Lineare Algebra II

Sommersemester 2016

Mohamed Barakat

Department Mathematik, Universität Siegen
mohamed.barakat@uni-siegen.de

Stand: 26. August 2016

Vorwort

Dies ist die geTEXte Version meiner Vorlesungsnotizen, die ich fortlaufend aktualisieren werde. Habt bitte Verständnis dafür, wenn Stand der Vorlesung und der Notizen nicht immer übereinstimmen werden. Daher gilt: Kommt zur Vorlesung und macht Eure eigenen Notizen. *Die sind sowieso besser als jedes Skript*. Die Form eines Skriptes erreichen diese Notizen vermutlich erst gegen Ende der Vorlesung, dies kann ich aber nicht garantieren. Die aktuelle Version ist unter der folgenden Adresse zu finden:

http://www.mathematik.uni-kl.de/~barakat/Lehre/SS15/LAII/Skript/LAII.pdf

Als Vorlage benutz(t)e ich das online-verfügbare Skript von Prof. Gabriele Nebe:

http://www2.math.rwth-aachen.de:8079/LAII.pdf

und ihr LA I Skript, das mir Frau Nebe freundlicherweise zur Verfügung gestellt hat.

Für Korrektur- und Verbesserungsvorschläge bin ich stets dankbar
mohamed.barakat@uni-siegen.de

Inhaltsverzeichnis

Kapitel 0

Grundlagen

Hier sammeln wir alles, was sonst zur LA I gehört.

Schreibweise.

- K steht immer für einen Körper.
- $\mathcal{V}$ und $\mathcal{U}$ stehen immer für K-Vektorräume.
- $\mathcal{U} \leq \mathcal{V}$ bedeutetet, dass $\mathcal{U}$ ein Teilraum = Untervektorraum von $\mathcal{V}$ ist.

1 Restklassenräume und Homomorphiesatz

Definition 0.1. Sei $\mathcal{V}$ ein K-Vektorraum. Eine Äquivalenzrelation $\sim$ auf $\mathcal{V}$ heißt **verträglich** mit der Vektorraumstruktur oder einfach **linear** oder **Kongruenz**, falls aus $X \sim X'$ und $Y \sim Y'$ für $X, X', Y, Y' \in \mathcal{V}$ und $a, b \in K$ folgt $aX + bY \sim aX' + bY'$. Statt von einer Äquivalenzklasse reden wir in diesem Zusammenhang von **Restklasse**.

Beispiel 0.2.

1. Ist $\varphi : \mathcal{V} \to \mathcal{W}$ linear und $\sim_\varphi$= "Bildgleichheit bez. φ", so ist $\sim_\varphi$ eine Kongruenz.
2. Ist $\mathcal{U} \leq \mathcal{V}$ ein Teilraum von $\mathcal{V}$, so ist $\sim_\mathcal{U}$ eine Kongruenz definiert durch:

$$X \sim_\mathcal{U} Y :\iff X - Y \in \mathcal{U}.$$

Lemma 0.3. *Ist $\sim$ eine Kongruenz auf dem K-Vektorraum $\mathcal{V}$, so gilt:*

1. *Die Restklasse $[0]$ des Nullelementes ist ein Teilraum $\mathcal{U}$ von $\mathcal{V}$; $[0] =: \mathcal{U} \leq \mathcal{V}$.*
2. *$\sim = \sim_\mathcal{U}$ aus dem letzten Beispiel.*
3. *Für alle $X \in \mathcal{V}$ gilt für die Restklasse von X*

$$[X] = X + \mathcal{U} := \{X + U \mid U \in \mathcal{U}\}.$$

Beweis.

1. $[0] \neq \emptyset$, da $0 \in [0]$. Sind $X, Y \in [0]$ und $a, b \in K$, dann folgt $X \sim 0$ und $Y \sim 0$, also wegen der Verträglichkeit $aX + bY \sim a0 + b0 = 0$, d. h. $aX + bY \in [0]$.
2. Sei $\mathcal{U} := [0]$. Behauptung: Für $X, Y \in \mathcal{V}$ sind äquivalent: $X \sim Y$ und $X - Y \in \mathcal{U}$. Dies ist klar, da wegen der Verträglichkeit $X \sim Y$ äquivalent zu $X - Y \sim 0$ ist.

3. $Z \in X + \mathcal{U}$ ist äquivalent zu $Z = X + U$ für ein $0 \sim U$. Dies bedeutet wegen der Verträglichkeit, dass $Z \sim X$ ist, d. h. $Z \in [X]$. Die umgekehrte Inklusion ist eine Übung. □

Satz 0.4. *Sei $\mathcal{U} \leq \mathcal{V}$ ein Unterraum des K-Vektorraumes $\mathcal{V}$ und $\sim := \sim_{\mathcal{U}}$ die zugehörige Kongruenz. Die Menge $\mathcal{V}/\sim$ der Restklassen wird mit $\mathcal{V}/\mathcal{U}$ (lies $\mathcal{V}$ modulo $\mathcal{U}$ oder $\mathcal{V}$ nach $\mathcal{U}$) bezeichnet. Die Elemente von $\mathcal{V}/\mathcal{U}$ heißen auch* **Restklassen nach** *$\mathcal{U}$ und $\mathcal{V}/\mathcal{U}$ heißt auch* **Faktorraum**, **Quotientenraum** *oder* **Restklassenraum** *von $\mathcal{V}$ nach $\mathcal{U}$.*

1. *$\mathcal{V}/\mathcal{U}$ wird mit der wohldefinierten Addition*

$$(X + \mathcal{U}) + (Y + \mathcal{U}) := (X + Y) + \mathcal{U} \text{ für alle } X, Y \in \mathcal{V}$$

und Multiplikation

$$a(X + \mathcal{U}) := aX + \mathcal{U} \text{ für alle } X \in \mathcal{V}, a \in K$$

zu einem K-Vektorraum.

2. *Die Abbildung*

$$\nu : \mathcal{V} \to \mathcal{V}/\mathcal{U} : X \mapsto X + \mathcal{U}$$

ist eine lineare Abbildung, genannt der **natürliche Epimorphismus** *von $\mathcal{V}$ auf $\mathcal{V}/\mathcal{U}$. Es gilt $\operatorname{Kern}(\nu) = \mathcal{U}$.*

Dieser Satz sagt also insbesondere, dass jeder Teilraum eines Vektorraumes Kern eines geeigneten Homomorphismus ist.

Beweis.

1. Wir müssen zeigen, dass die Definition **vertreterunabhängig** ist, d. h. ist $X' + \mathcal{U} = X + \mathcal{U}$ und $Y' + \mathcal{U} = Y + \mathcal{U}$, so ist zu zeigen $(X' + Y') + \mathcal{U} = (X + Y) + \mathcal{U}$. Aber offenbar existieren $U_1, U_2 \in \mathcal{U}$ mit $X' = X + U_1, Y' = Y + U_2$, also $(X' + Y') - (X + Y) = U_1 + U_2 \in \mathcal{U}$, d. h. $(X' + Y') + \mathcal{U} = (X + Y) + \mathcal{U}$.
   Wohldefiniertheit von $a(X + \mathcal{U})$: Sei also $X' + \mathcal{U} = X + \mathcal{U}$, dann ist $X' - X \in \mathcal{U}$, also auch $aX' - aX = a(X' - X) \in \mathcal{U}$, also $aX + \mathcal{U} = aX' + \mathcal{U}$.
   Jetzt müssen die Vektorraumaxiome überprüft werden. Z. B. das Assoziativgesetz für $\mathcal{V}$ impliziert die Assoziativität der Addition von $\mathcal{V}/\mathcal{U}$ und $\mathcal{U} = 0 + \mathcal{U}$ ist das Nullelement von $\mathcal{V}/\mathcal{U}$. Den Rest lassen wir als Übung.

2. $\nu(aX + bY) = (aX + bY) + \mathcal{U} = a(X + \mathcal{U}) + b(Y + \mathcal{U}) = a\nu(X) + b\nu(Y)$ für alle $a, b \in K, X, Y \in \mathcal{V}$. Damit ist ν linear; dass ν surjektiv ist, ist klar und ebenso, dass $\operatorname{Kern}(\nu) = \mathcal{U}$. □

Ende Vorl. 2

Jetzt ist alles für den Hauptsatz vorbereitet, der in einer ähnlichen Form für Mengen und beliebige Abbildungen auch gilt.

Hauptsatz 0.5. *(**Homomorphiesatz**) Sei $f : \mathcal{V} \to \mathcal{W}$ eine lineare Abbildung von K-Vektorräumen. Dann faktorisiert f in die Komposition des natürlichen Epimorphismus $\nu := \nu_f : \mathcal{V} \to \mathcal{V}/\operatorname{Kern}(f)$ und des Monomorphismus $\overline{f} : \mathcal{V}/\operatorname{Kern}(f) \to \mathcal{W} : X + \operatorname{Kern}(f) \mapsto f(X)$, also $f = \overline{f} \circ \nu$. D. h. wir haben das* **kommutative Diagramm** *linearer Abbildungen*

$$\begin{array}{ccc} \mathcal{V} & \xrightarrow{f} & \mathcal{W} \\ {\scriptstyle \nu_f}\searrow & & \nearrow{\scriptstyle \overline{f}} \\ & \mathcal{V}/\operatorname{Kern}(f) & \end{array}$$

Insbesondere induziert $\overline{f}$ einen Isomorphismus von $\mathcal{V}/\operatorname{Kern}(f)$ auf $\operatorname{Bild}(f)$.

Beweis. $\nu := \nu_f$ wurde bereits in 0.4 eingeführt, wobei wir als Teilraum $\mathcal{U} := \mathrm{Kern}(f)$ wählen. Die beiden Bildgleichheitsäquivalenzrelationen $\sim_f$ und $\sim_\nu$ sind gleich, denn seien $X, Y \in \mathcal{V}$, dann gilt $f(X) = f(Y)$ genau dann, wenn $X - Y \in \mathrm{Kern}(f) = \mathcal{U} = \mathrm{Kern}(\nu)$, was also äquivalent zu $\nu(X) = \nu(Y)$ ist. Letzteres impliziert aber sowohl die Wohldefiniertheit als auch die Injektivität von $\overline{f}$. Die Linearität von ν hatten wir schon in 0.4 gesehen, die von $\overline{f}$ folgt unmittelbar aus der von Linearität von f. □

Aufgrund der letzten beiden Sätze kennen wir bis auf Isomorphie alle epimorphen Bilder von $\mathcal{V}$, sobald wir alle Teilräume von $\mathcal{V}$ kennen.

Beispiel 0.6. Was sagt uns der Homomorphiesatz über direkte Summen?
Sei $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$ mit $\mathcal{T}_1 \cap \mathcal{T}_2 = \{0\}$. Die Projektionsabbildung $\pi_1 : \mathcal{T}_1 \oplus \mathcal{T}_2 \to \mathcal{T}_1 : T_1 + T_2 \mapsto T_1$ ist linear und surjektiv (Epimorphismus) mit $\mathrm{Kern}(\pi_1) = \mathcal{T}_2$ und der Homomorphiesatz sagt

$$(\mathcal{T}_1 \oplus \mathcal{T}_2)/\mathcal{T}_2 \cong \mathcal{T}_1.$$

Insbesondere ist $\mathcal{T}_1$ ein Vertretersystem für die Restklassen von $\mathcal{T}_1 \oplus \mathcal{T}_2$ nach $\mathcal{T}_2$.

Springe
Folg. 1.14

Kapitel 1

Ringe und Moduln

Schreibweise.

- $K^{m\times n} := M_{m\times n}(K)$.
- Sind M und I Mengen, so bezeichnet M^I die Menge aller Abbildungen $f : I \to M$.

1 Ringe

Definition 1.1. R, genauer $(R, +, 0, \cdot, 1)$ heißt ein **Ring mit Eins**, für uns kurz **Ring**, falls folgende drei Eigenschaften gelten:

1. $(R, +, 0)$ ist eine abelsche Gruppe (mit 0 als neutrales Element).
2. $(R, \cdot, 1)$ ist ein Monoid (mit 1 als neutrales Element).
3. Es gelten die **Distributivgesetze**:

$$\begin{aligned} a(b+c) &= ab+ac \\ (b+c)a &= ba+ca \end{aligned}$$

für alle $a, b, c \in R$.

Falls $(R, \cdot, 1)$ kommutativ ist, heißt R **kommutativer Ring**. Ist $(R\setminus\{0\}, \cdot, 1)$ eine abelsche Gruppe ist, so ist R ein **Körper**.

Beispiel 1.2.

1. $\mathbb{Z}$, genauer $(\mathbb{Z}, +, 0, \cdot, 1)$, der **Ring der ganzen Zahlen**, ist ein kommutativer Ring.
2. Sind R und S Ringe, so ist auch

$$R \times S := \{(r, s) \mid r \in R, s \in S\}$$

ein Ring mit komponentenweiser Addition und Multiplikation. Das Einselement ist $(1, 1)$ und das Nullelement ist $(0, 0)$. Es gilt z.B. $(1, 0)+(0, 1) = (1, 1)$ und $(1, 0)\cdot(0, 1) = (0, 0)$. Der Ring $R \times S$ ist also nicht nullteilerfrei, d.h. es gibt Ringelemente ungleich Null deren Produkt Null ist.

3. Sei R ein Ring und I eine Menge. Dann ist die Menge R^I (aller R-wertigen Abbildungen) mit punktweiser Addition und Multiplikation

$$\begin{aligned} (f+g)(i) &:= f(i)+g(i), \\ (f\cdot g)(i) &:= f(i)\cdot g(i) \end{aligned}$$

für alle $i \in I$ wieder ein Ring.

