, da

$$\begin{aligned}\varphi_m([k] + [l]) &= m \cdot [k + l] = [m \cdot (k + l)] = [m \cdot k + m \cdot l] \\ &= [m \cdot k] + [m \cdot l] = m \cdot [k] + m \cdot [l] = \varphi_m([k]) + \varphi_m([l])\end{aligned}$$

für alle $k, l \in \mathbb{Z}$. (Siehe Bemerkung 2.27 für die entsprechenden Rechenregeln.) Sind außerdem $m_1, m_2 \in \{0, \dots, p-1\}$ mit $\varphi_{m_1} = \varphi_{m_2}$, so ist

$$[m_1] = m_1 \cdot [1] = \varphi_{m_1}([1]) = \varphi_{m_2}([1]) = m_2 \cdot [1] = [m_2]$$

und deshalb $m_1 = m_2$. Also sind die Gruppenhomomorphismen $\varphi_0, \dots, \varphi_m$ paarweise verschieden.

Ist $\psi \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ ein Gruppenhomomorphismus und $m \in \{0, \dots, p-1\} \subseteq \mathbb{N}$ mit $\psi([1]) = [m]$, so ist für alle $k \in \{0, \dots, p-1\}$

$$\psi([k]) = \psi(k \cdot [1]) = k \cdot \psi([1]) = k \cdot [m] = [k \cdot m] = [m \cdot k] = m \cdot [k] = \varphi_m([k]).$$

Also ist $\psi = \varphi_m$.

Die Abbildung

$$\begin{aligned}\{0, \dots, p-1\} &\to \{\psi \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \mid \psi \text{ ist ein Gruppenhomomorphismus}\}, \\ m &\mapsto \varphi_m\end{aligned}$$

ist nach den obigen Diskussionen sowohl injektiv als auch surjektiv, also eine Bijektion. Es gilt also zu bestimmen, für welche $m \in \{0, \dots, m-1\}$ der Gruppenhomomorphismus φ_m bijektiv ist.

Da $\varphi_0([k]) = 0 \cdot [k] = 0$ für alle $k \in \mathbb{Z}$ ist φ_0 weder injektiv noch surjektiv und somit nicht invertierbar. Ist $m \in \{1, \dots, p-1\}$, so sind m und p teilerfremd. Deshalb gibt es dann $a, b \in \mathbb{Z}$ mit $am + bp = 1$. Somit ist

$$\varphi_m([a]) = m \cdot [a] = [m \cdot a] = [am + bp] = [1].$$

Für alle $k \in \{0, \dots, p-1\}$ ist deshalb

$$\varphi_m([ka]) = m \cdot [ka] = [mka] = k[m \cdot a] = k \cdot [1] = [k].$$

Also ist φ_m injektiv. Da $\mathbb{Z}/p\mathbb{Z}$ endlich ist, ist φ_m damit bereits bijektiv.

Damit haben wir gezeigt, dass

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) = \{\varphi_m \mid \{1, \dots, p-1\}\},$$

wobei die Gruppenautomorphismen φ_m mit $m \in \{1, \dots, p-1\}$ paarweis verschieden sind und $\varphi_1 = \mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$. Es lässt sich zeigen, dass $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ bereits isomorph zu $\mathbb{Z}/(p-1)\mathbb{Z}$ ist.

2.12.2. Automorphismengruppen von Körpern

Definition 2.32. *Ist K ein Körper, so heißt*

$$\mathrm{Aut}(K) = \{\phi\colon K \to K \mid \phi \textit{ ist ein Körperautomorphismus}\}$$

die Automorphismengruppen von K.

Es sei K ein Körper. Wir zeigen, dass $\mathrm{Aut}(K)$ eine Gruppe bezüglich der Funktionskomposition $\circ$ ist, indem wir zeigen, dass $\mathrm{Aut}(K) \subseteq S(K)$ eine Untergruppe bildet. Dass $\mathrm{Aut}(K) \subseteq S(K)$ ein Teilmenge ist, folgt direkt daraus, dass Körperautomorphismen bijektiv sind.

Die Identität $\mathrm{id}_K\colon K \to K$ ist ein Körperautomorphismus, also ist $\mathrm{id}_K \in \mathrm{Aut}(K)$.

Sind $\phi, \psi \in \mathrm{Aut}(K)$ zwei Körperautomorphismen, so sind ϕ und ψ bijektive Körperhomomorphismen. Damit ist auch die Verknüpfung $\phi \circ \psi\colon K \to K$ ein bijektiver Körperhomomorphismus, also ein Körperautomorphismus. Deshalb ist auch $\phi \circ \psi \in \mathrm{Aut}(K)$.

Ist $\phi \in \mathrm{Aut}(K)$ ein Körperautomorphismus, so ist ϕ ein bijektiver Körperhomomorphismus. Deshalb ist auch $\phi^{-1}\colon K \to K$ ein bijektiver Körperhomomorphismus, und somit ϕ^{-1} ein Körperautomorphismus. Also ist auch $\phi^{-1} \in \mathrm{Aut}(K)$

Ingesamt zeigt dies, dass $\mathrm{Aut}(K)$ ein Untergruppe von $S(X)$ ist.

Beispiel(e). 1. Wir bestimmen $\mathrm{Aut}(\mathbb{Q})$. Hierfür überlegen wir uns zunächst, dass ein Körperhomomorphismus $\phi\colon \mathbb{Q} \to \mathbb{Q}$ bereits eindeutig dadurch bestimmt ist, dass $\phi(1) = 1$. Für alle natürlichen Zahlen $n \in \mathbb{N}$ ist deshalb nämlich schon

$$\phi(n) = \phi\left(\sum_{i=1}^{n} 1\right) = \sum_{i=1}^{n} \phi(1) = \sum_{i=1}^{n} 1 = n.$$

Ist $n \in \mathbb{Z}$ mit $n \leq 0$, so ist $-n \geq 0$ und deshalb

$$\phi(n) = \phi(-(-n)) = -\phi(-n) = -(-n) = n.$$

Also ist bereits $\phi(n) = n$ für alle $n \in \mathbb{Z}$. Sind $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ mid $q \neq 0$ so ist damit sogar schon $\phi(p/q) = p/q$, da

$$q \cdot \phi\left(\frac{p}{q}\right) = \sum_{i=1}^{q} \phi\left(\frac{p}{q}\right) = \phi\left(\sum_{i=1}^{q} \frac{p}{q}\right) = \phi\left(q \cdot \frac{p}{q}\right) = \phi(p) = p.$$

Damit haben wir gezeigt, dass berets $\phi(x) = x$ für alle $x \in \mathbb{Q}$. Also ist $\phi = \mathrm{id}_{\mathbb{Q}}$.

Die Identität $\mathrm{id}_{\mathbb{Q}}$ ist also der einzige Körperhomomorphismus $\mathbb{Q} \to \mathbb{Q}$, inbesondere also der einzige Körperautomorphismus. Somit ist $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$.

2. Analog zur obigen Rechnung ergibt sich, dass für jeden Körper K mit $\operatorname{char}(K) = 0$ und Körperhomomorphismus $\phi\colon \mathbb{Q} \to K$ gilt, dass

$$\phi\left(\frac{p}{q}\right) = \frac{p \cdot 1_K}{q \cdot 1_K} \quad \text{für alle } p \in \mathbb{Z} \text{ und } q \in \mathbb{N} \text{ mit } q \neq 0.$$

Die Bedingung, dass $\operatorname{char}(K) = 0$ wird hier benötigt, damit $q \cdot 1_K \neq 0$ für alle $q \in \mathbb{N}$ mit $q > 0$.

3. Wie in 3.6.1 gezeigt wird, ist $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ ein Unterkörper. Wir bestimmen $\operatorname{Aut}(\mathbb{Q}[i])$.

Zunächst bemerken wir, dass es neben der Identität $\mathrm{id}_{\mathbb{Q}[i]}\colon \mathbb{Q}[i] \to \mathbb{Q}[i]$ noch einen weiteren Körperautomorphismus $\mathbb{Q}[i]$ gibt: Für die komplexe Konjugation gilt nämlich, dass $\overline{1} = 1$, $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$ für alle $z, w \in \mathbb{C}$, und somit inbesondere für alle $z, w \in \mathbb{Q}[i]$. Ist $z \in \mathbb{Q}[i]$, also $z = a + bi$ mit $a, b \in \mathbb{Q}$, so ist auch $\overline{z} = a - bi \in \mathbb{Q}[i]$. Also ergibt such durch die Einschränkung der komplexen Konjugation auf $\mathbb{Q}[i]$ in Körperhomomorphismus

$$k\colon \mathbb{Q}[i] \to \mathbb{Q}[i], \quad z \mapsto \overline{z}.$$

Da $k(k(z)) = k(\overline{z}) = \overline{(\overline{z})} = z$ für alle $z \in \mathbb{Q}[i]$ ist $k \circ k = \mathrm{id}_{\mathbb{Q}[i]}$, also k bijektiv mit $k^{-1} = k$. Also ist k ein Körperautomorphismus.

Die Identitat $\mathrm{id}_{\mathbb{Q}[i]}$ und die komplexe Konjugation k sind tatsächlich schon die einzigen Körperautomorphismen von $\mathbb{Q}[i]$: Um dies zu zeigen, sei $\phi\colon \mathbb{Q}[i] \to \mathbb{Q}[i]$ ein Körperhomomorphismus. Wie bereits oben bemerkt ist $\phi(a) = a$ für alle $a \in \mathbb{Q}$. Da $i^2 = -1$ ist daher

$$\phi(i)^2 = \phi(i^2) = \phi(-1) = -1.$$

Also muss $\phi(i) = i$ oder $\phi(i) = -i$. Im Falle von $\phi(i) = i$ ist

$$\phi(a + bi) = \phi(a) + \phi(b)\phi(i) = a + bi \quad \text{für alle } a, b \in \mathbb{Q},$$

also $\phi(z) = z$ für alle $z \in \mathbb{Q}[i]$ und somit $\phi = \mathrm{id}_{\mathbb{Q}[i]}$. Ist andererseits $\phi(i) = -i$, so ist

$$\phi(a + bi) = \phi(a) + \phi(b)\phi(i) = a + b(-i) = a - bi = k(a + bi) \quad \text{für alle } a, b \in \mathbb{Q},$$

also $\phi(z) = k(z)$ für alle $z \in \mathbb{Q}[i]$ und somit $\phi = k$.

Also sind ϕ und k die einzigen Körperhomomorphismen $\mathbb{Q}[i] \to \mathbb{Q}[i]$, und somit insbesondere die einzigen Körperautomorphismen. Somit ist $\operatorname{Aut}(\mathbb{Q}[i]) = \{\mathrm{id}_{\mathbb{Q}[i]}, k\}$ mit $k^2 = \mathrm{id}_{\mathbb{Q}[i]}$ die zweielementige Gruppe.

4. Mithilfe von analytischer Methoden lässt sich zeigen, dass $\operatorname{Aut}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$. Es ergibt sich nämlich, dass ein Körperisomorphismus $\phi\colon \mathbb{R} \to \mathbb{R}$ bereits stetig ist, und da $\phi(x) = x$ für alle $x \in \mathbb{Q}$ ergibt sich damit, dass bereits $\phi(x) = x$ für alle $x \in \mathbb{R}$.

2.12.3. Automorphismengruppen von Vektorräumen

Definition 2.33. *Für einen K-Vektorraum V ist*

$$\mathrm{Aut}_K(V) \coloneqq \{f\colon V \to V \mid f \text{ ist ein (K-linearer) Automorphismus}\}$$

die Automorphismengruppe *von V.*

Bemerkung 2.34. 1. Für einen K-Vektorraum V schreibt man auch $\mathrm{GL}_K(V)$ statt $\mathrm{Aut}_K(V)$.

2. Ist klar, über welchem Körper K man sich bewegt, schreibt man auch nur $\mathrm{Aut}(V)$ statt $\mathrm{Aut}_K(V)$, bzw. $\mathrm{GL}(V)$ statt $\mathrm{GL}_K(V)$.

Es sei V ein K-Vektorraum. Wir zeigen, dass $\mathrm{Aut}_K(V)$ zusammen mit der Funktionskomposition eine Gruppe bildet, indem wir zeigen, dass $\mathrm{Aut}_K(V) \subseteq S(V)$ eine Untergruppe bildet. Dass $\mathrm{Aut}_K(V) \subseteq S(V)$ eine Teilmenge ist, folgt dabei direkt daraus, dass Automorphismen bijektiv sind.

Die Identität $\mathrm{id}_V\colon V \to V$ ist ein Automorphismus, also ist $\mathrm{id}_V \in \mathrm{Aut}_K(V)$.

Sind $f, g \in \mathrm{Aut}(V)$ Automorphismen, so sind f und g bijektiv und K-linear. Also ist auch die Verknüpfung $f \circ g\colon V \to V$ bijektiv und K-linear, und somit $f \circ g$ ein Automorphismus. Also ist auch $f \circ g \in \mathrm{Aut}_K(V)$.

Ist $f \in \mathrm{Aut}(V)$ ein Automorphismus, so ist f bijektiv und K-linear. Deshalb ist auch $f^{-1}\colon V \to V$ bijektiv und K-linear, also ein Automorphismus. Also ist auch $f^{-1} \in \mathrm{Aut}(V)$.

Ingesamt zeigt dies, dass $\mathrm{Aut}_K(V) \subseteq S(V)$ eine Untergruppe ist.

2.12.4. Automorphismengruppen geordneter Mengen

2.12.5. Automorphismengruppe eines Graphen

2.12.6. Innere Automorphismen einer Gruppe

Definition 2.35. *Es sei G eine Gruppe. Für $\alpha \in G$ sei*

$$c_\alpha\colon G \to G, \quad g \mapsto \alpha g \alpha^{-1},$$

und es sei

$$\mathrm{Int}(G) = \{c_\alpha \mid \alpha \in G\}.$$

Es sei G eine Gruppe. Wir zeigen, dass c_α für alle $\alpha \in G$ ein Gruppenautomorphismus von G ist, und dass $\mathrm{Int}(G)$ eine Untergruppe von G ist.

Es sei $\alpha \in G$. Für alle $g \in G$ ist

$$(c_\alpha \circ c_{\alpha^{-1}})(g) = c_\alpha(c_{\alpha^{-1}}(g)) = c_\alpha(\alpha^{-1} g \alpha) = \alpha\alpha^{-1} g \alpha\alpha^{-1} = 1 \cdot g \cdot 1 = g,$$

also $c_\alpha \circ c_{\alpha^{-1}} = \mathrm{id}_G$. Deshalb ist auch $c_{\alpha^{-1}} \circ c_\alpha = c_{\alpha^{-1}} \circ c_{(\alpha^{-1})^{-1}} = \mathrm{id}_G$. Als ist c_α bijektiv mit $c_\alpha^{-1} = c_{\alpha^{-1}}$. Für alle $g, h \in G$ ist

$$c_\alpha(gh) = \alpha g h \alpha^{-1} = \alpha g \alpha^{-1} \alpha h \alpha^{-1} = c_\alpha(g) c_\alpha(h),$$

also ist c_α ein Gruppenhomomorphismus. Zusammen zeigt dies, dass c_α ein Gruppenautomorphismus ist. Das zeigt bereits, dass $\mathrm{Int}(G) \subseteq \mathrm{Aut}(G)$ eine Teilmenge ist.

Für alle $g \in G$ ist $c_1(g) = 1 \cdot g \cdot 1^{-1} = g$, also ist $\mathrm{id}_G = c_1 \in \mathrm{Int}(G)$. Für $\alpha, \beta \in G$ ist für alle $g \in G$

$$(c_\alpha \circ c_\beta)(g) = c_\alpha(c_\beta(g)) = \alpha\beta g\beta^{-1}\alpha^{-1} = (\alpha\beta)g(\alpha\beta)^{-1} = c_{\alpha\beta}(g),$$

also ist $c_\alpha \circ c_\beta \in \mathrm{Int}(G)$. Außerdem ist $c_\alpha^{-1} = c_{\alpha^{-1}} \in \mathrm{Int}(G)$ für alle $\alpha \in G$. Ingesamt zeigt dies, dass $\mathrm{Int}(G) \subseteq \mathrm{Aut}(G)$ bereits eine Untergruppe ist.

Man bezeichnet die Elemente von $\mathrm{Int}(G)$ als die *innere Automorphismen* und $\mathrm{Int}(G)$ als die *Gruppe der inneren Automorphismen.*

Bemerkung 2.36. Die obigen Rechnungen lassen sich auch umgehen: Da $c_\alpha \circ c_\beta = c_{\alpha\beta}$ für alle $\alpha\beta$ ist die Abbildung $c\colon G \to \mathrm{Aut}(G)$, $\alpha \mapsto c_\alpha$ ein Gruppenhomomorphismus. Also ist $\mathrm{Aut}(G) = \mathrm{im}(c)$ eine Untergruppe.

Auch $\ker(c) \subseteq G$ ist eine Untergruppe. Das $\alpha \in \ker(c)$ bedeutet, dass $c_\alpha = \mathrm{id}_G$, also $g = c_\alpha(g) = \alpha g \alpha^{-1}$ für alle $g \in G$. Dies ist äquivalent dazu, dass $g\alpha = \alpha g$ für alle $g \in G$, also $\alpha \in Z(G)$. Also ist $\ker(c) = Z(G)$.

2.13. Einheitengruppen

2.13.1. Einheitengruppe eines Monoids

Definition 2.37. *Ein* Monoid *ist ein Tupel $(M, \cdot)$ bestehend aus einer Menge M und einer binären Verknüpfung $\cdot\colon M \times M \to M$, die die folgenden Bedingungen erfüllt:*

i) Die Verknüpfung $\cdot$ ist assoziativ, d.h. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in M$.

ii) Es gibt ein neutrales Element $e \in M$ bezüglich $\cdot$, d.h. $m \cdot e = e \cdot m$ für alle $m \in M$.

Bemerkung 2.38.

1. Der Unterschied zwischen der Definition eines Monoids und der Definition einer Gruppe besteht darin, dass in einem Monoid nicht jedes Element ein Inverses besitzen muss. Inbesondere ist jede Gruppe ein Monoid.
2. Die Verknüpfung eines Monoids wird häufig nicht explizit genannt, d.h. statt von einem Monoid $(M, \cdot)$ spricht man von einem Monoid M.
3. Das neutrale Element eines Monoids ist eindeutig, d.h. ist M ein Monoid und sind $e, e' \in M$ neutrale Elemente, dann ist $e = e \cdot e' = e'$. Man spricht daher auch von *dem* neutralen Element von M.
4. Das neutrale Element eines Monoids wird auch als 1 geschrieben.

Definition 2.39. *Ein Element $m \in M$ eines Monoids M heißt* invertierbar*, bzw. eine* Einheit*, falls es ein inverses Element $n \in M$ gibt, d.h. dass $m \cdot n = n \cdot m = 1$. Es ist*

$$M^\times = \{m \in M \mid m \text{ ist invertierbar}$$

die Einheitengruppe *von M.*

Bemerkung 2.40. 1. Ist $m \in M$ invertierbar, so ist das Inverse von m eindeutig: Sind nämlich $n_1, n_2 \in M$ invers zu m, so ist $n_1 = n_1 \cdot 1 = n_1 \cdot m \cdot n_2 = 1 \cdot n_2 = n_2$. Das Inverse von m wird als m^{-1} bezeichnet.

2. Ist $m \in M$, so ist $m \cdot m^{-1} = m^{-1} \cdot m = 1$, also m invers zu m^{-1}. Daher ist auch m^{-1} invertierbar mit $(m^{-1})^{-1} = m$.

Es sei M ein Monoid. Wir zeigen, dass $M^\times$ eine Gruppe bildet: Sind $m, n \in M^\times$, so ist

$$(m \cdot n) \cdot (n^{-1} \cdot m^{-1}) = m \cdot n \cdot n^{-1} \cdot m^{-1} = m \cdot 1 \cdot m^{-1} = m \cdot m^{-1} = 1,$$

also ist auch $m \cdot n$ invertierbar. Das zeigt, dass auch $m \cdot n \in M^\times$. Als lässt sich die Verknüpfung $\cdot$ auf M einschränken.

Die Assoziativität von $\cdot$ auf $M^\times$ ergibt sich direkt aus der Assoziativität von $\cdot$ auf M.

Da $1 = 1 \cdot 1$ ist $1 \in M$ invertierbar mit $1^{-1} = 1$, also auch $1 \in M^\times$. Da $1 \cdot m = m \cdot 1 = m$ für alle $m \in M$ gilt dies insbesondere für alle $m \in M^\times$, also ist 1 auch in $M^\times$ neutral bezüglich $\cdot$.

Ist $m \in M^\times$ so ist auch m^{-1} invertierbar, also $m^{-1} \in M^\times$. Auch in $M^\times$ sind m und m^{-1} invers zueinander.

Ingesamt zeigt dies, dass $M^\times$ eine Gruppe bildet.

Bemerkung 2.41. Ein Monoid M ist genau dann eine Gruppe, wenn $M^\times = M$.

Beispiel(e). 1. Für eine Menge X sei $E(X) \coloneqq \{f \mid f\colon X \to X\}$ die Menge aller Abbildungen $X \to X$. Funktionskomposition ist assoziativ und für alle $f \in E(X)$ ist $f \circ \mathrm{id} = f = \mathrm{id} \circ f$, also ist id_X auf $E(X)$ neutral bezüglich der Funktionskomposition. Also bildet $E(X)$ zusammen mit der Funktionskomposition ein Monoid. Es gilt $E(X)^\times = S(X)$.

2. Ist G eine Gruppe, so sei

$$\mathrm{End}(G) \coloneqq \{\varphi\colon G \to G \mid \varphi \text{ ist ein Gruppenhomomorphismus}\}.$$

Funktionskomposition ist assoziativ und die Verknüpfung zweier Gruppenhomomorphismen ist ebenfalls ein Gruppenhomomorphismus. Deshalb bildet $\mathrm{End}(G)$ zusammen mit der Funktionskomposition ein Monoid bildet, und es gilt $\mathrm{End}(G)^\times = \mathrm{Aut}(G)$.

2.13.2. Einheitengruppe eines Rings

2.14. Produkte von Gruppen

Es sei I ein Indexmenge und für jedes $i \in I$ sei G_i eine Gruppe. Wir definieren auf dem Produkt $\prod_{i \in I} G_i$ eine Multiplikation durch

$$(g_i)_{i \in I} \cdot (h_i)_{i \in I} = (g_i \cdot h_i)_{i \in I} \quad \text{für alle } (g_i)_{i \in I}, (h_i)_{i \in I} \in \prod_{i \in I} G_i.$$

Wir zeigen, dass $\prod_{i \in I} G_i$ zusammen mit dieser Multiplikation $\cdot$ eine Gruppe ist:

Für alle $(g_i)_{i\in I}, (h_i)_{i\in I}, (k_i)_{i\in I} \in \prod_{i\in I} G_i$ ist

$$\begin{aligned}((g_i)_{i\in I} \cdot (h_i)_{i\in I}) \cdot (k_i)_{i\in I} = (g_i h_i)_{i\in I} \cdot (k_i)_{i\in I} = (g_i h_i k_i)_{i\in I}\\ r = (g_i)_{i\in I} \cdot (h_i k_i)_{i\in I} = (g_i)_{i\in I} \cdot ((h_i)_{i\in I} \cdot (k_i)_{i\in I}),\end{aligned}$$

also ist $\cdot$ assoziativ.

Für alle $(g_i)_{i\in I} \in \prod_{i\in I}$ ist

$$\begin{aligned}(1)_{i\in I} \cdot (g_i)_{i\in I} = (1 \cdot g_i)_{i\in I} = (g_i)_{i\in I} \text{ und}\\ (g_i)_{i\in I} \cdot (1)_{i\in I} = (g_i \cdot 1)_{i\in I} = (g_i)_{i\in I},\end{aligned}$$

also ist $(1)_{i\in I}$ neutral bezüglich $\cdot$.

Für jedes $(g_1, \dots, g_n) \in G$ ist

$$\begin{aligned}(g_i)_{i\in I} \cdot (g_i^{-1})_{i\in I} = (g_i g_i^{-1})_{i\in I} = (1)_{i\in I} \text{ und}\\ (g_i^{-1})_{i\in I} \cdot (g_i)_{i\in I} = (g_i^{-1} \cdot g_i)_{i\in I} = (1)_{i\in I}\end{aligned}$$

Also ist $(g_i^{-1})_{i\in I}$ invers zu (g_i) bezüglich $\cdot$.

Insgesamt zeigt dies, dass $\prod_{i\in I} G_i$ bezüglich $\cdot$ eine Gruppe ist.

Insbesondere ist für beliebige Gruppen $G_1, \dots, G_n$ auch $G_1 \times \cdots \times G_n$ mit der eintragsweisen Multiplikation

$$(g_1, \dots, g_n) \cdot (h_1, \dots, h_n) = (g_1 h_1, \dots, g_n h_n)$$

eine Gruppe. Für eine beliebige Gruppe G ist daher auch G^n mit der eintragsweisen Multiplikation eine Gruppe.

Bemerkung 2.42. 1. Das Produkt $\prod_{i\in I} G_i$ ist genau dann abelsch, wenn für alle $i \in I$ die Gruppe G_i abelsch ist. Inbesondere ist auch das Produkt $G_1 \times \cdots \times G_n$ genau dann abelsch, wenn $G_1, \dots, G_n$ alle abelsch sind, und das Produkt G^n ist genau dann abelsch, wenn G abelsch ist.

2. Die hier angegebene Gruppenstruktur auf $\prod_{i\in I} G_i$ ist die einzige Gruppenstruktur auf $\prod_{i\in I} G_i$, so dass für jedes $j \in I$ die Projektionsabbildung

$$\pi_j \colon \prod_{i\in I} G_i \to G_j, (g_i)_{i\in I} \mapsto g_j$$

ein Gruppenhomomorphismus ist.

3. Das Produkt $\prod_{i\in I} G_i$ hat die folgende Eigenschaft: Ist G eine beliebige Gruppe und für jedes $i \in I$ ein Gruppenhomomorphismus $\varphi_i \colon G \to G_i$ gegeben, so gibt es einen eindeutigen Gruppenhomomorphismus $\varphi \colon G \to \prod_{i\in I} G_i$ mit $\pi_i \circ \varphi = \varphi_i$ für jedes $i \in I$. φ ist dann durch

$$\varphi(g) = (\varphi_i(g))_{i\in I} \quad \text{für alle } g \in G$$

gegeben.

2.15. Die Potenzmenge als abelsche Gruppe

Es sei X eine beliebige Menge und $\mathcal{P}(X) = \{S \mid S \subseteq X\}$ die Potenzmenge. Für je zwei Teilmengen $A, B \subseteq X$ ist auch $A \triangle B = (A \cup B) \setminus (A \cap B) \subseteq X$. Also ist

$$\triangle \colon \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X), (A, B) \mapsto A \triangle B$$

eine binäre Verknüpfung. Wir zeigen, dass $\mathcal{P}(X)$ zusammen mit $\triangle$ ein abelsche Gruppe bildet:

Die Kommutativität ergibt sich daraus, dass für alle $A, B \subseteq X$

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B \triangle A.$$

Für jede Teilmenge $A \subseteq X$ ist

$$A \triangle \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A,$$

also ist $\emptyset$ neutral bezüglich $\triangle$. Für jede Teilmeng $A \subseteq X$ ist

$$A \triangle A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset,$$

also ist A selbstinvers bezöglich $\triangle$.

Es muss nur noch die Assoziativität gezeigt werden: Hierfür bemerken wir zunächst, dass für alle Teilmengen $A, B \subseteq X$

$$\begin{aligned} A \triangle B &= (A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A \cap B)^C = (A \cup B) \cap (A^C \cup B^C) \\ &= (A \cap A^C) \cup (A \cap B^C) \cup (B \cap A^C) \cup (B \cap B^C) = (A \cap B^C) \cup (A^C \cap B). \end{aligned}$$

Für alle Teilmengen $A, B, C \subseteq X$ ist daher

$$\begin{aligned} & A \triangle (B \triangle C) \\ =& (A \cap (B \triangle C)^C) \cup (A^C \cap (B \triangle C)) \\ =& \big(A \cap ((B \cap C^C) \cup (B^C \cup C))^C\big) \cup \big(A^C \cap ((B \cap C^C) \cup (B^C \cap C))\big) \\ =& \big(A \cap ((B \cap C^C)^C \cap (B^C \cup C)^C)\big) \cup \big(A^C \cap ((B \cap C^C) \cup (B^C \cap C))\big) \\ =& \big(A \cap (B^C \cup C) \cap (B \cap C^C)\big) \cup \big(A^C \cap ((B \cap C^C) \cup (B^C \cap C))\big) \\ =& (A \cap B^C \cap B) \cup (A \cap B^C \cap C^C) \cup (A \cap C \cap B) \cup (A \cap C \cap C^C) \\ & \cup (A^C \cap B \cap C^C) \cup (A^C \cap B^C \cap C) \\ =& (A \cap B \cap C) \cup (A \cap B^C \cap C^C) \cup (B \cap A^C \cap C^C) \cup (C \cap A^C \cap B^C). \end{aligned}$$

Da der rechte Ausdruck invariant unter Permutation von A, B und C ist, ist

$$\begin{aligned} & (A \triangle B) \triangle C = C \triangle (A \triangle B) \\ =& (C \cap A \cap B) \cup (C \cap A^C \cap B^C) \cup (A \cap C^C \cap B^C) \cup (B \cap C^C \cap A^C) \\ =& (A \cap B \cap C) \cup (A \cap B^C \cap C^C) \cup (B \cap A^C \cap C^C) \cup (C \cap A^C \cap B^C) \\ =& A \triangle (B \triangle C). \end{aligned}$$

Dies zeigt die Assoziativität von $\triangle$ auf $\mathcal{P}(X)$.

Ingesamt zeigt dies, dass $\mathcal{P}(X)$ bezüglich $\triangle$ eine abelsche Gruppe bildet.

Bemerkung 2.43. Dieses Beispiel dient in erster Linie der Belustigung des Lesers und des Schreibers.

