Algebra Script

RWTH Aachen

Melkonian Dmytro

14 October 2018

Inhoudsopgave

Hoofdstuk 1

Gruppen, Ringe, Körper

Definition 1.1 (Gruppe) Eine **Gruppe** ist eine nicht-leere Menge G versehen mit einer inneren Verknüpfung $G \times G \to G, (a, b) \mapsto a \cdot b$, die folgende Axiomen genügt:

1. **Asoziativität** $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. **neutrales Element** $\exists e \in G : \forall a \in G : a \cdot e = e \cdot a$
3. **inverses Element** $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$

Die Gruppe G heisst **kommutativ** (oder **abelsch**), falls

4. **Kommutavität** $\forall a, b \in G : a \cdot b = b \cdot a$

Example 1 $(\mathbb{Z}, +)$

- G1: $(a + b) + c = a + (b + c)$
- G2: $e = 0 : 0 + a = a + 0 = a$
- G3: $a^{-1} = -a : (-a) + a = a + (-a) = 0$
- G4: $a + b = b + a$

$\forall a, b, c \in \mathbb{Z}$

Example 2 $(S_m, \circ)$ $\sigma_1 \circ \sigma_2 : \{1, \ldots, m\} \to \{1, \ldots, m\}$
$S_m = \{\sigma\{1, \ldots, m\} \to \{1, \ldots, m\} | \sigma - \text{Bijektiv}\}$

- G2: $e = id = \begin{pmatrix} 1, \ldots, m \\ 1, \ldots, m \end{pmatrix} = (1)(2), \ldots, (m)$
- G3: Sei $\sigma \in S_m : \sigma \circ \sigma^{-1} = e = \sigma^{-1} \circ \sigma$
- G4: $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$

Proposition 1.2 *Eine Gruppe hat die folgenden Eigenschaften:*

1. *Das neutrale Elemenet e ist eindeutig bestimmt.*
2. *Das inverse Element zu a inG ist eindeutig bestimmt.*
3. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ *für alle* $a, b \in G$.
4. *Für alle* $a, b \in G$ *hat die Gleichung* $a \cdot x = b$ *eine eindeutige Lösung in* G. *Die Gleichung* $y \cdot a = b$ *hat eindeutige Lösung in* G. *Es gilt* $x = a^{-1} \cdot b$ *und* $y = b \cdot a^{-1}$.

PROOF Sei G - Gruppe

1. Angenohmen $\exists e_1, e_2 \in G$ - Neutralelemente

$$\implies e_1 = e_1 \circ e_2 = e_2 \iff e_1 = e_2$$

2. Angenohmen $\exists a_1, a_2$ sind inverse Elemente zu $a \in G$

$$\implies a_1 = a_1 \circ e = a_1 \circ (a \circ a_2) = (a_1 \circ a) \circ a_2 = e \circ a_2 = a_2 \iff a_1 = a_2$$

3.

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ ((a^{-1} \circ a) \circ b) = b^{-1} \circ (e \circ b) = b^{-1} \circ b = e$$

Definition 1.3 (Gruppenhomomorphismus) Sei $\phi : G_1 \to G_2$ eine Abbildung zwischen zwei Gruppen. Dann heisst ϕ **Gruppenhomomorphismus** falls für alle $g_1, g_2 \in G_1$:

$$\phi(g_1 \cdot_{G_1} g_2) = \phi(g_1) \cdot_{G_2} \phi(g_2)$$

Der **Kern** von ϕ ist die Menge

$$Ker(\phi) := \{g \in G_1 | \phi(g) = e_{G_2}\}$$

Ein bijektiver (resp. surjektiver bzw. injektiver) Gruppenhomomorphismus heisst **Isomorphismus** (resp. **Epimorphismus** bzw. **Monomorphismus**).

Example 3 $exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$

$$x \mapsto e^x = exp(x)$$

$$epx(x + y) = exp(x)exp(y)$$

Proposition 1.4 *Sei $\phi : G_1 \to G_2$ ein Gruppenhomomorphismus, dann gelten:*

1. $\phi(e_1) = e_2$
2. $\phi(a^{-1}) = (\phi(a))^{-1}$ *für alle* $a \in G_1$.
3. *Sei $\psi : G_2 \to G_3$ ein weiterer Gruppenhomomorphismus, dann ist acuh $\psi \circ \phi : G_1 \to G_3$ ein Gruppenhomomorphismus.*

PROOF 1. ($\phi(e_1) = e_2$) Sei $a \in G_1$, dann

$$\begin{aligned} \phi(a) &= \phi(a \cdot e_1) = \phi(a) \cdot \phi(e_1) \\ \phi(a)^{-1} \cdot \phi(a) &= \phi(a)^{-1} \cdot \phi(a) \cdot \phi(e_1) \\ e_2 &= e_2 \cdot \phi(e_1) = \phi(e_1) \end{aligned}$$

2. $(\phi(a^{-1}) = (\phi(a))^{-1}$ für alle $a \in G_1)$

$$e_2 = \phi(e_1) = \phi(a \cdot a^{-1}) = \phi(a) \cdot \phi(a^{-1})$$
$$\implies \phi(a^{-1}) \text{ ist das inverse zu } \phi(a)$$

Definition 1.5 (Untergruppe) Eine Teilmenge H von G heisst **Untergruppe** von G, wenn folgende Axiome erfüllt sind:

1. $a, b \in H \implies a \cdot b \in H$ (abgeschlossen unter $\cdot$).
2. $e \in H$.
3. $a \in H \implies a^{-1} \in H$.

Example 4 $(\mathbb{Z}, +)$

$$m\mathbb{Z} = \{a \in \mathbb{Z} | a = lm : l \in \mathbb{Z}\}$$
$$3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\}$$

Behauptung: $(m\mathbb{Z}, +) \subset (\mathbb{Z}, +)$ - Untergruppe

- u1: $a_1 = l_1 m = a_2 = l_2 m \implies a_1 + a_2 = l_1 m + l_2 m = (l_1 + l_2)m$
- u2: $0 \in m\mathbb{Z}$, da $0 = 0 \cdot m$
- u3: Sei $a = lm \in m\mathbb{Z} \implies -a = (-l)m \in \mathbb{Z}$

Example 5

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$
$$(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$$

Example 6

$$(S_m, \circ) \supseteq (S_{m-1}, \circ)$$

Proposition 1.6 *Es sei $\phi : G_1 \to G_2$ ein Gruppenhomomorphismus.*

1. $\ker(\phi)$ *ist eine Untergruppe von* G_1.