Definition 1.3. Seien R, S Ringe. Eine Abbildung $\varphi : R \to S$ heißt **Ringhomomorphismus**, falls gilt

$$\begin{aligned} \varphi(a+b) &= \varphi(a)+\varphi(b), \\ \varphi(ab) &= \varphi(a)\varphi(b), \\ \varphi(1_R) &= 1_S \end{aligned}$$

für alle $a, b \in R$. Ist φ zusätzlich injektiv, surjektiv oder bijektiv, so spricht man vom Mono-, Epi-, bzw. Isomorphismus. Ist φ ein Isomorphismus, so schreiben wir $\varphi : R \xrightarrow{\sim} S$ oder $R \cong S$ und nennen R und S **isomorph**.

Definition 1.4. Sei R ein Ring, der gleichzeitig ein K-Vektorraum für den Körper K ist. Man nennt dann R eine **assoziative K-Algebra** mit Eins oder kürzer **K-Algebra** , falls gilt:

$$k(ab) = (ka)b = a(kb)$$

für alle $a, b \in R$ und $k \in K$. Ist S eine weitere K-Algebra mit Eins, so heißt eine K-lineare Abbildung $\varphi : R \to S$ ein K-Algebrenhomomorphismus, falls $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in R$ ist und $\varphi(1_R) = 1_S$ gilt.

Beispiel 1.5.

1. $K^{n\times n}$ ist mit Matrixaddition und Matrixmultiplikation eine K-Algebra, die für $n \geq 2$ nicht kommutativ ist.
2. K^I ist mit punktweiser Addition und Multiplikation eine kommutative K-Algebra.

Definition 1.6. Sei R ein Ring. Dann heißt

$$R^* := \{r \in R | \text{ es existiert } a \in R \text{ mit } ar = ra = 1\}$$

die **Einheitengruppe** von R. Ihre Elemente heißen auch **Einheiten** von R.

Beispiel 1.7.

1. $\mathbb{Z}^* = \{1, -1\}$.
2. Für jeden Körper K ist $K^* = K \setminus \{0\}$ und $(K^{n\times n})^* = \mathrm{GL}_n(K)$.
3. $(R \times S)^* = R^* \times S^*$.

2 Polynomringe

Lernziel: Formelle Einführung von Polynomen, Polynomdivision und EUKLIDischer Algorithmus, Körper der rationalen Funktionen, Restklassenkörper des Polynomrings, diverse Beispiele von Vektorräumen

Wir haben jetzt einerseits über kommutative Ringe und andererseits über Vektorräume gesprochen. Wir wollen jetzt über einen ganz wichtigen Ring sprechen, der gleichzeitig Vektorraum ist und der eine absolut grundlegende Rolle in der linearen Algebra spielt.

$(\mathbb{Z}_{\geq 0}, +, 0)$ ist ein (abelsches) Monoid. Dies nutzen wir aus, um auf $K^{\mathbb{Z}_{\geq 0}}$ eine zweite Multiplikation zu definieren, die eine interessantere Ringstruktur/K-Algebrenstruktur liefert.

Definition 1.8. Sei K ein Körper.

1. Auf dem K-Vektorraum $K^{\mathbb{Z}_{\geq 0}}$ definieren wir eine Multiplikation durch

$$(a_0, a_1, a_2, a_3, \ldots) \cdot (b_0, b_1, b_2, b_3, \ldots) := (c_0, c_1, c_2, c_3, \ldots)$$

mit

$$c_0 := a_0b_0, c_1 := a_0b_1 + a_1b_0, c_2 := a_0b_2 + a_1b_1 + a_2b_0, \ldots$$

allgemein für alle $n \geq 0$:

$$c_n := a_0b_n + a_1b_{n-1} + \ldots + a_nb_0$$

$(K^{\mathbb{Z}_{\geq 0}}, +, \cdot)$ zusammen mit der K-Vektorraumstruktur von $K^{\mathbb{Z}_{\geq 0}}$ wird auch mit $K[[x]]$ bezeichnet, dem **Potenzreihenring** über K in der **Unbestimmte**n $x := (0, 1, 0, 0, \ldots)$, genauer, dem Ring der **formalen Potenzreihen** über K.
(Statt $(a_0, a_1, a_2, a_3, \ldots)$ schreibt man auch $\sum_{i=0}^{\infty} a_i x^i$.)

2. Eine Potenzreihe $a = (a_0, a_1, a_2, a_3, \ldots) \in K[[x]]$ heißt **Polynom**, falls ein $n \in \mathbb{Z}_{\geq 0}$ existiert mit $a_i = 0$ für alle $i > n$. Für $a \neq 0$ heißt das kleinste derartige n der **Grad** von a. Wir setzen $\mathrm{Grad}(0) := -\infty$. Die Menge aller Polynome zusammen mit der Vektorraumstruktur und der von $K[[x]]$ ererbten Multiplikation heißt der **Polynomring** $K[x]$ über K (Selbstverständlich kann man auch einen anderen Buchstaben als x für die Unbestimmte benutzen.)

Beachte: Es gilt $x \cdot (a_0, a_1, a_2, \ldots) = (0, a_0, a_1, \ldots)$ insbesondere ist die Multiplikation mit x linear.

Übung 1.1. Sei $a \in K[[x]]$. Zeige (z. B. durch Induktion), dass

$$\mu_a : K[[x]] \to K[[x]] : b \mapsto ab$$

eine lineare Abbildung ist. Diese ist genau dann injektiv, wenn $a \neq 0$ gilt.

Beispiel 1.9 (Schriftliche Multiplikation ohne Übertrag)**.** In $\mathbb{Q}[x]$ berechnen wir ab mit $a := (1, 2, 0, 1, 0, 0, \ldots) = 1 + 2x + 1x^3$ und $b := (4, 3, 2, 1, 0, 0, \ldots) = 4 + 3x + 2x^2 + x^3$:

4	3	2	1	0	0	0	0	0
0	8	6	4	2	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	4	3	2	1	0	0
4	11	8	9	5	2	1	0	0

d.h. $ab = (4, 11, 8, 9, 5, 2, 1, 0, 0, \ldots) = 4 + 11x + 8x^2 + 9x^3 + 5x^4 + 2x^5 + x^6$.

Bemerkung 1.10.

1. $1 := (1, 0, 0, \ldots) \in K[x]$ ist neutrales Element der Multiplikation in $K[[x]]$ und in $K[x]$.
2. $xa = (0, a_0, a_1, \ldots)$ für alle $a \in K[[x]]$.
3. Es gilt $x^i x^j = x^{i+j}$. Man setzt $x^0 := 1$. (Man sieht, wie die Multiplikation der Monome x^i der Addition der Exponenten entspricht. Man sagt: $K[x]$ ist die Halbgruppenalgebra von von $(\mathbb{Z}_{\geq 0}, +)$ über K.)
4. Sei $a \in K[x]$ ein Polynom vom Grad n, dann gilt

$$a = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n.$$

Dies liefert eine offensichtliche Identifikation von K mit

$$\{0\} \cup \{a \in K[x] \mid \mathrm{Grad}(a) = 0\}.$$

5. $K[x]_{\mathrm{Grad}<n} := \{0\} \cup \{a \in K[x] \mid \mathrm{Grad}(a) < n\}$ ist ein Teilvektorraum von $K[x]$.
6. Für $a, b \in K[x] - \{0\}$ gilt $\mathrm{Grad}(ab) = \mathrm{Grad}(a) + \mathrm{Grad}(b)$.

Jede einzelne Aussage dieser Bemerkung ist sehr leicht zu beweisen und gleichzeitig sehr wichtig.

Satz 1.11. *Sei K ein Körper.*

1. *$K[x]$ ist ein kommutativer Ring, genauer, eine kommutative K-Algebra.*
2. *(Polynomdivision als Division mit Rest) Für $a, b \in K[x]$ mit $b \neq 0$ existieren eindeutige $q, r \in K[x]$ mit*
$$a = qb + r, \quad \mathrm{Grad}(r) < \mathrm{Grad}(b) \text{ oder } r = 0.$$

Ende Vorl. 1

Beweis.

1. Dass die Multiplikation kommutativ ist und wir ein Einselement haben, ergibt sich direkt aus der Definition der Multiplikation.
Das Distributivgesetz folgt direkt aus der Bilinearität der Multiplikation.
Es bleibt die Assoziativität zu zeigen. Behauptung: $a(bc) = (ab)c$ für alle $a, b, c \in K[x]$.
Beweis durch Induktion nach $\mathrm{Grad}(c)$: Die Behauptung ist sicher richtig, wenn $\mathrm{Grad}(c) = 0$. Angenommen sie gilt für alle a, b, c mit $\mathrm{Grad}(c) \leq n$. Wir zeigen, dass sie dann auch für $\mathrm{Grad}(c) = n + 1$ gilt. Zu diesem Zweck schreiben wir $c = C + c_{n+1}x^{n+1}$ mit $\mathrm{Grad}(C) \leq n$ (schließt den Fall $C = 0$ ein). Dann gilt:
$$\begin{aligned} a(bc) &= a(b(C + c_{n+1}x^{n+1})) \\ &= a(bC + c_{n+1}bx^{n+1}) \\ &= a(bC) + c_{n+1}a(bx^{n+1}) \\ &= (ab)C + c_{n+1}(ab)x^{n+1} \\ &= (ab)(C + c_{n+1}x^{n+1}) \\ &= (ab)c \end{aligned}$$
wobei im entscheidenden vierten Schritt einerseits die Induktionsvoraussetzung und andererseits eine einfache Beobachtung über Verschieben eingeht.

2. Sie kennen vermutlich das Verfahren von der langen Division her, nur dass hier die Situation einfacher ist, als bei ganzen Zahlen, da man keine Überträge hat. Sei $\mathrm{Grad}(a) = m$, $\mathrm{Grad}(b) = n$. Falls $m < n$, sind wir bereits fertig mit $q = 0, r = a$. Falls nicht, ersetzen wir a durch $a - \frac{a_m}{b_n}x^{m-n}b$ und belassen b. Nach endlich vielen Schritten ist der Grad des ersten Polynoms schließlich kleiner als n und wir können $q = \frac{a_m}{b_n}x^{m-n} + \ldots$ sowie r als das letzte der Polynome aus der Folge der a's ablesen. Soweit die Existenz von q und r.
Zur Eindeutigkeit: Sei $a = q'b + r'$ mit $\mathrm{Grad}(r') < \mathrm{Grad}(b)$. Dann folgt
$$r - r' = (q - q')b$$
Wäre $q - q' \neq 0$, dann folgt $\mathrm{Grad}(r - r') \geq \mathrm{Grad}(b)$, was ein Widerspruch ist. Also ist $q = q'$ und $r = r'$. □

Beispiel 1.12. $a := x^6 - x - 1, b = x^2 - x + 1 \in \mathbb{Q}[x]$. Wir suchen den Quotienten q und den Rest r. Wir haben also
$$q = -1 - x + x^3 + x^4, r = -x.$$
Man vergleiche dieses Schema mit dem von der schriftlichen Division.

Bemerkung 1.13 (In der Vorlesung übersprungen)**.** Bei der Bestimmung von q und r handelt es sich bei der Polynomdivision um das Lösen eines linearen Gleichungssystems, welches bereits in Dreiecksgestalt gegeben ist.

$$\begin{array}{cc|ccccccccc|r}
0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & \dots & 1x^4 \cdot b \\
0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & \dots & 1x^3 \cdot b \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0x^2 \cdot b \\
0 & -1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & \dots & -1x \cdot b \\
-1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & -1 \cdot b \\
\hline
-1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \dots & a
\end{array}$$

An den Spalten 3 $(= 1+\mathrm{Grad}(b))$ bis 7 $(= 1+\mathrm{Grad}(a))$ sieht man, welches Gleichungssystem man lösen muss, aus den ersten 2 $(= \mathrm{Grad}(b))$ kann man den Rest bestimmen und die Lösung des Gleichungssystems, also q kann man aus der letzten Spalte ablesen.

Springe Kap. 0

Folgerung 1.14. *Sei $0 \neq p \in K[x]$ von Grad n. Dann bilden die Vielfache von p einen Teilraum $pK[x] \leq K[x]$ und der Faktorraum $K[x]/pK[x]$ hat $K[x]_{\mathrm{Grad}<n}$ als Vertretersystem. Mit anderen Worten:*

$$K[x] = K[x]_{\mathrm{Grad}<n} \oplus pK[x].$$

Beweis. Jedes $f \in K[x]$ läßt sich eindeutig schreiben als $f = qp+r$ mit $r, q \in K[x]$, $\mathrm{Grad}(r) < n = \mathrm{Grad}(p)$. Also ist $K[x] = K[x]_{\mathrm{Grad}<n} \oplus pK[x]$. Nach dem Homomorphiesatz ist somit $K[x]/pK[x] \cong K[x]_{\mathrm{Grad}<n}$, was man ganz konkret so verstehen kann, dass jede Restklasse $f + pK[x]$ einen kanonischen Vertreter $r = f - pq \in f + pK[x]$ hat, mit $\mathrm{Grad}(r) < n$. □

Bemerkung 1.15. Sei $p = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n \in K[x]$. Die Multiplikation mit x induziert einen Endomorphismus von $K[x]/pK[x]$

$$x^i + pK[x] \mapsto x^{i+1} + pK[x] \text{ für } i = 0, \ldots, n-1,$$

und

$$x^{n-1} + pK[x] \mapsto x^n + pK[x] = -a_0 - a_1x - \ldots - a_{n-1}x^{n-1} + pK[x].$$

Beweis. Dass die Multiplikation mit x auf $K[x]$ linear ist, wissen wir schon. Wir müssen zeigen, dass sie eine wohldefinierte Abbildung von $K[x]/pK[x]$ in sich induziert, die dann natürlich automatisch linear ist. Sei also $r+pK[x] = s+pK[x]$ für zwei Elemente $r, s \in K[x]$. Behauptung: $xr+pK[x] = xs+pK[x]$. Beweis: $r-s \in pK[x]$, also $xr-xs = x(r-s) \in pK[x]$, also $xr + pK[x] = xs + pK[x]$. Der Rest ist klar. □

Schreibweise. Für $a + pK[x] = b + pK[x]$ schreiben wir oft $a \equiv b \pmod{p}$.

