Glossar zu Lektion 1

Lineare Algebra (Modul 61112)

Kompakte Zusammenfassung aller wesentlichen Definitionen, Merkregeln und Sätze. Nummerierungen entsprechen dem Lehrtext.

1.1 Gruppen

1.1.1 Gruppe

Ein Paar $(G, *)$ aus einer Menge G und einer Verknüpfung $* : G \times G \to G$ heißt **Gruppe**, wenn gilt:

(G1) Assoziativgesetz: $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.

(G2) Neutrales Element: $\exists\, e \in G$ mit $a * e = e * a = a$ für alle $a \in G$.

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

Eine Gruppe heißt **abelsch** (oder kommutativ), wenn zusätzlich $a * b = b * a$ gilt.

1.1.3 Merkregel (Rechnen mit Inversen)

Sei $(G, *)$ eine Gruppe. Für alle $a, b \in G$ gilt: $(a * b)^{-1} = b^{-1} * a^{-1}$; $\quad (a^{-1})^{-1} = a$.

1.1.17 Satz (äquivalentes Gruppenkriterium)

$(G, *)$ mit Assoziativgesetz ist genau dann eine Gruppe, wenn es ein *linksneutrales* Element und zu jedem Element ein *Linksinverses* gibt.

1.1.18 Untergruppe

Eine Teilmenge $H \subseteq G$ heißt **Untergruppe**, wenn $e \in H$, H unter $*$ abgeschlossen ist und mit jedem $h \in H$ auch $h^{-1} \in H$ gilt.

1.2 Ringe und Körper

1.2.1 Ring

Ein Tripel $(R, +, \cdot)$ heißt **Ring**, wenn $(R, +)$ eine abelsche Gruppe (mit neutralem Element 0) ist, $\cdot$ assoziativ ist und die Distributivgesetze gelten: $a(b + c) = ab + ac$, $(a + b)c = ac + bc$. Ist $\cdot$ kommutativ, heißt R **kommutativer Ring**. Gibt es ein Einselement 1, heißt R **Ring mit Eins**.

1.2.5 Lemma (Rechenregeln in Ringen)

In jedem Ring R: $a \cdot 0 = 0 \cdot a = 0$; $\quad (-a) \cdot b = -(ab)$; $\quad (-a)(-b) = ab$.

1.2.14 Einheit

$a \in R$ heißt **invertierbar** (oder **Einheit**), falls $\exists\, b \in R$ mit $ab = ba = 1$.

1.2.19 Einheitengruppe

Die Menge $R^\times$ aller Einheiten von R bildet mit der Multiplikation eine Gruppe, die **Einheitengruppe** von R.

1.2.20 Körper

Ein kommutativer Ring $(K, +, \cdot)$ mit $1 \neq 0$ heißt **Körper**, wenn $K^\times = K \setminus \{0\}$, d. h. jedes Element $\neq 0$ ist invertierbar.

1.2.22 Nullteilerfreiheit

R heißt **nullteilerfrei**, wenn aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.

1.2.23 Lemma

Jeder Körper ist nullteilerfrei.

1.2.28 Satz (Matrizenring)

Sei R ein Ring, $n \in \mathbb{N}$. Dann ist $M_{n,n}(R)$ mit komponentenweiser Addition und Matrizenmultiplikation ein Ring.

1.2.30 Spur

Für $A = (a_{ij}) \in M_{n,n}(R)$: $\mathrm{Spur}(A) := \sum_{i=1}^{n} a_{ii}$.

1.2.31 Transponierte

Für $A = (a_{ij}) \in M_{m,n}(R)$: $A^\top = (a_{ji}) \in M_{n,m}(R)$. Es gilt $(AB)^\top = B^\top A^\top$.

1.3 Restklassenringe und endliche Körper

1.3.4 Restklasse

Für $a \in \mathbb{Z}$, $n \in \mathbb{N}$: $[a]_n := \{b \in \mathbb{Z} \mid n \mid (b - a)\}$. Die Menge aller Restklassen ist $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

1.3.11 Satz

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ mit $[a] + [b] := [a + b]$ und $[a] \cdot [b] := [ab]$ ist ein kommutativer Ring mit Eins.

