LinA 2
Algebraische Strukturen

Anton Deitmar

Sommer 25

Inhaltsverzeichnis

Teil I

Algebraische Strukturen

1 Gruppen

1.1 Permutationen

Für eine beliebige Menge M bezeichnen wir mit $\mathrm{Per}(M)$ die Gruppe der **Permutationen** von M, d.h., die Menge aller bijektiven Abbildungen $\sigma : M \to M$ mit der Hintereinunderausführung als Gruppenmultiplikation. Für eine natürliche Zahl n sei dann $\mathrm{Per}(n)$ die Gruppe $\mathrm{Per}(\{1,\dots,n\})$. Wir nennen $\mathrm{Per}(n)$ auch die Gruppe der Permutationen in n Buchstaben.

Die Elemente der Permutationsgruppe $\mathrm{Per}(n)$ schreibt man zB in der Form $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, wobei wir das Bild jeweils unter das Element schreiben, also in diesem Beispiel $\tau(1) = 2$, $\tau(2) = 3$ und $\tau(3) = 1$. Eine undere Schreibweise für dasselbe Element ist die **Zykelschreibweise**:

$$\tau = (1,2,3)$$

was soviel bedeutet wie 1 geht auf 2 geht auf 3 geht auf 1. Das Element, das 1 und 2 vertauscht, schreibt sich dann als $(1,2)$. Nicht jedes Element von $\mathrm{Per}(n)$ ist als ein einziger Zykel schreibbar, so ist zum Beispiel in $\mathrm{Per}(4)$ das Element $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ in der Zykelschreibweise gleich

$$(1,2)(3,4).$$

Definition 1.1.1. Ein **Zykel** in $\mathrm{Per}(n)$ ist ein Tupel $(j_1, j_2, \dots, j_r)$, $r \geq 2$ von verschiedenen natürlichen Zahlen $1 \leq j_1, j_2, \dots, j_r \leq n$. Ein Zykel

repräsentiert eine Permutation, die j_ν auf $j_{\nu+1}$ und j_r auf j_1 wirft und alle underen Zahlen festhält. Der Zykel $(j_1, \ldots, j_r)$ repräsentiert dieselbe Permutation wie der Zykel $(j_2, j_3, \ldots, j_r, j_1)$, deshalb kann man den Zykel stets durch einen ersetzen, für den j_1 die kleinste der Zahlen $j_1, \ldots, j_k$ ist. Ein Zykel in dieser Form heisst **kanonisch**.

Zwei Zykel $(j_1, \ldots, j_k)$ und $(i_1, \ldots, i_s)$ heissen **disjunkt**, falls sie keine gemeinsamen Zahlen haben, also falls

$$\{j_1, \ldots, j_k\} \cap \{i_1, \ldots, i_s\} = \varnothing.$$

Beispiel 1.1.2. Wir schreiben die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 5 & 2 & 4 & 3 \end{pmatrix}$ als Produkt kanonischer Zykel:

$$(2,6,4,5)(3,7).$$

Satz 1.1.3.

(a) *Zwei kanonische Zykel stellen genau dann dieselbe Permutation dar, wenn sie gleich sind.*

(b) *Zwei disjunkte Zykel, aufgefasst als Elemente von* $\mathrm{Per}(n)$*, kommutieren miteinander.*

(c) *Jede Permutation* $\neq \mathrm{Id}$ *in* $\mathrm{Per}(n)$ *lässt sich als Produkt paarweise disjunkter kanonischer Zykel schreiben, diese sind eindeutig bestimmt bis auf die Reihenfolge.*

Beweis. (a) Seien $(j_1, j_2, \ldots, j_r)$ und $(i_1, i_2, \ldots, i_s)$ zwei kanonische Zykel, die dieselbe Permutation γ darstellen. Dann ist j_1 das kleinste Element von $\{1, \ldots, n\}$, das von γ überhaupt vertauscht wird und dasselbe gilt

von i_1, also folgt $j_1 = i_1$. Ferner ist $j_2 = \gamma(j_1) = \gamma(i_1) = i_2$ und so weiter.

(b) Sei $\gamma = (j_1, \ldots, j_k)$ ein Zykel in $\mathrm{Per}(n)$ und sei $\tau \in \mathrm{Per}(n)$. Es gilt dann

$$\tau\gamma\tau^{-1} = (\tau(j_1), \ldots, \tau(j_k)).$$

Ist $\tau = (i_1, \ldots, i_s)$ auch ein Zykel, dann sind die $i_1, \ldots, i_s$ genau die Zahlen, die von τ überhaupt verändert werden. Ist also τ zu γ disjunkt, so folgt $\tau\gamma\tau^{-1} = \gamma$.

(c) Wir geben ein Verfahren zum Finden der Zykel zu einem gegebenen $\gamma \in \mathrm{Per}(n)$. Sei j_1 die kleinste Zahl in $\{1, \ldots, n\}$, die von γ überhaupt verändert wird. Sei dann $j_2 = \gamma(j_1)$ und so weiter. Die Folge $j_1, j_2, \ldots$ kann nicht unendlich sein, also gibt es ein kleinstes $k \in \mathbb{N}$ und zu diesem ein kleinstes $s \in \mathbb{N}$ so dass $j_{k+s} = j_k$ gilt. Das heisst also $\gamma(j_{k+s-1}) = j_k$. Ist $k > 1$, so gilt aber auch $\gamma(j_{k-1}) = j_k$, woraus aber $j_{k+s-1} = j_{k-1}$ folgt, was der Minimalität von k widerspricht. Es ist also $k = 1$ und damit ist $\alpha = (j_1, \ldots, j_s)$ ein Zykel, der die Zahlen $(j_1, \ldots, j_s)$ genauso abbildet wie γ, so dass $\alpha^{-1}\gamma$ sie alle festhält. Dieser ist dann gleich e oder nicht, in welchem Fall wir das Verfahren wiederholen und einen zweiten Zykel β finden, der disjunkt zu α ist und so weiter. Das Verfahren bricht wegen Endlichkeit des Problems ab. □

Beispiel 1.1.4. Wir können die Elemente von $\mathrm{Per}(3)$ als Zykel hinschreiben: $e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$.

1.2 Ordnung

Definition 1.2.1. Ist G eine endliche Gruppe, so nennt man die Anzahl $|G|$ der Elemente die **Ordnung** der Gruppe G,

$$\mathrm{ord}(G) = |G|.$$

Wir schreiben auch 1 für das neutrale Element e einer Gruppe.

Ist $a \in G$, so bezeichnet $\langle a \rangle$ die von a **erzeugte Gruppe**, also die kleinste Untergruppe von G, die a enthält. Diese beschreibt man einmal als

$$\langle a \rangle = \bigcap_{\substack{H \text{ Untergruppe} \\ H \ni a}} H,$$

wobei man sich klarmachen muss, dass dies wieder eine Untergruppe ist. Andererseits kann man $\langle a \rangle$ konstruktiv beschreiben:

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

Ist $\langle a \rangle$ eine endliche Gruppe, so nennt man die Ordnung von $\langle a \rangle$ auch die **Ordnung** des Elements a und man schreibt

$$\operatorname{ord}(a) = \operatorname{ord}(\langle a \rangle) = |\langle a \rangle|.$$

Ist $\langle a \rangle$ nicht endlich, so setzt man $\operatorname{ord}(a) = \infty$.

Beispiel 1.2.2. Ist $z \in \operatorname{Per}(n)$ ein Zykel $z = (j_1, \ldots, j_k)$, dann gilt

$$\operatorname{ord}(z) = k.$$

Wir nennen k dann wahlweise die Ordnung oder die **Länge** des Zykels z.

Lemma 1.2.3. *Sei a ein Element der Gruppe G. Die von a erzeugte Gruppe $\langle a \rangle$ ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 1$. Es gilt*

$$\operatorname{ord}(a) = \min\{n \in \mathbb{N} : a^n = 1\}.$$

Ist k die Ordnung von a so gilt für jedes $n \in \mathbb{N}$

$$a^n = 1 \quad \Leftrightarrow \quad k \mid n.$$

Beweis. Sei $\langle a \rangle$ endlich. Da die Elemente $1, a, a^2, \ldots$ nicht alle verschieden sein können, gibt es ein $m, n \in \mathbb{N}$ so dann $a^m = a^{m+n}$, also $1 = a^n$ gilt. Die

Umkehrung ist klar, da $\langle a \rangle$ genau aus den Potenzen von a besteht. Ist schliesslich $k \in \mathbb{N}$ die kleinste natürliche Zahl mit $a^k = 1$, dann besteht $\langle a \rangle$ genau aus den Elementen $1, a, a^2, \ldots, a^{k-1}$.

Zum Schluss sei $k = \mathrm{ord}(a)$ und $a^n = 1$. Dann folgt $n \geq k$, wir können also $n = rk + s$ schreiben mit $0 \leq s < k$. Es ist dann

$$1 = a^n = a^{rk+s} = (a^k)^r a^s = a^s,$$

so dass $s = 0$, also $k \mid n$ folgt. Die Umkehrung ist klar. □

Lemma 1.2.4. *Ist G eine abelsche Gruppe und $a, b \in G$ von endlichen Ordnungen m, n. Sind m und n teilerfremd, dann hat ab die Ordnung mn.*

Beweis. Ist $1 = (ab)^k = a^k b^k$, also $a^k = b^{-k}$. Die Ordnung von a^k ist ein Teiler von m, die Ordnung von b^{-k} ist ein Teiler von n, daher müssen beide Ordnungen gleich 1 sein, also $a^k = 1 = b^k$. Damit ist k ein Vielfaches von m und von n, die Ordnung von ab ist also mn. □

Definition 1.2.5. Sind G, H zwei Gruppen, so wird das Produkt $G \times H$ durch die Vorschrift

$$(g, h)(g', h') = (gg', hh')$$

eine Gruppe. Das neutrale Element ist $(1, 1)$. Das Inverse zu (g, h) ist (g^{-1}, h^{-1}). Für die Ordnungen gilt

$$\mathrm{ord}(G \times H) = \mathrm{ord}(G)\,\mathrm{ord}(H).$$

Beispiele 1.2.6.

- Wir bezeichnen mit $\mathbb{Z}/m\mathbb{Z}$ oder auch $\mathbb{Z}/m$ die **zyklische Gruppe** mit m Elementen, $m \in \mathbb{N}$, also die Gruppe $\{0, 1, 2, \ldots, m-1\}$ mit Verknüpfung: $a \boxplus b =$ Rest von $a + b$ modulo m.
- Sei $n \in \mathbb{N}$ die **Diedergruppe** D_{2n} der Ordnung $2n$ ist eine Gruppe

erzeugt von zwei Elementen σ, τ mit den Relationen

$$\sigma^n = 1 = \tau^2 \quad \text{und} \quad \tau\sigma\tau^{-1} = \sigma^{-1}.$$

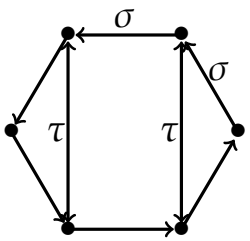
Insbesondere soll σ die Ordnung n haben und τ die Ordnung 2.

Das bedeutet, D_{2n} besteht genau aus den Elementen

$$1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}$$

und die Produkte dieser Elemente rechnet man mit den Relationen aus.

Man kann sie als Untergruppe von $\mathrm{Per}(n)$ wie folgt darstellen. Stellen wir uns die Elemente von $\{1, 2, \ldots, n\}$ auf einem Kreis in gleichen Abständen angeordnet vor. Dann ist σ die Rotation um den Winkel $2\pi/n$ und τ ist irgendeine Spiegelung an einer Geraden, die die Menge $\{1, \ldots, n\}$ in sich abbildet.



Es gilt $D_2 \cong \mathbb{Z}/2$, sowie $D_4 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$ und schliesslich

$$D_6 \cong \mathrm{Per}(3).$$

Proposition 1.2.7. *Ist $g \in \mathrm{Per}(n)$ eine Permutation, die wir gemäß Satz 1.1.3 als Produkt disjunkter Zykel schreiben:*

$$g = z_1 \cdots z_k$$

und sei $l_j = l(z_j)$ die jeweilige Länge des j-ten Zykels. Dann gilt

$$\mathrm{ord}(g) = \mathrm{kgV}(l_1, \ldots, l_k).$$

Beweis. Die z_j vertauschen miteinander. Da jedes z_j eine undere Teilmenge von $\{1, \dots, n\}$ permutiert, folgt für $\nu \in \mathbb{N}$

$$g^\nu = 1 \quad \Leftrightarrow \quad z_j^\nu = 1 \text{ für jedes } j = 1, \dots, k.$$

Dies ist genau dann der Fall, wenn ν ein Vielfaches von $\operatorname{ord}(z_j) = l_j$ ist für jedes j, daher ist die Ordnung $\operatorname{ord}(g) = \min\{\nu \in \mathbb{N} : g^\nu = 1\}$ das kleinste gemeinsame Vielfache der Einzelordnungen. □

1.3 Nebenklassen

Definition 1.3.1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Ist $a \in G$, so ist die **Linksnebenklasse** von a nach H gleich der Menge

$$aH = \{ah : h \in H\}.$$

Da H eine Gruppe ist, gilt für $h \in H$ schon

$$hH = H.$$

Beispiele 1.3.2.

- Ist V ein Vektorraum und $U \subset V$ ein Unterraum, dann sind die Nebenklassen nach U genau die affinen Räume $v + U$, die U als linearen Teil haben.
- Sei $G = D_{2n}$ die Diedergruppe und sei $H = \langle \tau \rangle$ die von τ erzeugte Untergruppe, dann ist $H = \{1, \tau\}$ und die H-Linksnebenklassen sind

$$\underbrace{\{1, \tau\}}_{=H}, \underbrace{\{\sigma, \sigma\tau\}}_{=\sigma H}, \dots, \underbrace{\{\sigma^{n-1}, \sigma^{n-1}\tau\}}_{=\sigma^{n-1}H}.$$

Lemma 1.3.3. *Sei G eine Gruppe und H eine Untergruppe. Zwei Linksnebenklassen sind entweder gleich oder disjunkt, daher kann man G disjunkt in seine Nebenklassen zerlegen, es gibt also eine Familie $(x_i)_{i \in I}$ in G so*

dass

$$G = \bigsqcup_{i \in I} x_i H.$$

Beweis. Sei $xH \cap yH \neq \varnothing$. Wir zeigen $xH \subset yH$. Aus Symmetrie folgt dann die undere Richtung. Sei also $z \in xH \cap yH$, dann existieren $h_1, h_2 \in H$ so dass $z = xh_1 = yh_2$. Es folgt $x = yh_2h_1^{-1} \in yH$ und ist $u \in xH$, also $u = xh_3$, so folgt $u = xh_3 = y \underbrace{h_2h_1^{-1}h_3}_{\in H} \in yH$. □

Proposition 1.3.4. *Sei G eine endliche Gruppe. Ist H eine Untergruppe, dann ist die Ordnung $|H|$ ein Teiler der Ordnung $|G|$ von G. Genauer gilt*

$$|G| = |H||G/H|,$$

wobei G/H die Menge aller Nebenklassen aH ist.

Insbesondere gilt für jedes Element x

$$\operatorname{ord}(x) \mid \operatorname{ord}(G),$$

d.h., die Ordnung von x teilt die Gruppenordnung. Insbesondere folgt

$$x^{\operatorname{ord}(G)} = 1.$$

Beweis. Wir haben $G = \bigsqcup_{i \in I} x_i H$, und da G endlich ist, muss I endlich sein, wir finden also $x_1, \ldots, x_n \in G$ so dass $G = \bigsqcup_{j=1}^{n} x_j H$. Also folgt

$$\operatorname{ord}(G) = \sum_{j=1}^{n} |x_j H|.$$

Die Untergruppe H bildet selbst eine Nebenklasse, wir können also $x_1 = e$ annehmen. Die Abbildung $h \mapsto x_j H$ ist eine Bijektion von H nach $x_j H$, also haben alle Nebenklassen gleich viele Elemente, nämlich

$\operatorname{ord}(H)$ viele, es ist also

$$\operatorname{ord}(G) = \sum_{j=1}^{n} \operatorname{ord}(H) = n \operatorname{ord}(H).$$

Ist $a \in G$ ein beliebiges Element und ist $H = \langle a \rangle$ die von a erzeugte Untergruppe, dann ist $\operatorname{ord}(a) = \operatorname{ord}(H)$ ein Teiler von $\operatorname{ord}(G)$. □

1.4 Homomorphismen und Operationen

Definition 1.4.1. Eine Abbildung $\phi : G \to H$ zwischen zwei Gruppen heisst **Gruppenhomomorphismus**, falls

$$\phi(ab) = \phi(a)\phi(b)$$

für alle $a, b \in G$ gilt.

Lemma 1.4.2. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(1) = 1$ und $\phi(a^{-1}) = \phi(a)^{-1}$.*

Beweis. Übungsaufgabe Blatt 1. □

Beispiele 1.4.3.

- Ist G eine Gruppe und ist $a \in G$, dann ist die Abbildung

  $$\phi : x \mapsto axa^{-1}$$

  Ein Homomorphismus von G nach G.

  Beweis. Für $x, y \in G$ gilt $\phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$. □

- Sind V, W Vektorräume über einem Körper K, so ist jede lineare Abbildung $T : V \to W$ ein Gruppenhomomorphismus $(V, +) \to (W, +)$.

- Sei G die Gruppe $\mathrm{GL}_n(K)$ aller invertierbarer $n \times n$ Matrizen über dem Körper K. Dann ist die Abbildung $\psi : G \to G$,

$$\psi(A) = A^{-t} = (A^t)^{-1} = (A^{-1})^t$$

  ein Gruppenhomomorphismus.

- Ist $G = \mathrm{Per}(n)$ die Gruppe der Permutationen in $\{1, \ldots, n\}$, dann ist die Vorzeichen- oder **Signumabbildung**

$$\mathrm{sign} : \mathrm{Per}(n) \to \{\pm 1\}$$

  ein Gruppenhomomorphismus, wie in der Linearen Algebra gezeigt wird.

Definition 1.4.4. Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Der **Kern** von G ist

$$\ker \phi = \big\{ g \in G : \phi(g) = 1 \big\}.$$

Es ist leicht einzusehen, dass $\ker(\phi)$ eine Untergruppe von G ist.

Lemma 1.4.5. *Ein Gruppenhomomorphismus $\phi : G \to H$ ist genau dann injektiv, wenn sein Kern trivial ist.*

Proof. Ist ϕ injektiv, dann gilt für jedes $x \in G \setminus \{1\}$, dass $\phi(x) \neq 1$, also ist der Kern trivial.

Ist umgekehrt der Kern trivial und sind $x, y \in G$ mit $\phi(x) = \phi(y)$, dann gilt, weil ϕ ein Gruppenhomomorphismus ist, dass

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

und daher $x^{-1}y \in \ker \phi$ und also $x^{-1}y = 1$ oder $x = y$. □

Definition 1.4.6. Sei G eine Gruppe und M eine Menge. Eine **Operation**

von G auf M ist eine Abbildung

$$G \times M \to M$$
$$(g, m) \mapsto g.m$$

mit den Eigenschaften

- $1.m = m$ (das neutrale Element operiert neutral)
- $(ab).m = a.(b.m)$ (Operation und Multiplikation sind kompatibel)

Beispiele 1.4.7.

- Sei G eine Gruppe. Dann definiert die Vorschrift

  $$g.m = gm$$

  eine Operation der Gruppe auf sich selbst, die **Linkstranslationsoperation**.

  Beweis. Es gilt $1.m = 1m = m$ und $(ab).m = (ab)m = a(bm) = a.(b.m)$. □

- Sei G eine Gruppe, dann operiert G durch

  $$g.m = mg^{-1}$$

  auf sich selbst, dies ist die **Rechtstranslationsoperation**.

  Beweis. Es gilt $1.m = m1^{-1} = m1 = m$ und $(ab).m = m(ab)^{-1} = (mb^{-1})a^{-1} = a.(b.m)$. □

- Sei G eine Gruppe, dann operiert G auf sich selbst durch die Vorschrift

  $$g.m = gmg^{-1}$$

  dies ist die **Konjugationsoperation**.

Beweis. Es gilt $1.m = 1m1^{-1} = m$ und
$(ab).m = abm(ab)^{-1} = abmb^{-1}a^{-1} = a.(b.m)$. □

- (Abgeleitete Operationen.) Operiert die Gruppe G auf der Menge M und ist S eine weitere Menge, dann operiert G auf der Menge $A = \mathrm{Abb}(M, S)$ aller Abbildungen von M nach S durch

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

Beweis. Es ist $e.\phi(m) = \phi(e^{-1}.m) = \phi(m)$ und $(ab).\phi(m) = \phi((ab)^{-1}.m) = \phi(b^{-1}.a^{-1}.m) = b.\phi(a^{-1}.m) = a.(b.\phi)(m)$. □

Lemma 1.4.8. *Sei $M \neq \varnothing$ eine Menge. Operiert die Gruppe G auf der Menge M, dann ist die Abbildung $\phi : G \to \mathrm{Per}(M)$, $g \mapsto (m \mapsto gm)$ ein Gruppenhomomorphismus. Ist umgekehrt $\phi : G \to \mathrm{Per}(M)$ ein Gruppenhomomorphismus, dann definiert*

$$gm = \phi(g)(m)$$

eine Operation. Diese Zuordnungen (Operation)↦(Gruppenhomomorphismus) und umgekehrt sind invers zueinander. Also ist eine Operation dasselbe wie ein Gruppenhomomorphismus nach $\mathrm{Per}(M)$.

Beweis. Die Gruppe G operiere auf M. Für $g \in G$ sei $\phi(g) : M \to M$, $m \mapsto gm$. Zunächst müssen wir zeigen, dass $\phi(g)$ bijektiv ist, wir also wirklich in $\mathrm{Per}(M)$ lunden. Wir behaupten, dass $\phi(g^{-1})$ eine Umkehrabbildung zu $\phi(g)$ ist. Dies folgt aus

$$\phi(g)(\phi(g^{-1})(m)) = \phi(g)(g^{-1}m) = gg^{-1}m = 1m = m$$

und

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

Wir haben also in der Tat eine Abbildung $\phi : G \to \mathrm{Per}(M)$. Wir rechnen nun nach, dass dies ein Gruppenhomomorphismus ist. Für $g, h \in G$ gilt

$$\phi(gh)(m) = (gh)m = g(hm) = \phi(g)(hm) = \phi(g)(\phi(h)(m)) = \phi(g)\phi(h)(m).$$

Also ist ϕ ein Gruppenhomomorphismus. Die Umgekehrte Richtung ist leicht nachzurechnen und die Tatsache, dass diese Zuordnungen invers zueinander sind, auch. □

Die Gruppe G operiere auf der Menge M. Für gegebenes $m \in M$ nennen wir die Menge

$$[m] = Gm = \{gm : g \in G\}$$

die **Bahn** oder das **Orbit** von m. Ferner ist

$$G_m = \{g \in G : gm = m\}$$

der **Stabilisator** von m.

Satz 1.4.9. *Die Gruppe G operiere auf der Menge M.*

(a) *Der Stabilisator eines Punktes $m \in M$ ist eine Untergruppe von G. Er wird auch die* **Stundgruppe** *von m genannt.*

(b) *Sei $H = G_m$ der Stabilisator von m. Die Abbildung $gH \mapsto gm$ ist eine Bijektion von G/H zum Orbit von m.*

(c) *Die Orbiten zweier Punkte sind entweder gleich oder disjunkt, man kann deshalb M disjunkt in seine Orbiten zerlegen. Man schreibt $G\backslash M$ für die Menge aller Orbiten.*

(d) *(Bahnengleichung) Sind G und M endliche Mengen und seien $[m_1], \ldots, [m_k]$ die Bahnen, so gilt*

$$|M| = \sum_{j=1}^{k} \frac{|G|}{|G_{m_j}|}.$$

Man kann Teil (c) auch so ausdrücken, dass man sagt: die Operation von G definiert eine Äquivalenzrelation auf M, wobei m und m' äquivalent heissen, falls sie in demselben Orbit liegen. Der Quotient nach dieser Äquivalenzrelation wird dann mit $G\backslash M$ bezeichnet.

Beweis. (a) Sei $H = G_m$, dann gilt offensichtlich $e \in H$. Sind $a, b \in H$, dann ist

$$(ab)m = a(bm) = am = m,$$

also liegt auch ab wieder in H. Ferner folgt aus $am = m$ durch Anwenden von a^{-1} schon $m = a^{-1}m$, so dass auch $a^{-1} \in H$ folgt. Also ist H eine Untergruppe.

(b) Sei $\psi : G/H \to Gm$ diese Abbildung. Zunächst ist festzustellen, dass sie überhaupt wohldefiniert ist, ist also $gH = g'H$, dann ist $g' = gh$ für ein $h \in H$ und damit ist $g'm = g(hm) = gm$, somit ist ψ wohldefiniert.
Injektivität. Sei $\psi(aH) = \psi(bH)$, dann ist $am = bm$ also $a^{-1}bm = m$, was soviel heisst wie $a^{-1}b \in H$ und somit $bH = aH$.
Surjektivität. Sei $z \in Gm$, also $z = gm$ für ein $g \in G$, dann folgt $z = \phi(gH)$.

(c) Sei $Gm \cap Gm' \neq \varnothing$, dann ist zu zeigen, dass $Gm = Gm'$ gilt. Sei $z \in Gm \cap Gm'$ dann existieren also $g, g' \in G$ so dass $gm = z = g'm'$. Es folgt $m' = (g')^{-1}gm$ so dass $m' \in Gm$ und damit $hm' \in Gm$ für jedes $h \in G$, was soviel heisst wie $Gm' \subset Gm$. Aus Symmetrie folgt die umgekehrte Inklusion.