Übung 1.2. Zeige $x^{100} \equiv x \pmod{x^2 + x + 1}$.
Hinweis: Rechne erst modulo $x^3 - 1$.

Übung 1.3. Zeige, dass der Potenzreihenring $K[[x]]$ ein kommutativer Ring mit 1, sogar kommutative K-Algebra ist. Man beachte, dass bei der üblichen Schreibweise für $a \in K[[x]]$ als Potenzreihe

$$a = \sum_{i=0}^{\infty} a_i x^i$$

es sich um eine formale Schreibweise handelt. Im algebraischen Sinne sind Summen mit unendlich vielen Summanden nicht definiert.

Übung 1.4. Zeige: Elemente $a = \sum_{i=0}^{\infty} a_i x^i \in K[[x]]$ mit $a_0 \neq 0$ sind invertierbar. Modifiziere das Schema des letzten Beispiels um ein Schema anzugeben, wie man die ersten n Glieder von a^{-1} ausrechnen kann. Gibt es Alternativen? Betrachte $(1-x)^{-1}$. Betrachte auch $(1-x-x^2)^{-1} = \sum_{i=0}^{\infty} a_i x^i$. Zeige: $a_0 = a_1 = 1$ und $a_{i+2} = a_i + a_{i+1}$ für $i \geq 0$.

Inzwischen sollte die Parallelität vieler Eigenschaften von $\mathbb{Z}$ und $K[x]$ klar sein:

1. In $\mathbb{Z}$ gilt $|ab| = |a||b|$, in $K[x]$ gilt $\mathrm{Grad}(ab) = \mathrm{Grad}(a) + \mathrm{Grad}(b)$, insbesondere hat $K[x]$ auch einen Quotientenkörper.

2. In beiden Ringen haben wir Division mit Rest und damit hat $K[x]$ auch einen erweiterten EUKLIDischen Algorithmus (siehe 2. Übungsblatt), größte gemeinsame Teiler sind definiert und eindeutig bis auf Faktoren vom Grad 0. Weiter hat man auch das Analogon von Primzahlen in $K[x]$: **irreduzible** Polynome, also solche, die nicht als Produkt von zwei Polynomen echt kleineren Grades geschrieben werden können.

3. In Analogie zu den Restklassenkörpern $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ für Primzahlen p (siehe 2. Übungsblatt), hat man Restklassenkörper $K[x]/pK[x]$ für irreduzible Polynome $p = p(x) \in K[x]$.

Übung 1.5. Ausgehend von einem Körper K konstruiere aus dem Polynomring $K[x]$ einen Körper $K(x)$ in Analogie zu der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.
Hinweis: $K(x) := (K[x] \times (K[x] - \{0\}))/\sim$ mit $(p, q) \sim (r, t)$ genau dann, wenn $pt = qr$. Man nennt $K(x)$ den Körper der rationalen Funktionen über K.

Satz 1.16. *Sei $p \in K[x]$, $p \neq 0$, $\mathrm{Grad}(p) \geq 1$. Dann ist $K[x]/pK[x]$ durch vertreterweise Addition und Multiplikation ein Ring. Ist $p \in K[x]$* **irreduzibel**, *d.h. $n := \mathrm{Grad}(p) > 0$ und p hat keine Teiler in $K[x]$ von Grad g mit $0 < g < \mathrm{Grad}(p)$, so ist $K[x]/pK[x]$ ein Körper.*

Beweis. $K[x]$ ist assoziative, kommutative K-Algebra mit Eins, so dass sich die meisten Gesetze auf die Restklassenalgebra $K[x]/pK[x]$ sofort vererben. Jedoch ist die Wohldefiniertheit der Multiplikation zu zeigen. Sind $a, a', b, b' \in K[x]$ mit $a = a' + pu, b = b' + pv$ so gilt

$$ab = (a' + pu)(b' + pv) = a'b' + p(ab' + a'v + puv) \in a'b' + pK[x]$$

Ist nun $p \in K[x]$ irreduzibel, so ist jedes Element $\neq 0$ invertierbar: Sei also $a \in K[x]$ mit $\overline{a} \neq 0$ in $K[x]/pK[x]$. Da p irreduzibel ist, liefert der erweiterte Euklidische Algorithmus $\alpha, \beta \in K[x]$ mit $\alpha a + \beta p = 1$. Es folgt $\overline{a}^{-1} = \overline{\alpha}$. □

Beispiel 1.17.

1. Neue Konstruktion von $\mathbb{C}$: In $\mathbb{R}[x]$ ist $p = x^2 + 1$ irreduzibel. Bezeichne die Restklasse von x mit $\overline{x}$. Dann gilt somit $\overline{x}^2 = -1$. Die Element von $\mathbb{R}[x]/p\mathbb{R}[x]$ sind gegeben durch $a + b\overline{x}$ mit $a, b \in \mathbb{R}$. Es gilt

   $$(a + b\overline{x})(c + d\overline{x}) = ac - bd + (ad + bc)\overline{x}$$

   d.h. wir haben den komplexen Zahlkörper neu konstruiert.
   Übung: Benutze den EUKLIDischen Algorithmus um $a + b\overline{x}$ zu invertieren.

2. Körper mit vier Elementen: In $\mathbb{F}_2[x]$ ist $p = x^2 + x + 1$ irreduzibel. Damit ist $\mathbb{F}_2[x]/p\mathbb{F}_2[x]$ ein Körper mit vier Elementen: $0, 1, \overline{x}, 1 + \overline{x}$.
   Übung: Man gebe die Additions- und Multiplikationstabellen an.

3. ($\mathbb{Q}[\sqrt[3]{2}]$) Das Polynom $x^3 - 2 \in \mathbb{Q}[x]$ ist sicher irreduzibel, da es sonst einen Teiler der Form $x - a$ mit $a \in \mathbb{Q}$ hätte. Indem man eine Primfaktorzerlegung für Zähler und Nenner ansetzt kommt man wegen $a^3 = 2$ schnell zu einem Widerspruch.
   Also ist $\mathbb{Q}[x]/(x^3 - 2)\mathbb{Q}[x]$ ein Körper. Setze $(\sqrt[3]{2} :=)\overline{x} := x + (x^3 - 2)\mathbb{Q}[x]$.

Aufgabe: Bestimme die Normalform von $(\overline{x}^2+\overline{x}+1)^{-1}$.
Lösung:

$$x^3-2=(x-1)(x^2+x+1)-1,$$

Nach einem einschrittigen EUKLIDischen Algorithmus erhalten wir also

$$(\overline{x}^2+\overline{x}+1)^{-1}=-1+\overline{x}$$

oder

$$\frac{1}{\sqrt[3]{2}^2+\sqrt[3]{2}+1}=-1+\sqrt[3]{2}.$$

Mit dem Begriff der Irreduzibilität von Polynomen ist der der Wurzel eng verbunden.

Bemerkung 1.18. Sei K ein Körper und A eine assoziative K-Algebra (also z.B. $A=K$ oder $A=K^{n\times n}$). Ende Vorl. 3

1. Für jedes $a\in A$ ist durch $x^i\mapsto a^i$ eine lineare Abbildung $\varepsilon_a: K[x]\to A: p\mapsto p(a)$ definiert (genannt der **Einsetzungshomomorphismus**), sogar ein K-Algebrenisomorphismus.

2. Ein Element $a\in K$ heißt **Wurzel** des Polynoms p, falls $p(a)=0$, also $\varepsilon_a(p)=0$.

3. Für $a\in K$ ist $\mathrm{Kern}(\varepsilon_a)=(x-a)K[x]$. Insbesondere gilt $p(a)=0$ genau dann, wenn $(x-a)$ ein Teiler von p ist.

4. Ein Polynom vom Grad n hat höchstens n verschiedene Wurzeln in K.

5. Eine Abbildung $f\in K^K$ heißt **Polynomfunktion**, falls ein $p\in K[x]$ existiert mit $f(a)=p(a)$ für alle $a\in K$. In diesem Fall heißt $f=:f_p$ die von p induzierte Polynomfunktion. Es ist

$$\varepsilon: K[x]\to K^K: p\mapsto f_p$$

ein K-Algebrenhomomorphismus. Das Bild bezeichnen wir mit $PolFu(K)$. Die Abbildung ist genau dann surjektiv, wenn K endlich ist. Die Abbildung ist genau dann injektiv, wenn K unendlich ist.

Beweis.

1. Ist $f=\sum_{i=0}^n f_ix^i\in K[x]$, so ist $\varepsilon_a(f)=\sum_{i=0}^n f_ia^i\in A$. Die so gegebene Abbildung $\varepsilon_a: K[x]\to A$ ist wohldefiniert, da durch das Polynom $f=(f_0,f_1,\ldots,f_n,0,\ldots)\in K^{\mathbb{Z}_{\geq 0}}$ seine Koeffizienten f_i eindeutig bestimmt sind und die Potenzen von a Elemente des K-Vektorraums A sind.
ε_a ist linear: Seien $f=\sum_{i=0}^n f_ix^i, g=\sum_{j=0}^m g_jx_j\in K[x]$, $h,k\in K$, wobei wir nach Ergänzung von Nullen ohne Einschränkung annehmen dürfen, dass $m=n$ ist. Dann ist

$$\varepsilon_a(hf+kg)=\sum_{i=0}^n(hf_i+kg_i)a^i=\sum_{i=0}^n hf_ia^i+kg_ia^i=h\sum_{i=0}^n f_ia^i+k\sum_{i=0}^n g_ia^i=h\varepsilon_a(f)+k\varepsilon_a(g).$$

Dass es ein K-Algebrenisomorphismus ist, ist nun völlig analog.

2. Ist eine Definition.

3. Übung: Division von p durch $(x-a)$ mit Rest $p(a)$.

4. Sind $a_1, \ldots, a_s$ paarweise verschiedene Wurzeln von p, so gilt $(x - a_i)$ teilt p für $i = 1, \ldots, s$. Da die $(x - a_i)$ paarweise verschiedene irreduzible Polynome sind, ist auch das Polynom $\prod_{i=1}^{s}(x - a_i)$ vom Grad s ein Teiler von p und somit $\mathrm{Grad}(p) \geq s$.

5. Übung.

□

Übung 1.6. Sei $p \in K[x]$ vom Grad 2 oder 3. Zeige: p ist genau dann irreduzibel, falls p keine Wurzeln (in K) hat. Was ist bei Polynomen vom Grad 4?

Übung 1.7 (LAGRANGEinterpolation)**.** Seien $a_1, \ldots, a_n \in K$ beliebige Elemente und $s_1, \ldots, s_n \in K$ paarweise verschiedene Elemente. Man zeige: Es existiert genau ein $p \in K[x]_{\mathrm{Grad}<n}$ mit $p(s_i) = a_i$ für $i = 1, \ldots, n$. (Hinweis: Setze $q := (x - s_1) \ldots (x - s_n)$ und arbeite mit den $\frac{q}{x - s_i}$.)

Übung 1.8. Definiere die Vielfachheit einer Wurzel.

Übung 1.9. Gib Normalformen der Elemente von $K(x)/K[x]$ an. Was versteht man unter Partialbruchzerlegung?

Definition 1.19. Ein Körper K heißt **algebraisch abgeschlossen**, falls jedes nicht konstante Polynom über K eine Wurzel hat, d.h. falls jedes Polynom in Linearfaktoren zerfällt.

Wir zitieren ohne Beweis:

Hauptsatz 1.20 (GAUSS , sogenannter Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Bemerkung 1.21.

1. Sei R ein kommutativer Ring. $R^{\mathbb{Z}_{\geq 0}} =: R[[x]]$ mit der bekannten Multiplikation heißt der Potenzreihenring über R und entsprechend $R[x]$ der Polynomring über R. Beides sind kommutative Ringe.

2. Nimmt man in 1.) $R := K[t]$ den Polynomring in t über dem Körper K, so erhält man $K[t, x] := K[t][x]$, den Polynomring über K in t, x, eine kommutative K-Algebra. Es gilt:
$$K[t, x] \to K[x, t] : \sum_i (\sum_j a_{i,j} t^j) x^i \mapsto \sum_j (\sum_i a_{i,j} x^j) t^i$$
is ein K-Algebrenisomorphismus. Man nennt das maximale $i + j$ mit $a_{i,j} \neq 0$ auch den Gesamtgrad oder einfach Grad des Polynoms $\sum_{i,j} a_{i,j} t^i x^j$.

3. Analog konstruiert man $K[[t, x]] := K[[x]][[t]]$ und sieht dass diese K-Algebra zu $K[[x, t]]$ isomorph ist.

Übung 1.10. Sind $K[[t]][x]$ und $K[t][[x]]$ auch isomorph, und zwar durch einen Isomorphismus, der Isomorphismus von 1.21 2) forsetzt?

Kapitel 2

Endomorphismen

Schreibweise.

- Wir setzen ${}^{\mathcal{C}}f^{\mathcal{B}} := M_{\mathcal{B}}^{\mathcal{C}}(f)$.
- $\mathrm{id}_{\mathcal{V}}$ ist die Identitätsabbildung auf $\mathcal{V}$.
- Anstelle von K^n schreiben wir ab und zu $K^{n\times 1}$.
- Die zur Matrix $A \in K^{n\times n}$ zugehörigen linearen Abbildung $K^{n\times 1} \to K^{n\times 1},\ b \mapsto Ab$ bezeichnen wir mit $\widetilde{A}$.

1 Der Endomorphismenring

Lernziel: Matrizen von Endomorphismen, Ähnlichkeit von Matrizen, Einsetzungshomomorphismus, Minimalpolynom und seine Berechnung, Begleitmatrizen.

Definition 2.1. Sei $\mathcal{V}$ ein K-Vektorraum . Dann heißt

$$\mathrm{End}(\mathcal{V}) := \mathrm{Hom}(\mathcal{V}, \mathcal{V})$$

zusammen mit der Addition von linearen Abbildungen und der Komposition der **Endomorphismenring** von $\mathcal{V}$.