2.16. Das semidirekte Produkt $\mathbb{Z} \rtimes \mathbb{Z}$

Wir definieren auf der Menge $\mathbb{Z} \rtimes \mathbb{Z} := \{(n, m) \mid n, m \in \mathbb{Z}\}$ eine Verknüpfung $*$ durch

$$(n_1, m_1) * (n_2, m_2) = (n_1 + (-1)^{m_1} n_2, m_1 + m_2) \quad \text{für alle } n_1, n_2, m_1, m_2 \in \mathbb{Z}.$$

Wir zeigen, dass $\mathbb{Z} \rtimes \mathbb{Z}$ zusammen mit der Verknüpfung $*$ eine nicht-abelsche Gruppe bildet:
Für alle $(n_1, m_1), (n_2, m_2), (n_3, m_3) \in \mathbb{Z} \rtimes \mathbb{Z}$ ist

$$\begin{aligned}(n_1, m_1) * ((n_2, m_2) * (n_3, m_3)) &= (n_1, m_1) * (n_2 + (-1)^{m_2} n_3, m_2 + m_3) \\ &= (n_1 + (-1)^{m_1}(n_2 + (-1)^{m_2} n_3), m_1 + m_2 + m_3) \\ &= (n_1 + (-1)^{m_1} n_2 + (-1)^{m_1 + m_2} n_3, m_1 + m_2 + m_3) \\ &= (n_1 + (-1)^{m_1} n_2, m_1 + m_2) * (n_3, m_3) \\ &= ((n_1, m_1) * (n_2, m_2)) * (n_3, m_3),\end{aligned}$$

was die Assoziativität zeigt. Für alle $(n, m) \in \mathbb{Z} \rtimes \mathbb{Z}$ ist

$$\begin{aligned}(0, 0) * (n, m) &= (0 + (-1)^0 n, 0 + m) = (n, m) \text{ und} \\ (n, m) * (0, 0) &= (n + (-1)^m \cdot 0, m + 0) = (n, m),\end{aligned}$$

also ist $(0, 0)$ neutral bezüglich $*$. Für $(n, m) \in \mathbb{Z} \rtimes \mathbb{Z}$ ist

$$\begin{aligned}(n, m) * \big((-1)^{m+1} n, -m\big) &= \big(n + (-1)^m (-1)^{m+1} n, m + (-m)\big) \\ &= (n - n, m - m) = (0, 0)\end{aligned}$$

und

$$\big((-1)^{m+1} n, -m\big) * (n, m) = \big((-1)^{m+1} n + (-1)^{-m} n, -m + m\big) = (0, 0),$$

also $((-1)^{m+1} n, -m)$ invers zu (n, m) bezüglich $*$. Das zeigt, dass $(\mathbb{Z} \rtimes \mathbb{Z}, *)$ eine Gruppe ist.

Diese Gruppe ist nicht abelsch, da etwa

$$\begin{aligned}(1, 0) * (0, 1) &= (1 + (-1)^0 \cdot 0, 0 + 1) = (1, 1) \text{ und} \\ (0, 1) * (1, 0) &= (0 + (-1)^1 \cdot 1, 1 + 0 = (-1, 1).\end{aligned}$$

Man bezeichnet die Gruppe $\mathbb{Z} \rtimes \mathbb{Z}$ als das *semidirekte Produkt* von $\mathbb{Z}$ und $\mathbb{Z}$.

2.17. Ausblick: Semidirekte Produkte

Als Verallgemeinerung des vorherigen Beispiels geben wir hier die allgemeine Konstruktion von semidirekten Produkten an:

Es seien G und H zwei Gruppen und $\theta\colon H \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus. (Hier bezeichnet $\mathrm{Aut}(G)$ die Automorphismengruppe von G, siehe 2.12.1.) Auf der Menge $G \times H = \{(g,h) \mid g \in G, h \in H\}$ definieren wir eine binäre Verknüpfung durch

$$(g_1,h_1)\cdot(g_2,h_2) = (g_1\theta(h_1)(g_2), h_1h_2).$$

Wir zeigen, dass $G \rtimes_\theta H$ zusammen mit dieser Verknüpfung eine Gruppe bildet: Hierfür bemerken wir zunächst, dass für alle $h, h' \in H$ und $g \in G$

$$\theta(h)(\theta(h')(g)) = (\theta(h)\circ\theta(h'))(g) = \theta(hh')(g),$$

da θ ein Gruppenhomomorphismus ist. Für alle $(g_1,h_1),(g_2,h_2),(g_3,h_3) \in G\times H$ ist daher

$$\begin{aligned}
&(g_1,h_1)\cdot((g_2,h_2)\cdot(g_3,h_3)) = (g_1,h_1)\cdot(g_2\theta(h_2)(g_3), h_2h_3)\\
=&(g_1\theta(h_1)(g_2\theta(h_2)(g_3)), h_1h_2h_3) = (g_1\theta(h_1)(g_2)\theta(h_1)(\theta(h_2)(g_3))\\
=&(g_1\theta(h_1)(g_2)\theta(h_1h_2)(g_3), h_1h_2h_3) = (g_1\theta(h_1)(g_2), h_1h_2)\cdot(g_3,h_3)\\
=&((g_1,h_1)\cdot(g_2,h_2))\cdot(g_3,h_3),
\end{aligned}$$

was die Assoziativität von $\cdot$ zeigt.

Für alle $h \in H$ ist $\theta(h)$ ein Gruppenhomomorphismus, und somit $\theta(h)(1) = 1$; außerdem ist $\theta(1) = \mathrm{id}_G$. Für alle $(g,h) \in G \times H$ ist deshalb

$$(g,h)\cdot(1,1) = (g\theta(h)(1), h\cdot 1) = (g\cdot 1, h\cdot 1) = (g,h)$$

und

$$(1,1)\cdot(g,h) = (1\cdot\theta(1)(g), 1\cdot h) = (1\cdot g, 1\cdot h) = (g,h).$$

Also ist $(1,1)$ neutral bezüglich $\cdot$.

Für alle $h \in H$ ist $\theta(h^{-1}) = \theta(h)^{-1}$, da θ ein Gruppenhomomorphismus ist, sowie $\theta(h)(g^{-1}) = \theta(h)(g)^{-1}$ für alle $g \in G$, da $\theta(h)$ ein Gruppenhomomorphismus ist. Für alle $(g,h) \in G \times H$ ist deshalb

$$\begin{aligned}
&(g,h)\cdot(\theta(h^{-1})(g^{-1}), h^{-1}) = (g\theta(h)(\theta(h^{-1})(g^{-1})), hh^{-1})\\
=&(g\theta(h)(\theta(h)^{-1}(g^{-1})), hh^{-1}) = (gg^{-1}, hh^{-1}) = (1,1)
\end{aligned}$$

und

$$\begin{aligned}
(\theta(h^{-1})(g^{-1}), h^{-1})\cdot(g,h) &= (\theta(h^{-1})(g^{-1})\theta(h^{-1})(g), h^{-1}h)\\
&= (\theta(h^{-1})(g)^{-1}\theta(h^{-1})(g), h^{-1}h) = (1,1).
\end{aligned}$$

Also ist $(\theta(h^{-1})(g^{-1}), h^{-1})$ invers zu (g,h) bezüglich $\cdot$.

Ingesamt zeigt dies, dass die Menge $G \times H$ zusammen mit der Verknüpfung $\cdot$ eine Gruppe bildet. Man bemerke, dass die Multiplikation $\cdot$ von dem Gruppenhomomorphismus $\cdot$ abhängt.

Definition 2.44. *Es seien G und H Gruppen und $\theta\colon H \to G$ ein Gruppenhomomorphismus. Dann sei die binäre Verknüpfung $\cdot_\theta$ auf $G \times H$ definiert als*

$$(g_1,h_1)\cdot_\theta(g_2,h_2) = (g_1\theta(h_1)(g_2), h_1h_2) \quad \textit{für alle } (g_1,h_1),(g_2,h_2) \in G\times H.$$

Die Gruppe $(G \times H, \cdot_\theta)$. Bezeichnet man als ein semidirektes Produkt *der Gruppen G und H, und schreibt dieses als $G \rtimes_\theta H$.*

Beispiel(e). 1. Sind G und H Gruppen und ist $\theta\colon H \to \mathrm{Aut}(G)$ der triviale Gruppenhomomorphismus, d.h. $\theta(h) = \mathrm{id}_G$ für alle $h \in H$, so ist die Multiplikation auf $G \rtimes_\theta H$ für alle $(g_1, h_1), (g_2, h_2) \in G \rtimes_\theta H$ gegeben durch

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1\theta(h_1)(g_2), h_1h_2) = (g_1g_2, h_1h_2).$$

Es handelt sich also um das gewöhnliche Produkt $G \times H$.

2. Für jedes $m \in \mathbb{Z}$ ist die Abbildung

$$\theta(m)\colon \mathbb{Z} \to \mathbb{Z}, \quad n \mapsto (-1)^m n$$

ein Gruppenautomorphismus: Da $\theta(m)^2 = \mathrm{id}_\mathbb{Z}$ ist $\theta(m)$ invertierbar mit $\theta(m)^{-1} = \theta(m)$, und $\theta(m)$ ist ein Gruppenhomomorphismus, denn für alle $n_1, n_2 \in \mathbb{Z}$ ist

$$\begin{aligned}\theta(m)(n_1 + n_2) &= (-1)^m(n_1 + n_2)\\ &= (-1)^m n_1 + (-1)^m n_2 = \theta(m)(n_1) + \theta(m)(n_2)\end{aligned}$$

Die Abbildung $\theta\colon \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z})$ ist außerdem eine Gruppenhomomorphismus, denn für alle $m_1, m_2 \in \mathbb{Z}$ ist

$$\begin{aligned}\theta(m_1 + m_2)(n) &= (-1)^{m_1+m_2}n = (-1)^{m_1}(-1)^{m_2}n\\ &= \theta(m_1)(\theta(m_2)(n)) = (\theta(m_1) \circ \theta(m_2))(n)\end{aligned}$$

für alle $n \in \mathbb{Z}$, also $\theta(m_1+m_2) = \theta(m_1)\circ\theta(m_2)$. Ingesamt zeigt dies, dass $\theta\colon \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z})$ ein Gruppenhomomorphismus ist.

Die Multiplikation auf dem entsprechenden semidirekten Produkt $\mathbb{Z} \rtimes_\theta \mathbb{Z}$ ist gegeben durch

$$(n_1, m_1) \cdot (n_2, m_2) = (n_1 + \theta(m_1)(n_2), m_1 + m_2) = (n_1 + (-1)^{m_1}n_2, m_1 + m_2)$$

für alle $(n_1, m_1), (n_2, m_2) \in \mathbb{Z} \rtimes_\theta \mathbb{Z}$. Dies ist das semidirekte Produkt aus 2.16.

3. Es sei G eine Gruppe. Wie in 2.12.6 gesehen, ist die Abbildung $c\colon G \to \mathrm{Aut}(G), h \mapsto c_h$ mit

$$c_h(g) = hgh^{-1} \quad \text{für alle } h, g \in G$$

ein wohldefnierter Gruppenhomomorphismus. Ist $H \subseteq G$ eine Untergruppe, so ist daher auch die Einschränkung $c|_H\colon H \to \mathrm{Aut}(G)$, $h \mapsto c_h$ ein Gruppenhomomorphismus. Hieraus ergibt sich das semidirekte Produkt $H \rtimes_{c|_H} G$ mit

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1c_{h_1}(g_2), h_1h_2) = (g_1h_1g_2h_1^{-1}, h_1h_2)$$

für alle $(g_1, h_1), (g_2, h_2) \in G \rtimes_{c|_H} H$.

4. Es sei $S = \{1, -1\}$ und $G = \mathbb{Z}/3\mathbb{Z}$. ($S$ ist eine Gruppe bezüglich der üblichen Multiplikation.) Für $s \in S$ sei $\theta(s)\colon G \to G, x \mapsto sx$; für alle $g \in G$ ist also $\theta(1)(g) = g$ und $\theta(-1)(g) = -g$.

Da $\theta(-1)^2 = \mathrm{id}_G$ ist $\theta(-1)$ bijektiv mit $\theta(-1)^{-1} = \theta(-1)$; $\theta(-1)$ ist auch ein Gruppenhomomorphismus, da

$$\theta(-1)(g_1 + g_2) = -(g_1 + g_2) = (-g_1) + (-g_2) = \theta(-1)(g_1) + \theta(-1)(g_2)$$

für alle $g_1, g_2 \in G$. Also sind $\theta(1) = \mathrm{id}_G$ und $\theta(-1)$ Gruppenautomorphismen von G. Somit ist die Abbildung $\theta\colon S \to \mathrm{Aut}(G)$ wohldefiniert. θ ist ein Gruppenhomomorphismus, denn

$$\begin{aligned}
\theta(1 \cdot 1 = \theta(1) = \mathrm{id}_G = \mathrm{id}_G \circ \mathrm{id}_G = \theta(1) \circ \theta(1),\\
\theta((-1) \cdot 1) = \theta(-1) = \theta(-1) \circ \mathrm{id}_G = \theta(-1) \circ \theta(1),\\
\theta(1 \cdot (-1)) = \theta(-1) = \mathrm{id}_G \circ \theta(-1) = \theta(1) \circ \theta(-1),\\
\theta((-1) \cdot (-1)) = \theta(1) = \mathrm{id}_G = \theta(-1) \circ \theta(-1).
\end{aligned}$$

Damit ergibt sich das semidirekte Produkt $G \rtimes_\theta S = (\mathbb{Z}/3\mathbb{Z}) \rtimes_\theta S$ mit

$$(g_1, s_1) \cdot (g_2, s_2) = (g_1 + \theta(s_1)(g_2), s_1 s_2) = (g_1 + s_1 g_2, s_1 s_2)$$

für alle $(g_1, s_1), (g_2, s_2) \in (\mathbb{Z}/3\mathbb{Z}) \rtimes_\theta S$.

Bemerkung 2.45. Die Gruppe $(\mathbb{Z}/3\mathbb{Z}) \rtimes_\theta S$ hat 6 Element, und es lässt sich zeigen, dass $(\mathbb{Z}/3\mathbb{Z}) \rtimes_\theta S \cong S_3$. Da S zweielementig ist, gibt es, wie in 2.2 gesehen, außerdem einen eindeutigen Gruppenisomorphismus $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to S$, der durch $\varphi(0) = 1$ und $\varphi(1) = -1$ gegeben ist.

Da φ und θ Gruppenhomomorphismen sind, ist auch $\theta \circ \varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ ein Gruppenhomomorphismus. Durch den Gruppenhomomorphismus $\theta \circ \varphi$ ergibt sich auch ein semidirektes Produkt $(\mathbb{Z}/3\mathbb{Z}) \rtimes_{\theta\circ\varphi} (\mathbb{Z}/2\mathbb{Z})$.

Es lässt sich zeigen, dass φ einen Gruppenisomorphismus

$$\varphi_*\colon (\mathbb{Z}/3\mathbb{Z}) \rtimes_{\theta\circ\varphi} (\mathbb{Z}/2\mathbb{Z}) \to (\mathbb{Z}/3\mathbb{Z}) \rtimes_\theta S, \quad (g, h) \mapsto (g, \varphi(h))$$

induziert. Damit ergibt sich dann, dass

$$(\mathbb{Z}/3\mathbb{Z}) \rtimes_{\theta\circ\varphi} (\mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes_\theta S \cong S_3.$$

Die symmetrische Gruppe S_3 lässt sich daher als semidirektes Produkt von $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}$ auffassen.

3. Beispiele für Körper

3.1. Einige kleine Beispiele

1. Die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ bilden zusammen mit der üblichen Addition und Multiplikation jeweils einen Körper. $\mathbb{Q}$ ist ein Unterkörper von $\mathbb{R}$.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden zusammen mit der üblichen Addition und Multiplikation *keinen* Körper: Ansonsten wäre $(\mathbb{Z} \setminus \{0\}, \cdot)$ ein Körper, aber $2 \in \mathbb{Z} \setminus \{0\}$ besitzt kein multiplikativ Inverses in $\mathbb{Z}$.
3. Für einen beliebigen Körper K und $n \in \mathbb{N}$, $n \geq 2$ bilden die quadratischen Matrizen $\mathrm{Mat}(n \times n, K)$ zusammen mit der gewöhnlichen Addition und Multiplikation von Matrizen keinen Körper: Zum einen ist die Multiplikation in diesem Fall nicht kommutativ, da
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{aber} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$
Zum anderen ist nicht jede Matrix $A \in \mathrm{Mat}(n \times n, K) \setminus \{0\}$ bezüglich der Matrixmultiplikation invertierbar, da etwa
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
für alle $a, b, c, d \in K$.

3.2. Bilder von Körperhomomorphismen

Sind K und L Körper und ist $\phi\colon K \to L$ ein Körperhomomorphismus, so ist $\mathrm{im}(\phi) \subseteq L$ ein Unterkörper:

Es ist $0 = \phi(0) \in \mathrm{im}(\phi)$. Für $x, y \in \mathrm{im}(\phi)$ gibt es $x', y' \in K$ mit $\phi(x') = x$ und $\phi(y') = y$, weshalb auch
$$x + y = \phi(x') + \phi(y') = \phi(x' + y') \in \mathrm{im}(\phi).$$
Für $x \in \mathrm{im}(\phi)$ gibt es $x' \in K$ mit $\phi(x') = x$, weshalb auch
$$-x = -\phi(x') = \phi(-x') \in \mathrm{im}(\phi).$$
Also ist $\mathrm{im}(\phi)$ eine Untergruppe der additiven Gruppe von L.

Bemerkung 3.1. Kürzer und eleganter lässt sich die obige Rechnung so zusammenfassen: Da ϕ insbesondere ein Gruppenhomomorphismus von der additiven Gruppe von K in die additive Gruppe von L ist, ist $\mathrm{im}(\phi) \subseteq L$ eine abelsche Untergruppe, da Bilder von Gruppenhomomorphismen stets Untergruppen sind.

Es ist $1 = \phi(1) \in \text{im}(\phi)$. Sind $x, y \in \text{im}(\phi)$, so gibt es $x', y' \in K$ mit $x = \phi(x')$ und $y = \phi(x')$, weshalb dann auch

$$x \cdot y = \phi(x') \cdot \phi(y') = \phi(x' \cdot y')\text{im}(\phi).$$

Ist schließlich $x \in \text{im}(\phi)$ mit $x \neq 0$, so gibt es $x' \in K$ mit $x = \phi(x')$. Da $x \neq 0$ ist auch $x \neq 0$. Da ϕ ein Körperhomomorphismus ist, ist somit $\phi(x')$ invertierbar mit $\phi(x')^{-1} = \phi((x')^{-1}) \in \text{im}(\phi)$, also $x^{-1} = \phi(x')^{-1} \in \text{im}(\phi)$.

Insgesamt zeigt dies, dass $\text{im}(\phi)$ ein Unterkörper von L ist.

Bemerkung 3.2. 1. Da ϕ als Körperhomomorphismus injektiv ist, ist die Abbildung $K \to \text{im}(\phi), x \mapsto \phi(x)$ ein bijektiv und ein Körperhomomorphismus, also ein Körperisomorphismus. Inbesondere ist also $\text{im}(\phi)$ isomorph zu K.

2. Ist L ein Körper und $K \subseteq L$ ein Unterkörper, so ist die Inklusion $K \to L, x \mapsto x$ ein Körperhomomorphismus. Es ist also jeder Unterkörper von L gegeben als Bild eines Körperhomomorphismus $\phi\colon K \to L$, und wie bereits zuvor bemerkt $\text{im}(\phi)$ ist isomorph zu K.

   Man kann deshalb einen Unterkörper K eines Körpers L statt als eine Teilmenge, die unter entsprechenden Rechenoperationen abgeschlossen ist, und somit selber wieder einen Körper bildet, auch als einen Körperhomomorphismus $K \to L$ definieren.

3.3. Schnitte und Vereinigungen von Unterkörpern

3.3.1. Schnitte von Unterkörpern

Es sei L ein Körper und $\{K_i\}_{i \in I}$ eine Kollektion von Unterkörpern, d.h. für alle $i \in I$ ist $K_i \subseteq L$ ein Unterkörper. Dann ist auch der Schnitt $K \coloneqq \bigcap_{i \in I} K_i$ ein Unterkörper:

Da K_i für jedes $i \in I$ ein Unterkörper ist, ist $0, 1 \in K_i$ für alle $i \in I$ und somit auch $0, 1 \in \bigcap_{i \in I} K_i$.

Sind $x, y \in K$, so sind $x, y \in K_i$ für alle $i \in I$. Da K_i für alle $i \in I$ ein Unterkörper ist, ist damit auch $x + y \in K_i$ für alle $i \in I$ und $x \cdot y \in K_i$ für alle $i \in I$. Somit ist damit auch $x + y, x \cdot y \in K$.

Sind $x, y \in K$ mit $y \neq 0$, so sind $x, y \in K_i$ für alle $i \in I$. Da K_i für alle $i \in I$ ein Unterkörper ist, ist damit auch $-x, y^{-1} \in K_i$ für alle $i \in I$. Also ist damit auch $-x, y^{-1} \in K$.

Ingesamt zeigt dies, dass $K = \bigcap_{i \in I} K_i$ ein Unterkörper ist.

3.3.2. Vereinigung von Unterkörpern

3.4. Die komplexen Zahlen $\mathbb{C}$

Die komplexen Zahlen $\mathbb{C}$ sind ein Körper, der die reellen Zahlen $\mathbb{R}$ enthält, und in dem es ein Element $i \in \mathbb{C}$ gibt, für das $i^2 = -1$. Wir geben an dieser Stelle zwei mögliche Konstruktionen der komplexen Zahlen an:

3.4.1. Die komplexen Zahlen als besserer $\mathbb{R}^2$

Wir beginnen mit der additiven Gruppe $\mathbb{C} \coloneqq \mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$. Die Addition ist gegeben durch

$$(a_1,b_1)+(a_2,b_2) = (a_1+a_2, b_1+b_2) \quad \text{für alle } (a_1,b_1),(a_2,b_2) \in \mathbb{C}.$$

Wir definieren zusätzlich eine Multiplikation $\cdot$ auf $\mathbb{C}$ durch

$$(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \quad \text{für alle } (a_1,b_1),(a_2,b_2) \in \mathbb{C}.$$

Behauptung. *$\mathbb{C}$ ist zusammen mit der obigen Addition und Multiplikation ein Körper.*

Beweis. Wir wissen bereits, dass $\mathbb{C}$ zusammen mit der Addition $+$ eine abelsche Gruppe bildet. Das additiv neutrale Element ist $(0,0)$ und das additiv Inverse zu $(a,b) \in \mathbb{C}$ ist $(-a,-b)$ Für alle $(a_1,b_1),(a_2,b_2),(a_3,b_3) \in \mathbb{C}$ ist

$$\begin{aligned}
&(a_1,b_1)\cdot((a_2,b_2)\cdot(a_3,b_3)) = (a_1,b_1)\cdot(a_2a_3 - b_2b_3, a_2b_3 + a_3b_2)\\
=&(a_1a_2a_3 - a_1b_2b_3 - a_2b_1b_3 - a_3b_1b_2, a_2a_3b_1 - b_1b_2b_3 + a_1a_2b_3 + a_1a_3b_2)\\
=&(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)\cdot(a_3,b_3) = ((a_1,b_1)\cdot(a_2,b_2))\cdot(a_3,b_3),
\end{aligned}$$

also ist die Multiplikation assoziativ. Für alle $(a_1,b_1),(a_2,b_2) \in \mathbb{C}$ ist

$$\begin{aligned}
(a_1,b_1)\cdot(a_2,b_2) &= (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)\\
&= (a_2a_1 - b_2b_1, a_2b_1 + a_1b_2) = (a_2,b_2)\cdot(a_1,b_1),
\end{aligned}$$

also ist die Multiplikation kommutativ. Für alle $(a,b) \in \mathbb{C}$ ist

$$(1,0)\cdot(a,b) = (1\cdot a - 0\cdot b, 0\cdot a + 1\cdot b) = (a,b),$$

also ist $(1,0)$ neutral bezüglich der Multiplikation. Ist $(a,b) \in \mathbb{C}$ mit $(a,b) \neq (0,0)$, so ist $a \neq 0$ oder $b \neq 0$, also $a^2 + b^2 \neq 0$. Daher ist

$$(a,b)\cdot\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = \left(a\frac{a}{a^2+b^2} + b\frac{b}{a^2+b^2}, b\frac{a}{a^2+b^2} - a\frac{b}{a^2+b^2}\right) = (1,0).$$

Also ist $(a/(a^2+b^2), -b/(a^2+b^2))$ multiplikativ invers zu (a,b).

Die Distributivität folgt daraus, dass für alle $(a_1,b_1),(a_2,b_2),(a_3,b_3) \in \mathbb{C}$

$$\begin{aligned}
&(a_1,b_1)\cdot((a_2,b_2)+(a_3,b_3))\\
=&(a_1,b_1)\cdot(a_2+a_3, b_2+b_3)\\
=&(a_1(a_2+a_3) - b_1(b_2+b_3), a_1(b_2+b_3) + (a_2+a_3)b_1)\\
=&(a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3, a_1b_2 + a_1b_3 + a_2b_1 + a_3b_1)\\
=&(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) + (a_1a_3 - b_1b_3, a_1b_3 + a_3b_1)\\
=&(a_1,b_1)\cdot(a_2,b_2) + (a_1,b_1)\cdot(a_3,b_3).
\end{aligned}$$

Ingesamt zeigt dies, dass $\mathbb{C}$ zusammen mit der angegebenen Addition und Multiplikation ein Körper ist. □

Wir wollen noch etwas Notation einführen, um den Umgang mit $\mathbb{C}$ angenehmer zu gestalten: Wir schreiben $0 = (0,0)$ und $1 = (1,0)$. Wir bemerken zunächst, dass für alle $a, a' \in \mathbb{R}$

$$(a,0) + (a',0) = (a+a',0)$$

und

$$(a,0) \cdot (a',0) = (aa' - 0 \cdot 0, a \cdot 0 + 0 \cdot a') = (aa',0)$$

und $1 = (1,0)$. Deshalb ist die Abbildung $\phi\mathbb{R}\colon \mathbb{C}$, $a \mapsto (a,0)$ ein Körperhomomorphismus. Daher ist $\mathrm{im}(\phi) = \{(a,0) \mid a \in \mathbb{R}\} \subseteq \mathbb{C}$ ein Unterkörper, den wir durch ϕ mit $\mathbb{R}$ identifizieren. Wir unterscheiden also im Folgenden nicht mehr zwischen $a \in \mathbb{R}$ und $(a,0) \in \mathbb{C}$.

Wir schreiben $i \coloneqq (0,1) \in \mathbb{C}$. Für jedes $b \in \mathbb{R}$ gilt

$$b \cdot i = (b,0) \cdot (0,1) = (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (0,b).$$

Ein beliebiges Element $z = (a,b) \in \mathbb{C}$ lässt sich daher als

$$z = (a,b) = (a,0) + (0,b) = a + bi$$

schreiben. Die beiden reellen Zahlen $a, b \in \mathbb{R}$ mit $z = a + bi$ sind eindeutig, da $z = (a,b)$.

Bemerke, dass $i^2 = (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -1$. Die Addition lässt sich nun auch so darstellen, dass für alle $a_1, a_2, b_1, b_2 \in \mathbb{R}$

$$(a_1 + b_1 i) + (a_2 + b_2 i) = a_1 + a_2 + b_1 i + b_2 i = (a_1 + a_2) + (b_1 + b_2)i,$$

und die Multiplikation so, dass

$$\begin{aligned}(a_1 + b_1 i)(a_2 + b_2 i) &= a_1 a_2 + a_1 b_2 i + a_2 b_1 i + b_1 b_2 i^2 \\ &= a_1 a_2 - b_1 b_2 + a_1 b_2 i + a_2 b_1 i \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.\end{aligned}$$

3.4.2. Die komplexen Zahlen als reelle (2×2)-Matrizen

Unabhängig von der ersten Methode geben wir noch eine weitere Konstruktion der komplexen Zahlen an: Es sei

$$C \coloneqq \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\} \subseteq \mathrm{Mat}(2 \times 2, \mathbb{R}).$$

Wir zeigen, dass C zusammen mit der gewöhnlichen Matrixaddition und -multiplikation einen Körper bildet:

Für alle $a, b \in \mathbb{R}$ schreiben wir abkürzend

$$Z(a,b) \coloneqq \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Für alle $a_1, a_2, b_1, b_2 \in \mathbb{R}$ ist

$$\begin{aligned} Z(a_1, b_1) + Z(a_2, b_2) &= \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 + a_2 & -b_1 + b_2 \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} = Z(a_1 + a_2, b_1 + b_2) \end{aligned}$$

und außerdem

$$\begin{aligned} Z(a_1, b_1) \cdot Z(a_2, b_2) &= \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - a_2b_1 \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{pmatrix} = Z(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1). \end{aligned}$$

Um zu zeigen, dass C bezüglich der Addition eine abelsche Gruppe bildet genügt es zu zeigen, dass C eine Untergruppe der additiven Gruppe von $\mathrm{Mat}(2 \times 2, \mathbb{R})$ bildet.

Es ist $0 = Z(0, 0) \in C$ und für alle $a_1, a_2, b_1, b_2 \in \mathbb{R}$ ist

$$Z(a_1, b_1) + Z(a_2, b_2) = Z(a_1 + a_2, b_1 + b_2) \in C.$$

Für alle $a, b \in \mathbb{R}$ ist außerdem

$$-Z(a, b) = -\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} -a & b \\ -b & -a \end{pmatrix} = Z(-a, -b) \in C.$$

Also ist C eine abelsche Untergruppe der additiven Gruppe von $\mathrm{Mat}(2 \times 2, \mathbb{R})$.

Die Assoziativität der Multiplikation ist bekannt. Die Matrixmultiplikation ist auf C kommutativ, da für alle $a_1, a_2, b_1, b_2 \in \mathbb{R}$

$$\begin{aligned} Z(a_1, b_1) \cdot Z(a_2, b_2) &= Z(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \\ &= Z(a_2a_1 - b_2b_1, a_2b_1 + a_1b_2) = Z(a_2, b_2) \cdot Z(a_1, b_1). \end{aligned}$$

Da die Einheitsmatrix $I_2 \in \mathrm{Mat}(2 \times 2, \mathbb{R})$ das Einselement bezüglich der Matrixmultiplikation ist und $I_2 \in C$ ist I_2 das Einselement in C. Für $a, b \in \mathbb{R}$ mit $Z(a, b) \neq 0$ ist $a \neq 0$ oder $b \neq 0$ und somit $a^2 + b^2 \neq 0$. Da

$$\begin{aligned} &Z(a, b) \cdot Z\left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right) \\ &= Z\left(a\frac{a}{a^2 + b^2} + b\frac{b}{a^2 + b^2}, b\frac{a}{a^2 + b^2} - a\frac{b}{a^2 + b^2}\right) \\ &= Z(1, 0) = I_2 \end{aligned}$$

ist $Z(a/(a^2 + b^2), -b/(a^2 + b^2))$ das multiplikativ Inverse zu $Z(a, b)$ (da die Matrixmultiplikation auf C kommutativ ist, zeigt die obige Rechnung, dass $Z(a/(a^2 + b^2), -b/(a^2 + b^2))$ bereits beidseitig Invers zu $Z(a, b)$ ist).

Insgesamt zeigt dies, dass C mit der üblichen Matrixaddition und -multiplikation einen Körper bildet.

3.4.3. Äquivalenz der beiden Konstruktionen

Die beiden Konstruktionen der komplexen Zahlen sind insofern äquivalent, als dass die Abbildung

$$\phi\colon \mathbb{C} \to C, a + ib \mapsto Z(a, b) \quad \text{für alle } a, b \in \mathbb{R}$$

ein Körperisomorphismus ist: Die Bijektivität von ϕ folgt daraus, dass die beiden Abbildungen $\psi_1\colon \mathbb{R}^2 \to \mathbb{C}, (a, b) \mapsto a + ib$ und $\psi_2\colon \mathbb{R}^2 \to C, (a, b) \mapsto Z(a, b)$ bijektiv sind, und daher auch $\phi = \psi_2\psi_1^{-1}$. Außerdem ist $\phi(1) = \phi(1) = Z(1, 0) = I_2$. Für alle $a, a', b, b' \in \mathbb{R}$ ist zudem

$$\begin{aligned}\phi((a + ib) + (a' + ib')) &= \phi((a + a') + i(b + b')) = Z(a + a', b + b')\\ &= Z(a, b) + Z(a', b') = \phi(a + ib) + \phi(a' + ib')\end{aligned}$$

und

$$\begin{aligned}\phi((a + ib) \cdot (a' + ib')) &= \phi((aa' - bb') + i(ab' + a'b))\\ &= Z(aa' - bb', ab' + a'b) = Z(a, b) \cdot Z(a', b').\end{aligned}$$

Ingesamt zeigt dies, dass ϕ ein Körperisomorphismus ist.