(d) Wir haben die disjunkte Zerlegung $M = \bigsqcup_{j=1}^{k} [m_j]$. Daher ist $|M| = \sum_{j=1}^{k} \left|[m_j]\right|$. Nach Teil (b) ist fuer jedes $m \in M$ mit Stabilisator $H = G_m$,

$$\left|[m]\right| = \left|G/H\right|.$$

Es bleibt also zu zeigen $\left|G/H\right| = |G|/|H|$ oder $|G| = |H|\,\left|G/H\right|$. Seien

$h_1H, \ldots, h_lH$ die Nebenklassen, dann zerlegen sie G disjunkt, also

$$|G| = \sum_{j=1}^{j} \underbrace{|h_jH|}_{|H|} = l|H|.$$

Hierbei beachte, dass die Abbildung $h \mapsto m_jh$ eine Bijektion $H \to m_jH$ ist. Nach Definition ist $l = |G/H|$, also folgt die Behauptung. □

Lemma 1.4.10. *Eine Gruppe G mit n Elementen operiere auf einer Menge M mit m Elementen. Seien $1 = d_1 \leq \cdots \leq d_r = n$ die Teiler von n. Dann gibt es Zahlen $k_1, \ldots, k_r \in \mathbb{N}_0$, so dass*

$$m = \sum_{j=1}^{r} k_j \, d_j.$$

Hierbei ist k_j die Anzahl der Bahnen mit d_j Elementen.

Beweis. Seien $[m_1], \ldots, [m_k]$ die Bahnen in M. Nach der Bahnengleichung ist

$$|M| = \sum_{j=1}^{k} \frac{|G|}{|G_{m_j}|}.$$

Jedes $|G_{m_j}|$ ist ein Teiler von $n = |G|$, also ist auch $\frac{|G|}{|G_{m_j}|}$ ein Teiler von n. Wir ordnen diese Summe nach den Teilern $d_1, \ldots d_r$ und bezeichnen mit k_j die Anzahl, mit der der Teiler d_j unter den $\frac{|G|}{|G_{m_j}|}$ auftritt. □

Beispiel 1.4.11. Operiert eine Gruppe G der Ordnung 77 auf einer Menge M der Ordnung 5, dann gilt $g.m = m$ für jedes $m \in M$, d.h., die Operation ist trivial.

Beweis. Der kleinste nichttriviale Teiler von 7 ist 7 und 5 ist kleiner als 7, also sind in der Summe des Lemmas alle $k_j = 0$ für $j \geq 1$. Es gibt also nur Bahnen der Länge 1. □

1.5 Zyklische Gruppen

Eine Gruppe G heisst **zyklisch**, wenn G von einem Element erzeugt ist.

Beispiele 1.5.1.
- Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch von unendlicher Ordnung.
- Für jedes $n \in \mathbb{N}$ gibt es eine zyklische Gruppe der Ordnung n, nämlich $\mathbb{Z}/n$.

Proposition 1.5.2. (a) *Ist G zyklisch, dann ist G isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n$, wobei $n = \mathrm{ord}(G)$.*

(b) *Ist G eine zyklische Gruppe der Ordnung n und ist d ein Teiler von n, dann gibt es ein Element der Ordnung d.*

Beweis. (a) Sei G zyklisch und sei τ ein Erzeuger.

1. Fall. τ hat endliche Ordnung $n \in \mathbb{N}$. Dann ist die Abbildung $\mathbb{Z}/n \to G$, $k \mapsto \tau^k$ ein Gruppenisomorphismus.
2. Fall. τ hat keine endliche Ordnung. Dann ist die Abbildung $\mathbb{Z} \to G$, $k \mapsto \tau^k$ ein Isomorphismus.

(b) Ist τ ein Erzeuger und ist $k = n/d$, dann ist $\alpha = \tau^k$ von Ordnung d, denn erstens ist $\alpha^d = \tau^n = 1$ und zweitens, gölte $\alpha^l = 1$ für ein $1 < l < d$, dann hieße das $1 = \alpha^l = \tau^{ln/d}$, was einen Widerspruch ergibt, da ln/d echt kleiner ist als n. □

Satz 1.5.3. *Sei p eine Primzahl. Jede Gruppe der Ordnung p ist zyklisch, also isomorph zu der Gruppe $\mathbb{Z}/p$.*

Beweis. Sei G eine Gruppe der Ordnung p. Sei $e \neq \tau \in G$. Dann muss $\mathrm{ord}(\tau)$ ein Teiler von p sein. Da $\tau \neq e$, ist die Ordnung $\neq 1$, also ist

ord$(\tau) = p$, damit hat die zyklische Untergruppe $\langle\tau\rangle$, die von τ erzeugt wird, die Ordnung p, ist also gleich G. □

Satz 1.5.4. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Proof. Sei $G = \langle\tau\rangle$ eine zyklische Gruppe und sei $\{1\} \neq H \subset G$ eine Untergruppe. Sei N die kleinste natuerliche Zahl mit $\gamma = \tau^N \in H$. Wir zeigen, dass H von γ erzeugt ist. Sei hierzu $h = \tau^n \in H$, dann ist $h\gamma^k = \tau^{n+kN} \in H$. Es gibt ein $k \in \mathbb{Z}$ mit $0 \leq n + kN < N$. Aus der Minimalitaet von N folgt $n + kN = 0$ und daher $h = \gamma^{-k}$. □

Satz 1.5.5 (Gruppen bis zur Ordnung 7)**.**

(a) *Es gibt jeweils nur eine Gruppe (bis auf Isomorphie) der Ordnung 1,2,3,5,7, nämlich die jeweils zyklische Gruppe.*

(b) *Es gibt zwei Gruppen der Ordnung 4, nämlich* $\mathbb{Z}/4$ *und* $\mathbb{Z}/2 \times \mathbb{Z}/2$.

(c) *Es gibt zwei Gruppen der Ordnung 6, nämlich* $\mathbb{Z}/6$ *und* Per(3).

Beweis. (a) ist klar, da die genannten Ordnungen Primzahlen sind.

(b) Sei G eine Gruppe der Ordnung 4, die nicht zyklisch ist. Das bedeutet, dass jedes Element $\neq e$ die Ordnung 2 haben muss. Dann ist G abelsch (nach übungsaufgabe). Seien nun a, b zwei verschiedene Elemente von $G \setminus \{e\}$. Dann liefert die Abbildung $(\mathbb{Z}/2) \times (\mathbb{Z}/2) \to G$, $(i, j) \mapsto a^i b^j$ einen injektiven Gruppenhomomorphismus. Das Bild hat Ordnung 4, ist also G und G damit isomorph zur Vierergruppe.

(c) Sei G eine Gruppe der Ordnung 6. Hat G ein Element der Ordnung 6, so ist $G - \mathbb{Z}/6$. Nehmen wir also an, dass alle Elemente Ordnung 1,2,3 haben.

1. Es gibt Elemente der Ordnung 2 und der Ordnung 3.
Haben alle Elemente Ordnung 2, dann ist die Gruppe abelsch. Sind dann a, b verschiedene Elemente. Wie im Fall der Ordnung 4 ist dann $\{1, a, b, ab\}$ eine Untergruppe der Ordnung 4, was nicht sein kann, da 4 kein Teiler von 6 ist. Daher gibt es Elemente der Ordnung 3.
Angenommen, alle Elemente haben Ordnung 3. Sei dann $a \neq 1$ und $H = \langle a \rangle$. Die Gruppe G operiert auf der Menge G/H der H-Nebenklassen. Diese Menge hat 2 Elemente. Sei $a \in G \setminus H$. Dann ist $aH \neq H$, also $a^2H \neq aH$, also $a^2H = H$ oder $a^2 \in H$. Nun ist $a^2 = a^{-1}$ in H und da H eine Gruppe ist, ist $a \in H$, **Widerspruch!**

Sei $b \in G \setminus H$, dann vertauscht b die beiden Nebenklassen H bH, also folgt $H = b(bH) = b^2H$, d.h., $b^2 \in H$. Waere nun $b^2 = a$ oder a^2, dann haette a oder a^2 die Ordnung 6, Widerspruch. Also folgt $b^2 = 1$, das Element b hat demnach Ordnung 2.

1. Fall: G **ist abelsch.** Seien dann $a, b \in G$ von Odnung 2 und 3. Sei dann $\tau = ab$. Dann ist $\tau^2 = a^2b^2 = b^2 \neq 1$. Ferner ist $\tau^3 = a^3b^3 = a^3 = a^2a = a \neq 1$, also hat τ weder Ordnung 2, noch 3, also Ordnung 6 und G ist zyklisch.

2. Fall: G **ist nicht abelsch.** Seien a, b der Ordnungen 2 und 3 und sei $H = \langle a \rangle$. Dann operiert G auf der Menge G/H der Nebenklassen, diese hat 3 Elemente, wir erhalten also einen Gruppenhomomorphismus

$$\phi : G \to \mathrm{Per}(G/H) \cong \mathrm{Per}(3).$$

Wenn wir zeigen, dass ϕ injektiv ist, ist es wegen $|G| = 6 = |\mathrm{Per}(3)|$ ein Isomorphismus. Da $b \notin H$ ist $bH \neq H$ und daher $b^2H \neq H$. Wäre nun $b^2H = H$, also $b^2 \in H$, dann wäre $b^2 = 1$, also $b = bb^3 = b^4 = (b^2)^2 = 1$, Widerspruch! Damit ist auch $b^2H \neq H$ und die Nebenklassen sind

H, bH, b^2H. Insbesondere wird G von den beiden Elementen a und b erzeugt. Das Element b vertauscht die Nebenklassen zyklisch und a fixiert die Nebenklasse H. Wir wollen zeigen, dass a die Klassen bH und b^2H vertauscht. **Wäre** $abH = bH$, so wäre entweder $ab = b$, was nicht geht, oder $ab = ba$. Damit vertauschen a und b und da sie die Gruppe erzeugen, ist diese abelsch, **Widerspruch!** Es folgt also, dass a und b beide nichttrivial operieren. Das bedeutet, dass beide nicht im Kern von ϕ liegen. Da a und b beliebig gewählt werden können, ist der Kern trivial, also ist ϕ nach Lemma 1.4.5 injektiv. □

2 Ringe

2.1 Definition

Definition 2.1.1. Ein **kommutativer Ring mit Eins** ist eine abelsche Gruppe $(R, +)$ mit einer weiteren Verknüpfung $\times$, die assoziativ ist,

$$(ab)c = a(bc)$$

und kommutativ

$$ab = ba$$

und das Distributivgesetz erfüllt:

$$a(b + c) = ab + ac.$$

Ferner existiert ein Element $1_R \in R$ mit

$$1_R a = a$$

für jedes $a \in R$. Dieses Element ist dann eindeutig bestimmt, denn ist $1'$ ein zweites, dann gilt

$$1' = 11' = 1'1 = 1.$$

Wenn wir im Folgenden **Ring** schreiben, meinen wir immer einen kommutativen Ring mit Eins.

Ein Ring ist also dasselbe wie ein Körper, bis auf die Tatsache, dass nicht jedes Element $\neq 0$ invertierbar sein muss.

Beispiele 2.1.2. (a) $(\mathbb{N}, +, \times)$ ist **kein** Ring, da es keine inversen Elemente der Addition gibt.

(b) $(\mathrm{M}_n(K), +, \times)$ ist kein kommutativer Ring für $n \geq 2$, da Matrixmultiplikation nicht kommutativ ist.

(c) Jeder Körper ist ein Ring.

(d) $\mathbb{Z}$ ist ein Ring, der kein Körper ist.

(e) Ist K ein Körper, dann ist die Menge der Polynome $K[x]$ ein Ring.

(f) Der einfachste Ring ist der **Nullring** $N = \{0\}$. In diesem Ring gilt $0 = 1$. Ist R ein Ring, in dem $0 = 1$ gilt, dann ist R der Nullring, denn für $a \in R$ gilt

$$a = 1a = 0a = (1 - 1)a = a - a = 0.$$

Der Nullring ist ein dummes Beispiel und wir werden uns im Folgenden in der Regel auf Ringe mit $0 \neq 1$ einschränken.

(g) Sei $\alpha = \sqrt{2} \in \mathbb{R}$. Dann gilt $\alpha^2 = 2$. Wir definieren

$$\mathbb{Z}[\sqrt{2}] = (k + l\alpha : k, l \in \mathbb{Z}) .$$

Wegen $(k + l\alpha)(m + n\alpha) = km + 2ln + (kn + lm)\alpha$ ist $\mathbb{Z}[\sqrt{2}]$ ein Unterring von $\mathbb{R}$.

(h) Der **Gaußsche Zahlring** ist definiert als

$$\mathbb{Z}[i] = \left\{a + bi : a, b \in \mathbb{Z}\right\} \subset \mathbb{C}.$$

(i) Ist R ein Ring, dann definiert man den Polynomring $R[x]$ genau wie im Körperfall. Elemente sind formale Ausdrücke der Form

$$a_0 + \cdots + a_n x^n$$

und die Multiplikation ist definiert durch

$$(a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = c_0 + \cdots + c_{m+n} x^{m+n},$$

wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere kann man also den Uebergang von einem Ring zum Polynomring wiederholen und erhaelt den

Polynomring in mehreren Unbekannten,

$$R[X_1, \ldots, X_r].$$

Die Elemente dieses Rings sind formale Ausdruecke der Form

$$\sum_{\alpha} c_\alpha X^\alpha,$$

wobei α durch $\mathbb{N}_0^r$ laeuft, $c_\alpha \in R$ ein Koeffizient ist, der nur für endlich viele α nicht Null ist und

$$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}$$

ist.

(j) Im Polynomring $R[x]$ gilt

$$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m},$$

wobei $c_0 = a_0 b_0, c_1 = a_0 b_1 + a_1 b_0$ und allgemein

$$c_k = \sum_{i+j=k} a_i b_j.$$

Also haengt der Koeffizient c_k nur von den Koeffizienten $a_0, \ldots, a_k$ und $b_0, \ldots b_k$ ab und nicht von denen hoeheren Grades. Dasselbe gilt für die Addition. Daher kann man Addition und Multiplikation des Polynomrings $R[x]$ auch auch die Menge aller Koeffizientenfolgen $(a_0, a_1, \ldots)$ ausdehnen, die nicht notwendigerweise endlich sind. Alternativ kann man diese Menge $R^{\mathbb{N}_0} = \mathrm{Abb}(N_0, R)$ auch als Menge aller formalen Reihen

$$\sum_{j=0}^{\infty} a_j x^j$$

beschreiben. Der so entstehende Ring wird der Ring der **formalen**

Potenzreihen genannt und als

$$R[[x]]$$

geschrieben.

(k) Sei p eine Primzahl und sei $\mathbb{Z}_{(p)}$ die Menge aller rationalen Zahlen $\frac{a}{b} \in \mathbb{Q}$ für die der Nenner b zur Primzahl p teilerfremd ist, also von p nicht geteilt wird. Dies ist ein Unterring von $\mathbb{Q}$.

Beispiel 2.1.3. Sei $m \in \mathbb{N}$ und sei $R = \mathbb{Z}/m$ gleich der Menge $\{0, 1, \ldots, m-1\}$. Wir definieren Addition und Multiplikation wie folgt

$$a \boxplus b = \text{Rest von } a + b \text{ nach Division durch } m.$$

Und die Multiplikation

$$a \boxtimes b = \text{Rest von } ab \text{ nach Division durch } m.$$

Man verifiziert, dass $\mathbb{Z}/m$ mit diesen Operationen ein Ring ist.

Zweite Definition: Auf $\mathbb{Z}$ definiert man folgende Äquivalenzrelation $a \sim b \Leftrightarrow a - b \in m\mathbb{Z}$. Sei $\mathbb{Z}/m$ die Menge $\mathbb{Z}/\sim$ der Äquivalenzklassen. Es ist klar, dass es genau m Äquivalenzklassen gibt $[0], [1], \ldots, [m-1]$. Addition und Multiplikation werden wie folgt definiert

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

Hier ist Wohldefiniertheit zu prüfen: etwa $a \sim a'$, $b \sim b'$, dann ist zu zeigen, dass $(a + b) \sim (a' + b')$ und $ab \sim a'b'$. Für die erste Aussage betrachte

$$(a + b) - (a' + b') = a - a' + b - b' \in M\mathbb{Z}.$$

Für die zweite:

$$ab - a'b' = ab - a'b + a'b - a'ba = (a - a')b + a'(b - b') \in m\mathbb{Z}.$$

Definition 2.1.4. Ein Element $0 \neq a \in R$ eines Rings heißt **invertierbar** oder **Einheit** des Rings, wenn es ein $b \in R$ gibt mit $ab = 1$. Die Menge $R^\times$ der invertierbaren Elemente ist eine abelsche Gruppe bzgl. der Multiplikation. Ein Ring R ist genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$ gilt.

Beispiele 2.1.5. (a) Die Einheiten von $\mathbb{Z}$ sind ± 1.

(b) Sei K ein Körper und sei $R = K[x]$ der Polynomring. Die Einheiten von R sind genau die konstanten Polynome $\neq 0$.

(c) Die Einheiten des Rings $R = \mathbb{Z}[i\sqrt{5}]$ sind genau die Zahlen 1 und -1.

Beweis. Seien $a, b \in R$ mit $ab = 1$. Da $a, b \in \mathbb{C}$ ist, gilt diese Gleichung auch dort, also ist auch $1 = |ab|^2 = |a|^2|b|^2$. Damit gilt $|a|^2 \leq 1$ oder $|b|^2 \leq 1$. Nehmen wir $|a|^2 \leq 1$ an. Sei $a = k + il\sqrt{5}$, dann ist $|a|^2 = k^2 + 5l^2$ und da $k, l \in \mathbb{Z}$, folgt $l = 0$ und $a = k = \pm 1$. Damit ist auch $b = \pm 1$ und die Beauptung ist gezeigt. □

(d) Die Einheiten des Rings $\mathbb{Z}/m$ sind genau die Zahlen $1 \leq x \leq m - 1$, die zu m teilerfremd sind. Dies zeigt man mit Hilfe der Division mit Rest (Übungsaufgabe!)

Definition 2.1.6. Ein Element $a \neq 0$ eines Rings R heißt **Nullteiler**, falls es ein $b \neq 0$ gibt mit $ab = 0$.

Ein Ring R mit $0 \neq 1$ heißt **nullteilerfrei**, oder **integer**, oder **Integritätsring**, falls es keine Nullteiler in R gibt, wenn also gilt

$$ab = 0 \quad \Rightarrow \quad a = 0 \text{ oder } b = 0.$$

Beispiele 2.1.7. (a) Der Nullring ist kein Integritätsring.

(b) Körper sind Integritätsringe.

(c) Jeder Unterring eines Integritätsrings ist ein Integritätsring. So ist zum Beispiel $\mathbb{Z}[i\sqrt{5}]$ ein Integritätsring, da er ein Unterring des Körpers $\mathbb{C}$ ist.

(d) $\mathbb{Z}$ ist ein Integritätsring.

(e) $\mathbb{Z}/m$ ist nur dann ein Integritaetsring, wenn m eine Primzahl ist.

(f) Ist R ein Integritätsring, dann auch der Polynomring $R[x]$.

Beweis. Seien $f, g \in R[x]$, beide $\neq 0$. Wir zeigen $fg \neq 0$. Sei dazu

$$f(x) = a_0 + \cdots + a_n x^n,$$
$$g(x) = b_0 + \cdots + b_m x^m$$

mit $a_n \neq 0 \neq b_m$. Dann gilt

$$f(x)g(x) = c_0 + \cdots + c_{m+n} x^{m+n},$$

wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere ist dann $c_{m+n} = a_n b_m \neq 0$, da R ein Integritätsring ist. □

(g) Sind R, S Ringe, dann ist auch das kartesische Produkt $R \times S$ ein Ring, indem man die Operationen Komponentenweise definiert. Das Nullelement ist $(0,0)$ und die Eins ist $(1,1)$. Dieser Ring ist kein Integritaetsring, auch wenn R und S welche sind, denn es gilt

$$(0,1) \cdot (1,0) = (0,0).$$

Definition 2.1.8. Seien R, S Ringe. Ein **Ringhomomorphismus** ist eine Abbildung $\phi : R \to S$ so dass

- ϕ ist ein Gruppenhomomorphismus $(R,+) \to (S,+)$,
- $\phi(1) = 1$,
- $\phi(ab) = \phi(a)\phi(b)$.

Beispiele 2.1.9. (a) Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Ringhomomorphismen.

(b) Sei $m \in \mathbb{N}$. Die Projektion $\mathbb{Z} \to \mathbb{Z}/m$ ist ein Ringhomomorphismus.

(c) Ist $R = K[x]$ ein Polynomring und ist $\alpha \in K$. dann ist die Abbildung $\delta_\alpha : K[x] \to K$, die $f(x)$ auf $f(\alpha)$ schickt, ein Ringhomomorphismus.

Satz 2.1.10. *Ein Ring R ist genau dann ein Integritaetsring, wenn R ein Unterring eines Körpers ist.*

In dem Fall gibt es bis einen Körper $\mathrm{Quot}(R)$*, der R enthaelt und von R erzeugt wird. (D.h. es gibt keinen Körper, der zwischen R und* $\mathrm{Quot}(R)$ *liegt.) Er heißt der* **Quotientenkörper** *von R.*

Beweis. Ist R Unterring eines Körpers, dann ist er offen sichtlich integer. Sei umgekehrt R ein Integritaetsring. Wir wollen einen Körper $K = \mathrm{Quot}(R)$ konstruieren. Dieser soll aus den Quotienten $\frac{a}{b}$ bestehen, mit $a, b \in R$ und $b \neq 0$, so dass die ueblichen Rechenregeln, also $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ und $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ gelten. Man konstruiert K genauso, wie man $\mathbb{Q}$ aus $\mathbb{Z}$ konstruiert: Auf der Menge $R \times R \setminus \{0\}$ definiert man eine Aequivalenzrelation durch

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad ad = bc.$$

Man sieht leicht, dass dies eine Arquivalenzrelation ist, der schwerste Teil ist die Transitivitaet: Seien also $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$, dann gilt also

$$ad = bc \quad \text{und} \quad cf = de.$$

Damit folgt $afcd = becd$, also $cd(af - be) = 0$ und da wir in einem Integritaetsring sind und $cd \neq 0$, folgt $af = be$, also $(a, b) \sim (e, f)$, d.h. es gilt Transitivitaet.

Sei $K = \big(R \times R \setminus \{0\}\big)/\sim$. Wir schreiben die Aequivalenzklassen als Brueche, also $\frac{a}{b} = [(a,b)]$. Wir definieren dann die Addition und Multiplikation durch

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{und} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Hierbei ist natuerlich Wohldefiniertheit zu pruefen. Wir tun das für die Addition. Sei also $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$. Wir muessen dann zeigen, dass $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ gilt. Wir wollen also zeigen

$$ab'dd' + bb'cd' \stackrel{!}{=} a'bdd' + bb'c'd. \qquad (*)$$

Wir haben

$$ab' = a'b \quad \text{und} \quad cd' = c'd.$$

Durch direktes Anwenden dieser beiden Formeln folgt allerdings die Behauptung (*) und damit die Wohldefiniertheit der Addition. Die Multiplikation geht aehnlich und der Nachweis, dass es sich um einen Körper hundelt, ist leicht. Der interessante Punkt ist hier nur, warum jedes Element $\neq 0$ invertierbar ist: Sei $\frac{a}{b} \neq 0$, dann ist insbesondere $b \neq 0$, also liegt auch $\frac{b}{a}$ in K und es gilt $\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$ und dies ist die Eins in K.

Wir muessen nun zeigen, dass R durch die Abbbildung $x \mapsto \frac{x}{1}$ in K eingebettet wird. Wegen

$$\frac{x}{1} + \frac{y}{1} = \frac{x+y}{1} \quad \text{und} \quad \frac{x}{1}\frac{y}{1} = \frac{xy}{1}$$

ist diese Abbildung ein Ringhomomorphismus. Er ist injektiv, denn $\frac{x}{1} = \frac{y}{1}$ ist aequivalent zu der Identitaet $1 \cdot x = 1 \cdot y$ in R. Also koennen wir R als einen Unterring von K auffassen und K besteht komplett aus Elementen, die Quotienten von Elementen aus R sind. □

2.2 Das Lemma von Zorn

Definition 2.2.1. Eine **partielle Ordnung** auf einer Menge M ist eine Relation $\leq$ auf I so dass für alle $x, y, z \in M$ gilt

(a) $x \leq x$ (Reflexivität)

(b) $x \leq y, y \leq x \quad \Rightarrow \quad x = y$ (Antisymmetrie)

(c) $x \leq y, y \leq z \quad \Rightarrow \quad x \leq z$ (Transitivität)

Beispiele 2.2.2. (a) Auf jeder Menge ist die Identität "=" eine partielle Ordnung.

(b) Auf der Menge $\mathbb{N}$ der natürlichen Zahlen ist die übliche "kleiner gleich" Relation eine partielle Ordnung. Desgleichen für $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(c) Ist X irgendeine Menge. Auf der Potenzmenge $\mathcal{P}(X)$ liefert die Mengeninklusion eine partielle Ordnung.

Definition 2.2.3. Eine partiell geordnete Menge $(M, \leq)$ heißt **vollständig geordnet** oder **linear geordnet**, wenn je zwei Elemente vergleichbar sind. Also wenn für je zwei Elemente x, y mit $x \neq y$ entweder $x \leq y$ oder $y \leq y$ gilt.

Beispiele 2.2.4. (a) Die Identität "=" auf M ist genau dann linear, wenn die Menge höchstens ein Element hat.

(b) Die natürliche Ordnungen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind alle linear.