Die Endomorphismen von $\mathcal{V}$ bilden einen Ring mit $\mathrm{id}_{\mathcal{V}}$ als Eins, der für $\mathrm{Dim}\,\mathcal{V} > 1$ nichtkommutativ ist. Die invertierbaren Elemente bilden die Einheitengruppe des Ringes, die wir bereits früher als generelle lineare Gruppe $\mathrm{GL}(\mathcal{V})$ bezeichnet haben. Was bewirkt die Festlegung einer Basis?

Bemerkung 2.2. Sei $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$. Dann ist

$$\mathrm{End}(\mathcal{V}) \to K^{n\times n} : \alpha \mapsto {}^{B}\alpha^{B}$$

ein K-Algebrenisomorphismus.

Unser Thema ist weniger die algebraische Struktur von $\mathrm{End}(\mathcal{V})$ als Ring sondern vielmehr, wie wir vorgegebene Endomorphismen besser verstehen können, indem wir die Basis B so wählen, dass die Matrix eine besonders einfache Gestalt annimmt. Am einfachsten ist Diagonalgestalt. Dabei ist zu beachten, dass nur eine Basis gewählt wird, bezüglich der sowohl Urbilder als auch Bilder ausgedrückt werden. Zuerst rekapitulieren wir, wie ein Basiswechsel sich auswirkt:

Bemerkung 2.3.

1. $\alpha \in \mathrm{End}(V)$ und $B, B' \in \mathcal{V}^n$ Basen von $\mathcal{V}$. Es gilt
$$ {}^{B'}\alpha^{B'} = ({}^{B}\,\mathrm{id}_{\mathcal{V}}^{B'})^{-1} \cdot {}^{B}\alpha^{B} \cdot {}^{B}\,\mathrm{id}_{\mathcal{V}}^{B'} .$$
2. Zwei Matrizen $A, A' \in K^{n\times n}$ heißen **ähnlich** wenn es eine Matrix $C \in \mathrm{GL}(n, K)$ existiert, mit $A' = C^{-1}AC$. Die Äquivalenzklassen heißen **Ähnlichkeitsklassen**. Insbesondere sind ${}^{B}\alpha^{B}$ und ${}^{B'}\alpha^{B'}$ ähnlich.

Es ist recht schwierig, trennende Invarianten oder Normalformen für die Ähnlichkeitsklassen anzugeben. Dies wird für algebraisch abgeschlossene Körper im dritten Kapitel geschehen und für allgemeine Körper wahrscheinlich erst in der Algebravorlesung im dritten Semester. Aber wir können jetzt schon einige erste Schritte unternehmen. Klar ist, dass ähnliche Matrizen denselben Rang haben. Eine zweite einfache Invariante ist die Spur.

Definition 2.4.

1. Für $A \in K^{n\times n}$ heißt $\mathrm{Spur}(A) := \sum_{i=1}^{n} A_{ii}$ die **Spur** der Matrix A.
2. Sei $\mathcal{V}$ ein endlich dimensionaler K-Vektorraum. Für $\alpha \in \mathrm{End}(\mathcal{V})$ definiert man die **Spur** von α als
$$\mathrm{Spur}(\alpha) := \mathrm{Spur}({}^{B}\alpha^{B})$$
für irgendeine Basis $B \in \mathcal{V}^n$ von $\mathcal{V}$.

Bemerkung 2.5.

1. Für $A \in K^{m\times n}$ und $B \in K^{n\times m}$ gilt:
$$\mathrm{Spur}(AB) = \sum_{i,j} A_{ij}B_{ji} = \mathrm{Spur}(BA).$$
2. Für $A \in K^{n\times n}$ und $g \in GL(n, K)$ gilt
$$\mathrm{Spur}(g^{-1}Ag) = \mathrm{Spur}(A).$$
3. $\mathrm{Spur}(\alpha)$ für $\alpha \in \mathrm{End}(\mathcal{V})$ ist wohldefiniert.

Beweis.

1. Klar.
2. Aus 1.: $\mathrm{Spur}(g^{-1}Ag) = \mathrm{Spur}(gg^{-1}A) = \mathrm{Spur}(A)$.
3. Aus 2. und 4.1. □

2 Das Minimalpolynom

Hier kommt eine brauchbarere Invariante, die auf einem Test der linearen Abhängigkeiten der Potenzen einer linearen Abbildung beruht.

Beispiel 2.6. Wir halten folgende Spezialfälle von Einsetzhomomorphismen fest:

1. Für $A \in K^{n\times n}$ und $p = p(x) = a_0 + a_1x + \ldots + a_dx^d \in K[x]$ sei $p(A)$ definiert als $p(A) := a_0I_n + a_1A + \ldots + a_dA^d$. Weiter heißt

$$\varepsilon_A : K[x] \to K^{n\times n} : p \to p(A)$$

der **Einsetzungshomomorphismus** zu A.

2. Für $\alpha \in \mathrm{End}(\mathcal{V})$ und $p = p(x) = a_0 + a_1x + \ldots + a_dx^d \in K[x]$ sei $p(\alpha)$ definiert als $p(\alpha) := a_0\,\mathrm{id}_\mathcal{V} + a_1\alpha + \ldots + a_d\alpha^d$. Weiter heißt

$$\varepsilon_\alpha : K[x] \to \mathrm{End}(\mathcal{V}) : p \to p(\alpha)$$

der **Einsetzungshomomorphismus** zu α.

Bemerkung 2.7. Ist $A \in K^{n\times n}$ so ist ε_A ein K-Algebrenhomomorphismus, d.h. für $p, q \in K[x]$ und $a, b \in K$ ist

$$\varepsilon_A(ap + bq) = a\varepsilon_A(p) + b\varepsilon_A(q),\ \varepsilon_A(pq) = \varepsilon_A(p)\varepsilon_A(q).$$

Ist $\alpha \in \mathrm{End}(\mathcal{V})$ so ist ε_α ein K-Algebrenhomomorphismus.

Lemma 2.8.

1. *Ist $A \in K^{n\times n}$, so gibt es genau ein normiertes Polynom $\mu_A \in K[x]$ mit $\mathrm{Kern}(\varepsilon_A) = \mu_AK[x]$. Dieses Polynom heißt das* **Minimalpolynom** *von A.*

2. *Ist $\mathcal{V}$ ein endlich dimensionaler K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$, so gibt es genau ein normiertes Polynom $\mu_\alpha \in K[x]$ mit $\mathrm{Kern}(\varepsilon_\alpha) = \mu_\alpha K[x]$. Dieses Polynom heißt das* **Minimalpolynom** *von α.*

Beweis. 2. geht genauso wie 1.

1. Sei $s \in \mathbb{N}$ minimal, so dass $(I_n, A, \ldots, A^s)$ linear abhängig im K-Vektorraum $K^{n\times n}$ ist und $a_0, \ldots, a_{s-1} \in K$ mit $A^s + a_{s-1}A^{s-1} + \ldots + a_0I_n = 0$. Setze $a_s = 1$ und $\mu_A = \sum_{i=0}^{s} a_ix^i \in K[x]$.
Behauptung: $\mu_AK[x] = \mathrm{Kern}(\varepsilon_A)$.
$\subseteq$: klar, da $\mu_A(A) = 0$.
$\supseteq$: Sei $0 \neq q \in \mathrm{Kern}(\varepsilon_A)$. Dann gibt es $a, b \in K[x]$ mit $q = a\mu_A + b$ mit $\mathrm{Grad}(b) < \mathrm{Grad}(\mu_A) = s$. Es gilt jedoch

$$0 = q(A) = a(A)\mu_A(A) + b(A) = 0 + b(A) \text{ also auch } b(A) = 0.$$

Wegen der Minimalität von $s = \mathrm{Grad}(\mu_A)$ folgt also $b = 0$. Somit ist $q \in \mu_AK[x]$. □

Übung 2.1. Zeige: Für $A \in K^{n\times n}$, $g \in \mathrm{GL}_n(K)$ und $p \in K[x]$ ist

$$p(g^{-1}Ag) = g^{-1}p(A)g.$$

Ende Vorl. 4

Bemerkung 2.9.

1. Der Grad des Minimalpolynoms von A ist das kleinste $s \in \mathbb{N}$ mit $(I_n, A, \ldots, A^s)$ linear abhängig. Insbesondere ist das Minimalpolynom wohldefiniert.

2. Das Minimalpolynom, genauer

$$\mu : K^{n\times n} \to K[x] : A \mapsto \mu_A(x)$$

ist eine Invariante der Ähnlichkeitsklassen in $K^{n\times n}$, sprich zwei ähnliche Matrizen haben das gleiche Minimalpolynom.

3. Sei $\alpha \in \mathrm{End}(\mathcal{V})$, $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$ und $A = {}^B\alpha^B \in K^{n\times n}$. Dann sind die Minimalpolynome von α und A gleich:

$$\mu_\alpha(x) = \mu_A(x).$$

Beweis. Übung. □

Beispiel 2.10.

1. Sei $A = 0 \in K^{n\times n}$ die Nullmatrix. Dann gilt $\mu_0(x) = x$. Entsprechend $\mu_{0_\mathcal{V}} = x$, wobei wir mit $0_\mathcal{V}$ den Nullendomorphismus bezeichnet.
2. Sei $A = I_n \in K^{n\times n}$. Dann gilt $\mu_{I_n}(x) = x - 1$ für $n > 0$. Entsprechend $\mu_{\mathrm{id}_\mathcal{V}} = x - 1$ falls $\mathcal{V} \neq \{0\}$.
3. Sei $A = \begin{pmatrix} 2 & 0 \\ 0 & -5 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$. Dann gilt $\mu_A = (x-2)(x+5)$.
4. Sei $\mathcal{V} = \langle \sin, \cos\rangle \leq \mathbb{R}^\mathbb{R}$ der von Sinus und Cosinus erzeugte Teilraum von $\mathbb{R}^\mathbb{R}$ und $\partial \in \mathrm{End}(\mathcal{V})$ die Ableitung. Dann gilt $\partial(\sin) = \sin' = \cos$ linear unabhängig von $\sin$, und $\partial^2(\sin) = -\sin$ und $\partial^2(\cos) = -\cos$, also $\mu_\partial(x) = x^2+1$. Man beachte, wir erhalten dadurch eine neue Realisierung der komplexen Zahlen $\mathbb{C} = \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ als den Teilring von $\mathrm{End}(\mathcal{V}) \cong \mathbb{R}^{2\times 2}$, der als $\mathbb{R}$-Vektorraum von $\mathrm{id}_\mathcal{V}$ und ∂ erzeugt wird.
5. Im Allgemeinen gilt für $A \in K^{n\times n}$:

$$K[A] := \langle I_n, A, A^2, \ldots, A^s\rangle = \mathrm{Bild}(\varepsilon_A) \cong K[x]/\mathrm{Kern}(\varepsilon_A) = K[x]/\mu_A K[x]$$

als K-Algebra.

Lemma 2.11. *Sei $\alpha \in \mathrm{End}(\mathcal{V})$ und $\mathcal{U} \leq \mathcal{V}$ ein α-invarianter Teilraum, d.h. $\alpha(\mathcal{U}) \subseteq \mathcal{U}$. Dann definiert α zwei lineare Abbildungen:*

$$\beta := \alpha_{|\mathcal{U}} \in \mathrm{End}(\mathcal{U}) \text{ und } \gamma \in \mathrm{End}(\mathcal{V}/\mathcal{U}), \gamma(X+\mathcal{U}) := \alpha(X)+\mathcal{U}.$$

Es gilt

$$kgV(\mu_\beta, \mu_\gamma) \mid \mu_\alpha \mid \mu_\beta\mu_\gamma,$$

d.h. $kgV(\mu_\beta, \mu_\gamma)$ teilt μ_α und μ_α teilt $\mu_\beta\mu_\gamma$.

Beweis. Es gilt ist $\mu_\beta K[X] = \mathrm{Kern}(\varepsilon_\beta)$, insbesondere ist jedes Polynom $f \in K[X]$ mit $f(\beta) = 0$ durch μ_β teilbar. Jetzt genügt es zu beobachten, dass $\mu_\alpha(\beta) = 0$ da

$$\mu_\alpha(\beta) = \mu_\alpha(\alpha)_{|\mathcal{U}}.$$

Also gilt μ_β teilt μ_α. Es ist leicht einzusehen, dass γ wohldefiniert ist und $\mu_\alpha(\gamma) = 0$ gilt. Daraus ergibt sich die erste Teilbarkeitsrelation.
Für die zweite Teilbarkeit sei $X \in \mathcal{V}$. Dann gilt

$$(\mu_\beta\mu_\gamma(\alpha))(X) = \mu_\beta(\alpha)(\mu_\gamma(\alpha)(X)) = \mu_\beta(\alpha)(Y) = 0$$

wobei $Y = \mu_\gamma(\alpha)(X) \in \mathcal{U}$ ist und daher $\mu_\beta(\alpha)(Y) = \mu_\beta(\beta)(Y) = 0$. □

Bemerkung 2.12. Lemma 2.11 liest sich für Matrizen wie folgt: Sei $A = \begin{pmatrix} B & \star \\ 0 & C \end{pmatrix} \in K^{n\times n}$ mit quadratischen Matrizen B und C. Dann gilt

$$\mathrm{kgV}(\mu_C, \mu_B) \mid \mu_A \mid \mu_B\mu_C,$$

d.h. $\mathrm{kgV}(\mu_C, \mu_B)$ teilt μ_A und μ_A teilt $\mu_B\mu_C$.