3.5. Die endlichen Körper $\mathbb{F}_p$

Es sei $n \in \mathbb{N}$, $n \geq 1$. In 2.9 haben wir die endlichen abelschen Gruppen $\mathbb{Z}/n\mathbb{Z}$ konstruiert, indem wir auf $\mathbb{Z}$ die Äquivalenzrelation $\sim$ mit

$$k \sim l \iff \exists s \in \mathbb{Z} : k = l + sn$$

definieren und auf der Menge der Äquivalenzklassen $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\sim$ die Addition

$$[k] + [l] = [k + l] \quad \text{für alle } k, l \in \mathbb{Z}$$

definieren.

Die Multiplikation von $\mathbb{Z}$ liefert auf $\mathbb{Z}/n\mathbb{Z}$ eine Multiplikation durch

$$[k] \cdot [l] = [k \cdot l] \quad \text{für alle } k, l \in \mathbb{Z}.$$

Wir zeigen im Folgenden, dass diese Multiplikation wohldefiniert ist, und dass $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der obigen Addition und Multiplikation genau dann einen Körper bildet, wenn n eine Primzahl ist.

Wir zeigen zunächst, dass die Multiplikation wohldefiniert ist: Es seien $k, k', l, l' \in \mathbb{Z}$ mit $k \sim k'$ und $l \sim l'$. Dann gibt es $s, t \in \mathbb{Z}$ mit $k = k' + sn$ und $l = l' + tn$. Deshalb ist

$$k \cdot l = (k' + sn) \cdot (l' + tn) = k' \cdot l' + l'sn + k'tn + stn^2 = k' \cdot l' + (l's + k't + stn)n,$$

also auch $k \cdot l \sim k' \cdot l'$. Also ist die Multiplikation wohldefiniert.

Für alle $k_1, k_2, k_3 \in \mathbb{Z}$ ist

$$[k_1] \cdot ([k_2] \cdot [k_3]) = [k_1] \cdot [k_2 \cdot k_3] = [k_1 \cdot k_2 \cdot k_3] = [k_1 \cdot k_2] \cdot [k_3] = ([k_1] \cdot [k_3]) \cdot [k_3],$$

also ist die Multiplikation assoziativ. Für alle $k, l \in \mathbb{Z}$ ist

$$[k] \cdot [l] = [k \cdot l] = [l \cdot k] = [l] \cdot [k],$$

also ist die Multiplikation kommutativ. Für alle $k \in \mathbb{Z}$ ist

$$[1] \cdot [k] = [1 \cdot k] = [k],$$

also ist $[1]$ ein Einselement bezüglich der Multiplikation (dass auch $[k] \cdot [1] = [k]$ folgt sofort mithilfe der Kommutativität).

Es bleibt zu zeigen, dass $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper ist, wenn n prim ist.

Angenommen, p ist eine Primzahl. Es sei $x \in \mathbb{Z}/p\mathbb{Z}$ mit $x \neq 0$, also $x \neq [0]$. Dann gibt es $k \in \mathbb{Z}$ mit $0 < k < p$, so dass $x = [k]$. Nach Euklid gibt es $s, t \in \mathbb{Z}$ mit $sk + tp = \mathrm{ggT}(k, p)$. Da $0 < k < p$ und p prim ist, sind k und p teilerfremd. Also ist $\mathrm{ggT}(k, p) = 1$ und somit $sk + tp = 1$. Es folgt, dass

$$[s] \cdot x = [s] \cdot [k] = [sk] = [sk + tp] = [1],$$

also $[s] \cdot x = 1$. Somit ist x multiplikativ invertierbar.

Angenommen, $n \in \mathbb{N}$, $n \geq 1$ ist keine Primzahl. Ist $n = 1$, so ist $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/1\mathbb{Z} = \{[0]\}$. Insbesondere ist daher $[0] = [1]$, also $\mathbb{Z}/n\mathbb{Z}$ kein Körper. Wir betrachten als den Fall, dass zusätzlich $n \geq 2$. Da n nach Annahme nicht prim ist, gibt es $1 <\leq k, l < n$ mit $n = k \cdot l$. Da $0 < k, l < n$ ist $[k] \neq [0]$ und $[l] \neq [0]$. Da $n = k \cdot l$ ist aber

$$[k] \cdot [l] = [k \cdot l] = [n] = [0].$$

Wäre $\mathbb{Z}/n\mathbb{Z}$ ein Körper, so würde aus $[k] \cdot [l]$ aber folgen, dass $[k] = 0$ oder $[l] = 0$, was im Widerspruch zu $[k] \neq [0]$ oder $[l] \neq [0]$ stünde. Also ist $\mathbb{Z}/n\mathbb{Z}$ unter den obigen Annahmen kein Körper.

Für eine Primzahl p bezeichnet man den Körper $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ als $\mathbb{F}_p$. Dabei identifiziert man die Elemente von $\mathbb{Z}/p\mathbb{Z}$ wie bereits in 2.9 erläutert mit den entsprechenden Repräsentanten aus $\{0, \ldots, p-1\}$, hat also $\mathbb{F}_p = \{0, \ldots, p-1\}$. Bezeichnen $+$ und $\cdot$ die Addition und Multiplikation auf $\mathbb{Z}$ und $\tilde{+}$ und $\tilde{\cdot}$ die Multiplikation auf $\mathbb{F}_p$, so gilt dann

$$x \mathbin{\tilde{+}} y = (x + y) \bmod p \quad \text{und} \quad x \mathbin{\tilde{\cdot}} y = (x \cdot y) \bmod p \quad \text{für alle } x, y \in \mathbb{F}_p.$$

Beispiel(e). 1. Es ist $\mathbb{F}_2 = \{0, 1\}$. Die Addition ist gegeben durch $0 + 0 = 1 + 1 = 0$ und $0 + 1 = 1 + 0 = 1$, und die Multiplikation durch $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ und $1 \cdot 1 = 1$.

2. Es ist $\mathbb{F}_3 = \{0, 1, 2\}$. Die Addition und Multiplikation sind wie in den folgenden Tabellen gegeben:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

und

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

3. Es ist $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ und die Addition und Multiplikation sind wie in den folgenden Tabellen gegeben:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

und

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

4. Für $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ sind die Tabellen der Addition und Multiplikation gegeben durch

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

und

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

5. Man beachte, dass die obigen Tabelle alle symmetrisch sind, da die Addition und Multiplikation kommutativ sind.

6. In $\mathbb{F}_{11}$ gilt etwa $1/9 = 5$ und $1/7 = 8$, sowie $10 + 6 + 8 - 5 = 8$.

7. Wir wollen die Matrix $A \in \mathrm{Mat}(4 \times 5, \mathbb{F}_{11})$ mit

$$A = \begin{pmatrix} 4 & 9 & 6 & 3 & 2 \\ 3 & 9 & 6 & 10 & 10 \\ 5 & 5 & 5 & 5 & 2 \\ 0 & 8 & 8 & 1 & 1 \end{pmatrix}$$

durch elementare Zeilenumformungen in Zeilenstufenform bringen. Da wir uns über $\mathbb{F}_{11}$

bewegen, müssen wir hierfür nicht mit Brüchen hantieren.

$$\begin{pmatrix} 4 & 9 & 6 & 3 & 2 \\ 3 & 9 & 6 & 10 & 10 \\ 5 & 5 & 5 & 5 & 2 \\ 0 & 8 & 8 & 1 & 1 \end{pmatrix} \xrightarrow[3\mathrm{I}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 3 & 9 & 6 & 10 & 10 \\ 5 & 5 & 5 & 5 & 2 \\ 0 & 8 & 8 & 1 & 1 \end{pmatrix} \xrightarrow[\substack{\mathrm{II}+8\mathrm{I} \\ \mathrm{III}+6\mathrm{I}}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 0 & 5 & 7 & 5 & 3 \\ 0 & 2 & 3 & 4 & 5 \\ 0 & 8 & 8 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow[9\mathrm{II}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 0 & 1 & 8 & 1 & 5 \\ 0 & 2 & 3 & 4 & 5 \\ 0 & 8 & 8 & 1 & 1 \end{pmatrix} \xrightarrow[\substack{\mathrm{III}+9\mathrm{II} \\ \mathrm{IV}+3\mathrm{II}}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 0 & 1 & 8 & 1 & 5 \\ 0 & 0 & 9 & 2 & 6 \\ 0 & 0 & 10 & 4 & 5 \end{pmatrix}$$

$$\xrightarrow[5\mathrm{III}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 0 & 1 & 8 & 1 & 5 \\ 0 & 0 & 1 & 10 & 8 \\ 0 & 0 & 10 & 4 & 5 \end{pmatrix} \xrightarrow[\mathrm{IV}+\mathrm{III}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 0 & 1 & 8 & 1 & 5 \\ 0 & 0 & 1 & 10 & 8 \\ 0 & 0 & 0 & 3 & 2 \end{pmatrix}$$

$$\xrightarrow[4\mathrm{IV}]{} \begin{pmatrix} 1 & 5 & 7 & 9 & 6 \\ 0 & 1 & 8 & 1 & 5 \\ 0 & 0 & 1 & 10 & 8 \\ 0 & 0 & 0 & 1 & 8 \end{pmatrix} \xrightarrow[\substack{\mathrm{I}+2\mathrm{IV} \\ \mathrm{II}+10\mathrm{IV} \\ \mathrm{III}+\mathrm{IV}}]{} \begin{pmatrix} 1 & 5 & 7 & 0 & 0 \\ 0 & 1 & 8 & 0 & 8 \\ 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 8 \end{pmatrix}$$

$$\xrightarrow[\substack{\mathrm{I}+4\mathrm{III} \\ \mathrm{II}+3\mathrm{III}}]{} \begin{pmatrix} 1 & 5 & 0 & 0 & 9 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 8 \end{pmatrix} \xrightarrow[\mathrm{I}+6\mathrm{II}]{} \begin{pmatrix} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 8 \end{pmatrix}$$

3.6. Quadratische Körpererweiterungen

Definition 3.3. *Es sei K ein Körper und $x \in K$. Ein Element $y \in K$ heißt* Quadratwurzel von x, *falls $y^2 = x$.*

Beispiel(e). 1. Für $K = \mathbb{C}$ ist $i^2 = -1$, also ist i eine Quadratwurzel von -1. Analog ist auch $-i$ eine Quadratwurzel von -1.

2. Für $K = \mathbb{R}$ ist $x^2 \leq 0$ für alle $x \in \mathbb{R}$ und somit $x^2 \neq -1$ für alle $x \in \mathbb{R}$. Also hat -1 keine Quadratwurzel in $\mathbb{R}$.

3. Für $K = \mathbb{Q}$ ist $4/9 = (2/3)^2 = (-2/3)^2$, also sind $2/3$ und $-2/3$ Quadratwurzeln von $2/3$. Da $x^2 \neq 2$ für alle $x \in \mathbb{Q}$ hat 2 keine Quadratwurzel in $\mathbb{Q}$.

4. Ist $x \in K$ und $y \in K$ eine Quadratwurzel von x, so ist auch $-y$ eine Quadratwurzel von x, da dann $(-x)^2 = x^2 = y$. Dies sind dann die einzigen beiden Quadratwurzeln von x: Ist $z \in K$ eine Quadratwurzel von x, so ist

$$0 = x - x = z^2 - y^2 = (z - y)(z + y),$$

also $z - y = 0$ oder $z + y = 0$, und somit $z = y$ oder $z = -y$.

5. Für $K = \mathbb{F}_3$ ist $0^2 = 0$, $1^2 = 1$ und $2^2 = 1$, also hat $2 \in \mathbb{F}_3$ keine Quadratwurzel.

6. Für $K = \mathbb{F}_5$ ist $0^2 = 0$, $1^2 = 4^2 = 1$ und $2^2 = 3^2 = 4$, also haben 0, 1 und 4 Quadratwurzeln in $\mathbb{F}_5$, und 2 und 3 keine Quadratwurzeln in $\mathbb{F}_5$.

7. Für $K = \mathbb{F}_7$ ist $0^2 = 0$, $1^2 = 6^2 = 1$, $2^2 = 5^2 = 4$ und $3^2 = 4^2 = 2$. Also haben 0, 1, 2 und 4 Quadratwurzeln in $\mathbb{F}_7$, und 3, 5 und 6 haben keine Quadratwurzeln in $\mathbb{F}_7$.

8. Ist $y \in K$ eine Quadratwurzel von $x \in K$, so mag es naheliegend sein, dies als $y = \sqrt{x}$ zu schreiben. Wir wollen hier vor dieser Notation warnen: Wie bereits gesehen, ist auch $-y$ eine Quadratwurzel von x, und ist $\mathrm{char}(K) \neq 2$, so ist $y \neq -y$. Der Ausdruck $\sqrt{x}$ ist daher a priori nicht eindeutig definiert.

   Im Falle von $K = \mathbb{R}$ ist es möglich, $\sqrt{x}$ konsistent als die nicht-negative der beiden Wurzeln y und $-y$ zu definieren; in diesem Sonderfall werden wir daher die Notation $\sqrt{x}$ für $x \in \mathbb{R}$ mit $x \geq 0$ nutzen.

Die komplexen Zahlen $\mathbb{C}$ entstehen aus den reellen Zahlen $\mathbb{R}$ durch hinzufügen einer Quadratwurzel von -1, d.h. eines Elementes i mit $i^2 = -1$. Wir wollen hier noch weiter Beispiele von Körpern angeben, die durch hinzufügen von Quadratwurzeln aus bereits bekannten Körpern entstehen.

3.6.1. Der Körper $\mathbb{Q}[i]$

Es sei

$$\mathbb{Q}[i] \coloneqq \{q_1 + q_2 i \mid q_1, q_2 \in \mathbb{Q}\} \subseteq \mathbb{C}$$

Wir zeigen, dass $\mathbb{Q}[i]$ ein Unterkörper von $\mathbb{C}$ ist. (Man bezeichnet $\mathbb{Q}[i]$ als „$\mathbb{Q}$ adjungiert i“.)

Es ist $0 = 0 + 0 \cdot i \in \mathbb{Q}[i]$. Für $z, w \in \mathbb{Q}[i]$ ist $z = q_1 + q_2 i$ und $w = p_1 + p_2 i$ mit $q_1, q_2, p_1, p_2 \in \mathbb{Q}$. Daher ist auch

$$z + w = (q_1 + q_2 i) + (p_1 + p_2 i) = (q_1 + p_1) + (q_2 + p_2)i \in \mathbb{Q}[i].$$

Ist $z \in \mathbb{Q}$ so ist $z = q_1 + q_2 i$ mit $q_1, q_2 \in \mathbb{Q}$, weshalb auch

$$-z = -(q_1 + q_2 i) = (-q_1) + (-q_2)i \in \mathbb{Q}[i].$$

Das zeigt, dass $\mathbb{Q}[i]$ eine Untergruppe der additiven Gruppe von $\mathbb{C}$ ist.

Es ist auch $1 = 1 + 0 \cdot i \in \mathbb{Q}[i]$. Sind $z, w \in \mathbb{Q}[i]$ so gibt es $q_1, q_2, p_1, p_2 \in \mathbb{Q}$ mit $z = q_1 + iq_2$ und $w = p_1 + ip_2$. Es ist daher auch

$$z \cdot w = (q_1 + iq_2)(p_1 + ip_2) = (q_1 p_1 - q_2 p_2) + i(q_1 p_2 + q_2 p_1) \in \mathbb{Q}[i].$$

Ist $z \in \mathbb{C}[i]$ mit $z \neq 0$ so ist $z = q_1 + iq_2$ mit $q_1, q_2 \in \mathbb{Q}$ und $q_1 \neq 0$ oder $q_2 \neq 0$. Da $z \neq 0$ ist auch $q_1 - iq_2 = \overline{z} \neq 0$ Deshalb ist auch

$$\frac{1}{z} = \frac{1}{q_1 + iq_2} = \frac{q_1 - iq_2}{(q_1 + iq_2)(q_1 - iq_2)} = \frac{q_1 - iq_2}{q_1^2 + q_2^2} = \frac{q_1}{q_1^2 + q_2^2} + i\frac{-q_2}{q_1^2 + q_2^2} \in \mathbb{Q}[i].$$

Ingesamt zeigt dies, dass $\mathbb{Q}[i]$ ein Unterkörper von $\mathbb{C}$ ist. $\mathbb{Q}[i]$ ist der kleinste Unterkörper von $\mathbb{C}$, der i enthält, d.h. ist $K \subseteq \mathbb{C}$ ein Unterkörper mit $i \in K$, so ist bereits $\mathbb{Q}[i] \subseteq K$.

3.6.2. Der Körper $\mathbb{Q}\left[\sqrt{2}\right]$

Nach gleichen Prinzip zeigen wir, dass

$$\mathbb{Q}\left[\sqrt{2}\right] \coloneqq \{q_1 + q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\} \subseteq \mathbb{R}$$

ein Unterkörper von $\mathbb{R}$ ist. (Man bezeichnet $\mathbb{Q}\left[\sqrt{2}\right]$ als „$\mathbb{Q}$ adjungiert $\sqrt{2}$“.)

Es ist $0 = 0 + 0 \cdot 0 \in \mathbb{Q}\left[\sqrt{2}\right]$. Sind $x, y \in \mathbb{Q}\left[\sqrt{2}\right]$, so gibt es $q_1, q_2, p_1, p_2 \in \mathbb{Q}$ mit $x = q_1 + q_2\sqrt{2}$ und $y = p_1 + p_2\sqrt{2}$. Es ist daher auch

$$x + y = (q_1 + q_2\sqrt{2}) + (p_1 + p_2\sqrt{2}) = (q_1 + p_1) + (q_2 + p_2)\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right].$$

Ist $x \in \mathbb{Q}\left[\sqrt{2}\right]$ mit $x = q_1 + q_2\sqrt{2}$ für $q_1, q_2 \in \mathbb{Q}$, so ist auch

$$-x = -(q_1 + q_2\sqrt{2}) = (-q_1) + (-q_2)\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right].$$

Das zeigt, dass $\mathbb{Q}\left[\sqrt{2}\right]$ eine Untergruppe der additiven Gruppe von $\mathbb{R}$ ist.

Bemerkung 3.4. Die obigen Rechnungen lassen sich auch großteils umgehen: Die Abbildung $\varphi\colon \mathbb{Q}^2 \to \mathbb{R}$, $(q_1, q_2) \to \mathbb{Q}\left[\sqrt{2}\right]$ ist ein Gruppenhomomorphismus, da

$$\begin{aligned}\varphi((q_1, q_2) + (p_1, p_2)) &= \varphi((q_1 + p_1, q_2 + p_2)) = (q_1 + p_1) + (q_2 + p_2)\sqrt{2} \\ &= (q_1 + q_2\sqrt{2}) + (p_1 + p_2\sqrt{2}) = \varphi((q_1, q_2)) + \varphi((p_1, p_2))\end{aligned}$$

für alle $(q_1, q_2), (p_1, p_2) \in \mathbb{Q}^2$. Daher ist

$$\mathbb{Q}\left[\sqrt{2}\right] = \{q_1 + q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\} = \operatorname{im}(\varphi)$$

eine Untergruppe der additiven Gruppe von $\mathbb{R}$.

Es ist $1 = 1 + 0 \cdot \sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$. Für $x, y \in \mathbb{Q}\left[\sqrt{2}\right]$ ist $x = q_1 + q_2\sqrt{2}$ und $y = p_1 + p_2\sqrt{2}$ mit $q_1, q_2, p_1, p_2 \in \mathbb{Q}$. Deshalb ist auch

$$x \cdot y = (q_1 + q_2\sqrt{2})(p_1 + p_2\sqrt{2}) = q_1q_2 + 2p_1p_2 + (q_1p_2 + q_2p_1)\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right].$$

Es sei $x \in \mathbb{Q}\left[\sqrt{2}\right]$ mit $x \neq 0$. Dann ist $x = q_1 + q_2\sqrt{2}$ mit $q_1, q_2 \in \mathbb{Q}$. Da $x \neq 0$ ist $q_1 \neq 0$ oder $q_2 \neq 0$. Es folgt, dass auch $q_1 - q_2\sqrt{2} \neq 0$. Andernfalls wäre nämlich $\sqrt{2} = q_1/q_2$ (falls $q_2 \neq 0$) oder $1/\sqrt{2} = q_2/q_1$ und somit ebenfalls $\sqrt{2} = q_1/q_2$ (falls $q_1 \neq 0$). Dies stünde im Widerspruch zur Irrationalität von $\sqrt{2}$. Es folgt, dass auch

$$\begin{aligned}\frac{1}{x} &= \frac{1}{q_1 + q_2\sqrt{2}} = \frac{q_1 - q_2\sqrt{2}}{(q_1 + q_2\sqrt{2})(q_1 - q_2\sqrt{2})} \\ &= \frac{q_1 - q_2\sqrt{2}}{q_1^2 - 2q_2^2} = \frac{q_1}{q_1^2 - 2q_2^2} + \frac{-q_2}{q_1^2 - 2q_2^2}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right].\end{aligned}$$

Insgesamt zeigt dies, dass $\mathbb{Q}\left[\sqrt{2}\right]$ ein Unterkörper von $\mathbb{R}$ ist. Man bezeichnet $\mathbb{Q}[\sqrt{2}]$ als „$\mathbb{Q}$ adjungiert $\sqrt{2}$“. $\mathbb{Q}\left[\sqrt{2}\right]$ ist der kleinste Unterkörper von $\mathbb{R}$, der $\sqrt{2}$ enthält, d.h. ist $K \subseteq \mathbb{R}$ ein Unterkörper mit $\sqrt{2} \in K$, so ist bereits $\mathbb{Q}\left[\sqrt{2}\right] \subseteq K$.

3.6.3. $K[\alpha]$ mit $\alpha \notin K$ und $\alpha^2 \in K$

Die Konstruktion von $\mathbb{Q}[i]$ und $\mathbb{Q}\left[\sqrt{2}\right]$ lässt sich wie folgt verallgemeimern: Es sei L ein Körper und $K \subseteq L$ ein Unterkörper. Es gebe ein Element $d \in K$, das in K keine Quadratwurzel besitzt, d.h. $x^2 \neq d$ für alle $x \in K$, das aber in L eine Quadratwurzel ω besitzt, also $\omega \in L$ mit $\omega^2 = d$. Dann ist

$$K[\omega] \coloneqq \{x + y\omega \mid x, y \in K\}$$

ein Unterkörper von L. $K[\omega]$ ist dann der kleinste Unterkörper von L, der K und ω enthält. Wir zeigen, dass $K[\omega]$ ein Unterkörper von L ist:

Es ist $0 = 0 + 0 \cdot \omega \in K[\omega]$. Für $z_1, z_2 \in K[\omega]$ gibt es $x_1, y_1, x_2, y_2 \in \mathbb{R}$ mit $z_1 = x_1 + y_1\omega$ und $z_2 = x_2 + y_2\omega$, weshalb auch

$$z_1 + z_2 = (x_1 + y_1\omega) + (x_2 + y_2\omega) = (x_1 + x_2) + (y_1 + y_2)\omega \in K[\omega].$$

Für $z \in K[\omega]$ gibt es es $x, y \in K$ mit $z = x + y\omega$, weshalb auch

$$-z = -(x + y\omega) = (-x) + (-y)\omega \in K[\omega].$$

Das zeigt, dass $K[\omega]$ eine Untergruppe der additiven Gruppe von L ist.

Bemerkung 3.5. Auch hier lässt sich die Rechnung damit abkürzen, dass die Abbildung $\varphi\colon K^2 \to L, (x, y) \mapsto x + y\omega$ ein Gruppenhomomorphismus ist, da

$$\begin{aligned}\varphi((x, y) + (x', y')) &= \varphi(x + x', y + y') \\ &= (x + x') + (y + y')\omega = (x + y\omega) + (x' + y'\omega)\end{aligned}$$

für alle $(x, y), (x', y') \in K^2$, und somit

$$\operatorname{im}(\varphi) = \{\varphi((x, y)) \mid (x, y) \in K^2\} = \{x + y\omega \mid x, y \in K\} = K[\omega]$$

eine Untergruppe.

Es ist $1 = 1 + 0 \cdot \omega \in K[\omega]$. Für $z_1, z_2 \in K[\omega]$ gibt es $x_1, x_2, y_1, y_2 \in K$ mit $z_1 = x_1 + y_1\omega$ und $z_2 = x_2 + y_2\omega$. Da $\omega^2 = d \in K$ ist

$$z_1 \cdot z_2 = (x_1 + y_1\omega)(x_2 + y_2\omega) = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\omega \in K[\omega].$$

Ist $z \in K[\omega]$ mit $z \neq 0$, so gibt es $x, y \in K$ mit $z = x + y\omega$ und $x \neq 0$ oder $y \neq 0$. Dann ist auch $x - y\omega \neq 0$. Ansonsten wäre nämlich $\omega = x/y \in K$ (falls $y \neq 0$) oder $\omega^{-1} = y/x \in K$ (falls $x \neq 0$) und somit auch dann $\omega = x/y \in K$. Dies wiederspräche aber der Annahme, dass $\omega \notin K$ (da $a^2 \neq d$ für alle $a \in K$). Deshalb ist auch

$$\frac{1}{z} = \frac{1}{x + y\omega} = \frac{x - y\omega}{(x + y\omega)(x - y\omega)} = \frac{x - y\omega}{x^2 + dy^2} = \frac{x}{x^2 + dy^2} + \frac{-y}{x^2 + dy^2}\omega \in K[\omega].$$

Ingesamt zeigt dies, dass $K[\omega]$ ein Unterkörper von L ist.

3.6.4. Formales Hinzufügen von Wurzeln

Das vorherige Beispiel zeigt: Ist K ein Körper und besitzt $d \in K$ keine Quadratwurzel, und gibt es einen größeren Körper $L \supsetneq K$, in dem d ein Quadratwurzel besitzt, so lässt sich K zu einem neuem Körper K' erweitern, in dem d eine Quadratwurzel besitzt (nämlich eine aus L). Das „Problem“ hierbei ist allerdings, dass diese Konstruktion auf den größeren Körper L angewiesen ist, in dem eine entsprechende Quadratwurzel existiert.

Wir wollen hier noch zeigen, wie man zu einem beliebigen Körper auf formale Art und Weise Quadratwurzeln hinzufügen kann. Die Konstruktion läuft analog dazu, wie sich $\mathbb{C}$ als besserer $\mathbb{R}^2$ konstruieren lässt.

Es sei also K ein Körper und es sei $d \in K$ ein Element, dass keine Quadratwurzel in K besitzt, d.h. $x^2 \neq d$ für alle $x \in K$. Wir definieren $L \coloneqq K^2$. L ist eine abelsche Gruppe mit der Addition

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{für alle } x, x', y, y' \in K.$$

Wir definieren auf L eine Multiplikation $\cdot$ durch

$$(x_1, y_1) \cdot (x_2, y_2) \coloneqq (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1).$$

Wir zeigen, dass diese Multiplikation die abelsche Gruppe L zu einem Körper erweitert: Die Multiplikation ist assoziativ, denn für alle $x_1, x_2, x_3, y_1, y_2, y_3 \in K$ ist

$$\begin{aligned}
&(x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)) \\
&= (x_1, y_1) \cdot (x_2x_3 + dy_2y_3, x_2y_3 + x_3y_2) \\
&= (x_1(x_2x_3 + dy_2y_3) + dy_1(x_2y_3 + x_3y_2), x_1(x_2y_3 + x_3y_2) + (x_2x_3 + dy_2y_3)y_1) \\
&= (x_1x_2x_3 + dx_1y_2y_3 + dx_2y_1y_3 + dx_3y_1y_2, x_1x_2y_3 + x_1x_3y_2 + x_2x_3y_1 + dy_1y_2y_3) \\
&= ((x_1x_2 + dy_1y_2)x_3 + d(x_1y_2 + x_2y_1)y_3, (x_1x_2 + dy_1y_2)y_3 + x_3(x_1y_2 + x_2y_1)) \\
&= (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1) \cdot (x_3, y_3) \\
&= ((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3).
\end{aligned}$$

Die Multiplikation ist kommutativ, da für alle $x_1, x_2, y_1, y_2 \in K$

$$\begin{aligned}
(x_1, y_1) \cdot (x_2, y_2) &= (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1) \\
&= (x_2x_1 + dy_2y_1, x_2y_1 + x_1y_2) = (x_2, y_2) \cdot (x_1, y_1).
\end{aligned}$$

Für alle $x, y \in K$ ist

$$(1, 0) \cdot (x, y) = (1 \cdot x + d \cdot 0 \cdot y, 1 \cdot y + 0 \cdot x) = (x, y),$$

also ist $(1, 0)$ neutral bezüglich der Multiplikation. Für $(x, y) \in L$ mit $(x, y) \neq 0$ ist $x \neq 0$ oder $y \neq 0$. Dann ist $x^2 - dy^2 \neq 0$: Ansonsten wäre $d = (x/y)^2$ (falls $y \neq 0$) oder $1/d = (y/x)^2$ (falls $x \neq 0$) und somit ebenfalls $d = (x/y)^2$. Dies würde im Widerspruch dazu stehen, dass d keine Quadratwurzel in K hat. Da also $x^2 - dy^2 \neq 0$ ist

$$\begin{aligned}
&(x, y) \cdot \left(\frac{x}{x^2 - dy^2}, \frac{-y}{x^2 - dy^2} \right) \\
&= \left(x\frac{x}{x^2 - dy^2} + dy\frac{-y}{x^2 - dy^2}, x\frac{-y}{x^2 - dy^2} + y\frac{x}{x^2 - dy^2} \right) = (1, 0),
\end{aligned}$$

weshalb $(x/(x^2 - dy^2), -y/(x^2 - dy^2))$ multiplikativ invers zu (x, y) ist.

Insgesamt zeigt dies, dass L zusammen mit der angegebenen Addition und Multiplikation ein Körper ist.

Wie bereits bei der Konstruktion von $\mathbb{C}$ führen wir noch Notation ein: Wir schreiben $1 = (1, 0)$ und $0 = (0, 0)$. Wir bemerken zunächst, dass für alle $x, x' \in K$

$$(x, 0) + (x', 0) = (x + x', 0)$$

und

$$(x, 0) \cdot (x', 0) = (x \cdot x' + 0 \cdot 0, x \cdot 0 + 0 \cdot x') = (x \cdot x', 0).$$

Die Abbildung $\phi\colon K \to L, x \mapsto (x, 0)$ ist also ein Körperhomomorphismus. Deshalb ist das Bild $\operatorname{im}(\phi) = \{(x, 0) \mid x \in K\} \subseteq L$ ein Unterkörper, den wir durch ϕ mit K identifizieren. Wir unterscheiden also nicht zwischen dem Element $x \in K$ und dem entsprechenden Tupel $\phi(x) = (x, 0) \in L$.