(c) Die Ordnung auf der Potenzmenge $\mathcal{P}(X)$ ist in der Regel nicht linear. (Nur dann, wenn $|X| \leq 1$)

Lemma 2.2.5 (Lemma von Zorn)**.** *Sei $(M, \leq)$ eine partiell geordnete Menge. Existiert zu jeder linear geordneten Teilmenge $L \subset M$ eine obere Schranke $s \in M$, dann hat M maximale Elemente.*

Hierbei ist $s \in M$ eine **obere Schranke** zu $L \subset M$, wenn $x \leq s$ für jedes $x \in L$ gilt.

Ferner heißt ein Element $m \in M$ **maximales Element**, wenn $m \leq x \Rightarrow m = x$ gilt.

Die Bedingung, dass jede linear geordnete Teilmenge eine obere Schranke besitzt, wird auch **Kettenbedingung** genannt. Diese Sprechweise kommt daher, dass linear geordnete Teilmengen auch Ketten genannt werden.

Man kann das Lemma von Zorn aus dem **Auswahlaxiom** der Mengenlehre folgern. Dieses Axiom besagt, dass ein Produkt nichtleerer Mengen eine nichtleere Menge ist. Genauer besagt es, dass zu einer gegebenen Indexmenge $I \neq \emptyset$ und gegebene Mengen $X_i \neq \emptyset$ das Produkt $X = \prod_{i \in I} X_i$ eine nichtleere Menge ist. (D.h., man kann simultan in allen Mengen X_i jeweils ein Element auswählen.) Man kann sogar zeigen, dass das Lemma von Zorn, auf der Basis der underen Axiome der Mengenlehre, zum Auswahlaxiom äquivalent ist. Es ist daher legitim, das Lemma von Zorn selbst als ein Axiom aufzufassen.

2.3 Ideale

Definition 2.3.1. Sei R ein Ring (kommutativ mit Eins). Ein **Ideal** in R ist eine Teilmenge $I \subset R$ mit den folgenden Eigenschaften

- I ist eine additive Untergruppe von R und
- ist $r \in R$ und $a \in I$, dann ist $ra \in I$. Kurz geschrieben lautet diese Bedingung

$$RI \subset I.$$

Beispiele 2.3.2. (a) 0 und der ganze Ring R sind Ideale.

(b) Sei $I \subset R$ ein Ideal. Enthält I ein invertierbares Element, so ist $I = R$.

(c) Ist $\phi : R \to S$ ein Ringhomomorphismus, dann ist $\ker(\phi) = (x \in R : \phi(x) = 0)$ ein Ideal.

Beweis. Da ϕ ein additiver Gruppenhomomorphismus ist, ist der Kern eine Untergruppe. Sei also $a \in I$ und $r \in R$. Dann folgt $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$, also ist $ar \in I$. □

(d) Ist $r \in R$, so ist die Menge

$$(r) = rR = (rx : x \in R)$$

ein Ideal. Ein solches Ideal nennt man **Hauptideal**.

(e) Ist $a \in R$, so ist die Menge

$$\mathrm{Ann}(a) := (r \in R : ra = 0)$$

ein Ideal, genannt der **Annullator** von a.

Definition 2.3.3. In der Regel ist nicht jedes Ideal ein Hauptideal. Ein **Hauptidealring** ist ein Ring R, der

(a) nullteilerfrei ist und in dem

(b) jedes Ideal ein Hauptideal ist.

Beispiele 2.3.4. (a) Jeder Körper K ist ein Hauptidealring, denn er hat nur zwei Ideale, $\{0\} = (0)$ und $K = (1)$.

(b) $\mathbb{Z}$ ist ein Hauptidealring.

Beweis. Sei $I \subset \mathbb{Z}$ ein Ideal. Ist $I \cap \mathbb{N} = \varnothing$, dann ist auch $I \cap (-\mathbb{N}) = \varnothing$ und daher $I = \{0\} = (0)$. Ist $I \cap \mathbb{N} \neq \varnothing$, dann gibt es eine kleinste natürliche Zahl $m \in I$. Wir behaupten, dass $I = (m) = m\mathbb{Z}$. Klar ist $(m) \subset I$. Se also $k \in I$, dann existiert ein $p \in (m)$ so dass $0 \leq k - p < m$. Da m minimal in $I \cap \mathbb{N}$ ist, folgt $k - p = 0$, also $k = p \in (m)$. □

(c) Ist K ein Körper, so ist der Polynomring $K[x]$ ein Hauptidealring.

Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Polynom von minimalem Grad. Sei $f \in I$ beliebig, dann ist $\text{grad}(f) \geq \text{grad}(g)$, also existieren nach der **Division mit Rest** Polynome q, r mit

$$f = qg + r$$

und $\text{grad}(r) < \text{grad}(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = gq \in (g)$. □

(d) Der Polynomring $\mathbb{Z}[x]$ ist kein Hauptidealring.

Beweis. Betrachte das Ideal I, das von 2 und x erzeugt wird, also

$$I = 2\mathbb{Z}[x] + x\mathbb{Z}[x].$$

Wäre I ein Hauptideal (g), so müsste g, da $2 \in I$, den Grad Null haben, also gleich einer Zahl $m \in \mathbb{N}$ gewählt werden können. Da m dann die Zahl 2 teilt, folgte $m = 2$, aber $x \in I$ und $x \notin (2)$. □

(e) Der Ring $R = \mathbb{Z}[i\sqrt{5}]$ ist kein Hauptidealring, denn das Ideal $I = \alpha R + 3R$, das von $\alpha = i\sqrt{5}$ und 3 erzeugt wird, ist kein Hauptideal. *Angenommen*, es wäre eines, etwa $I = \eta R$. Da $\alpha \in I$, folgt $\alpha = \eta z$ für ein $z \in R$. Dann ist $5 = |\alpha|^2 = |\alpha|^2|z|^2 = 5|z|^2$. Nun ist für jedes $(a + b\alpha) \in R$ das Quadrat des Betrages $a^2 + 5b^2$ in $\mathbb{Z}$, also ist $|z| = 1$ und damit $z = \pm 1$, wir können $\eta = \alpha$ annehmen. Dann ist aber $3 = \alpha w$ für ein $w \in R$, was zu $9 = |3|^2 = |\alpha|^2|w|^2 = 5|w|^2$ führt, also ist 9 in $\mathbb{Z}$ ein Vielfaches von 5, *Widerspruch!*

Definition 2.3.5. Ein Integritätsring R heißt **euklidischer Ring**, falls es eine Abbildung $\delta : R \setminus 0 \to \mathbb{N}_0$ gibt, so dass zu je zwei $a, b \in R \setminus \{0\}$ zwei Elemente $q, r \in R$ existieren mit

$$a = bq + r$$

und $r = 0$ oder $\delta(r) < \delta(b)$. Man nennt δ die **Gradabbildung** des euklidischen Rings.

Proposition 2.3.6. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Element von minimalem Grad, also $\delta(g)$ minimal unter allen $\delta(f)$ mit $f \in I$. Da $g \in I$, folgt $(g) \subset I$. Sei $f \in I$ beliebig, dann ist also $\delta(f) \geq \delta(g)$, also existieren Elemente q, r mit

$$f = qg + r$$

und $\delta(r) < \delta(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = gq \in (g)$. □

Beispiele 2.3.7. (a) $\mathbb{Z}$ ist ein euklidischer Ring mit $\delta(k) = |k|$.

(b) Sei K ein Körper, dann ist der Polynomring $K[x]$ euklidisch mit $\delta(f) = \text{grad}(f)$.

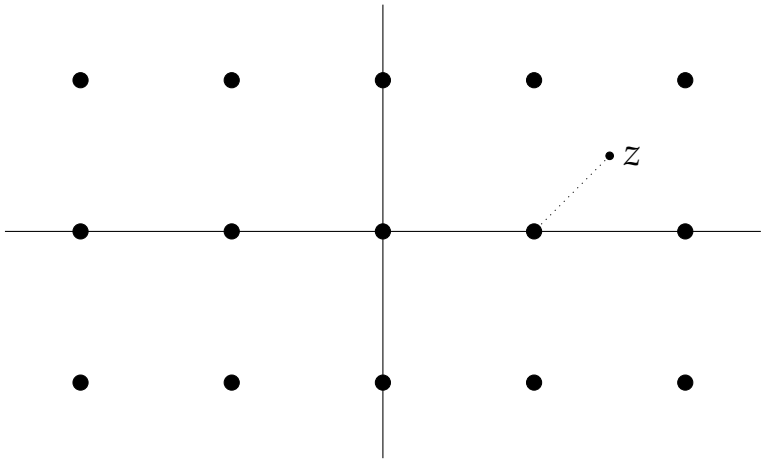
(c) Der Ring $R = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ aller komplexer Zahlen $m + ni$ mit $m, n \in \mathbb{Z}$ ist ein euklidischer Ring mit

$$\delta(m + ni) = m^2 + n^2, \quad \text{also} \quad \delta(z) = |z|^2 = z\overline{z}.$$

Beweis. Beachte zunaechst, dass die Funktion δ auf ganz $\mathbb{C}$ definiert ist und mutliplikativ ist, d.h., für $z, w \in \mathbb{C}$ gilt stets

$$\delta(zw) = \delta(z)\delta(w).$$

Wir stellen fest, dass für jedes $z \in \mathbb{C}$ der Abstund zum naechsten Punkt $c \in R$ stets $\leq \frac{1}{\sqrt{2}}$ ist.



Mit underen Worten, zu jedem $z \in \mathbb{C}$ existiert ein $c \in R$ mit $\delta(z-c) \leq \frac{1}{2}$. Seien nun $a = m + ni$ und $b = k + li$ in $\mathbb{Z}[i] \setminus \{0\}$ und sei $z = \frac{a}{b} \in \mathbb{C}$. Dann existiert also ein $c \in \mathbb{Z}[i]$ mit $\delta(z-c) \leq \frac{1}{2}$. Setze $r = a - bc \in R$. Dann ist

$$\delta(r) = \delta(b)\delta\Big(\frac{a}{b} - c\Big) \leq \delta(b)\frac{1}{2} < \delta(b).$$

Damit ist $R = \mathbb{Z}[i]$ ein euklidischer Ring, also insbesondere ein Hauptidealring. □

Definition 2.3.8. Sei R ein Ring und $I \subset R$ ein Ideal. Dann ist I eine Untergruppe von $(R, +)$ und wir können die Menge R/I der Nebenklassen betrachten.

Satz 2.3.9. *Auf der Menge R/I gibt es genau eine Ringstruktur, so dass die Projektion $\pi : R \to R/I$ ein Ringhomomorphismus ist. Für diesen Ringhomomorphismus gilt $I = \ker(\pi)$, also ist jedes Ideal der Kern eines Ringhomomorphismus.*

Beweis. Wir machen uns zunächst klar, dass für $a, b \in R$ die Bedingung $a + I = b + I$ gleichwertig ist zu $a - b \in I$.

Wir definieren Addition und Multiplikation durch
$(a + I) + (b + I) = (a + b) + I$ und $(a + I)(b + I) = ab + I$. Hier ist

Wohldefiniertheit zu prüfen. Seien $a_I = a' + I$ und $b + I = b'I$, also $a - a', b - b' \in I$, dann folgt

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

also folgt $(a + b) + I = (a' + b') + I$ und damit die Wohldefiniertheit der Addition. Für die Multiplikation rechne

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b - b') + (a - a')b' \in I. \end{aligned}$$

Die Eindeutigkeit der Ringstruktur ist wegen der Surjektivität von π klar und der Kern der Projektion $R \to R/I$ ist die triviale Nebenklasse, also I. □

Beispiel 2.3.10. Der Ring $\mathbb{Z}/m$ ist gleich $\mathbb{Z}/m\mathbb{Z}$.

Ein Ideal $\mathfrak{m}$ eines Rings R heisst **maximales Ideal**, wenn $\mathfrak{m} \neq R$ und $\mathfrak{m}$ ist maximal in der Menge aller Ideale $I \neq R$, also mit underen Worten:

(a) $1 \notin \mathfrak{m}$ und

(b) ist I ein Ideal mit $\mathfrak{m} \subset I$ und $I \neq R$, dann ist $\mathfrak{m} = I$.

Satz 2.3.11. (a) *Jedes Ideal $I \neq R$ liegt in einem maximalen Ideal.*

(b) *Jedes Element von $R \setminus R^\times$ liegt in einem maximalen Ideal.*

(c) *Ein Ideal J ist genau dann maximal, wenn R/J ein Körper ist.*

Proof. (a) Sei $I \neq R$ ein Ideal und sei S die Menge aller Ideale J mit $1 \notin J$ und $J \supset I$. Dann ist S mit der Inklusion partiell geordnet und die Kettenbedingung ist erfüllt, denn sei $\varnothing \neq K \subset S$ eine Kette, also eine linear geordnete Teilmenge und sei $\mathfrak{a} = \bigcup_{J \in K} J$, dann ist $\mathfrak{a}$ wieder ein

Ideal und es gilt $I \subset \mathfrak{a}$, sowie $1 \notin \mathfrak{a}$. Dieses $\mathfrak{a}$ ist dann eine obere Schranke zu K. Nach dem Lemma von Zorn gibt es ein maximales Element $\mathfrak{m}$ in S, also liegt I in einem maximalen Ideal.

(b) Sei $r \in R \setminus R^\times$ eine Nichteinheit und sei $I = (r) = rR$ das Hauptideal. Dann gilt $1 \notin I$, da r nicht invertierbar ist. Also gibt es nach Teil (a) ein maximales Ideal, das I und damit auch r enthaelt.

(c) Sei J ein maximales Ideal und sei $r \in R \setminus J$. Wegen der Maximalitaet von J muss das Ideal $rR + J$ gleich dem ganzen Ring sein, also auch die Eins enthalten, es gibt also $r' \in R$ und ein $\alpha \in J$ mit $rr' + \alpha = 1$ oder $rr' \in 1 + J$, so dass in R/J gilt $(r + J)(r' + J) = rr' + J = 1 + J$, das heisst, dass r im Quotienten R/J invertierbar ist, also ist in R/J jedes Element $\neq 0$ invertierbar, d.h., R/J ist ein Körper.

Sei umgekehrt R/J ein Körper und sei $r \in R \setminus J$, dann ist r modulo J invertierbar, also existiert ein $r' \in R$ mit $rr' \in 1 + J$, so dass $1 \in rR + J$, also ist J maximal. □

Beispiele 2.3.12. (a) Die maximalen Ideale von $\mathbb{Z}$ sind genau die Hauptideale $p\mathbb{Z}$, wobei p eine Primzahl ist.

(b) Die maximalen Ideale von $R = \mathbb{C}[x]$ sind genau die Hauptideale der Form $I_\lambda = (x - \lambda)\mathbb{C}[x]$ für $\lambda \in \mathbb{C}$. Die Abbildung $f(x) \mapsto f(\lambda)$ induziert einen Isomorphismus

$$R/I_\lambda \cong \mathbb{C}.$$

Definition 2.3.13. Ein Ideal $I \neq R$ eines Rings R heisst **Primideal**, falls

$$ab \in I \quad \Rightarrow \quad a \in I \text{ oder } b \in I.$$

Satz 2.3.14. *Ein Ideal I von R ist genau dann ein Primideal, wenn R/I integer ist.*

Beweis. Sei I ein Primideal und seien $(a+I), (b+I) \in R/I$ mit $(a+I)(b+I) = [0]$, also $0 = [ab]$ was soviel heisst wie $ab \in I$. Da I ein Primideal ist, folgt $a \in I$ oder $b \in I$, also sagen wir, es sei $a \in I$. das heisst aber $(a+I) = [0]$, also ist $(a+I)$ in R/I das Nullelement, damit ist R/I integer.

Sei umgekehrt R/I integer und seien $a, b \in R$ mit $ab \in I$. Das bedeutet $[0] = [ab] = (a+I)(b+I)$. Da R/I integer ist, folgt $(a+I) = [0]$ oder $(b+I) = [0]$ also sagen wir $(a+I) = [0]$, also $a \in I$ und damit ist I ein Primideal. □

2.4 Teilbarkeit

Definition 2.4.1. Seien a, b Elemente eines Rings R.

(a) Man sagt a **teilt** b oder ist ein **Teiler** von b, falls es ein $c \in R$ gibt so dass $ac = b$. in diesem Fall schreibt man $a \mid b$. Ist a kein Teiler von b, so schreibt man $a \nmid b$.

(b) a und b heißen **assoziiert**, wenn es eine Einheit $u \in R^\times$ gibt mit $a = bu$.

Beispiele 2.4.2. (a) Für zwei natürliche Zahlen m, n gilt m teilt n in $\mathbb{Z}$ genau dann, wenn m ein Teiler im üblichen Sinne ist.

(b) Zwei Elemente a, b in $\mathbb{Z}$ sind genau dann assoziiert, wenn $a = \pm b$ gilt.

Lemma 2.4.3. *Für zwei Elemente a, b eines Integritaetsrings R sind äquivalent*

(i) $a \mid b$ *und* $b \mid a$,

(ii) $aR = bR$,

(iii) *a und b sind assoziiert.*

Beweis. (i)⇒(iii): Es gelte $a = bc$ und $b = ad$. Wir nehmen an, dass $a \neq 0$, da sonst auch $b = 0$. Es ist $a = bc = acd$, also $a(1 - cd) = 0$ und da $a \neq 0$ und R integer ist, folgt $cd = 1$, also sind c, d Einheiten und a und b sind assoziiert.

(iii)⇒(ii) Es sei $a = bu$ mit einer Einheit u. Wegen $uR = R$ folgt dann $aR = buR = bR$.

(ii)⇒(i) Sei $aR = bR$, dann folgt $a \in bR$, also gibt es ein $c \in R$ mit $a = bc$, also $b \mid a$. Ebenso folgt $b \mid a$. □

Definition 2.4.4. Sei R ein Integritätsring und p ein Element, das weder Null noch eine Einheit ist.

(a) Das Element p heißt **irreduzibel**, falls aus der Gleichung $p = ab$ in R stets folgt, dass a oder b eine Einheit ist.

(b) Das Element p heißt **Primelement**, falls aus $p \mid ab$ stets folgt $p \mid a$ oder $p \mid b$.

Beispiele 2.4.5. (a) In $R = \mathbb{Z}$ sind die Primelemente genau die Elemente der Form $\pm p$, wobei p eine Primzahl ist.

(b) In $R = \mathbb{C}[x]$ sind die Primelemente genau die Elemente $c(x - a)$ mit $c \in \mathbb{C}^\times$, $a \in \mathbb{C}$.

(c) In $R = \mathbb{R}[x]$ sind die Primelemente genau die Polynome der Form $c(x - \alpha)$ für ein $\alpha \in \mathbb{R}$ oder $c(x^2 + ax + b)$, falls dieses Polynom keine reelle Nullstelle hat.

Proposition 2.4.6. *Sei R ein Integritätsring. Dann ist jedes Primelement von R auch irreduzibel.*

Beweis. Seien p ein Primelement und sei $p = ab$. Dann teilt p das Produkt ab also teilt p einen der Faktoren, sagen wir a. Das heißt $a = pc = abc$, also $a(1 - bc) = 0$, also $bc = 1$, so dass b eine Einheit ist. □

Beispiel 2.4.7. In dem Integritätsring $R = \mathbb{Z}[i\sqrt{5}]$ ist das Element 3 irreduzibel, aber kein Primelement.

Beweis. Sei $\alpha = i\sqrt{5}$. Wir zeigen, dass 3 irreduzibel ist. Ist $3 = zw$ in R, dann folgt $9 = |3|^2 = |z|^2|w|^2$. Ist $|z|^2 = 1$, dann ist $z = \pm 1$ eine Einheit. Ist $|z|^2 = 9$, dann ist $|w|^2 = 1$ und w ist eine Einheit. *Angenommen,* $|z|^2 = 3$. Sei $z = a + b\alpha$, dann ist $3 = |z|^2 = a^2 + 5b^2$, also ist $b = 0$, da der Betrag sonst zu gross wäre. Dann ist $3 = a^2$, aber 3 ist kein Quadrat in $\mathbb{Z}$, *Widerspruch!* Also ist 3 irreduzibel.

Wir zeigen, dass 3 kein Primelement ist. Hierzu beachte, dass $3 \mid 9 = (2+\alpha)(2-\alpha)$, aber 3 teilt keinen der Faktoren, denn würde 3 etwa $2 + \alpha$ teilen, also $2 + \alpha = 3z$, dann ist $9 = |2 + \alpha|^2 = |3|^2|z|^2$, also $|z| = 1$ und damit ist $z = \pm 1$, also $3 = \pm(2 + i\sqrt{5})$ was ein Widerspruch ist, da 3 den Imaginaerteil 0 hat. □

Satz 2.4.8. *Sei R ein Hauptidealring und sei $p \in R$. Dann sind äquivalent*

(a) *p irreduzibel,*

(b) *p ist ein Primelement.*

Beweis. Wir müssen nur (a)⇒(b) zeigen: Sei p irreduzibel und p teile ab und $p \nmid a$. Wir muessen zeigen, dass p das Element b teilt. Sei I das von p und a erzeugte Ideal, also $I = aR + pR$. Dann ist dies ein Hauptideal, also etwa $I = cR$. Dann folgt $c \mid a$ und $c \mid p$, also etwa $cd = p$. Da p irreduzibel ist, ist c oder d eine Einheit. **Angenommen**, d ist eine Einheit, so ist $pR = cR = I = aR + pR$, also ist $a \in pR$, d.h. p teilt a, was der Voraussetzung **widerspricht**.

Also ist d keine Einheit und damit muss c eine Einheit sein, d.h., $I = cR = R$ und es gibt $r, s \in R$ mit $ar + ps = 1$, also $b = abr + psb$. Nun teilt p

das Produkt ab, also ist $b = p(r' + sb)$ für ein $r' \in R$, also $p \mid b$ wie verlangt. □

Korollar 2.4.9. *In einem Hauptidealring R lässt sich jedes Element von $R \setminus \{0\}$, das keine Einheit ist, als endliches Produkt von Primelementen Schreiben.*

Beweis. Da jedes irreduzible Element prim ist, genügt es, eine Zerlegung in irreduzible zu konstruieren. Sei $a \in R$ ungleich Null und keine Einheit. *Angenommen*, a lässt sich nicht als Produkt von Irreduziblen schreiben. Dann ist a reduzibel und kann selbst als Produkt $a_1 a_1'$ von Nichteinheiten geschrieben werden. Da a kein Produkt von Irreduziblen ist, gilt dasselbe für mindestens einen der Faktoren, sagen wir a_1, und a_1 kann als Produkt $a_2 a_2'$ zweier Nichteinheiten geschrieben werden. Iteration liefert eine Folge von Elementen

$$a = a_0, a_1, \cdots \in R$$

so dass a_{j+1} ein Teiler von a_j, aber nicht assoziiert zu a_j ist. Also folgt für die Hauptideale

$$aR = a_0 R \subsetneq a_1 R \subsetneq a_2 R \subsetneq \dots$$

Man prüft leicht nach, dass die Vereinigung einer aufsteigenden Folge von Idealen wieder ein Ideal ist, also ist

$$I = \bigcup_{j \in \mathbb{N}} (a_j)$$

wieder ein Ideal in R, also ein Hauptideal $I = bR$. Dann ist $b \in a_j R$ für ein j und daher

$$bR \subset a_j R \subset a_{j+1} R \subset bR,$$

woraus Gleichheit folgt, also $a_j R = a_{j+1} R$ ein *Widerspruch!* Daher ist die Annahme falsch, also ist jedes Element als Produkt von Irreduziblen darstellbar. □

Lemma 2.4.10. *Gilt in einem Integritätsring R die Gleichung*

$$p_1 \cdots p_r = q_1 \cdots q_s$$

für Primelemente p_j und irreduzible Elemente q_i, dann ist $r = s$ und nach Umnummerierung ist jedes p_j assoziiert zu q_j.

Beweis. Da $p_1 \mid q_1 \cdots q_s$, gibt es ein j mit $p_1 \mid q_j$. Nach Umnummerierung können wir $p_1 \mid q_1$ annehmen. Es folgt $q_1 = \varepsilon_1 p_1$, wobei ε_1 auf Grund der Irreduzibilität von q_1 eine Einheit ist. Da wir uns in einem Integritätsring befinden, folgt

$$p_2 \cdots p_r = \varepsilon_1 q_2 \cdots q_s.$$

Wir iterieren diesen Vorgang und können die q_i so umnummerieren, dass p_j zu q_j assoziiert ist. Insbesondere folgt $r \leq s$. Ist $r < s$ erhalten wir

$$1 = \varepsilon q_{r+1} \cdots q_s,$$

woraus folgt, dass q_s eine Einheit ist, was ein Widerspruch ist, also ist $r = s$. □

Definition 2.4.11. Ein Integritätsring R heißt **faktoriell**, falls jede Nichteinheit in $R \setminus \{0\}$ als Produkt von Primelementen darstellen lässt, das heißt wenn wir eine sogenannte **Primfaktorzerlegung** haben. Diese ist dann nach dem Lemma 2.4.10 eindeutig.

Proposition 2.4.12. *In einem faktoriellen Ring ist jedes irreduzible Element prim.*

Proof. Sei q irreduzibel und $p_1 \cdots p_n$ die Primfaktorzerlegung. Angenommen $n > 1$, dann ist p_1 oder $p_2 \cdots p_n$ einer Einheit, was nicht sein kann. Also ist $q = p_1$, also prim. □

Satz 2.4.13. *Jeder Hauptidealring ist faktoriell. Insbesondere ist $\mathbb{Z}$ faktoriell und für jeden Körper K ist der Polynomring $K[x]$ faktoriell.*

Beweis. Folgt aus Korollar 2.4.9 und Lemma 2.4.10. □

Beispiel 2.4.14. Der Ring $R = \mathbb{Z}[i\sqrt{5}]$ is nicht faktoriell, denn wir wissen ja schon, das es Irreduzible gibt, die nicht prim sind.

