

Körper und Lineare Gleichungssysteme

Übersicht Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

Erinnerung: Wo stehen wir

Mengen

Abbildungen

Vollständige Induktion

Erinnerung: Wo stehen wir

Mengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

$\{1, 2, 3\}$, $\{x \in \mathbb{Q} ; x < 0\}$

Abbildungen

$f: X \rightarrow Y$, $f(S)$ Bild von $S \subseteq X$
 $f^{-1}(T)$ Urbild von $T \subseteq Y$

injektiv
surjektiv
bijektiv
Umkehrfunktion

Vollständige Induktion

$P(n)$ Aussage über $n \in \mathbb{N}$

IA $P(0)$
IS $P(n-1) \Rightarrow P(n)$ für alle $n \geq 1$ } $\Rightarrow P(n)$ für alle $n \in \mathbb{N}$.

Körper

keine Division durch 0



Idee: Zahlbereich, in dem die Grundrechenarten $+$, $-$, $\cdot$, $/$ zur Verfügung stehen

Körper

Idee: Zahlbereich, in dem die Grundrechenarten $+$, $-$, $\cdot$, $/$ zur Verfügung stehen und nach den üblichen Regeln funktionieren, zum Beispiel

$$x + y = y + x, \quad (x + y) \cdot z = x \cdot z + y \cdot z, \dots$$

Beispiele

$\mathbb{Q}$, $\mathbb{R}$, ...

$\mathbb{C}$
komplexe Zahlen

$\mathbb{F}_p$

endl. Kp. mit p Elementen
(p Primzahl)

Kein Körper $\mathbb{N}$, $\mathbb{Z}$

Lineare Gleichungssysteme

Abschnitt 5.1 im Skript

Lineare Gleichungssysteme

Vokabeln:

- Lineares Gleichungssystem (LGS), Koeffizienten
- Lösungsmenge
- homogen, inhomogen

Lineare Gleichungssysteme

K Körper ^{z.B.} $\mathbb{Q}, \mathbb{R}, \dots$

Vokabeln:

- Lineares Gleichungssystem (LGS), Koeffizienten
- Lösungsmenge
- homogen, inhomogen

Spaltenvektor

Addition und Skalarmultiplikation auf $K^n = \underbrace{K \times \dots \times K}_n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ; x_i \in K, i=1, \dots, n \right\}$

Matrizen

Körper

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

Axiome der Addition

Def Ein Körper ist eine Menge K

zusammen mit Abbildungen ("Verknüpfungen")

$$+ : K \times K \rightarrow K, \quad (a, b) \mapsto a + b,$$

$$\cdot : K \times K \rightarrow K, \quad (a, b) \mapsto a \cdot b, \quad \underline{\underline{\text{so dass}}}$$

(Assoziativgesetz)

$$(a + b) + c = a + (b + c) \quad \text{für alle } a, b, c \in K$$

(Kommutativgesetz)

$$a + b = b + a \quad \text{für alle } a, b \in K$$

(Neutrales Element)

Es gibt ein eind. bestimmtes Element $0 \in K$ ("Nullelement")
so dass $a + 0 = a = 0 + a$ für alle $a \in K$.

(Inverse Elemente)

Zu jedem $a \in K$ existiert $b \in K$ mit $a + b = 0$.

Axiome der Multiplikation

$$K, \quad + : K \times K \rightarrow K, \quad \cdot : K \times K \rightarrow K$$

$$0 \in K$$

(Assoziativgesetz) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in K$

(Kommutativgesetz) $a \cdot b = b \cdot a$ für alle $a, b \in K$

(Neutrales Element) Es existiert ein eindeutig bestimmtes Element $1 \in K$
so dass $1 \cdot a = a = a \cdot 1$ für alle $a \in K$.

(Inverse Elemente) Für jedes $a \in K \setminus \{0\}$ gibt es ein Element $b \in K$
mit $a \cdot b = 1 = b \cdot a$.

Weitere Axiome

- $0 \neq 1$

- Distributivgesetz

$$(a+b) \cdot c = a \cdot c + b \cdot c \quad \text{für alle } a, b, c \in K$$

Subtraktion und Division

$+$, $-$, $\cdot$, $/$

Wir sehen: zu $a \in K$ ist das additive Inverse b eindeutig bestimmt

$$a + b = 0$$

Wir schreiben

$$-a := b$$

↙ additives Inverses
von $a \in K$

$$c - d := c + (-d)$$

→ Subtraktion auf K

↑
Add. in K

$$K \times K \rightarrow K$$

Auch: zu $a \in K \setminus \{0\}$ ist das
multiplikative Inverse
eind. bestimmt, für $ab = 1$ schreibe $a^{-1} := b$,

Division: $\frac{c}{d} := c \cdot d^{-1} \quad (d \neq 0)$

Schreibweise:

$$K^\times = K \setminus \{0\}$$

Körperaxiome für K , $+: K \times K \rightarrow K$, $\cdot: K \times K \rightarrow K$

Addition	Assoziativgesetz:	$(a + b) + c = a + (b + c)$
	Kommutativgesetz:	$a + b = b + a$
	Neutrales Element 0:	$a + 0 = 0 + a = a$
	Inverses Element $-a$ zu a :	$a + (-a) = 0 = -a + a$
Multiplikation	Assoziativgesetz:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
	Kommutativgesetz:	$a \cdot b = b \cdot a$
	Neutrales Element 1:	$a \cdot 1 = 1 \cdot a = a$
	Inverses Element a^{-1} zu a :	$a \cdot a^{-1} = 1 = a^{-1} a$
		$0 \neq 1$
Distributivgesetz		$(a + b) \cdot c = ac + bc$

