Lineare Algebra

Prof. Dr. Ghislain Fourier

Wichtige Emailadresse: kalmbach@mathb.rwth-aachen.de

Sprechstunde: Do, 14:00 - 15:00 Uhr, Raum 403, Pontdriesch 10-16

Literatur:

- Gerd Fischer: Lineare Algebra eine Einführung für Studienanfänger
- weitere siehe RWTH-Online

1. Propädeutikum

Alles notwendige dazu haben Sie im Propädeutikum gelernt!

Dort haben Sie vor allem erste Begriffe, Beweise, Definitionen gelernt.

Neben der Logik brauchen Sie für die Lineare Algebra 1 vor allem die folgenden Begriffe:

1. Menge
2. Abbildung
3. bijektiv, surjektiv, injektiv
4. Relation

2. Gruppen, Ringe, Körper

Wir nähern uns der Algebra...

Definition 2.1 (Gruppe)

Eine **Gruppe** ist eine nichtleere Menge G versehen mit einer inneren Verknüpfung $G \times G \longrightarrow G$, $(a,b) \mapsto a \cdot b$, die folgenden Axiomen genügt:

G1 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in G$ (**Assoziativität**)

G2 $\exists\, e \in G$ so, dass $\forall\, a \in G : a \cdot e = e \cdot a = a$. (**neutrales Element**)

G3 $\forall\, a \in G : \exists\, a^{-1} \in G$ mit $a^{-1} \cdot a = a \cdot a^{-1} = e$ (**inverses Element**)

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

G4 $\forall\, a, b \in G : a \cdot b = b \cdot a$.

***Beispiele*: Gruppen**

Proposition 2.2

Eine Gruppe hat die folgenden Eigenschaften

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

***Beweis* von Proposition 2.2**

Der wichtige Begriff: Die strukturerhaltende Abbildung!

Definition 2.3 (Gruppenhomomorphismus)

Es sei $\phi : G_1 \longrightarrow G_2$ eine Abbildung zwischen zwei Gruppen. Dann heißt ϕ **Gruppenhomomorphimus** 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

$$\mathrm{Ker}(\phi) := \{g \in G_1 \mid \phi(g) = e_{G_2}\}.$$

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

***Beispiele*: Gruppenhomomorphismen**

Proposition 2.4

Sei $\phi : G_1 \longrightarrow G_2$ 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 $\psi : G_2 \longrightarrow G_3$ ein weiterer Gruppenhomomorphimus, dann ist auch $\psi \circ \phi : G_1 \longrightarrow G_3$ ein Gruppenhomomorphimus.

***Beweis* von Proposition 2.4**

Definition 2.5

Eine Teilmenge H von G heißt Untergruppe von G, wenn folgende Axiome erfüllt sind

U1 $a, b \in H \Longrightarrow a \cdot b \in H$ (abgeschlossen unter $\cdot$).

U2 $e \in H$.

U3 $a \in H \Longrightarrow a^{-1} \in H$.

***Beispiele*: Untergruppe**

Proposition 2.6

Es sei $\phi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus.

1. $\mathrm{Ker}(\phi)$ ist eine Untergruppe von G_1.
2. $\mathrm{Im}(\phi)$ ist eine Untergruppe von G_2.
3. ϕ ist injektiv $\Leftrightarrow \mathrm{Ker}(\phi) = \{e_1\}$.

***Beweis* von Proposition 2.6**

Es sei G eine Gruppe, H eine Untergruppe von G. Für $g_1, g_2 \in G$ definieren wir

$$g_1 \equiv g_2 (\mathrm{mod}\, H) :\Leftrightarrow g_1 (g_2)^{-1} \in H.$$

Wir sagen, dass g_1 **kongruent zu** g_2 ist **modulo** H.
***Beispiele*: für Kongruenzen modulo H**

Proposition 2.7

Die Kongruenz modulo H ist eine Äquivalenzrelation. Wir schreiben G/H für die Menge der Äquivalenzklassen.

***Beweis* von Proposition 2.7**

Proposition 2.8

Sei G eine abelsche Gruppe. Dann ist G/H eine abelsche Gruppe mit der Verknüpfung

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

***Beweis* von Proposition 2.8**

Lemma 2.9

Es sei G eine abelsche Gruppe, $H \subseteq G$ eine Untergruppe. Die Abbildung

$$\pi : G \longrightarrow G/H, g \mapsto [g]$$

ist ein surjektiver Gruppenhomomorphimus mit $\mathrm{Ker}(\pi) = H$.

***Beweis* von Lemma 2.9**

***Beispiel*:** $\mathbb{Z}/m\,\mathbb{Z}$

Korollar 2.10

$\mathbb{Z}/m\mathbb{Z}$ ist eine abelsche Gruppe für jedes $m \in \mathbb{Z}$ und besteht aus m paarweise verschiedenen Restklassen.

***Beweis* von Korollar 2.10**

Normalteiler und Isomorphisatz
Wann ist G/H eigentlich wieder eine Gruppe mit $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$?

Definition 2.11

Eine Untergruppe $N \subseteq G$ heißt **Normalteiler** von G falls für alle $g \in G$ gilt:

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

***Beispiele*: Normalteiler** $A_n \subset S_n$

Satz 2.12

Sei N ein Normalteiler von G, dann ist G/N mit obiger Verknüpfung eine Gruppe.