Definition 2.4.15. Sei R ein faktorieller Ring. Sei P ein Vertretersystem der Primelemente modulo Assoziiertheit, also P enthalte zu jeder Klasse von assoziierten Primelementen genau ein Element. Hat man ein solches P fest gewählt, kann man jede Nichteinheit $z \in R \setminus \{0\}$ eindeutig in der Form

$$z = \varepsilon \prod_{p \in P} p^{k_p}$$

schreiben, wobei ε eine Einheit ist und $k_p \in \mathbb{N}_0$, fast alle Null sind. Sind dann

$$z = \varepsilon \prod_{p \in P} p^{k_p}, \qquad w = \eta \prod_{p \in P} p^{n_p}$$

zwei solche Darstellungen, dann ist klar, dass z das Element w genau dann teilt, wenn $k_p \leq n_p$ für jedes $p \in P$ gilt. Wir definieren wir den **größten gemeinsamen Teiler** der Elemente z, w als

$$\mathrm{ggT}(z, w) = \prod_{p \in P} p^{\min k_p, n_p},$$

sowie das **kleinste gemeinsame Vielfache** als

$$\mathrm{kgV}(z, w) = \prod_{p \in P} p^{\max k_p, n_p}$$

Beispiele 2.4.16. (a) Im Fall $R = \mathbb{Z}$ kann man die Menge der Primzahlen als P nehmen.

(b) Im Fall $R = K[x]$ für einen Körper K sind die Einheiten genau die konstanten in $K^\times$, also ist jedes Polynom zu einem eindeutig bestimmten normierten Polynom assoziiert. Damit kann man als P die Menge aller normierter Primpolynome wählen.

(c) Im Allgemeinen hat man keine kanonische Wahl für P. Daher hängen die Begriffe ggT und kgV dann von der Wahl von P ab und sind daher nur bis auf Assoziiertheit definiert.

Satz 2.4.17. *Seien a, b, z von Null verschiedene Elemente eines Hauptidealrings R.*

(a)
$$\big(z \mid a, \ \textit{und} \ \ z \mid b\big) \quad \Leftrightarrow \quad z \mid \mathrm{ggT}(a,b).$$

(b)
$$\big(a \mid z, \ \textit{und} \ \ b \mid z\big) \quad \Leftrightarrow \quad \mathrm{kgV}(a,b) \mid z.$$

(c) *Für den größten gemeinsamen Teiler $d = \mathrm{ggT}(a,b)$ gilt dann*
$$aR + bR = dR.$$
Insbesondere gibt es Elemente $x, y \in R$ mit
$$\mathrm{ggT}(a,b) = ax + by.$$

(d) *Zwei Elemente $r, s \in R$ heissen* **teilerfremd**, *falls $\mathrm{ggT}(r,s) = 1$. Dies ist genau dann der Fall, wenn es $x, y \in R$ gibt mit*
$$rx + sy = 1.$$

Beweis. (a) und (b) sind klar, wenn man die Produktzerlegungen betrachtet.

(c) Das Ideal $aR + bR$ ist ein Hauptideal, etwa $aR + bR = d'R$. Wegen $a, b \in (d')$ ist d' dann ein gemeinsamer Teiler von a und b, teilt demnach d. Andererseits teilt d auch a und b und teilt demnach d', so dass d und d' assoziiert sind.

(d) Sind r, s teilerfremd, so gibt es x und y nach Teil (c). Umgekehrt gelte $rx + sy = 1$. Dann gilt $aR + bR = R$, also $\mathrm{ggT}(a, b) = 1$. □

Korollar 2.4.18. *Sei R ein Hauptidealring und $p \in R \setminus \{0\}$. Dann sind äquivalent;*

(a) *p ist ein Primelement.*

(b) *R/pR ist ein Körper.*

Beweis. Sei p ein Primelement und sie $\bar{z} \in R/pR \setminus \{0\}$ die Äquivalenzklasse von $z \in R$. Dass $\bar{z} \neq 0$ ist bedeutet, dass $z \notin pR$ ist, was bedeutet, dass p in der Primfakorzerlegung von z nicht vorkommt und damit ist $\mathrm{ggT}(z, p) = 1$. Daher ist $zR + pR = R$, also gibt es $x, y \in R$ mit $zx + py = 1$, oder $\bar{z}\bar{x} = 1$ in R/pR, so dass $\bar{z}$ invertierbar ist.

Für die Umkehrung sei R/pR ein Körper und p teile ein Produkt ab. Dann ist $\bar{a}\bar{b} = 0$ und daher $\bar{a} = 0$ oder $\bar{b} = 0$, also $p \mid a$ oder $p \mid b$. □

Beispiel 2.4.19. $\mathbb{Z}/m$ ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist. In diesem Fall schreibt man $\mathbb{F}_p = \mathbb{Z}/p$.

2.5 Lokalisierung

Sei R ein Integritaetsring und sei $S \subset R$ eine **multiplikativ abgeschlossene Teilmenge**, d.h., wir fordern

- $0 \notin S$, $1 \in S$,
- $x, y \in S \;\Rightarrow\; xy \in S$.

Beispiele 2.5.1. (a) Sei $f \in R \setminus \{0\}$ und sei $S = \{1, f, f^2, \dots\}$, dann ist S eine multiplikativ abgeschlossene Teilmenge.

(b) Ist $\mathfrak{p} \subset R$ ein Primideal, dann ist das Komplement $S = R \setminus \mathfrak{p}$ eine multiplikativ abgeschlossene Teilmenge.

(c) Da R ein Integritaetsring ist, ist $S = R \setminus \{0\}$ eine multiplikativ abgeschlossene Teilmenge.

Definition 2.5.2. Sei S eine multiplikativ abgeschlossene Teilmenge des Integritaetsrings R. Die **Lokalisierung** von R nach S ist der Unterring $S^{-1}R$ des Quotientenkoerpers $\mathrm{Quot}(R)$, der von R und

$$S^{-1} = \{s^{-1} : s \in S\}$$

erzeugt wird. Da S multiplikativ abgeschlossen ist, gilt

$$S^{-1}R = \left\{ \frac{a}{s} : a \in R,\ s \in S \right\}.$$

Beispiele 2.5.3. (a) Ist $R = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$, dann ist $S^{-1}\mathbb{Z} = \mathbb{Q}$.

(b) Ist $R = K[x]$ der Polynomring über einem Körper K, dann ist der Quotientenkoerper der Körper $K(x)$ der **rationalen Funktionen** über K.

2.6 Der chinesische Restsatz

Definition 2.6.1. Zwei Ideale I, J in einem Ring heißen **teilerfremd**, falls $I + J = R$ gilt.

Beispiel 2.6.2. In $R = \mathbb{Z}$ sind die Hauptideale $m\mathbb{Z}$ und $n\mathbb{Z}$ genau dann teilerfremd, wenn die Zahlen m und n keine echten gemeinsamen Teiler haben, wenn also m und n teilerfremd sind.

Beweis. Seien die Ideale teilerfremd, dann ist $1 \in m\mathbb{Z} + n\mathbb{Z}$, es gibt also

$a, b \in \mathbb{Z}$ mit $am + bn = 1$. Wuerden nun m und n von einer Primzahl p geteilt, dann wuerde auch 1 von p geteilt, was ein Widerspruch ist.

Seien umgekehrt die Zahlen m und n teilerfremd. Das Ideal $m\mathbb{Z} + n\mathbb{Z}$ ist ein Hauptideal, also von der Form $g\mathbb{Z}$ für ein $g \in \mathbb{N}$. Dann ist $m \in g\mathbb{Z}$ also folgt $g|m$ und ebenso $g|n$ und daher ist $g = 1$, also sind die Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ teilerfremd. □

Definition 2.6.3. Sind I und J Ideale, so definieren wir das Ideal IJ als

$$IJ = \left\{ \sum_{j=1}^{n} a_j b_j : a_j \in I,\ b_j \in J \right\}.$$

Sind etwa beides Hauptideale, $I = (a)$ und $J = (b)$, dann ist auch IJ ein Hauptideal, nämlich $IJ = (ab)$.

Lemma 2.6.4. *Sind die Ideale I und J teilerfremd, dann gilt*

$$IJ = I \cap J.$$

Beweis. Die Inklusion "$\subset$" gilt auch ohne die Teilerfremdheit, da $IJ \subset IR = I$ und ebenso für J.

Zum Beweis von "$\supset$" seien also I und J teilerfremd, also gibt es Elemente $a \in I$ und $b \in J$ mit $1 = a + b$. Sei dann $x \in I \cap J$, dann ist $x = ax + bx$ und da axund bx beide in IJ liegen, ist $x \in IJ$. □

Satz 2.6.5 (Chinesischer Restsatz)**.** *Sei R ein Ring und $I_1, \ldots, I_r$ seien parweise teilerfremde Ideale. Sei $I = I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$, dann liefern die kanonischen Projektionen einen Isomorphismus*

$$R/I \cong \prod_{\nu=1}^{r} R/I_\nu.$$

Beweis. Da $I_\nu \supset I$ für jedes ν, gibt es kanonische Projektionen $\pi_\nu : R/I \to R/I_\nu$, also einen Ringhomomorphismus

$$\pi : R/I \to \prod_{\nu=1}^{r} R/I_\nu.$$

Injektivität: Sei $\pi(\bar{x}) = 0$, und $x \in R$ ein Urbild von $\bar{x}$. Dann ist $x \in I_\nu$ für jedes ν. Mit dem Lemma folgt dann also

$$\begin{aligned} x &\in I_1 \cap I_2 \cap \cdots \cap I_r \\ &= (I_1 I_2) \cap I_3 \cap \cdots \cap I_r \\ &= (I_1 I_2 I_3) \cap I_4 \cap \cdots \cap I_r \\ &\vdots \\ &= I_1 I_2 \cdots I_r. \end{aligned}$$

Also gilt $\tilde{x} = x + I_1 \cdots I_r = 0$ in dem Ring R/I, also ist π injektiv.

Surjektivität. Für die Surjektivität reicht es, zu zeigen, dass es Elemente $x_j \in R$ gibt, mit $\pi_j(x_j) = 1$ und $\pi_k(x_j) = 0$ für $k \neq j$. Modulo Umnummerierung reicht es, x_1 nachzuweisen. Seien $a \in I$ und $b \in I_2 \cdots I_r$ mit $a + b = 1$. Dann ist $x_1 = b$ das gewünschte Element. □

Korollar 2.6.6. *Sei R ein Hauptidealring und sei*

$$a = \varepsilon p_1^{\nu_1} \cdots p_r^{\nu_r}$$

eine Primfaktorzerlegung mit einer Einheit und paaweise nicht assoziierten Primelementen p_i. Ist $\pi_i : R \to R/p_i^{\nu_i} R$ jeweils die kanonische Projektion, dann ist der Homomorphismus

$$\pi : R \to \prod_{i=1}^{r} R/p_i^{\nu_i} R$$

surjektiv mit Kern aR, induziert also einen Isomorphismus

$$R/aR \cong \prod_{i=1}^{r} R/p_i^{\nu_i} R.$$

Beweis. Klar nach Chinas Restsatz, da nichtassoziierte Primelemente teilerfremd sind. □

* * *

3 Moduln

3.1 Definition

Definition 3.1.1. Ein **Modul** über einem Ring R ist eine abelsche Gruppe M mit einer Abbildung

$$\begin{aligned} R \times M &\to M \\ (\lambda, m) &\mapsto \lambda m, \end{aligned}$$

so dass für alle $\lambda, \mu \in R$ und alle $m, n \in M$ gilt

- $1_R m = m$,
- $(\lambda\mu)m = \lambda(\mu m)$,
- $(\lambda + \mu)m = \lambda m + \mu m, \quad \lambda(m+n) = \lambda m + \lambda n.$

Beispiele 3.1.2. (a) Für einen Körper K sind die K-Moduln genau die K-Vektorraeume.

(b) Der Ring R selbst ist ein R-Modul und eine Teilmenge $T \subset R$ ist genau dann ein Untermodul, wenn T ein Ideal ist.

(c) Jede abelsche Gruppe $(M, +)$ ist auf genau eine Weise ein Modul unter $R = \mathbb{Z}$, denn $km = m + \cdots + m$ mit k-Kopien, wenn $k \in \mathbb{N}$ und es ist das Inverse, wenn $k < 0$. Es gilt also

$$\{\text{abelsche Gruppen}\} \;=\; \{\mathbb{Z}\text{-Moduln}\}$$

Es gilt auch, dass ein Gruppenhomomorphismus zwischen zwei abelschen Gruppen dasselbe ist, wie ein $\mathbb{Z}$-Modulhomomorphismus.

(d) Sei K ein Körper und R der Polynomring $K[x]$. Sei V ein K-Vektorraum und $T : V \to V$ ein Endomorphismus. Dann wird V

ein R-Modul durch

$$(f(x))v := f(T)v.$$

Ist also $f(x) = a_0 + \cdots + a_n x^n$, so ist

$$f(x)v = a_0 v + a_1 Tv + \cdots + a_n T^n v.$$

Definition 3.1.3. Eine **R-lineare Abbildung** oder ein **Modulhomomorphismus** zwischen zwei Moduln ist ein Gruppenhomomorphismus $\phi : M \to N$ mit der Eigenschaft

$$\Phi(rm) = r\phi(m)$$

für jedes $m \in M$ und jedes $r \in R$.

Definition 3.1.4. Ein **Untermodul** eines R-Moduls M ist eine Teilmenge $N \subset M$, die mit den Strukturen von M selbst wieder ein Modul ist.

Beispiel 3.1.5. Eine Teilmenge $I \subset R$ ist genau dann eine Untermodul, wenn sie ein Ideal ist.

Definition 3.1.6. Seien $M_1, \ldots, M_k$ Untermoduln eines Moduls M, dann ist die **Summe** der Moduln definiert als

$$U = M_1 + \cdots + M_k := \left(m_1 + \cdots + m_k : m_j \in M_j\right) \subset M.$$

Dies ist ein Untermodul, wie man leicht sieht. Gilt zusätzlich

$$m_1 + \cdots + m_k = m_1' + \cdots + m_{k'}' \quad \Rightarrow \quad k = k', m_1 = m_1', \ldots, m_k = m_k'$$

wobei $m_j, m_j' \in M_j$ für $1 \leq j \leq k$, so sagen wir, die Summe ist **direkt** und schreiben dies als

$$U = M_1 \oplus \cdots \oplus M_k.$$

Dann ist die Summe $U + V$ zweier Untermoduln genau dann direkt, wenn $U \cap V = 0$ gilt. Ist $U \oplus V = M$, sagen wir, die Moduln U und V sind **komplementär**.

Lemma 3.1.7. *Ist $U \subset M$ ein Untermodul, auf der Menge der Nebenklassen $M/U = \{m + U : m \in M\}$ definiert man eine Addition durch $(m + U) + (n + U) = m + n + U$ und eine Sklarmultiplikation $\lambda(m + U) = \lambda m + U$. Diese sind wohldefiniert und geben M/U eine Modulstruktur, derart dass die Projektion $M \to M/U$ ein Modulhomomorphismus wird.*

Proof. Gilt etwa $m + U = m' + U$ und $n + U = n' + U$, dann folgt

$$m' + n' + U = m' + n' + \underbrace{(m - m')}_{\in U} + \underbrace{(n - n')}_{\in U} + U = m + n + U.$$

Sowie

$$\lambda m' + U = \lambda m' + \lambda(m - n') + U = \lambda m + U.$$

Damit folgt die Wohldefiniertheit. Die Homomorphismus Eigenschaft gilt nach Definition. □

Beispiel 3.1.8. $n\mathbb{Z}$ ist ein Untermodul von $\mathbb{Z}$ und wir haben wiederholt $\mathbb{Z}/n\mathbb{Z}$ betrachtet.

Definition 3.1.9. Sei M ein R=Modul. Die **Länge** des Moduls M, geschrieben $\ell(M) = \ell_R(M)$ ist das Supremum der Längen ℓ von Ketten von Untermoduln

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M$$

Beispiele 3.1.10. (a) Ist $R = K$ ein Körper, dann ist die Länge eines Moduls (=Vektorraums) gleich seiner Dimension.

(b) Eine abelsche Gruppe $(M, +)$, aufgefasst als $\mathbb{Z}$-Modul hat genau dann endliche Länge, wenn sie endlich ist. Die Länge des $\mathbb{Z}$-Moduls $\mathbb{Z}/m$ für $m \in \mathbb{N}$ ist gleich der Anzahl aller Primteiler von m, mit Vielfachheit gezaehlt.

Lemma 3.1.11. *Sei R ein Hauptidealring und sei $a \in R \setminus \{0\}$ mit Primfaktorzerlegung $a = \varepsilon p_1 \cdots p_r$. Dann hat der Restklassenmodul R/aR die Länge $\ell_R(R/aR) = r$.*

Beweis. Sei $\pi : R \to R/aR$ die Projektion. Die Untermoduln $U \subset R/aR$ entsprechen bijektiv ihren Urbildern unter π und dies sind die Ideale I von R, die aR enthalten, so dass die Länge mit dem Supremum aller Längen von Idealketten der Art

$$aR \subsetneq I_1 \subsetneq \cdots \subsetneq I_l = R$$

übereinstimmt. Da R ein Hauptidealring ist, wird jedes I_ν von einem Element a_ν erzeugt. Die Inklusion $I_\nu \subsetneq I_{\nu+1}$ bedeutet, dass a_ν ein echter Teiler von $a_{\nu+1}$ ist. Daher müssen die Potenzen in der Primfaktorzerlegung absteigen und die maximale Länge einer solchen Kette ist r. □

Lemma 3.1.12. *Ist M die direkte Summe zweier Untermoduln L und N, so gilt*

$$\ell(M) = \ell(L) + \ell(N).$$

Beweis. Seien

$$0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_r = M_1,$$
$$0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_s = M_2$$

echt aufsteigende Ketten von Untermoduln, dann ist

$$0 \subsetneq \big(L_1 \oplus 0\big) \subsetneq \cdots \subsetneq \big(L_r \oplus 0\big) \subsetneq \big(L_r \oplus N_1\big) \subsetneq \cdots \subsetneq \big(L_r \oplus N_r\big) = M$$

eine Kette in M, also ist $\ell(L) + \ell(N) \leq \ell(M)$.

Für die umgekehrte Richtung sei

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M$$

eine echt aufsteigende Kette von Untermoduln. Seien π_L und π_N die Projektionen auf die beiden Summanden L und N. Ist etwa $M_j \cap L = M_{j+1} \cap L$, dann behaupten wir, dass $\pi_N(M_j) \neq \pi_N(M_{j+1})$ ist,

denn gilt auch hier Gleichheit, dann gibt es zu $m \in M_{j+1}$ ein $\tilde{m} \in M_j$ mit $\pi_N(m) = \pi_N(\tilde{m})$, also ist $m - \tilde{m} \in \ker \pi_N \cap M_{j+1} = L \cap M_{j+1} = L \cap M_j$ und damit ist $m \in M_{j+1}$, was ein Widerspruch zu $M_j \neq M_{j+1}$ ist. Damit wächst bei jedem j entweder $M_j \cap L$ oder $\pi_N(M_j)$ und so folgt $\ell \leq \ell(L) + \ell(N)$. □

Definition 3.1.13. Sind M, N Moduln, dann ist $V = M \times N$ auch einer. Man fasst $M \cong M \times 0$ und $N \cong 0 \times N$ jeweils als Untermoduln von V auf und schreibt dann $V = N \oplus M$. Entsprechend ist der Modul $M_1 \oplus M_2 \oplus \cdots \oplus M_k = \bigoplus_{j=1}^{k} M_j$ definiert.

Lemma 3.1.14. *Sei R ein Hauptidealring und Q ein Modul mit*

$$Q \cong \bigoplus_{j=1}^{n} R/\alpha_j R,$$

wobei $\alpha_j \in R \setminus 0$ Nichteinheiten so dass $\alpha_j \mid \alpha_{j+1}$ für $1 \leq j \leq n-1$, dann sind die α_j bis auf Assoziiertheit durch den Modul Q eindeutig bestimmt.

Beweis. Aus technischen Gründen invertieren wir die Nummerierung der α_j und betrachten zwei Darstellungen

$$Q \cong \bigoplus_{j=1}^{n} R/\alpha_j R \cong \bigoplus_{j=1}^{m} R/\beta_j R,$$

mit $\alpha_{j+1} \mid \alpha_j$ und desgleichen für β_i. Falls es einen Index $k \leq \min(m, n)$ mit $\alpha_k R \neq \beta_k R$ gibt, so wähle k minimal mit dieser Eigenschaft. Da $\alpha_i R = \beta_i R$ für $1 \leq i < k$, und da $\alpha_{k+1}, \ldots, \alpha_n$ sämtlich Teiler von α_k sind,

zerlegt sich $\alpha_k Q$ zu

$$\begin{aligned}\bigoplus_{i=1}^{k-1} \alpha_k \cdot (R/\alpha_i R) &\cong \alpha_k Q \\ &\cong \alpha_k \left(\bigoplus_{j=1}^{m} R/\beta_j R \right) \\ &\cong \bigoplus_{i=1}^{k-1} \alpha_k \cdot (R/\alpha_i R) \oplus \bigoplus_{j=k}^{m} \alpha_k \cdot (R/\beta_j R)\end{aligned}$$

Aus Lemma 3.1.11 und Lemma 3.1.12 folgt $\ell\big(\alpha_k \cdot (R/\beta_j R)\big) = 0$ für $k \le j \le m$. Dies bedeutet aber insbesondere $\alpha_k \cdot (R/\beta_k R) = 0$, oder $\alpha_k R \subset \beta_k R$. Analog zeigt man $\alpha_k R \supset \beta_k R$, also $\alpha_k R = \beta_k R$, also gibt es solches k gar nicht. □

3.2 Der Elementarteilersatz

Definition 3.2.1. Wir betrachten Matrizen über einem beliebigen Ring R. Eine Matrix $A \in \mathrm{M}_n(R)$ heißt **invertierbar**, falls es eine Matrix $B \in \mathrm{M}_n(R)$ gibt, mit $AB = BA = I$.

Lemma 3.2.2. *Sei R ein kommutativer Ring mit Eins.*

(a) *Fuer $A, B \in \mathrm{M}_n(R)$ gilt*

$$\det(AB) = \det(A)\det(B).$$

(b) *Eine Matrix $A \in \mathrm{M}_n(R)$ ist genau dann invertierbar, wenn $\det(A) \in R$ eine Einheit ist.*

Beweis. (a): Die Aussage gilt fuer Matrizen ueber dem Quotientenkoerper K des Integritaetsrings

$$S = Z[X_1, \ldots, X_N],$$

daher gilt sie auch fuer alle Matrizen in $\mathrm{M}_n(S)$. Seien $r_1, \ldots, r_N$ alle Eintraege von A und B. Fuer den Ringhomomorphismus

$$\begin{aligned} \phi : S = Z[X_1, \ldots, X_N] &\to R, \\ X_j &\mapsto r_j \end{aligned}$$

gibt es Matrizen $\hat{A}, \hat{B} \in \mathrm{M}_n(S)$ mit $\phi\big(\hat{A}\big) = A$ und $\phi\big(\hat{B}\big) = B$. Da ϕ ein Ringhomomorphismus ist, folgt $\phi(\hat{A}\hat{B}) = AB$ und damit

$$\begin{aligned} \det(AB) &= \det\big(\phi\big(\hat{A}\hat{B}\big)\big) \\ &= \det\big(\phi\big(\hat{A}\big)\phi\big(\hat{B}\big)\big) \\ &= \det\big(\phi\big(\hat{A}\hat{B}\big)\big) \\ &= \phi\big(\det\big(\hat{A}\hat{B}\big)\big) \\ &= \phi\big(\det\big(\hat{A}\big)\det\big(\hat{B}\big)\big) \\ &= \phi\big(\det\big(\hat{A}\big)\big)\phi\big(\det\big(\hat{B}\big)\big) \\ &= \det\big(A\big)\det\big(B\big). \end{aligned}$$

(c) Sei $A^{\#}$ die Komplementärmatrix. Man stellt fest, dass in dem Beweis der Formel

$$AA^{\#} = A^{\#}A = \det(A)I$$

nirgends benutzt wurde, dass man über einem Körper rechnet. Er gilt also auch über R. Ist also $\det(A) \in R^{\times}$, so ist $\det(A)^{-1}A^{\#}$ eine Inverse zu A.

Für die Umkehrung sei A invertierbar. Dann gilt
$\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det I = 1$, also ist $\det(A)$ eine Einheit. □

Beispiel 3.2.3. Eine Matrix $A \in \mathrm{M}_n(\mathbb{Z})$ ist genau dann in $\mathrm{M}_n(\mathbb{Z})$ invertierbar, wenn gilt $\det(A) = \pm 1$. Wir bestimmen also mal die Inverse

zu $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Es ist

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

Wir stellen also fest, dass $\begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}$ die gesuchte Inverse ist.

