1. Teil: Lineare Algebra

1.1: Ein wenig über Gruppen und Ringe

Bemerkung: In diesem Abschnitt stellen wir einige Begriffe und Resultate aus der Algebra zusammen, die später verwendet werden.

Definition: Es sei $G \neq \emptyset$ eine Menge und $\cdot$ eine Verknüpfung auf G (d.h. eine Abbildung $G \times G \to G$, $(a,b) \mapsto a \cdot b$. Gelten die Eigenschaften

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

so wird $(G, \cdot)$ eine Gruppe genannt.

Definition: Es sei $(G, \cdot)$ eine Gruppe. Gilt zusätzlich

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

so wird $(G, \cdot)$ eine abelsche (oder kommutative) Gruppe genannt.

Bemerkungen: 1) In der Aussage, dass $\cdot$ eine Verknüpfung auf G ist, ist bereits enthalten, dass G bezüglich $\cdot$ abgeschlossen ist. D.h. in einer Gruppe muss stets erfüllt sein, dass $a \cdot b \in G \; \forall a,b \in G$. Diese Eigenschaft muss, wenn sie nicht offensichtlich erfüllt ist, überprüft werden und wird oft als ein Punkt in den Gruppenaxiomen angeführt.

2) Die Verknüpfung $\cdot$ wird oft nicht geschrieben. D.h. man schreibt kurz ab statt $a \cdot b$.

3) Die Verknüpfung wird (besonders bei abelschen Gruppen) oft auch als $+$ geschrieben, d.h. man schreibt $a+b$ statt $a \cdot b$. Das neutrale Element wird dann üblicherweise als 0 und das inverse Element zu a mit $-a$ bezeichnet. Die Gruppenaxiome der (abelschen) Gruppe $(G,+)$ lauten dann

1) $(a+b)+c = a+(b+c) \quad \forall a,b,c \in G$ (Assoziativität)
2) $\exists 0 \in G \quad \forall a \in G: a+0 = 0+a = a$ (neutrales Element)
3) $\forall a \in G \quad \exists -a \in G: a+(-a) = (-a)+a = 0$ (inverses Element)
4) $a+b = b+a \quad \forall a,b \in G$ (Kommutativität)

4) Ist klar, welche Verknüpfung gemeint ist, schreibt man oft kurz (und ein wenig schlampig) nur G statt $(G,\cdot)$.

<u>Beispiele</u>: 1) $(\mathbb{Z},+)$ ist eine abelsche Gruppe.

2) $(\mathbb{Q},+)$, $(\mathbb{R},+)$ und $(\mathbb{C},+)$ sind abelsche Gruppen.

3) Allgemeiner gilt (nach Definition): Ist $(K,+,\cdot)$ ein Körper, so ist $(K,+)$ eine abelsche Gruppe.

4) $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{C}\setminus\{0\},\cdot)$ sind abelsche Gruppen.

5) Allgemeiner gilt: Ist $(K,+,\cdot)$ ein Körper, so ist $(K\setminus\{0\},\cdot)$ eine abelsche Gruppe.

6) Versieht man $\mathbb{R}^2=\left\{\begin{pmatrix}x\\y\end{pmatrix} \,\middle|\, x,y\in\mathbb{R}\right\}$ mit der Addition $\begin{pmatrix}x_1\\y_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\end{pmatrix}:=\begin{pmatrix}x_1+x_2\\y_1+y_2\end{pmatrix}$ (komponentenweise Addition bzw. Addition von Vektoren), so ist $(\mathbb{R}^2,+)$ eine abelsche Gruppe:

- Abgeschlossenheit ist klar, da $\begin{pmatrix}x_1+x_2\\y_1+y_2\end{pmatrix}\in\mathbb{R}^2 \quad \forall \begin{pmatrix}x_1\\y_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\end{pmatrix}\in\mathbb{R}^2$
- $$\left(\begin{pmatrix}x_1\\y_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\end{pmatrix}\right)+\begin{pmatrix}x_3\\y_3\end{pmatrix}=\begin{pmatrix}(x_1+x_2)+x_3\\(y_1+y_2)+y_3\end{pmatrix}=\begin{pmatrix}x_1+(x_2+x_3)\\y_1+(y_2+y_3)\end{pmatrix}=\begin{pmatrix}x_1\\y_1\end{pmatrix}+\left(\begin{pmatrix}x_2\\y_2\end{pmatrix}+\begin{pmatrix}x_3\\y_3\end{pmatrix}\right)$$
  für $\begin{pmatrix}x_1\\y_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\end{pmatrix},\begin{pmatrix}x_3\\y_3\end{pmatrix}\in\mathbb{R}^2$
- $\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}+\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix} \quad \forall \begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$
- $\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}-x\\-y\end{pmatrix}=\begin{pmatrix}-x\\-y\end{pmatrix}+\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix} \quad \forall \begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$
- $\begin{pmatrix}x_1\\y_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\end{pmatrix}=\begin{pmatrix}x_1+x_2\\y_1+y_2\end{pmatrix}=\begin{pmatrix}x_2+x_1\\y_2+y_1\end{pmatrix}=\begin{pmatrix}x_2\\y_2\end{pmatrix}+\begin{pmatrix}x_1\\y_1\end{pmatrix} \quad \forall \begin{pmatrix}x_1\\y_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\end{pmatrix}\in\mathbb{R}^2$

7) Versieht man $\mathbb{R}^3=\left\{\begin{pmatrix}x\\y\\z\end{pmatrix} \,\middle|\, x,y,z\in\mathbb{R}\right\}$ mit der Addition $\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}:=\begin{pmatrix}x_1+x_2\\y_1+y_2\\z_1+z_2\end{pmatrix}$ (wieder komponentenweise Addition bzw. Addition von Vektoren), so ist $(\mathbb{R}^3,+)$ eine abelsche Gruppe.

8) Es sei $n\in\mathbb{N}\setminus\{0\}$. Versieht man (allgemein) $\mathbb{R}^n=\left\{\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix} \,\middle|\, x_1,\dots,x_n\in\mathbb{R}\right\}$ mit der komponentenweisen Addition $\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}+\begin{pmatrix}y_1\\\vdots\\y_n\end{pmatrix}:=\begin{pmatrix}x_1+y_1\\\vdots\\x_n+y_n\end{pmatrix}$, so ist $(\mathbb{R}^n,+)$ eine abelsche Gruppe.

9) Es sei K ein Körper und $n \in \mathbb{N} \setminus \{0\}$. Dann gilt (allgemeiner): Versieht man $K^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| \, x_1, \dots, x_n \in K \right\}$ mit der komponentenweisen Addition $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$, so ist $(K^n, +)$ eine abelsche Gruppe.

10) Es sei $G = \{-1, 1\}$ $(\subseteq \mathbb{Z})$, versehen mit der üblichen Multiplikation ganzer Zahlen (dh $1 \cdot 1 = (-1) \cdot (-1) = 1$ und $1 \cdot (-1) = (-1) \cdot 1 = -1$). Dann ist $(G, \cdot)$ eine abelsche Gruppe. (Abgeschlossenheit ist klar, Assoziativität gilt, da sie für ganze Zahlen gilt, 1 ist neutrales Element, $1^{-1} = 1$, $(-1)^{-1} = -1$ und Kommutativität gilt, da sie für ganze Zahlen gilt)

<u>Lemma 1</u> Es sei $(G, \cdot)$ eine Gruppe.

(i) Das neutrale Element von G ist eindeutig bestimmt,

(ii) Das inverse Element eines Gruppenelements $a \in G$ ist eindeutig bestimmt.

<u>Beweis</u>: (i) Angenommen, $e, f \in G$ sind beide neutrale Elemente. Dann folgt $e = e \cdot f = f$.

(ii) Angenommen, $x, y \in G$ sind beide inverse Elemente von $a \in G$ (dh $ax = xa = e = ay = ya$). Dann ist $x = xe = x(ay) = (xa)y = ey = y$.

<u>Bemerkung</u>: Die Notation a^{-1} für das inverse Element ist nur sinnvoll, weil Lemma 1 (ii) gilt.

<u>Lemma 2</u>: Es sei $(G, \cdot)$ eine Gruppe.

(i) $(a^{-1})^{-1} = a \quad \forall a \in G$,

(ii) $(ab)^{-1} = b^{-1} a^{-1} \quad \forall a, b \in G$.