Wir schreiben außerdem $\alpha := (0, 1) \in L$. Man bemerke, dass

$$\alpha^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 + d \cdot 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (d, 0) = d.$$

Also ist α eine Quadratwurzel von d in L. Für alle $y \in K$ gilt

$$y\alpha = (y, 0) \cdot (0, 1) = (y \cdot 0 + d \cdot 0 \cdot 1, y \cdot 1 + 0 \cdot 0) = (0, y).$$

Für alle $x, y \in L$ gilt deshalb

$$(x, y) = (x, 0) + (0, y) = x + y\alpha.$$

Mit den obigen Notationen erhalten wir also, dass

$$L = \{x + y\alpha \mid x, y \in K\}$$

und $\alpha^2 = d$, und für jedes $z \in L$ ist die Zerlegung $z = x + y\alpha$ mit $x, y \in K$ eindeutig.

Beispiel(e). 1. Für $K = \mathbb{R}$ und $d = -1$ ergibt sich die Konstruktion von $\mathbb{C}$ aus 3.4.1.

2. Für $K = \mathbb{F}_3$ und $d = 2 \in \mathbb{F}_3$ besitzt d keine Quadratwurzeln in $\mathbb{F}_3$, da $0^2 = 0$ und $1^1 = 2^2 = 1$. Die obige Konstruktion liefert einen neuen Körper

   $$L = \{x + y\alpha \mid x, y \in \mathbb{F}_3 \ = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\},$$

   so dass $\mathbb{F}_3 \subseteq L$ ein Unterkörper ist, und $\alpha^2 = d = 2$.

3. Für $K = \mathbb{F}_7$ hat $d = 3$ keine Quadratwurzel in $\mathbb{F}_7$, da $0^0 = 0$, $1^1 = 6^2 = 1$, $2^2 = 5^2 = 4$ und $3^2 = 4^2 = 2$. Die obige Konstruktion liefert dann einen neuen Körper

   $$L = \{x + y\alpha \mid x, y \in \mathbb{F}_7\},$$

   so dass $\mathbb{F}_7 \subseteq L$ ein Unterkörper ist, und $\alpha^2 = d = 3$. Auch 5 und 6 haben in $\mathbb{F}_7$ keine Quadratwurzeln. Da aber

   $$(2\alpha)^2 = 4\alpha^2 = 4 \cdot 3 = 5 \quad \text{und} \quad (3\alpha)^2 = 3^2 \cdot \alpha^2 = 2 \cdot 3 = 6$$

   besitzen auch diese beiden Element Quadratwurzeln in L. Es besitzt also schon jedes Element aus $\mathbb{F}_7$ eine Quadratwurzel in L, obwohl bei der Konstruktion von L nur eine Quadratwurzel von 3 hinzugefügt wurde.

3.7. Quotientenkörper

3.8. Primkörper eines Körpers

Definition 3.6. *Für einen Körper K und $U = \{L \subseteq K \mid L \text{ ist ein Unterkörper von } K\}$ heißt*

$$P(K) := \bigcap_{L \in U} L$$

der Primkörper *von K.*

Es sei K ein Körper. Da Schnitte von Unterkörpern wieder Unterkörper sind, ist $P(K)$ ein Unterkörper von K. $P(K)$ ist der *kleinste* Unterkörper von K, d.h. ist $L \subseteq K$ ein Unterkörper, so ist $P(K) \subseteq L$. Dies folgt direkt daraus, dass $P(K)$ der Schnitt *aller* Unterkörper von K ist.

Wir untersuchen im Folgenden, wie $P(K)$ aussieht, und zeigen, dass es einen eindeutigen Isomorphismus von Körpern $\mathbb{Q} \to P(K)$ gibt falls $\text{char}(K) = 0$, und einen eindeutigen Isomorphismus von Körpern $\mathbb{F}_p \to P(K)$ falls $\text{char}(K) = p > 0$.

3.8.1. Körper mit Charakteristik p

Wir betrachten zunächst den Falls, dass $\text{char}(K) = p > 0$.

Wir zeigen zunächst die Eindeutigkeit, d.h. dass es höchstens einen Körperhomomorphismus $\mathbb{F}_p \to P(K)$ gibt: Sind nämlich $\phi, \psi \colon \mathbb{F}_p \to P(K)$ zwei Körperhomomorphismen, so ist für alle $n \in \mathbb{Z}$

$$\phi([n]) = \phi(n \cdot [1]) = n \cdot \phi([1]) = n \cdot \phi(1_{\mathbb{F}_p}) = n \cdot 1_K.$$

Analog ist für alle $n \in \mathbb{Z}$ auch $\psi([n]) = n \cdot 1_K$ und somit $\psi([n]) = \psi([n])$. Also ist bereits $\phi = \psi$. Das zeigt die Eindeutigkeit.

Um die Existenz zu zeigen konstruieren wir einen Isomorphismus $\mathbb{F}_p \to K$. Wie dieser aussehen muss, wissen wir aus dem obigen Beweis der Eindeutigkeit; es sei also

$$\tilde{\phi} \colon \mathbb{F}_p \to K, \quad [n] \mapsto n \cdot 1_K.$$

$\tilde{\phi}$ ist wohldefiniert, denn sind $n, m \in \mathbb{Z}$ mit $[n] = [m]$, so ist $n - m = pk$ für ein $k \in \mathbb{Z}$, weshalb

$$n \cdot 1_K = (m + (n - m)) \cdot 1_K = m \cdot 1_K + (n - m) \cdot 1_K = m \cdot 1_K + pk \cdot 1_K = m \cdot 1_K.$$

Dabei nutzen wir, dass $pk \cdot 1_K = 0$, da $\text{char}(K) = p$. $\tilde{\phi}$ ist ein Körperhomomorphismus, denn es ist $\tilde{\phi}(1_{\mathbb{F}_p}) = \tilde{\phi}([1]) = 1 \cdot 1_K = 1_K$, und für alle $n, m \in \mathbb{Z}$ ist

$$\tilde{\phi}([n] \cdot [m]) = \tilde{\phi}([nm]) = (nm) \cdot 1_K = (n \cdot 1_K) \cdot (m \cdot 1_K) = \tilde{\phi}([n]) \cdot \tilde{\phi}([m])$$

und

$$\tilde{\phi}([n] + [m]) = \tilde{\phi}([n + m]) = (n + m) \cdot 1_K = (n \cdot 1_K) + (m \cdot 1_K) = \tilde{\phi}([n]) + \tilde{\phi}([m]).$$

Da $\tilde{\phi}$ ein Körperhomomorphismus ist, ist $P := \mathrm{im}(\tilde{\phi}) \subseteq K$ ein Unterkörper. Indem wir den Bildbereich von K auf P einschränken, schränkt sich $\tilde{\phi}$ zu einer Abbildung $\phi\colon \mathbb{F}_p \to P$, $x \mapsto \tilde{\phi}(x)$ ein. ϕ ist dann ein surjektiver Körperhomomorphismus. Da Körperhomomorphismen stets injektiv sind, ist ϕ auch injektiv, und somit bereits ein Körper*isomorphismus*.

Da $\mathbb{F}_p = \{[0], \dots, [p-1]\}$ und ϕ bijektiv ist, ist

$$\begin{aligned} P = \mathrm{im}(\tilde{\phi}) = \mathrm{im}(\phi) &= \{\phi([0]), \dots, \phi([p-1])\} \\ &= \{0 \cdot 1_K, \dots, (p-1) \cdot 1_K\} = \{0, 1_K, 2 \cdot 1_K, \dots, (p-1) \cdot 1_K\}. \end{aligned}$$

Da P ein Unterkörper von K ist, und $P(K)$ der kleinste Unterkörper von K ist, folgt zum einen, dass $P(K) \subseteq P$. Da $0, 1_K \in P(K)$ und $P(K)$ unter Summen abgeschlossen ist, ist auch $P(K) \subseteq P$. Somit ist $P = P(K)$ der Primkörper von K. Deshalb ist $\phi\colon \mathbb{F}_p \to P(K)$, $[n] \mapsto n \cdot 1_K$ ein Körperisomorphismus.

Damit haben wir insgesamt gezeigt, dass $P(K) = \{0, 1_K, \dots, (p-1) \cdot 1_K\}$, dass die Abbildung $\mathbb{F}_p\colon P(K)$, $[n] \mapsto n \cdot 1_K$ ein Körperisomorphismus ist, und dass dies der einzige Körperisomorphismus $\mathbb{F}_p \to P(K)$ ist.

3.8.2. Körper mit Charakteristik 0

Nun betrachten wir den Fall, dass $\mathrm{char}(K) = 0$, wobei wir uns am Vorgehen des Falls $\mathrm{char}(K) = p > 0$ orientieren:

Sind $\phi, \psi\colon \mathbb{Q} \to P(K)$ zwei Körperisomorphismen, so ist

$$\phi(n) = \phi(n \cdot 1) = n \cdot \phi(1) = n \cdot 1_K \quad \text{für alle } n \in \mathbb{Z}.$$

Analog ergibt sich, dass auch $\psi(n) = n \cdot 1_K$ für alle $n \in \mathbb{Z}$. Also ist bereits $\phi(n) = \psi(n)$ für alle $n \in \mathbb{Z}$. Sind nun $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ mit $q > 0$, so ist

$$(q \cdot 1_K) \cdot \phi\left(\frac{p}{q}\right) = \phi(q) \cdot \phi\left(\frac{p}{q}\right) = \phi\left(q \cdot \frac{p}{q}\right) = \phi(p) = p \cdot 1_K.$$

Da $\mathrm{char}(K) = 0$ ist $q \cdot 1_K \neq 0$, durch Teilen von $q \cdot 1_K$ auf beiden Seiten der obigen Gleichung ergibt sich damit, dass

$$\phi\left(\frac{p}{q}\right) = \frac{p \cdot 1_K}{q \cdot 1_K}.$$

Analog ergibt sich, dass auch $\psi(p/q) = (p \cdot 1_K)/(q \cdot 1_K)$. Also ist $\phi(x) = \psi(x)$ für alle $x \in \mathbb{Q}$ und somit $\phi = \psi$. Das zeigt die Eindeutigkeit.

Wir zeigen die Existenz eines Isomorphismus $\mathbb{Q} \to P(K)$, indem wir diesen explizit konstruieren. Dabei wissen wir aus der obigen Definition der Eindeutigkeit, wie dieser aussehen muss: Es sei

$$\tilde{\phi}\colon \mathbb{Q} \to K, \quad \frac{p}{q} \mapsto \frac{p \cdot 1_K}{q \cdot 1_K}.$$

Wir zeigen zunächst, dass $\tilde{\phi}$ wohldefiniert ist: Ist $q \in \mathbb{Z}$ mit $q \neq 0$, so ist $q \cdot 1_K \neq 0$. Also ist der Quotient $(p \cdot 1_K)/(q \cdot 1_K)$ für alle $p, q \in \mathbb{Z}$ mit $q \neq 0$ definiert. Sind $p_1, p_2, q_1, q_2 \in \mathbb{Z}$

mit $q_1, q_2 \neq 0$, so ist

$$\begin{aligned}\frac{p_1 \cdot 1_K}{q_1 \cdot 1_K} = \frac{p_2 \cdot 1_K}{q_2 \cdot 1_K} &\iff (p_1 \cdot 1_K)(q_2 \cdot 1_K) = (p_2 \cdot 1_K)(q_1 \cdot 1_K) \\ &\iff (p_1 q_2) \cdot 1_K = (p_2 q_1) \cdot 1_K \iff (p_1 q_2 - p_2 q_1) \cdot 1_K = 0.\end{aligned}$$

da $\operatorname{char}(K) = 0$ ist genau dann $(p_1 q_2 - p_2 q_1) \cdot 1_K = 0$, wenn $p_1 q_2 - p_2 q_1 = 0$, was wiederum äquivalent dazu ist, dass $p_1/q_1 = p_2/q_2$. Ist also $p_1/q_1 = p_2/q_2$, so ist deshalb $(p_1 \cdot 1_K)/(q_1 \cdot 1_K) = (p_2 \cdot 1_K)/(q_2 \cdot 1_K)$. Also ist $(p \cdot 1_K)/(q \cdot 1_K)$ von der Wahl des Repräsentanten p/q unabhängig, und die Abbildung $\tilde{\phi}$ somit wohldefiniert.

Die Abbildung $\tilde{\phi}$ ist ein Körperhomomorphismus, denn es ist

$$\tilde{\phi}(1_{\mathbb{Q}}) = \tilde{\phi}\left(\frac{1}{1}\right) = \frac{1 \cdot 1_K}{1 \cdot 1_K} = \frac{1_K}{1_K} = 1_K,$$

und für alle $p_1/q_1, p_2/q_2 \in \mathbb{Q}$ ist

$$\begin{aligned}\tilde{\phi}\left(\frac{p_1}{q_1} \cdot \frac{p_2}{q_2}\right) = \tilde{\phi}\left(\frac{p_1 p_2}{q_1 q_2}\right) &= \frac{(p_1 p_2) \cdot 1_K}{(q_1 q_2) \cdot 1_K} = \frac{(p_1 \cdot 1_K) \cdot (p_2 \cdot 1_K)}{(q_1 \cdot 1_K) \cdot (q_2 \cdot 1_K)} \\ &= \frac{p_1 \cdot 1_K}{q_1 \cdot 1_K} \cdot \frac{p_2 \cdot 1_K}{q_2 \cdot 1_K} = \tilde{\phi}\left(\frac{p_1}{q_1}\right) \cdot \tilde{\phi}\left(\frac{p_2}{q_2}\right).\end{aligned}$$

und

$$\begin{aligned}\tilde{\phi}\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right) = \tilde{\phi}\left(\frac{p_1 q_2 + p_2 q_1}{q_1 q_2}\right) &= \frac{(p_1 q_2 + p_2 q_1) \cdot 1_K}{(q_1 q_2) \cdot 1_K} \\ &= \frac{(p_1 \cdot 1_K) \cdot (q_2 \cdot 1_K) + (p_2 \cdot 1_K) \cdot (q_1 \cdot 1_K)}{(q_1 \cdot 1_K) \cdot (q_2 \cdot 1_K)} \\ &= \frac{p_1 \cdot 1_K}{q_1 \cdot 1_K} \cdot \frac{p_2 \cdot 1_K}{q_2 \cdot 1_K} = \tilde{\phi}\left(\frac{p_1}{q_1}\right) \cdot \tilde{\phi}\left(\frac{p_2}{q_2}\right).\end{aligned}$$

Da $\tilde{\phi}$ ein Körperhomomorphismus ist, ist $P \coloneqq \operatorname{im}(\tilde{\phi})$ ein Unterkörper von K. Indem wir den Bildbereich von $\tilde{\phi}$ von K auf P einschränken erhalten wir einen surjektiven Körperhomomorphismus $\phi\colon \mathbb{Q} \to P$, $x \mapsto \tilde{\phi}(x)$. Da Körperhomomorphismen stets injektiv sind, ist ϕ auch injektiv. Somit ist ϕ bereits ein Körperisomorphismus.

Da P ein Unterkörper von K ist, ist $P \subseteq P(K)$. Da $0, 1_K \in P(K)$ und $P(K)$ unter Summen und Brüchen abgeschlossen ist, und

$$P = \operatorname{im}(\phi) = \left\{ \frac{p \cdot 1_K}{q \cdot 1_K} \mid \frac{p}{q} \in \mathbb{Q} \right\},$$

ist auch $P \subseteq P(K)$. Somit ist $P = P(K)$ und $\phi\colon \mathbb{Q} \to P(K), p/q \mapsto (p \cdot 1_K)/(q \cdot 1_K)$ ein Körperisomorphismus. Wie bereits gezeigt, ist dies auch der einzige Körperisomorphismus $\mathbb{Q} \to P(K)$.

3.8.3. Anwendung: Endliche Körper

Als Anwendung der obigen Ergebnisse ergibt sich insbesondere, dass es für jeden endlichen Körper K eindeutige $p, n \in \mathbb{N}$ gibt, mit p prim und $n \geq 1$, so dass $|K| = p^n$; dabei ist $p = \text{char}(K)$.

Die Eindeutigkeit von p und n folgt direkt aus der Eindeutigkeit von Primfaktorzerlegungen.

Für die Existenz von p und n bemerken wir, dass K ein $P(K)$-Vektorraum ist. Da K endlich ist, ist K inbesondere endlichdimensional über $P(K)$, also $n \coloneqq \dim_{P(K)} K < \infty$. Da $|K| \geq 2$ ist auch $n > 0$. Da K endlich ist, ist $p \coloneqq \text{char}(K) > 0$ prim. Da $P(K)$ als Körper isomorph zu $\mathbb{F}_p$ ist, ist $|P(K)| = |\mathbb{F}_p| = p$. Als n-dimensionaler $P(K)$-Vektorraum ist K isomorph zu $P(K)^n$. Somit ist $|K| = |P(K)^n| = p^n$, wobei $p = \text{char}(K)$ und $n = \dim_{P(K)}(K)$.

Bemerkung 3.7. Es lässt sich zeigen, dass es für jede Primzahl $p > 0$ und jedes $n \in \mathbb{N}$, $n > 0$ auch tatsächlich einen Körper K mit p^n Elementen gibt. Dieser Körper ist bis auf Isomorphismus eindeutig, d.h. sind K und L zwei Körper mit p^n Elementen, so gibt es einen Körperisomorphismus $K \to L$.

4. Beispiele für Vektorräume

Sofern nicht anders angegeben, bezeichnen K und L im folgenden Körper mit $K \subseteq L$.

4.1. Einige kleinere Beispiele

1. K ist ein K-Vektorraum, indem man die Multiplikation $K \times K \to K$, $(x, y) \mapsto x \cdot y$ als Skalarmultiplikation wählt. Dass $\lambda \cdot (v + w) = \lambda v + \lambda w$ und $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ für alle $\lambda, \mu \in K$ und $v, w \in V$ folgt direkt aus der Distributivität der Multiplikation. Dass $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$ für alle $\lambda, \mu \in K$ folgt aus der Assoziativität der Multiplikation. Dass $1 \cdot v = v$ für alle $v \in V$ folgt aus der Definition des Einselementes 1.

2. Wie bereits in 2.14 gesehen ist $K^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in K\}$ mit der eintragsweisen Addition

   $$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

   eine abelsche Gruppe. Mit der eintragsweise Skalarmultiplikation

   $$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n) \quad \text{für alle } \lambda \in K \text{ und } (x_1, \ldots, x_n) \in K^n$$

   ist K^n zu einem K-Vektorraum: Für alle $\lambda \in K$ und $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$ ist

   $$\begin{aligned} &\lambda \cdot ((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) = \lambda \cdot (x_1 + y_1, \ldots, x_n + y_n) \\ &= (\lambda(x_1 + y_1), \ldots, \lambda(x_n + y_n)) = (\lambda x_1 + \lambda y_m, \ldots, \lambda x_n + \lambda y_n) \\ &= (\lambda x_1, \ldots, \lambda x_n) + (\lambda y_1, \ldots, \lambda y_n) = \lambda \cdot (x_1, \ldots, x_n) + \lambda \cdot (y_1, \ldots, y_n). \end{aligned}$$

   Für alle $\lambda, \mu \in K$ und $(x_1, \ldots, x_n) \in K^n$ ist

   $$\begin{aligned} &(\lambda + \mu) \cdot (x_1, \ldots, x_n) = ((\lambda + \mu)x_1, \ldots, (\lambda + \mu)x_n) \\ &= (\lambda x_1 + \mu x_1, \ldots, \lambda x_n + \mu x_n) = (\lambda x_1, \ldots, \lambda x_n) + (\mu x_1, \ldots, \mu x_n) \\ &= \lambda \cdot (x_1, \ldots, x_n) + \mu \cdot (x_1, \ldots, x_n) \end{aligned}$$

   und

   $$\begin{aligned} \lambda \cdot (\mu \cdot (x_1, \ldots, x_n)) &= \lambda \cdot (\mu x_1, \ldots, \mu x_n) \\ &= (\lambda \mu x_1, \ldots, \lambda \mu x_n) = (\lambda \mu) \cdot (x_1, \ldots, x_n). \end{aligned}$$

   Für alle $(x_1, \ldots, x_n) \in K^n$ gilt schließlich

   $$1 \cdot (x_1, \ldots, x_n) = (1 \cdot x_1, \ldots, 1 \cdot x_n) = (x_1, \ldots, x_n).$$

   Ingesamt zeigt dies, dass K^n mit der eintragsweisen Addition und Skalarmultiplikation einen K-Vektorraum bildet.

3. Ist V ein K-Vektorraum, so ist $\{0\} \subseteq V$ ein Untervektorraum. Man bezeichnet diesen als den *Nulluntervektorraum*.

4. Die L-Vektorraum auf L schränkt sich zu einer K-Vektorraumstruktur auf L ein. L ist also ein K-Vektorraum durch $\lambda \cdot v = \lambda v$ für alle $\lambda \in K$ und $v \in L$, wobei die punktlose Multiplikation auf der rechten Seite die Multiplikation des Körpers L bezeichnet.

5. Ist allgemein V ein L-Vektorraum, so wird V durch Einschränkung der Skalarmultiplikation zu einem K-Vektorraum. Dass die Axiome eines K-Vektorraums erfüllt sind, folgt direkt daraus, dass sie für Skalare aus L erfüllt sind. Man bezeichnet diese Einschränkung von L-Vektorräumen zu K-Vektorräumen als *Skalarrestriktion*.

6. Ist V ein $\mathbb{C}$-Vektorraum, so ist V auch durch die Skalarmultiplikation

$$\lambda * v = \overline{\lambda} \cdot v \quad \text{für alle } \lambda \in Cbb \text{ und } v \in V$$

ein $\mathbb{C}$-Vektorraum: Für alle $\lambda \in \mathbb{C}$ und $v, w \in V$ ist

$$\lambda * (v + w) = \overline{\lambda} \cdot (v + w) = \overline{\lambda} \cdot v + \overline{\lambda} \cdot w = \lambda * v + \lambda * w.$$

Für alle $\lambda, \mu \in \mathbb{C}$ und $v \in V$ ist

$$(\lambda + \mu) * v = \overline{\lambda + \mu} \cdot v = (\overline{\lambda} + \overline{\mu}) \cdot v = \overline{\lambda} \cdot v + \overline{\mu} \cdot v = \lambda * v + \mu * v.$$

und

$$\lambda * (\mu * v) = \overline{\lambda} \cdot (\overline{\mu} \cdot v) = (\overline{\lambda} \cdot \overline{\mu}) \cdot v = \overline{\lambda \cdot \mu} \cdot v = (\lambda \cdot \mu) * v.$$

Außerdem ist für alle $v \in V$

$$1 * v = 1 \cdot v = v.$$

7. Ist allgemeinen $\phi \colon K \to K'$ ein Körperhomomorphismus und V ein K'-Vektorraum, so wird V ein K-Vektorraum durch die Skalarmultiplikation

$$\lambda * v = \phi(\lambda) \cdot v \quad \text{für alle } \lambda \in K \text{ und } v \in V.$$

Für alle $\lambda, \mu \in K$ und $v, w \in V$ ist nämlich

$$\lambda * (v + w) = \phi(\lambda) \cdot (v + w) = \phi(\lambda) \cdot v + \phi(\lambda) \cdot w = \lambda * v + \lambda * w$$

und

$$\begin{aligned}(\lambda + \mu) * v = \phi(\lambda + \mu) \cdot v &= (\phi(\lambda) + \phi(\mu)) \cdot v \\ &= \phi(\lambda) \cdot v + \phi(\mu) \cdot v = \lambda * v + \mu * v,\end{aligned}$$

sowie

$$\begin{aligned}\lambda * (\mu * v) = \phi(\lambda) \cdot (\phi(\mu) \cdot v) &= (\phi(\lambda) \cdot \phi(\mu)) \cdot v \\ &= \phi(\lambda \cdot \mu) \cdot v = (\lambda \cdot \mu) * v,\end{aligned}$$

und für alle $v \in V$ gilt

$$1 * v = \phi(1) \cdot v = 1 \cdot v = v.$$

Die vorherigen beiden Beispiele ergeben sich als Sonderfall hievon: Die Skalarrestriktion ergibt sich durch die Inklusion $K \hookrightarrow L$ und das vorherige Beispiel durch die Konjugation $\mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$.

4.2. Untervektorräume bezüglich linearer Abbildungen

Es seien V und W K-Vektorräume und $f\colon V \to W$ sei eine K-lineare Abbildung.

4.2.1. Kern und Bild einer linearen Abbildung

Wir zeigen, dass der *Kern* von f

$$\ker(f) \coloneqq \{v \in V \mid f(v) = 0\}$$

ein Untervektorraum von V ist: Da f insbesondere ein Gruppenhomomorphismus der unterliegenden abelschen Gruppen ist, haben wir in 2.3 bereits gesehen, dass $\ker(f)$ eine additive Untergruppe ist. Für alle $\lambda \in K$ und $v \in \ker(f)$ ist auch

$$f(\lambda v) = \lambda f(v) = \lambda \cdot 0 = 0,$$

also $\lambda v \in \ker(f)$. Das zeigt, dass $\ker(f)$ ein Untervektorraum ist.

Bemerkung 4.1. Wir haben in 2.3 auch schon gesehen, dass f genau dann injektiv ist, wenn $\ker(f) = \{0\}$.

Das *Bild* von f

$$\operatorname{im}(f) = \{f(v) \mid v \in V\}$$

ist ein Untervektorraum von W: Da f insbesondere ein Gruppenhomomorphismus der unterliegenden abelschen Gruppen ist, haben wir in 2.3 bereits gesehen, dass $\operatorname{im}(f)$ eine additive Untergruppe ist. Für $w \in \operatorname{im}(f)$ gibt es ein $v \in V$ mit $w = f(v)$, weshalb für alle $\lambda \in K$ auch

$$\lambda w = \lambda f(v) = f(\lambda w) \in \operatorname{im}(f).$$

Das zeigt, dass $\operatorname{im}(f)$ ein Untervektorraum ist.

4.2.2. Bilder und Urbilder von Untervektorräumen

Ist $U \subseteq V$ ein Untervektorraum, so ist das Bild $f(U)$ ein Untervektorraum von W: Da f inbesondere ein Gruppenhomomorphismen der unterliegenden abelschen Gruppen ist haben wir bereits in 2.3 gesehen, dass $f(U)$ ein additive Untergruppe ist. Ist $w \in f(U)$, so gibt es $u \in U$ mit $w = f(u)$. Da U ein Untervektorraum ist, ist für alle $\lambda \in K$ auch $\lambda u \in U$, weshalb für alle $\lambda \in K$ auch

$$\lambda w = \lambda f(u) = f(\lambda u) \in f(U).$$

Also ist $f(U)$ ein Untervektorraum von f.

Bemerkung 4.2. Wie bereits in 2.3 lassen sich Rechnungen auch hier umgehen: Da f linear ist, ist es auch die Einschränkung $f|_U\colon U \to W, u \mapsto f(u)$. Wie bereits gesehen, ist deshalb $f(U) = \operatorname{im}(f|_U)$ ein Untervektorraum.

Ist $U \subseteq W$ ein Untervektorraum, so ist das Urbild $f^{-1}(U)$ ein Untervektorraum von V: Da f inbesondere ein Gruppenhomomorphismus zwischen den unterliegenden abelschen Gruppen ist, haben wir bereits in 2.3 gesehen, dass $f^{-1}(U)$ eine additive Untergruppe der unterliegenden abelschen Gruppe von V ist. Für $v \in f^{-1}(U)$ ist $f(v) \in U$, also für alle $\lambda \in K$ auch

$$f(\lambda v) = \lambda f(v) \in U,$$

da U ein Untervektorraum ist. Also ist $f^{-1}(U)$ ein Untervektorraum.

Bemerkung 4.3. Ähnlich wie in 2.3 folgt auch hieraus, dass

$$\ker(f) = f^{-1}(\{0\})$$

ein Untervektorraum ist.

4.3. Schnitte und Vereinigungen von Untervektorräumen

4.3.1. Schnitte von Untervektorräumen

Es sei V ein K-Vektorraum und $\{U_i\}_{i\in I}$ eine Kollektion von Untervektorräumen, d.h. für jedes $i \in I$ ist $U_i \subseteq V$ ein Untervektorraum. Wir zeigen, dass dann auch der Schnitt $U := \bigcap_{i\in I} U_i$ ein Untervektorraum von V ist:

Für alle $i \in I$ ist U_i ein Untervektorraum, und somit $0 \in U_i$. Deshalb ist auch $0 \in U$. Sind $x, y \in U$, so ist $x, y \in U_i$ für alle $i \in I$. Für jedes $i \in I$ ist U_i ein Untervektorraum und deshalb auch $x + y \in U_i$. Also ist auch $x + y \in U$. Ist außerdem $\lambda \in K$, so ist daher auch $\lambda x \in U_i$ für alle $i \in I$ und somit $\lambda x \in U$. Insgesamt zeigt dies, dass $U = \bigcap_{i\in I} U_i$ ein Untervektorraum von V ist.

4.3.2. Vereinigungen von Untervektorräumen

Die beliebige Vereinigung von Untervektorräumen ist im Allgemeinen kein Untervektorraum. Für einen Körper K sind beispielsweise $U_1, U_2 \subseteq K^2$ mit $U_1 = \{(x, 0) \mid x \in K\}$ und $U_2 = \{(0, y) \mid y \in K\}$ zwei Untervektorräume, deren Vereinigung $U := U_1 \cup U_2$ kein Untervektorraum ist, da $(1, 0), (0, 1) \in U$ aber $(1, 0) + (0, 1) = (1, 1) \notin U$.

Ist V ein beliebiger K-Vektorraum, und sind $U_1, U_2 \subset V$ zwei Untervektorräume, so ist die Vereinigung $U_1 \cup U_2$ genau dann ein Untervektorraum, wenn $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$: Es sind nämlich U_1 und U_2 Untergruppen der unterliegenden abelschen Gruppe von V, und ist $U_1 \cup U_2$ ebenfalls ein Untervektorraum von V, so ist dann auch $U_1 \cup U_2$ eine Untergruppe der unterliegenden abelschen Gruppe von V. Wie bereits in 2.4.2 gesehen, muss daher $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$.

4.3.3. Aufsteigende Vereinigung von Untervektorräumen

Es sei V ein K-Vektorraum und $\{U_n\}_{n\in\mathbb{N}}$ eine Kollektion von Untervektorräumen mit $U_n \subseteq U_m$ falls $n \leq m$, d.h. wir haben eine aufsteigende Kette

$$U_0 \subseteq U_1 \subseteq U_2 \subseteq U_3 \subseteq U_4 \subseteq \cdots \subseteq V$$

von Untervektorräumen. Dann ist auch die Vereinigung $U := \bigcup_{n\in\mathbb{N}} U_n$ ein Untervektorraum:

Es ist $0 \in U_0 \subseteq U$. Sind $x, y \in U$ so gibt es $n_x, n_y \in \mathbb{N}$ mit $x \in U_{n_x}$ und $y \in U_{n_y}$. Für $m := \max\{n_x, n_y\}$ ist $U_{n_x}, U_{n_y} \subseteq U_m$ und somit auch $x, y \in U_m$. Damit ist auch $x + y \in U_m \subseteq U$, da U_m ein Untervektorraum ist. Für alle $\lambda \in K$ ist außerdem $\lambda x \in U_{n_x} \subseteq U$, da U_{n_x} ein Untervektorraum ist. Ingesamt zeigt dies, dass U ein Untervektorraum von V ist.