Beispiele : $\mathbb{Q}$, $\mathbb{R}$,

$\mathbb{C}$
komplexe Zahlen

$\mathbb{F}_p$
endliche Körper

kein Körper: $\mathbb{N}$, $\mathbb{Z}$

Körper: Rechenregeln

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

Erinnerung: Körperaxiome für K , $+: K \times K \rightarrow K$, $\cdot: K \times K \rightarrow K$

Addition	Assoziativgesetz:	$(a + b) + c = a + (b + c)$
	Kommutativgesetz:	$a + b = b + a$
	Neutrales Element 0:	$a + 0 = 0 + a = a$
	Inverses Element $-a$ zu a :	$a + (-a) = 0 = -a + a$
Multiplikation	Assoziativgesetz:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
	Kommutativgesetz:	$a \cdot b = b \cdot a$
	Neutrales Element 1:	$a \cdot 1 = 1 \cdot a = a$
	Inverses Element a^{-1} zu a :	$a \cdot a^{-1} = 1 = a^{-1} a$
		$0 \neq 1$
Distributivgesetz		$(a + b) \cdot c = ac + bc$

Konventionen

Klammern $(a + (b+c)) + d = (a + b) + (c+d) = \dots = a+b+c+d$

Punkt - vor Strichrechnung

- weglassen, falls nicht erforderlich

}

$$(a+b)c = \underline{a \cdot c} + \underline{b \cdot c}$$

Eindeutigkeit neutraler und inverser Elemente

Neutrale Elemente: Sind $e, e' \in K$ neutrale Elemente bezüglich $+$

$$\Rightarrow \begin{array}{ccc} e' & = & e + e' = e \\ \uparrow & & \uparrow \\ e \text{ neutr.} & & e' \text{ neutr.} \\ \text{Elem.} & & \text{Elem. f\"ur } + \end{array}$$

Sie $a \in K$. Dann ist das inverse Element von a bzgl. $+$ eindeutig bestimmt. Notation
 $-a$

Begründung: Sind $b, b' \in K$ mit $a+b=0$, $a+b'=0$, so gilt

$$b = b + 0 = b + (a + b') = \underbrace{(b+a)}_{= a+b=0} + b' = 0 + b' = b'.$$

Analog: $a \in K^\times := K \setminus \{0\}$. Dann ist das mult. Inverse von a eindeutig bestimmt. a^{-1}
 $(= \frac{1}{a})$

Lemma 4.7 im Skript

Kürzungsregeln

+ Sind $a, b, c \in K$ mit $a + c = b + c$, dann gilt $a = b$.

Begründung: $a + c = b + c \Rightarrow \underbrace{(a + c)}_a + (-c) = \underbrace{(b + c)}_b + (-c)$

• Sind $a, b, c \in K$, $c \neq 0$, mit $ac = bc$, so gilt $a = b$.

Begründung: $ac = bc \Rightarrow a = a \cdot \overset{\uparrow}{c} \cdot c^{-1} = b c c^{-1} = b$
 $c \neq 0$

Multiplikation mit 0

Sei $a \in K$. Dann gilt $0 \cdot a = 0$

Begründung: Es ist $\underbrace{0 \cdot a}_{= 0 + 0 \cdot a} = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$

$$\Rightarrow 0 = 0 \cdot a.$$

Sei $a \in K$. Dann gilt $\underbrace{-(-a)}_{= a} = a$, denn $-a + a = 0$.

Auch: $\underbrace{(-1)}_{= -1} \cdot a = -a : (-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = \underbrace{(-1+1)}_{= 0} \cdot a = 0.$

Weiteres

"Nullteilerfreiheit" Sind $a, b \in K$ mit $ab = 0$, dann gilt $a = 0$ oder $b = 0$.

Begründung: Sei $ab = 0$, und sei $a \neq 0$.

$$\text{Dann folgt } b = \underbrace{a^{-1}a}_{=1} b = \underbrace{a^{-1} \cdot 0}_{ab} = 0.$$

Binomische Formeln: $(x+y)^2 = (x+y)(x+y)$

$$= (x+y)x + (x+y)y = x^2 + \underbrace{xy + xy}_{(1+1) \cdot xy} + y^2$$
$$=: 2_K = 2$$

Potenzen

$$\left\{ \begin{array}{l} n \in \mathbb{N}, a \in K, \\ a^n = \underbrace{a \cdot \dots \cdot a}_{i \text{ Faktoren}} = \prod_{i=1}^n a \\ a^0 = 1, a^1 = a, a^2 = a \cdot a, \dots \end{array} \right.$$

Abschnitt 4.1.3 im Skript

Summen- und Produktsymbol



$$\sum_{i=0}^n a_i = a_0 + a_1 + \dots + a_n$$

Für $n \in \mathbb{N}$ schreibe

$$n_K := \underbrace{1 + \dots + 1}_{n \text{ Summanden}} \in K$$

$$(0_K = 0 \in K)$$

$$1_K = 1 \in K$$

$$2_K = 1+1$$

$$3_K = 1+1+1$$

$\vdots$

$$(-n)_K = -n_K$$

$$\prod_{i=0}^n a_i$$

$$\sum_{i \in I} a_i, \quad I \text{ endliche Menge}$$

Was im allgemeinen nicht zur Verfügung steht

- ~~$a < b$~~

- ~~Grenzwerte, unendliche Summen/Reihen, f' , $\int f(x) dx$~~

Der Körper der komplexen Zahlen

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

Die komplexen Zahlen

Suche Erweiterungskörper von $\mathbb{R}$, in dem ein Element i mit der Eigenschaft $i^2 = -1$ ex.