Beispiel 2.13. Sei $\mathcal{V}$ endlich erzeugter K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$. Wähle $0 \neq V \in \mathcal{V}$ und schreibe die erste lineare Abhängigkeit von $(V, \alpha(V), \alpha^2(V), \ldots, \alpha^{k-1}(V), \alpha^k(V)) \in \mathcal{V}^{k+1}$ mit k minimal als Polynom:

$$a_0 V + a_1\alpha(V) + \ldots + a_{k-1}\alpha^{k-1}(V) + 1\alpha^k(V) = 0$$

und definiere $q := a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + x^k \in K[x]$, so gilt nach der gleichen Beweisführung wie oben, dass $q|\mu_\alpha(x)$ und, falls $\langle V, \alpha(V), \alpha^2(V), \ldots, \alpha^{k-1}(V)\rangle = \mathcal{V}$, so gilt sogar $q = \mu_\alpha(x)$. Z. B.

$$A := \begin{pmatrix} 1 & -2 & 3 \\ -4 & 0 & -4 \\ 3 & -2 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$$

liefert mit dem Vektor $V := \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in \mathbb{Q}^{3\times 1}$ die Folge

$$(V, \widetilde{A}(V), \widetilde{A}^2(V), \widetilde{A}^3(V)) = (\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -4 \\ 3 \end{pmatrix}, \begin{pmatrix} 18 \\ -16 \\ 14 \end{pmatrix}, \begin{pmatrix} 92 \\ -128 \\ 100 \end{pmatrix})$$

Man setzt ein lineares Gleichungssystem an und bekommt

$$32V + 24\widetilde{A}(V) + 2\widetilde{A}^2(V) = \widetilde{A}^3(V),$$

da die ersten drei Vektoren noch linear unabhängig sind, und somit $x^3 - (32 + 24x + 2x^2)$ als Minimalpolynom von A. Man beachte, $B := (V, \widetilde{A}(V), \widetilde{A}^2(V))$ ist eine Basis von $\mathbb{Q}^{3\times 1}$ und

$${}^B\widetilde{A}^B = \begin{pmatrix} 0 & 0 & 32 \\ 1 & 0 & 24 \\ 0 & 1 & 2 \end{pmatrix}$$

Nicht immer ist die Bestimmung des Minimalpolynoms so schmerzfrei wie bei den obigen Beispielen. Wir geben daher einen Algorithmus an, der die Bestimmung des Minimalpolynoms eines Endomorphismus α auf die (leichtere) Bestimmung hinreichend vieler Minimalpolynome von Vektoren von $\mathcal{V}$ reduziert.

Bemerkung 2.14. Sei $\mathcal{V}$ endlich erzeugter K-Vektorraum, $\alpha \in \mathrm{End}(\mathcal{V})$ und $0 \neq V \in \mathcal{V}$. Dann gibt es ein kleinstes $k \leq \mathrm{Dim}(\mathcal{V})$, so dass

$$(V, \alpha(V), \alpha^2(V), \ldots, \alpha^k(V)) \in \mathcal{V}^{k+1}$$

linear abhängig ist und eine eindeutige lineare Abhängigkeit $(a_0, a_1, \ldots, a_{k-1}, 1) \in K^{k+1}$mit

$$a_0 V + a_1\alpha(V) + \cdots + a_{k-1}\alpha^{k-1}(V) + \alpha^k(V) = 0.$$

Dann heißt

$$\mu_{\alpha,V}(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + x^k$$

das **Minimalpolynom** des Vektors V bezüglich α. Der k-dimensionale Teilraum $\mathcal{W} := K[\alpha]V := \langle V, \alpha(V), \alpha^2(V), \ldots, \alpha^{k-1}(V)\rangle$ ist invariant unter α, d.h. $\alpha(\mathcal{W}) \subseteq \mathcal{W}$ und $\mu_{\alpha,V}(x)$ ist das Minimalpolynom der Einschränkung

$$\beta : \mathcal{W} \to \mathcal{W} : W \mapsto \alpha(W).$$

Mit Lemma 2.11 gilt $\mu_{\alpha,V}(x)$ teilt $\mu_\alpha(x)$.

Beweis. Übungsaufgabe. □

Bemerkung 2.15. Sei $p = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in K[x]$ normiert vom Grad d. Die Multiplikation mit x induziert eine lineare Abbildung m_p auf $K[x]/pK[x]$, die bezüglich der Basis

$$B = (\overline{1}, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{d-1}) \in (K[x]/pK[x])^d \quad \text{mit } \overline{x} := x + pK[x]$$

die Matrix

$${}^B m_p^B =: M_p = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & 0 & -a_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 & -a_{d-2} \\ 0 & 0 & 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix} \in K^{d \times d}$$

hat. Diese Matrix heißt die **Begleitmatrix** von p. Es gilt $p = \mu_{M_p}$.

Algorithm 2.16. Gegeben: $\alpha \in \mathrm{End}(\mathcal{V})$, $\mathcal{V}$ endlich erzeugter K-Vektorraum.
Gesucht: Das Minimalpolynom $\mu_\alpha(x)$.
Algorithmus:

1. Wähle $V \in \mathcal{V} \setminus \{0\}$.
2. Bestimme das Minimalpolynom $\mu_{\alpha,V}(x)$ von V, setze $\mathcal{W} := K[\alpha]V$ und $\mu(x) := \mu_{\alpha,V}(x)$.
3. Solange $\mathcal{W} \neq \mathcal{V}$, wähle $V \in \mathcal{V} \setminus \mathcal{W}$, und bestimme das Minimalpolynom $\mu_{\alpha,V}(x)$. Ersetze
$$\mu(x) \qquad \text{durch} \qquad \mathrm{kgV}(\mu(x), \mu_{\alpha,V}(x)) = \frac{\mu(x)\mu_{\alpha,V}(x)}{\mathrm{ggT}(\mu(x), \mu_{\alpha,V}(x))}$$
und
$$\mathcal{W} \qquad \text{durch} \qquad \mathcal{W} + K[\alpha]V := \langle \mathcal{W}, K[\alpha]V \rangle.$$
Falls $\mathcal{W} \neq \mathcal{V}$, wiederhole Schritt 3.
4. Sobald $\mathcal{W} = \mathcal{V}$ ist, gilt $\mu_\alpha(x) = \mu(x)$.

Ende Vorl. 5

Beweis. Der Algorithmus terminiert nach spätestens $\mathrm{Dim}(\mathcal{V})$ Schritten. Wir zeigen durch Induktion nach der Anzahl der Schritte, dass das $\mathcal{W}$ in jedem Schritt invariant unter α und $\mu(x)$ das Minimalpolynom der Einschränkung von α auf $\mathcal{W}$ ist. Der Induktionsanfang ist gerade Bemerkung 2.14.
Induktionsannahme: Für das letzte $\mathcal{W}$ gilt: $\mathcal{W}$ ist invariant unter α und $\mu(x)$ ist das Minimalpolynom der Einschränkung von α auf $\mathcal{W}$.
Induktionsschritt: Sei nun $V \in \mathcal{V} \setminus \mathcal{W}$. Da $\mathcal{W}$ und $K[\alpha]V$ invariant unter α sind, gilt dies auch für das Erzeugnis $\mathcal{W} + K[\alpha]V$. Da $\widetilde{\mu}(x) := \mathrm{kgV}(\mu(x), \mu_{\alpha,V}(x))$ sowohl Vielfaches von $\mu(x)$ als auch von $\mu_{\alpha,V}(x)$ ist, gilt $\widetilde{\mu}(\alpha)(U) = 0$ sowohl für alle $U \in \mathcal{W}$ als auch für alle $U \in K[\alpha]V$, somit auch für alle U in dem Erzeugnis der beiden. Ein Polynom $r(x)$ mit $r(\alpha)(\mathcal{W} + K[\alpha]V) = \{0\}$ muss sowohl ein Vielfaches von $\mu(x)$ als auch von $\mu_{\alpha,V}(x)$ sein, also ein Vielfaches des kleinsten gemeinsamen Vielfaches $\widetilde{\mu}(x)$. □

Übung 2.2. Zeige, dass $\mathrm{Grad}(\mu_\alpha(x)) \leq \mathrm{Dim}(\mathcal{V})$.
Hinweis: Benutze die Beweisidee des Algorithmus. Das Minimalpolynom der Einschränkung von α auf $\mathcal{W} \cap K[\alpha]V$ teilt $\mu(x)$ und $\mu_{\alpha,V}(x)$.

Man beachte, dass der Algorithmus, wenn er nicht schon nach einem Schritt terminiert, wie im Beispiel 2.13 der Fall war, dann eine Faktorisierung des Minimalpolynoms gleichzeitig mitliefert. Dies wird sich als vorteilhaft erweisen.

3 Eigenvektoren und Diagonalisierbarkeit

Lernziel: Eigenwerte und Eigenvektoren, Beispiele von Eigenvektorbasen, diagonalisierbare Matrizen.

Definition 2.17. Sei $\alpha : \mathcal{V} \to \mathcal{V}$ Endomorphismus des K-Vektorraumes $\mathcal{V}$.

1. Ein $a \in K$ heißt **Eigenwert** von α, falls ein Vektor $V \in \mathcal{V}$ existiert mit

$$\alpha(V) = aV \text{ und } V \neq 0.$$

   In diesem Fall heißt V **Eigenvektor** und

$$E_\alpha(a) = E(a) := \mathrm{Kern}(\alpha - a\,\mathrm{id}_\mathcal{V})$$

   der **Eigenraum** zum Eigenwert a von α. Eine Zahl $a \in K$ ist also genau dann Eigenwert von α, wenn $E_a(A) \neq \{0\}$, also genau dann, wenn es einen Eigenvektor von α zu a gibt.

2. Ist E eine Basis aus Eigenvektoren bezüglich α von $\mathcal{V}$, so heißt E auch eine **Eigenvektorbasis** für α.

3. Wir nennen α **diagonalisierbar**, falls eine Eigenvektorbasis für α existiert.

4. Vermöge des K-Algebrenisomorphismus

$$\widetilde{\cdot} : K^{n\times n} \to \mathrm{End}(K^{n\times 1}), A \mapsto \widetilde{A}$$

   lassen sich die Begriffe auf quadratische Matrizen übertragen: Für $A \in K^{n\times n}$ heißt ein Vektor $X \in K^{n\times 1} \setminus \{0\}$ **Eigenvektor** von A zu $a \in K$, falls $AX = aX$ gilt und $E_a(A) = \{X \in K^{n\times 1} \mid AX = aX\}$ der **Eigenraum** von A zu a, etc.

Übung 2.3. Sei $A \in K^{n\times n}$. Zeige:

1. Für $g \in \mathrm{GL}_n(K)$ ist $g^{-1}Ag$ genau dann eine Diagonalmatrix, wenn die Spalten von g eine Eigenvektorbasis von A bilden.

2. Der Endomorphismus $\widetilde{A}$ (bzw. die Matrix A) ist genau dann diagonalisierbar, wenn eine Matrix $g \in \mathrm{GL}_n(K)$ existiert mit $g^{-1}Ag$ eine Diagonalmatrix.

Beispiel 2.18. Seien $s_1, \ldots, s_d \in K$ genau d verschiedene Elemente von K und $p := (x - s_1)\cdots(x - s_d) \in K[x]$. Dann ist

$$(q_1, \ldots, q_d) \text{ mit } q_i := p/(x - s_i) \in K[x]$$

eine Basis von $K[x]_{\mathrm{Grad}<d}$ und somit $E := (\overline{q_1}, \ldots, \overline{q_d}) \in (K[x]/pK[x])^d$ eine Basis von $K[x]/pK[x]$. Wegen $(x - s_i)q_i = p$ sieht man sofort $\overline{xq_i} = s_i\overline{q_i}$, d.h. die Matrix von m_p bezüglich der Basis E hat Diagonalgestalt:

$${}^E m_p^E = \mathrm{Diag}(s_1, \ldots, s_d) := \begin{pmatrix} s_1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & s_2 & 0 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & s_{d-1} & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & s_d \end{pmatrix}$$

Jedes $\overline{q_i}$ ist also Eigenvektor von m_p zum Eigenwert s_i.

Satz 2.19. *Sei $\alpha : \mathcal{V} \to \mathcal{V}$ Endomorphismus des endlich erzeugten K-Vektorraumes $\mathcal{V}$. Genau dann ist $a \in K$ Eigenwert von α, falls a Wurzel des Minimalpolynoms ist (d.h. $\mu_\alpha(a) = 0$).*

Beweis. Sei a Eigenwert von α, d.h. $E_\alpha(a) = \mathrm{Kern}(\alpha - a\,\mathrm{id}_\mathcal{V}) \neq \{0\}$. Dann induziert α auf $E_\alpha(a)$ die lineare Abbildung $\beta =$ Multiplikation mit a. Diese hat $x - a$ als Minimalpolynom. Wegen Lemma 2.11 ist also a Wurzel von $\mu_\alpha(x)$.
Sei umgekehrt $a \in K$ Wurzel von $\mu_\alpha(x)$, also $\mu_\alpha(x) = (x - a)q$ für ein $q \in K[x]$. Angenommen $E_\alpha(a) = \{0\}$. Dann ist der Kern von $\alpha - a\,\mathrm{id}_\mathcal{V}$ gleich 0, also $\alpha - a\,\mathrm{id}_\mathcal{V}$ bijektiv. Insbesondere

$$\mu_\alpha(\alpha) = 0 \text{ genau dann, wenn } q(\alpha) = 0,$$

was der Definition von $\mu_\alpha(x)$ als Minimalpolynom widerspricht. □

Beispiel 2.20. Sei $\mathcal{V}$ ein 2-dimensionaler $\mathbb{R}$-Vektorraum mit Basis $B \in \mathcal{V}^2$ und Endomorphismus $\alpha \in \mathrm{End}(\mathcal{V})$, so dass

$${}^B\alpha^B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Man sieht sofort, dass $\mu_\alpha(x) = x^2 - 1$ das Minimalpolynom ist, also 1 und -1 die Eigenwerte sind. Die Koordinatenspalten ${}^BV$ der Eigenvektoren zu Eigenwert 1 bzw. -1 bekommen wir durch Lösen des linearen Gleichungssystems

$$({}^B\alpha^B - I_2)X = 0 \text{ bzw. } ({}^B\alpha^B + I_2)X = 0$$

und erhalten

$$E_\alpha(1) = \{V \mid {}^BV = \begin{pmatrix} a \\ a \end{pmatrix}, a \in \mathbb{R}\} \text{ und } E_\alpha(-1) = \{V \mid {}^BV = \begin{pmatrix} a \\ -a \end{pmatrix}, a \in \mathbb{R}\}.$$

Also eine mögliche Eigenvektorbasis E ist gegeben durch die Spalten der Matrix

$${}^B\,\mathrm{id}_\mathcal{V}^E = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

wobei man aber auch jede Spalte durch ein Vielfaches $\neq 0$ ersetzen kann. Jedenfalls liefert diese oder eine in dieser Weise modifizierte Eigenvektorbasis die Matrix

$${}^E\alpha^E = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

für α, und zwar ohne jede weitere Rechnung. Insbesondere braucht die Inverse ${}^E\,\mathrm{id}_\mathcal{V}^B = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ von ${}^B\,\mathrm{id}_\mathcal{V}^E$ nicht berechnet zu werden.

