1.6 Gruppen, Ringe, Körper [Arfken 4.1-2]

Bevor weitere Begriffe der linearen Algebra eingeführt werden, wird die allgemeine Struktur der Vektorräume hier ein wenig verallgemeinert.

Gruppe: Unter einer Gruppe wird ein Paar $(G, \cdot)$ verstanden, bestehend aus einer Menge G und einer Abbildung („Verknüpfung")

$$G \times G \to G \quad : \quad (a,b) \mapsto a \cdot b \, ,$$

so dass die folgenden Axiome erfüllt sind:

(i) „Assoziativität": $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\, a,b,c \in G$

(ii) „Einselement": $\exists\, e \in G$ mit $e \cdot a = a \quad \forall\, a \in G$

(iii) „Inverse": $\exists\, a^{-1} \in G$ mit $a^{-1} \cdot a = e \quad \forall\, a \in G$.

Beispiele:

* $(\mathbb{Z}, +)$; $e \overset{!}{=} 0$; $a^{-1} \overset{!}{=} -a$
* $(\mathbb{R}^+, \cdot)$; $e = 1$; $a^{-1} = \frac{1}{a}$
* Vektorräume bzgl. Addition; $e \overset{!}{=} \vec{0}$; $a^{-1} \overset{!}{=} -\vec{x}$.

Bemerkungen:

* Einselement ist eindeutig. $\left[\, e' = e \cdot e' = (e'^{-1} \cdot e') \cdot e' = e'^{-1} \cdot (e' \cdot e') = e'^{-1} \cdot e' = e \,\right]$
* —"— fungiert auch vom rechts. $\left[\, a \cdot e = a \cdot (a^{-1} \cdot a) = (a \cdot a^{-1}) \cdot a = e \cdot a = a \,\right]$
* Inverse ist eindeutig. $\left[\, (a^{-1})' = e \cdot (a^{-1})' = (a^{-1} \cdot a) \cdot (a^{-1})' = a^{-1} \cdot \underbrace{(a \cdot (a^{-1})')}_{e} = a^{-1} \cdot e = a^{-1} \,\right]$
* —"— fungiert auch vom rechts. $\left[\, a \cdot a^{-1} = e \cdot a \cdot a^{-1} = (a^{-1})^{-1} \cdot \underbrace{a^{-1} \cdot a}_{e} \cdot a^{-1} = \underbrace{(a^{-1})^{-1} \cdot a^{-1}}_{e} = e \,\right]$

Definitionen:

* Eine Gruppe $(G, \cdot)$ heißt „kommutativ" oder „abelsch", wenn $a \cdot b = b \cdot a$ für alle $a, b \in G$ gilt.

* Eine Teilmenge $H \subset G$ mit den Eigenschaften

  (i) $a \cdot b \in H \quad \forall\, a, b \in H$

  (ii) $e \in H$

  (iii) $a^{-1} \in H \quad \forall\, a \in H$

  heißt eine Untergruppe von G.

* Seien G und G' Gruppen. Eine Abbildung $\varphi : G \to G'$ heißt „Gruppenhomomorphismus", falls

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall\, a, b \in G$$

gilt, d.h. „die Abbildung respektiert die Verknüpfung".

(Es können auch wieder $\operatorname{Kern} \varphi := \{ a \in G \mid \varphi(a) = e \}$ und $\operatorname{Bild} \varphi := \{ \varphi(a) \mid a \in G \}$ definiert werden. Beide sind Untergruppen.)

* Wenn auch φ^{-1} existiert, geht es um einen „Gruppenisomorphismus" (vgl. Seite 5) ; die Gruppen sind dann „äquivalent".

Ring: Unter einem Ring versteht man ein Tripel $(R,+,\cdot)$, bestehend aus einer Menge R und zwei Verknüpfungen $R\times R\to R$,

$$(a,b)\mapsto a+b \quad \text{„Addition"}$$
$$(a,b)\mapsto a\cdot b \quad \text{„Multiplikation"},$$

so dass die folgenden Axiome erfüllt sind:

(i) $(R,+)$ ist eine abelsche Gruppe

(ii) Die Multiplikation ist assoziativ

(iii) Es gelten Distributivgesetze, d.h.