Sei $\mathbb{C} = \mathbb{R}^2 = \{(a, b); a, b \in \mathbb{R}\}$ die Menge aller Paare von reellen Zahlen.

Definiere Addition $(a, b) + (c, d) := (a+c, b+d)$

Multiplikation $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$

Betrachte $\mathbb{R} \xrightarrow{\iota} \mathbb{C}, a \mapsto (a, 0)$.

$$(a, 0) + (c, 0) = (a+c, 0)$$

$$(a, 0) \cdot (c, 0) = (ac, 0)$$

$\leadsto$ können $\mathbb{R}$ identifizieren

mit $\{(a, 0); a \in \mathbb{R}\} \subseteq \mathbb{C}$

verhlt sich mit Add u. Mult. auf $\mathbb{R}$ und $\mathbb{C}$

$\begin{matrix} \uparrow & \uparrow & \uparrow \\ & & \text{Add./Mult. in } \mathbb{R} \end{matrix}$

Beispiel 4.5 im Skript

Die komplexen Zahlen

$$(a,b) + (c,d) = (a+c, b+d)$$

$$(a,b) \cdot (c,d) = (ac-bd, ad+bc)$$

$$\bullet (a,b) + (0,0) = (a,b)$$

(und mittels Identifikation $\mathbb{R} = \{(a,0), a \in \mathbb{R}\} \subseteq \mathbb{C}$)

$$a \stackrel{""}{=} (a,0) \quad \bullet$$

$$\rightarrow (0,0) = 0$$

$$\bullet (a,b) \cdot (1,0) = (a,b)$$

$$1 = 1_{\mathbb{C}} = 1_{\mathbb{R}} = (1,0)$$

$$\bullet (0,1)^2 = (0,1) \cdot (0,1) = (-1,0) = -1$$

$$\underbrace{(-1,0)}_{-1} + \underbrace{(1,0)}_{1_{\mathbb{C}}} = (0,0) = 0_{\mathbb{C}}$$

$$\downarrow$$

$$-1 \in \mathbb{C}$$

Definiere $i := (0,1) \in \mathbb{C}$ ($i \notin \mathbb{R}$)

Dann können wir schreiben

$$(a,b) = (a,0) + (0,b) = a + bi$$

a "Realteil" b "Imaginärteil" $\circledast$ $\circledast$

Königsplatz 11.11.2020

Beispiel 4.5 im Skript

$$b \cdot i = (b,0) \cdot (0,1) = (0,b)$$

Quiz

Berechnen Sie in $\mathbb{C}$:

$$\underline{2} + \underline{i} + \underline{(3 - 2i)} = ? \quad 5 - i$$

$$\underbrace{(1+i)(1-i) = 1 - i^2 = 2}$$

$$\| (1+i)(1-i) = ? \quad (1+i)1 - (1+i)i = \underline{1+i-i-i^2} = 2$$

$$1+i = \frac{2}{1-i}$$

$$i^3 = ? \quad i \cdot i \cdot i = -i$$

$$i^{-1} = ? \quad \text{muss gelten: } i^{-1} \cdot i = 1. \quad \text{Es ist } i \cdot i = -1, \\ \text{also } \underline{-i \cdot i = 1}, \text{ also } i^{-1} = -i$$

$$\frac{2}{1-i} = ?$$

$$\frac{2}{1-i} = \frac{2(1+i)}{(1-i)(1+i)} = \frac{2+2i}{2} = 1+i.$$

$$a + b \cdot i$$

Die komplexen Zahlen

$\mathbb{C}$ ist ein Körper

Assoziativgesetze $+$, $\cdot$
Kommutativgesetze $+$, $\cdot$
Distributivgesetz

✓ Neutralemente $+$ $0 = (0, 0)$
 $\cdot$ $= 0 + 0i$
 $1 = (1, 0) = 1 + 0i$

$0 \neq 1$ ✓

Inversen Elemente $+$
 $\cdot$

nachrechnen (langweilig)
oder später

Inversen Element von $a + bi$ bzgl. $+$: $-a - bi$

Inversen Element von $a + bi \in \mathbb{C} \setminus \{0\}$ bzgl. $\cdot$ ($a + bi \neq 0 \Leftrightarrow \underbrace{a \neq 0 \text{ oder } b \neq 0}$)