<u>Beweis</u>: (i) $aa^{-1} = a^{-1}a = e$ und die Behauptung folgt aus der Eindeutigkeit des Inversen von a^{-1} (also von $(a^{-1})^{-1}$) nach Lemma 1 (ii).

(ii) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ und analog $(b^{-1}a^{-1})(ab) = e$. Die Behauptung folgt aus der Eindeutigkeit des Inversen von ab (also von $(ab)^{-1}$) nach Lemma 1 (ii).

<u>Bemerkung</u>: In einer abelschen Gruppe $(G, +)$ werden die beiden Aussagen von Lemma 2 (ii) zu $-(-a) = a$ und $-(a+b) = (-b) + (-a)$ $\big(= (-a) + (-b)\big)$.

Definition: Es sei $(G,\cdot)$ eine Gruppe, $a \in G$ und $n \in \mathbb{N} \cup \{0\}$. Dann setzt man $a^0 := e$ und $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ Stück}}$ für $n \geq 1$ (wobei e das neutrale Element von G bezeichnen soll).

Lemma 3: Es sei $(G,\cdot)$ eine Gruppe und $a \in G$. Dann ist $(a^n)^{-1} = (a^{-1})^n \; \forall n \in \mathbb{N} \cup \{0\}$.

Beweis: Induktion nach n. Für $n=0$ ist $(a^0)^{-1} = e^{-1} = e = (a^{-1})^0$ (und für $n=1$ ist $(a^1)^{-1} = a^{-1} = (a^{-1})^1$). Schließlich ist

$$(a^{n+1})(a^{-1})^{n+1} = \underbrace{(a \cdots a)}_{n \text{ Stück}} a a^{-1} \underbrace{(a^{-1} \cdots a^{-1})}_{n \text{ Stück}} = \underbrace{a \cdots a}_{n \text{ Stück}} e \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ Stück}} = \underbrace{a \cdots a}_{n \text{ Stück}} \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ Stück}} \overset{IV}{=} e$$

und analog $(a^{-1})^{n+1}(a^{n+1}) = e$. Die Behauptung folgt aus Lemma 1 (ii)

Definition: Es sei $(G,\cdot)$ eine Gruppe, $a \in G$ und $n \in \mathbb{N} \setminus \{0\}$. Dann setzt man $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.

Bemerkung: In einer abelschen Gruppe $(G,+)$ werden die beiden letzten Definitionen als $0 \cdot a = 0$ (dabei ist links $0 \in \mathbb{Z}$ und rechts $0 \in G$!), $na = \underbrace{a + \cdots + a}_{n \text{ Stück}}$ und $(-n)a = -(na) = n(-a)$ (für $n > 0$) geschrieben.

4.10.2021

Satz 4 Es sei $(G,\cdot)$ eine Gruppe.

(i) $a^m a^n = a^{m+n} \quad \forall a \in G \; \forall m,n \in \mathbb{Z}$,

(ii) $(a^m)^n = a^{mn} \quad \forall a \in G \; \forall m,n \in \mathbb{Z}$,

(iii) Ist G abelsch, so ist $(ab)^n = a^n b^n \quad \forall a,b \in G \; \forall n \in \mathbb{Z}$.

Der Beweis ist recht technisch. Abgesehen von Lemma 3 verwendet man Fallunterscheidungen und Induktion. Wir lassen ihn darum aus.

Bemerkung: Ist $(G,+)$ eine abelsche Gruppe, so wird Satz 4 zu

(i) $ma + na = (m+n)a \quad \forall a \in G \; \forall m,n \in \mathbb{Z}$,

(ii) $n(ma) = (nm)a \quad \forall a \in G \; \forall m,n \in \mathbb{Z}$,

(iii) $n(a+b) = na + nb \quad \forall a,b \in G \; \forall n \in \mathbb{Z}$.