Beispiel 2.21 (Projektionen)**.** Eine **Projektion** ist eine Abbildung $\pi \in \mathrm{End}(\mathcal{V})$ mit $\pi^2 = \pi$. Sieht man von den Grenzfällen $\pi = \mathrm{id}_\mathcal{V}$ und $\pi = 0_\mathcal{V}$ ab, so heißt dies, dass $x^2 - x = x(x-1)$ das Minimalpolynom von π ist. Offenbar sind 0 und 1 die Eigenwerte von π und aus $\mathrm{id}_\mathcal{V} = \pi + (\mathrm{id}_\mathcal{V} - \pi)$ folgt, dass $\mathcal{V} = E_\pi(0) \oplus E_\pi(1)$ gilt mit $E_\pi(0) := \mathrm{Kern}(\pi) = \mathrm{Bild}(\mathrm{id}_\mathcal{V} - \pi)$ und $E_\pi(1) := \mathrm{Kern}(\pi - \mathrm{id}_\mathcal{V}) = \mathrm{Bild}(\pi)$. Z.B. sieht man die letzte Gleichheit so: $(\pi - \mathrm{id}_\mathcal{V}) \circ \pi = 0$ besagt, dass $\mathrm{Bild}(\pi) \leq \mathrm{Kern}(\pi - \mathrm{id}_\mathcal{V})$. Umgekehrt ist $X \in \mathrm{Kern}(\pi - \mathrm{id}_\mathcal{V}) \iff \pi(X) - X = 0 \iff X = \pi(X)$, also $X \in \mathrm{Bild}(\pi)$. Die Trivialität des Durchschnittes $E_\pi(0) \cap E_\pi(1)$ folgt daraus, dass kein Vektor ungleich Null Eigenvektor zu zwei verschiedenen Eigenwerten sein kann.

Insbesondere hat man eine Eigenvektorbasis E für π mit ${}^E\pi^E = \mathrm{Diag}(\underbrace{1, \ldots, 1}_{\mathrm{Dim}\,E(1)}, \underbrace{0, \ldots, 0}_{\mathrm{Dim}\,E(0)})$.

Ende Vorl. 6

Lemma 2.22. *Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$. Sei $\pi \in \mathrm{End}(\mathcal{V})$ eine mit α vertauschbare Projektion, d.h. $\pi^2 = \pi$ und $\alpha \circ \pi = \pi \circ \alpha$. Dann sind $\mathrm{Kern}(\pi)$ und $\mathrm{Bild}(\pi) = \mathrm{Kern}(\pi - \mathrm{id}_\mathcal{V})$ beides α-invariante Teilräume von $\mathcal{V}$ und $\mathcal{V} = \mathrm{Kern}(\pi) \oplus_i \mathrm{Bild}(\pi)$.*

Beweis. Übung. □

Übung 2.4. Seien $\mathcal{V}$ ein endlich erzeugter K-Vektorraum, $\alpha \in \mathrm{End}(\mathcal{V})$ und $\mathcal{V} = \mathcal{T}_1 \oplus_i \mathcal{T}_2$ eine α-invariante direkte Summenzerlegung mit $\alpha_i := \alpha_{|\mathcal{T}_i} : \mathcal{T}_i \to \mathcal{T}_i$. Dann ist $\mu_\alpha = \mathrm{kgV}(\mu_{\alpha_1}, \mu_{\alpha_2})$. Vergleiche diese Aussage mit Lemma 2.11. Formuliere analog zu Bemerkung 2.12 die „Matrixversion" dieser Aussage aus.

Satz 2.23. *Sei $\mathcal{V}$ endlich erzeugter K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$ mit Minimalpolynom $\mu_\alpha(x) \in K[x]$.*

1. *Ist $\mu_\alpha(x) = p_1(x)p_2(x)$ mit $p_1, p_2 \in K[x]$ teilerfremd von positiven Graden und normiert, d.h. $\mathrm{ggT}(p_1, p_2) = 1$, dann gibt es eine mit α verträgliche direkte Summenzerlegung $\mathcal{V} = \mathcal{T}_1 \oplus \mathcal{T}_2$, so dass $\alpha_i : \mathcal{T}_i \to \mathcal{T}_i : T \mapsto \alpha(T)$ Minimalpolynom p_i für $i = 1, 2$ hat. Insbesondere hat ${}^B\alpha^B$ Blockdiagonalgestalt für angepaßte Basen B von $\mathcal{V}$.*

2. *Ist $\mu_\alpha(x) = \prod_{i=1}^d p_i$ mit $p_i \in K[x]$ paarweise teilerfremd und normiert, dann gibt es eine mit α verträgliche direkte Summenzerlegung $\mathcal{V} = \bigoplus_{i=1}^d \mathcal{T}_i$, so dass $\alpha_i := \alpha_{|\mathcal{T}_i} : \mathcal{T}_i \to \mathcal{T}_i$ Minimalpolynom p_i hat.*

Bemerkung 2.24. $\mathcal{V} = \bigoplus_{i=1}^d \mathcal{T}_i$ bedeutet, dass sich jedes $X \in \mathcal{V}$ eindeutig schreiben läßt als $X = \sum_{i=1}^d X_i$ mit $X_i \in \mathcal{T}_i$. Aus der linearen Algebra I (oder als leichte Übung) wissen wir, dass folgende Aussagen äquivalent sind:

1. $\mathcal{V} = \bigoplus_{i=1}^d \mathcal{T}_i$
2. Sind B_i Basen von $\mathcal{T}_i$ ($i = 1, \ldots, d$), so ist $B = \cup_{i=1}^d B_i$ eine Basis von $\mathcal{V}$ (eine solche Basis heißt **eine an die Zerlegung angepasste Basis**).
3. $\mathcal{V} = \mathcal{T}_1 + \mathcal{T}_2 + \ldots + \mathcal{T}_d =: \sum_{i=1}^d \mathcal{T}_i$. Der Vektorraum $\mathcal{V}$ wird also erzeugt von den $\mathcal{T}_i$ und für jedes $j \in \{1, \ldots, d\}$ ist $\mathcal{T}_j \cap (\sum_{i \neq j} \mathcal{T}_i) = \{0\}$.

Beweis von Satz 2.23. Wir übertragen eine Polynomrechnung in eine Rechnung mit Endomorphismen vermöge des Einsetzhomomorphismus $K[x] \to \mathrm{End}(\mathcal{V}) : p(x) \mapsto p(\alpha)$, welcher nach dem Homomorphiesatz einen Monomorphismus $K[x]/\mu_\alpha K[x] \to \mathrm{End}(\mathcal{V})$ induziert.

1. Wegen der Teilerfremdheit liefert der EUKLIDische Algorithmus Polynome $q_1, q_2 \in K[x]$ mit $1 = q_1p_1 + q_2p_2$. Setze $\pi_1 := (q_2p_2)(\alpha) = q_2(\alpha) \circ p_2(\alpha)$ und $\pi_2 := q_1(\alpha) \circ p_1(\alpha) = \mathrm{id}_\mathcal{V} - \pi_1$.
   Dann gilt für $i = 1, 2$:
   (a) $\pi_1 + \pi_2 = \mathrm{id}_\mathcal{V}$, denn $1 = q_1p_1 + q_2p_2$.
   (b) $\pi_i \circ \alpha = \alpha \circ \pi_i$, denn $q_ip_ix = xq_ip_i$; insbesondere sind $\mathrm{Kern}(\pi_1) = \mathrm{Bild}(\pi_2)$ und $\mathrm{Kern}(\pi_2) = \mathrm{Bild}(\pi_1)$ beides α-invariante Teilräume.
   (c) $\pi_1 \circ \pi_2 = \pi_2 \circ \pi_1 = 0$ da $p_1(\alpha)p_2(\alpha)$ ein Faktor von beiden ist.
   (d) $\pi_i^2 = \pi_i$, denn
   $$\pi_1 \circ \pi_1 = \pi_1 \circ (1 - \pi_2) = \pi_1 - \pi_1 \circ \pi_2 = \pi_1$$
   Also ist π_1 eine mit α vertauschbare Projektion und man erhält mit dem vorigen Lemma die α-invariante direkte Summenzerlegung
   $$\mathcal{V} = \mathrm{Bild}(\pi_1) \oplus_i \mathrm{Bild}(\pi_2) = \mathcal{T}_1 \oplus \mathcal{T}_2$$
   wobei $\mathcal{T}_i := \pi_i(\mathcal{V})$. Wegen $\mathcal{T}_1 = \mathrm{Kern}(\pi_2)$ und $\mathcal{T}_2 = \mathrm{Kern}(\pi_1)$ folgt (leichte Übung), dass p_i das Minimalpolynom von $\alpha_i := \alpha_{|\mathcal{T}_i} : \mathcal{T}_i \to \mathcal{T}_i$ ist.

2. Aus 1. durch Iteration. □

Beispiel 2.25. Sei $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 3}$. Dann ist

$$(E_1, AE_1, A^2E_1, A^3E_1) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

also $\mu_{A,E_1} = x^3 + x^2 + x = x(x^2 + x + 1) = \mu_A$,

$$\mathrm{ggT}(x, x^2 + x + 1) = 1 = (x + 1)x + (x^2 + x + 1).$$

Also ist $\pi_1 = A^2 + A + 1$ und $\pi_2 = A^2 + A = I_3 - \pi_1$. Bezüglich geeigneter Basen von $\mathrm{Bild}(\pi_1)$ und $\mathrm{Kern}(\pi_1)$ hat $\widetilde{A}$ die Gestalt $\mathrm{Diag}(0, M_{X^2+X+1}) = \mathrm{Diag}(0, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix})$. Es ist $\mathrm{Bild}(\pi_1) = \mathrm{Kern}(\pi_2)$ eindimensional, $\mathrm{Bild}(\pi_1) = \langle E_1 + AE_1 + A^2E_1 = (1, 1, 1)^{tr}\rangle$. Eine geeignete Basis von $\mathrm{Bild}(\pi_2)$ erhält man als $(A^2E_1 + AE_1 = (0, 1, 1)^{tr}, A(A^2E_1 + AE_1) = A^3E_1 + A^2E_1 = (1, 0, 1)^{tr}$, so dass $g^{-1}Ag = \mathrm{Diag}(0, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix})$ mit $g = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_2)$. Wieso gilt $\mathrm{Bild}(\pi_2) = \mathrm{Bild}(\widetilde{A})$?

Beispiel 2.26. Sei $\mathcal{V}$ ein 6-dimensionaler $\mathbb{F}_2$-Vektorraum mit Basis B und $\alpha \in \mathrm{End}(\mathcal{V})$ mit

$${}_B\alpha^B = \begin{pmatrix} \cdot & 1 & \cdot & 1 & \cdot & \cdot \\ 1 & 1 & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & 1 & 1 & 1 & 1 \\ \cdot & 1 & 1 & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot & 1 \\ \cdot & 1 & 1 & \cdot & \cdot & 1 \end{pmatrix}$$

Wenn wir α und seine Potenzen auf B_1 anwenden, sind die Koordinatenspalten der resultierenden Vektoren die Spalten der folgenden Matrix:

$$\begin{pmatrix} 1 & \cdot & 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & 1 & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & 1 & \cdot & 1 & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \end{pmatrix}$$

Die ersten 5 Spalten sind noch linear unabhängig, die letzte ist abhängig von den ersten 5 und wir erhalten $1 + x^4 + x^5$ als Teiler des Minimalpolynoms. $1 + x^4 + x^5$ hat keine Wurzeln in $\mathbb{F}_2$, aber $1 + x + x^2$ als irreduziblen Teiler, so dass wir

$$1 + x^4 + x^5 = (1 + x + x^2)(1 + x + x^3)$$

bekommen. Wenn wir geeignete Basen gefunden haben, so dass die Matrix von α Blockdiagonalgestalt hat, wird $1+x+x^2$ den Diagonalblock $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ betragen und $1+x+x^3$ den Diagonalblock $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Es kann höchstens noch ein Diagonalblock vom Grad 1 dazukommen. Wenn wir Spuren vergleichen, kommen wir zu dem Schluss, dass es (0) sein muss.