Idee: $\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2}$

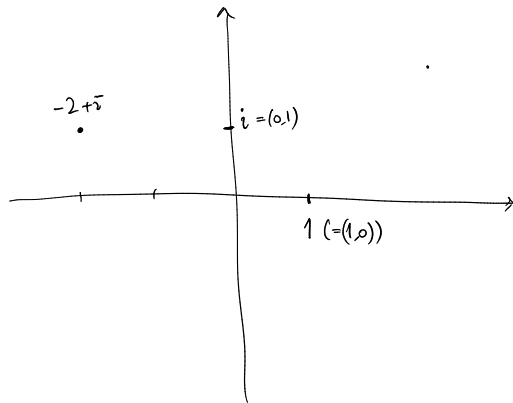
Das Inverse von $a + bi$ ($\neq 0$) ist

$$\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i$$

$\Downarrow$
 $a^2+b^2 \neq 0$

Komplexe Zahlenebene

$$\mathbb{C} = \mathbb{R}^2 \quad \text{als Menge}$$



Endliche Körper

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

$$\mathbb{F}_2 = \{0, 1\}$$

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

$$\mathbb{F}_3 = \{0, 1, a\}$$

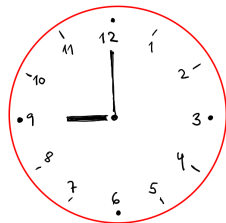
⋮

Rechnen mit Restklassen

$$\mathbb{Z}/n = \{\overline{0}, \dots, \overline{n-1}\}$$

$$n = 12$$

$$\overline{9} + \overline{6} = \overline{3}$$



6 Std. nach 9 Uhr
ist 3 Uhr

Quiz

Berechnen Sie

$$\text{in } \mathbb{Z}/11: \bar{7} + \bar{9} = ? \quad \bar{5} \in \mathbb{Z}/11$$

$$\text{in } \mathbb{Z}/16: \bar{7} + \bar{9} = ? \quad \bar{0} \in \mathbb{Z}/16$$

$$\text{in } \mathbb{Z}/11: \bar{7} \cdot \bar{9} = ? \quad \bar{8} \in \mathbb{Z}/11$$

$$\text{in } \mathbb{Z}/8: \underbrace{\bar{2} \cdot \bar{2} \cdot \bar{2}} \cdot \bar{7} = ? \quad \bar{0} \in \mathbb{Z}/8$$

Werden sehen,

für n Primzahl

ist $\mathbb{Z}/n$ ein Körper

Die kanonische Projektion $(\pi): \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$

Definiere Abbildung $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$

$$a \mapsto \overline{r}$$

r der Rest bei Division
von a durch n

Damit $\overline{a} + \overline{b} = \pi(a+b)$

$$\overline{a} \cdot \overline{b} = \pi(ab)$$

(schreibe $a = q \cdot n + r$
mit $q \in \mathbb{Z}$, $r \in \mathbb{Z}$,
 $0 \leq r \leq n-1$)

Bem. $\pi(a) = \pi(b) \Leftrightarrow a, b$ haben selben
Rest bei Division durch n

$$\Leftrightarrow a-b \text{ ist ein Vielfaches von } n$$

Die kanonische Projektion $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$

Lemma Für alle $x, y \in \mathbb{Z}$ gilt:

$$\pi(x+y) = \pi(x) + \pi(y), \quad \pi(xy) = \pi(x) \cdot \pi(y).$$

↑
Add in $\mathbb{Z}$

↑
Add in
 $\mathbb{Z}/n$

↑
Mult.
in $\mathbb{Z}$

↑
Mult. in
 $\mathbb{Z}/n$

Beweis Schreibe $x = qn + r, \quad 0 \leq r \leq n-1$
 $y = un + s, \quad 0 \leq s \leq n-1$

$$\text{Dann gilt} \quad \pi(x+y) = \pi((\underbrace{q+u}n) + r+s) = \pi(r+s) = \bar{r} + \bar{s} = \pi(x) + \pi(y)$$

$$\begin{aligned} \pi(xy) &= \pi((qn+r)(un+s)) = \pi(\underbrace{n(qun+qs+ur)} + rs) = \pi(rs) \\ &= \bar{r} \cdot \bar{s} = \pi(x) \cdot \pi(y). \end{aligned}$$

Die kanonische Projektion $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$

Lemma

$$\pi(x + y) = \pi(x) + \pi(y), \quad \pi(xy) = \pi(x) \cdot \pi(y).$$

Körperaxiome für $\mathbb{Z}/n\mathbb{Z}$

$$\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n$$

Assoziativgesetz für $+$: Seien $x, y, z \in \mathbb{Z}/n$, $\dot{x}, \dot{y}, \dot{z} \in \mathbb{Z}$ mit
 $\pi(\dot{x}) = x, \pi(\dot{y}) = y, \pi(\dot{z}) = z$

$$(x + y) + z = (\pi(\dot{x}) + \pi(\dot{y})) + \pi(\dot{z}) \stackrel{L}{=} \pi(\dot{x} + \dot{y}) + \pi(\dot{z})$$

$$\stackrel{L}{=} \pi((\dot{x} + \dot{y}) + \dot{z}) = \pi(\dot{x} + (\dot{y} + \dot{z})) \stackrel{L}{=} \pi(\dot{x}) + \pi(\dot{y} + \dot{z})$$

$\uparrow$
Ass₊ in $\mathbb{Z}$

$$\stackrel{L}{=} \pi(\dot{x}) + (\pi(\dot{y}) + \pi(\dot{z})) = x + (y + z)$$

Genauso: Kommutativges. $+$, Assoziativges. $\cdot$, Komm-ges. $\cdot$, Distributivges.

Neutrale Elem: $\bar{0} + \bar{a} = \bar{a}, \quad \bar{1} \cdot \bar{a} = \bar{a}.$

Inverse Elem bzgl. $+$: $a = \pi(\dot{a})$, dann $a + \pi(-\dot{a}) = \pi(\dot{a}) + \pi(-\dot{a}) = \pi(0) = \bar{0}$

$\rightarrow \pi(-\dot{a})$ add. Inverse von $a = \pi(\dot{a})$ (oder $-\bar{a} = \overline{n-a} \quad (a \neq 0)$)

Körperaxiome für $\mathbb{Z}/n\mathbb{Z}$?