Definition: Es sei $R \neq \emptyset$ eine Menge und $+$ und $\cdot$ zwei Verknüpfungen auf R (d.h. Abbildungen $R \times R \to R, (a,b) \mapsto a+b$ und $R \times R \to R, (a,b) \mapsto a \cdot b$). Gelten die Eigenschaften

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

2) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a,b,c \in R$ (Assoziativität der Multiplikation),

3) $a\cdot(b+c) = a\cdot b + a\cdot c$ und $(a+b)\cdot c = a\cdot c + b\cdot c$ $\forall a,b,c \in R$ (Distributivgesetze)

so wird $(R,+,\cdot)$ ein Ring genannt. Gilt zusätzlich (zu 1), 2), und 3))

4) $\exists 1 \in R\ \forall a \in R: 1\cdot a = a \cdot 1 = a$ (Existenz des Einselements),

so wird $(R,+,\cdot)$ Ring mit Einselement (oder kurz Ring mit 1) genannt.

Gilt zusätzlich (zu 1) 2) und 3))

5) $a\cdot b = b \cdot a$ $\forall a,b \in R$ (Kommutativität der Multiplikation)

so wird $(R,+,\cdot)$ kommutativer Ring genannt.

Gelten alle fünf Bedingungen 1) - 5), so wird $(R,+,\cdot)$ kommutativer Ring mit Einselement genannt.

Bemerkungen: 1) Auch bei Ringen ist die Abgeschlossenheit bezüglich der beiden Verknüpfungen (d.h. $a+b \in R$ $\forall a,b \in R$ und $a\cdot b \in R$ $\forall a,b \in R$) darin enthalten, dass $+$ und $\cdot$ beides Verknüpfungen sind, müssen aber überprüft werden, wenn sie nicht offensichtlich sind.

2) Auch bei Ringen wird die Verknüpfung $\cdot$ oft nicht geschrieben (d.h. man schreibt ab statt $a\cdot b$).

3) $(R,+)$ ist nach Definition eine abelsche Gruppe und man verwendet die Bezeichnungen einer (additiv geschriebenen) abelschen Gruppe dafür, wie sie oben beschrieben wurden. Insbesondere wird das neutrale Element mit 0 bezeichnet (und das Nullelement des Rings genannt) und das additive Inverse zu $a \in R$ wird $-a$ geschrieben.

4) Da $(R,+)$ eine abelsche Gruppe ist, gelten alle bisher dafür bewiesenen (oder auch nur angegebenen) Aussagen.

5) Ist klar, welche Verknüpfungen gemeint sind, schreibt man kurz R statt $(R,+,\cdot)$

Notation: Ist $(R,+,\cdot)$ ein Ring und $a,b \in R$, so schreibt man kurz $a-b$ für $a+(-b)$ (d.h. $a-b := a+(-b)$)

Lemma 5 Es sei $(R,+,\cdot)$ ein Ring. Dann gelten

(i) $0\cdot a = a \cdot 0 = 0$ $\forall a \in R$,

(ii) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$ $\forall a,b \in R$,

(iii) $(-a)\cdot(-b) = a \cdot b$ $\forall a,b \in R$

(iv) $a\cdot(b-c)=a\cdot b-a\cdot c$ und $(a-b)\cdot c=a\cdot c-b\cdot c$ $\forall a,b,c\in R$

(v) $(na)\cdot b=a\cdot(nb)=n(a\cdot b)$ $\forall n\in\mathbb{Z}$ $\forall a,b\in R$

(Ohne Beweis)

Beispiele: 1) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer Ring mit Einselement.

2) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ sind kommutative Ringe mit Einselement.

3) Allgemeiner gilt: Ist $(K,+,\cdot)$ ein Körper, so ist $(K,+,\cdot)$ ein kommutativer Ring mit Einselement. (Wir haben den Begriff des Körpers vorausgesetzt, hätten aber auch definieren können: Ein Körper $(K,+,\cdot)$ ist ein kommutativer Ring mit Einselement, in dem $0\neq 1$ gilt und jedes $a\in K\setminus\{0\}$ ein multiplikatives Inverses besitzt.)

Definition: Es sei $(R,+,\cdot)$ ein Ring mit Einselement. Ein $a\in R$ heißt invertierbar (oder eine Einheit), wenn ein $a^{-1}\in R$ mit der Eigenschaft $a\cdot a^{-1}=a^{-1}\cdot a=1$ existiert. Das Element a^{-1} wird als das Inverse von a bezeichnet.

Lemma 6 Es sei $(R,+,\cdot)$ ein Ring mit Einselement.