Beweis von Satz 2.12.

Satz 2.13

Sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus, dann gilt

1. $\operatorname{Ker} \varphi$ ist ein Normalteiler von G.
2. φ induziert einen Isomorphismus von Gruppen $\overline{\varphi} : G/\operatorname{Ker} \varphi \longrightarrow \operatorname{Im}(\varphi), [g] \mapsto \varphi(g)$.

Beweis von Satz 2.13

Wiederholung aus dem Propädeutikum:

Definition 2.14

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

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$.

D2 $(b + c) \cdot a = b \cdot a + c \cdot a$.

***Beispiele*:** $\mathbb{Z}$ **und** $\mathbb{Z}/m\,\mathbb{Z}$

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 $a + (-b)$.
Das Einselement der Multiplikation bezeichnen wir mit 1.

Definition 2.15 (Körper)

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

***Beispiele*:** $\mathbb{R}$ **und** $\mathbb{Q}$.

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

***Beispiel*: Quaternionen**

Definition 2.17

Es seien R und S zwei Ringe und $\varphi : R \longrightarrow S$ eine Abbildung. Dann heißt φ ein **Ringhomomorphismus** falls für alle $a, b, c \in R$ gilt

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

***Beispiele*: Ringhomomorphismen**

Proposition 2.18

$\mathbb{Z}/m\,\mathbb{Z}$ ist genau dann ein Körper wenn m eine Primzahl ist.

***Beweis* von Proposition 2.18**

***Beispiel*: $\mathbb{F}_p$ und komplexe Zahlen**

Diese Definition von Polynom ist NICHT die aus dem Propädeutikum.

Definition 2.19

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 $K[x]$.

Bemerkung: 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 $i \in \mathbb{N}_0$.
Beispiele: **Polynome**

Überlegung (mit Beispielen):
Es seien $(a_i)_{i\in\mathbb{N}_0}$ und $(b_i)_{i\in\mathbb{N}_0}$ Elemente in $K[x]$, dann ist auch

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} := (a_i + b_i)_{i\in\mathbb{N}_0} \in K[x]$$

(die komponentenweise **Addition** von Folgen).
Wir definieren eine Folge $(c_i)_{i\in\mathbb{N}_0}$ durch

$$c_i := \sum_{k+\ell=i} a_k b_\ell = a_i b_0 + a_{k-1} b_1 + \ldots a_1 b_{i-1} + a_0 b_i.$$

Dann definieren wir $(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} := (c_i)_{i\in\mathbb{N}_0} \in K[x]$ (die **Multiplikation** ist ein Faltungsprodukt).
Ein $\lambda \in K$ identifieren wir mit $(\lambda\delta_{i,0})_{i\in\mathbb{N}_0}$. Dann gilt

$$\lambda \cdot (a_i)_{i\in\mathbb{N}_0} = (\lambda a_i)_{i\in\mathbb{N}_0} \in K[x]$$

(die **skalare Muliplikation**).

Proposition 2.20

Mit den Operationen $+$ und $\cdot$ wird $K[x]$ zu einem kommutativen Ring.

***Beweis* von Proposition 2.20**

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 (siehe Tafel).

***Beispiele*: Polynome und zur verkürzten Schreibweise**
ACHTUNG: Funktionen vs. Polynome!

Definition 2.21

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 den **Grad** von p als $\deg p = m$.
Konvention: $\deg (0)_{i\in\mathbb{N}_0} = -\infty$.

***Beispiele*: Leitkoeffizienten und Grade**

Satz 2.22

Es sei $\alpha \in K$ gegeben, dann ist die Abbildung

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

ein Ringhomomorphimus, der **Einsetzungshomomorphismus**.

***Beispiele*: Einsetzungshomomorphimus**
***Beweis* von Satz 2.22**

Definition 2.23

Es sei $\alpha \in K$ gegeben. Dann heißt α eine **Nullstelle** von $p \in K[x]$ falls $\pi_\alpha(p) = p(\alpha) = 0$.

***Beispiele*: Nullstellen von Polynomen**

Einiges über Polynome:

Proposition 2.24

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. $\deg(p \cdot q) = \deg p + \deg q$.

***Beweis* von Proposition 2.24**

Korollar 2.25

Im Ring $K[x]$ gilt die Kürzungsregel

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

und er ist **nullteilerfrei**

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

***Beweis* von Korollar 2.25**.

Theorem 2.26 (Polynomdivision)

Für $p, q \in K[x]$ mit $q \neq 0$ gibt es eindeutige $a, b \in K[x]$ mit

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

***Beispiele*: Polynomdivision**
***Beweis* von Theorem 2.26**

Korollar 2.27

Es sei $\alpha \in K$ eine Nullstelle von $p \in K[x]$. Dann $\exists!\, q \in K[x]$ mit $\deg(q) = \deg(p) - 1$ und

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

***Beweis* von Korollar 2.27**

Daraus folgern wir sofort:

Korollar 2.28

Es sei $p \in K[x]$ ein Polynom vom Grad m. Dann hat p höchstens m paarweise verschiedene Nullstellen.

Wichtigste Begriffe des Kapitels:

- Gruppe
- Gruppenhomomorphismus
- Körper
- Polynom

Ende des Skripts