Quiz: Multiplikative Inverse

Rechnen Sie

$$\text{in } \mathbb{Z}/13\mathbb{Z}: \bar{4} \cdot \bar{10} = ? \quad \bar{1}$$

$$\text{in } \mathbb{Z}/7\mathbb{Z}: \bar{2}^{-1} = ? \quad \bar{2} \cdot \bar{4} = \bar{1}, \text{ also } \bar{2}^{-1} = \bar{4} \text{ in } \mathbb{Z}/7$$

$$\text{in } \mathbb{Z}/p\mathbb{Z} \ (p \text{ ungerade Primzahl}): \cancel{\frac{1}{2}} = ? \quad \frac{\bar{1}}{\bar{2}} = \overline{\frac{p+1}{2}} \left\{ \in \{1, \dots, p-1\} \right\} \in \mathbb{Z}/p$$

$$\text{in } \mathbb{Z}/14\mathbb{Z}: \bar{2} \cdot \bar{7} = ? \quad \bar{0}$$

(obwohl $\bar{2}, \bar{7} \neq \bar{0} \rightarrow \mathbb{Z}/14$ kein Körper)

allgemein: n keine Primzahl $\Rightarrow \mathbb{Z}/n$ kein Körper

Die Primeigenschaft

Sei p eine Primzahl

Dann gilt: Sind $a, b \in \mathbb{Z}$ und ist p ein Teiler von ab ,
dann ist p ein Teiler von a oder ein Teiler von b .

Bsp 6 ist ein Teiler von $3 \cdot 4$.

$\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p

Sei $a \in \mathbb{Z}/p \setminus \{\bar{0}\}$. Wollen zeigen: es existiert $b \in \mathbb{Z}/p$ mit $ab = \bar{1}$.

Genügt: die Abb. $m_a: \mathbb{Z}/p \rightarrow \mathbb{Z}/p, x \mapsto ax$, ist surjektiv

Dann genügt zz: m_a injektiv.

(denn $m_a(x) = \bar{1}$
bedeutet $ax = \bar{1}$)

Gelte also $m_a(x) = m_a(y), x, y \in \mathbb{Z}/p$

Das bedeutet $ax = ay$, also $a(x-y) = \bar{0}$

Schreibe $a = \pi(\tilde{a}), x = \pi(\tilde{x}), y = \pi(\tilde{y}), \tilde{a}, \tilde{x}, \tilde{y} \in \mathbb{Z}$

Dann $a \neq \bar{0} \in \mathbb{Z}/p \Leftrightarrow \tilde{a}$ kein Vielf. von p

$a(x-y) = \bar{0} \Leftrightarrow \underbrace{\tilde{a}(\tilde{x}-\tilde{y})}_{\text{ist Vielfaches von } p}$

$\left. \begin{array}{l} \Rightarrow \tilde{x}-\tilde{y} \text{ Vielf. von } p \\ \text{Primteiler} \end{array} \right\} \Rightarrow$

$\Downarrow$
 $\pi(\tilde{x}) = \pi(\tilde{y})$
 $\Downarrow$
 $x = y$

$\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p

Bemerkungen

Schreibweisen: $\mathbb{Z}/p$

- $\mathbb{F}_p$ statt $\mathbb{Z}/p\mathbb{Z}$ für p Primzahl
- $[a]$ oder einfach a statt $\bar{a}$

Bemerkungen

Schreibweisen:

- $\mathbb{F}_p$ statt $\mathbb{Z}/p\mathbb{Z}$ für p Primzahl
- $[n]$ oder einfach n statt $\bar{n}$.

Achtung: Es gibt einen Körper mit 4 Elementen, aber $\mathbb{Z}/4$ ist kein Körper (denn $2 \cdot 2 = 0$ in $\mathbb{Z}/4$).

Lineare Gleichungssysteme

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

Quiz: Lineare Gleichungssysteme

Bestimmen Sie die Lösungsmenge des linearen Gleichungssystems über $\mathbb{Q}$:

$$3X_1 + 2X_2 = 2$$

$$-2X_1 + X_2 = 4$$

$$\mathbb{L} = \left\{ \left(-\frac{6}{7}, \frac{16}{7} \right) \right\}$$

Bestimmen Sie die Lösungsmenge des linearen Gleichungssystems über $\mathbb{F}_7$:

$$3X_1 + 2X_2 = 2$$

$$-2X_1 + X_2 = 4$$

$$\mathbb{L} = \emptyset$$

Sei K ein Körper, seien m, n natürliche Zahlen. Ein *lineares Gleichungssystem (LGS)* von m Gleichungen in n Unbestimmten $X_1, \dots, X_n$ über K ist gegeben durch m Gleichungen

1. Gleichung $\rightarrow$

$$a_{11}X_1 + a_{12}X_2 + \dots + a_{1n}X_n = b_1$$

$\vdots$

$$a_{21}X_1 + a_{22}X_2 + \dots + a_{2n}X_n = b_2$$

$\vdots$

$\vdots$

m -te Gleichung

$$a_{m1}X_1 + a_{m2}X_2 + \dots + a_{mn}X_n = b_m$$

mit $a_{ij} \in K$ für alle $i = 1, \dots, m$, $j = 1, \dots, n$, $b_i \in K$, $i = 1, \dots, m$.