Bemerkung 4.4. Wie bereits in Bemerkung 2.5 über die aufsteigende Vereinigung von Untergruppen lässt sich hier $\mathbb{N}$ durch eine total geordnete Menge, oder sogar durch eine gerichtete Menge ersetzen.

4.4. Die lineare Hülle einer Teilmenge

Definition 4.5. *Für einen K-Vektorraum V und eine Teilmenge $S \subseteq V$ ist*

$$\mathcal{L}(S) := \left\{ \sum_{s\in S} \lambda_s s \;\middle|\; s \in S, \lambda_s \in K \text{ für alle } s \in S \text{ mit } \lambda_s = 0 \text{ für fast alle } s \in S \right\}$$

die lineare Hülle *von S, bzw. den* (K-)Span *von S.*

Bemerkung 4.6. Die Formulierung „für fast alle“ bedeutet „alle bis auf endlich viele“. Das $\lambda_s = 0$ für fast alle $s \in S$ bedeutet also, dass die Menge $\{s \in S \mid \lambda_s \neq 0\}$ endlich ist.

Es sei V ein K-Vektorraum und $S \subseteq V$ eine Teilmenge. Wir zeigen, dass $\mathcal{L}(S)$ ein Untervektorraum von V ist:

Setzt man $\lambda_s = 0$ für alle $s \in S$, so ist $\sum_{s\in S} \lambda_s s = \sum_{s\in S} 0 = 0$, also ist $0 \in \mathcal{L}(S)$.

Sind $x, y \in \mathcal{L}(S)$ so gibt es Koeffizienten $\lambda_s, \mu_s \in K$, $s \in S$ mit $\lambda_s = 0$ für fast alle $s \in S$ und $\mu_s = 0$ für fast alle $s \in S$, so dass $x = \sum_{s\in S} \lambda_s s$ und $y = \sum_{s\in S} \mu_s s$. Es ist damit auch $\lambda_s + \mu_s = 0$ für fast alle $s \in S$ und

$$x + y = \sum_{s\in S} \lambda_s s + \sum_{s\in S} \mu_s s = \sum_{s\in S} (\lambda_s + \mu_s) s.$$

Also ist auch $x + y \in \mathcal{L}(S)$. Für $\mu \in K$ ist außerdem auch $\mu \cdot \lambda_s = 0$ für fast alle $s \in S$ und

$$\mu x = \mu \sum_{s\in S} \lambda s = \sum_{s\in S} (\mu\lambda_s) x.$$

Also ist auch $x \in \mathcal{L}(S)$. Ingesamt zeigt dies, dass $\mathcal{L}(S)$ ein Untervektorraum von V ist.

Bemerkung 4.7. $\mathcal{L}(S)$ ist der kleinste Untervektorraum, der S enthält, d.h. ist $U \subseteq V$ ein Untervektorraum mit $S \subseteq U$, so ist auch $\mathcal{L}(S) \subseteq U$. Dies folgt direkt daraus, dass U unter der Skalarmultiplikation und Addition von V abgeschlossen ist.

Für $\mathcal{U} := \{U \subseteq V \mid U \text{ ist ein Untervektorraum mit } S \subseteq U\}$ ist auch $W := \bigcap_{U\in\mathcal{U}} U$ ein Untervektorraum von V, da Schnitte von Untervektorräumen wieder Untervektorräume sind. Da $S \subseteq U$ für alle $U \in \mathcal{U}$ ist auch $S \subseteq \bigcap_{U\in\mathcal{U}} U = W$. Ist $U \subseteq V$ ein beliebiger

Untervektorraum mit $S \subseteq U$ so ist $U \in \mathcal{U}$ und somit $W = \bigcap_{U' \in \mathcal{U}} U' = W$. Also ist auch W der kleinste Untervektorraum von V, der S enthält.

Es ist daher $\mathcal{L}(S) = W = \bigcap_{U \in \mathcal{U}} U$. (Da $\mathcal{L}(S)$ der kleinste Untervektorraum von V ist, der S enthält, und W ein Untervektorraum ist, der S enthält, ist $\mathcal{L}(S) \subseteq W$. Da W der kleinste Untervektorraum ist, der S enthält, und auch $\mathcal{L}(S)$ ein Untervektorraum ist, der S enthält, ist auch $W \subseteq \mathcal{L}(S)$. Also ist bereits $\mathcal{L}(S) = W$.)

4.5. Summen von Untervektorräumen

Definition 4.8. *Es sei V ein K-Vektorraum und $\{U_i\}_{i \in I}$ eine Kollektion von Untervektorräumen von V, d.h. für alle $i \in I$ ist $U_i \subseteq V$ ein Untervektorraum. Dann ist*

$$\sum_{i \in I} U_i := \left\{ \sum_{i \in I} u_i \;\middle|\; u_i \in U_i \text{ für alle } i \in I, \text{ und } u_i = 0 \text{ für fast alle } i \in I \right\}.$$

die Summe *der Untervektorräume U_i, $i \in I$.*

Wir zeigen, dass $\sum_{i \in I} U_i$ ein Untervektorraum von V ist: Indem man $u_i = 0$ für alle $i \in I$ wählt, ergibt sich, dass $0 = \sum_{i \in I} u_i \in \sum_{i \in I} U_i$. Sind $x, y \in \sum_{i \in I} U_i$, so gibt es $u_i, v_i \in U_i$, $i \in I$ mit $u_i = 0$ für fast alle $i \in I$ und $v_i = 0$ für fast alle $i \in I$, so dass $x = \sum_{i \in I} u_i$ und $y = \sum_{i \in I} v_i$. Es ist daher auch $u_i + v_i = 0$ für fast alle $i \in I$ mit

$$x + y = \sum_{i \in I} u_i + \sum_{i \in I} v_i = \sum_{i \in I} (u_i + v_i).$$

Also ist auch $x + y \in \sum_{i \in I} U_i$. Ist außerdem $\mu \in K$, so ist auch $\mu u_i = 0$ für fast alle $i \in I$, und somit

$$\mu x = \mu \sum_{i \in I} u_i = \sum_{i \in I} (\mu u_i).$$

Also ist auch $\mu x \in \sum_{i \in I} U_i$. Ingesamt zeigt dies, dass $\sum_{i \in I} U_i$ ein Untervektorraum von V ist.

Bemerkung 4.9. 1. Analog zu Bemerkung 4.7 ergibt sich, dass $\sum_{i \in I} U_i$ der kleinste Untervektorraum von V ist, der U_i für alle $i \in I$ enthält, und dass somit

$$\sum_{i \in I} U_i = \bigcap \{W \subseteq V \mid W \text{ ist ein Untervektorraum mit } U_i \subseteq W \text{ für alle } i \in I\}.$$

2. Dass $\sum_{i \in I} U_i$ der kleinte Untervektorraum ist, der U_i für alle $i \in I$ enthält, ist äquivalent dazu, dass $\sum_{i \in I} U_i$ der kleinste Untervektorraum ist, der $\bigcup_{i \in I} U_i$ enthält. Deshalb ist $\sum_{i \in I} U_i = \mathcal{L}(\bigcup_{i \in I} U_i)$.

3. Ist $S \subseteq V$ ist $\mathcal{L}(\{s\}) = \{\lambda s \mid \lambda \in K\}$. Daher ist

$$\begin{aligned} \mathcal{L}(S) &= \left\{ \sum_{s \in S} \lambda_s s \;\middle|\; s \in S,\ \lambda_s \in K \text{ für alle } s \in S \text{ mit } \lambda_s = 0 \text{ für fast alle } s \in S \right\} \\ &= \left\{ \sum_{s \in S} u_s \;\middle|\; u_s \in \mathcal{L}(s) \text{ für alle } s \in S, \text{ und } u_s = 0 \text{ für fast alle } i \in I \right\} = \sum_{s \in S} \mathcal{L}(\{s\}). \end{aligned}$$

4. Für endlich viele Untervektorräume $U_1, \dots, U_n \subseteq V$ schreibt man auch $U_1 + \cdots + U_n$ und $\sum_{i=1}^{n} U_i$ für $\sum_{i \in \{1,\dots,n\}} U_i$.

5. Für je zwei endlichdimensional Untervektorräume $U, W \subseteq V$ gilt die Dimensionsformel

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

4.6. Abbildungen in einen Vektorraum

Es sei X eine beliebige Menge und V ein K-Vektorraum. Auf der Menge

$$\mathrm{Abb}(X, V) = \{f \colon f \colon X \to V\}$$

Wir definieren für $f, g \in \mathrm{Abb}(X, V)$ und $\lambda \in K$ eine die punktweise Addition und Skalarmultiplikation durch

$$(f + g)(x) \coloneqq f(x) + g(x) \quad \text{für alle } x \in X$$

und

$$(\lambda \cdot f)(x) \coloneqq \lambda \cdot f(x) \quad \text{für alle } x \in X.$$

Wir zeigen, dass $\mathrm{Abb}(X, V)$ zusammen mit dieser Addition und Skalarmultiplikation einen K-Vektorraum bildet:
Für alle $f, g, h \in \mathrm{Abb}(X, V)$ ist

$$\begin{aligned}(f + (g + h))(x) &= f(x) + (g + h)(x) = f(x) + g(v) + h(x) \\ &= (f + g)(x) + h(x) = ((f + g) + h)(x)\end{aligned}$$

für alle $x \in X$ und somit $f + (g + h) = (f + g) + h$. Also ist die Addition assoziativ. Für alle $f, g \in \mathrm{Abb}(X, V)$ ist

$$(f + g)(x) = f(x) + g(x) = g(x) + h(x) = (g + h)(x) \quad \text{für alle } x \in X,$$

also ist $f + g = g + f$, die Addition also kommutativ. Die *Nullfunktion* ist definiert als

$$N \colon X \to V, x \mapsto 0.$$

Für alle $f \in \mathrm{Abb}(X, V)$ ist

$$(f + N)(x) = f(x) + N(x) = f(x) + 0 = f(x) \quad \text{für alle } x \in X,$$

also ist $f + N = f$. Also ist N neutral bezüglich der Addition. Für $f \in \mathrm{Abb}(X, V)$ sei

$$\tilde{f} \colon X \to V \quad \text{und} \quad \tilde{f}(x) \coloneqq -f(x) \quad \text{für alle } x \in X.$$

Es ist dann

$$(f + \tilde{f})(x) = f(x) + \tilde{f}(x) = f(x) - f(x) = 0 = N(x) \quad \text{für alle } x \in X,$$

also $f + \tilde{f} = N$. Somit ist $\tilde{f}$ additiv invers zu f. Ingesamt zeigt dies, dass $+$ tatsächlich eine Addition auf $\mathrm{Abb}(X, V)$ definiert.

Für alle $\lambda, \mu \in K$ und $f, g \in \mathrm{Abb}(X, V)$ ist

$$\begin{aligned}(\lambda \cdot (f+g))(x) &= \lambda \cdot (f+g)(x) = \lambda \cdot (f(x) + g(x)) \\ &= \lambda \cdot f(x) + \lambda \cdot g(x) = (\lambda \cdot f)(x) + (\lambda \cdot g)(x) = (\lambda \cdot f + \lambda \cdot g)(x)\end{aligned}$$

für alle $x \in X$ und somit $\lambda \cdot (f+g) = \lambda \cdot f + \lambda \cdot g$; es ist

$$\begin{aligned}((\lambda+\mu) \cdot f)(x) = (\lambda+\mu) \cdot f(x) &= \lambda \cdot f(x) + \mu \cdot f(x) \\ &= (\lambda \cdot f)(x) + (\mu \cdot f)(x) = (\lambda \cdot f + \mu \cdot f)(x)\end{aligned}$$

für alle $x \in X$ und somit $(\lambda+\mu) \cdot f = \lambda \cdot f + \mu \cdot f$; es ist

$$(\lambda \cdot (\mu \cdot f))(x) = \lambda \cdot (\mu \cdot f)(x) = \lambda \cdot (\mu \cdot f(x)) = (\lambda \cdot \mu) \cdot f(x) = ((\lambda \cdot \mu) \cdot f)(x)$$

für alle $x \in X$ und somit $\lambda \cdot (\mu \cdot f) = (\lambda \cdot \mu) \cdot f$. Außerdem ist für jedes $f \in \mathrm{Abb}(X, V)$

$$(1 \cdot f)(x) = 1 \cdot f(x) = f(x) \quad \text{für alle } x \in X,$$

und somit $1 \cdot f = f$.

Ingesamt zeigt dies, dass $\mathrm{Abb}(X, V)$ zusammen mit der punktweisen Addition und Skalarmultiplikation einen K-Vektorraum bildet.

4.7. Hom-Räume

Es seien V und W zwei K-Vektorräume und

$$\mathrm{Hom}_K(V, W) \coloneqq \{f \colon V \to W \mid f \text{ ist linear}\}.$$

Wir zeigen, dass $\mathrm{Hom}_K(V, W) \subseteq \mathrm{Abb}(V, W)$ einen Untervektorraum bildet, und somit ebenfalls einen Vektorraum bezüglich der punktweisen Addition und Skalarmultiplikation.

Die Nullfunktion $0 \in \mathrm{Abb}(V, W)$ ist linear, da $0(v+w) = 0 = 0(v) + 0(w)$ sowie $0(\lambda v) = 0 = \lambda 0(v)$ für alle $v, w \in V$ und $\lambda \in K$. Also ist $0 \in \mathrm{Hom}_K(V, W)$.

Sind $f, g \in \mathrm{Hom}_K(V, W)$ und $\lambda \in K$, so ist für alle $v, w \in V$ und $\mu \in K$

$$\begin{aligned}(f+g)(v+w) &= f(v+w) + g(v+w) = f(v) + f(w) + g(v) + g(w) \\ &= f(v) + g(v) + f(w) + g(w) = (f+g)(v) + (f+g)(w)\end{aligned}$$

und

$$(\lambda f)(\mu v) = \lambda f(\mu v) = \lambda \mu f(v) = \mu \lambda f(v) = \mu(\lambda f)(v),$$

also auch $f + g \in \mathrm{Hom}_K(V, W)$ und $\lambda f \in \mathrm{Hom}_K(V, W)$. Dies zeigt, dass $\mathrm{Hom}_K(V, W)$ ein Untervektorraum von $\mathrm{Abb}(V, W)$ ist.

Bemerkung 4.10. 1. Für einen K-Vektorraum V ist $\mathrm{End}_K(V) \coloneqq \mathrm{Hom}_K(V, V)$.

2. Ist V ein K-Vektorraum, so heißt $V^* \coloneqq \mathrm{Hom}(V, K)$ der *Dualraum* von V.

4.8. Matrizenräume

4.8.1. Die $(m \times n)$-Matrizen $\mathrm{Mat}(m \times n, K)$

Die $(m \times n)$-Matrizen $\mathrm{Mat}(m \times n, K)$ bilden zusammen mit der eintragsweisen Addition

$$(a_{ij})_{\substack{i=1,\dots,m\\j=1,\dots,n}} + (b_{ij})_{\substack{i=1,\dots,m\\j=1,\dots,n}} = (a_{ij} + b_{ij})_{\substack{i=1,\dots,m\\j=1,\dots,n}}$$

eine abelsche Gruppe. Zusammen mit der eintragsweisen Skalarmultiplikation

$$\lambda \cdot (a_{ij})_{\substack{i=1,\dots,m\\j=1,\dots,n}} = (\lambda a_{ij})_{\substack{i=1,\dots,m\\j=1,\dots,n}}$$

wird $\mathrm{Mat}(m \times n, K)$ zu einem K-Vektorraum: Für alle Skalare $\lambda, \mu \in K$ und Matrizen $(a_{ij})_{i,j}, (b_{ij})_{i,j} \in \mathrm{Mat}(m \times n, K)$ ist

$$\begin{aligned}\lambda \cdot ((a_{ij})_{i,j} + (b_{ij})_{i,j}) &= \lambda \cdot (a_{ij} + b_{ij})_{i,j} = (\lambda(a_{ij} + b_{ij}))_{i,j}\\ &= (\lambda a_{ij} + \lambda b_{ij})_{i,j} = (\lambda a_{ij})_{i,j} + (\lambda b_{ij})_{i,j} = \lambda(a_{ij})_{i,j} + \lambda(b_{ij})_{i,j},\end{aligned}$$

und

$$\begin{aligned}(\lambda + \mu) \cdot (a_{ij})_{i,j} &= ((\lambda + \mu)a_{ij})_{i,j}\\ &= (\lambda a_{ij} + \mu a_{ij})_{i,j} = \lambda \cdot (a_{ij})_{i,j} + \mu \cdot (a_{ij})_{i,j},\end{aligned}$$

sowie

$$\lambda \cdot (\mu \cdot (a_{ij})_{i,j}) = \lambda \cdot (\mu \cdot a_{ij})_{i,j} = (\lambda \cdot \mu a_{ij})_{i,j} = (\lambda \cdot \mu) \cdot (a_{ij})_{i,j},$$

und für alle $(a_{ij})_{i,j} \in \mathrm{Mat}(m \times n, K)$ gilt

$$1 \cdot (a_{ij})_{i,j} = (1 \cdot a_{ij})_{i,j} = (a_{ij})_{i,j}.$$

Ingesamt zeigt dies, dass $\mathrm{Mat}(m \times n, K)$ zusammen mit der üblichen eintragsweisen Addition und Skalarmultiplikation einen K-Vektorraum bildet.

4.8.2. Diagonalmatrizen und Dreiecksmatrizen

Definition 4.11. *Es sei* $\mathfrak{d}_n(K) = \{D \in \mathrm{Mat}(n \times n, K) \mid D$ *ist eine Diagonalmatrix*$\}$.

(Der Begriff einer Diagonalmatrix wurde in Definition 2.18 eingeführt.)

Definition 4.12. *Eine quadratische Matrix* $B \in \mathrm{Mat}(n \times n, K)$ *heißt* obere Dreiecksmatrix, *falls* $A_{ij} = 0$ *für alle* $1 \leq j < i \leq n$, *falls also* A *von der Form*

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

ist. A heißt echte obere Dreiecksmatrix, *falls zusätzlich $a_{ii} = 0$ für alle $1 \leq i \leq n$, also A von der Form*

$$A = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{n-1,n} \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

ist. Analog heißt A untere Dreiecksmatrix, *falls $A_{ij} = 0$ für alle $1 \leq i < j \leq n$, also A von der Form*

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}$$

ist, und A heißt echte untere Dreiecksmatrix, *falls zusätzlich $A_{ii} = 0$ für alle $1 \leq i \leq n$, also A von der Form*

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ a_{21} & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,n-1} & 0 \end{pmatrix}$$

ist. Es seien

$$\mathfrak{b}_n^+(K) \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A \text{ ist eine obere Dreiecksmatrix}\},$$
$$\mathfrak{b}_n^-(K) \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A \text{ ist eine untere Dreiecksmatrix}\},$$
$$\mathfrak{n}_n^+(K) \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A \text{ ist eine echte obere Dreiecksmatrix}\},$$
$$\mathfrak{n}_n^-(K) \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A \text{ ist eine echte untere Dreiecksmatrix}\}.$$

Wir zeigen, dass $\mathfrak{d}_n(K)$, $\mathfrak{b}_n^+(K)$, $\mathfrak{b}_n^-(K)$, $\mathfrak{n}_n^+(K)$ sowie $\mathfrak{n}_n^-(K)$ Untervektorräume von $\mathrm{Mat}(n \times n, K)$ sind. Wir zeigen dies mithilfe der folgenden Verallgemeinerung:

Für eine Teilmenge $\mathcal{I} \subseteq \{1, \ldots, m\} \times \{1, \ldots, n\}$ sei

$$M_{\mathcal{I}} = \{A \in \mathrm{Mat}(m \times n, K) \mid A_{ij} = 0 \text{ für alle } (i,j) \in \mathcal{I}\}.$$

Wir zeigen, dass $M_{\mathcal{I}}$ ein Untervektorraum von $\mathrm{Mat}(m \times n, K)$ ist:

Für die Nullmatrix $0 \in \mathrm{Mat}(m \times n, K)$ ist $0_{ij} = 0$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$ und somit insbesondere für alle $(i,j) \in \mathcal{I}$. Also ist $0 \in M_{\mathcal{I}}$.

Sind $A, B \in M_{\mathcal{I}}$, so ist $A_{ij} = 0$ für alle $(i,j) \in \mathcal{I}$ und $B_{ij} = 0$ für alle $(i,j) \in \mathcal{I}$. Somit ist

$$(A + B)_{ij} = A_{ij} + B_{ij} = 0 + 0 = 0 \quad \text{für alle } (i,j) \in \mathcal{I},$$

also auch $A + B \in \mathcal{I}$. Für alle $\lambda \in K$ ist zudem

$$(\lambda A)_{ij} = \lambda A_{ij} = \lambda \cdot 0 = 0 \quad \text{für alle } (i,j) \in \mathcal{I},$$

also auch $\lambda A \in M_{\mathcal{I}}$. Ingesamt zeigt dies, dass $M_{\mathcal{I}}$ ein Untervektorraum von $\mathrm{Mat}(m \times n, K)$ ist.

Bemerkung 4.13. Die obige Rechnungen lassen sich auch umgehen: Für jeden Einträgen $(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}$ ist die Abbildng $p_{ij}\colon \mathrm{Mat}(m \times n, K) \to K$, $A \mapsto A_{ij}$ linear, denn für alle $A, B \in \mathrm{Mat}(m \times n, K)$ ist

$$p_{ij}(A+B) = (A+B)_{ij} = A_{ij} + B_{ij} = p_{ij}(A) + p_{ij}(B)$$

und für alle $A \in \mathrm{Mat}(m \times n, K)$ und $\lambda \in K$ ist

$$p_{ij}(\lambda A) = (\lambda A)_{ij} = \lambda A_{ij} = \lambda p_{ij}(A).$$

Wegen der Linearität von p_{ij} ist

$$\ker(p_{ij}) = \{A \in \mathrm{Mat}(n \times n, K) \mid A_{ij} = 0\}$$

ein Untervektorraum. Für eine beliebige Menge von Einträgen $\mathcal{I} \subseteq \{1,\dots,m\} \times \{1,\dots,n\}$ ist daher auch

$$\begin{aligned} M_{\mathcal{I}} &= \{A \in \mathrm{Mat}(m \times n, K) \mid A_{ij} = 0 \text{ für alle } (i,j) \in \mathcal{I}\} \\ &= \bigcap_{(i,j)\in\mathcal{I}} \{A \in \mathrm{Mat}(m \times n, K) \mid A_{ij} = 0\} \end{aligned}$$

ein Untervektorraum von $\mathrm{Mat}(m \times n, K)$, da Schnitte von Untervektorräumen wieder Untervektorräume sind.

Für die Einträge

$$\begin{aligned} \mathcal{I}_1 &= \{(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\} \mid i \neq j\}, \\ \mathcal{I}_2 &= \{(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\} \mid j < i\}, \\ \mathcal{I}_3 &= \{(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\} \mid i < j\}, \\ \mathcal{I}_4 &= \{(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\} \mid j \leq i\} \\ \mathcal{I}_5 &= \{(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\} \mid i \leq j\} \end{aligned}$$

ist nun $\mathfrak{d}_n(K) = M_{\mathcal{I}_1}$, $\mathfrak{b}_n^+(K) = M_{\mathcal{I}_2}$, $\mathfrak{b}_n^-(K) = M_{\mathcal{I}_3}$, $\mathfrak{n}_n^+(K) = M_{\mathcal{I}_4}$ und $\mathfrak{n}_n^-(K) = M_{\mathcal{I}_5}$. Also sind $\mathfrak{d}_n(K)$, $\mathfrak{b}_n^+(K)$, $\mathfrak{b}_n^-(K)$, $\mathfrak{n}_n^+(K)$ und $\mathfrak{n}_n^-(K)$ Untervektorräume von $\mathrm{Mat}(n \times n, K)$.

Bemerkung 4.14. Die Untervektorräume $\mathfrak{d}_n(K)$, $\mathfrak{b}_n^+(K)$, $\mathfrak{b}_n^-(K)$, $\mathfrak{n}_n^+(K)$ und $\mathfrak{n}_n^-(K)$ sind auch unter der Matrixmultiplikation abgelschlossen.

Dass $\mathfrak{d}_n(K)$ unter der Matrixmultiplikation abgelschlossen ist, also das Produkt von Diagonalmatrizen ebenfalls eine Diagonalmatrix ist, haben wir in 2.8.2 gesehen.

Wir zeigen beispielsweise, dass auch die oberen Dreiecksmatrizen $\mathfrak{b}_n^+(K)$ unter der Matrixmultiplikation abgeschlossen sind; für die anderen Räume läuft das vorgehen analog.

Sind $A, B \in \mathfrak{b}_n^+(K)$ obere Dreiecksmatrizen, so ist $A_{ij} = 0$ für alle $1 \leq j < i \leq n$ und $B_{ij} = 0$ für alle $1 \leq j < i \leq n$. Für alle $1 \leq j < i \leq n$ ist deshalb

$$(A \cdot B)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj} = \sum_{k=1}^{i-1} \underbrace{A_{ik}}_{=0} B_{kj} + \sum_{k=i}^{n} A_{ik} \underbrace{B_{kj}}_{=0} = 0,$$

weshalb auch $A \cdot B$ eine obere Dreiecksmatrix ist, also $A \cdot B \in \mathfrak{b}_n^+(K)$.

4.8.3. Die (schief)symmetrischen Matrizen

Definition 4.15. *Es sei $A \in \mathrm{Mat}(m \times n, K)$. Dann ist die* transponierte *Matrix die $(n \times m)$-Matrix A^T definiert durch*

$$(A^T)_{ij} = A_{ji} \quad \textit{für alle } 1 \leq i \leq n \textit{ und } 1 \leq j \leq m,$$

also

$$A^T = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{pmatrix}^T = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{m1} \\ A_{12} & A_{22} & \cdots & A_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{mn} \end{pmatrix}.$$

Bemerkung 4.16. 1. Anschaulich gesehen entsteht A^T aus A durch Spiegelung der Matrix an der Diagonalen.

2. Transponieren ist linear, d.h. die Abbildung

$$\mathcal{T} \colon \mathrm{Mat}(m \times n, K) \to \mathrm{Mat}(n \times m, K), A \mapsto A^T$$

ist linear: Für alle Skalare $\lambda \in K$ und Matrizen $A, B \in \mathrm{Mat}(m \times n, K)$ gilt für alle $1 \leq i \leq n$ und $1 \leq j \leq m$, dass

$$((A+B)^T)_{ij} = (A+B)_{ji} = A_{ji} + B_{ji} = (A^T)_{ij} + (B^T)_{ij} = (A^T + B^T)_{ij}$$

und somit $(A+B)^T = A^T + B^T$, sowie

$$((\lambda A)^T)_{ij} = (\lambda A)_{ji} = \lambda A_{ji} = \lambda (A^T)_{ij} = (\lambda A^T)_{ij}$$

und somit $(\lambda A)^T = \lambda A^T$.

Definition 4.17. *Eine Matrix $A \in \mathrm{Mat}(n \times n, K)$ heißt* symmetrisch*, falls $A^T = A$, und* schiefsymmetrisch*, bzw.* alternierend*, falls $A^T = -A$. Es ist*

$$\mathrm{Sym}_n(K) \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A \textit{ ist symmetrisch}\}$$

und

$$\mathrm{Alt}_n(k) \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A \textit{ ist schiefsymmetrisch}\}.$$

Bemerkung 4.18. 1. Eine quadratische Matrix $A \in \mathrm{Mat}(n \times n, K)$ ist nach der Definition der Transponierten genau dann symmetrisch (bzw. schiefsymmetrisch), falls $A_{ij} = A_{ji}$ (bzw. $A_{ij} = -A_{ji}$) für alle $1 \leq i, j \leq n$.

2. Ist $A \in \mathrm{Mat}(m \times n, K)$ mit $A^T = A$ oder $A^T = -A$, so ist notwendigerweise $m = n$. Es genügt daher, den Begriff einer symmetrischen, bzw. schiefsymmetrischen Matrix für quadratische Matrizen zu definieren.

Beispiel(e). Die Einheitsmatrix $I_n \in \mathrm{Mat}(n \times n, K)$ ist symmetrisch. Die Matrizen

$$\begin{pmatrix} 4 & 7 & -6 \\ 7 & 9 & 2 \\ -6 & 2 & 4 \end{pmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{Q}) \quad \text{und} \quad \begin{pmatrix} 1 & \sqrt{2} & 3 \\ \sqrt{2} & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{R})$$

sind symmetrisch. Die beiden Matrizen

$$\begin{pmatrix} 0 & i & 2 & -3-i \\ -i & 0 & \sqrt{2}i & 5 \\ -2 & -\sqrt{2}i & 0 & -6+2i \\ 3+i & -5 & 6-2i & 0 \end{pmatrix} \in \mathrm{Mat}(3\times 3, \mathbb{C}), \begin{pmatrix} 0 & 8 & 9 & 1 \\ 5 & 0 & 6 & 8 \\ 4 & 7 & 0 & 3 \\ 12 & 5 & 10 & 0 \end{pmatrix} \in \mathrm{Mat}(4\times 4, \mathbb{F}_{13})$$

sind schiefsymmetrisch. Die Matrizen

$$\begin{pmatrix} 5 & 1 & 3 \\ 2 & 2 & 1 \\ 3 & 2 & 5 \end{pmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{Q}) \quad \text{und} \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{F}_2)$$

sind weder symmetrisch noch schiefsymmetrisch.

Wir zeigen, dass $\mathrm{Sym}_n(K)$ und $\mathrm{Alt}_n(K)$ Untervektorräume von $\mathrm{Mat}(n \times n, K)$ bilden: Da $0^T = 0 = -0$ ist $0 \in \mathrm{Sym}_n(K)$ und $0 \in \mathrm{Alt}_n(K)$.

Für $A, B \in \mathrm{Sym}_n(K)$ und $\lambda \in A$ ist

$$(A+B)^T = A^T + B^T = A + B \quad \text{und} \quad (\lambda A)^T = \lambda A^T = \lambda A,$$

also auch $A + B \in \mathrm{Sym}_n(K)$ und $\lambda A \in \mathrm{Sym}_n(K)$. Das zeigt, dass $\mathrm{Sym}_n(K)$ ein Untervektorraum von $\mathrm{Mat}(n \times n, K)$ ist.