2. $\mathrm{Im}(\phi)$ *ist eine Untergruppe von* G_2.

3. ϕ *ist injecktiv* $\iff \ker(\phi) = \{e_1\}$.

PROOF 1. ($\ker(\phi)$ ist eine Untergruppe von G_1) Seien $a, b \in \ker(\phi)$

- u1: D.h. $\phi(a) = e_2 = \phi(b)$

$$\implies \phi(a \cdot b) = \phi(a) \cdot \phi(b) = e_2 \cdot e_2 = e_2$$

- u2: zz $e_1 \in \ker(\phi)$. Gilt $\phi(e_1) = e_2$.
- u3: Sei $a \in \ker(\phi)$. D.h. $\phi(a) = e_2$

$$\phi(a^{-1} = (\phi(a))^{-1} = e_2^{-1} = e_2$$

2. ($\mathrm{Im}(\phi)$ ist eine Untergruppe von G_2)

- u1: Das Bild von ϕ.

$$\mathrm{Im}(\phi) = \{x \in G_2 | \exists a \in G_1 : \phi(a) = x\}$$

Seien $x, y \in \mathrm{Im}(\phi)$. D.h.

$$\begin{aligned} &\exists a_1, a_2 \in G_1 : \phi(a_1) = x, \phi(a_2) = y \\ \implies &x \cdot y = \phi(a_1) \cdot \phi(a_2) = \phi(a_1 \cdot a_2) \\ \implies &x \cdot y \in \mathrm{Im}(\phi) \end{aligned}$$

3. (ϕ ist injecktiv $\iff \ker(\phi) = \{e_1\}$) Sei ϕ-injektiv

$$\implies \big(\phi(a) = \phi(b) \implies a = b\big)$$

$$\text{Sei} a \in \ker(\phi) \implies \phi(a) = e_2 = \phi(e_1) \implies a = e_1$$

$$\text{Sei} \ker(\phi) = \{e_1\}$$

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

$$\begin{aligned} &\implies \phi(a) \cdot \phi(b)^{-1} = e_2 \iff \phi(a \cdot b^{-1}) = e_2 \\ &\implies a \cdot b^{-1} = e_1 \iff a = b \end{aligned}$$

Remark 1 Sei G eine Gruppe, H eine Untergruppe von G. Für $g_1, g_2 \in G$ definieren wir

$$g_1 \equiv g_2 \pmod{H} :\iff g_1(g_2)^{-1} \in H$$

Wir sagen, dass g_1 **kongruent zu** $g2$ **modulo** H ist.

Proposition 1.7 *Die Kongruenz modulo H ist eine Äquivalenzrelation. Wir schreiben $G \setminus H$ für Menge der Äquivalenzklassen.*

Proposition 1.8 *Sei G eine abelesche Gruppe. Dann ist $G \setminus H$ eine abelesche Gruppe mit der Verknüpfung*

$$+ : G \setminus H \times G \setminus H, ([g_1], [g_2]) \mapsto [g_1] + [g_2] := [g_1 + g_2]$$

Lemma 1 *Sei G eine abelescha Gruppe, $H \subseteq G$ eine Untergruppe. Die Abbildung*

$$\pi : G \to G \setminus G, g \mapsto [g]$$

ist ein surjektiver Gruppenhomomorphismus mit $\ker(\pi) = H$

Corollary 1 *$\mathbb{Z} \setminus m\mathbb{Z}$ ist eine abelesche Gruppe für jedes $m \in \mathbb{Z}$ und besteht aus m paarweise verschiedene Restklassen.*

Definition 1.9 (Normalteiler) Eine Untergruppe $N \subseteq G$ heisst **Normalteiler** von G falls für alle $g \in G$ gilt:

$$\{g \cdot n | n \in N\} =: gN = Ng := \{n \cdot g | n \in N\}$$

Proposition 1.10 *Sei N ein Normalteiler von G, dann ist $G \setminus N$ mit obiger Verknüpfung eine Gruppe.*

Proposition 1.11 *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, dann gilt*

1. $\ker \varphi$ *ist ein Normalteiler von* G
2. φ *induziert einen Isomorphismus von Gruppen* $\bar{\varphi} : G \backslash \ker \varphi \to \mathrm{Im}\,(\varphi), [g] \mapsto \varphi(g)$

Definition 1.12 (Ring) Ein **Ring** ist eine Menge R mit zwei inneren Verknüpfungen $+, \cdot$ so, dass $(R, +)$ eine abelesche Gruppe ist und $\cdot$ eine assoziative Verknüpfung für R mit einem neutrales Element (**Einselement**) ist. Es sollen für alle $a, b, c \in R$ gelten:

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

Remark 2 Ein Ring R heisst **kommutativ**, falls $\forall a, b \in R$ gilt: $a \cdot b = b \cdot a$. Das neutrale Element bezüglich der Addition $+$ bezeichnen wir mit 0 und das Inverse von a mit $-a$. Wir schreiben $a - b$ für $a + (-b)$. Der Einselement der Multiplikation bezeichnen wir mit 1.

Definition 1.13 (Kürper) Ein **Körper** ist ein kommutativer Ring K so, dass $K \setminus \{0\}$ mit der Multiplikation als Verknüpfung eine Gruppe ist. Insbesondere ist $0 \neq 1$.