$\uparrow$ Koeffizienten
(von X_j in der i -ten Gl.)

Lösungsvektor $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (x_1, \dots, x_n)^t \in K^n$ so dass

$$a_{i1}x_1 + \dots + a_{in}x_n = b_i \quad \text{für alle } i = 1, \dots, m$$

Lösungsmenge: Menge aller Lösungsgesamtheiten $\in K^n$

Sei K ein Körper, seien m, n natürliche Zahlen. Ein *lineares Gleichungssystem (LGS)* von m Gleichungen in n Unbestimmten $X_1, \dots, X_n$ über K ist gegeben durch m Gleichungen

$$a_{11}X_1 + a_{12}X_2 + \dots + a_{1n}X_n = b_1$$

$$a_{21}X_1 + a_{22}X_2 + \dots + a_{2n}X_n = b_2$$

$$\vdots \quad \quad \quad \vdots$$

$$a_{m1}X_1 + a_{m2}X_2 + \dots + a_{mn}X_n = b_m$$

homogen

alle $b_i = 0$

inhomogen

nicht alle $b_i = 0$

mit $a_{ij} \in K$ für alle $i = 1, \dots, m, j = 1, \dots, n, b_i \in K, i = 1, \dots, m$.

lösbar : $\mathbb{L} \neq \emptyset$,
↑ Lösungsmenge

eindeutig lösbar : $\mathbb{L}$ hat genau
ein Element

Jedes homogene LGS hat die triviale Lösung $(0, \dots, 0)^t$.

Sei $K = \mathbb{R}$. Wir betrachten als Beispiel das folgende Gleichungssystem:

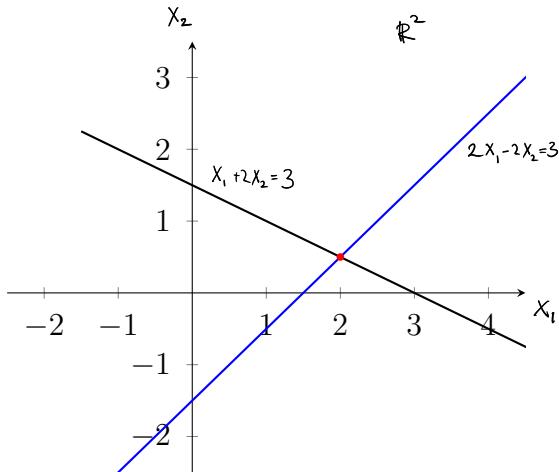
$$2X_1 - 2X_2 = 3$$

(blaue)
Gerade
in $\mathbb{R}^2$

$$X_1 + 2X_2 = 3$$

(schwarze)
Geraden

$$\mathbb{L} = \left\{ \left(2, \frac{1}{2} \right)^t \right\}.$$



Quiz

Finden Sie LGS mit

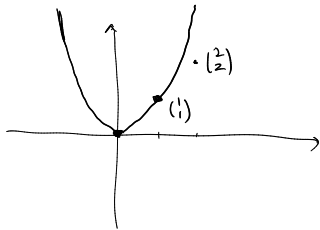
- Lösungsmenge $\{0\}$,

- Lösungsmenge K^n ,

- $(K = \mathbb{R})$, Lösungsmenge $\{(2x, 4x - 1)^t; x \in \mathbb{R}\}$, $\in \mathbb{R}^2$ $\perp$ $2x_1 - x_2 = 1$

- $(K = \mathbb{R})$, Lösungsmenge $\{(x, x^2)^t; x \in \mathbb{R}\}$, $\in \mathbb{R}^2$

ist nicht Lösungsmenge
eines LGS sein



$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ Lösung

↓

$\begin{pmatrix} 2 \\ 2 \end{pmatrix}$ Lösung

$X_1 = 0$ hat Lösungsmenge $\{0\} \subset K$

n Unbestimmte

$$0 \cdot X_1 + \dots + 0 \cdot X_n = 0$$

Rechnen in K^n und Matrizen

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

K^n K Körper,

$$K^n = K \times \dots \times K = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}; x_1, \dots, x_n \in K \right\}$$

Addition $+: K^n \times K^n \rightarrow K^n$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

Skalar multiplication

$$\cdot: K \times K^n \rightarrow K^n$$

Skalar = Element
von K

$$a \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} ax_1 \\ \vdots \\ ax_n \end{pmatrix}$$

$\begin{matrix} a \in K \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \end{matrix}$

Spaltenvektor

$$\psi \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \text{ "Nullvektor"} \\ = (0, \dots, 0)^t$$

Assoziativgesetz,

Kommutativgesetz

Neutrales Element $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = 0$

Inverse Element $(x_1, \dots, x_n)^t + (-x_1, \dots, -x_n)^t \\ = (0, \dots, 0)^t$

$$(a \cdot b) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = a \left(b \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right)$$

Distributivgesetz

$$1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Quiz

Berechnen Sie

in $\mathbb{Q}^2$:

$$\begin{pmatrix} 1 \\ 4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1/2 \end{pmatrix} = ? \quad \begin{pmatrix} 1+1 \\ 4+\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 2 \\ 9\frac{1}{2} \end{pmatrix}$$

in $\mathbb{C}^2$:

$$\begin{pmatrix} 0 \\ i \end{pmatrix} + \begin{pmatrix} 1-i \\ 1 \end{pmatrix} = ? \quad \begin{pmatrix} 0 \\ i \end{pmatrix} + \begin{pmatrix} i+1 \\ i \end{pmatrix} = \begin{pmatrix} 1+i \\ 2i \end{pmatrix}$$

in $\mathbb{F}_3^2$:

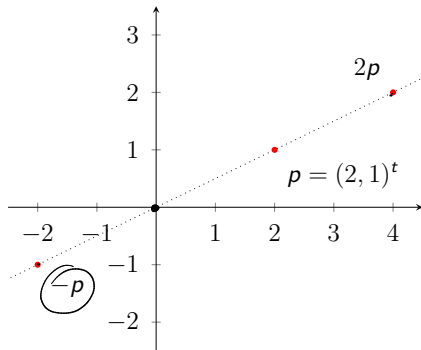
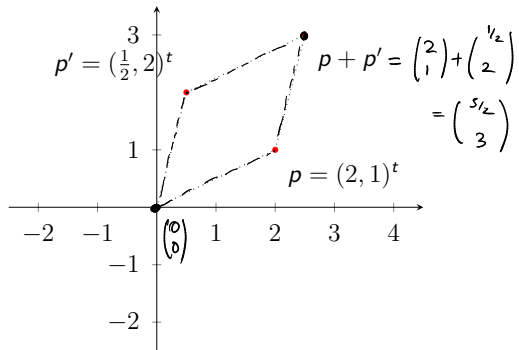
$$\mathbb{F}_3 = \{ \bar{0}, \bar{1}, \bar{2} \}$$

$\parallel$
 $1+1$

$1+2=0$
 $-2=1$
 $-1=2$

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} - \begin{pmatrix} 2 \\ 1 \end{pmatrix} = ? \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} -2 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

$\nwarrow$
 $x, y \in K^n, \quad x-y := x+(-y)$

$\mathbb{R}^2$ 

Matrizen

$$\text{Matrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & -1 & -2 & -3 \end{pmatrix} \in M_{3 \times 4}(\mathbb{Q})$$

Matrizen

K Körper

Definition (Matrix)

Seien $\underline{m}, \underline{n}$ natürliche Zahlen. Eine *Matrix* der Größe $m \times n$ über K ist eine Familie $(a_{ij})_{i=1, \dots, m, j=1, \dots, n}$ von Elementen von K . Die Elemente a_{ij} heißen die *Einträge* oder *Koeffizienten* der Matrix. Eine Matrix stellen wir uns immer in der Form vor:

m Anzahl Zeilen
 n Anzahl Spalten

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & \widehat{a_{1n}} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Lineare Gleichungssysteme und Matrizen

$$a_{11}X_1 + \dots + a_{1n}X_n = b_1$$

$\vdots$

$$a_{m1}X_1 + \dots + a_{mn}X_n = b_m$$

$\rightarrow$

Koeffizientenmatrix

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

$m \times n$ -Matrix

Menge aller $(m \times n)$ -Matrizen über K :

$$M_{m \times n}(K) (= \text{Mat}_{m \times n}(K) = K^{m \times n})$$

Quadratisch: $m = n$

statt $M_{n \times n}(K)$ schreibe $M_n(K)$

Erweiterte Koeffizientenmatrix

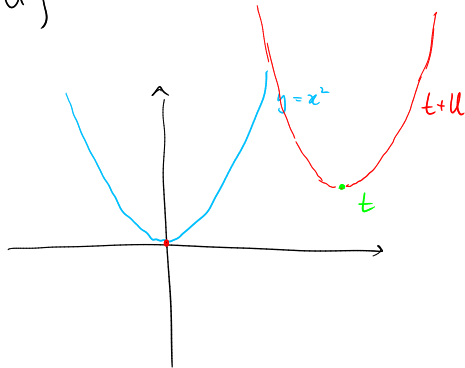
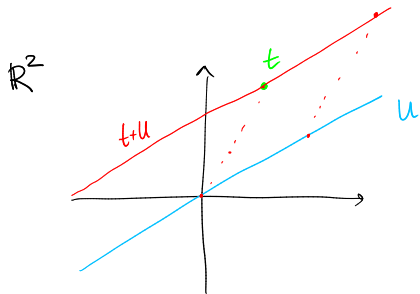
$$\left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right)$$

Lineare Gleichungssysteme und Matrizen

K Körper

$U \subseteq K^n$ Teilmenge, $t \in K^n$

Schreibe $t + U = \{ t + u ; u \in U \}$



Lösungsmenge inhomogenes/zugeh. homogenes LGS

LGS mit erw. Koeff. matrix

$$\left(\begin{array}{c|c} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{array} \middle| \begin{array}{c} b_1 \\ \vdots \\ b_m \end{array} \right)$$

→ zugeh. homogenes LGS ist das LGS mit erw. Koeff.-matrix

$$\left(\begin{array}{c|c} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{array} \middle| \begin{array}{c} 0 \\ \vdots \\ 0 \end{array} \right)$$

↑
alles Null $\hat{=}$ homogen

Lösungsmenge inhomogenes/zugeh. homogenes LGS

Satz

Seien K ein Körper, $A \in M_{m \times n}(K)$ und $b \in (K^m)$

$\mathbb{L}$ die Lösungsmenge des LGS $(A \mid b)$,

$\mathbb{L}_0$ die Lösungsmenge des zugeh. homogenen LGS $(A \mid 0)$.