Satz 3.2.4 (Elementarteilersatz für Matrizen)**.** *Sei R ein Hauptidealring und $A \in \mathrm{M}_n(R)$ eine quadratische Matrix über R. Dann existieren invertierbare Matrizen $S, T \in \mathrm{GL}_n(R)$ mit*

$$SAT = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

wobei alle $d_j \neq 0$ und $d_j \mid d_{j+1}$ für $1 \leq j \leq k-1$ gilt. Dabei sind k die d_j bis auf Assoziiertheit eindeutig bestimmt, man nennt sie die **Elementarteiler** *der Matrix A.*

Beweis. Wir betrachten die Menge aller Ideale der Form Ra, wobei a irgendein Eintrag von A ist. In dieser Menge gibt es ein maximales Ideal Ru. Durch Zeilen- und Spaltenvertauschung erreichen wir, dass

$u = a_{1,1}$ links oben steht. Sei nun die Matrix von der Gestalt

$$A = \begin{pmatrix} u & \dots \\ v & \dots \\ \vdots & \dots \end{pmatrix}$$

und sei w der ggT von u und v. Dann gibt es $a, b \in R$ mit $w = au + bv$ und $w|u$, sowie $w|v$. Sei $\hat{X}$ die Matrix

$$\hat{X} = \begin{pmatrix} a & b \\ -v/w & u/w \end{pmatrix}.$$

Dann ist $\det \hat{X} = 1$, also ist $\hat{X}$ invertierbar und die Matrix

$$X = \begin{pmatrix} \hat{X} & 0 \\ 0 & I \end{pmatrix}$$

ist ebenfalls invertierbar. Die Matrix XA hat links oben $\begin{pmatrix} w \\ 0 \end{pmatrix}$ stehen. Man wiederholt dies mit den anderen Zeilen statt der zweiten und sieht, dass es ein $Y \in \mathrm{GL}_n(R)$ gibt mit

$$YA = \begin{pmatrix} w' & \dots \\ 0 & \dots \end{pmatrix}.$$

Ebenso findet man ein $Z \in \mathrm{GL}_n(R)$, so dass $YAZ = \begin{pmatrix} w'' & 0 \\ 0 & B \end{pmatrix}$. Wiederholung desselben mit der Matrix B und so fort liefert Matrizen $F, G \in \mathrm{GL}_n(R)$ so dass FAG diagonal ist. Wir muessen nun noch die Teilbarkeitsbedingung herstellen. Durch Zeilen und Spaltentausch koennen wir voraussetzen, dass die Matrix von der Form $\begin{pmatrix} D & \\ & 0 \end{pmatrix}$ ist, wobei D eine Diagonalmatrix mit allen Diagonaleintraegen $\neq 0$ ist. Wir verfahren aehnlich, schreiben jetzt nur den oberen linken 2×2 Block auf. Sei also $A = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}$. Sei $\alpha = au + bv$ der ggT. Die Matrix

$\hat{X} = \begin{pmatrix} a & b \\ -v/\alpha & u/\alpha \end{pmatrix}$ erfuellt

$$\hat{X}A = \begin{pmatrix} au & bv \\ -uv/\alpha & uv/\alpha \end{pmatrix}.$$

Addiert man die zweite Spalte zur ersten, was durch Rechtsmultiplikation mit $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ erreicht wird, erhaelt man $\begin{pmatrix} \alpha & bv \\ 0 & uv/\alpha \end{pmatrix}$. Da $\alpha | v$, kann man ein Vielfaches der ersten Spalte zur zweiten addieren und erhaelt $\begin{pmatrix} \alpha & 0 \\ 0 & uv/\alpha \end{pmatrix}$, wobei nun α den Eintrag uv/α teilt. Iteration liefert eine Diagonalmatrix SAT, bei der der erste Eintrag alle folgenden teilt. Iteration liefert die Existenzbehauptung.

Die Eindeutigkeitsbehauptung reduziert sich darauf, zu zeigen, dass aus

$$S\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} = \begin{pmatrix} f_1 & & & & & \\ & \ddots & & & & \\ & & f_l & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} T \qquad S, T \in \mathrm{GL}_n(R),$$

folgt $k = l$ und $d_j = f_j$, falls beide Diagonalmatrizen die Teilbarkeitsbedingung erfuellen. Da $\det(S)$ und $\det(T)$ Einheiten sind, ist d_1 der ggT aller Eintraege links, also auch der ggT aller Eintraege rechts und damit gilt $d_1 = f_1$ bis auf Assoziiertheit. Weiter ist $d_1 d_2$ der ggT aller 2×2 Unterminoren links, also ist $f_1 f_2$ dieselbe Zahl. Iteration mit den Minoren wachsender Dimension liefert die Eindeutigkeit. □

Definition 3.2.5. Eine **Basis** eines Moduls M ist eine Teilmenge $\mathfrak{b} \subset M$, so dass jedes $m \in M$ eine Linearkombination ist

$$m = \sum_{j=1}^{k} \lambda_k b_k$$

mit eindeutig bestimmten $b_j \in \mathfrak{b}$ und eindeutig bestimmten $\lambda_j \in R$. Nicht

jeder Modul hat eine Basis, wie zB $\mathbb{Z}/n\mathbb{Z}$ als $\mathbb{Z}$-Modul betrachtet.

Hat M eine endliche Basis $\mathcal{b}$, dann ist $M \cong R^n$, wobei $n = |\mathcal{b}|$, der Beweis geht genauso wie in LinA1 im Falle eines Körpers. Wir sprechen dann von einem **endlich-freien Modul**.

Satz 3.2.6 (Elementarteilersatz für Moduln)**.** *Sei R ein Hauptidealring und F ein endlich-freier Modul, sowie $M \subset F$ ein Untermodul. Dann existieren Elemente $x_1, \dots, x_k$ von F, die Teil einer Basis sind, sowie Koeffizienten $a_1, \dots, a_k \in R$ mit*

- *$a_i \mid a_{i+1}$ falls $1 \leq i \leq k-1$ und*
- *$a_1 x_1, \dots, a_k x_k$ ist eine Basis von M.*

Die a_j sind bis auf Assoziiertheit durch M eindeutig bestimmt, sie werden die **Elementarteiler** *von M genannt.*
Insbesondere folgt: Ein Untermodul eines endlich-freien Moduls ist endlich-frei!

Beweis. Sei $b_1, \dots, b_n$ eine Basis von F. Wir zeigen durch Induktion nach n, dass M endlich erzeugt ist, und zwar durch höchstens n Erzeuger. Für $n = 1$ ist M ein Ideal und also durch ein Element erzeugt. Sei also $n > 1$. Setze $F' = \sum_{j=1}^{n-1} Rb_j$ und $F'' = Rb_n$. Sei $\pi : F \to F''$ die Projektion. Die Moduln $M \cap F'$ und $\pi(M)$ sind erzeugt durch $n-1$ bzw einen Erzeuger und man zeigt wie im Körperfall, dass ein Erzeugendensystem von $M \cap F'$ erweitert um ein Urbild eines Erzeugers von $\pi(M)$ ein Erzeugendensystem von M bildet, M ist also endlich erzeugt mit $\leq n$ Erzeugern. Sei $z_1, \dots, z_n$ ein Erzeugendensystem von M und betrachte die Matrix A der linearen Abbildung $F \cong R^n \to R^n \cong F$ gegeben durch $b_j \mapsto z_j$. Fasse die Matrizen S und T aus Satz 3.2.4 als Basiswechsel auf, so folgt die Behauptung. □

3.3 Endlich erzeugte Moduln über Hauptidealringen

Definition 3.3.1. Sei M ein Modul des Hauptidealrings R. Der **Torsionsuntermodul** ist definiert als

$$T = (x \in M : \exists_{r \in R}\, r \neq 0,\ rx = 0)\,.$$

Dann ist T ein Untermodul. M heißt **Torsionsmodul**, falls M mit T übereinstimmt.

Beispiele 3.3.2. (a) Ist M eine abelsche Gruppe als $\mathbb{Z}$-Modul aufgefasst, dann ist der Torsionsuntermodul genau die Menge der Elemente endlicher Ordnung.

(b) $\mathbb{Z}/m$ ist ein Torsionsmodul unter $\mathbb{Z}$.

(c) Ist K ein Körper und ist $R = K[x]$. Sei V ein R-Modul, der als K-Vektorraum endliche Dimension hat. Dann ist V ein Torsionsmodul.

Beweis. Sei T der Operator auf V, durch den x operiert. Sei $f(x)$ das charakteristische Polynom von T. Dann ist $f(T)v = 0$ für jedes v, also ist jedes v Torsion. □

Satz 3.3.3. *Sei M ein endlich erzeugter Modul über einem Hauptidealring R und $T \subset M$ sein Torsionsmodul. Dann gibt es einen endlich-erzeugten freien Untermodul $F \subset M$, etwa $F \cong R^d$, sowie Nichteinheiten $\alpha_1, \ldots, \alpha_n \in R \setminus 0$, mit $\alpha_j \mid \alpha_{j+1}$ für $1 \leq j \leq n-1$ und*

$$M = F \oplus T, \quad T \cong \bigoplus_{j=1}^{n} R/\alpha_j R.$$

Dabei ist d eindeutig bestimmt und wird der **Rang** *von M genannt. Die Elemente $\alpha_1, \ldots, \alpha_n$ sind eindeutig bestimmt bis auf Assoziiertheit.*

Es gilt ferner

$$T \cong \bigoplus_{\nu=1}^{N} R/p_\nu^{e_\nu} R,$$

wobei $p_1, \ldots, p_N$ Primelemente sind und $e_1, \ldots, e_N \in \mathbb{N}$ und die Primpotenzen $p_\nu^{e_\nu}$ sind bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt.

Beweis. Da M endlich erzeugt ist, gibt es einen surjektiven Homomorphismus $\phi : R^r \to M$, also $M \cong R^r/\ker(\phi)$. Nach dem Elementarteilersatz für Moduln existiert eine Basis $x_1, \ldots, x_r$ von R^r und Elemente $\alpha_1, \ldots, \alpha_n \in R$ mit $\alpha_1 \mid \ldots \mid \alpha_n$, so dass $\alpha_1 x_1, \ldots, \alpha_n x_n$ eine Basis von $\ker\phi$ ist. Wir setzen $\alpha_{n+1} = \cdots = \alpha_r = 0$ und betrachten den surjektiven Homomorphismus

$$\psi : R^r = \bigoplus_{j=1}^{r} R \to \bigoplus_{j=1}^{r} R/\alpha_j R.$$

mit $\psi(\gamma_1, \ldots, \gamma_r) = (\bar{\gamma}_1, \ldots, \bar{\gamma}_r)$. Nach Konstruktion ist $\ker\phi = \ker\psi$ und daher

$$M \cong R^r/\ker\phi \cong R^{n-r} \oplus \bigoplus_{j=1}^{n} R/\alpha_j R,$$

wobei wir eventuelle Summanden mit $\alpha_j \in R^\times$, also $R/\alpha_j R = 0$ unterdrücken. Die Summe $\bigoplus_{j=1}^{n} R/\alpha_j R$ ist genau der Torsionsmodul der rechten Seite und daher ist die Zerlegung eindeutig.

Der Zusatz folgt, indem man die Primfaktorzerlegung der α_j betrachtet und den chinesischen Restsatz benutzt. Die Eindeutigkeit der Primpotenzen folgt aus der Eindeutigkeit der α_j und der Eindeutigkeit der Primfaktorzerlegung. □

3.4 Der Hauptsatz über endlich-erzeugte abelsche Gruppen

Satz 3.4.1. *Sei G eine endlich-erzeugte abelsche Gruppe, dann gibt es eine eindeutig bestimmte Zahl $r \in \mathbb{N}_0$ und eindeutig bestimmte Primzahlpotenzen $q_1 \leq q_2 \leq \cdots \leq q_s$ so dass*

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{j=1}^{s} \mathbb{Z}/q_j\mathbb{Z}$$

Beweis. Folgt direkt aus Satz 3.3.3 für den Ring $R = \mathbb{Z}$, denn $\mathbb{Z}$-Moduln sind dasselbe wie abelsche Gruppen. □

3.5 Jordan-Normalform

Wir betrachten nun den Fall $R = K[x]$ für einen Körper K. Ein Modul über R besteht aus einem K-Vektorraum V zusammen mit einem Endomorphismus $T : V \to V$, wobei $x \in R$ durch T operiert. Ein Modulhomomorphismus $\Phi : (V, T) \to (W, S)$ ist eine lineare Abbildung $\Phi : V \to W$ mit $\Phi T = S\Phi$.

Zu $\lambda \in K$ sei p_λ das Primelement $p_\lambda(x) = x - \lambda$ in R. Sei $W = R/p_\lambda^k$ für ein $k \in \mathbb{N}$. Dann ist W ein K-Vektorraum der Dimension k mit der Basis $v_1 = [(x-\lambda)^{k-1}], v_2 = [(x-\lambda)^{k-2}], \ldots, v_k = [(x-\lambda)^0]$. Sei $T : W \to W$ der durch x induzierte Operator, dann folgt $(T - \lambda)v_j = v_{j+1}$, wenn wir formal $v_{k+1} = 0$ setzen. Mit underen Worten, in der Basis $v_1, \ldots, v_k$ ist T durch die Jordan-Matrix

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

gegeben.

Satz 3.5.1 (Jordan-Normalform)**.** *Sei $T : V \to V$ ein Endomorphismus des endlich-dimensionalen K-Vektorraums V. Nimm an, dass das charakteristische Polynom χ_T in Linearfaktoren zerfällt. Dann hat V eine Basis bezüglich der T durch eine Jordan-Matrix der Form*

$$\begin{pmatrix} J_{k_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{k_s}(\lambda_s) \end{pmatrix}$$

dargestellt wird.

Beweis. Der R-Modul (V, T) ist Torsion, hat also eine Zerlegung der Form

$$\bigoplus_{j=1}^{N} R/p_j^{s_j}R,$$

wobei die p_j Primelemente sind. Da χ_T durch Null operiert, ist $\chi_T R \subset p_j^{s_j}R$ für jedes j. Das bedeutet $p_j \mid \chi_T$. Da χ_T in Linearfaktoren zerfällt, muss p_j selbst einer sein, also $p_j(x) = x - \lambda_j$. Damit folgt die Behauptung nach unseren Vorbemerkungen. □

* * *

Teil II

Multilineare Algebra

4 Multilineare Algebra

In diesem Abschnitt sei K ein Körper.

4.1 Basen

Definition 4.1.1. Eine Teilmenge $T \subset V$ eines Vektorraums V heißt **linear unabhängig**, falls jede endliche Teilmenge linear unabhängig ist, oder, äquivalent, falls beliebige $v_1, \dots, v_n \in T$ und $\lambda_1, \dots, \lambda_n \in K$ gilt

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \qquad \Rightarrow \qquad \lambda_1 = \lambda_2 = \cdots = 0.$$

Definition 4.1.2. Eine Teilmenge E eines Vektorraums V heißt **Erzeugersystem**, falls jeder Vektor $v \in V$ eine Linearkombination von Vektoren aus E ist. Man schreibt das auch als $V = \mathrm{Span}(E)$.

Lemma 4.1.3. *Für eine Teilmenge $\mathcal{B}$ eines Vektorraums V sind die folgenden äquivalent:*

(a) *$\mathcal{B}$ ist eine maximale linear unabhängige Menge,*

(b) *$\mathcal{B}$ ist ein linear unabhängiges Erzeugersystem,*

(c) *$\mathcal{B}$ ist ein minimales Erzeugersystem,*

(d) *zu jedem $v \in V$ gibt es eindeutig bestimmte Koeffizienten λ_b, $b \in B$, fast alle Null, so dass*

$$v = \sum_{b \in \mathcal{B}} \lambda_b b.$$

Ist dies der Fall, nennen wir $\mathcal{B}$ eine **Basis** *von V.*

Man kann (c) auch so formulieren: zu jedem $v \in V$ gibt es eindeutig bestimmte $v_1, \dots, v_n \in \mathcal{B}$ und eindeutig bestimmte $\lambda_1, \dots, \lambda_n \in \mathbb{K} \setminus \{0\}$, so dass

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Beweis. Der Beweis verläuft genau so wie in LinA 1. Als Beispiel soll hier mal (a)⇒(b) gezeigt werden: Sei $\mathcal{B}$ maximal linear unabhängig. Wir zeigen dass $\mathcal{B}$ ein Erzeugersystem ist. Sei hierzu $v \in V$. **Angenommen**, $v \notin \operatorname{Span}(\mathcal{B})$. Wir behaupten, dass dann $\mathcal{B}' = \mathcal{B} \cup \{v\}$ linear unabhängig ist. Sei also $\lambda v + \lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ eine Linearkombination der Null mit $v_j \in \mathcal{B}$. Ist $\lambda \neq 0$, dann folgt $v = \frac{-1}{\lambda}\left(\lambda_1 v_1 + \cdots + \lambda_n v_n\right) \in \operatorname{Span}(\mathcal{B})$, was nicht sein kann. Daher ist also $\lambda = 0$ und damit $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ und da $\mathcal{B}$ linear unabhängig ist, folgt $\lambda_1 = \cdots = \lambda_n = 0$. Damit ist also $\mathcal{B}'$ linear unabhängig, wegen Maximalität also $\mathcal{B}' = \mathcal{B}$ und damit $v \in \mathcal{B}$ **Widerspruch!** Das heißt also, dass $\mathcal{B}$ ein linear unabhängiges Erzeugersystem ist. □

Satz 4.1.4. (a) *Jeder Vektorraum hat eine Basis.*

(b) *Ist $T \subset V$ eine linear unabhängige Teilmenge, dann gibt es eine Basis $\mathcal{B}$ mit $T \subset \mathcal{B}$.*

(c) *Je zwei Basen eine Vektorraums haben dieselbe Mächtigkeit. Diese nennt man die* **Dimension** *des Raums.*

(d) *Zwei Vektorräume gleicher Dimension sind isomorph.*

Proof. (a) folgt aus (b), indem man $T = \varnothing$ nimmt. Sei also $T \subset V$ linear unabhängig. Die Menge $\mathcal{S}$ aller linear unabhängigen Teilmengen $\mathcal{T} \subset V$ mit $T \subset \mathcal{T}$ ist durch Inklusion geordnet. Sei $\mathcal{K} \subset \mathcal{S}$ eine linear geordnete Teilmenge. Sei dann S die Vereinigung aller Elemente von K. Dann ist S

linear unabhängig, denn jede endliche Teilmenge von S liegt schon in einem Element von $\mathcal{K}$, da $\mathcal{K}$ linear geordnet ist. Also ist S eine obere Schranke von $\mathcal{K}$. Nach dem Lemma von Zorn gibt es eine maximale linear unabhängige Menge $\mathcal{T}$ mit $T \subset \mathcal{T}$. Wie in Lemma 4.1.3, (a)⇒(b), sieht man ein, dass $\mathcal{T}$ auch ein Erzeugersystem ist.

(c) Seien $\mathcal{A}$ und $\mathcal{B}$ Basen. Es reicht, beide als unendlich anzunehmen. In diesem Fall gibt es eine Surjektion $\mathcal{A} \twoheadrightarrow \mathcal{A} \times \mathbb{N}$.
(Dies ist bekannt, wenn $\mathcal{A}$ abzählbar und allgemein folgt es mit ZORN, angewendet auf die Menge der Paare (A, ϕ), wobei $A \subset \mathcal{A}$ und $\phi : A \to A \times \mathbb{N}$ surjektiv.)

Für jedes $v \in \mathcal{A}$ gibt es genau eine Darstellung

$$v = \sum_{w \in E_v} \lambda_{v,w} w$$

mit einer endlichen Teilmenge $E_v \subset \mathcal{B}$ und $\lambda_{v,w} \in K \setminus \{0\}$. Sei $(j_{v,1}, j_{v,2}, \dots)$ eine Folge in E_v, in der jedes Element vorkommt. Definiere dann

$$\begin{aligned} \phi : \mathcal{A} \times \mathbb{N} &\to \mathcal{B}, \\ (v, k) &\mapsto j_{v,k}. \end{aligned}$$

Diese Abbildung ist surjektiv. Wir erhalten Surjektionen $\mathcal{A} \twoheadrightarrow \mathcal{A} \times \mathbb{N} \twoheadrightarrow \mathcal{B}$. Da wir die Rollen von $\mathcal{A}$ und $\mathcal{B}$ vertauschen können, gibt es auch eine Surjektion $\mathcal{B} \to \mathcal{A}$ und daher eine Bijektion $\mathcal{A} \to \mathcal{B}$.

(d) Sei $\phi : V \to W$ ein Isomorphismus. Dann ist das Bild einer Basis eine Basis und daher bleibt die Mächtigkeit derselben erhalten. Seien umgekehrt $\mathcal{A} \subset V$ und $\mathcal{B} \subset W$ Basen gleicher Mächtigkeit, dann gibt es also eine Bijektion $\phi : \mathcal{A} \to \mathcal{B}$. Diese kann dann zu einer linearen Abbildung fortgesetzt werden. Die Fortsetzung von ϕ^{-1} ist dann eine Inverse der Fortsetzung von ϕ. □

Beispiele 4.1.5. (a) Sei V der $\mathbb{R}$-Vektorraum aller Folgen in $\mathbb{R}$, die nur

endlich viele Glieder $\neq 0$ haben. Dann ist die Menge $E = \{e_1, e_2, \dots\}$ mit $e_j = (0, 0, \dots, 0, 1, 0, \dots)$, wobei die 1 an der j-ten Stelle steht, eine Basis.

(b) In der Regel sind Basen für unendlich-dimensionale Räume nicht so einfach anzugeben. Der Vektorraum aller Folgen in $\mathbb{F}_2$ hat zum Beispiel eine überabzählbare Dimension.

Proposition 4.1.6. *Jeder Unterraum hat ein Komplement. Genauer sei $U \subset V$ ein Untervektorraum. Dann gibt es einen Unterraum $W \subset V$, so dass*

$$V = U \oplus W.$$

Proof. Sei $\mathcal{A}$ eine Basis von U. Setze sie zu einer Basis $\mathcal{B}$ von V fort. Sei dann $W = \mathrm{Span}(\mathcal{B} \setminus \mathcal{A})$. Wir behaupten $V = U \oplus W$. Sei hierzu $v \in U \cap W$ und sei $v = \sum_{a \in \mathcal{A}} \lambda_a a + \sum_{b \in \mathcal{B} \setminus \mathcal{A}} \mu_b b$ die eindeutige Darstellung in der Basis. Da $v \in U$, folgt $\mu_b = 0$ für alle $b \in \mathcal{B} \setminus \mathcal{A}$. Da $v \in W$ folgt ebenso $\lambda_a = 0$ für alle a. Also ist $v = 0$. Bleibt zu zeigen, dass $V = U + W$ gilt. Sei also jetzt $v \in V$ beliebig. Mit der eindeutigen Darstellung wie oben gilt

$$v = \underbrace{\sum_{a \in \mathcal{A}} \lambda_a a}_{\in U} + \underbrace{\sum_{b \in \mathcal{B} \setminus \mathcal{A}} \mu_b b}_{\in W} \in U + W. \qquad \square$$

4.2 Dualraum

Definition 4.2.1. Sei V ein Vektorraum über dem Körper K. Eine **Linearform** auf V ist eine lineare Abbildung $\alpha : V \to K$. Sind α, β Linearformen und sind $\lambda, \mu \in K$, so ist $\lambda\alpha + \mu\beta$, definiert durch

$$(\lambda\alpha + \mu\beta)(v) = \lambda\alpha(v) + \mu\beta(v),$$

wieder eine Linearform. Man sieht, dass V^* ein linearer Unterraum des Vektorraums $\mathrm{Abb}(V, K)$ ist.

Beispiele 4.2.2. (a) Ist $V = K$, so ist jede Linearform von der Form $x \mapsto \lambda x$ für ein $\lambda \in K$.

(b) Ist $V = K^n$, so ist jede Koordinatenabbildung $v \mapsto v_j$ eine Linearform.

(c) Ist S eine Menge in $V = \mathrm{Abb}(S, K)$ der Vektorraum aller Abbildungen von S nach K, so ist für jedes $s \in S$ die Punktauswertung $\delta_s : V \to K; f \mapsto f(s)$ eine Linearform.

Definition 4.2.3. Sei $v_1, \ldots, v_n$ eine Basis von V. Für $j = 1, \ldots, n$ sei v_j^* die Linearform

$$v_j^*(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_j.$$

Warnung: Die Vektoren $v_1^*, \ldots, v_n^*$ hängen von der Wahl der gesamten Basis $\mathcal{B} = (v_1, \ldots, v_n)$ ab, es sollte also besser $v_{1,\mathcal{B}}^*, \ldots, v_{n,\mathcal{B}}^*$ heißen.

Beispiele 4.2.4. (a) Sei $V = K^n$ und $e_1, \ldots, e_n$ die Stundard-Basis. Dann gilt

$$e_j^* \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_j.$$

(b) Sei die Charakteristik von $K \neq 2$ und sei $v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, sowie $v_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Dann ist v_1, v_2 eine Basis von K^2 und es gilt

$$v_1^* \begin{pmatrix} x \\ y \end{pmatrix} = \frac{x+y}{2}, \qquad v_2^* \begin{pmatrix} x \\ y \end{pmatrix} = \frac{x-y}{2}.$$

Lemma 4.2.5. *Ist $v_1, \ldots, v_n$ eine Basis von V, so ist $v_1^*, \ldots, v_n^*$ eine Basis von V^*, genannt die* **duale Basis**. *Insbesondere ist V endlich-dimensional, falls V dies ist.*

Beweis. Sei $\alpha \in V^*$. definiere $\lambda_j = \alpha(v_j)$. Wir behaupten, dass $\alpha = \lambda_1 v_1^* + \cdots + \lambda_n v_n^*$. Es reicht zu zeigen, dass diese beiden linearen auf den Basisvektoren übereinstimmen. Es ist aber gerade

$$(\lambda_1 v_1^* + \cdots + \lambda_n v_n^*)(v_j) = \lambda_1 v_1^*(v_j) + \cdots + \lambda_n v_n^*(v_j) = \lambda_j = \alpha(v_j).$$

damit ist also $\alpha = \lambda_1 v_1^* + \cdots + \lambda_n v_n^*$ und $v_n^*, \ldots, v_n^*$ ein Erzeugendensystem. Um die lineare Unabhängigkeit zu zeigen nimm an wir habe eine Linearkombination der Null: $\mu_1 v_1^* + \cdots + \mu_n v_n^* = 0$. Für $1 \leq j \leq n$ gilt dann

$$0 = (\mu_1 v_1^* + \cdots + \mu_n v_n^*)(v_j) = \mu_j,$$

also $\mu_1 = \cdots = \mu_n = 0$. □

Bemerkungen.