Remark 3 Es gelten folgende Rechenregeln für alle $a, b, c \in R$:

1. $a \cdot 0 = 0 \cdot a = 0$
2. Das Einselement ist eindeutig. Wenn $1 = 0$, dann ist $R = \{0\}$
3. $-a = (-1) \cdot a$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$ und $(b - c) \cdot a = b \cdot a - c \cdot a$

Definition 1.14 (Ringhomomorphismus) Es seien R und S zwei Ringe und $\varphi : R \to S$ eine Abbildung. Dann heisst φ ein **Ringhomomorphismus** falls für alle $a, b, c \in R$ gilt

$$\varphi(a \cdot b + c) = \varphi(a) \cdot \varphi(b) + \varphi(c) \text{ und } \varphi(1_R) = \varphi(1_S)$$

Proposition 1.15 *$\mathbb{Z} \setminus m\mathbb{Z}$ ist genau dann ein Körper, wenn m ein Primzahl ist.*

Definition 1.16 (Polynom) Ein **Polynom** ist eine Folge $(a_i)_{i \in \mathbb{N}_0}$ von Elementen aus K, so dass nur endlich viele $a_i \neq 0$. Wir definieren $x := (\delta_{i,1})_{i \in \mathbb{N}_0}$. Die Menge aller Polynome mit Koeffizienten in K bezeichnen wir als $K[x]$.

Remark 4 Zwei Polynome $(a_i)_{i \in \mathbb{N}_0}$ und $(b_i)_{i \in \mathbb{N}_0}$ sind per Definition gleich, wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$.

Proposition 1.17 *Mit den Operation $+$ und $\cdot$ wird $K[x]$ zu einem kommutativer Ring.*

PROOF Für ein Polynom $(a_i)_{i \in \mathbb{N}_0} \in K[x]$ gilt

$$(a_i)_{i \in \mathbb{N}_0} = \sum_{i \in \mathbb{N}_0} a_i x^i$$

Dann ist $+$ (bzw. $\cdot$) die übliche Addition (bzw, Multiplikation) von Polynomen.

Definition 1.18 (Leitkoeffizienten und Grad) Es sei $p = \sum_{i \in \mathbb{N}_0} a_i x^i \in K[x]$ und m maximal mit $a_m \neq 0$. Dann heisst a_m der **Leitkoeffizient** von p. In diesem Fall definieren wir den **Grad** von p als $\deg p = m$. Konvention: $\deg(0)_{i \in \mathbb{N}_0} = -\infty$.

Proposition 1.19 *Sei $\alpha \in K$ gegeben, dann ist die Abbildung*

$$\pi_\alpha : K[x] \to K; p \mapsto p(\alpha) := \sum_{i \in \mathbb{N}_0} a_i \alpha^i$$

ein Ringhomomorphismus, der ***Einsetzungshomomorphismus****.*

Definition 1.20 (Nullstelle von Polynome) Sie $\alpha \in K$ gegeben. Dann heisst α eine **Nullstelle** von $p \in K[x]$ falls $\pi_\alpha(p) = p(\alpha) = 0$.

Proposition 1.21 *Für Polynome $p, q \in K[x]$ gilt:*

1. $\deg(p+q) \leq \max \deg p, \deg q$. *Falls* $\deg p \neq \deg q$, *dann gilt* $=$.
2. $\deg(p \cdot q) = \deg p + \deg q$.

Corollary 2 *Im Ring $K[x]$ gilt die Kürzungsregel*

$$p \cdot q = p \cdot r \wedge p \neq 0 \implies q = r$$

und er ist ***nullteilerfrei***

$$p \cdot q = 0 \implies p = 0 \vee q = 0$$

Theorem 1 *(Polynomdivision) Für $p, q \in K[x]$ mit $q \neq 0$ gibt es eindeutige $a, b \in K[x]$ mit*

$$p = a \cdot q + b \wedge \deg b < \deg q$$

Corollary 3 *Sei $\alpha \in K$ eine Nullstelle von $p \in K[x]$. Dann $\exists! q \in K[x]$ mit* $\deg q = \deg p - 1$ *und*

$$p = (x - \alpha) \cdot q$$

Corollary 4 *Sei $p \in K[x]$ ein Polynom vom Grad m. Dann hat p höchstens m paarweise verschiedene Nullstellen.*

Hoofdstuk 2

Matrizen und Lineare Gleichungen

Definition 2.1 (Lineares Gleichungssystem) Es sei K ein Körper, $m, n \in \mathbb{N}, a_{ij}, b_i \in K$. Dann nennt man

$$\begin{array}{ccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \dots & + & a_{m,n}x_n & = & b_m \end{array}$$

ein **lineares Gleichungssystem (LGS)**, wobei die Menge aller $(x_1, \dots, x_n) \in K^n$ gesucht ist, die alle Gleichungen erfüllen.

Definition 2.2 (Matrix) Etwas kompakter: Für $n, m \in \mathbb{N}$ und $a_{ij} \in K$, nennt man

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

eine $m \times n$-**Matrix**, die Zahlen a_{ij} heissen **Einträge** oder **Elemente** der Matrix.

Definition 2.3 (Operationen mit Matrizen) Die Menge aller $m \times n$-Matrizen mit Einträgen in K bezeichnen wir mit $M_{m,n}(K)$.

1. Es seien $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n}, B = (b_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(K)$. Dann definieren wir $A + B \in M_{m,n}(K)$ durch

$$(A + B) := C = (c_{ij})_{1\leq i\leq m, 1\leq j\leq n} \text{ wobei } c_{ij} := a_{ij} + b_{ij}.$$

2. Es seien $A \in M_{m,n}(K)$ und $B \in M_{n,\ell}(K)$. Dann definieren wir $A \cdot B \in M_{m,\ell}(K)$ durch

$$(A \cdot B) := C = (c_{ij})_{1\leq i\leq m, 1\leq j\leq \ell} \text{ wobei } c_{ij} := \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Definition 2.4 Das lineare Gleichungssystem $Ax = b$ heisst **homogen**, falls $b = 0$, ansonsten heisst es **inhomogen**

Remark 5 Jedes homogene LGS besitzt immer die **triviale Lösung** $x = 0$. Wir suchen also vor allem Lösungen $x \neq 0$.

Für ein LGS $Ax = b$ betrachten wir die **erweiterte Koeffizientenmatrix** $(A|b)$:

$$(A|b) = \left(\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{array}\right)$$

Definition 2.5 (Gaussalgorithmus) **Bestandteil des Gaussalgorithmus:**

1. Vorwärtselimination ($\rightarrow$ erreiche **Zeilenstufenform**)
2. Lösbarkeitsentscheidung
3. Rückwärtssubstitution ($\rightarrow$ Unterscheidung **freie und abhängige Variable**)

Zeilenstufenform: Eine Matrix $A \in M_{m,n}(K)$ ist in Zeilenstufenform, wenn es eine Zahl $0 \leq r \leq m$ gibt, so dass

- in den ersten r-Zeilen jeweils nicht nur Nullen stehen und in den Zeilen $r+1$ bis m nur Nullen stehen
- $j_1 < j_2 < \ldots < j_r$ wobei für $1 \leq i \leq r, j_i$ den minimale Index, so dass $a_{i,j_i} \neq 0$ ist.