Insbesondere sollte 0 Eigenwert sein. Man überzeugt sich davon, dass $x(1+x+x^2)(1+x+x^3)$ das Minimalpolynom von α ist und weiß, dass es eine Basis C gibt mit

$$ {}^C\alpha^C = \mathrm{Diag}(0, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}). $$

Wie bestimmt man nun ${}^B\,\mathrm{id}_{\mathcal{V}}^C$? Der Weg, die Projektionen in die Komponenten mit Hilfe des EUKLIDischen Algorithmus auszurechnen, ist langwierig, weil man ja die Matrix einsetzen muss, aber möglich:

$$ 1 = (1+x)x + (1+x+x^2) $$

wird mit $1+x+x^3$ multipliziert und in

$$ 1 = xx(1+x+x^2) + (1+x)(1+x+x^3) $$

eingesetzt ergibt

$$ 1 = xx(1+x+x^2) + (1+x)^2x(1+x+x^3) + (1+x)(1+x+x^2)(1+x+x^3) $$

Statt nun α in jeden der drei Summanden einzusetzen, um die Projektionen zu bekommen kann man sich damit begnügen, nur jeweils einen Vektor in $\mathrm{Bild}(\alpha \circ (1+\alpha+\alpha^2)), \mathrm{Bild}(\alpha \circ (1+\alpha+\alpha^3)), \mathrm{Bild}((1+\alpha+\alpha^2)\circ(1+\alpha+\alpha^3))$ zu bestimmen. Dies bekommt man mit einer sehr schmerzfreien Rechnung, weil die $\alpha^i(B_1)$ schon bekannt sind. In den ersten beiden Fällen bekommt man die Vektoren mit den Komponenten

$$ \begin{pmatrix} 1 \\ 1 \\ 1 \\ \cdot \\ 1 \\ 1 \end{pmatrix} \text{ bzw. } \begin{pmatrix} 1 \\ 1 \\ \cdot \\ 1 \\ \cdot \\ \cdot \end{pmatrix} $$

jedoch beim dritten Fall leider Null. Also muss man einen anderen Vektor als B_1 iterieren. Im vorliegenden Fall kann man sich auch noch anders helfen: Man berechnet $\mathrm{Kern}(\alpha) = E_\alpha(0)$. Mit diesen Vektoren erhalten wir nach Umstellung der Komponenten entsprechend unserer angestrebten Blockdiagonalmatrix für α:

$$ {}^B\,\mathrm{id}_{\mathcal{V}}^C = \left(\begin{array}{c|cc|ccc} \cdot & 1 & \cdot & 1 & 1 & 1 \\ 1 & 1 & \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & 1 & \cdot & 1 \\ 1 & 1 & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 & 1 & 1 \end{array}\right) $$

Man würde jetzt nicht auf die Idee kommen, nach der Formel ${}^C\alpha^C = ({}^B\,\mathrm{id}_{\mathcal{V}}^C)^{-1}{}^B\alpha^B\,{}^B\,\mathrm{id}_{\mathcal{V}}^C$ nachzurechnen, ob wirklich die gewünschte Blockdiagonalmatrix herauskommt, sondern nur überprüfen, wie sich die Bilder der Spalten vor dem | jeweils aus den vorausgehenden Spalten (eine, zwei oder drei) linearkombinieren. Ende Vorl. 7

$$ \left(\begin{array}{cc|ccc|cccc} \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot \\ 1 & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 \\ 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot \end{array}\right) $$

Folgerung 2.27. *Sei $\mathcal{V}$ endlich erzeugter K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$ mit Minimalpolynom vom Grad d. Genau dann existiert eine Eigenvektorbasis für α, wenn $\mu_\alpha(x)$ genau d verschiedene Wurzeln $s_1, \ldots, s_d$ in K hat. (Also $\mu_\alpha(x) = \prod_{i=1}^{d}(x - s_i)$ für paarweise verschiedene $s_i \in K$.)*

Beweis. Sei E eine Eigenvektorbasis. Aus der Matrix

$$ {}^{E}\alpha^{E} = \mathrm{Diag}(a_1, \ldots, a_n) $$

lesen wir sofort das Minimalpolynom als $\prod_{i=1}^{d}(x-s_i)$ ab, wo s_i die *verschiedenen* Eigenwerte a_j durchläuft.
Sei umgekehrt $\mu_\alpha(x) = \prod_{i=1}^{d}(x - s_i)$ mit $s_i \in K$ paarweise verschieden. Wir wenden Satz 2.23 an mit den teilerfremden Polynomen $p_i := x - s_i$ $(i = 1, \ldots, d)$ und erhalten eine Zerlegung $\mathcal{V} = \bigoplus_{i=1}^{d} \mathcal{T}_i$ von $\mathcal{V}$ in α-invariante Teilräume $\mathcal{T}_i$ mit $\alpha_{|\mathcal{T}_i} = s_i \,\mathrm{id}_{\mathcal{T}_i}$. Es ist also $\mathcal{T}_i = E_\alpha(s_i)$. Eine Eigenvektorbasis von $\mathcal{V}$ erhält man durch Zusammenfügen beliebiger Basen der Teilräume $\mathcal{T}_i$. □

Beispiel 2.28. Seien $a_1, \ldots, a_n \in K$ paarweise verschieden und $A \in K^{n\times n}$ mit $A_{i,i} = a_i$ und $A_{i,j} = 0$ für $i > j$, $1 \le i, j \le n$ (also eine obere Dreiecksmatrix). Dann ist $\mu_A = \prod_{i=1}^{n}(x - a_i)$ (etwa mit Bemerkung 2.12) und A ist diagonalisierbar also ähnlich zu $\mathrm{Diag}(a_1, \ldots, a_n)$.

4 Das charakteristische Polynom

4.1 Das charakteristische Polynom eines Endomorphismus

Definition 2.29.

1. Sei $A \in K^{n\times n}$. Das **charakteristische Polynom** von A ist $\chi_A(x) = \det(xI_n - A) \in K[x]$.
2. Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$. Dann heißt

   $$ \chi_\alpha(x) := \det(xI_n - {}^{B}\alpha^{B}) $$

   das **charakteristische Polynom** von α, wobei $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$ ist.

Lemma 2.30. *Das charakteristische Polynom $\chi_\alpha(x)$ ist wohldefiniert und hängt insbesondere nicht von der Wahl der Basis B ab.*

Beweis. Man beachte zuerst, $xI_n - {}^{B}\alpha^{B} \in K(x)^{n\times n}$ und auf $K(x)^{n\times n}$ haben wir eine Determinante. Weiter ist das Ergebnis ein Polynom, also in $K[x]$ nach der Leibniz Regel für Determinanten. Schließlich sei $C \in \mathcal{V}^n$ eine weitere Basis von $\mathcal{V}$. Dann gilt mit $T = {}^{B}\mathrm{id}_{\mathcal{V}}^{C}$:

$$ \begin{aligned} \det(xI_n - {}^{C}\alpha^{C}) &= \det(xI_n - T^{-1}({}^{B}\alpha^{B})T) \\ &= \det(T^{-1}(xI_n - {}^{B}\alpha^{B})T) \\ &= \det(T)^{-1}\det(xI_n - {}^{B}\alpha^{B})\det(T) \\ &= \det(xI_n - {}^{B}\alpha^{B}) \end{aligned} $$

□

Beispiel 2.31.

1. Ist

   $$ A = \begin{pmatrix} a_1 & * & \ldots & * \\ 0 & a_2 & * & \vdots \\ \vdots & \ddots & & * \\ 0 & \ldots & 0 & a_n \end{pmatrix} $$

   so ist $\chi_A = (x - a_1)(x - a_2)\ldots(x - a_n)$.

2. Ist $A = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}$, so ist $\chi_A = \chi_{A_1}\chi_{A_2}$.

3. Ähnliche Matrizen haben das gleiche charakteristische Polynom.

4. Ist also A diagonalisierbar, so ist

$$\chi_A = \prod_{a \in EW(A)} (x-a)^{\dim E_A(a)},$$

wo $EW(A)$ die Menge der Eigenwerte von A bezeichnet.

Übung 2.5. Ist $A = aI_n + bJ_n$ mit $b \neq 0$ und

$$J_n = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \dots & \vdots \\ 1 & \dots & 1 \end{pmatrix} \in K^{n\times n}.$$

Zeige: J_n und somit A ist genau dann diagonalisierbar wenn $n1_K \neq 0$. In diesem Fall ist $EW(A) = \{a+nb, a\}$ und die Dimension der Eigenräume ist 1 bzw. $n-1$. Also ist $\chi_A = (x-(a+nb))(x-a)^{n-1}$, $\mu_A = (x-(a+nb))(x-a)$.

Hier sind die wichtigsten Eigenschaften des charakteristischen Polynoms.

Satz 2.32. *Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$. Dann gilt:*

1. *$\chi_\alpha(x) \in K[x]$ ist normiert vom Grad $n = \mathrm{Dim}(\mathcal{V})$. Der Koeffizient von x^{n-1} ist gleich $-\mathrm{Spur}(\alpha)$ und der Koeffizient von x^0 ist $(-1)^n \det(\alpha)$.*

2. *$a \in K$ ist Eigenwert von α genau dann, wenn $\chi_\alpha(a) = 0$, d.h. falls a eine Wurzel von $\chi_\alpha(x)$. In anderen Worten, das Minimalpolynom und das charakteristische Polynom haben dieselben Nullstellen[1].*

3. *(HAMILTON-CAYLEY) $\chi_\alpha(\alpha) = 0$, d.h. das Minimalpolynom teilt das charakteristische Polynom: $\mu_\alpha(x) | \chi_\alpha(x)$.*

Beweis.

1. Setze $A := {}^B\alpha^B$ und $M := xI_n - A$ und für jede Teilmenge $T \subseteq \underline{n} := \{1, \dots, n\}$ sei $M_T \in K(x)^{n\times n}$ gegeben durch die Spalten

$$(M_T)_{-,i} := \begin{cases} x(I_n)_{-,i} & i \notin T \\ -A_{-,i} & i \in T \end{cases}$$

Dann ist wegen der Multilinearität der Determinante und dem Laplaceschen Entwicklungssatz

$$\begin{aligned} \chi_\alpha(x) &= \det(M) \\ &= \textstyle\sum_{T\subseteq\underline{n}} \det(M_T) \\ &= \textstyle\sum_{T\subseteq\underline{n}} x^{n-|T|} \det(-A_{|T\times T}), \end{aligned}$$

wobei $\det(-A_{|T\times T})$ für $T = \emptyset$ als 1 zu interpretieren ist. Die erste Behauptung folgt nun leicht.

2. $\mathrm{Kern}(\alpha - a\,\mathrm{id}_\mathcal{V}) \neq \{0\}$ ist äquivalent mit $\det(\alpha - a\,\mathrm{id}_\mathcal{V}) = 0$, d.h. $\chi_\alpha(a) = 0$.

[1] ZUNÄCHST NOCH IN K, DAHER IST HAMILTON-CAYLEY ist schärfer.

3. Da $\chi_\alpha(x) \neq 0$, ist $xI - A \in K(x)^{n\times n}$ invertierbar. Sei die Matrix der Kofaktoren[2] von $xI_n - A$ gleich $M \in K(x)^{n\times n}$. Nach der Cramerschen Regel ist klar, dass die Einträge von M Polynome vom Grad $\leq n-1$ sind, so dass wir schreiben können:

$$M = M^{(0)} + xM^{(1)} + x^2M^{(2)} + \ldots + x^{n-1}M^{(n-1)}$$

mit $M^{(i)} \in K^{n\times n}$. Wir wissen wegen der Darstellung der Inversen nach der CRAMERschen Regel:

$$\begin{aligned}\chi_\alpha(x)I_n &= (xI_n - A)M \\ &= (xI_m - A)(M^{(0)} + xM^{(1)} + x^2M^{(2)} + \ldots + x^{n-1}M^{(n-1)}) \\ &= -AM^{(0)} + x(M^{(0)} - AM^{(1)}) + x^2(M^{(1)} - AM^{(2)}) + \cdots \\ &\quad + x^{n-1}(M^{(n-2)} - AM^{(n-1)}) + x^nM^{(n-1)}\end{aligned}$$

Ist nun $\chi_\alpha(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$, so bekommen wir durch Vergleich der Matrixkoeffizienten der x^i aus der letzten Formel

$$a_0I_n = -AM^{(0)}, a_1I_n = M^{(0)} - AM^{(1)}, \ldots$$

$$\ldots, a_{n-1}I_n = M^{(n-2)} - AM^{(n-1)}, I_n = M^{(n-1)}.$$

Multiplizieren wir jedes a_iI_n mit A^i und summieren auf, bekommen wir eine Teleskopreihe, d.h. $\chi_\alpha(A) = 0$. □

Folgerung 2.33. *Ist $p \in K[x]$ normiert vom Grad n und $A = M_p$ die Begleitmatrix von p, dann gilt $\chi_A = \mu_A = p$. Allgemeiner gilt wegen $\mu_A \mid \chi_A$, dass $\chi_A = \mu_A$, falls $\mathrm{Grad}(\mu_A) = n$.*

Ende Vorl. 8

4.2 Die Zerlegung in Haupträume

Bemerkung 2.34. (Erinnerung) Sei $\mathcal{V}$ ein endlich dimensionaler K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$. Schreibe das Minimalpolynom $\mu_\alpha = \prod_{i=1}^{\ell} p_i^{m_i}$ mit p_i irreduzibel normiert und paarweise verschieden. Setzt man $q_i := \prod_{j\neq i} p_j^{m_j}$, so sind die Teilräume

$$\mathcal{U}_i := \mathrm{Kern}(p_i(\alpha)^{m_i}) = \mathrm{Bild}(q_i(\alpha)),$$

α-invariante Teilräume von $\mathcal{V}$, die wir auch **Haupträume** nennen wollen. Es gilt

$$\mathcal{V} = \bigoplus_i \mathcal{U}_i$$

und für $\alpha_i := \alpha_{|\mathcal{U}_i}$ ist $\mu_{\alpha_i} = p_i^{m_i}$. Ist B_i eine Basis von $\mathcal{U}_i$ $(1 \leq i \leq \ell)$, so ist $B := (B_1, \ldots, B_\ell)$ eine Basis von $\mathcal{V}$ und

$${}^B\alpha^B = \mathrm{Diag}({}^{B_1}\alpha_1^{B_1}, \ldots, {}^{B_l}\alpha_\ell^{B_\ell}).$$

Beweis. Schreibt man

$$1 = \sum_{i=1}^{\ell} a_iq_i \in K[x],$$

so sind die $\pi_i = a_i(\alpha)q_i(\alpha)$ mit α vertauschbare Projektionen. Es ist

$$\pi_i \circ \pi_j = \delta_{ij}\pi_i, \ \mathrm{id}_\mathcal{V} = \pi_1 + \ldots + \pi_\ell.$$

[2] Die Matrix der Kofaktoren von $A \in K^{n\times n}$ ist die nach der Cramerschen Regel eindeutig bestimmte Matrix B mit $(\det A)I_n = AB$.