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

Bemerkungen:

* Es gibt ein Einselement (bezeichnet mit 0) und eine Inverse (bezeichnet mit $-a$) nur bezüglich Addition!

* Ein Homomorphismus (vgl. Seite 21) soll die beiden Verknüpfungen respektieren, d.h.

$$\varphi(a+b)=\varphi(a)+\varphi(b)$$
$$\varphi(ab)=\varphi(a)\cdot\varphi(b).$$

* In jedem Ring gilt $a\cdot 0=0\cdot a=0 \quad \forall a\in R$.

(Beweis: $a\cdot 0=a\cdot(b-b)=a\cdot b-a\cdot b=0$.)

Körper: Ein Ring $(\mathbb{K},+,\cdot)$ heißt ein Körper („field"), wenn auch $(\mathbb{K}\setminus 0,\cdot)$ eine abelsche Gruppe ist.

D.h. man kann nicht nur addieren, subtrahieren und multiplizieren, sondern auch dividieren (also multiplizieren durch Inverse).

Beispiele:

* $(\mathbb{Q},+,\cdot)$ der Körper der rationalen Zahlen

$$\left[\ \mathbb{Q}=\left\{\tfrac{p}{q}\ \middle|\ p,q\in\mathbb{Z}\ ,\ q\neq 0\right\}\ \right]$$

* $(\mathbb{R},+,\cdot)$ der Körper der reellen Zahlen.

* Der Körper der rationalen Funktionen:

$$\left\{\frac{p(x)}{q(x)}\ \middle|\ p(x),q(x)\text{ sind Polynome};\ q(x)\neq 0\right\}.$$

Addition und Multiplikation wie gewöhnlich.

* Der Körper komplexer Zahlen. Dieser muß genauer betrachtet werden!

Die komplexen Zahlen: Wenn im $\mathbb{R}^2$ neben der normalen Addition „+" die als „komplexe Multiplikation" bezeichnete Verknüpfung

$$\begin{pmatrix} u \\ v \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} ux - vy \\ uy + vx \end{pmatrix}$$

definiert wird, dann ist $(\mathbb{R}^2, +, *)$ ein Körper.

Beweis:

Ring:

(i) $(\mathbb{R}^2, +)$ ist eine abelsche Gruppe.

(ii) Assoziativität: $\left(\begin{pmatrix} u \\ v \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix}\right) * \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix} * \left(\begin{pmatrix} x \\ y \end{pmatrix} * \begin{pmatrix} s \\ t \end{pmatrix}\right)$?

Explizit nachrechnen $\Rightarrow$ OK!

(iii) Distributivgesetz: $\begin{pmatrix} u \\ v \end{pmatrix} * \left(\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} s \\ t \end{pmatrix}\right) = \begin{pmatrix} u \\ v \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} * \begin{pmatrix} s \\ t \end{pmatrix}$?

$\begin{pmatrix} u \\ v \end{pmatrix} *$ fungiert wie eine lineare Abbildung $\Rightarrow$ Ok!

Körper:

(iv) Abelsch: $\begin{pmatrix} u \\ v \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} * \begin{pmatrix} u \\ v \end{pmatrix} \Rightarrow$ Ok!

(v) Einselement: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow$ Ok!

(vi) Inverse: Wenn $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, kann $\begin{pmatrix} x \\ y \end{pmatrix}^{-1} := \begin{pmatrix} \frac{x}{x^2+y^2} \\ \frac{-y}{x^2+y^2} \end{pmatrix}$ definiert werden, und es gilt

$$\begin{pmatrix} x \\ y \end{pmatrix}^{-1} * \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{x^2+y^2}{x^2+y^2} \\ \frac{xy-yx}{x^2+y^2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow \text{Ok!}$$

Die übliche Notation:

* Spricht man vom Körper $(\mathbb{R}^2, +, *)$ so benutzt man die Bezeichnung $\mathbb{C} := \mathbb{R}^2$ und nennt $z \in \mathbb{C}$ komplexe Zahlen.

* Statt $z_1 * z_2$ schreibt man einfach $z_1 z_2$.