Proposition 2.6 *Der Gaussalgorithm liefert nach endlich vielen Schritten entweder alle Lösungen des inhomogenen LGS oder endet mit einer negativen Entscheidung über Lösbarkeit des LGS.*

Es sei G eine abelesche Gruppe, dann ist G^n auch eine abelesche Gruppe.

Definition 2.7 Es sei $\mathrm{End}(G^n) = \{f : G^n \rightarrow G^n | f$ ist Gruppenhomomorphismus $\}$. Wir definiern

$$+ : \mathrm{End}(G^n) \times \mathrm{End}(G^n) \rightarrow \mathrm{End}(G^n),\ (f_1, f_2) \mapsto \big(\underline{g} \mapsto f_1(\underline{g}) + f_2(\underline{g})\big)$$

und

$$\circ : \mathrm{End}(G^n) \times \mathrm{End}(G^n) \rightarrow \mathrm{End}(G^n),\ (f_1, f_2) \mapsto \big(\underline{g} \mapsto f_1(\underline{g}) f_2(\underline{g})\big)$$

Proposition 2.8 $\mathrm{End}(G^n)$ *ist ein Ring.*

Proposition 2.9 *Die Menge* $M_{n,n}(K)$ *mit Addition und Multiplikation bildet einen Ring.*

Hoofdstuk 3

Vektorräume

Definition 3.1 (Vektorraum) Sei K ein Körper. Ein K-**Vektorraum** ist ein Menge V mit einer **Addition** $+ : V \times V \to V$ und einer **skalaren Multiplikation** $K \times V \to V,\ (\lambda, v) \mapsto \lambda \cdot v$ die folgende Axiomen genügen für alle $\lambda, \mu \in K, v, \omega \in V$:

1. $(V, +)$ ist eine abeleshe Gruppe.
2. $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ und $\lambda \cdot (\mu + v) = \lambda \cdot v + \mu \cdot v$
3. $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$
4. $1 \cdot v = v$

Die Elementen in einem Vektorraum nennen wir **Vektoren**.

Proposition 3.2 *Für $\lambda \in K$ und v aus einem K-Vektorraum V gilt:*

1. $\lambda \cdot 0_V = 0_V$
2. $0_K \cdot v = 0_v$
3. $(-\lambda) \cdot v = \lambda \cdot (-v) = -(\lambda \cdot v)$
4. $\lambda \cdot v = 0_V \implies \lambda = 0_K$ *oder* $v = 0_V$

Definition 3.3 (Lineare Abbildung) Eine **lineare Abbildung** von (oder **Vektorraumhomomorphismus**) $\phi : V \to W$ zwischen K-Vektorräumen V und W ist ein Gruppenhomomorphismus der abeleschen Gruppen $(V, +)$ und $(W, +)$ so, dass $\phi(\lambda v) = \lambda\phi(v)$ für alle $v \in V, \lambda \in K$.

Proposition 3.4 *Es sei $\varphi : V \to W$ ein e linerare Abbildund von K-Vektorräumen. Dann gilt:*

1. $\varphi(0) = 0$
2. $\varphi(-v) = -\varphi(v)$
3. *Wenn $\psi : W \to U$ eine weitere K-lineare Abbildung ist, dann ist $\psi \circ \varphi : V \to U$ eine K-lineare Abbildung.*

Definition 3.5 (Isomorphismus) Eine K-leneare Abbildung $\varphi : V \to W$ heisst **Isomorphismus**, wenn es eine K-lineare Abbildung $\psi : W \to V$ gibt mit:

$$\psi \circ \varphi = \mathrm{id}_V \text{ und } \varphi \circ \psi = \mathrm{id}_W$$

Proposition 3.6 *Sei $\varphi : V \to W$ eine lineare Abbildung. Dann sind äquivalent:*

1. *φ ist ein Isomorphismus*
2. *φ ist bijektiv.*

Definition 3.7 (Unterraum) Eine Teilmenge U des K-Vektorraums V heisst **Unterraum** genau dann, wenn folgende Axiome erfüllt sind

1. $u_1, u_2 \in U \implies u_1 + u_2 \in U$

2. $\lambda \in K, u \in U \implies \lambda u \in U$

3. $0 \in U$

(3) ist notwendig um $U = \emptyset$ auszuschliessen.

Proposition 3.8 *Sei $\varphi : V \to W$ eine lineare Abbildung. Dann ist* $\ker \varphi$ *ein Unterraum von V,* $\operatorname{Im} \varphi$ *ein Unterraum von W.*

Proposition 3.9 *Seien U_1, U_2 Unterräume eines Vektorraums V, dann ist auch*

$$U_1 + U_2 = \{u_1 + u_2 \in V | u_1 \in U_1, u_2 \in U_2\}$$

ein Unterraum von V.

Proposition 3.10 *Sei $(U_i)_{i \in I}$ eine Familie von Unterräumen eines Vektorraums V. Dann ist auch $\bigcap_{i \in I} U_i$ eine Unterraum von V.*

Proposition 3.11 *Seien U_1, U_2 Unterräume eines Vektorraums V und $U := U1 + U2$. Dann sind die folgenden Bedingungen äquivalent*

1. $U_1 \cap U_2 = \{0\}$

2. $\forall u \in U$ *gilt:* $\exists!(u_1, u_2) \in U_1 \times U_2$ *mit* $u = u_1 + u_2$

Ist eine der beiden Bedingungen erfüllt, so heisst U die ***direkte Summe*** *von U_1 und U_2.*

Proposition 3.12 *$V \setminus W$ ist ein K-Vektorraum mit den Operationen*

$$[v] + [\omega] := [v + \omega] \text{ und } \lambda[v] := [\lambda v]$$

Proposition 3.13 *Die kanonishe Abbildung $\pi : V \to V \setminus W, v \mapsto [v]$ ist eine surjektive , lineare Abbildung mit* $\ker(\pi) = W$.