Für $A, B \in \mathrm{Alt}_n(K)$ und $\lambda \in K$ ist

$$(A+B)^T = A^T + B^T = -A - B = -(A+B)$$

und

$$(\lambda A)^T = \lambda A^T = \lambda(-A) = -\lambda A,$$

also auch $A + B \in \mathrm{Alt}_n(K)$ und $\lambda A \in \mathrm{Alt}_n(K)$. Das zeigt, dass $\mathrm{Alt}_n(K)$ ein Untervektorraum von $\mathrm{Mat}(n \times n, K)$ ist

Beispiel(e). 1. Es sind

$$\mathrm{Sym}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{R} \right\} \quad \text{und} \quad \mathrm{Alt}_2(\mathbb{R}) = \left\{ \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \,\middle|\, a \in \mathbb{R} \right\}.$$

(Man bemerke, dass die Diagonaleintrage einer schiefsymmetrischen Matrix $A \in \mathrm{Alt}_n(\mathbb{R})$ alle 0 seien müssen, da $A_{ii} = -A_{ii}$ für alle $1 \leq i \leq n$ gilt.)

2. Es ist ist

$$\mathrm{Sym}_4(\mathbb{Q}) = \left\{ \begin{pmatrix} a & b & c & d \\ b & e & f & g \\ c & f & h & i \\ d & g & i & j \end{pmatrix} \middle| \, a,b,c,d,e,f,g,h,i,j \in \mathbb{Q} \right\}.$$

sowie

$$\mathrm{Alt}_5(\mathbb{Q}) = \left\{ \begin{pmatrix} 0 & a & b & c & d \\ -a & 0 & e & f & g \\ -b & -e & 0 & h & i \\ -c & -f & -h & 0 & j \\ -d & -g & -i & -j & 0 \end{pmatrix} \middle| \, a,b,c,d,e,f,g,h,i,j \in \mathbb{Q} \right\}.$$

3. Ist K ein Körper mit $\mathrm{char}(K) = 2$, so ist $x = -x$ für alle $x \in K$. Daher ist dann $\mathrm{Alt}_n(K) = \mathrm{Sym}_n(K)$ für alle $n \in \mathbb{N}$.

Bemerkung 4.19. 1. Analog lässt sich zeigen, dass

$$E_\lambda \coloneqq \{A \in \mathrm{Mat}(n \times n, K) \mid A^T = \lambda A\}$$

für alle $\lambda \in K$ einen Untervektorraum ist. Dabei ist insbesondere $\mathrm{Sym}_n(K) = E_1$ und $\mathrm{Alt}_n(K) = E_{-1}$.

2. Ist $\mathrm{char}(K) = 2$, so ist $1 = -1$ und somit $\mathrm{Sym}_n(K) = \mathrm{Alt}_n(K)$.

3. Ist $\mathrm{char}(K) \neq 2$, so lässt sich jede Matrix $M \in \mathrm{Mat}(n \times n, K)$ als Summe $M = S + A$ mit $S \in \mathrm{Sym}_n(K)$ und $A \in \mathrm{Alt}_n(K)$ schreiben, wobei A und S beide eindeutig sind: Existiert eine solche Zerlegung, so ist sie Eindeutig, da dann $S = (M + M^T)/2$ und $A = (M - M^T)/2$. Ist andererseits $M \in \mathrm{Mat}(n \times n, K)$ eine beliebige quadratische Matrix, so ist $S = (M + M^T)/2$ symmetrisch und $A = (M - M^T)/2$ schiefsymmetrisch (wegen der Linearität des Transponierens) und es gilt $M = S + A$.

   Für $A \in \mathrm{Mat}(4 \times 4, \mathbb{C})$ mit

$$A = \begin{pmatrix} 6+8i & 1+8i & 2+7i \\ -1-i & 9-8i & 5-7i \\ -7 & -3-6i & 7-2i \end{pmatrix}$$

   ist

$$\begin{aligned} A &= \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T) \\ &= \begin{pmatrix} 6+8i & \frac{7}{2}i & -\frac{5}{2}+\frac{7}{2}i \\ \frac{7}{2}i & 9-8i & 1-\frac{13}{2}i \\ -\frac{5}{2}+\frac{7}{2}i & 1-\frac{13}{2}i & 7-2i \end{pmatrix} + \begin{pmatrix} 0 & 1+\frac{9}{2}i & \frac{9}{2}+\frac{7}{2}i \\ -1-\frac{9}{2}i & 0 & 4-\frac{1}{2}i \\ -\frac{9}{2}-\frac{7}{2}i & -4+\frac{1}{2}i & 0 \end{pmatrix}. \end{aligned}$$

4.8.4. Die spurlosen Matrizen $\mathfrak{sl}_n(K)$

Definition 4.20. *Die* Spur *(engl.* trace*) einer quadratischen Matrix $A \in \mathrm{Mat}(n \times n, K)$ ist die Summe ihrer Diagonaleinträge, d.h.*

$$\mathrm{spur}(A) = \mathrm{spur}\left(\begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix}\right) = A_{11} + \cdots + A_{nn}.$$

Die Matrix A heißt spurlos*, falls* $\mathrm{spur}(A) = 0$*. Es ist*

$$\mathfrak{sl}_n(K) = \{A \in \mathrm{Mat}(n \times n, K) \mid A \textit{ ist spurlos}\}.$$

Wir zeigen, dass $\mathfrak{sl}_n(K)$ ein Untervektorraum von $\mathrm{Mat}(n \times n, K)$ ist: Als Abbildung $\mathrm{spur}\colon \mathrm{Mat}(n\times n, K) \to K$ ist die Spur linear, denn für alle $\lambda \in K$ und $A, B \in \mathrm{Mat}(n\times n, K)$ ist

$$\begin{aligned}\mathrm{spur}(A + B) &= \sum_{i=1}^{n} (A + B)_{ii} = \sum_{i=1}^{n} (A_{ii} + B_{ii}) = \sum_{i=1}^{n} A_{ii} + \sum_{i=1}^{n} B_{ii} \\ &= \mathrm{spur}(A) + \mathrm{spur}(B)\end{aligned}$$

und

$$\mathrm{spur}(\lambda A) = \sum_{i=1}^{n} (\lambda A)_{ii} = \sum_{i=1}^{n} \lambda A_{ii} = \lambda \sum_{i=1}^{n} A_{ii} = \lambda \mathrm{spur}(A).$$

Da $\mathfrak{sl}_n(K) = \ker(\mathrm{spur})$ ist $\mathfrak{sl}_n(K)$ somit ein Untervektorraum.

Bemerkung 4.21. 1. Für $A, B \in \mathrm{Mat}(n \times n, K)$ ist

$$\begin{aligned}\mathrm{spur}(AB) &= \sum_{i=1}^{n} (AB)_{ii} = \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} B_{ji} = \sum_{j=1}^{n} \sum_{i=1}^{n} B_{ji} A_{ij} = \sum_{j=1}^{n} (BA)_{jj} \\ &= \mathrm{spur}(BA).\end{aligned}$$

Hierdurch ist die Spur als lineare Abbildung bis auf skalares Vielfaches eindeutig bestimmt, d.h. ist $\varphi\colon \mathrm{Mat}(n \times n, K) \to K$ eine lineare Abbildung mit $\varphi(AB) = \varphi(BA)$ für alle $A, B \in \mathrm{Mat}(n \times n, K)$, so gibt es einen eindeutigen Skalar $\lambda \in K$ mit $\varphi = \lambda\,\mathrm{spur}$.

2. Dass $\mathrm{spur}(AB) = \mathrm{spur}(BA)$ für alle $A, B \in \mathrm{Mat}(n \times n, K)$ ist wegen der Linearität der Spur äquivalent dazu, dass $\mathrm{spur}(AB - BA) = 0$ für alle $A, B \in \mathrm{Mat}(n \times n, K)$. Also ist $AB - BA \in \mathfrak{sl}_n(K)$ für alle $A, B \in \mathrm{Mat}(n \times n, K)$. Es lässt sich zeigen, dass sogar

$$\mathfrak{sl}_n(K) = \mathcal{L}(\{AB - BA \mid A, B \in \mathrm{Mat}(n \times n, K)\}),$$

wobei $\mathcal{L}$ die linear Hülle bezeichnet.

3. Als lineare Abbildung spur: $\mathrm{Mat}(n \times n, K) \to K$ ist die Spur surjektiv, denn für alle $\lambda \in K$ ist $\lambda = \mathrm{spur}(\mathrm{diag}(\lambda, 0, \ldots, 0))$. Daher ist

$$\begin{aligned}\dim(\mathfrak{sl}_n(K)) &= \dim(\ker(\mathrm{spur})) = \dim(\mathrm{Mat}(n \times n, K)) - \dim(\mathrm{im}(\mathrm{spur})) \\ &= \dim(\mathrm{Mat}(n \times n, K)) - \dim(K) = n^2 - 1.\end{aligned}$$

Bezeichnet $E_{ij} \in \mathrm{Mat}(n \times n, K)$ für $1 \leq i, j \leq n$ die Matrix mit

$$(E_{ij})_{kl} = \begin{cases} 1 & \text{falls } (k,l) = (i,j), \\ 0 & \text{sonst,} \end{cases}$$

so ist $\{E_{ij} \mid 1 \leq i \neq j \leq n\} \cup \{E_{ii} - E_{i+1,i+1} \mid i \in \{1, \ldots, n-1\}\}$ eine Basis von $\mathfrak{sl}_n(K)$.

4.9. Funktionenräume

Wie in 4.6 gesehen wird $\mathrm{Abb}(X, K)$ vermöge der punktweisen Addition und Skalarmultiplikation zu einem K-Vektorraum, d.h. für alle $f, g \in \mathrm{Abb}(X, K)$ und $\lambda \in K$ ist

$$(f+g)(x) = f(x) + g(x) \quad \text{und} \quad (\lambda \cdot f)(x) = \lambda \cdot f(x) \quad \text{für alle } x \in X.$$

Wir geben in diesem Abschnitt verschiedene Beispiele für Vektorräume von reellwertigen Funktionen, wie sie etwa in der Analysis eine Rolle spielen. Wir werden diese jeweils als Untervektorräume von Vektorräumen der Form $\mathrm{Abb}(X, \mathbb{R})$ konstruieren.

4.9.1. Beschränkte Funktionen

Es sei X eine beliebige Menge. Eine Funktion $f\colon X \to \mathbb{R}$ heißt *beschränkt*, falls es eine Konstante $C \geq 0$ gibt, so dass $|f(x)| \leq C$ für alle $x \in X$. Es sei

$$B(X, \mathbb{R}) \coloneqq \{f\colon X \to \mathbb{R} \mid f \text{ ist beschränkt}\} \subseteq \mathrm{Abb}(X, \mathbb{R}).$$

Wir zeigen, dass $B(X, \mathbb{R})$ bezüglich der punktweisen Addition und Skalarmultiplikation einen $\mathbb{R}$-Vektorraum bildet. Hierfür zeigen wir, dass $B(X, \mathbb{R}) \subseteq \mathrm{Abb}(X, \mathbb{R})$ ein Untervektorraum ist.

Die Nullfunktion $N \in \mathrm{Abb}(X, \mathbb{R})$ ist beschränkt, denn für $C \coloneqq 0$ ist

$$|N(x)| = |0| = 0 \leq C \quad \text{für alle } x \in X.$$

Also ist die Nullfunktion N beschränkt und deshalb $N \in B(X, \mathbb{R})$. Sind $f, g \in B(X, \mathbb{R})$, so gibt es Konstanten $C_f, C_g \geq 0$ mit

$$|f(x)| \leq C_f \quad \text{und} \quad |g(x)| \leq C_g \quad \text{für alle } x \in X.$$

Für $C_{f+g} \coloneqq C_f + C_g$ ist $C_{f+g} \geq 0$ und nach der Dreieckungleichung ist

$$|(f+g)(x)| = |f(x) + g(x)| \leq |f(x)| + |g(x)| \leq C_f + C_g = C_{f+g} \quad \text{für alle } x \in X.$$

Also ist auch $f+g$ beschränkt und somit $f+g \in B(X,\mathbb{R})$. Für $\lambda \in \mathbb{R}$ und $C_{\lambda f} \coloneqq |\lambda| C_f \geq 0$ ist nach der Homogenität des Betrags

$$|(\lambda f)(x)| = |\lambda f(x)| = |\lambda||f(x)| \leq |\lambda| C_f = C_{\lambda f} \quad \text{für alle } x \in X.$$

Also ist auch λf beschränkt und somit $\lambda f \in B(X,\mathbb{R})$. Ingesamt zeigt dies, dass $B(X,\mathbb{R})$ ein Untervektorraum von $\mathrm{Abb}(X,\mathbb{R})$ ist.

Bemerkung 4.22. Ersetzt man $\mathbb{R}$ und $\mathbb{C}$, so enthält man den $\mathbb{C}$-Vektorraum $B(X,\mathbb{C})$ der komplexwertigen beschränkten Funktionen auf X.

4.9.2. Gerade und ungerade Funktionen

Eine Funktion $f\colon \mathbb{R} \to \mathbb{R}$ heißt *gerade*, falls $f(x) = f(-x)$ für alle $x \in \mathbb{R}$ und *ungerade*, falls $f(-x) = -f(x)$ für alle $x \in \mathbb{R}$. Es seien

$$G(\mathbb{R},\mathbb{R}) \coloneqq \{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ ist gerade}\}$$

und

$$U(\mathbb{R},\mathbb{R}) \coloneqq \{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ ist ungerade}\}.$$

Wir zeigen, dass G und U mit der punktweisen Addition und Skalarmultiplikation einen $\mathbb{R}$-Vektorraum, indem wir zeigen, dass $G(\mathbb{R},\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R},\mathbb{R})$ und $U(\mathbb{R},\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R},\mathbb{R})$ Untervektorräume sind.

Für die Nullfunktion $N\colon \mathbb{R} \to \mathbb{R}$ gilt $N(x) = 0 = N(-x)$ und $N(-x) = 0 = -0 = -N(x)$ für alle $x \in \mathbb{R}$, also ist N gerade und ungerade, und somit $N \in G(\mathbb{R},\mathbb{R})$ und $N \in U(\mathbb{R},\mathbb{R})$.

Sind $f, g \in G(\mathbb{R},\mathbb{R})$ und ist $\lambda \in \mathbb{R}$, so ist

$$(f+g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f+g)(x) \quad \text{für alle } x \in \mathbb{R}$$

und

$$(\lambda f)(-x) = \lambda f(-x) = \lambda f(x) = (\lambda f)(x) \quad \text{für alle } x \in \mathbb{R}.$$

Also sind dann auch $f+g$ und λf gerade und somit $f+g, \lambda f \in G(\mathbb{R},\mathbb{R})$. Das zeigt, dass $G(\mathbb{R},\mathbb{R})$ ein Untervektorraum von $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ ist.

Sind $f, g \in U(\mathbb{R},\mathbb{R})$ und ist $\lambda \in \mathbb{R}$, so ist

$$(f+g)(-x) = f(-x) + g(-x) = -f(x) - g(x) = -(f(x) + g(x)) = -(f+g)(x)$$

und

$$(\lambda f)(-x) = \lambda f(-x) = -\lambda f(x) = -(\lambda f)(x)$$

für alle $x \in \mathbb{R}$. Also sind dann auch $f+g$ und λf ungerade und somit $f+g, \lambda f \in U(\mathbb{R},\mathbb{R})$. Das zeigt, dass $U(\mathbb{R},\mathbb{R})$ ein Untervektorraum von $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ ist.

Bemerkung 4.23. 1. Ist $f\colon \mathbb{R} \to \mathbb{R}$ eine beliebige Funktion, so gibt es eine eindeutige gerade Funktion $g\colon \mathbb{R} \to \mathbb{R}$ und eindeutige ungerade Funktion $u\colon \mathbb{R} \to \mathbb{R}$ mit $f = g + u$. Die

Eindeutigkeit folgt daraus, falls $f = g + u$ mit g gerade und u ungerade, sich g und u durch $g(x) = (f(x) + f(-x))/2$ und $u(x) = (f(x) - f(-x))/2$ für alle $x \in \mathbb{R}$ ergeben.

Ist andererseits $f\colon \mathbb{R} \to \mathbb{R}$ beliebig, so definiert $g(x) \coloneqq (f(x) + f(-x))/2$ eine gerade Funktion und $u(x) \coloneqq (f(x) - f(-x))/2$ eine ungerade Funktion, und es gilt $f = g + u$. Das zeigt die Existenz.

2. Für einen beliebigen Körper K und zwei K-Vektorräume V und W kann man eine Funktion $f\colon V \to W$ als gerade definieren, falls $f(v) = f(-v)$ für alle $v \in V$, und als ungerade, falls $f(-v) = -f(v)$ für alle $v \in V$. Dann sind

$$G(V, W) \coloneqq \{f\colon V \to W \mid f \text{ ist gerade}\}$$

und

$$U(V, W) \coloneqq \{f\colon V \to W \mid f \text{ ist ungerade}\}$$

Untervektorräume des K-Vektorraums $\mathrm{Abb}(V, W)$, und somit selber K-Vektorräume bezüglich der punktweisen Addition und Skalarmultiplikation.

Ist $f\colon V \to W$ linear, so ist $f(-v) = -f(v)$ für alle $v \in V$, also f ungerade. Daher ist $\mathrm{Hom}_K(V, W) \subseteq U(V, W)$ ein Untervektorraum.

4.9.3. Radialsymmetrische reellwertige Funktionen auf $\mathbb{R}^n$

Definition 4.24. *Eine Funktion $f\colon \mathbb{R}^n \to \mathbb{R}$ heißt* radialsymmetrisch, *falls es eine Funktion $\rho_f\colon [0, \infty) \to \mathbb{R}$ gibt, so dass $f(x) = \rho(|x|)$ für alle $x \in \mathbb{R}^n$.*

Es sei

$$R \coloneqq \{f\colon \mathbb{R}^n \to \mathbb{R} \mid f \text{ ist radialsymmetrisch}\}.$$

Wir zeigen, dass R ein Vektorraum bezüglich der punktweisen Addition und Skalarmultiplikation ist, indem wir zeigen, dass $R \subseteq \mathrm{Abb}(\mathbb{R}^n, \mathbb{R})$ ein Untervektorraum ist:

Die Nullfunktion $N\colon \mathbb{R}^n \to \mathbb{R}$ ist radialsymmetrisch, denn für $\rho_N\colon [0, \infty) \to \mathbb{R}$, $r \mapsto 0$ ist

$$N(x) = 0 = \rho_N(|0|) \quad \text{für alle } x \in \mathbb{R}^n.$$

Also ist $N \in R$. Sind $f, g \in R$, so gibt es Funktionen $\rho_f, \rho_g\colon [0, \infty) \to \mathbb{R}$ mit $f(x) = \rho_f(|x|)$ und $g(x) = \rho_g(|x|)$ für alle $x \in \mathbb{R}^n$. Für $\rho_{f+g} = \rho_f + \rho_g$ ist daher

$$(f + g)(x) = f(x) + g(x) = \rho_f(|x|) + \rho_g(|x|) = (\rho_f + \rho_g)(|x|) = \rho_{f+g}(|x|)$$

für alle $x \in \mathbb{R}^n$. Also ist $f + g$ radialsymmetrisch und deshalb auch $f + g \in R$. Ist ferner $\lambda \in \mathbb{R}$, so gilt für $\rho_{\lambda f} = \lambda \rho_f$, dass

$$(\lambda f)(x) = \lambda f(x) = \lambda \rho_f(|x|) = (\lambda \rho_f)(|x|) = \rho_{\lambda f}(|x|) \quad \text{für alle } x \in \mathbb{R}^n.$$

Also ist auch λf radialsymmetrisch und somit $\lambda f \in R$. Dies zeigt, dass $R \subseteq \mathrm{Abb}(\mathbb{R}^n, \mathbb{R})$ ein Untervektorraum ist.

4.9.4. Periodische Funktionen auf $\mathbb{R}$

Definition 4.25. *Eine reellwertige Funktion $f\colon \mathbb{R} \to \mathbb{R}$ heißt* periodisch *mit* Periode $T > 0$, *oder auch* T-periodisch, *falls*

$$f(x+T) = f(x) \quad \textit{für alle } x \in \mathbb{R}.$$

Für $T > 0$ sei $P_T(\mathbb{R}) \coloneqq \{f\colon \mathbb{R} \to \mathbb{R} \mid f \textit{ ist } T\textit{-periodisch}\}$.

Es sei $T > 0$. Wir zeigen, dass Summen und Vielfache von T-periodischen Funktionen ebenfalls T-periodisch sind, dass also $P_T(\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ ein Untervektorraum ist:
Die Nullfunktion $N\colon \mathbb{R} \to \mathbb{R}$ ist T-periodisch, denn

$$N(x+T) = 0 = N(x) \quad \text{für alle } x \in \mathbb{R}.$$

(Allgemeiner gilt, dass jede konstante Funktion T-periodisch ist.) Sind $f, g \in P_T(\mathbb{R})$, so ist

$$(f+g)(x+T) = f(x+T) + g(x+T) = f(x) + g(x) = (f+g)(x) \quad \text{für alle } x \in \mathbb{R},$$

also auch $f + g \in P_T(\mathbb{R})$. Ist $f \in P_T(\mathbb{R})$ und $\lambda \in \mathbb{R}$, so ist

$$(\lambda f)(x+T) = \lambda f(x+T) = \lambda f(x) = (\lambda f)(x) \quad \text{für alle } x \in \mathbb{R},$$

also auch $\lambda f \in P_T(\mathbb{R})$. Das zeigt, dass $P_T(\mathbb{R})$ ein Untervektorraum von $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ ist.

Bemerkung 4.26. Statt den T-periodischen reellwertigen Funktionen lassen sich auch die T-periodische komplexwertige Funktionen betrachten, d.h. die Funktionen der Form $f\colon \mathbb{R} \to \mathbb{C}$ mit $f(x+T) = f(x)$ für alle $x \in \mathbb{R}$. Anstelle des reellen Vektorraums $P_T(\mathbb{R})$ erhalten wir dann den komplexen Vektorraum $P_T(\mathbb{C}) = \{f\colon \mathbb{R} \to \mathbb{C} \mid f \text{ ist } T\text{-periodisch}\}$. Dabei ist eine Funktion $f\colon \mathbb{R} \to \mathbb{C}$ genau dann T-periodisch, falls der Realteil $\Re(f)\colon \mathbb{R} \to \mathbb{R}$ und der Imaginärteil $\Im(f)\colon \mathbb{R} \to \mathbb{R}$ beide T-periodisch ist.
Fassen wir $P_T(\mathbb{C})$ als reellen Vektorraum auf, so ist $P_T(\mathbb{R}) \subseteq P_T(\mathbb{C})$ ein Untervektorraum.

4.9.5. Stetige reellwertige Funktionen auf $\mathbb{R}$

Wir werden für dieses Beispiel den Begriff konvergenter Folgen nutzen. An die entsprechenden Begriffe und Eigeschaften erinnern wir in B. Wir werden insbesondere die Eigenschaften aus Bemerkung 2.3 nutzen.

Definition 4.27. *Eine Funktion $f\colon \mathbb{R} \to \mathbb{R}$ heißt* stetig, *falls für jede konvergente Folge reeller Zahlen $(x_n)_{n\in\mathbb{N}}$ auch die Bildfolge $(f(x_n))_{n\in\mathbb{N}}$ konvergiert und dann auch*

$$f\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} f(x_n).$$

Es sei

$$C(\mathbb{R}, \mathbb{R}) \coloneqq \{f\colon \mathbb{R} \to \mathbb{R} \mid f \textit{ ist stetig}\}.$$

(Der Buchstabe C steht hier für continuous, *die englische Übersetzung von* stetig.*)*

Wir zeigen, dass Summen und skalare Vielfache von stetigen Funktionen wieder stetig sind, dass also $C(\mathbb{R},\mathbb{R})$ zusammen mit der punktweisen Addition und Skalarmultiplikation einen Vektorraum bildet, indem wir zeigen, dass $C(\mathbb{R},\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R},\mathbb{R})$ ein Untervektorraum ist.

Für die Nullfunktion $N\colon \mathbb{R} \to \mathbb{R}$ ist $N(x) = 0$ für alle $x \in \mathbb{R}$. Ist $(x_n)_{n\in\mathbb{N}}$ eine konvergente Folge reeller Zahlen, so ist deshalb die Bildfolge $(N(x_n))_{n\in\mathbb{N}}$ die konstante Nullfolge. Inbesondere ist die Bildfolge konvergent und

$$\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} 0 = 0 = f\left(\lim_{n\to\infty} x_n\right).$$

Also ist die Nullfunktion stetig und somit $N \in C(\mathbb{R},\mathbb{R})$.

Sind $f, g \in C(\mathbb{R},\mathbb{R})$ und ist $(x_n)_{n\in\mathbb{N}}$ eine konvergente Folge reeller Zahlen, so konvergieren auch die beiden Folgen $(f(x_n))_{n\in\mathbb{N}}$ und $(g(x_n))_{n\in\mathbb{N}}$ und

$$\lim_{n\to\infty} f(x_n) = f\left(\lim_{n\to\infty} x_n\right) \quad \text{und} \quad \lim_{n\to\infty} g(x_n) = g\left(\lim_{n\to\infty} x_n\right).$$

Daher ist konvergiert auch die Folge $(f(x_n) + g(x_n))_{n\in\mathbb{N}} = ((f+g)(x_n))_{n\in\mathbb{N}}$ und es gilt

$$\begin{aligned}\lim_{n\to\infty} (f+g)(x_n) &= \lim_{n\to\infty} (f(x_n) + g(x_n)) = \left(\lim_{n\to\infty} f(x_n)\right) + \left(\lim_{n\to\infty} g(x_n)\right) \\ &= f\left(\lim_{n\to\infty} x_n\right) + g\left(\lim_{n\to\infty} x_n\right) = (f+g)\left(\lim_{n\to\infty} x_n\right).\end{aligned}$$

Also ist auch $f + g$ stetig und somit $f + g \in C(\mathbb{R},\mathbb{R})$.

Ist $\lambda \in \mathbb{R}$, $f \in C(\mathbb{R},\mathbb{R})$ und $(x_n)_{n\in\mathbb{N}}$ eine konvergente Folge reeller Zahlen, so konvergiert auch die Folge $(f(x_n))_{n\in\mathbb{N}}$ und es ist $\lim_{n\to\infty} f(x_n) = f(\lim_{n\to\infty} x_n)$. Daher konvergiert auch die Folge $(\lambda f(x_n))_{n\in\mathbb{N}} = ((\lambda f)(x_n))_{n\in\mathbb{N}}$ und

$$\lim_{n\to\infty} (\lambda f)(x_n) = \lim_{n\to\infty} (\lambda f(x_n)) = \lambda \lim_{n\to\infty} f(x_n) = \lambda f\left(\lim_{n\to\infty} x_n\right) = (\lambda f)\left(\lim_{n\to\infty} x_n\right).$$

Also ist auch λf stetig und somit $\lambda f \in C(\mathbb{R},\mathbb{R})$.

Ingesamt zeigt dies, dass $C(\mathbb{R},\mathbb{R})$ ein Untervektorraum von $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ ist.

Bemerkung 4.28. Statt reellwertige Funktionen lassen sich auch komplexwertige Funktionen betrachten, und statt $\mathbb{R}$ lässt sich auch $\mathbb{C}$ als Definitionsbereich nutzen. So erhält man die $\mathbb{R}$-Vektorräume

$$C(\mathbb{R},\mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ ist stetig}\} \quad \text{und} \quad C(\mathbb{C},\mathbb{R}) = \{f\colon \mathbb{C} \to \mathbb{R} \mid f \text{ ist stetig}\}$$

und die $\mathbb{C}$-Vektorräume

$$C(\mathbb{R},\mathbb{C}) = \{f\colon \mathbb{R} \to \mathbb{C} \mid f \text{ ist stetig}\} \quad \text{und} \quad C(\mathbb{C},\mathbb{C}) = \{f\colon \mathbb{C} \to \mathbb{C} \mid f \text{ ist stetig}\}.$$

Fasst man $C(\mathbb{R},\mathbb{C})$ und $C(\mathbb{C},\mathbb{C})$ als $\mathbb{R}$-Vektorräume auf, so sind $C(\mathbb{R},\mathbb{R}) \subseteq C(\mathbb{R},\mathbb{C})$ und $C(\mathbb{C},\mathbb{R}) \subseteq C(\mathbb{C},\mathbb{C})$ Untervektorräume.

4.9.6. Hölder-stetige Funktionen auf $\mathbb{R}$

Es sei $\alpha > 0$.

Definition 4.29. *Eine Abbildung $f\colon \mathbb{R} \to \mathbb{R}$ heißt* Hölder-stetig mit Exponent α *falls es eine Konstante $C_f \geq 0$ gibt, so dass $|f(x) - f(y)| \leq C_f|x - y|$ für alle $x, y \in \mathbb{R}$. Es sei*

$$C^\alpha(\mathbb{R}) \coloneqq \{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ ist Hölder-stetig mit Exponent } \alpha\}.$$

Wir zeigen, dass die Hölder-stetigen Funktionen mit Exponent α zusammen mit der punktweisen Addition und Skalarmultiplikation einen $\mathbb{R}$-Vektorraum bildet, indem wir zeiges, dass $C^\alpha(\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ ein Untervektorraum ist.

Für die Nullfunktion $N\colon \mathbb{R} \to \mathbb{R}$ und $C_0 \coloneqq 0$ ist

$$|N(x) - N(y)| = |0 - 0| = 0 = 0 \cdot |x - y|^\alpha \leq C_0 \cdot |x - y|^\alpha \quad \text{für alle } x, y \in \mathbb{R}.$$

Also ist N Hölder-stetig mit Exponent α und somit $N \in C^\alpha(\mathbb{R})$.

Sind $f, g \in C^\alpha(\mathbb{R})$, so gibt es Konstanten $C_f, C_g \geq 0$ mit $|f(x) - f(y)| \leq C_f|x - y|$ und $|g(x) - g(y)| \leq C_g|x - y|$ für alle $x, y \in \mathbb{R}$. Für $C_{f+g} \coloneqq C_f + C_g$ ergibt sich mithilfe der Dreiecksungleichung, dass

$$\begin{aligned} |(f+g)(x) - (f+g)(y)| &= |f(x) + g(x) - f(y) - g(y)| = |f(x) - f(y) + g(x) - g(y)| \\ &\leq |f(x) - f(y)| + |g(x) - g(y)| \leq C_f|x - y|^\alpha + C_g|x - y|^\alpha \\ &= (C_f + C_g)|x - y|^\alpha = C_{f+g}|x - y|^\alpha \end{aligned}$$

für alle $x, y \in \mathbb{R}$. Also ist auch $f + g$ Hölder-stetig mit Exponent α und somit $f + g \in C^\alpha(\mathbb{R})$.

Ist $f \in C^\alpha(\mathbb{R})$ und $\lambda \in \mathbb{R}$, so gibt es eine Konstante $C_f \geq 0$ mit $|f(x) - f(y)| \leq C_f|x - y|$ für alle $x, y \in \mathbb{R}$. Für $C_{\lambda f} \coloneqq |\lambda| C_f$ ist deshalb

$$\begin{aligned} |(\lambda f)(x) - (\lambda f)(y)| &= |\lambda f(x) - \lambda f(y)| = |\lambda(f(x) - f(y))| \\ &= |\lambda||f(x) - f(y)| \leq |\lambda| C_f|x - y|^\alpha = C_{\lambda f}|x - y|^\alpha \end{aligned}$$

für alle $x, y \in \mathbb{R}$. Also ist auch λf Hölder-stetig mit Exponent α und somit $\lambda f \in C^\alpha(\mathbb{R})$.