Ist $t \in \mathbb{L}$, so gilt $\mathbb{L} = t + \mathbb{L}_0$.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

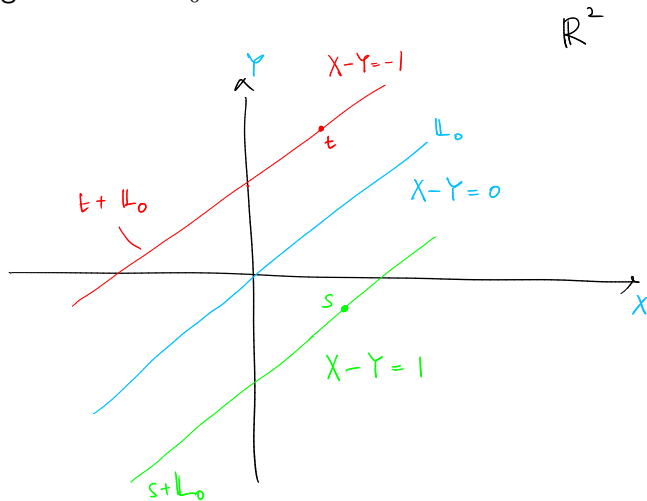
$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

Beweis Zunächst: $x \in t + \mathbb{L} \Leftrightarrow \exists u \in \mathbb{L}: x = t + u \Leftrightarrow \exists u \in \mathbb{L}: u = x - t$
 $(x, t \in K^n, u \in K^n)$
 $\Leftrightarrow x - t \in \mathbb{L}$

Also Aussage des Satzes $\Leftrightarrow x \in \mathbb{L} \Leftrightarrow x - t \in \mathbb{L}_0$

Aber $x \in \mathbb{L} \Leftrightarrow \forall i=1, \dots, m: \sum_{j=1}^n a_{ij} x_j = b_i$
 $(x_1, \dots, x_n)^t$
 $\Leftrightarrow \sum_{j=1}^n a_{ij} t_j$
 $\Leftrightarrow \sum_{j=1}^n a_{ij} (x_j - t_j) = 0$
 $\Leftrightarrow x - t \in \mathbb{L}_0$

Ist $t \in \mathbb{L}$, so gilt $\mathbb{L} = t + \mathbb{L}_0$.



Polynomfunktionen

Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra I, WS 20/21



Essen Seminar for Algebraic
Geometry and Arithmetic

UNIVERSITÄT
DUISBURG
ESSEN

Definition Polynomfunktion

Sei K ein Körper.

$$\begin{aligned} f: K &\rightarrow K \\ x &\mapsto 2x^3 - x^2 + 1 \end{aligned}$$

$$2 := 1+1 \in K$$

Definition Polynomfunktion

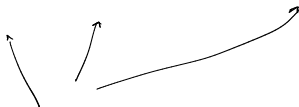
Sei K ein Körper.

Def Eine Polynomfunktion ist eine Abb. $f: K \rightarrow K$, so dass $n \geq 0$

und $a_0, a_1, \dots, a_n \in K$ existieren mit

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \left(= \sum_{i=0}^n a_i x^i \right)$$

für alle $x \in K$.


Koeffizienten

$a \in K$ heißt Nullstelle von f , wenn $f(a) = 0$.

Polynomdivision

/Q

$$(X^3 + X^2 - 1) : (X-1) = X^2 + 2X + 2, \text{ Rest } 1$$
$$\begin{array}{r} - (X^3 - X^2) \\ \hline \end{array}$$

$$\begin{array}{r} 2X^2 - 1 \\ - (2X^2 - 2X) \\ \hline +2X - 1 \\ - (2X - 2) \\ \hline \cdot 1 \\ \hline \end{array}$$

das bedeutet

$$X^3 + X^2 - 1 = (X^2 + 2X + 2)(X-1) + 1$$

↑
Rest,
höchste Potenz
von $X <$ als
höchste Potenz
in Divisor

Quiz: Nullstellen von Polynomfunktionen

Bestimmen Sie die Nullstellen von

$$f: \mathbb{Q} \rightarrow \mathbb{Q}, f(x) = x^2 - 5x + 6,$$

← Nullstellen 2, 3

$$g: \mathbb{C} \rightarrow \mathbb{C}, g(x) = x^2 - 2x + 2,$$

← Nullstellen $1-i$, $1+i$

$$h: \mathbb{Q} \rightarrow \mathbb{Q}, h(x) = x^3 - 3x^2 + 3x - 2$$

Nullstelle 2

$$(x^3 - 3x^2 + 3x - 2) : (x-2) = \boxed{x^2 - x + 1}$$

← hat keine Nullstellen in $\mathbb{Q}$

$$\boxed{} \cdot (x-2) + \text{Rest} = x^3 - 3x^2 + 3x - 2 \Rightarrow$$

für $x=2$

↓
0

↓
Rest=0

↓
0

Nullstellen von
 $x^3 - 3x^2 + 3x - 2$

sind 2 und
Nullstellen von $\boxed{}$

Nullstellen von Polynomfunktionen

Satz Sei K ein Körper, $f: K \rightarrow K$ eine Polynomfunktion,

es gelte
$$f(x) = \sum_{i=0}^n a_i \cdot x^i \quad \text{für alle } x \in K$$

mit $n \geq 0$, $a_0, \dots, a_n \in K$. Es sei mindestens ein $a_i \neq 0$.

Dann hat f höchstens n verschiedene Nullstellen in K .