- Ist V endlich-dimensional und $v_1, \ldots, v_n$ eine Basis, so liefert die lineare Abbildung gegeben durch $v_j \mapsto v_j^*$ einen Isomorphismus der Vektorräume $V \to V^*$. Dieser hängt allerdings von der Wahl der Basis ab.
- Ist V unendlich-dimensional, so ist V^* nicht isomorph zu V (ohne Beweis).

Beispiele 4.2.6. (a) Ist $V = K^n$, so ist der durch die Stundard-Basis induzierte Isomorphismus $V \to V^*$ gegeben durch $x \mapsto x^t$, wobei x^t für die transponierte Matrix steht und damit für die lineare Abbildung $y \mapsto x^t y$.

(b) Die Basis $v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ und $v_2 - \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ von K^2 induziert einen Isomorphismus $K^2 \to (K^2)^*$ gegeben durch $x \mapsto (\frac{1}{2}x)^t$.

Lemma 4.2.7. *Sei $T : V \to W$ eine lineare Abbildung, so ist $T^* : W^* \to V^*$, gegeben durch*

$$T^*(\alpha) = \alpha \circ T$$

eine lineare Abbildung. Sie heißt die zu T **duale Abbildung**. *Es gilt*

$$(\lambda T + \mu S)^* = \lambda T^* + \mu S^*, \text{ sowie } (T \circ R)^* = R^* \circ T^*,$$

wobei $T, S : V \to W$, $R : U \to V$ linear sind und $\lambda, \mu \in K$.

Beweis. Wir müssen zuerst zeigen, dass $f^*(\alpha)$ wieder linear ist. Hierzu rechnen wir

$$\begin{aligned} T^*(\alpha)(\lambda v + \mu v') &= \alpha(T(\lambda v + \mu v') \\ &= \alpha(\lambda T(v) + \mu T(v') \\ &= \lambda\alpha(T(v)) + \mu\alpha(T(v')) = \lambda T^*(\alpha)(v) + \mu T^*(\alpha)(v'). \end{aligned}$$

Daher ist $T^*(\alpha)$ wieder linear und $T^* : W^* \to V^*$ wohldefiniert. Als nächstes ist zu zeigen, dass $\alpha \mapsto T^*(\alpha)$ linear ist. Dies sieht man durch

$$T^*(\lambda\alpha+\mu\beta)(v) = (\lambda\alpha+\mu\beta)(T(v)) = \lambda\alpha(T(v))+\mu\beta(T(v)) = \lambda T^*(\alpha)(v)+\mu T^*(\beta)(v).$$

Schließlich ist zu zeigen, dass für festes α die Abbildung $T \mapsto T^*(\alpha)$ linear ist, was man ähnlich zeigt.

Am Ende schließlich zur Hintereinunderausführung:

$$(T \circ R)^*(\alpha) = \alpha \circ (T \circ R) = (\alpha \circ T) \circ R = (T^*(\alpha)) \circ R = R^*(T^*(\alpha)) = R^* \circ T^*(\alpha).$$

□

Lemma 4.2.8. *Die Duale Abbildung wird durch die transponierte Matrix dargestellt. Genauer, sei $T : V \to W$ eine lineare Abbildung. Sei $\mathcal{B}$ eine Basis von V und $\mathcal{C}$ eine von W. Dann gilt*

$$\mathcal{M}_{\mathcal{B}^*}^{\mathcal{C}^*}(T^*) = \left(\mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(T)\right)^t.$$

Beweis. Sei $A = \mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(T)$, das heißt

$$T(v_j) = \sum_{i=1}^{m} a_{i,j} w_i.$$

Damit $T^*(w_k^*)(v_j) = w_k^*(T(v_j)) = a_{k,j}$, also

$$T^*(w_k^*) = \sum_{j-1}^{n} a_{k,j} v_j^*,$$

was gerade bedeutet, dass T^* durch die Matrix A^t dargestellt wird. □

Korollar 4.2.9. *Sei $T : V \to W$ linear, wobei V und W endlich-dimensional sind. Dann gilt*

(a) $\dim \text{Bild}\, T = \dim \text{Bild}\, T^*$,

(b) $\dim \ker T - \dim \ker T^* = \dim V - \dim W$,

(c) *T injektiv $\Leftrightarrow$ T^* surjektiv,*

(d) *T^* injektiv $\Leftrightarrow$ T surjektiv,*

(e) *T bijektiv $\Leftrightarrow$ T^* bijektiv.*

Beweis. (a) Sei T durch die Matrix A dargestellt. Dann ist $\dim \text{Bild}\, T$ gerade der Rang von A. Dieser ist gleich dem Rang von A^t, also gleich $\dim \text{Bild}(T^*)$.

(b) Nach den Dimensionsformeln und Teil (a) ist

$$\begin{aligned}\dim \ker T - \dim \ker T^* &= (\dim V - \dim \text{Bild}\, T) - (\dim W^* - \dim \text{Bild}\, T^*) \\ &= \dim V - \dim W.\end{aligned}$$

(c) T ist genau dann injektiv, wenn $\dim \ker T = 0$ und dies ist nach (b) äquivalent zu $\dim \ker T^* = \dim W - \dim V$ oder $\dim V = \dim \text{Bild}\, T^*$ nach Dimensionsformel. (d) folgt ähnlich und (e) folgt aus (c) und (d). □

Definition 4.2.10. Sei V ein Vektorraum. Sei $V^{**} = (V^*)^*$ der **Bidualraum**. Betrachte die Abbildung $\delta : V \to V^{**}$, $v \mapsto \delta_v$ mit

$$\delta_v(\alpha) = \alpha(v).$$

Satz 4.2.11. *Ist V endlich-dimensional, dann ist δ ein Isomorphismus.*

Beweis. Wir zeigen zunächst, dass δ linear ist. Für $v, w \in V$ und $\lambda, \mu \in K$, sowie $\alpha \in V^*$ gilt

$$\begin{aligned}\delta_{\lambda v+\mu w}(\alpha) &= \alpha(\lambda v + \mu w)\\ &= \lambda\alpha(v)_\mu\alpha(w)\\ &= \lambda\delta_v(\alpha) + \mu\delta_w(\alpha),\end{aligned}$$

also $\delta_{\lambda v+\mu w} = \lambda\delta_v + \mu\delta_w$. Damit ist δ linear. Sei $v_1, \ldots, v_n$ eine Basis von V, sei $v_1^*, \ldots, v_n^*$ die Duale Basis und sei $v_1^{**}, \ldots, v_n^{**}$ die hierzu duale Basis von V^{**}. Wir zeigen $\delta_{v_j} = \delta(v_j) = v_j^{**}$. Hierzu berechne

$$\delta_{v_j}(v_k^*) = v_k^*(v_j) = \delta_{k,j} = v_j^{**}(v_k^*). \qquad \square$$

4.3 Quotienten

Bei Vektorräumen haben wir, anders als bei Moduln, einen Komplementärraum. Damit können wir auch Quotienten besser verstehen.

Proposition 4.3.1. *Ist W ein Komplementärraum zu U, also*

$$V = U \oplus W,$$

dann ist die Abbildung $\psi : W \to V/U$; $w \mapsto [w] = w + U$ ein linearer Isomorphismus.

Beweis. ψ ist linear, denn

$$\psi(\lambda w + w') = (\lambda w + w' + U = \lambda(w + U) + (w' + U) = \lambda\psi(w) + \psi(w').$$

Die Abbildung ψ ist injektiv, denn

$$\psi(w) = 0 \;\Rightarrow\; w \in U \;\Rightarrow\; w = 0,$$

da $w \in W$. ψ ist surjektiv, denn sei $v \in V$, dann kann man $v = u + w$ schreiben mit $u \in U$ und $w \in W$. Es folgt $v + U = w + U = \psi(w)$ und daher ist ψ surjektiv. □

Korollar 4.3.2. *Ist $U \subset V$ ein linearer Unterraum, so liefern die natürlichen Abbildungen eine exakte Sequenz*

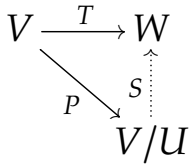
$$0 \to U \xrightarrow{\alpha} V \xrightarrow{\beta} V/U \to 0.$$

Beweis. α ist die Inklusion des Unterraums, also injektiv. β ist die Projektion des Quotienten, also surjektiv. Das Bild von α ist U und dies ist der Kern von β. □

Proposition 4.3.3 (Universelle Eigenschaft)**.** *Sei $U \subset V$ ein Unterraum und sei $P : V \to V/U$ die Projektion. Zu jeder linearen Abbildung*

$$T : V \to W$$

mit $T(U) = 0$ gibt es genau eine linear Abbildung $S : V/U \to W$ so dass das Diagramm



kommutiert. Diese universelle Eigenschaft induziert einen linearen Isomorphismus

$$(T \in \mathrm{Hom}(V, W) : T(U) = 0) \xrightarrow{\cong} \mathrm{Hom}(V/U, W).$$

Beweis. Sei die Situation wie oben. Definiere $S : V/U \to W$ durch

$$S(v + U) = T(v).$$

Für die Wohldefiniertheit sei $v + U = v' + U$. Dann folgt $v - v' \in U$, also $T(v - v') = 0$ oder $T(v) = T(v')$, was die Wohldefiniertheit zeigt. Für $v \in V$ gilt nun $T(v) = S(v + U) = S(P(v))$, also $T = S \circ P$ und damit kommutiert das Diagramm. Zur Eindeutigkeit sei $S' : V/U \to W$ eine weitere Abbildung, die das Diagramm kommutativ macht. Es gilt dann

$$S'(v + U) = T(v) = S(v + U).$$

Sei dann $\psi : (T \in \mathrm{Hom}(V, W) : T(U) = 0) \to \mathrm{Hom}(V/U, W)$ die entstehende Abbildung. Eine Stundardverifikation zeigt, dass ψ linear ist. Fuer die Injektivitaet sei T gegeben mit $S = \psi(T) = 0$. Aus der Formel $T = S \circ P$ folgt dann auch $T = 0$ und damit ist ψ injkektiv. Fuer die Surjektivitaet sei S gegeben, dann definiere T durch $T = S \circ P$, so folgt $\psi(T) = S$. □

Definition 4.3.4. Sei $T : V \to W$ linear. Den Quotienten $W/\mathrm{Bild}(T)$ nennt man den **Cokern** von T und schreibt ihn als $\mathrm{coker}(T)$. Dann ist die Sequenz

$$0 \to \ker(T) \to V \xrightarrow{T} W \to \mathrm{coker}(T) \to 0$$

exakt.

Satz 4.3.5 (Homomorphiesatz)**.** *Sei $T : V \to W$ linear, dann ist die Abbildung $\tilde{T} : v + \ker(T) \mapsto T(v)$ ein Isomorphismus*

$$V/\ker(T) \xrightarrow{\cong} \mathrm{Bild}(T).$$

Beweis. Da $T(\ker(T)) = 0$, ist die lineare Abbildung $\tilde{T}$ wohldefiniert. Sie ist offensichtlich injektiv und surjektiv. □

Satz 4.3.6. *Sei V ein K-Vektorraum und seien U, W Unterraeume.*

(a) *Die Abbildung $\phi : u + (U \cap W) \mapsto u + W$ ist ein Isomorphismus*

$$U/(U \cap W) \to (U + W)/W.$$

(b) *Gilt $W \subset U$, dann ist die Abbildung $\psi : (v + W) + (U/W) \mapsto v + U$ ein Isomorphismus*

$$\big(V/W\big)/\big(U/W\big) \to V/U.$$

Beweis. Die Wohldefiniertheit ist bei beiden Abbildungen leicht einzusehen. Zur Injektivitaet von ϕ sei $u \in U$ mit $\phi\big(u + (U \cap W)\big) = 0$. Dann folgt $u \in W$, also $u \in U \cap W$, also $u + (U \cap W) = 0 + (U \cap W)$, die Abbildung ϕ ist also injektiv. Fuer die Surjektivitaet sei $u + w + W \in (U + W)/W$ gegeben. Dann gilt $u + w + W = u + W = \phi(u + (U \cap W))$.

Fuer die Injektivitaet von ψ sei $v + W + (U/W) \in \big(V/W\big)/\big(U/W\big)$ mit $\psi\big(v + W + (U/W)\big) = 0$ gegeben. Das bedeutet, dass $v \in U$ liegt, damit also $v + W$ in $U + W$ und daher ist $v + W + (U/W)$ das Nullelement. Die Surjektivitaet von ψ ist klar. □

Korollar 4.3.7 (Alternative Formulierung des letzten Satzes)**.** *Sei V ein K-Vektorraum und seien U, W Unterraeume. Wir schreiben die Elemente von V/U nun als Aequivalenzklassen $[v]_U$, $v \in V$.*

(a) *Die Abbildung $\phi : [u]_{U+W} \mapsto [u]_W$ ist ein Isomorphismus*

$$U/(U \cap W) \xrightarrow{\cong} (U + W)/W.$$

(b) *Gilt $W \subset U$, dann ist die Abbildung $\psi : [[v]_W]_{U+W} \mapsto [v]_U$ ein*

Isomorphismus

$$(V/W)/(U/W) \to V/U.$$

4.4 Tensorprodukt

Definition 4.4.1. Für eine beliebige Menge $S \neq 0$ sei $K[S]$ der Vektorraum der formalen Summen

$$\sum_{s \in S} \lambda_s s, \quad \lambda_s \in K, \text{ fast alle Null.}$$

Dies wird ein Vektorraum durch

$$\sum_{s \in S} \lambda_s s + \sum_{s \in S} \mu_s s = \sum_{s \in S} (\lambda_s + \mu_s) s, \qquad \lambda \sum_{s \in S} \lambda_s s = \sum_{s \in S} \lambda \lambda_s s.$$

Genauer kann man $K[S]$ auch als die Menge aller Abbildungen $S \to K$, $s \mapsto \lambda_s$ auffassen, die für fast alle s verschwinden.

Definition 4.4.2. Seien U, V, W Vektorräume über K. Eine Abbildung $b : V \times W \to U$ heißt **bilinear**, falls

- $v \mapsto b(v, w)$ ist linear für jedes feste $w \in W$ und
- $w \mapsto b(v, w)$ ist linear für jedes feste $v \in V$.

Wir schreiben $\mathrm{Bil}(V \times W, U)$ für den Vektorraum aller bilinearen Abbildungen $V \times W \to U$.

Beispiele 4.4.3. (a) Bilinearformen sind bilineare Abbildungen.

(b) Das Matrixprodukt $\mathrm{M}_{m \times n} \times \mathrm{M}_{n \times p} \to \mathrm{M}_{m \times p}$ ist bilinear.

(c) Die Kommutator-Klammer $[.,.] \mathrm{M}_n \to \mathrm{M}_n$, gegeben durch

$$[A, B] = AB - BA$$

ist bilinear.

Satz 4.4.4. *Zu gegebenen Vektorräumen V und W gibt es einen Vektorraum $V \otimes W$ und eine bilineare Abbildung $b_0 : V \times W \to V \otimes W$ mit der folgenden universellen Eigenschaft:*
Ist $b : V \times W \to U$ eine bilineare Abbildung, dann existiert genau eine lineare Abbildung $\phi_b : V \otimes W \to U$ so dass das Diagramm

$$\begin{array}{ccc} V \times W & \xrightarrow{b_0} & V \otimes W \\ & \searrow^{b} & \downarrow \exists! \, \phi_b \\ & & U \end{array}$$

kommutiert. Diese universelle Eigenschaft legt den Raum $V \otimes W$ und die universelle Bilinearform b_0 bis auf Isomorphie eindeutig fest.
Diese universelle Eigenschaft induziert einen linearen Isomorphismus

$$\mathrm{Bil}(V \times W, U) \xrightarrow{\cong} \mathrm{Hom}(V \otimes W, U).$$

Wir nennen den Raum $V \otimes W$ das **Tensorprodukt** *von V und W und schreiben $v \otimes w \in V \otimes W$ für das Element $b_0(v, w)$.*

Proof. Betrachte den Vektorraum $K[V \times W]$ und definiere den Unterraum M erzeugt von allen Elementen der Form

$$[(v + v', w)] - [(v, w)] - [(v', v)], \quad [(v, w + w')] - [(v, w)] - [(v, w')],$$
$$[(\lambda v, w)] - \lambda[(v, w)] \quad [(v, \lambda w)] - \lambda[(v, w)].$$

mit $v \in V$, $w \in W$ und $\lambda \in K$. Definiere dann

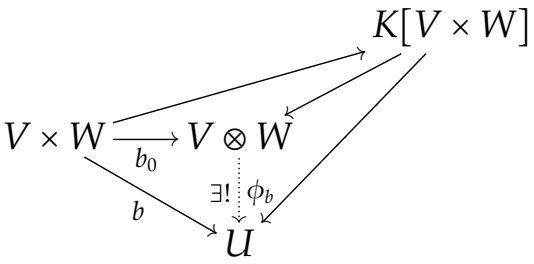
$$V \otimes W := K[V \times W]/M$$

Schreibe $v \otimes w$ für das Bild von (v, w) in $V \otimes W$. Die Abbildung $b_0 : V \times W \to V \otimes W$, $b(v, w) = v \otimes w$ ist erzwungenermaßen bilinear. Ist nun $b : V \times W \to U$ bilinear, dann definiere eine lineare Abbildung

$\tilde{\phi} : K[V \times W] \to U$ durch

$$\tilde{\phi}(v, w) = b(v, w).$$

Die Bilinearität von b impliziert, dass $\tilde{\phi}(M) = 0$, also faktorisiert $\tilde{\phi}$ über ein eindeutig bestimmtes $\phi_b : V \otimes W \to U$.



Die Kommutativität des Dreiecks links unten folgt aus der Surjektivitaet von $L[V \times W] \to V \otimes W$ und der Kommutativtät der undren beide Dreiecke. Die Eindeutigkeit von $V \otimes W$ geht wieder über Trick der universellen Eigenschaft. □

Definition 4.4.5. Die Elemente der Form $v \otimes w$ mit $v \in V$ und $w \in W$ heißen **reine Tensoren** oder auch **einfache Tensoren**.

Proposition 4.4.6. (a) *Ist $(e_i)_{i \in I}$ eine Basis von V, dann hat jeder Vektor von $x \in V \otimes W$ eine eindeutige Darstellung der Form*

$$x = \sum_{i \in I} e_i \otimes w_i$$

mit $w_i \in W$, fast alle Null.

(b) *Ist $(f_j)_{j \in J}$ eine Basis von W, dann ist $(e_i \otimes f_j)_{(i,j) \in I \times J}$ eine Basis von $V \otimes W$. Insbesondere folgt*

$$\dim(V \otimes W) = \big(\dim V\big)\big(\dim W\big).$$

Proof. (a) Jedes Element $x \in V \otimes W$ hat eine Darstellung der Form

$x = \sum_{k=1}^{n} v_k \otimes w_k$. Dann ist $v_k = \sum_{i \in I} \mu_i e_i$ und daher

$$x = \sum_{k=1}^{n} \left(\sum_{i \in I} \mu_i e_i \right) \otimes w_k = \sum_{i \in I} e_i \otimes \left(\sum_{k=1}^{n} \mu_i w_k \right).$$

Für die Eindeutigkeit gelte

$$\sum_{i \in I} e_i \otimes w_i = \sum_{i \in I} e_i \otimes w_i'.$$

Fixiere $i_0 \in I$ und betrachte die Bilinearform $b : V \times W \to W$ gegeben durch $b\left(\sum_{i \in I} \lambda_i e_i, w\right) = \lambda_{i_0} w$. Sei ϕ_b die entsprechende lineare Abbildung, dann folgt

$$w_{i_0} = \phi_b \left(\sum_{i \in I} e_i \otimes w_i \right) = \phi_b \left(\sum_{i \in I} e_i \otimes w_i' \right) = w_i'.$$

(b) folgt aus (a), denn jedes x hat eine eindeutige Darstellung $\sum_{i \in I} e_i \otimes v_i$ und jedes v_i hate eine eindeutige Darstellung $v_i = \sum_{j \in J} \lambda_{i,j} f_j$. □

Beispiele 4.4.7. (a) Wir können $\mathbb{C}$ als Vektorraum über $\mathbb{R}$ auffassen. Für einen beliebigen $\mathbb{R}$-Vektorraum V sei dann

$$V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V = \big(1 \otimes V\big) \oplus \big(i \otimes V\big) = V + iV.$$

Man nennt $V_{\mathbb{C}}$ die **Komplexifizierung** von V.

(b) Allgemeiner seien $L \supset K$ zwei Körper. Wir fassen L als K-Vektorraum auf und definieren

$$V_L = L \otimes_K V$$

für einen beliebigen K-Vektorraum V.

Satz 4.4.8. *Seien V, W endlich-dimensionale K-Vektorräume und sei V^**

der Dualraum von V. Die Abbildung

$$\psi : V^* \otimes W \to \mathrm{Hom}(V, W),$$
$$(\alpha, w) \mapsto [v \mapsto \alpha(v)w]$$

ist eine lineare Bijektion.

Beweis. Die Abbildung $V^* \times W \to \mathrm{Hom}(V, W)$, $(\alpha, w) \mapsto \psi(\alpha, w)$ ist bilinear, daher verlängert sie zu einer linearen Abbildung wie im Satz. Die Dimensionen der beiden Räume sind gleich, daher reicht es zu zeigen, dass die Abbildung ψ surjektiv ist. Seien $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$ Basen von V und W und sei $v_1^*, \ldots, v_n^*$ die duale Basis von V^*. Ist $T : V \to W$ in diesen Basen durch die Matrix $A = (a_{i,j})$ gegeben und ist $v = \sum_{j=1}^n \lambda_j v_j$ dann gilt

$$T\Big(\sum_{j=1}^n \lambda_j v_j\Big) = \sum_{j=1}^n \sum_{i=1}^m \lambda_j a_{i,j} w_i.$$

Nun ist $\lambda_j = v_j^*(v)$, also haben wir $T(v) = \sum_{j=1}^n \sum_{i=1}^m v_j^*(v) a_{i,j} w_i$ oder

$$T = \sum_{j=1}^n \sum_{i=1}^m a_{i,j} v_j^* w_i = \sum_{j=1}^n \sum_{i=1}^m a_{i,j} \psi(v_j^* \otimes w_j) = \psi\Big(\sum_{j=1}^n \sum_{i=1}^m a_{i,j} v_j^* \otimes w_j\Big). \qquad \square$$

Proposition 4.4.9. *Sind $S : V \to V'$ und $T : W \to W'$ lineare Abbildungen, so induzieren sie eine lineare Abbildung*

$$S \otimes T : V \otimes W \to V' \otimes W',$$

gegeben durch

$$(S \otimes T)(v \otimes w) = Sv \otimes Tw.$$

Beweis. Die Abbildung $b : V \times W \to V' \otimes W'$ gegeben durch $b(v, w) = Sv \otimes Tw$ ist bilinear, faktorisiert also eindeutig über eine lineare

Abbildung $V \otimes W \to V' \otimes W'$ die wir $S \otimes T$ nennen und die das Gewünschte leistet. □

Beispiel 4.4.10. Seien in der Proposition $V = W = V' = W' = K^2$. Seien S und T in der stundard Basis durch die Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ gegeben. In der Basis $e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2$ von $V \otimes W$ ist dann $S \otimes W$ durch die Matrix

$$\begin{pmatrix} a\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) & b\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \\ c\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) & d\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix}$$

gegeben.

Definition 4.4.11. Das **Kronecker Produkt** zweier Matrizen $A \in M_n(K)$ und $B \in M_m(K)$ ist die $nm \times nm$ Matrix definiert als $\begin{pmatrix} A_{11}B & \dots & A_{1,n}B \\ \vdots & & \vdots \\ A_{n,1}B & \dots & A_{n,n}B \end{pmatrix}$. Sie gibt die lineare Abbildung $A \otimes B$ wieder.

Satz 4.4.12. *Seien V, W endlich-dimensionale K-Vektorräume und $A, A' : V \to V$ und $B, B' : W \to W$ linear. Dann gilt*

$$(A \otimes B)(A' \otimes B') = AA' \otimes BB'$$

sowie

$$\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \operatorname{tr}(B)$$

und

$$\det(A \otimes B) = \det(A)^m \det(B)^n,$$

wobei $n = \dim V$ und $m = \dim W$.

Proof. Für $v \in V$ und $w \in W$ gilt

$$(A \otimes B)(A' \otimes B')(v \otimes w) = (A \otimes B)(A'v \otimes B'w) = AA'(v) \otimes BB'(w).$$

Damit stimmen die beiden Seiten für reine Tensoren überein und da beide Seiten lineare Abbildungen sind, stimmen sie überall überein. Die Formel für die Spur sieht man am Kronecker-Produkt und für die Determinante benutzt man
$\det(A \otimes B) = \det((A \otimes I)(I \otimes B)) = \det(A \otimes I)\det(I \otimes B)$. Man sieht etwa $\det(A \otimes I) = \det(A)^m$ wieder am Kronecker-Produkt. □

4.5 Die Tensorielle Algebra

Definition 4.5.1. Eine **Algebra** über dem Körper K ist ein K-Vektorraum A zusammen mit einer bilinearen Abbildung

$$A \times A \to A$$
$$(a, b) \mapsto ab,$$

die **assoziativ** ist, d.h., es gilt

$$(ab)c = a(bc)$$

für alle $a, b, c \in A$. Wir sagen, die Algebra A hat eine **Eins** oder ist eine **Algebra mit Eins**, oder eine **unitale Algebra**, falls es ein Element 1_A in A gibt mit der Eigenschaft

$$1_A a = a 1_A = a$$

für jedes $a \in A$. In dieser Vorlesung betrachten wir nur Algebren mit Eins! Deshalb gilt ab jetzt die **Sprachkonvention, dass Algebra immer Algebra mit Eins heissen soll. Andernfalls sprechen wir von einer Algebra ohne Eins.**

Das Einselement ist eindeutig bestimmt, denn ist $1'$ ein zweites Einselement, dann gilt

$$1' = 1'1_A = 1_A.$$

Beispiele 4.5.2. (a) Ist A irgendein K-Vektorraum, dann macht die Nullmultiplikation $ab = 0$ den Raum A zu einer Algebra ohne Eins!