Theorem 2 *(Homomorphiesatz) Sei $\varphi : V_1 \to V_2$ eine lineare Abbildung, $W_1 \subset V_1$ ein Unterraum mit $W_1 \subseteq \ker(\phi)$. Dann gibt es geanu eine lineare Abbildung:*

$$\bar{\varphi} : V_1 \setminus W_1 \to V_2$$

mit $\bar{\varphi}([v_1] = \varphi(v_1)$ für alle $v_1 \in V_1$.

Hoofdstuk 4

Bilinearformen, euklidische Räume und ihre komplexen Varianten

Definition 4.1 (Bilinearform) Es sei V ein K-Vektorraum. Eine Bilinearform b auf V ist eine Abbildung $b : V \times V \to K$, die bilinear ist, d.h. linear in beiden Argumenten:

$$b(\lambda v_1 + v_2, w) = \lambda b(v_1, w) + b(v_2, w)$$
$$b(v, \mu w_1 + w_2) = \mu b(v, w_1) + b(v, w_2)$$

für alle $\lambda, \mu \in K, v, w, v_1, v_2, w_1, w_2 \in V$.

Definition 4.2 (Gramsche Matrix) Es sei $dimV < \infty$ und $(v_1, \dots v_n)$ eine Basis von V. Wir nennen die Matrix $A_B(b) = (a_{ij}) \in M_{n,n}(K)$, difiniert durch $(a_{ij}) = b(v_i, v_j)$, die Matrix zur Bilinearform b bezüglich der Basis B oder auch **Gramsche Matrix**.

Definition 4.3 (Sequilinearform) Es sei V ein $\mathbb{C}$-Vektorraum. Eine Abbildung $b : V \times V \to \mathbb{C}$ heisst Sequilinearform auf V falls

$b(\alpha v_1 + v_2, w) = \alpha b(v_1, w) + b(v_2, w)$ linear in 1. Argument
$b(v, \alpha w_1 + w_2) = \overline{\alpha} b(v, w_1) + b(v, w_2)$ konjugiert linear in 2. Argument.

für alle $\alpha \in \mathbb{C}, v, w, v_1, v_2, w_1, w_2 \in V$

Definition 4.4 (kongruent) Zwei Matrizen $A_1, A_2 \in M_{n,n}(\mathbb{C})$ heissen **kongruent** wenn es ein $B \in GL_n(\mathbb{C})$ gibt, so dass $A_1 = B^t A_2 \overline{B}$ gibt.

Definition 4.5 (Orthogonal) Es sei b eine Bilinearform auf V. Wir sagen $v \in V$ ist **orthogonal** zu $w \in V$ bezüglich b, wenn $b(v, w) = 0$. Wir schreiben dann $v \perp w$. Für $S \subset V$ definieren wir

$$S^{\perp} := \{w \in V | b(v, w) = 0 \, \forall v \in S\}.$$

als Menge aller Vektoren, die **rechtsorthogonal** auf S bzgl. b sind. Analog ist die Menge der **linksorthogonalen** Vektoren auf S

$$^{\perp}S := \{w \in V | b(w, v) = 0 \, \forall v \in S\}.$$

Definition 4.6 (Nicht ausgeartet) Eine Bilinearform b auf V heisst **nicht ausgeartet**, wenn $V^{\perp} = 0$ und $^{\perp}V = 0$.

Definition 4.7 (Symmetrisch/ Hermitesch) Es sei V ein K-Vektorraum und b eine Bilinearform auf V. Dann heisst b **symmetrisch**, falls $b(v,w) = b(w,v)$ für alle $v, w \in V$.

Es sei V ein $\mathbb{C}$-Vektorraum und b eine Sequilinearform auf V. dann heisst b **hermitesch**, falls $b(v,w) = \overline{b(w,v)}$ für alle $v, w \in V$.

Definition 4.8 (Quadratische Form) Eine **quadratische Form** auf V ist eine Funktion $q : V \to K$ mit folgende Eigenschaften

$q(\alpha v) = \alpha^2 q(v), \forall \alpha in K, v \in V.$
$b_q : V \times V \to K, b_q(v,w) := q(v+w) - q(v) - q(w)$ ist eine Bilinearform auf V..

b_q heisst die zu q **assozierte (symmetrische) Bilinearform**.

Definition 4.9 (Orthonormalbasis) Es sie b eine symmetrische oder hermitesche Form auf V.

- Eine Orthogonalbasis von V ist eine Basis $B = \{v_i | i \in I\}$ so, dass $b(v_i, v_j) = 0$ für $i \neq j$.
- Eine Orthogonalbasis mit $b(v_i, v_i) = 1$ für alle $i \in I$ heisst Orthonormalbasis.
- Allgemein heisst jede Familie von Vektoren $\{x_i | i \in I\}$ eine orthogonale Familie falls $b(x_i, x_j) = 0$ für $i \neq j$, und orthonormal falls auch $b(x_i, x_i) = 1$ für alle $i \in I$.

Definition 4.10 (Hauptminor) Es sei A eine $n \times n$-Matrix und $1 \leq k \leq n$. Der k-**Hauptminor** D_k von A ist die Determinant der $k \times k$-Matrix mit dem Einträgen $(a_{ij})_{1 \leq i,j \leq k}$

Definition 4.11 Es sei b eine hermitesche Form auf V. Dann b heisst:

- **positiv definit**, falls $\forall v \in V \setminus \{0\} : b(v,v) > 0$
- **negativ definit**, falls $\forall v \in V \setminus \{0\} : b(v,v) < 0$
- **positiv semidefinit**, falls $\forall v \in V \setminus \{0\} : b(v,v) \geq 0$
- **negativ semidefinit**, falls $\forall v \in V \setminus \{0\} : b(v,v) \leq 0$
- **indefinit**, falls $\exists v, w \in V : b(v,v) > 0 \wedge b(w,w) < 0$

Definition 4.12 (Signatur) Es sei nun b entweder eine reell-symmetrische oder komplex-hermitesche Form. Weiter sei V endlich-dimensional, also finden wir für b eine Orthogonalbasis $B = (v_1, \dots v_n)$. Es sei $c_i = b(v_i, v_i)$. Falls $c_i \neq 0$, so normieren wir v_i durch $\frac{1}{\sqrt{c_i}} v_i$. Damit erhalten wir für die Gramsche Matrix

$$E_n^{p,q} = diag(\underbrace{1, \dots, 1}_{p}, \underbrace{-1, \dots, -1}_{q}, 0, \dots, 0)..$$

Weiter definieren wir für b die **Signatur** (p,q) und wir sagen b ist **vom Typ** (p,q). Eine hermitesche Matrix ist **vom Typ** (p,q) wenn sie die Matrix einer hermiteschen Form vom Typ (p,q) ist.