Ingesamt zeigt dies, dass $C^\alpha(\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ ein Untervektorraum ist.

Bemerkung 4.30. 1. Es lässt sich zeigen, dass Hölder-stetige Funktionen bereits stetig sind (wie der Name vermuten lässt). Für $\alpha > 1$ ist zudem $C^\alpha(\mathbb{R}) = \{0\}$, d.h. die Nullfunktionen ist die einzige Hölder-stetige Funktion $\mathbb{R} \to \mathbb{R}$ mit Exponent $\alpha > 1$.

2. Hölder-stetige Funktionen mit Exponenten $\alpha = 1$ heißen auch *Lipschitz-stetig*

4.9.7. Funktionen mit kompakten Träger

4.10. Folgenräume

Für einen Körper K sei

$$\ell(K) \coloneqq \mathrm{Abb}(\mathbb{N}, K) = \{a\colon \mathbb{N} \to K\} = \{(a_n)_{n\in\mathbb{N}} \mid a_n \in K \text{ für alle } n \in K\}$$

der Raum der Folgen in K. Wie bereits in 4.6 gesehen, ist $\ell(K)$ ein K-Vektorraum bezüglich der eintragsweisen Addition

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{für alle } (a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \ell(K).$$

und eintragsweisen Skalarmultiplikation

$$\lambda \cdot (a_n)_{n\in\mathbb{N}} = (\lambda \cdot a_n)_{n\in\mathbb{N}} \quad \text{für alle } \lambda \in K \text{ und } (a_n)_{n\in\mathbb{N}} \in \ell(K).$$

4.10.1. Beschränkte Folgen

4.10.2. Konvergente Folgen

Für $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ sei

$$\mathcal{K}(\mathbb{K}) \coloneqq \{(a_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K}) \mid (a_n)_{n\in\mathbb{N}} \text{ konvergiert (mit Grenzwert in } \mathbb{K})\}.$$

Wir zeigen, dass $\mathcal{K}(\mathbb{K})$ ein $\mathbb{K}$-Vektorraum bezüglich der eintragsweisen Addition und Skalarmultiplikation ist, indem wir zeigen, dass $\mathcal{K}(\mathbb{K}) \subseteq \ell(\mathbb{K})$ ein Untervektorraum ist:

Wie bereits in Bemerkung 2.3 konvergiert die konstante Nullfolge $(0)_{n\in\mathbb{N}}$ gegen 0. Also ist $(0)_{n\in\mathbb{N}} \in \mathcal{K}(\mathbb{K})$.

Sind $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{K}(\mathbb{K})$, so konvergiert auch die Folge $(x_n + y_n)_{n\in\mathbb{N}}$, weshalb auch $(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}} \in \mathcal{K}(\mathbb{K})$.

Ist $(x_n)_{n\in\mathbb{N}} \in \mathcal{K}(\mathbb{K})$ und $\lambda \in \mathbb{K}$, so konvergiert auch die Folge $(\lambda x_n)_{n\in\mathbb{N}}$, weshalb auch $\lambda(x_n)_{n\in\mathbb{N}} = (\lambda x_n)_{n\in\mathbb{N}} \in \mathcal{K}(\mathbb{K})$.

Insgesamt zeigt dies, dass $\mathcal{K}(\mathbb{K})$ ein Untervektorraum von $\ell(\mathbb{K})$ ist.

4.10.3. Cauchy-Folgen

Für $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ sei

$$\mathcal{C}(\mathbb{K}) \coloneqq \{(a_n)_{n\in\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ ist eine Cauchy-Folge}\}.$$

4.10.4. ℓ^p-Räume

4.10.5.

4.10.6. Rekursiv definierte Folgen

4.11. Potenzmengen als $\mathbb{F}_2$-Vektorräume

4.12. Eigenräume

Definition 4.31. *Es sei V ein K-Vektorraum und $f\colon V \to V$ ein Endomorphismus. Ein Vektor $v \in V$ mit $v \neq 0$ heißt* Eigenvektor *von f, falls es ein $\lambda \in K$ gibt, so dass $f(v) = \lambda v$. Der*

Skalar λ heißt dann Eigenwert *von f. Für alle $\lambda \in K$ ist*

$$\begin{aligned}\operatorname{Eig}(f,\lambda) &:= \{v \in V \mid f(v) = \lambda v\} \\ &= \{v \in V \mid v \text{ ist ein Eigenvektor von } f \text{ zum Eigenwert } \lambda\} \cup \{0\}.\end{aligned}$$

der Eigenraum *von f zum Eigenwert λ.*

Es sei V ein K-Vektorraum, $f\colon V \to V$ ein Endomorphismus und $\lambda \in K$. Wir zeigen, dass der Eigenraum $\operatorname{Eig}(f,\lambda)$ ein Untervektorraum von V ist.

Da $f(0) = 0 = \lambda \cdot 0$ ist $0 \in \operatorname{Eig}(f,\lambda)$. Für $v, w \in \operatorname{Eig}(f,\lambda)$ ist $f(v) = \lambda v$ und $f(w) = \lambda w$ und somit

$$f(v+w) = f(v) + f(w) = \lambda v + \lambda w = \lambda(v+w),$$

also auch $v + w \in \operatorname{Eig}(f,\lambda)$. Ist $v \in \operatorname{Eig}(f,\lambda)$ und $\mu \in K$, so ist wegen $f(v) = \lambda v$ auch

$$f(\mu v) = \mu f(v) = \mu\lambda f(v) = \lambda(\mu v),$$

also auch $\mu v \in \operatorname{Eig}(f,\lambda)$. Ingesamt zeigt dies, dass $\operatorname{Eig}(f,\lambda)$ ein Untervektorraum von V ist.

Bemerkung 4.32. Die obigen Rechnungen lassen sich auch umgehen: Für $v \in V$ ist

$$f(v) = \lambda v \iff f(v) - \lambda v = 0 \iff (f - \lambda \mathrm{id}_V)(v) = 0.$$

Wegen der Vektorraumstruktur von $\operatorname{End}_K(V)$ ist auch $f - \lambda\mathrm{id}_V\colon V \to V$ linear. Also ist

$$\ker(f - \lambda\mathrm{id}_V) = \operatorname{Eig}(f,\lambda)$$

ein Untervektorraum.

Beispiel(e).

1. Ist V ein K-Vektorraum und $f\colon V \to V$ ein Endomorphismus, so ist

   $$\operatorname{Eig}(f,0) = \{v \in V \mid f(v) = 0 \cdot v\} = \{v \in V \mid f(v) = 0\} = \ker(f).$$

   Die Elemente von

   $$\operatorname{Eig}(f,1) = \{v \in V \mid f(v) = 1 \cdot v\} = \{v \in V \mid f(v) = v\}$$

   sind die *Fixpunkte* von f.

2. Es sei $\mathcal{T}\colon \operatorname{Mat}(n\times n, K) \to \operatorname{Mat}(n\times n, K)$, $A \mapsto A^T$ das Transponieren. Wie bereits in Bemerkung 4.16 gesehen ist $\mathcal{T}$ linear. Es ist

   $$\operatorname{Eig}(\mathcal{T},1) = \{A \in \operatorname{Mat}(n\times n, K) \mid A^T = 1 \cdot A = A\} = \operatorname{Sym}_n(K)$$

   und

   $$\operatorname{Eig}(\mathcal{T},-1) = \{A \in \operatorname{Mat}(n\times n, K) \mid A^T = (-1)\cdot A = -A\} = \operatorname{Alt}_n(K).$$

   Für alle $\lambda \in K$ mit $\lambda \notin \{1,-1\}$ ist $\operatorname{Eig}(\mathcal{T},\lambda) = \{0\}$, d.h. 1 und -1 sind die einzigen Eigenwerte von $\mathcal{T}$. Ist nämlich $\lambda \in K$ ein Eigenwert von $\mathcal{T}$ und $A \in \operatorname{Mat}(n\times n, K)$ ein Eigenvektor von $\mathcal{T}$ zum Eigenwert λ, so ist

   $$A = (A^T)^T = \mathcal{T}(\mathcal{T}(A)) = \mathcal{T}(\lambda A) = \lambda\mathcal{T}(A) = \lambda^2 A.$$

   Da A ein Eigenvektor ist, ist insbesondere $A \neq 0$; daher folgt aus der obigen Gleichung, dass $\lambda^2 = 1$, also $\lambda = \pm 1$.

3. Wir betrachten den reellen Vektorraum $V := \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ und den Endomorphismus $\Phi\colon V \to V$ mit

$$\Phi(f)(x) = f(-x) \quad \text{für alle } x \in \mathbb{R}.$$

Φ ist linear, denn für alle $f, g \in V$ ist

$$\begin{aligned}\Phi(f+g)(x) &= (f+g)(-x)\\ &= f(-x) + g(-x) = \Phi(f)(x) + \Phi(g)(x) = (\Phi(x) + \Phi(g))(x)\end{aligned}$$

für alle $x \in \mathbb{R}$, und somit $\Phi(f+g) = \Phi(f) + \Phi(g)$; für alle $f \in V$ und $\lambda \in \mathbb{R}$ ist

$$\Phi(\lambda f)(x) = (\lambda f)(-x) = \lambda f(-x) = \lambda\Phi(f)(x) = (\lambda\Phi(f))(x)$$

für alle $x \in \mathbb{R}$, und somit $\Phi(\lambda f) = \lambda\Phi(f)$.

Eine Funktion $f \in V$ ist ein Eigenvektor von Φ zum Eigenwert 1, falls $f = \Phi(f)$, also

$$f(x) = \Phi(f)(x) = f(-x) \quad \text{für alle } x \in \mathbb{R}.$$

Also ist $\mathrm{Eig}(\Phi, 1)$ der Vektorraum der geraden Funktionen (siehe 4.9.2. Eine Funktion $f \in V$ ist ein Eigenvektor von Φ zum Eigenwert -1, falls $f = -\Phi(f)$, also

$$f(-x) = \Phi(f)(x) = (-f)(x) = -f(x) \quad \text{für alle } x \in \mathbb{R}.$$

Also ist $\mathrm{Eig}(\Phi, -1)$ der Vektorraum der ungeraden Funktionen.

Für alle $f \in V$ ist

$$\Phi(\Phi(f))(x) = \Phi(f)(-x) = f(-(-x)) = f(x) \quad \text{für alle } x \in \mathbb{R},$$

also $\Phi(\Phi(f)) = f$. Analog wie beim vorherigen Beispiel der Transposition ergibt sich daraus, dass 1 und -1 die einzigen Eigenwerte von Φ sind.

4.13. Ausblick: $\mathbb{Q}$-Vektorräume und teilbare abelsche Gruppen

4.14. Produkte und direkte Summen

4.14.1. Produkte

4.14.2. Direkte Summen

4.15. Ausblick: Quotientenvektorräume

4.16. Ausblick: Freie Vektorräume

4.17. (Ausblick?) Bilineare Abbildungen

4.17.1. Allgemeine bilineare Abbildungen

Definition 4.33. *Es seien V_1, V_2 und W drei K-Vektorräume. Eine Abbildung $B\colon V_1 \times V_2 \to W$ heißt* K-bilinear*, falls*

i) $B(x_1 + x_2, y) = B(x_1, y) + B(x_2, y)$ *für alle* $x_1, x_2 \in V_1$ *und* $y \in V_2$*,*

ii) $B(x, y_1 + y_2) = B(x, y_1) + B(x, y_2)$ *für alle* $x \in V_1$ *und* $y_1, y_2 \in V_2$*,*

iii) $B(\lambda x, y) = \lambda B(x, y)$ *und* $B(x, \lambda y) = 0$ *für alle* $\lambda \in K$*,* $x \in V_1$ *und* $y \in V_2$*.*

Es sei

$$\mathrm{Bil}(V_1, V_2; W) = \{B\colon V_1 \times V_2 \to W \mid B \text{ ist bilinear}\}.$$

Bemerkung 4.34. Die Bilinearität von $B\colon V_1 \times V_2 \to W$ ist äquivalent dazu, dass die Abbildungen

$$B(x, -)\colon V_2 \to W, \quad y \mapsto B(x, y)$$

und

$$B(-, y)\colon V_1 \to W, \quad x \mapsto B(x, y)$$

für alle $x \in V_1$ und $y \in V_2$ linear sind. Daher erklärt den Begriff „bilinear“.

Die folgenden Beispiele erläutern, dass man sich Skalarprodukte im Großen und Ganzen als Produkte vorstellen kann.

Beispiel(e). 1. Für alle $l, m, n \in \mathbb{N}$ ist die Matrixmultiplikation

$$m\colon \mathrm{Mat}(l \times m, K) \times \mathrm{Mat}(m \times n, K) \to \mathrm{Mat}(l \times n, K), \quad (A, B) \mapsto AB$$

K-bilinear.

2. Das *Standardskalarprodukt*

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, \quad (x, y) \mapsto x \cdot y \coloneqq \sum_{i=1}^{n} x_i y_i$$

ist $\mathbb{R}$-bilinear.

3. Das *Kreuzprodukt*

$$\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}, \quad (x, y) \mapsto x \times y \coloneqq (x_1 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1)$$

ist eine $\mathbb{R}$-lineare Abbildung.

4. Allgemeiner ist für jedes $n \in \mathbb{N}$ die *Standardbilinearform*

$$\langle -, - \rangle : K^n \times K^n \to K, \quad (x, y) \mapsto \langle x, y \rangle \coloneqq \sum_{i=1}^{n} x_i y_i$$

K-bilinear.

5. Ist V ein K-Vektorraum, so ist die *Evaluation*

$$\mathrm{ev} \colon V^* \times V \to K, \quad (f, v) \mapsto f(v)$$

K-bilinear.

6. Ist V ein K-Vektorraum, so ist die *Anwendung*

$$A \colon \mathrm{End}(V) \times V \to V, \quad (f, v) \mapsto f(v)$$

K-bilinear.

7. Ist K ein Körper, so ist die Multiplikation des Körpers

$$m \colon K \times K \to K, \quad (x, y) \mapsto x \cdot y$$

eine K-bilineare Abbildung.

8. Für jedes $n \in \mathbb{N}$ ist der *Kommutator*

$$\begin{aligned} \mathrm{Mat}(n \times n, K) \times \mathrm{Mat}(n \times n, K) &\to \mathrm{Mat}(n \times n, K), \\ (A, B) &\mapsto [A, B] \coloneqq AB - BA \end{aligned}$$

eine K-bilineare Abbildung.

4.17.2. Symmetrische, alternierende und schiefsymmetrische bilneare Abbildungen

4.17.3. Unterräume bezüglich bilinearer Abbildungen

4.18. Ausblick: Zusätzliche Strukturen auf Vektorräumen

4.18.1. K-Algebren

4.18.2. Lie-Algebren

Anhänge

A. Äquivalenz- und Ordnungsrelationen

Definition 1.1. *Eine* Relation *auf einer Mengen X ist eine Teilmenge $R \subseteq X \times X$. Für $x, y \in X$ sagen wir, dass x in Relation zu y steht, wenn $(x, y) \in R$.*
Die Relation R heißt

i) reflexiv, *falls $(x, x) \in R$ für alle $x \in X$,*

ii) symmetrisch, *falls für alle $x, y \in X$ mit $(x, y) \in R$ auch $(y, x) \in R$,*

iii) anti-symmetrisch, *falls für alle $x, y \in X$ mit $(x, y) \in R$ und $(y, x) \in R$ bereits $x = y$.*

iv) transitiv, *falls für alle $x, y, z \in X$ mit $(x, y) \in R$ und $(y, z) \in R$ auch $(x, z) \in R$,*

Bemerkung 1.2. Manche Autoren nutzen für $(x, y) \in R$ auch die Notation xRy.

Beispiel(e). 1. Auf der Menge $\mathbb{R}$ der reellen Zahlen definieren wir die Relation R durch

$$R \coloneqq \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}.$$

R ist reflexiv, denn für alle $x \in \mathbb{R}$ ist $x \leq x$, also $(x, x) \in R$.

R ist *nicht* symmetrisch, da etwa $(1, 2) \in R$ aber $(2, 1) \notin R$.

R ist allerdings schief-symmetrisch, denn für $x, y \in \mathbb{R}$ mit $(x, y), (y, x) \in R$ ist $x \leq y$ und $y \leq x$, also $x = y$.

R ist auch transitiv, denn für $x, y, z \in \mathbb{R}$ mit $(x, y), (y, z) \in R$ ist $x \leq y$ und $y \leq z$, also auch $x \leq z$, und somit $(x, z) \in \mathbb{R}$.

2. Wir definieren auf der Menge $\mathbb{Q}$ der rationalen Zahlen eine Relation R durch

$$R = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x < y\}.$$

R ist nicht reflexiv, da etwa $(1, 1) \notin R$.

R ist auch nicht symmetrisch, da etwa $(1, 2) \in R$ aber $(2, 1) \notin R$.

R ist anti-symmetrisch, allerdings aus anderen Gründen als in dem vorherigen Beispiel: Sind $x, y \in \mathbb{Q}$ mit $(x, y), (y, x) \in R$, so ist $x < y$ und $y < x$. Dann ist also $x \leq y$ und $y \leq x$ mit $x \neq y$. also $x = y$ mit $x \neq y$. Da dies nicht möglich ist, *gibt es keine* $x, y \in \mathbb{Q}$, so dass sowohl $(x, y) \in R$ also auch $(y, x) \in R$. Die Anti-symmetrie von R ist daher eine leere Aussage und somit erfüllt.

R ist auch transitiv, denn für $x, y, z \in \mathbb{Q}$ mit $(x, y), (y, z) \in R$ ist $x < y$ und $y < z$, also auch $x < z$, und somit $(x, z) \in R$.

3. Es sei X eine beliebige Menge und

$$R = \{(x, x) \mid x \in X\}.$$

(Es steht also jedes Element nur zu sich selbst in Relation.) Es folgt direkt, dass R reflexiv ist. R ist symmetrisch, denn für $(x, y) \in R$ ist $x = y$, also $(y, x) = (x, y) \in R$. R ist auch anti-symmetrisch, denn für $x, y \in X$ mit $(x, y), (y, x) \in R$ ist $x = y$. R ist transitiv, den für $x, y, z \in X$ mit $(x, y), (y, z) \in R$ ist $x = y$ und $y = z$, also auch $x = z$, und somit $(x, z) \in R$.

4. Auf der Menge $\mathbb{Z}$ der ganzen Zahlen definieren wir die Relation

$$R = \{(n, n + 1) \mid n \in \mathbb{Z}\}.$$

(Es steht also jedes ganze Zahl mit genau ihrem Nachfolger in Relation.)

R ist nicht reflexiv, da etwa $(1, 1) \notin R$.

R ist auch nicht symmetrisch, denn für $n, m \in \mathbb{Z}$ mit $(n, m) \in R$ ist $m = n + 1$, also $(m, n) = (n + 1, n) \notin R$.

R ist auch nicht transitiv, denn für $l, m, n \in \mathbb{Z}$ mit $(l, m), (m, n) \in R$ ist $m = l + 1$ und $n = m + 1$, also $n = l + 2$ und somit $(l, n) = (l, l + 2) \notin R$.

R ist allerdings anti-symmetrisch: Sind $n, m \in \mathbb{Z}$ mit $(n, m), (m, n) \in R$, so ist $m = n+1$ ud $n = m + 1$, also $n = n + 2$, was nicht möglich ist. Es gibt also keine $n, m \in \mathbb{Z}$ mit $(n, m) \in R$; daher handelt es sich bei der Anti-Symmetrie von R um eine leere Aussage, die daher gilt.

5. Auf $\mathbb{R}$ definieren wir die Reation

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = \pm y\}.$$

(Zwei Zahlen sind also in Relation, wenn sie bis auf Vorzeichen gleich sind.)

Für jedes $x \in \mathbb{R}$ ist $x = \pm x$, also $(x, x) \in R$. Somit ist R reflexiv.

R ist symmetrisch, denn sind $x, y \in \mathbb{R}$ mit $(x, y) \in R$, so ist $x = \pm y$, also auch $y = \pm x$, und somit $(y, x) \in R$.

R ist allerdings nicht anti-symmetrisch, da etwa $(1, -1), (-1, 1) \in R$ aber $1 \neq -1$.

R ist allerdings transitiv, denn für $x, y, z \in \mathbb{R}$ mit $(x, y), (y, z) \in R$ ist $x = \pm y$ und $y = \pm z$, also auch $x = \pm z$, und somit $(x, z) \in R$.

6. Wir definieren auf der Menge der reellen Zahlen $\mathbb{R}$ eine Relation

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}.$$

(x steht also in Relation zu y, falls x ein Quadratwurzel von y ist.)

R ist nicht reflexiv, da etwa $(2, 2) \notin R$.

R ist auch nicht symmetrisch, da etwa $(2, 4) \in R$ aber $(4, 2) \notin R$.

R ist auch nicht transitiv, da etwa $(2,4) \in R$ und $(4,16) \in R$, aber $(2,16) \notin R$.

R ist allerdings schief-symmetrisch: Sind $x, y \in \mathbb{R}$ mit $(x,y), (y,x) \in R$, so ist $y = x^2$ und $x = y^2$. Inbesondere sind daher $x, y \geq 0$ (da Quadrate reeller Zahlen stets nicht-negativ sind) mit $x = y^2 = (x^2)^2 = x^4$ und analog $y = y^4$. Deshalb ist $x, y \in \{0, 1\}$. Ist $x = 0$, so ist $y = x^2 = 0$ und $x = 0 = y$. Ist $x = 1$, so ist $y = x^2 = 1$ und somit $x = 1 = y$. Es ist also in beiden Fällen $x = y$.

7. Für $x, y \in \mathbb{R}$ sei

$$I(x,y) = \begin{cases} [x,y] & \text{falls } y \geq x, \\ [y,x] & \text{falls } x \leq y. \end{cases}$$

($I(x,y)$ ist also das nicht-leere Intervall mit Randpunkten x und y.) Man bemerke, dass $I(x,z) \subseteq I(x,y) \cup I(y,z)$ für alle $x, y, z \in \mathbb{R}$:

Ist $x \leq z$ und $a \in I(x,z) = [x,z]$, so ist $x \leq a \leq z$; ist dann $a \leq y$, so ist $x \leq a \leq y$, also $a \in [x,y] = I(x,y)$; ist wiederum $y \leq a$, so ist $y \leq a \leq z$, also $a \in [y,z] = I(y,z)$; es ist also in jedem Fall $a \in I(x,y) \cup I(y,z)$.

Ist andererseits $z \leq x$ und $a \in I(x,z) = [z,x]$, so ist $z \leq a \leq x$; ist dann $y \leq a$, so ist $y \leq a \leq x$, also $a \in [y,x] = I(y,x)$; ist andererseits $a \leq y$, so ist $z \leq a \leq y$, also $a \in [z,y] = I(z,y)$; es ist also in jedem Fall $a \in I(y,x) \cup I(z,y) = I(x,y) \cup I(y,z)$.

Für eine Teilmenge $X \subseteq \mathbb{R}$ sei nun

$$R(X) \coloneqq \{(x,y) \in X \times X \mid I(x,y) \subseteq X\}.$$

(Zwei Elemente von $x, y \in X$ stehen also in Relation, wenn man innerhalb der Menge X von x nach y laufen kann.)

$R(X)$ ist transitiv, denn für jedes $x \in X$ ist $I(x,x) = [x,x] = \{x\} \subseteq X$.

Sind $x, y \in X$ mit $(x,y) \in R(X)$, so ist $I(x,y) \subseteq X$. Daher ist $I(y,x) = I(x,y) \subseteq X$, also $(y,x) \in R(X)$. Das zeigt, dass $R(X)$ symmetrisch ist.

Sind $x, y, z \in X$ mit $(x,y), (y,z) \in X$, so ist $I(x,y), I(y,z) \subseteq X$. Damit ist auch $I(x,z) \subseteq I(x,y) \cup I(y,z) \subseteq X$, also $(x,z) \in R$. Somit ist $R(X)$ transitiv.

Ob $R(X)$ anti-symmetrisch ist, hängt von der Menge X ab. Für alle $x, y \in X$ ist nämlich $I(x,y) = I(y,x)$, und deshalb

$$(x,y) \in R(X) \iff I(x,y) \subseteq X \iff I(y,x) \subseteq X \iff (y,x) \in R(X).$$

Daher ist $R(X)$ genau dann anti-symmetrisch, wenn es keine $x, y \in X$ mit $x \neq y$ gibt, so dass $I(x,y) \subseteq X$, wenn also X keine Intervall positiver Länge enthält.

A.1. Äquivalenzrelationen

Definition 1.3. *Eine Relation $\sim$ auf einer Menge X heißt* Äquivalenzrelation, *falls $\sim$ reflexiv, symmetrisch und transitiv ist. Für alle $x, y \in X$ schreibt man $x \sim y$ statt $(x,y) \in \sim$.*

Beispiel(e). 1. Es sei X eine Menge. Wie bereits gesehen ist Gleichheit $=$ eine Äquivalenzrelation auf X, d.h.

$$R = \{(x, y) \mid x = y\} \subseteq X \times X$$

ist eine Äquivalenzrelation.

2. Für $n, m \in \mathbb{Z}$ sei $n \sim m$ genau dann, wenn $n - m$ gerade ist, d.h. falls es $k \in \mathbb{Z}$ mit $n - m = 2k$ gibt. Wir zeigen, dass $\sim$ eine Äquivalenzrelation auf $\mathbb{Z}$ definiert:

   $\sim$ ist reflexiv, denn alle $n \in \mathbb{Z}$ ist $n - n = 0$ gerade, also $n \sim n$.

   Sind $n, m \in \mathbb{Z}$ mit $n \sim m$, so ist $n - m$ gerade, also $n - m = 2k$ für ein $k \in \mathbb{Z}$. Dann ist auch $m - n = 2(-k)$ gerade, also $m \sim n$. Also ist $\sim$ symmetrisch.

   Sind $p, q, r \in \mathbb{Z}$ mit $p \sim q$ und $q \sim r$, so sind $p-q$ und $q-r$ ungerade, d.h. es gibt $k, l \in \mathbb{Z}$ mit $p-q = 2k$ und $q-r = 2l$. Daher ist auch $p-r = (p-q)+(q-r) = 2k+2l = 2(k+l)$ gerade, also $p \sim r$. Das zeigt, dass $\sim$ auch transitiv ist.

3. Es sei X ein Menge und $f\colon X \to Y$ eine Funktion. Für $x_1, x_2 \in X$ sei $x_1 \sim x_2$ genau dann, wenn $f(x_1) = f(x_2)$. Dann ist $\sim$ ein Äquivalenzrelation:

   Dass $\sim$ reflexiv ist, folgt direkt daraus, dass $f(x) = f(x)$ für alle $x \in X$.

   Sind $x_1, x_2 \in X$ mit $x_1 \sim x_2$, also $f(x_1) = f(x_2)$, so ist auch $f(x_2) = f(x_1)$, also $x_2 \sim x_2$. Das zeigt, dass $\sim$ symmetrisch ist.

   Sind $x_1, x_2, x_3 \in X$ mit $x_1 \sim x_2$ und $x_2 \sim x_3$, also $f(x_1) = f(x_2)$ und $f(x_2) = f(x_3)$, so ist deshalb $f(x_1) = f(x_3)$, also $x_1 \sim x_3$. Somit ist $\sim$ auch transitiv.

4. Auf $x, y \in \mathbb{R}$ sei $x \sim y$ genau dann, wenn $x - y \in \mathbb{Z}$. Hierdurch wird eine Äquivalenzrelation auf $\mathbb{R}$ definiert:

   Dass $\sim$ reflexiv ist, also $x \sim x$ für alle $x \in \mathbb{R}$, folgt direkt daraus, dass $x - x = 0 \in \mathbb{Z}$ für alle $x \in \mathbb{R}$.

   Sind $x, y \in \mathbb{R}$ mit $x \sim y$, also $x - y \in \mathbb{Z}$, so ist auch $y - x \in \mathbb{Z}$, und somit $y \sim x$. Deshalb ist $\sim$ symmetrisch.

   Sind $x, y, z \in \mathbb{R}$ mit $x \sim y$ und $y \sim z$, so ist $x - y, y - z \in \mathbb{Z}$. Deshalb ist auch $x - z = (x - y) + (y - z) \in \mathbb{Z}$, also $x \sim z$. Das zeigt die Transitivität von $\sim$.

5. Für einen Körper K sei $R \subseteq \mathrm{Mat}(n \times n, K) \times \mathrm{Mat}(n \times n, K)$ gegeben durch

   $$(A, B) \in R \iff \text{es gibt eine invertierbare Matrix } S \in \mathrm{GL}_n(K) \text{ mit } SAS^{-1} = B;$$

   man sagt auch, dass die Matrix A äquivalent zu der Matrix B ist. Hierdurch ergibt sich eine Äquivalenzrelation auf $\mathrm{Mat}(n \times n, K)$:

   Jede Matrix $A \in \mathrm{Mat}(n \times n, K)$ ist zu sich selbst äquivalent, da $A = I_n A I_n^{-1}$ für die Einheitsmatrix $I_n \in \mathrm{GL}_n(K)$. Also ist R reflexiv.

   Sind $A, B \in \mathrm{Mat}(n \times n, K)$, so dass A äquivalent zu B ist, also $SAS^{-1} = B$ für eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$, so ist auch $S^{-1} \in \mathrm{GL}_n(K)$ invertierbar mit

   $$SAS^{-1} = B \iff A = S^{-1}BS = S^{-1}B(S^{-1})^{-1}.$$

Also ist dann auch B äquivalent zu A. Somit ist R symmetrisch.

Sind $A, B, C \in \mathrm{Mat}(n \times n, K)$, so dass A äquivalent zu B ist, und B äquivalent zu C ist, so gibt es invertierbare Matrizen $S, T \in \mathrm{GL}_n(K)$ mit $B = SAS^{-1}$ und $C = TBT^{-1}$. Dann ist auch $TS \in \mathrm{GL}_n(K)$ invertierbar mit

$$C = TBT^{-1} = TSAS^{-1}T^{-1} = (TS)A(TS)^{-1},$$

weshalb auch C äquivalent zu A ist. Also ist R auch transitiv.

6. Es sei G ein Gruppe und $R \subseteq G \times G$ dadurch gegeben, dass

$$(g, h) \in G \iff \text{es gibt } \alpha \in G \text{ mit } g = \alpha h \alpha^{-1}.$$

Man sagt, dass g konjugiert zu h ist. Dies liefert eine Äquivalenzrelation auf G:

Jedes Element $g \in G$ ist zu sich selbst konjugiert, da $g = ege^{-1}$ für das neutrale Element $e \in G$. Also ist R reflexiv.

Sind $g, h \in G$, so dass g konjugiert zu h ist, so gibt es $\alpha \in G$ mit $g = \alpha h \alpha^{-1}$. Da

$$g = \alpha h \alpha^{-1} \iff h = \alpha^{-1} g \alpha = \alpha^{-1} g (\alpha^{-1})^{-1}$$

ist dann auch h äquivalent zu g. Das zeigt, dass R symmetrisch ist.