(b) Der Körper K selbst ist eine K-Algebra.

(c) $\mathrm{M}_n(K)$ ist mit dem Matrixprodukt eine Algebra mit Eins.

(d) Ist V irgendein Vektorraum (auch unendlich-dimensional), dann ist die Menge

$$\mathrm{End}(V) = \mathrm{Hom}(V, V)$$

eine Algebra mit der Komposition als Multiplikation.

(e) Ist S eine Menge und ist $A = \mathrm{Abb}(S, K)$ der Vektorraum aller Abbildungen von S nach K. Dann ist A eine Algebra mit dem punktweisen Produkt:

$$fg(s) = f(s)g(s), \qquad s \in S.$$

(f) Über dem Körper $\mathbb{R}$ der reellen Zahlen betrachtet man die **Quaternionenalgebra** $\mathcal{H}$, dies ist ein vierdimensionaler $\mathbb{R}$-Vektorraum mit einer Basis $\mathbf{1}, i, j, k$. Die Relationen

$$\mathbf{1}x = x\mathbf{1} = x \qquad i^2 = j^2 = -1 \qquad ij = k = -ji$$

definieren eine Algebrenstruktur auf $\mathcal{H}$. Dies ist eine Algebra mit Eins. Diese Algebra ist nichtkommutativ, aber dennoch ist jedes Element $\neq 0$ invertierbar, es hundelt sich also um einen sogenannten **Schiefkörper**.

Beweis. Die Tatsache, dass $\mathcal{H}$ in der Tat die Axiome einer Algebra erfüllt, muss man nachrechnen. Bei der Assoziativität reicht es,

diese auf den Basiselementen nachzuweisen. Wir zeigen, dass jedes Element $\neq 0$ invertierbar ist. Zunächst stellen wir fest, dass

$$ik = iij = -j \quad \text{und} \quad ki = iji = -iij = j$$

gilt und ebenso $jk = i = -kj$. Für ein Quaternion $z = a + bi + cj + dk$ sei $\overline{z} = a - bi - cj - dk$ definiert. Es folgt

$$\begin{aligned} z\overline{z} &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + abi + b^2 - bck + bdj \\ &\quad + acj + bck + c^2 - cdi + adk - bdj + cdi \\ &= a^2 + b^2 + c^2 + d^2. \end{aligned}$$

Ist $z \neq 0$, dann ist $a^2 + b^2 + c^2 + d^2 \neq 0$ und also ist dann

$$\frac{1}{a^2 + b^2 + c^2 + d^2}\overline{z}$$

ein Inverses zu z. □

Definition 4.5.3. Sind A, B Algebren über einem Körper K, dann ist ein **Algebrenhomomorphismus** von A nach B eine lineare Abbildung $\phi : A \to B$, für die

$$\phi(ab) = \phi(a)\phi(b) \quad \text{und} \quad \phi(1) = 1$$

gilt. Das heißt also, ein K-linearer Ringhomomorphismus.

Beispiele 4.5.4. (a) Der Algebrenhomomorphismus $\mathrm{M}_n(K) \to \mathrm{M}_{2n}(K)$, $A \mapsto \begin{pmatrix} A & \\ & A \end{pmatrix}$.

(b) Ist $S \neq \varnothing$ eine Menge und $\mathcal{A} = \mathrm{Abb}(S, K)$ die Algebra aller Abbildungen von S nach K mit punktweiser Addition und Multiplikation. Sei $s_0 \in S$, dann ist die Abbildung $\phi : \mathcal{A} \to K$, $f \mapsto f(s_0)$ ein Algebrenhomomorphismus.

Lemma 4.5.5. *Sei $\phi : \mathcal{A} \to \mathcal{B}$ ein Algebrenhomomorphismus. Ist ϕ bijektiv, so*

ist die Umkehrabbildung $\phi^{-1} : \mathcal{B} \to \mathcal{A}$ ebenfalls ein Algebrenhomomorphismus. In diesem Fall heisst ϕ ein **Algebrenisomorphismus**.

Beweis. Wir wissen bereits, dass ϕ^{-1} linear ist. Seien also $b, b' \in \mathcal{B}$, so gilt

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

Da ϕ injektiv ist, folgt

$$\phi^{-1}(bb') = \phi^{-1}(b)\phi^{-1}(b'),$$

also ist ϕ^{-1} ein Algebrenhomomorphismus. Aus $\phi(1) = 1$, folgt durch Anwenden von ϕ^{-1} auch $\phi^{-1}(1) = 1$. Die Umkehrung folgt durch Vertauschung der Rollen von ϕ und ϕ^{-1}. □

Ist I eine Indexmenge und ist für jedes $i \in I$ ein K-Vektorraum V_i gegeben, so ist

$$V = \prod_{i \in I} V_i$$

ein K-Vektorraum, wobei die Addition und die skalare Multiplikation komponentenweise erklaert sind. Wir betrachten den Unterraum

$$\bigoplus_{i \in I} V_i := \left\{ v \in \prod_{i \in I} V_i : v_i = 0 \text{ für fast alle } i \right\}.$$

Man macht sich leicht klar, dass dies in der Tat ein Unterraum ist und dass für endliche Indexmengen diese Notation mit der bisherigen $\oplus$-Notation für Unterraeume kompatibel ist, wenn man jedes V_j als Teilraum von $V = \prod_{i \in I} V_i$ auffasst. Es ist der Teilraum der Elemente des Produktes, die nur an der j-Koordinate einen Eintrag ungleich Null haben duerfen.

Sei nun V ein K-Vektorraum und sei

$$\begin{aligned} T(V) &= K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V \otimes V) \oplus \dots \\ &= \bigoplus_{n=0}^{\infty} V^{\otimes n}, \end{aligned}$$

wobei $V^{\otimes 0} = K$ und

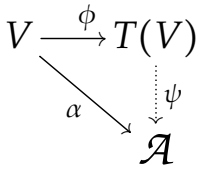
$$V^{\otimes n} = \underbrace{V \otimes V \otimes \cdots \otimes V}_{n \text{ mal}}$$

für $n \geq 1$ ist. Die Vorschrift

$$\big(v_1 \otimes \cdots \otimes v_n\big)\big(w_1 \otimes \cdots \otimes w_m\big) = v_1 \otimes \cdots \otimes v_n \otimes w_1 \otimes \cdots \otimes w_m$$

macht $T(V)$ zu einer Algebra, die man die **tensorielle Algebra** von V nennt.

Satz 4.5.6 (Universelle Eigenschaft der tensoriellen Algebra)**.** *Sei V ein K-Vektorraum, $\phi = \phi_V : V \to T(V)$ die Abbildung, die V auf die erste Tensorpotenz schickt. Dann hat ϕ folgende universelle Eigenschaft:*
Für jede K-Algebra $\mathcal{A}$ und jede lineare Abbildung $\alpha : V \to \mathcal{A}$ existiert genau ein Algebrenhomomorphismus $\psi : T(V) \to \mathcal{A}$, der α fortsetzt, d.h., so, dass das Diagramm



kommutiert.

Beweis. Sei eine lineare Abbildung $\alpha : V \to \mathcal{A}$ in die Algebra $\mathcal{A}$ gegeben. Wir definieren eine lineare Abbildung $\psi : T(V) \to \mathcal{A}$ durch $\psi(1) = 1$ und

$$\psi(v_1 \otimes \cdots \otimes v_n) = \alpha(v_1)\alpha(v_2)\cdots\alpha(v_n),$$

wobei rechts das Produkt in $\mathcal{A}$ genommen wird. Nach Definition ist ψ multiplikativ auf den Basiselementen, damit aber auch schon insgesamt

multiplikativ. Nach Konstruktion gilt $\psi(\phi(v)) = \alpha(v)$ und damit kommutiert das Diagramm. Sei nun ψ' ein weiterer Algebrenhomomorphismus, für den das Diagramm kommutiert, dann gilt

$$\psi'(v_1 \otimes \cdots \otimes v_n) = \psi'(v_1) \cdots \psi'(v_n) = \alpha(v_1) \cdots \alpha(v_n) = \psi(v_n \otimes \cdots \otimes v_n)$$

und damit $\psi' = \psi$. □

Bemerkung 4.5.7. Sei $\phi : \mathcal{A} \to \mathcal{B}$ ein Algebrenhomomorphismus und sei $I = \ker(\phi)$ der Kern. Dann gilt

- I ist ein Untervektorraum von $\mathcal{A}$ und
- $IA \subset I$ und $AI \subset I$, wobei

$$IA = \text{Spann}\left\{ya : y \in I,\ a \in \mathcal{A}\right\}$$

geschrieben wurde.

Die zweite Eigenschaft schreibt man auch so

$$y \in I, a \in \mathcal{A} \quad \Rightarrow \quad ay, ya \in I.$$

Eine Teilmenge $I \subset \mathcal{A}$ mit diesen beiden Eigenschaften nennt man ein **(zweiseitiges) Ideal** von $\mathcal{A}$.

Beispiel 4.5.8. Ist $M \subset \mathcal{A}$ eine Teilmenge, dann ist der Untervektorraum

$$I = \mathcal{A}M\mathcal{A} = \text{Spann}\left\{amb : a, b \in \mathcal{A},\ m \in M\right\}$$

ein Ideal. Dies ist das kleinste Ideal, das M enthaelt, man nennt es das von M **erzeugte Ideal**.

Beweis. Ist M leer, so ist I das Nullideal. Sei also $M \neq \varnothing$. Die Menge $\mathcal{A}M\mathcal{A}$ ist nach Definition ein Untervektorraum. Ist nun $y \in I$ und $a \in \mathcal{A}$,

dann kann man y schreiben als

$$y = \sum_{j=1}^{n} a_j m_j b_j$$

mit $b_j, b_j \in \mathcal{A}$ und $m_j \in M$. Also sind $ay = \sum_{j=1}^{n} a a_j m_j b_j$ und $ya = \sum_{j=1}^{n} a_j m_j b_j a$ wieder in I. □

Satz 4.5.9. *Ein Unterraum I einer Algebra $\mathcal{A}$ ist genau dann ein Ideal, wenn der Quotientenraum $\mathcal{A}/I$ eine Algebrenstruktur traegt, so dass die Projektion $P : \mathcal{A} \to \mathcal{A}/I$ ein Algebrenhomomorphismus ist. Diese Algebrenstruktur ist dann eindeutig bestimmt.*

Beweis. Sei I ein Ideal. Wir definieren eine Multiplikation auf dem Quotientenraum $\mathcal{A}/I$ durch

$$(a + I)(b + I) = ab + I.$$

Hier ist die Wohldefiniertheit zu pruefen. Seien also $a', b' \in \mathcal{A}$ mit $a + I = a' + I$ und $b' + I = b + I$, das heisst $a - a' \in I$ und $b - b' \in I$. Dann gilt

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= \underbrace{(a - a')}_{\in I} b + a' \underbrace{(b - b')}_{\in I} \in I, \end{aligned}$$

also $ab + I = a'b' + I$, d.h., die Multiplikation ist wohldefiniert. Wegen der Surjektivität der Projektion $P : \mathcal{A} \to \mathcal{A}/I$ ist diese Multiplikation eindeutig festgelegt. □

Satz 4.5.10 (Homomorphiesatz). *Ist $\phi : \mathcal{A} \to \mathcal{B}$ ein Algebrenhomomorphismus, dann ist das Bild eine Unteralgebra von $\mathcal{B}$ und es gilt*

$$\text{Bild}(\phi) \cong \mathcal{A}/\ker(\phi),$$

wobei eine Isomorphie als Algebren gemeint ist.

Beweis. Der Kern $\ker(\phi)$ ist ein Ideal, so dass die Algebra $\mathcal{A}/\ker(\phi)$ wohldefiniert ist. Die besagte Isomorphie ist uns als eine Isomorphie von Vektorraeumen bereits bekannt. Sie ist durch ϕ induziert und da ψ ein Algebrenhomomorphismus ist, ist die Isomorphie auch einer. □

Beispiele 4.5.11. (a) Sei S eine Menge und $\mathcal{A} = \text{Abb}(S, K)$, sowie $T \subset S$ eine Teilmenge und sei

$$I = \{f \in \mathcal{A} : f|_T = 0\}.$$

Dann ist T ein Ideal und $\mathcal{A}/I \cong \text{Abb}(T, K)$.

(b) Sind $\mathcal{A}$ und $\mathcal{B}$ Algebren, so ist auch $\mathcal{A} \times \mathcal{B}$ eine Algebra mit der komponentenweisen Multiplikation, also

$$(a, b)(a', b') = (aa', bb').$$

Die Projektion $P : \mathcal{A} \times \mathcal{B} \to \mathcal{A}$ ist ein Algebrenhomomorphismus mit Kern

$$I = \{0\} \times \mathcal{B}.$$

(c) Sei $1 \le k \le n$ und sei $\mathcal{A}$ die Menge aller Matrizen in $\text{M}_n(K)$ der Gestalt $\left(\begin{smallmatrix} A & B \\ D \end{smallmatrix}\right)$, also der untere linke $(n-k) \times k$-Block ist Null. Dann ist $\mathcal{A}$ eine Unteralgebra mit Eins von $\text{M}_n(K)$ und die Abbildung $\mathcal{A} \to \text{M}_k(K)$, $\left(\begin{smallmatrix} A & B \\ D \end{smallmatrix}\right) \mapsto A$ ist ein Algebrenhomomorphismus dessen Kern das Ideal I aller Matrizen der Form $\left(\begin{smallmatrix} 0 & B \\ D \end{smallmatrix}\right)$ ist.

Satz 4.5.12. *Jede Algebra $\mathcal{A}$ mit Eins ist Quotient einer tensoriellen Algebra, d.h. es gibt einen Vektorraum V und ein Ideal I von $T(V)$ so dass $\mathcal{A} \cong T(V)/I$.*

Beweis. Als Vektorraum kann man $V = \mathcal{A}$ selbst nehmen. Die lineare Abbildung $\mathcal{A} \to \mathcal{A}$, die durch die Identitaet gegeben ist, induziert nach der universellen Eigenschaft einen Algebrenhomomorphismus $\psi : T(V) \to \mathcal{A}$, der surjektiv ist, weil die Einschraenkung nach $V \cong \mathcal{A}$ schon surjektiv ist. Sei $I = \ker(\psi)$, so folgt $\mathcal{A} \cong T(V)/I$. □

4.6 Die äußere Algebra

Definition 4.6.1. Sei V ein K-Vektorraum. Die **äußere Algebra** $\bigwedge^* V$ ist definiert als

$$\bigwedge^* V = T(V)/\langle v \otimes v : v \in V \rangle$$

Man schreibt das Bild von $v \otimes w$ als $v \wedge w$. Es gilt dann

$$v \wedge w = -w \wedge v,$$

denn

$$0 = (v+w) \wedge (v+w) = v \wedge v + v \wedge w + w \wedge v + w \wedge w = v \wedge w + w \wedge v.$$

Die äußere Algebra ist ein Quotient der tensoriellen Algebra, es gibt also einen surjektiven Algebrenhomomorphismus

$$\phi : T(V) \to \bigwedge^* V.$$

Der Kern von ϕ ist das zweiseitige Ideal erzeugt von allen Elementen der Form $v \otimes v$ für $v \in V$.

Beispiele 4.6.2. (a)

(b) Sei $V = \mathbb{R}v_0$ ein eindimensionaler $\mathbb{R}$-Vektorraum. Man kann $\mathbb{C}$ als Quotienten der $\mathbb{R}$-Algebra $T(V)$ schreiben. Der Kern ist das Ideal erzeugt von $v_0 \otimes v_0 + 1$.

Satz 4.6.3. *Ist $v_1, \ldots, v_n$ eine Basis von V, dann ist*

$$(v_{i_1} \wedge \cdots \wedge v_{i_k})_{1 \le i_1 < \cdots < i_k \le n}$$

eine Basis von $\bigwedge^k V$. Insbesondere ist

$$\dim \bigwedge^k V = \binom{n}{k}$$

und damit insbesondere $\bigwedge^k V = 0$ falls $k > n$ und $\dim \bigwedge^\bullet V = 2^n$.

Beweis. Da die Tensoren $v_{i_1} \otimes \cdots \otimes v_{i_k}$ den Raum $V^{\otimes k}$ aufspannen, bilden die genannten Vektoren ein Erzeugersystem. Es reicht also, die Dimensionsaussage zu zeigen. Für $n = 0$ ist die Behauptung klar. Sei sie also für n bewiesen. Sei $W = V \oplus Kw_0$ mit einem neuen Vektor w_0. Dann ist $\bigwedge W = (\bigwedge V) \oplus (\bigwedge V \wedge w_0)$, woraus die Behauptung folgt. □

Beispiele 4.6.4. (a) Sei $V = K$, dann hat $\bigwedge V$ die Basis $1, e$ und die Multiplikation ist gegeben durch $e^2 = 0$.

(b) Sei $V = K^2$. Dann hat $\bigwedge V$ die Basis $1, e_1, e_2, e_1 \wedge e_2$.

(c) Sei $V = K^3$. Dann hat $\bigwedge V$ die Basis
$1, e_1, e_2, e_3, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3$.

4.7 Die symmetrische Algebra

Sei V ein K-Vektorraum und sei I das Ideal von $T(V)$ erzeugt von der Teilmenge

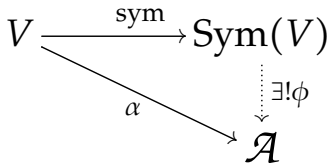
$$M = \{v \otimes w - w \otimes v : v, w \in V\}.$$

Sei

$$\mathrm{Sym}(V) = T(V)/I.$$

Man nennt $\mathrm{Sym}(V)$ die **symmetrische Algebra** über V. Man schreibt das Bild von $v_1 \otimes \cdots \otimes v_n$ in $\mathrm{Sym}(V)$ als $v_1 \cdots v_n$.

Satz 4.7.1. *Die Algebra* $\mathrm{Sym}(V)$ *ist kommutativ. Die kanonische Abbildung* $\mathrm{sym} : V \to \mathrm{Sym}(V)$ *ist injektiv.* $\mathrm{Sym}(V)$ *ist die universelle kommutative Algebra mit einer linearen Abbildung von* V*, genauer heisst das: Ist* $\alpha : V \to \mathcal{A}$ *eine lineare Abbildung in eine kommutative Algebra, so existiert genau ein Algebrenhomomorphismus* $\phi : \mathrm{Sym}(V) \to \mathcal{A}$ *der das Diagramm*



kommutativ macht.

Beweis. Der kanonische Algebrenhomomorphismus $T(V) \to \mathcal{A}$ über den α faktorisiert, annulliert das Ideal I, da $\mathcal{A}$ kommutativ ist. Daher existiert genau ein ϕ, welches das Diagramm kommutativ macht. □

Satz 4.7.2. *Sei* $V \neq 0$ *endlich-dimensional, dann ist die Algebra* $\mathrm{Sym}(V)$ *unendlich-dimensional. Sie kann geschrieben werden als*

$$\mathrm{Sym}(V) = \bigoplus_{j=0}^{\infty} \mathrm{Sym}_j(V),$$

wobei $\mathrm{Sym}_j(V)$ *das Bild von* $V^{\otimes n}$ *ist. Es gilt*

$$\mathrm{Sym}_k(V)\,\mathrm{Sym}_j(V) \subset \mathrm{Sym}_{k+j}(V).$$

Ist $e_1, \ldots, e_n$ *eine Basis von* V*, dann ist*

$$\left(e_1^{p_1} \cdots e_n^{p_n}\right)_{p_1+\cdots+p_n=j}$$

eine Basis von $\mathrm{Sym}_j(V)$*, wobei die* p_j *in* $\mathbb{N}_0$ *liegen. In diesem Fall definiert die Vorschrift*

$$\mathrm{Sym}(V) \to K[X_1, \ldots, X_n],$$
$$e_j \mapsto X_j$$

einen Algebrenisomorphismus.

Beweis. Schreibe $\mathrm{Sym}(V) = T(V)/I$ wie oben. Dann wird $\mathrm{Sym}(V)$ von den Elementen der Form $v_1 \cdots v_n$, genannt **Monome**, aufgespannt, da $T(V)$ von den reinen Tensoren aufgespannt wird. Dann ist $\mathrm{Sym}_j(V)$ der Spann der Monome der Laenge j und $\mathrm{Sym}(V)$ ist die Summe aller $\mathrm{Sym}_j(V)$. Es ist zu zeigen, dass $\mathrm{Sym}_j \cap \mathrm{Sym}_k = 0$ für $k \neq j$ gilt. Dies folgt allerdings automatisch, wenn wir die Aussage über die Basis zeigen. Es ist nun

$$v_1 \otimes \cdots \otimes v_k \otimes v_{k+1} \otimes \cdots \otimes v_m - v_1 \otimes \cdots \otimes v_{k+1} \otimes v_{k+} \otimes \cdots \otimes v_m$$

in I, hier wurden zwei aufeinunderfolgende Faktoren vertauscht. Das bedeutet, dass man in $\mathrm{Sym}(V)$ in einem Monom $v_1 \cdots v_m$ ebenfalls zwei aufeinunderfolgende Faktoren vertauschen kann. Ist nun $e_1, \ldots, e_n$ eine Basis von V, dann kann man in einem gegebenen Monom $v_1 \cdots v_m$ jdes v_j in der Basis entwickeln und alles ausdistribuieren, so dieht man , dass $\mathrm{Sym}(V)$ von den Monomen der Gestalt $e_{i_1} \cdots e_{i_m}$ erzeugt wird. Indem

man benachbarte Faktoren vertauscht, kann man ein solches Monom immer in die Form $e_1^{p_1} \cdots e_n^{p_n}$ bringen, so dass die behauptete Basis schon einmal ein Erzeugendensystem ist. Um die lineare Unabhängigkeit zu zeigen betrachten wir die lineare Abbildung $\alpha : V \to K[x_1, \ldots, x_n]$ definiert durch $\alpha(e_j) = x_j$, so induziert diese nach der universellen Eigenschaft einen Algebrenhomomorphismus $\phi : \mathrm{Sym}(V) \to K[x_1, \ldots, x_n]$ dessen Bild von $x_1, \ldots, x_n$ erzeugt wird, der also surjektiv ist. Da die Monome der Form $e_1^{p_1} \cdots e_n^{p_n}$ gerade auf die Monome im Polynomring abgebildet werden, die bekanntermaßen eine Basis von $K[x_1, \ldots, x_n]$ bilden, ist ϕ ein Algebrenisomorphismus und die Monome eine Basis von $\mathrm{Sym}(V)$ wie behauptet. □

4.8 Multilineare Abbildungen

Seien $V_1, \ldots, V_k, W$ Vektorräume über K. Eine Abbildung

$$m : V_1 \times \cdots \times V_k \to W$$

heißt **multilinear**, falls für jedes $1 \leq j \leq n$ und für fest gewählte Vektoren $v_i \in V$ für $i \neq j$ die Abbildung

$$v \mapsto m(v_1, \ldots, v_{j-1}, v, v_{j+1}, \ldots, v_n)$$

linear ist.

Beispiele 4.8.1. (a) Sei $V = K^n$, dann ist die Determinante

$$\det : V \times \cdots \times V \to K$$

eine multilineare Abbildung.

(b) Die Abbildung

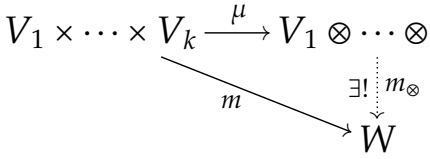
$$V_1 \times \cdots \times V_k \to V_1 \otimes V_2 \otimes \cdots \otimes V_k$$
$$(v_1, \ldots, v_k) \mapsto v_1 \otimes \cdots \otimes v_k$$

ist multilinear.

Satz 4.8.2. *Seien $V_1, \ldots, V_k, W$ Vektorräume. Zu jeder multilinearen Abbildung*

$$m : V_1 \times \cdots \times V_k \to W$$

gibt es genau eine lineare Abbildung $m_\otimes : V_1 \otimes \cdots \otimes V_k \to W$, so dass das Diagramm



kommutiert. Die Abbildung $m \mapsto m_\otimes$ ist eine lineare Bijektion

$$\mathrm{Mult}_k(V_1 \times \cdots \times V_k, W) \xrightarrow{\cong} \mathrm{Hom}(V_1 \otimes \cdots \otimes V_k, W).$$

Beweis. Man wiederholt die Konstruktion aus dem Produkt zweier Räume. □

Definition 4.8.3. Eine multilineare Abbildung $m : V^k \to U$ heißt **symmetrisch**, falls

$$m(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = m(v_1, \ldots, v_k)$$

für jede Permutation $\sigma \in \mathrm{Per}(n)$ gilt.

Sie heißt **alternierend**, wenn

$$m(v_1, \ldots, v_k) = 0,$$

falls $v_i = v_j$ für ein i und ein $j \neq i$.

Lemma 4.8.4. *Ist m alternierend, dann gilt*

$$m(v_{\sigma(1)},\dots,v_{\sigma(k)}) = \operatorname{sign}(\sigma) m(v_1,\dots,v_k) \qquad (*)$$

für jede Permutation $\sigma \in \mathrm{Per}(n)$. Ist $\mathrm{Char}(K) \neq 2$, so folgt aus (*) für alle σ schon, dass m alternierend ist.