Definition 4.13 (Skalarprodukt) Eine positiv-definite, nicht-ausgeartete, hermitesche Sequilinearform auf V heisst **Skalarprodukt** auf V.

- Ein **euklidischer Vektorraum** ist ein endlich-dimensionaler reeller Vektorraum mit einem gegebenen Skalarprodukt $\langle -, - \rangle$.
- Ein **unitärer Vektorraum** ist ein endlich- dimensionaler komplexer Vektorraum mit einem gegebenen Skalarprodukt.

Definition 4.14 (Seminorm) Es sei V ein K-Vektorraum ($K = \mathbb{R}, \mathbb{C}$). Eine Funktion $\| \cdot \| : V \to \mathbb{R}$ heisst **Seminorm**, wenn folgende Axiome erfüllt sind

$$\|\alpha v\| = |\alpha| \|v\|$$
$$\|v + w\| \leq \|v\| + \|w\| \text{ } \textbf{Dreiscksungleichung}.$$

für alle $\alpha \in K, v, w \in V$. Falls zusätzlich

$$\|v\| = 0 \implies v = 0.$$

erfüllt ist, so sprechen wir von einer **Norm**

Definition 4.15 (Metrik) Eine **Metrik** auf V ist eine Funktion $d : V \times V \to K$ mit

- $\forall x, y \in V : d(x, y) \geq 0$ und $d(x, y) = 0$ genau dann wenn $x = y$.
- $\forall x, y \in V : d(x, y) = d(y, x)$.
- $\forall x, y, z \in V : d(x, z) \leq d(x, y) + d(y, z)$.

Hoofdstuk 5

Unitäre Abbildungen und Operatoren in Unitären Räumen

Definition 5.1 (Projection) Es sei V ein K-Vktorraum und $p \in End(V)$. Dann heisst p eine **Projektion**, wenn $p^2 = p$.

Proposition 5.2 *Es sei* $p \in \mathrm{End}(V)$ *ein Projektion, dann gilt*

$$V = Im(p) \oplus Ker(p)$$

Falls $\dim V < \infty$*, so ist* p *diagonalisierbar mit den Eigenwerte* 1 *und* 0

Definition 5.3 (Orthogonale Projektion) Es sei V ein unitäre Raum, $W \subseteq V$ und $W \oplus W^{\perp} = V$, dann nennen wir die kanonische Abbildun $p_W : V \to W$, **orthogonale Projektion** von V auf W längs $W^{\perp}$.

Proposition 5.4 *Es sei* V *ein unitärer Raum und* $p : V \to V$ *eine Projektion. Dann ist* p *genau dann eine orthogonale Projektion, wenn für alle* $x \in V$ *gilt*

$$\|p(x)\| \leq \|x\| \text{ Besselsche Ungleichung}$$

In diesem Fall gilt: $\|p(x)\| = \|x\|$ *genau dann, wenn* $x \in p(V)$.

Proposition 5.5 *Es sei* V *ein unitärer Raum unt* $p : V \to V$ *eine Projektion. Dann ist* p *genau dann orthogonale Projektion, wenn für alle* $x, y \in V$ *gilt*

$$\langle p(x), y\rangle = \langle x, p(y)\rangle.$$

Satz 1 *Es sei* V *ein unitärer Raum,* $W \subseteq V$ *ein Unterraum mit* $V = W \oplus W^{\perp}$. *Für alle* $x \in V$ *ist* $p_W(x)$ *der eindeutig bestimmte Vektor* $y \in W$, *für den der Abstand* $d(x, y) = \|x - y\|$ *minimal ist.*

Proposition 5.6 *Bedingungen wie oben und es sei* $(w_1 \dots w_s)$ *eine Orthonormalbasis von* W. *Dann ist*

$$p_W(x) = \sum_{i=1}^{s} \langle x, w_i\rangle w_i.$$

Definition 5.7 (Isometrie) Es sei V ein K-Vektorraum mit hermiteschen Form b. $f \in End(V)$ heisst **isometisch** oder eine **Isometrie**, wenn $\forall v, w \in V$ gilt

$$b(f(v), f(w)) = b(v, w).$$

Einen isometischen Isomorphismus nennen wir auch **Kongruenzabbildung**

Definition 5.8

- Eine Matrix $A \in M_{n,n}(\mathbb{R})$ heisst **orthogonal**, wenn $E_n = A^t A$ ist.
- Eine Matrix $A \in M_{n,n}(\mathbb{C})$ heisst **unitär**, wenn $E_n = A^t \overline{A}$ ist.
- Die **orthogonale Gruppe** ist definiert als $O_n = \{A \in M_{n,n}(\mathbb{R}) | A \text{ ist orthogonal}\}$.
- Die **unitäre Gruppe** ist definiert als $U_n = \{A \in M_{n,n}(\mathbb{C}) | A \text{ ist unitär}\}$

Definition 5.9 (Adjungierte Operation) Es sei V ein K-Vektorraum mit einer nicht-ausgearteten hermiteschen Form $\langle , \rangle$. Dann hessen zwei lineare Abbildungen f und g **adjungiert bezüglich** $\langle , \rangle$, wenn $\forall v, w \in V$ gilt

$$\langle f(v), w \rangle = \langle v, g(w) \rangle.$$

Definition 5.10 (Selbstadjungiert) Es sei V ein Vektorraum mit Skalarprodukt. Ein $f \in End(V)$ heisst **selbstadjungiert**, wenn $f = \hat{f}$, d.h. $\forall v, w \in V$ gilt

$$\langle f(v), w \rangle = \langle v, f(w) \rangle.$$

Definition 5.11 (Normale Operatoren) Es sei V ein Vektorraum mit Skalarprodukt, $f \in End(V)$ und $\hat{f}$ existiere. Wir nennen f **normal** falls $f \circ \hat{f} = \hat{f} \circ f$ ist.