(i) Das Einselement $1\in R$ ist eindeutig bestimmt,

(ii) Ist $a\in R$ invertierbar, so ist das Inverse $a^{-1}\in R$ von a eindeutig bestimmt.

Beweis: Analog zu Lemma 1.

Lemma 7 Es sei $(R,+,\cdot)$ ein Ring mit Einselement.

(i) Ist $a\in R$ invertierbar, so ist auch $a^{-1}\in R$ invertierbar und $(a^{-1})^{-1}=a$.

(ii) Sind $a,b\in R$ beide invertierbar, so ist auch $a\cdot b\in R$ invertierbar und $(ab)^{-1}=b^{-1}\cdot a^{-1}$

Beweis: Analog zum Beweis von Lemma 2.

Definition: Es sei $(R,+,\cdot)$ ein Ring mit Einselement, $a\in R$ und $n\in\mathbb{N}\cup\{0\}$. Dann setzt man $a^0:=1$ und $a^n=a\cdot\ldots\cdot a$ für $n\geq 1$.

Definition: Es sei $(R,+,\cdot)$ ein Ring mit Einselement, $a\in R$ invertierbar und $n\in\mathbb{N}\setminus\{0\}$. Dann setzt man $a^{-n}:=(a^n)^{-1}=(a^{-1})^n$.

(Dass $(a^n)^{-1}=(a^{-1})^n$ gilt, zeigt man wie in Lemma 3.)

Lemma 8 Es sei $(R,+,\cdot)$ ein Ring mit Einselement.

(i) $a^m a^n = a^{m+n}$ $\forall a\in R$ $\forall m,n\in \mathbb{N}\cup\{0\}$,

(ii) $(a^m)^n = a^{mn}$ $\forall a\in R$ $\forall m,n\in\mathbb{N}\cup\{0\}$,

(iii) Ist R kommutativ, so ist $(ab)^n = a^n b^n$ $\forall a,b\in R$ $\forall n\in\mathbb{N}\cup\{0\}$.

Der Beweis verläuft wie der von Satz 4.

Lemma 9 Es sei $(R,+,\cdot)$ ein Ring mit Einselement.

(i) Ist $a\in R$ invertierbar, so ist $a^m a^n = a^{m+n}$ $\forall m,n\in\mathbb{Z}$

(ii) Ist $a\in R$ invertierbar, so ist $(a^m)^n = a^{mn}$ $\forall m,n\in\mathbb{Z}$

(iii) Ist R kommutativ und sind $a,b\in R$ invertierbar, so ist $(ab)^n = a^n b^n$ $\forall n\in\mathbb{Z}$

Der Beweis verläuft wie der von Satz 4.

Notation: Es sei $(R,+,\cdot)$ ein Ring mit Einselement. Dann bezeichne

$R^* = \{a\in R \mid a \text{ ist invertierbar}\}$.

Lemma 10 Es sei $(R,+,\cdot)$ ein Ring mit Einselement. Dann ist $(R^*,\cdot)$ eine Gruppe

Beweis: $R^*\neq\emptyset$, da $1\in R^*$ (aus $1\cdot 1=1$ folgt $1^{-1}=1$). Die Abgeschlossenheit folgt aus Lemma 7 (ii), die Assoziativität gilt, da sie für den Ring $(R,+,\cdot)$ gilt, $1\in R^*$ ist neutrales Element und inverse Elemente existieren wegen Lemma 7 (i).

Bemerkung: Die Gruppe $(R^*,\cdot)$ wird als Einheitengruppe des Rings $(R,+,\cdot)$ bezeichnet.

Beispiele: 1) $\mathbb{Z}^* = \{-1,1\}$,

2) $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$ und $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$,

3) Ist allgemein $(K,+,\cdot)$ ein Körper, so ist $K^* = K\setminus\{0\}$.

Bemerkung: Die Bezeichnung R^* ist in der Algebra üblich, stimmt mit der in der Schule üblichen aber nur überein, wenn R ein Körper ist. Beachten Sie, dass $\mathbb{Z}^*$ in der Schule üblicherweise eine andere Bedeutung hat (und die Bezeichnung $\mathbb{N}^*$ in unserem Zusammenhang sinnlos ist, da $(\mathbb{N},+,\cdot)$ kein Ring ist).