* $$\begin{pmatrix} u \\ v \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} = \left[u\begin{pmatrix} 1 \\ 0 \end{pmatrix} + v\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] * \left[x\begin{pmatrix} 1 \\ 0 \end{pmatrix} + y\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right]$$

$$\overset{\text{Distributivgesetz}}{=} ux \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix} * \begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} + vy \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix} * \begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{\begin{pmatrix} -1 \\ 0 \end{pmatrix}} + (uy + vx) \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix} * \begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}$$

$\Rightarrow$ bezeichne $\begin{pmatrix} 1 \\ 0 \end{pmatrix} =: 1$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix} =: i$, mit $1^2 = 1$, $i^2 = -1$; $1 \cdot i = i$!

* Komplexe Konjugation ist eine Abbildung $\mathbb{C} \to \mathbb{C}$, mit

$$z \mapsto z^* := x - iy .$$

Es gilt $(z_1 + z_2)^* = z_1^* + z_2^*$, und $(z_1 z_2)^* = z_1^* z_2^*$.

Linearfaktorzerlegung bzw. **Fundamentalsatz der Algebra** (ohne Beweis):

Zu jedem komplexen Polynom

$$P(z) = z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0, \qquad a_0, \ldots, a_{n-1} \in \mathbb{C},$$

gibt es (abgesehen von der Reihenfolge) eindeutig bestimmte Zahlen $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$, so dass $P(z)$ als

$$P(z) = (z - \lambda_1)(z - \lambda_2) \cdots (z - \lambda_n)$$

faktorisiert werden kann.

$\mathbb{K}$ - Vektorräume:

Anhand der neulich definierten Strukturen können die Begriffe der reellen Vektorräume (Seite 2) und ihrer Untervektorräume (Seite 4) jetzt verallgemeinert werden.

Sei $\mathbb{K}$ ein Körper. Unter einem $\mathbb{K}$ - Vektorraum versteht man ein Tripel $(V, +, \cdot)$, gegeben durch eine abelsche Gruppe $(V, +)$ [deren Elemente die „Vektoren" sind] und eine „skalare Multiplikation" genannte Verknüpfung

$$\mathbb{K} \times V \to V \quad ;$$
$$(\lambda, \vec{v}) \mapsto \lambda \vec{v} \quad ,$$

so dass die folgenden Axiome erfüllt sind $(\lambda, \mu \in \mathbb{K}; \vec{u}, \vec{v} \in V)$:

(i) $1\vec{v} = \vec{v}$ (~ Einselement)

(ii) $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$ (~ Assoziativität)

(iii) $\lambda(\vec{u}+\vec{v}) = \lambda\vec{u} + \lambda\vec{v}$

(iv) $(\lambda+\mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$.

(~ Distributivgesetze)

Wenn $\mathbb{K} = \mathbb{R}$ bzw $\mathbb{C}$ spricht man auch vom reellen bzw. komplexen Vektorraum.

Es folgt: $0\vec{v} = (\lambda-\lambda)\vec{v} = \lambda\vec{v} - \lambda\vec{v} = \vec{0}$;
$\lambda\vec{0} = \lambda(\vec{v}-\vec{v}) = \lambda\vec{v} - \lambda\vec{v} = \vec{0}$.

$\mathbb{K}$ - UVR:

Eine Teilmenge $V_0 \subset V$ heißt ein $\mathbb{K}$ - Untervektorraum von V, wenn

(i) $\vec{0} \in V_0$

(ii) $\lambda\vec{u} + \mu\vec{v} \in V_0 \quad \forall\ \lambda, \mu \in \mathbb{K}, \vec{u}, \vec{v} \in V_0$.

Was wurde erreicht?

Die Eigenschaften der „Koeffizienten" $\in \mathbb{K}$ sind durch die Körperstruktur genau definiert; in der Regel geht es um reelle oder komplexe Zahlen.

Die Eigenschaften der „Vektoren" $\in V$ sind dagegen wenig beschränkt: V brauch nicht mehr eine Teilmenge von $\mathbb{R}^n$ zu sein! V kann sogar „unendlichdimensional" sein, z.b. die Menge von Abbildungen bzw. Funktionen $\{f \mid f: M \to \mathbb{C}^n\}$, wobei M eine gegebene Menge ist.

— ∘ —