1.3.14 Satz (Körperkriterium)

$\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine **Primzahl** ist. Man schreibt dann $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

1.3.17 Euklidischer Algorithmus

Berechnet $\mathrm{ggT}(a, n)$ durch wiederholte Division mit Rest. Falls $\mathrm{ggT}(a, p) = 1$, liefert er das multiplikative Inverse $[a]^{-1}$ in $\mathbb{F}_p$.

1.4 Polynomringe

1.4.1 Polynom

Ein **Polynom** über K ist ein formaler Ausdruck $f = a_0 + a_1 X + \cdots + a_n X^n$ mit $a_i \in K$. Der **Grad** ist $\deg(f) = \max\{i \mid a_i \neq 0\}$ (Konvention: $\deg(0) = -\infty$).

1.4.7 Lemma (Gradformel)

Für $f, g \in K[X]$ gilt $\deg(fg) = \deg(f) + \deg(g)$.

1.4.9 Satz

$K[X]$ ist mit Addition und Multiplikation von Polynomen ein kommutativer Ring.

1.4.11 Satz (Division mit Rest)

Zu $f, g \in K[X]$ mit $g \neq 0$ gibt es eindeutige $q, r \in K[X]$ mit $f = q \cdot g + r$ und $\deg(r) < \deg(g)$.

1.4.20 Nullstelle

$\lambda \in K$ heißt **Nullstelle** von $f \in K[X]$, wenn $f(\lambda) = 0$.

1.4.21 Abspaltungssatz

$\lambda \in K$ ist Nullstelle von $f \iff (X - \lambda) \mid f$.

1.4.24 Vielfachheit

Die **Vielfachheit** einer Nullstelle λ ist das maximale k mit $(X - \lambda)^k \mid f$.

1.4.30 Satz (Nullstellen)

Ein Polynom $f \in K[X]$ vom Grad n hat höchstens n Nullstellen (mit Vielfachheit gezählt).

1.4.40 Algebraisch abgeschlossen

Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes nicht-konstante Polynom $f \in K[X]$ mindestens eine Nullstelle in K hat. Äquivalent: Jedes f zerfällt in Linearfaktoren.

1.4.45 Ideal

Eine Teilmenge $I \subseteq K[X]$ heißt **Ideal**, wenn I eine additive Untergruppe ist und $fg \in I$ für alle $f \in K[X]$, $g \in I$.

1.4.49 Satz (Hauptideal)

Jedes Ideal $I \subseteq K[X]$ ist ein **Hauptideal**: $I = (g) = \{fg \mid f \in K[X]\}$ für ein $g \in K[X]$.

1.4.53 Größter gemeinsamer Teiler

Der **ggT** zweier Polynome f, g ist der normierte Erzeuger des Ideals $(f) + (g)$.

1.5 Der Körper der komplexen Zahlen

1.5.1 Komplexe Zahlen

$\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$. Man schreibt $z = a + bi$ mit $a = \mathrm{Re}(z)$, $b = \mathrm{Im}(z)$, $i^2 = -1$.

1.5.2 Satz

$\mathbb{C}$ ist ein Körper.

1.5.15–1.5.24 Rechnen in $\mathbb{C}$

- **Konjugation**: $\bar{z} = a - bi$; $\quad z\bar{z} = |z|^2 = a^2 + b^2$.
- **Betrag**: $|z| = \sqrt{a^2 + b^2}$.
- **Inverses**: $z^{-1} = \bar{z}/|z|^2$ für $z \neq 0$.
- **Polarform**: $z = |z|(\cos\varphi + i\sin\varphi)$; Multiplikation: $|z_1 z_2| = |z_1||z_2|$.

1.5.25 Fundamentalsatz der Algebra

$\mathbb{C}$ ist algebraisch abgeschlossen: Jedes nicht-konstante Polynom $f \in \mathbb{C}[X]$ besitzt eine Nullstelle in $\mathbb{C}$.