Sind $g, h, k \in G$, so dass g konjugiert zu h ist, und h konjugiert zu k ist, so gibt es $\alpha, \beta \in G$ mit $g = \alpha h \alpha^{-1}$ und $h = \beta k \beta^{-1}$. Dann ist

$$g = \alpha h \alpha^{-1} = \alpha \beta k \beta^{-1} \alpha^{-1} = (\alpha\beta) k (\alpha\beta)^{-1},$$

also auch g konjugiert zu k. Das zeigt, dass R transitiv ist.

Definition 1.4. *Es sei $\sim$ eine Äquivalenzrelation auf einer Menge X. Für $x \in X$ ist*

$$[x]_\sim := \{y \in X \mid x \sim y\}$$

die Äquivalenzklasse *von x, und $X/\sim := \{[x] \mid x \in X\}$ ist die Menge der Äquivalenzklassen von X.*

Bemerkung 1.5. 1. Ist klar, um welche Äquivalenzrelation es sich handelt, so schreibt man auch nur $[x]$ statt $[x]_\sim$.

2. Ist $\sim$ eine Äquivalenzrelation auf einer Menge X, so gilt für alle $x, y \in X$, dass entweder $[x] \cap [y] = \emptyset$ oder $[x] = [y]$.

   Ist nämlich $x \sim y$, so ist für jedes $z \in X$ genau dann $z \sim x$, falls $z \sim y$, da

$$x \sim z \implies y \sim x, x \sim z \implies y \sim z$$

   und analog

$$y \sim z \implies x \sim y, y \sim z \implies x \sim z.$$

Also ist in diesem Fall

$$[x] = \{z \in X \mid x \sim z\} = \{z \in X \mid y \sim z\} = [y].$$

Ist andererseits $x \nsim y$, und gebe es ein $z \in [x] \cap [y]$, so wäre $x \sim z$ und $z \sim y$, wegen der Transitivität von $\sim$ also auch $x \sim y$, ein Widerspruch.

Es ist also $x \sim y \implies [x] = [y]$ und $x \nsim y \implies [x] \cap [y] = \emptyset$. Da entweder $x \sim y$ oder $x \nsim y$ handelt es sich schon jeweils um Äquivalenzen.

Beispiel(e). 1. Für die Gleichheit $=$ auf einer Menge X ist für jedes $x \in X$ die Äquivalenzklasse gegeben durch

$$[x] = \{y \in X \mid y = x\} = \{x\}.$$

Also ist die Abbildung

$$X \to X/\sim, \quad x \mapsto [x]$$

eine Bijektion.

2. Wir betrachten auf $\mathbb{Z}$ die Äquivalenzrelation $\sim$ mit $n \sim m$ genau dann wenn $n - m$ gerade ist, d.h. wenn $n - m = 2k$ für ein $k \in \mathbb{Z}$. Für $n \in \mathbb{Z}$ ist dann

$$[n] = \{m \in \mathbb{Z} \mid n - m = 2k \text{ für ein } k \in \mathbb{Z}\} = \{n + 2k \mid k \in \mathbb{Z}\} = n + 2\mathbb{Z}.$$

Inbesondere ist deshalb $[0] = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$ die Menge der geraden Zahlen und $[1] = \{1 + 2k \mid k \in \mathbb{Z}\} = 1 + 2\mathbb{Z}$ die Menge der ungeraden Zahlen. Ist $n \in \mathbb{Z}$ gerade, so ist $n \in [0]$, also $[n] \cap [0] \neq \emptyset$ und somit $[n] = [0]$ die Menge der geraden Zahlen. Ist andererseits n ungerade, so ist $[n] \in [1]$, also $n \cap [1] \neq \emptyset$ und somit $[n] = [1]$ die Menge der ganzen Zahlen.

Es gibt in diesem Fall also nur zwei verschieden Äquivalenzklassen, nämlich die geraden Zahlen $[0]$ und die ungeraden Zahlen $[1]$. Also ist die Abbildung

$$\{0, 1\} \mapsto \mathbb{Z}/\sim, \quad n \mapsto [n]$$

eine Bijektion.

3. Wir betrachten auf $\mathbb{R}$ die Äquivalenzrelation $\sim$ mit $x \sim y$ genau dann, wenn $x - y$ ganzzahlig ist, d.h. wenn $x - y \in \mathbb{Z}$. Für jedes $x \in \mathbb{R}$ ist dann

$$\begin{aligned}[x] &= \{y \in \mathbb{R} \mid x - y \in \mathbb{Z}\} = \{y \in \mathbb{R} \mid \text{es gibt } k \in \mathbb{Z} \text{ mit } x - y = k\} \\ &= \{x + k \mid k \in \mathbb{Z}\} = x + \mathbb{Z}.\end{aligned}$$

Für jede ganze Zahl $n \in \mathbb{Z}$ ist etwa $[n] = \mathbb{Z}$, und es sind

$$\left[\frac{1}{2}\right] = \left\{\dots, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \dots\right\}$$

und

$$[\pi] = \{\dots, \pi - 2, \pi - 1, \pi, \pi + 1, \pi + 2, \dots\}.$$

Es ist nun einfach zu sehen, dass es für jedes $x \in \mathbb{R}$ genau ein $x' \in [0,1)$ mit $x \sim x'$ gibt. Daher ist die Abbildung

$$[0,1) \to \mathbb{R}/\sim, \quad x \mapsto [x]$$

eine Bijektion.

4. Durch den Betracht $b\colon \mathbb{C} \to \mathbb{R}_{\geq 0}, z \mapsto |z|$ ergibt sich eine Äquivalenzrelation auf $\mathbb{C}$ durch

$$z \sim w \iff b(z) = b(w) \iff |z| = |w|.$$

Für jedes $r \in \mathbb{R}$ mit $r \geq 0$ ist

$$[r] = \{z \in \mathbb{C} \mid z \sim r\} = \{z \in \mathbb{C} \mid |z| = |r|\} = \{z \in \mathbb{C} \mid |z| = r\}.$$

Also ist $[0] = \{0\}$ und für alle $r > 0$ ist $[r] = \{z \in \mathbb{C} \mid |z| = r\}$ der Kreis mit Radius r um den Mittelpunkt $0 \in \mathbb{C}$. Da $[z] = [|z|]$ für alle $z \in \mathbb{C}$ und $[r_1] \cap [r_2] = \emptyset$ für alle $0 \leq r_1 < r_2$ ist die Abbildung

$$[0,\infty) \to \mathbb{C}/\sim, \quad z \mapsto [z]$$

eine Bjiektion.

Definition 1.6. *Es sei $\sim$ ein Äquivalenzrelation auf einer Menge X. Ein Element $x \in A$ einer Äquivalenzklasse $A \in X/\sim$ bezeichnet man als* Repräsentantensystem *der Äquivalenzklasse A. Eine Teilmenge $R \subseteq X$ heißt* Repräsentantensystem*, falls es für jedes $x \in X$ genau ein $r \in R$ gibt, so dass $x \sim r$, d.h. die Abbildung*

$$R \to X/\sim, \quad r \mapsto [r]$$

ist eine Bijektion.

Bemerkung 1.7. Allgemein erhält man für eine Äquivalenzrelation $\sim$ auf einer Menge X ein Repräsentantensystem, indem man aus jeder Äquivalenzklasse $A \in X/\sim$ einen Repräsentanten $r_A \in A$ wählt, und diese Repräsentanten anschließend zu $R = \{r_A \mid A \in X/\sim\}$ zusammenfasst.

Beispiel(e). 1. Ist X ein Menge, so ist für die Äquivalenzrelation der Gleichheit $=$ die Menge X selbst das einzige Repräsentantensystem.

2. Bezüglich der Äquivalenzrelation $\sim$ auf $\mathbb{Z}$ mit $n \sim m$ genau dann, wenn $n - m$ gerade ist, ist ein Repräsentantensystem gegeben durch $\{0,1\}$.

   Da $\mathbb{Z}/\sim = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$, die Äquivalenzklassen von $\sim$ also die geraden und ungeraden Zahlen sind, sind die Repräsentantensysteme von $\sim$ genau die Teilmengen $R \subseteq \mathbb{Z}$ von der Form $R = \{n, m\}$ mit n gerade und m ungerade.

3. Bezüglich der Äquivalenzrelation $\sim$ auf $\mathbb{R}$ mit $x \sim y$ genau dann, wenn $x - y \in \mathbb{Z}$, ist ein mögliches Repräsentantensystem durch $[0,1)$ gegeben. Allgemeiner ist für jedes $y \in \mathbb{R}$ eine Repräsentantensystem durch das halboffene Intervall $[y, y+1)$ gegeben.

4. Für die Äquivalenzrelation $\sim$ auf $\mathbb{C}$ mit $z \sim w$ genau dann, wenn $|z| = |w|$, ist ein mögliches Repräsentantensystem durch das halboffene reelle Intervall $[0,\infty) \subseteq \mathbb{R}$ gegeben.

A.2. Ordnungsrelationen

Definition 1.8. *Eine Relation R auf einer Menge X heißt* Ordnungsrelation*, falls R reflexiv, anti-symmetrisch und transitiv ist.*

Beispiel(e). 1. Wie bereits gesehen, ist

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$$

eine Ordnungsrelation auf $\mathbb{R}$.

2. Für eine Menge X sei

$$R = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid A \subseteq B\},$$

wobei $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ die Potenmenge von X bezeichnet. R ist reflexiv, den für jede Teilmenge $A \subseteq X$ ist $A \subseteq A$. R ist anti-symmetrisch, denn sind $A, B \subseteq X$ zwei Teilmengen mit $(A, B), (B, A) \in R$, also $A \subseteq B$ und $B \subseteq A$, so ist bereits $A = B$. R ist auch transitiv, denn für Teilmengen $A, B, C \subseteq X$ mit $(A, B), (B, C) \in R$ ist $A \subseteq B$ und $B \subseteq C$, also auch $A \subseteq C$, und somit $(A, C) \in R$.

3. Für zwei ganze Zahlen $n, m \in \mathbb{Z}$ sagen wir, n *teilt* m, wenn es ein $k \in \mathbb{Z}$ mit $m = kn$ gibt; wir schreiben dann $n \mid m$.

   a) Wir definieren auf $\mathbb{N}$ die Relation

   $$R = \{(n, m) \in \mathbb{N} \mid n \mid m\}.$$

   R ist reflexiv, denn für alle $n \in \mathbb{N}$ ist $n = 1 \cdot n$, also $n \mid n$.

   R ist anti-symmetrisch, denn sind $n, m \in \mathbb{N}$ mit $(n, m), (m, n) \in R$, so ist $n \mid m$ und $m \mid n$, d.h. es gibt $k, l \in \mathbb{Z}$ mit $m = kn$ und $n = lm$. Es ist dann $n = km = kln$. Ist $n = 0$, so ist auch $m = kn = 0$, also $n = m$. Ist $n \neq 0$, so folgt aus $n = kln$ dass $kl = 1$; da $k, l \in \mathbb{Z}$ ist bereits $k = l = \pm 1$. Da $m = kn$ muss $k = l = 1$. Somit ist $n = km = m$. In beiden Fällen ist also $n = m$.

   R ist auch transitiv, denn für $p, q, r \in \mathbb{N}$ mit $(p, q), (q, r) \in R$ ist $p \mid q$ und $q \mid r$, d.h. es gibt $k, l \in \mathbb{Z}$ mit $q = kp$ und $r = lq$. Es ist daher $r = lq = lkp$, also auch $p \mid r$, und somit $(p, r) \in R$.

   Also ist R eine Ordnungsrelation auf $\mathbb{N}$.

   b) Wir definieren auf $\mathbb{Z}$ die Relation

   $$R = \{(n, m) \in \mathbb{Z} \mid n \text{ teilt } m\}.$$

   Wie bereits zuvor ergibt sich, dass R reflexiv und transitiv ist. R ist allerdings nicht anti-symmetrisch. So ist etwa $(-1) \mid 1$ und $1 \mid (-1)$, da $1 = (-1) \cdot (-1)$ und $-1 = (-1) \cdot 1$, aber $1 \neq -1$. R definiert also keine Ordnungsrelation auf R.

Die obigen Beispiele motivieren die folgende Definition.

Definition 1.9. *Eine* geordnete Menge *ist ein Paar $(X, \leq)$ bestehend aus einer Menge X und einer Ordnungsrelation $\leq$ auf X. Für $x, y \in X$ schreibt man $x \leq y$ statt $(x, y) \in \leq$. Außerdem führt man für $x, y \in X$ die folgenden Notationen ein:*

i) Man schreibt $y \geq x$ falls $x \leq y$.

ii) Man schreibt $x < y$ falls $x \leq y$ und $x \neq y$.

iii) Man schreibt $y > x$ falls $y \geq x$ und $x \neq y$.

Bemerkung 1.10. 1. Häufig nennt man die Ordnungsrelation nicht explizit, d.h. statt von einer geordneten Menge $(X, \leq)$ spricht man von einer geordneten Menge X.

2. Ist $(X, \leq)$ eine geordnete Menge und $Y \subseteq X$ eine Teilmenge, so ist auch die Einschränkung $\leq_Y = \leq \cap (Y \times Y) \subseteq Y \times Y$ eine Ordnungsrelation auf Y, d.h.

$$y_1 \leq_Y y_2 \iff y_1 \leq y_2 \quad \text{für alle } y_1, y_2 \in Y.$$

Wegen dieser Äquivalenz schreibt man auch einfach nur $\leq$ statt $\leq_Y$, benutzt also kein zusätzliches Symbol für die eingeschränkte Ordnungsrelation.

Definition 1.11. *Eine geordnete Menge X heißt* linear geordnet, *bzw.* total geordnet, *falls für alle $x, y \in X$ gilt, dass $x \leq y$ oder $y \leq x$.*

Beispiel(e). 1. Die reellen Zahlen sind bezüglich der üblichen Ordnungsrelation $\leq$ linear geordnet.

2. Ist X eine Menge, so ist $\mathcal{P}(X)$ bezüglich der Teilmengenrelation $\subseteq$ im Allgemeinen nicht linear geordnet: Besitzt X mindestens zwei verschiedene Elemente $x, y \in X$, so sind $\{x\}, \{y\} \subseteq X$ zwei Teilmengen mit $\{x\} \not\subseteq \{y\}$ und $\{y\} \not\subseteq \{y\}$.

3. Die natürlichen Zahlen $\mathbb{N}$ sind bezüglich der Teilbarkeitsrelation $|$ nicht linear geordnet, da etwa $2 \nmid 3$ und $3 \nmid 2$.

4. Ist $(X, \leq)$ eine total geordnete Menge und $Y \subseteq X$ eine Teilmenge, so ist auch Y linear geordnet bezüglich $\leq$.

Definition 1.12. *Es sei X eine geordnete Menge und $Y \subseteq X$ eine Teilmenge. Ein Element $x \in X$ heißt*

i) obere Schranke *von Y, falls $y \leq x$ für all $y \in Y$,*

ii) untere Schranke *von Y, falls $x \leq y$ für alle $y \in Y$,*

iii) Supremum *von Y, falls x eine kleineste obere Schranke von Y ist, d.h. x ist eine obere Schranke von Y, und für jede obere Schranke s von Y ist $x \leq s$,*

iv) Infimum *von Y, falls x eine größte untere Schranke von Y ist, d.h. x ist eine untere Schranke von Y, und für jede untere Schranke t von Y ist $t \leq x$.*

B. Konvergenz und Summierbarkeit von Folgen

Wir erinnern hier an grundlegende Definitionen und Aussagen über konvergente Folgen und Reihen. In diesem Abschnitt sei $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Definition 2.1. *Es sei $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$, also $(x_n)_{n\in\mathbb{N}}$ eine Folge mit Werten in $\mathbb{K}$, und $x \in \mathbb{K}$. Wir sagen, dass die Folge $(x_n)_{n\in\mathbb{N}}$ gegen x* konvergiert, *falls es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass $|x_n - x| < \varepsilon$ für alle $n \geq N$. Die Folge $(x_n)_{n\in\mathbb{N}}$ heißt dann* konvergent *und x heißt* Grenzwert *der Folge $(x_n)_{n\in\mathbb{N}}$. Wir schreiben abkürzend, dass $x_n \to x$ für $n \to \infty$ falls die Folge $(x_n)_{n\in\mathbb{N}}$ gegen x konvergiert.*

Bemerkung 2.2. Ist $(x_n)_{n\in\mathbb{N}}$ eine konvergente $\mathbb{K}$-wertige Folge, so ist der Grenzwert eindeutig: Angenommen, es gibt $x, y \in \mathbb{K}$ mit $x_n \to x$ für $n \to \infty$ und $x_n \to y$ für $n \to \infty$, aber $x \neq y$. Dann ist $|x-y| > 0$ und somit auch $\varepsilon := |x-y|/3 > 0$. Da $x_n \to x$ für $n \to \infty$ gibt es $N_x \in \mathbb{N}$ mit $|x - x_n| < \varepsilon$ für alle $n \geq N_x$, und da $x_n \to y$ für $n \to \infty$ gibt es $N_y \in \mathbb{N}$ mit $|y - x_n| < \varepsilon$ für alle $n \geq N_y$. Für $n := \max\{N_1, N_2\}$ ist daher

$$|x-y| = |x - x_n + x_n - y| \leq |x - x_n| + |y - x_n| < \varepsilon + \varepsilon = \frac{2}{3}|x-y|,$$

was $|x-y| > 0$ widerspricht. Also muss bereits $x = y$.

Konvergiert eine $\mathbb{K}$-wertige Folge $(x_n)_{n\in\mathbb{N}}$ gegen ein Element $x \in \mathbb{K}$, so schreiben wir auch $\lim_{n\to\infty} x_n := x$.

Bemerkung 2.3. .

1. Ist $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ eine konstante Folge, d.h. es gibt $c \in \mathbb{K}$ mit $x_n = c$ für alle $n \in \mathbb{N}$, so konvergiert $(x_n)_{n\in\mathbb{N}}$ und $\lim_{n\to\infty} x_n = c$. Für beliebige $\varepsilon > 0$ ist nämlich $|c - x_n| = 0 < \varepsilon$ für alle $n \geq 0$.

2. Sind $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ konvergente Folgen, so konvergiert auch die Folge $(x_n + y_n)_{n\in\mathbb{N}}$ und es gilt

$$\lim_{n\to\infty} (x_n + y_n) = \left(\lim_{n\to\infty} x_n\right) + \left(\lim_{n\to\infty} y_n\right).$$

   Ist nämlich $x := \lim_{n\to\infty} x_n$, $y := \lim_{n\to\infty} y_n$ und $\varepsilon > 0$, so gibt es $N_x, N_y \in \mathbb{N}$ mit $|x - x_n| < \varepsilon/2$ für alle $n \geq N_x$ und $|y - y_n| < \varepsilon/2$ für alle $n \geq N_y$, weshalb für alle $n \geq N := \max\{N_x, N_y\}$ auch

$$|(x+y) - (x_n + y_n)| = |(x - x_n) + (y - y_n)| \leq |x - x_n| + |y - y_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

3. Ist $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ konvergent und $\lambda \in \mathbb{K}$, so ist auch die Folge $(\lambda x_n)_{n\in\mathbb{N}}$ konvergent und $\lim_{n\to\infty}(\lambda x_n) = \lambda \lim_{n\to\infty} x_n$: Es sei $x \coloneqq \lim_{n\to\infty} x_n$. Ist $\lambda = 0$, so ist $(\lambda x_n)_{n\in\mathbb{N}}$ die konstante Nullfolge und somit

$$\lim_{n\to\infty} \lambda x_n = \lim_{n\to\infty} 0 = 0 = 0 \cdot \lim_{n\to\infty} x_n.$$

Ist $\lambda \neq 0$ und $\varepsilon > 0$, so gibt es $N \in \mathbb{N}$ mit $|x - x_n| < \varepsilon/|\lambda|$ für alle $n \geq N$. Für alle $n \geq N$ ist daher auch

$$|\lambda x - \lambda x_n| = |\lambda||x - x_n| < |\lambda|\frac{\varepsilon}{|\lambda|} = \varepsilon.$$

Definition 2.4. *Eine Folge $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ heißt* Cauchy-Folge*, falls es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass $|x_n - x_m| < \varepsilon$ für alle $n, m \geq N$.*

Bemerkung 2.5. 1. Ist $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ konvergent, so ist $(x_n)_{n\in\mathbb{N}}$ auch eine Cauchy-Folge: Ist nämlich $\varepsilon > 0$ und $x \coloneqq \lim_{n\to\infty} x_n$, so gibt es $N \in \mathbb{N}$ mit $|x - x_n| < \varepsilon/2$ für alle $n \geq N$, weshalb für alle $n, m \geq N$ auch

$$|x_n - x_m| = |x_n - x + x - x_m| \leq |x_n - x| + |x - x_m| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

2. Für die reellen Zahlen $\mathbb{R}$ und komplexen Zahlen $\mathbb{C}$ gilt auch die Umkehrung: Ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge reeller oder komplexer Zahlen, also $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{R})$ oder $(x_n)_{n\in\mathbb{N}} \in \ell(\mathbb{C})$, so ist $(x_n)_{n\in\mathbb{N}}$ auch konvergent. Man sagt, dass $\mathbb{R}$ und $\mathbb{C}$ *vollständig* sind. (Wir werden dies hier nicht zeigen. Für die reellen Zahlen ist der Beweis abhängig davon, wie diese konstruiert werden. Die Vollständigkeit der komplexen Zahlen lässt sich dann aus der Vollständigkeit der reellen Zahlen folgern.)

3. Für die rationalen Zahlen $\mathbb{Q}$ gilt diese Aussage nicht: Es gibt Cauchy-Folgen von rationalen Zahlen, die in $\mathbb{Q}$ keinen Grenzwert besitzen. $\mathbb{Q}$ ist also nicht vollständig. (Auch diese Aussage werden wir hier nicht zeigen.)

Definition 2.6. *Für eine Folge $(a_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ und $m \in \mathbb{N}$ ist die m-te* Partialsumme *der Folge $(a_n)_{n\in\mathbb{N}}$ als $\sum_{n=0}^{m} a_n$ definiert. Die Folge $(a_n)_{n\in\mathbb{N}}$ heißt* summierbar*, falls die Folge der Partialsummen $(\sum_{n=0}^{m} a_n)_{m\in\mathbb{N}}$ konvergiert. Es ist dann $\sum_{n=0}^{\infty} a_n \coloneqq \lim_{m\to\infty} \sum_{n=0}^{m} a_n$.*

Bemerkung 2.7. 1. Die konstante Nullfolge $(0)_{n\in\mathbb{N}}$ ist summierbar mit $\sum_{n=0}^{\infty} a_n = 0$. Für alle $m \in \mathbb{N}$ ist nämlich $\sum_{n=0}^{m} 0 = 0$, also $(\sum_{n=0}^{m} a_n)_{m\in\mathbb{N}} = 0$, die Folge der Partialsummen also ebenfalls die Nullfolge. Daher konvergiert die Folge der Partialsummen gegen 0, also $\lim_{m\to\infty} \sum_{n=0}^{m} 0 = 0$. Dies bedeutet gerade, dass die Nullfolge $(0)_{n\in\mathbb{N}}$ summierbar ist, und dass $\sum_{n=0}^{\infty} 0 = 0$.

2. Sind $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ summierbare Folgen, so ist auch die Folge $(a_n + b_n)_{n\in\mathbb{N}}$ summierbar und $\sum_{n=0}^{\infty}(a_n + b_n) = (\sum_{n=0}^{\infty} a_n) + (\sum_{n=0}^{\infty} b_n)$.

   Ist nämlich $S_m \coloneqq \sum_{n=0}^{m} a_n$ und $T_n \coloneqq \sum_{n=0}^{m} b_n$ für alle $m \in \mathbb{N}$, so bedeutet die Summierbarkeit von $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$, dass die Folgen $(S_m)_{m\in\mathbb{N}}$ und $(T_m)_{m\in\mathbb{N}}$ konvergieren, und dass $S \coloneqq \lim_{m\to\infty} S_m = \sum_{n=0}^{\infty} a_n$ und $T \coloneqq \lim_{m\to\infty} T_m = \sum_{n=0}^{\infty} b_n$. Da

$(S_m)_{m\in\mathbb{N}}$ und $(T_m)_{m\in\mathbb{N}}$ konvergieren, konvergiert auch die Folge $(S_m + T_m)_{m\in\mathbb{N}}$ und $\lim_{m\to\infty}(S_m + T_m) = S + T$.

Für alle $m \in \mathbb{N}$ ist nun

$$S_m + T_m = \left(\sum_{n=0}^{m} a_n\right) + \left(\sum_{n=0}^{m} b_n\right) = \sum_{n=0}^{m}(a_n + b_n)$$

und es ist

$$\left(\sum_{n=0}^{\infty} a_n\right) + \left(\sum_{n=0}^{\infty} b_n\right) = S + T = \lim_{m\to\infty}(S_m + T_m) = \lim_{m\to\infty}\sum_{n=0}^{m}(a_n + b_n).$$

Das zeigt, dass die Folge der Partialsummen $(\sum_{n=0}^{m}(a_n + b_n))_{m\in\mathbb{N}}$ konvergiert, und dass $\lim_{m\to\infty}\sum_{n=0}^{m}(a_n+b_n) = (\sum_{n=0}^{\infty} a_n)+(\sum_{n=0}^{\infty} b_n)$. Dies bedeutet gerade, dass die Folge $(a_n + b_n)_{n\in\mathbb{N}}$ summierbar ist, und dass $\sum_{n=0}^{\infty}(a_n + b_n) = (\sum_{n=0}^{\infty} a_n) + (\sum_{n=0}^{\infty} b_n)$.

3. Ist $(a_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ summierbar und $\lambda \in \mathbb{K}$, so ist auch die Folge $(\lambda a_n)_{n\in\mathbb{N}}$ summierbar und $\sum_{n=0}^{\infty}(\lambda a_n) = \lambda\sum_{n=0}^{\infty} a_n$.

   Ist $S_m \coloneqq \sum_{n=0}^{m} a_n$ die m-te Partialsumme der Folge $(a_n)_{n\in\mathbb{N}}$, so bedeutet die Summierbarkeit der Folge $(a_n)_{n\in\mathbb{N}}$, dass die Folge der Partialsummen $(S_m)_{m\in\mathbb{N}}$ konvergiert, und dass $S \coloneqq \lim_{m\to\infty} S_m = \sum_{n=0}^{\infty} a_n$. Da die Folge $(S_m)_{m\in\mathbb{N}}$ konvergiert, konvergiert auch die Folge $(\lambda S_m)_{m\in\mathbb{N}}$ und es gilt $\lim_{m\to\infty}\lambda S_m = \lambda S$.

   Für alle $m \in \mathbb{N}$ ist nun

$$\lambda S_m = \lambda\sum_{n=0}^{m} a_n = \sum_{n=0}^{m}(\lambda a_n),$$

   und es gilt

$$\lambda\sum_{n=0}^{\infty} a_n = \lambda\lim_{m\to\infty} S_m = \lim_{m\to\infty}\lambda S_m = \lim_{m\to\infty}\lambda\sum_{n=0}^{m} a_n = \lim_{m\to\infty}\sum_{n=0}^{m}(\lambda a_n).$$

   Die Konvergenz der Folge $(\lambda S_m)_{m\in\mathbb{N}}$ bedeutet also genau die Summierbarkeit der Folge $(\lambda a_n)_{n\in\mathbb{N}}$, und es ist $\sum_{n=0}^{\infty}(\lambda a_n) = \lim_{m\to\infty}\sum_{n=0}^{m}(\lambda a_n) = \lambda\sum_{n=0}^{\infty} a_n$.

Definition 2.8. *Eine Folge $(a_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ heißt* absolut summierbar*, falls die Folge $(|a_n|)_{n\in\mathbb{N}}$ summierbar ist.*

Bemerkung 2.9. Ist $(a_n)_{n\in\mathbb{N}}$ eine absolut summierbare Folge reeller oder komplexer Zahlen, so ist $(a_n)_{n\in\mathbb{N}}$ auch summierbar: Dass die Folge $(a_n)_{n\in\mathbb{N}}$ absolut summierbar ist, bedeutet, dass die Folge $(|a_n|)_{n\in\mathbb{N}}$ summierbar ist. Das bedeutet, dass die Folge der Partialsummen $(\sum_{n=0}^{m}|a_n|)_{m\in\mathbb{N}}$ konvergiert. Also ist die Folge der Partialsummen $(\sum_{n=0}^{m}|a_n|)_{m\in\mathbb{N}}$ eine Cauchy-Folge.

Es sei $\varepsilon > 0$. Da die Folge der Partialsummen $(\sum_{n=0}^{m}|a_n|)_{m\in\mathbb{N}}$ eine Cauchy-Folge ist, gibt es $N \in \mathbb{N}$, so dass für alle $l \geq m \geq N$

$$\sum_{n=m+1}^{l}|a_n| = \left|\sum_{n=0}^{l}|a_n| - \sum_{n=0}^{m}|a_n|\right| < \varepsilon.$$

Für alle $l \geq m \leq N$ ist deshalb auch

$$\left| \sum_{n=0}^{l} a_n - \sum_{n=0}^{m} a_n \right| = \left| \sum_{n=m+1}^{l} a_n \right| \leq \sum_{n=m+1}^{l} |a_n| < \varepsilon.$$

Deshalb ist die Folge der Partialsummen $(\sum_{n=0}^{m} a_n)_{m\in\mathbb{N}}$ eine Cauchy-Folge. Da $\mathbb{R}$ und $\mathbb{C}$ vollständig sind, ist die Folge der Partialsummen $(\sum_{n=0}^{m} a_n)_{m\in\mathbb{N}}$ deshalb bereits konvergent. Dies bedeutet, dass die Folge $(a_n)_{n\in\mathbb{N}}$ summierbar ist.

Bemerkung 2.10. Ist die Folge $(a_n)_{n\in\mathbb{N}} \in \ell(\mathbb{K})$ summierbar, so ist $(a_n)_{n\in\mathbb{N}}$ eine Nullfolge, d.h. $(a_n)_{n\in\mathbb{N}}$ ist konvergent und $\lim_{n\to\infty} a_n = 0$: Für alle $m \in \mathbb{N}$ sei $S_m := \sum_{n=0}^{m} a_n$ die m-te Partialsumme von $(a_n)_{n\in\mathbb{N}}$. Dass $(a_n)_{n\in\mathbb{N}}$ summierbar ist, bedeutet, dass die Folge $(S_m)_{m\in\mathbb{N}}$ konvergiert. Es konvergiert daher die Folge $(S_{m+1})_{m\in\mathbb{N}}$ mit $\lim_{m\to\infty} S_{m+1} = \lim_{m\to\infty} S_m$. Daher konvergiert auch die Folge $(S_{m+1} - S_m)_{m\in\mathbb{N}}$ mit

$$\lim_{m\to\infty} (S_{m+1} - S_m) = \lim_{m\to\infty} S_{m+1} - \lim_{m\to\infty} S_m = \lim_{m\to\infty} S_m - \lim_{m\to\infty} S_m = 0.$$

Für alle $m \in \mathbb{N}$ ist jedoch

$$S_{m+1} - S_m = \sum_{n=0}^{m+1} a_n - \sum_{n=0}^{m} a_n = a_{m+1},$$

also ist $0 = \lim_{m\to\infty}(S_{m+1} - S_m) = \lim_{m\to\infty} a_{m+1} = \lim_{m\to\infty} a_m$.