Beweis. Ist $\sigma = \tau_{i,j}$ eine Transposition so gilt

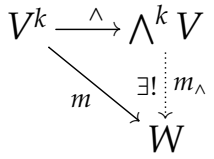
$$\begin{aligned} 0 &= m(v_1,\dots,\underbrace{v_i+v_j}_{i\text{–te Stelle}},\dots,\underbrace{v_i+v_j}_{j\text{–te Stelle}},\dots,v_k) \\ &= m(v_1,\dots,v_i,\dots,v_j,\dots,v_k) + m(v_1,\dots,v_j,\dots,v_i,\dots,v_k). \end{aligned}$$

Damit folgt die Behauptung falls σ eine Transposition ist. Für die allgemeine Aussage schreibt man σ als Produkt von Transpositionen und zieht bei jeder Transposition einen Faktor (-1) heraus. □

Beispiele 4.8.5. (a) Ist $V = K^n$, so ist die Determinante $\det : V^n \to K$ alternierend.

(b) Ist $V = K$, so ist die Abbildung $m : V^k \to K$, gegeben durch $m(a_1,\dots,a_k) = a_1 \cdots a_k$ symmetrisch.

Satz 4.8.6. *Zu jeder alternierenden Abbildung $m : V^k \to W$ existiert eine eindeutig bestimmte lineare Abbildung $m_\wedge : \bigwedge^k V \to W$, so dass das Diagramm*



kommutiert. Die Abbildung $m \mapsto m_\wedge$ ist ein linearer Isomorphismus

$$\mathrm{Alt}_k(V^k, W) \xrightarrow{\cong} \mathrm{Hom}(\textstyle\bigwedge^k V, W).$$

Beweis. Analog zum Beweis von Satz 4.7.2. □

4.9 Lineare Abbildungen

Sei $T : V \to V$ linear. Die Abbildung

$$m : V^k \to \bigwedge^k V$$
$$(v_1, \ldots, v_k) \mapsto Tv_1 \wedge \cdots \wedge Tv_k$$

ist alternierend. Nach der universellen Eigenschaft existiert eine lineare Abbildung

$$\bigwedge^k T : \bigwedge^k V \to \bigwedge^k V,$$

so dass

$$\bigwedge^k T(v_1 \wedge \cdots \wedge v_k) = Tv_1 \wedge \cdots \wedge Tv_k.$$

Beispiel 4.9.1. Sei die lineare Abbildung $A : K^3 \to K^3$ durch die Matrix

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}$$

gegeben. Wir bestimmen die Matrix von $\bigwedge^2 A$ in der Basis $e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3$. Wir rechnen

$$\begin{aligned} \bigwedge^2 A(e_1 \wedge e_2) &= (Ae_1) \wedge (Ae_2) \\ &= (ae_1 + de_2 + ge_3) \wedge (be_1 + ee_2 + he_3) \\ &= (ae - bd)e_1 \wedge e_2 + (ah - bg)e_1 \wedge e_3 + (dh - eg)e_2 \wedge e_3. \end{aligned}$$

Ebenso rechnet man die underen Terme durch und erhält am Ende die Matrix

$$\begin{pmatrix} \det\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} a & c \\ d & f \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} b & c \\ e & f \end{smallmatrix}\right) \\ \det\left(\begin{smallmatrix} a & b \\ g & h \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} a & c \\ g & j \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} b & c \\ h & j \end{smallmatrix}\right) \\ \det\left(\begin{smallmatrix} d & e \\ g & h \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} d & f \\ g & j \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} e & f \\ h & j \end{smallmatrix}\right) \end{pmatrix}.$$

Satz 4.9.2. *Ist* $\dim V = n$ *und* $T : V \to V$ *linear, so gilt*

$$\bigwedge^n T = \det(T)\mathrm{Id}.$$

Beweis. Sei $v_1 \dots v_n$ eine Basis von V. Der eindimensionale Raum $\bigwedge^n V$ wird von $v_1 \wedge \cdots \wedge v_n$ aufgespannt. Sei $(a_{i,j})$ die Matrix von T, d.h.

$$Tv_j = \sum_{i=1}^{n} a_{i,j} v_i.$$

es folgt

$$\begin{aligned}
\bigwedge^n T(v_1 \wedge \cdots \wedge v_n) &= Tv_1 \wedge \cdots \wedge Tv_n \\
&= \sum_{i_1 \dots i_n = 1}^{n} a_{i_1,1} \cdots a_{i_n,n} v_{i_1} \wedge \cdots \wedge v_{i_n} \\
&= \sum_{\sigma \in \mathrm{Per}(n)} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \underbrace{v_{\sigma(1)} \wedge \cdots \wedge V_{\sigma(n)}}_{= \mathrm{sign}(\sigma) v_1 \wedge \cdots \wedge v_n} \\
&= \det(T)\, v_1 \wedge \cdots \wedge v_n.
\end{aligned}$$

□

Lemma 4.9.3. (a) *Fuer lineare Abbildungen* $A, B : V \to V$ *gilt*

$$\bigwedge^k (AB) = \Big(\bigwedge^k A\Big)\Big(\bigwedge^k B\Big).$$

Insbesondere Folgt $\bigwedge^k (S^{-1}) = \bigwedge^k (S)^{-1}$ *und* $\mathrm{tr}(\bigwedge^k (STS^{-1}) = \mathrm{tr} \bigwedge^k (T)$.

(b) *Ist* $A = D + N$ *eine obere Dreiecksmatrix, wobei* D *diagonal ist und* N *nur Nullen auf der Diagonale hat. Dann gilt*

$$\mathrm{tr} \bigwedge^k (A) = \mathrm{tr} \bigwedge^k (D).$$

Beweis. (a) Fuer beliebige $v_1, \dots, v_k \in V$ gilt

$$\begin{aligned}\bigwedge^j(AB)v_1 \wedge \cdots \wedge v_k &= \big(ABv_1\big) \wedge \cdots \wedge \big(ABv_k\big) \\ &= \bigwedge^j(A)\big(Bv_1\big) \wedge \cdots \wedge \big(Bv_j\big) \\ &= \bigwedge^k(A) \bigwedge^k(B) v_1 \wedge \cdots \wedge v_k.\end{aligned}$$

Damit gilt auch $\bigwedge^k(S) \bigwedge^k(S^{-1}) = \bigwedge^k(I) = I$.

(b) Sei $e_1, \dots, e_n$ die Standard-Basis und sei $\mathcal{B}$ die Basis von $\bigwedge^k V$, die aus den Vektoren $e_{i_1} \wedge \cdots \wedge e_{i_k}$ mit $i_1 < i_2 < \cdots < i_k$ besteht. Definiere

$$F\big(e_{i_1} \wedge \cdots \wedge e_{i_k}\big) = 2^{i_1} + \cdots + 2^{i_k} \in \mathbb{N}.$$

Die Funktion $F : \mathcal{B} \to \mathbb{N}$ ist injektiv. Alle Elemente von $\mathcal{B}$ sind Eigenvektoren von D und es gilt

$$\begin{aligned}\bigwedge^k(D+N)e_{i_1} \wedge \cdots \wedge e_{i_k} &= \bigwedge^k(D)e_{i_1} \wedge \cdots \wedge e_{i_k} + \tilde{N}e_{i_1} \wedge \cdots \wedge e_{i_k} \\ &= \bigwedge^k(D)e_{i_1} \wedge \cdots \wedge e_{i_k} + \sum_{(R_1,\dots,R_k)} R_1 e_{i_1} \wedge \cdots \wedge R_k e_{i_k}\end{aligned}$$

wobei die Summe ueber verschiedene Tupel $(R_1, \dots, R_k)$ laeuft, wobei jedes R_k gleich D oder N ist, wobei bei jedem Summanden mindestens ein R_k gleich N ist. Wir setzen $F(\lambda b) = F(b)$, falls $0 \neq \lambda \in K$ und $b \in \mathcal{B}$. Ist $N(e_i) \neq 0$, dann ist $N(e_i) = e_{i-1}$ und daher folgt $F(R_1 e_{i_1} \wedge \cdots \wedge R_k e_{i_j}) < F(e_{i_1} \wedge \cdots \wedge e_{i_k})$. Ist $\mathcal{F}_n = F^{-1}(\{1, 2, \dots, n\})$ dann folgt $\tilde{N}(\mathcal{F}_n) \subset \mathcal{F}_{n-1}$. Das bedeutet, dass $\tilde{N}$ ind er Basis $\mathcal{B}$ durch eine obere Dreiecksmatrix mit Nullen auf der Diagonale gegeben ist. Da $\bigwedge^k D$ gleichzeitig durch eine Diagonalmatrix gegeben ist, folgt die Behauptung. □

Satz 4.9.4. *Ist* $\dim V = n$ *und* $T : V \to V$ *linear, so gilt*

$$\det(1 - T) = \sum_{k=0}^{n} (-1)^k \operatorname{tr} \bigwedge^k T.$$

Beweis. Beide Seiten der Gleichung aendern sich nicht, wenn wir den Körper K durch einen algebraischen Abschluss ersetzen, wir koennen also den Körper als algebraisch abgeschlossen annehmen. Da beide Seiten der Gleichung sich nicht aendern, wenn man T durch eine konjugierte ersetzt, kann man annehmen, dass T in Jordan-Normalform ist, also $T = D + N$, wobei D eine Diagonalmatrix ist. Es gilt dann $\det(1 - T) = \det(1 - D - N) = \det(1 - D)$. Nach dem Lemma ist $\operatorname{tr} \bigwedge^k T = \operatorname{tr} \bigwedge^k (D + N) = \operatorname{tr} \bigwedge^k D$.

Insgesamt kann man also T durch D ersetzen und annehmen, dass T eine Diagonalmatrix ist. Diese habe die Diagonaleinträge $\lambda_1, \ldots, \lambda_n$. Dann ist

$$\begin{aligned} \det(1 - T) = (1 - \lambda_1) \cdots (1 - \lambda_n) &= \sum_{k=0}^{n} \sum_{1 \le i_1 < \cdots < i_k \le n} (-1)^k \lambda_{i_1} \cdots \lambda_{i_k} \\ &= \sum_{k=0}^{n} (-1)^k \operatorname{tr} \bigwedge^k T. \end{aligned}$$

□

5 Kategorien

5.1 Kategorien

Definition 5.1.1. Eine **Kategorie** ist ein Tripel $(\mathrm{Ob}, \mathrm{Hom}, \circ)$, wobei Ob eine Klasse ist, deren Elemente Objekte der Kategorie genannt werden. Hom ist eine Familie von Mengen $(\mathrm{Hom}(X, Y))_{X,Y \in \mathrm{Ob}}$. Die Elemente von $\mathrm{Hom}(X, Y)$ heißen **Morphismen** oder **Pfeile** von X nach Y. Schließlich

ist $\circ$, die **Komposition** eine Familie von Abbildungen: fuer je drei Objekte X, Y, Z:

$$\begin{aligned} \mathrm{Hom}(X,Y) \times \mathrm{Hom}(Y,Z) &\to \mathrm{Hom}(X,Z) \\ (f,g) &\mapsto g \circ f, \end{aligned}$$

so dass

- $g \circ (f \circ h) = (g \circ f) \circ h$ wenn die Pfeile komponierbar sind.
- Fuer jedes Objekt X gibt es einen Pfeil $\mathbf{1}_X \in \mathrm{Hom}(X,X)$ mit $f \circ \mathbf{1}_X = f$ und $\mathbf{1}_X \circ g = g$ fuerr alle f, g, fuer die die jeweilige Komposition existiert.

Bemerkung 5.1.2. (a) Der **Einsmorphismus** $\mathbf{1}_X$ ist eindeutig bestimmt, denn, sei $\mathbf{1}'_X$ ein weiterer, dann gilt

$$\mathbf{1}_X = \mathbf{1}_X \mathbf{1}'_X = \mathbf{1}'_X.$$

(b) Wie bei Abbildungen aendert die Komposition die Reihenfolgt, also muss $g \circ f$ als "g nach f" gelesen werden.

Beispiele 5.1.3. (a) SET ist die Kategorie der Mengen und Abbildungen.

(b) AB ist die Kategorie der abelschen Gruppen und Gruppenhomomorphismen.

(c) RING ist die Kategorie der Ringe mit Eins und unitalen Ringhomomorphismen.

(d) $\mathbb{T}$ ist die Kategorie der topologischen Raeume und stetigen Abbildungen.

(e) SET_* ist die Kategorie der **punktierten Mengen**, d.h., Objekte sind Paare (X, x_0) wobei X eine Menge ist und $x_0 \in X$ ein Element.

Morphismen von (X, x_0) nach (Y, y_0) sind Abbildungen $f : X \to Y$ mit $f(x_0) = y_0$.

(f) Sei $\mathcal{C}$ eine Kategorie. Dann ist $\mathcal{C}^{\text{opp}}$ die **entgegengesetzte** oder **duale Kategorie** in der alle Pfeile umgedreht sind. Sie hat dieselben Objekte, aber

$$\text{Hom}_{\mathcal{C}^{\text{opp}}}(X, Y) = \text{Hom}_{\mathcal{C}}(Y, X).$$

(g) Eine Gruppe kann als Kategorie verstenden werden mit nur einem Objekt. Das bedeutet, eine gegebene Gruppe G definiert eine Kategorie $\mathcal{G}$ mit nur einem Objekt X und $\text{Hom}_{\mathcal{G}}(X, X) := G$. Die Komposition ist dann die der Gruppenstruktur.

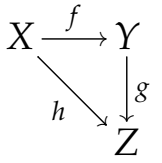
(h) Sei $(A, \geq)$ eine partiell geordnete Menge. Man definiert dann eine Kategorie mit Ob $= A$, wobei $\text{Hom}(x, y)$ hat genau ein Element hat, falls $x \leq y$ und sonst gilt $\text{Hom}(x, y) = \varnothing$.

(i) Seien $\mathcal{A}$ und $\mathcal{B}$ Kategorien. Die **Produktkategorie** $\mathcal{A} \times \mathcal{B}$ hat als Objekte die Paare (X, Y), wobei $X \in \mathcal{A}$ und $Y \in \mathcal{B}$. Ferner sei

$$\text{Hom}_{\mathcal{A}\times\mathcal{B}}((A, B), (X, Y)) = \text{Hom}(A, X) \times \text{Hom}(B, Y)$$

und die Komposition geht koordinatenweise.

Definition 5.1.4. Morphismen werden visualisiert durch Diagramme wie dieses



Ein Diagramm heisst **kommutativ**, falls je zwei Wege, die von einem Punkt zu einem andern führen, gleich sind. Das obige Diagramm ist also genau dann kommutativ, wenn $h = g \circ f$.

Definition 5.1.5. Ein Pfeil $f : X \to Y$ heisst **Isomorphismus**, falls es

einen Pfeil $g : Y \to X$ bibt, so dass

$$g \circ f = \mathbf{1}_X \quad \text{und} \quad f \circ g = \mathbf{1}_Y.$$

Beispiele 5.1.6. (a) Die Isomorphismen in der Kategorie der Mengen sind die Bijektionen.

(b) IsoMorphismen in der Kategorie der Gruppen sind Gruppenisomorphismen.

Definition 5.1.7. Sei $\mathcal{A}$ eine Kategorie. Eine **Unterkategorie** ist eine Kategorie $\mathcal{B}$, so dass $\mathrm{Ob}(\mathcal{B}) \subset \mathrm{Ob}(\mathcal{A})$ und

$$\mathrm{Hom}_{\mathcal{B}}(X, Y) \subset \mathrm{Hom}_{\mathcal{A}}(X, Y)$$

fuer alle $X, Y \in \mathcal{B}$, sowie die Kompositionen und Einheiten von $\mathcal{B}$ sind die von $\mathcal{A}$. Eine Unterkategorie $\mathcal{B}$ heisst eine **volle Unterkategorie**, falls fuer je zwei $X, Y \in \mathcal{B}$ gilt $\mathrm{Hom}_{\mathcal{B}}(X, Y) = \mathrm{Hom}_{\mathcal{A}}(X, Y)$. Jede Teilklasse von $\mathrm{Ob}(\mathcal{A})$ definiert genau eine volle Unterkategorie.

Beispiel 5.1.8. Die Kategorie der endlichen Gruppen ist eine volle Unterkategorie der Kategorie GRP aller Gruppen.

Definition 5.1.9. Eine volle Unterkategorie $\mathcal{D} \subset \mathcal{A}$ heisst **dicht**, falls es zu jedem $X \in \mathcal{A}$ ein $Y \in \mathcal{D}$ gibt, so dass X isomorph zu Y ist.

Beispiel 5.1.10. Sei K ein Koerper und $\mathcal{A}$ die Kategorie der endlich-dimensionalen K-Vektorraeume und linearen Abbildungen. Dann ist die volle Unterkategorie $\mathcal{D}$ mit den Objekten $\{0\}, K, K^2, K^3, \ldots$ eine dichte Unterkategorie.

* * *

5.2 Epis, Monos und Produkte

Definition 5.2.1. Ein Morphismus $f : X \to Y$ heist **Epimorphismus** oder **Epi**, falls fuer jedes (nichtkommutative!) Diagramm der Form

$$X \xrightarrow{f} Y \underset{\beta}{\overset{\alpha}{\rightrightarrows}} Z$$

gilt

$$\alpha f = \beta f \quad \Rightarrow \quad \alpha = \beta.$$

Beispiele 5.2.2. (a) In SET sind die Epis genau die surjektiven Abbildungen.

(b) In der Kategorie der Gruppen sind die Epis genau die surjektiven Gruppenhomomorphismen.

Beweis. Jeder surjektive Pfeil ist offensichjtlich ein Epi. Fuer die Umkehrung sei $f : G \to H$ ein Epi in GRP. Sei $H_0 \subset H$ das Bild von f. Sei $X = \{\omega\} \cup H/H_0$, wobei ω ein neuer Punkt ist. Sei $x_0 = 1H_0$ die triviale Nebenklasse. Sei $\alpha : H \to \mathrm{Per}(X)$ der Gruppenhomomorphismus, der durch die Linkstranslation definiert wird, genauer

$$\alpha(h)(x) = \begin{cases} hx, & x \in H/H_0, \\ \omega & x = \omega. \end{cases}$$

Der Stabilisator des Punktes x_0 ist H. Sei $\tau \in \mathrm{Per}(X)$ die Permutation, die ω und x_0 vertauscht und alle anderen Elemente unveraendert laesst, d.h.,

$$\tau(x) = \begin{cases} \omega & x = x_0, \\ x_0 & x = \omega, \\ x & \text{sonst.} \end{cases}$$

Ein gegebenes $h \in H$ kommutiert genau dann mit τ, wenn es trivial

auf x_0 operiert, d.h., wenn es in H_0 liegt. Sei $\beta : H \to \mathrm{Per}(X)$ der Gruppenhomomorphismus gegeben durch

$$\beta(h) = \tau\alpha(h)\tau^{-1}.$$

Für $h_0 \in H_0$ gilt $\alpha(h_0)\omega = \omega$ sowie $\alpha(h_0)x_0 = x_0$, so dass

$$\alpha(h_0) = \beta(h_0).$$

Also $\alpha f = \beta f$. Da f ein Epi ist, folgt $\alpha = \beta$, d.h., jedes Element von H kommutiert mit τ, also $H_0 = H$, d.h., f ist surjektiv. □

(c) In der Kategorie RING ist die Inklusion $\mathbb{Z} \to \mathbb{Q}$ ein Epi.

Definition 5.2.3. Ein Morphismus $f : X \to Y$ heisst a **Monomorphismus** oder **Mono**, falls fuer jedes Diagramm der Form

$$V \underset{\beta}{\overset{\alpha}{\rightrightarrows}} X \xrightarrow{f} Y$$

gilt

$$f\alpha = f\beta \quad \Rightarrow \quad \alpha = \beta.$$

Beispiele 5.2.4. (a) Eine Abbildung in SET is genau dann Mono, wenn sie injektiv ist.

(b) Ein Morphismus f ist genau dann Mono in einer Kategorie $\mathcal{C}^{\mathrm{opp}}$, wenn f ein Epi in $\mathcal{C}$ ist.

5.3 Terminale und initiale Objekte

Definition 5.3.1. Ein **terminales Objekt** einer Kategorie $\mathcal{C}$ ist ein Objekt X, so dass es von jedem anderen Objekt A genau einen Pfeil nach X gibt, also wenn gilt

$$|\mathrm{Hom}(A, X)| = 1$$

fuer jedes Objekt A.

Beispiele 5.3.2. (a) In der Kategorie SET ist eine Einpunktmenge terminal.

(b) In der Kategorie der Gruppen ist die triviale Gruppe $\{1\}$ terminal.

(c) In der Kategorie der Ringe ist der Nullring terminal.

(d) in der Kategorie $(\mathbb{N}, \leq)$ gibt es kein terminales Objekt.

Satz 5.3.3. *Ein terminales Objekt ist bis auf Isomorphie eindeutig bestimmt.*

Beweis. Seien S, T terminale Objekte in $\mathcal{C}$. Da T terminal ist, gibt es genau einen Pfeil $\alpha : S \to T$. Da S terminal ist, gibt es genau einen Pfeil $\beta : T \to S$. Da T terminal ist, gibt es genau einen Pfeil $T \to T$, naemlich die Eins $\mathbf{1}_T$. Damit folgt

$$\alpha\beta = \mathbf{1}_T.$$

Ebenso folgt $\beta\alpha = \mathbf{1}_S$ und damit sind α und β Isomorphismen. □

Definition 5.3.4. Ein **initiales Objekt** I in $\mathcal{C}$ ist ein terminales Objekt in $\mathcal{C}^{\mathrm{opp}}$.

Das heisst also: I ist genau dann initial, wenn

$$|\mathrm{Hom}(I, A)| = 1$$

fuer jedes $A \in \mathcal{C}$ gilt.

Beispiele 5.3.5. (a) In SET ist die leere Menge initial.

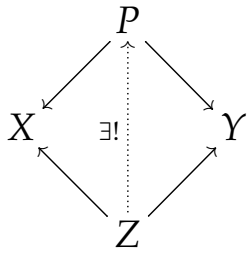
(b) In GRP ist die triviale Gruppe initial.

(c) In RING ist $\mathbb{Z}$ initial.

Bemerkung 5.3.6. Ein initiales Objekt ist ebenfalls bis auf Isomorphie eindeutig, was man entweder ebenso beweist wie den Satz, oder sich darauf zurueckzieht, dass Isomorphismen in $\mathcal{C}^{\mathrm{opp}}$ dasselbe sind wie Isomorphismen in $\mathcal{C}$.

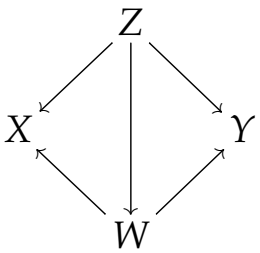
5.4 Produkte und Coprodukte

Definition 5.4.1. Seien X, Y Objekte einer Kategorie $\mathcal{C}$. Ein **Produkt** von X und Y ist ein Objekt P, zusammen mit Morphismen $p_1 : P \to X$ und $p_2 : P \to Y$, so dass die folgende universelle Eigenschaft gilt: Für jedes Objekt Z und Morphismen $\alpha : Z \to X$ und $\beta : Z \to Y$ gibt es genau einen Morphismus $Z \to P$, so dass das Diagramm



kommutiert. Das bedeutet, dass die Morphismen von Z nach X und Y ueber die universellen Morphismen von P nach X und Y faktorisieren.

Proposition 5.4.2. *Falls es existiert, ist ein Produkt eindeutig bestimmt bis auf Isomorphie. Genauer ist ein Produkt (P, p_X, p_Y) ein terminales Objekt in der Kategorie aller Tripel (Z, α, β) wie oben, wobei ein Morphismus $(Z, \alpha, \beta) \to (W, \gamma, \delta)$ ein Morphismus $Z \to W$ ist, der das Diagramm*



kommutativ macht.

Proof. Klar. □

Definition 5.4.3. Da das Produkt eindeutig bestimmt ist, kann man es als $X \times Y$ schreiben.

Beispiele 5.4.4. (a) In SET ist das kartesische Produkt ein Produkt. Dasselbe gilt in GRP, RING.

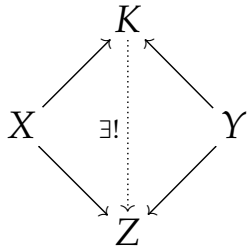
(b) In FIELD gibt es nicht immer ein Produkt, da es zum Beispiel keinen Körper K gibt, der sowohl nach $\mathbb{Q}$ als auch nach $\mathbb{F}_2$ abgebildet werden kann.

Die universelle Eigenschaft liefert eine Bijektion

$$\mathrm{Hom}(Z, X \times Y) \cong \mathrm{Hom}(Z, X) \times \mathrm{Hom}(Z, Y).$$

Definition 5.4.5. Ein **Coprodukt** von X und Y ist ein Product in C^{opp}.

Das bedeutet, es ist ein Objekt K mit Pfeilen $i_1 : X \to K$ und $i_2 : Y \to K$, so dass die folgende universelle Eigenschaft gilt: Für jedes objekt Z und Morphismen $p : X \to Z$ und $q : Y \to Z$ gibt es genau einen Pfeil $K \to Z$, so dass das Diagramm



kommutiert. Es ist eindeutig bestimmt, wenn es existiert und wir schreiben es dann als $K = X \coprod Y$ oder $C = X \oplus Y$. Die universelle Eigenschaft liefert Bijektionen:

$$\mathrm{Hom}(X \oplus Y, Z) \cong \mathrm{Hom}(X, Z) \times \mathrm{Hom}(Y, Z).$$

Beispiele 5.4.6. (a) In der Kategorie SET ist das Copruduct $X \coprod Y$ gleich

der disjunkten Vereinigung also

$$X \sqcup Y = X \coprod Y.$$

(b) In der Kategorie der Gruppe ist das Coprodukt gleich dem freien Produkt von Gruppen, also

$$G \coprod H = G * H.$$

(c) In der Kategorie RING ist das Coprodukt gleich dem Tensorprodukt über $\mathbb{Z}$.

(d) In der Kategorie FIELD gibt es im Allgemeinen kein Corpodukt, nimm etwa wieder zwei Koerper verschiedener Charakteristik.