Definition 5.12 Es sei $f \in End(V)$, V ein komplexer Vektorraum mit Skalarprodukt, und es existiere $\hat{f}$. Dann nennen wir

$$f_1 := \frac{1}{2}(f + \hat{f}) \ , \ f_2 := \frac{1}{2i}(f - \hat{f}).$$

die **selbstadjungierte Komponenten** von f.

Hoofdstuk 6

Normalformen

Definition 6.1 (Köcher) Ein Quadruopel $Q = (Q_0, Q_1, s, t)$ bestehend aus Mengen Q_0, Q_1 und Abbildungen $s, t : Q_1 \to Q_0$ nennen wir **Köcher**. Wir nennen die Elementen in Q_1 die **Pfeile** und die Elemente aus Q_0 die **Knoten** des Köchers. Für $\alpha \in Q_1$ schreiben wir $s(\alpha) \xrightarrow{\alpha} t(\alpha)$. Der Köcher heisst endlich, falls Q_0 und Q_1 jeweils endlich sind.

Definition 6.2 (Darstellung) Eine **Darstellung** $V = (V_i, f_\alpha)_{i \in Q_0, \alpha \in Q_1}$ eines Köchers Q ist eine Familie von K-Vektorräumen $(V_i)_{i \in Q_0}$ zusammen mit lineare Abbildungen $\left(f_\alpha : V_{s(\alpha)} \to V_{t(\alpha)}\right)_{\alpha \in Q_1}$.

Definition 6.3 Es sei V eine Darstellung eines endliches Köchers Q. Falls $\dim V_i < \infty$ für alle $i \in Q_0$, so sagen wir die Darstellung ist endlichdimensional und notieren den **Dimensionsvektor**

$$\underline{\dim} V = (\dim V_i)_{i \in Q_0} .$$

Definition 6.4 (Morphismus) Es sei Q ein Köcher und $V = (V_i, f_\alpha$, $W = (W_i, g_\alpha$ Darstellungen von Q. Eine Abbildung (Morphismus) zwischen V und W ist eine Familie $\phi = (\phi_i)_{i \in Q_0}$ von linearen Abbildungen $\phi_i : V_i \to W_i$ so, dass für alle $\alpha \in Q_1$ gilt:

$$\phi_{t(\alpha)} \circ f_\alpha = g_\alpha \circ \phi_{s(\alpha)}.$$

Ein Isomorphismus von Darstellung ist ein Morphismus bei dem alle ϕ_i invertierbar sind. Wir sagen dann, dass V und W isomorph sind.

Definition 6.5 Es seien $V = (V_i, f_\alpha)$ und $W = (W_i, g_\alpha)$ Darstellungen von Q, dann ist $M = (M_i, h_\alpha) = V \oplus W$, die **direkte Summe von Darstellungen**, eine Darstellung von Q mit $M_i = V_i \oplus W_i$ und $h_\alpha = (f_\alpha, g_\alpha)$

Definition 6.6 (Unzerlegbare Darstellung) Es sei $V \neq 0$ eine Darstellung von Q, dann heisst V unzerlegbar falls aus $V \cong V_1 \oplus V_2$ stets $V_1 = 0$ oder $V_2 = 0$ folgt.

Hoofdstuk 7

Ringe, Algebren, Moduln

Definition 7.1 Ein **Ring** ist eine Menge R mit zwei inneren Verknüpfungen $+, *$ so, dass $(R, +)$ eine abelshe Gruppe ist und $*$ eine assoziative Verknüpfung für R mit einem neutralen Element (**Einselement**) ist. Es sollfür alle $a, b, c \in R$ gelten:

$$a * (b + c) = a * b + a * c$$
$$(b + c) * a = b * a + c * a.$$

Definition 7.2 Es seien R und S zwei Ringe und $\phi : R \to S$ eine Abbildung. Dann heisst ϕ ein **Ringhomomorphismus** falls für alle $a, b, c \in R$ gilt

$$\phi(a * b + c) = \phi(a) * \phi(b) + \phi(c) \text{ und } \phi(1_R) = 1_S.$$

Definition 7.3 (Ideal) Es sei R ein Ring und $I \subseteq R$ eine Untergruppe (bzgl. +). Dann heisst I

- ein **Linksideal** von R, falls für alle $r \in R$ und $a \in I : ra \in I$.
- ein **Rechtsideal** von R, falls für alle $r \in R$ und $a \in I : ar \in I$.
- ein **(beidseitiges) Ideal** von R, falls für alle $r \in R$ und $a \in I : ra \in I \wedge ar \in I$.

Proposition 7.4 *Es sei $\varphi : R \to S$ ein Ringhomomorphismus, dann ist* $\ker \varphi$ *ein Ideal in R. Umgekehrt sei $I \subseteq R$ ein Ideal, dann ist die kanonische Abbildung $\pi : R \to R \setminus I, r \mapsto \overline{r}$ ein Ringhomomorphismus.*

Definition 7.5 (Algebra) Es sei K ein Körper. Ein K-Vektorraum A heisst **Algebra** über K, falls es eine Abbildung gibt,

$$A \times A \to A, (a, b) \mapsto a * b.$$

so, dass $(A, +, *)$ ein Ring mit Eins ist und für alle $a, b \in A, \lambda \in K$gilt

$$\lambda(a * b) = (\lambda a) * b = a * (\lambda b).$$

Definition 7.6 (Algebrahomomorphismus) Es seien A_1, A_2 jeweils K-Algebren. Es sei $\phi : A_1 \to A_2$ ein Vektorraumhomomorphismus. Dann heisst ϕ **Algebrenhomomorphismus** wenn ϕ auch ein Ringhomomorphismus ist.

Definition 7.7 (Modul) Es sei R ein Ring mit Eins, M eine abelshe Gruppe. Dann ist M ein R-**Linksmodul**, falls es ein Abbildung gibt

$$R \times M \to M, (r, m) \mapsto r.m.$$

so, dass für alle $r, s \in R$ und für alle $m, n \in M$ gilt

$$(r * s).m = r.(s.m) \text{ und } 1.m = m$$
$$(r + s).(m + n) = r.m + s.m + r.n + s.n.$$

Entsprechend isr R ein R-**Reschtsmodul**, falls es eine Abbildung gibt

$$M \times R, (m, r) \mapsto m.r.$$

so, dass für alle $r, s \in R$ und für alle $n, m\ inM$ gilt

$$m.(r * s) = (m.r).s \text{ und } m = m.1$$
$$(m + n).(r + s) = m.r + m.s + n.r + n.s.$$

Definition 7.8 (Untermodul) Es sei M ein R-Modul, eine Untergruppe $U \subseteq M$ heisst Untermodul von M, falls $\forall r \in R, u \in U : r.u \in U$.

Definition 7.9 (Modul-Homomorphismus) Es seien N, M zwei R-Moduln und $\varphi : M \to N$ ein Gruppenhomomorphismus. Dann heisst φ ein R-**Modul-Homomorphismus** genau dann, wenn

$$\forall m \in M, r \in R : \varphi(r.m) = r\varphi(m).$$

Die Menge der R-Modul-Homomorphismen beziechnen wir mit $\hom_R(M, N)$. Ein invertierbarer **Modul-Homomorphismus** heisst Isomorphismus, die Moduln M und N heisst dann **isomorph**

Definition 7.10 Es seien M und N zwei R-Moduln, dann wird $M \times N$ wieder zum einem R-Modul durch

$$r.(m,n) = (r.m, r.n).$$

Definition 7.11 (direkte Summe) Es sei M ein R-Modul, $U_1, U_2 \subseteq M$ R-Untermoduln, dann sagen wir M ist **direkte Summe** von U_1 und U_2, $M = U_1 \oplus U_2$, falls $U_1 \cap U_2 = 0$ und $U_1 + U_2 = M$.

Definition 7.12 Es sei $M \neq 0$ ein R-Modul. M heisst **unzerlegbar** falls für alle Untermoduln $U_1, U_2 \subseteq M$ gilt

$$U_1 \oplus U_2 = M \implies U_1 = 0 \vee U_2 = 0.$$

Anderfalls heisst M zerlgebar.

Proposition 7.13 *Es sei $U \subseteq M$ ein R-Untermodul, dann ist $M \setminus \ker\varphi$ isomoph zu $\Im\varphi$.*

Wir erhalten also eine kurze exacte Sequenz

$$0 \to \ker\varphi \to M \to \Im\varphi \to 0.$$

Definition 7.14 (Endlich-erzeugte Moduln) Es sei R ein Ring und M ein R-Modul. Ein **Erzeugendensystem** von M ist eine Teilmenge

$S = \{s_i | i \in I\} \subseteq M$ so, dass für jedes $m \in M$ existieren $\{r_i | i \in I\}$, wobei nur endlich vile $r_i \neq 0$ sind, mit

$$m = \sum_{i \in I} r_i s_i.$$

M heisst **endlich-erzuegt**, falls es ein endliches Erzeugendensystem gibt und **zyklisch**, falls es ein Erzuegendensystem S gibt, mit $|S| = 1$.

Example 7 Sei M eine R-Modul, $m_1, \ldots, m_l \in M$, dann ist $(m_1, \ldots, m_l) = \sum Rm_i \subseteq M$

$R = \mathbb{Z}, m_1 = 3, m_2 = 2 \implies (2, 3) = 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z} = (1)$
$R = \mathbb{C}[x, y](xy - 2, x + y) = \mathbb{C}[x, y](xy - 2) + \mathbb{C}[x, y](x + y)$
R als R-Linksmodul $\implies$ Untermodul $\simeq$ Linksideal

Proposition 7.15 *Es sei R ein Ring, dann ist die Abbildung*

$$\{(\textit{Links-})\textit{Ideale in } R\} \to \{\textit{zyklische (Links-) Moduln}\} \setminus \textit{Isomorphie}$$

eine Bijektion.

Definition 7.16 (Freier Modul) Es sei R ein Ring und M ein R-Modul. Eine **Basis** von M ist ein linear unabhängiges Erzeugendensystem von M. Wenn M eine Basis besitzt, so nennen wir M einen **freien Modul** über R. Für jede Indexmenge I, schreiben wir R^I für den freien R-Modul mit einer Basis indiziert durch I.

Proposition 7.17 *Es sei M ein R-Modul und $\{m_i | i \in I\}$ eine Teilmenge von M. Dann existiert genau ein Modulhomomorphismus*

$$\pi : R^I \to M, e_i \mapsto m_i \textit{ für alle } i \in I.$$

Das gilt insbesondere wenn $\{m_i | i \in I\}$ ein Erzeugendensystem von M ist.

Definition 7.18 (Kring) Einen kommutativen Ring mit 1 nennen wir einen **Kring**.

Definition 7.19 Es sei $R \neq 0$ ein Ring. Dann heisst R **nullteilerfrei**, wenn für alle $a, b \in R$ gilt:

$$a * b = 0 \implies a = 0 \vee b = 0.$$

Ist R darüber hinaus ein Kring, se nennen wir R einen **Integritätsbereich**

Definition 7.20 Ein R ein Integritätsberiech. R heisst ein **euklidischer Ring**, falls eine Funktion $\delta : R \setminus \{0\} \to \mathbb{N}$ existiert mit:

$$\forall a, b \in R, a \neq 0 \exists q, r \in R : b = qa + r, r \neq 0 \implies \delta(r) < \delta(a).$$

Definition 7.21 Es sei R ein Ring, die Menge der **Einheiten** R^* in R ist die Menge der multiplikativ invertierbaren Elemente. $r \in R$ heisst **irreduzible** wenn r keine Einheit hat und $r = fg$ impliziert, dass $f \in R^*$ oder $g \in R^*$.

Definition 7.22 Es sei R ein Ring und $\{f_i | i \in I\} \subseteq R$. Dann bezeichnet $(\{f_i | i \in I\}) = \sum_{i \in I} Rf_iR$ das von $\{f_i | i \in I\}$ **erzeugte Ideal** in R. R ist ein Hauptidealring, wenn jedes Ideal in R von einem Element erzeugt wird.