Setze $\mathcal{U}_i := \mathrm{Bild}(\pi_i) = \mathrm{Bild}(q_i(\alpha))$. Für jedes $X \in \mathcal{V}$ gilt $X = \mathrm{id}_\mathcal{V}(X) = \sum_{i=1}^{\ell} \pi_i(X)$, also ist $\mathcal{V} = \sum \mathcal{U}_i$. Weiter ist für alle $i \in \{1, \ldots, \ell\}$

$$\mathcal{U}_i \cap \sum_{j \neq i} \mathcal{U}_j = \mathrm{Bild}(\pi_i) \cap \mathrm{Bild}(1 - \pi_i) = E_{\pi_i}(1) \cap E_{\pi_i}(0) = \{0\}$$

und somit haben wir eine direkte Summenzerlegung in α-invariante Teilräume

$$\mathcal{V} = \mathcal{U}_1 \oplus \ldots \oplus \mathcal{U}_\ell.$$

Das Minimalpolynom μ_{α_i} von α_i teilt sicherlich $p_i^{m_i}$, da $p_i^{m_i}(\alpha)_{|\,\mathrm{Bild}(q_i)} = 0$. Andererseits teilt μ_α das Produkt $\prod_{i=1}^{\ell} \mu_{\alpha_i}$ und somit muss $\mu_{\alpha_i} = p_i^{m_i}$ gelten. □

Satz 2.35. *Sei $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\mu_\alpha = p^m$ für ein irreduzibles normiertes Polynom $p \in K[x]$. Dann gibt es $1 \leq m_1, m_2, \ldots, m_s \leq m$ und eine Basis B von $\mathcal{V}$ so dass*

$${}^B\alpha^B = \begin{pmatrix} M_{p^{m_1}} & * & \ldots & * \\ 0 & M_{p^{m_2}} & * & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \ldots & 0 & M_{p^{m_s}} \end{pmatrix}$$

Insbesondere gilt $d := \mathrm{Grad}(p) \mid \mathrm{Dim}(\mathcal{V}) =: n$ und $\chi_\alpha = p^c$ mit $c := m_1 + \cdots + m_s = \frac{n}{d} \geq m$. Schließlich gilt für mindestens ein $i \in \{1, \ldots, s\}$, dass $m_i = m$ ist.

Beweis. Eine solche Basis B erhält man, indem man zunächst ein $0 \neq X_1 \in \mathcal{V}$ wählt. Dieses X_1 erzeugt einen α-invarianten Teilraum $\mathcal{V}_1 \leq \mathcal{V}$, $\mathcal{V}_1 = \langle X_1, \alpha(X_1), \ldots, \alpha^{dm_1-1}(X_1)\rangle$ der Dimension dm_1 (Übung: Warum ist die Dimension ein Vielfaches von d?). Auf dem Faktorraum $\mathcal{V}/\mathcal{V}_1$ induziert α einen Endomorphismus dessen Minimalpolynom ein Teiler von μ_α ist. Dort wählt man wieder ein $0 \neq X_2 + \mathcal{V}_1$, bildet den von $X_2 + \mathcal{V}_1$ erzeugten α-invarianten Teilraum der Dimension dm_2 und setzt $\mathcal{V}_2 = \langle \alpha^t(X_1), \alpha^t(X_2) | t \in \mathbb{N}_0\rangle$, usw. Die Basis B ergibt sich dann als

$$B = (X_1, \alpha(X_1), \ldots, \alpha^{dm_1-1}(X_1), X_2, \alpha(X_2), \ldots, \alpha^{dm_2-1}(X_2), \ldots, \alpha^{dm_s-1}(X_s)). \quad \square$$

Folgerung 2.36. *Sei $\mu_\alpha(x) = \prod_{i=1}^{\ell} p_i^{m_i}$ eine Zerlegung des Minimalpolynoms in normierte irreduzible und paarweise verschiedene Polynome p_i. Dann gilt $\chi_\alpha(x) = \prod_{i=1}^{\ell} p_i^{c_i}$ mit $c_i \geq m_i$. Weiter gilt für die Dimension des p_i-***Hauptraumes*** $\mathcal{U}_i := \mathrm{Kern}(p_i^{m_i}(\alpha))$*

$$\mathrm{Dim}(\mathcal{U}_i) = \mathrm{Dim}(\mathrm{Kern}(p_i^{m_i}(\alpha))) = c_i \,\mathrm{Grad}(p_i).$$

Insbesondere ist $\sum_i c_i \,\mathrm{Grad}(p_i) = \mathrm{Dim}\,\mathcal{V}$.

Übung 2.6. Zeige $\mathrm{Kern}(p_i^{m_i}(\alpha)) = \mathrm{Kern}(p_i^{c_i}(\alpha)) = \mathrm{Bild}(q_i(\alpha)) = \mathrm{Bild}(r_i(\alpha))$ wobei $r_i := \prod_{j \neq i} p_j^{c_j}$. Man hätte also die Zerlegung auch mit dem charakteristischen Polynom bekommen. Man zähle die Vorteile des Minimalpolynoms auf und entscheide, ob diese durch die explizite Formel für das charakteristische Polynom sowie durch die Dimensionsformel für die Haupträume aufgehoben werden.

Beispiel 2.37. Sei

$$A := \begin{pmatrix} 1 & 1 & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & 1 & 1 & 1 \\ \cdot & \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 & 1 \\ \cdot & 1 & 1 & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix} \in \mathbb{F}_2^{6\times 6}$$

Die Vektoren $E_1, AE_1, A^2E_1, A^3E_1, A^4E_1$ bilden die Spalten der Matrix

$$M := \begin{pmatrix} 1 & 1 & 1 & 1 & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & 1 \\ \cdot & \cdot & 1 & 1 & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \end{pmatrix}$$

Man liest ab $\mu_{A,E_1} = x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Der Raum $\mathcal{V}_1 := \langle E_1, AE_1, A^2E_1, A^3E_1 \rangle$ ist 4-dimensional und enthält nicht E_2. Die Vektoren E_2, $AE_2 = (1,0,0,0,1,0)^{tr}$, $A^2E_2 = (1,0,1,1,0,1)^{tr}$ erfüllen $E_2 + AE_2 + A^2E_2 = (0,1,1,1,1,1)^{tr} \in \mathcal{V}_1$. Setzt man also

$$T := \begin{pmatrix} 1 & 1 & 1 & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & \cdot & \cdot \end{pmatrix}$$

so erhält man

$$T^{-1}AT = \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 \end{pmatrix}.$$

Es gilt $\mu_A = p^2$, $\chi_A = p^3$ wobei $p = x^2 + x + 1 \in \mathbb{F}_2[x]$. Was muss man machen um eine Matrix T_1 zu finden mit $T_1^{-1}AT_1 = \mathrm{Diag}(M_{p^2}, M_p)$?

Kapitel 3

Moduln

1 Moduln

Definition 3.1. Sei R ein Ring. Eine abelsche Gruppe $(M, +)$ heißt R-**Modul** (genauer R-Linksmodul), falls eine Abbildung

$$R \times M \to M : (r, m) \mapsto rm$$

gegeben ist mit

$$\begin{aligned} r(m+n) &= rm + rn, \\ (rs)m &= r(sm), \\ (r+s)m &= rm + sm \\ 1m &= m \end{aligned}$$

für alle $r, s \in R, m, n \in M$.
Ist M ein R-Modul, so heißt eine Teilmenge $T \subseteq M$ ein **Teilmodul** von M, in Zeichen $T \leq M$, falls $T \neq \emptyset$ und für alle $t_1, t_2 \in T$, $a \in R$ auch $at_1 + t_2 \in T$ gilt.

Man ist versucht zu sagen, dass Moduln Vektorräume über Ringen sind. Richtig ist natürlich, dass Vektorräume Moduln über Körpern sind.

Übung 3.1. Zeigen Sie, dass Teilmoduln genau die Teilmengen T von M sind, die mit der Einschränkung der Addition und Skalarmultiplikation von M auf T wieder zu R-Moduln werden.

Beispiel 3.2.

1. Jede abelsche Gruppe $(M, +)$ ist ein $\mathbb{Z}$-Modul mit

$$am := \begin{cases} \underbrace{m + \ldots + m}_{a}, & a \geq 0 \\ -\underbrace{(m + \ldots + m)}_{-a}, & -a \geq 0. \end{cases}$$

2. Sei $\mathcal{V}$ ein K-Vektorraum für einen Körper K und $\varphi \in \mathrm{End}_K(\mathcal{V})$. Dann wird V zu einem $K[x]$-Modul durch die Setzung

$$p(x)v := (p(\varphi))(v) \text{ für alle } p(x) \in K[x], v \in \mathcal{V}.$$

Übung 3.2. Sei $\psi : R \to S$ ein Ringhomomorphismus und M ein S-Modul. Dann wird M zu einem R-Modul, durch $rm := \psi(r)m$ für $r \in R, m \in M$.

Ist ψ injektiv (also $R \cong \psi(R)$ ein Teilring von S), so nennt man den R-Modul M auch die **Einschränkung** des S-Moduls M. Ist ψ surjektiv (also $S \cong R/\operatorname{Kern}(\psi)$), so nennt man den R-Modul M auch die **Aufblasung** (Inflation) des S-Moduls M.

Bemerkung 3.3.

1. Sei M ein R-Modul und $\mathcal{T}$ eine Menge von Teilmoduln von M. Dann gilt:

$$\bigcap_{T \in \mathcal{T}} T \leq M$$

   ist wieder ein Teilmodul von M.

2. Für $X \subseteq M$ so ist das **Erzeugnis** $\langle X \rangle := \bigcap_{X \subset T \leq M} T$ der kleinste Teilmodul von M, welcher X enthält.

3. Es gilt für $\emptyset \neq X \subseteq M$

$$\langle X \rangle = \{m \in M | \text{ es existieren } k \in \mathbb{N}, a \in R^k, v \in X^k \text{ mit } m = a_1 v_1 + \cdots + a_k v_k\}$$

   und $\langle \emptyset \rangle = \{0\}$.

Beweis. zu 3. Man rechnet leicht nach, dass die Menge $\overline{X}$ auf der rechten Seite ein R-Teilmodul von M ist. (Die Konvention, dass die leere Linearkombination gleich 0 ist, führt zu einer Vereinheitlichung der beiden Fälle.) Offenbar gilt $X \subseteq \overline{X}$. Also nach Definition gilt somit $\langle X \rangle \leq \overline{X}$. Aber andererseits ist $\overline{X}$ in jedem Teilmodul von M enthalten, der X enthält. Das liefert die Gleichheit. □

Definition 3.4. Eine Abbildung $\varphi : M \to N$ von R-Moduln M, N heißt R-**Modulhomomorphismus**, falls

$$\varphi(rm_1 + sm_2) = r\varphi(m_1) + s\varphi(m_2)$$

für alle $r, s \in R$ und alle $m_1, m_2 \in M$ gilt. In diesem Fall heißt die Faser über 0

$$\operatorname{Kern}(\varphi) := \{m \in M | \varphi(m) = 0\}$$

der **Kern** von φ.

Bemerkung 3.5.

1. Die Komposition von R-Modulhomomorphismen ist ein R-Modulhomomorphismus.

2. Ist $\varphi : M \to N$ ein R-Modulhomomorphismus, so ist $\operatorname{Kern}(\varphi)$ ein Teilmodul von M und $\operatorname{Bild}(\varphi) := \{\varphi(m) \mid m \in M\}$ ein Teilmodul von N.

3. φ ist injektiv genau dann wenn $\operatorname{Kern}(\varphi) = \{0\}$ ist.

4. φ ist surjektiv genau dann wenn $\operatorname{Bild}(\varphi) = N$ ist.

5. Ist φ bijektiv (also ein **Isomorphismus**), so ist die Umkehrabbildung φ^{-1} wieder ein R-Modulisomorphismus. Insbesondere ist Isomorphie von Moduln eine Äquivalenzrelation.

6. R-Modulhomomorphismen von M in sich selbst heißen **Endomorphismen**. $\operatorname{End}_R(M) := \{\varphi : M \to M \mid \varphi\ R-\text{Modulhomomomorphismus }\}$ heißt der **Endomorphismenring** des R-Moduls M. Es ist $\operatorname{End}_R(M)$ ein Ring, im Fall dass R kommutativ ist, sogar eine R-Algebra.

Beweis. Übungsaufgabe. □

Ende Vorl. 9

Übung 3.3. Die Spalten der Matrix A in $\mathbb{Z}^{n\times n}$ bilden genau dann ein Erzeugendensystem des $\mathbb{Z}$-Moduls $\mathbb{Z}^{n\times 1}$ wenn

$$A \in \mathrm{GL}_n(\mathbb{Z}) = (\mathbb{Z}^{n\times n})^* = \{g \in \mathbb{Z}^{n\times n} \mid \det(g) \in \{\pm 1\}\}.$$

Die Tatsache, dass R ein Ring ist, erlaubt es uns, beliebige Moduln als Faktormoduln freier Moduln zu beschreiben und so einen ersten Rahmen zu bekommen, wie man Moduln konstruiert.

Bemerkung 3.6. Sei R ein Ring.

1. $M = R$ kann als R-Modul aufgefasst werden durch

   $$R \times M \to M : (r, m) \mapsto rm \qquad \text{(Produkt in } R\text{)}.$$

   Diesen Modul bezeichnen wir mit ${}_RR$. Er heißt der **reguläre R-Modul**. Seine Teilmoduln nennt man auch **Linksideale**.

2. Ist M irgendein R-Modul und $m \in M$, dann gibt es genau einen R-Modulhomomorphismus

   $$\varphi_m : {}_RR \to M \text{ mit } \varphi_m(1) = m.$$

3. Sind M und N R-Moduln, so auch die direkte Summe $M \oplus N$ (entspricht dem direkten Produkt bei abelschen Gruppen in additiver Schreibweise) durch die R-Operation

   $$r(m, n) := (rm, rn) \text{ für alle } m \in M, n \in N, r \in R.$$

   $M \oplus N$ heißt die **direkte Summe** der R-Moduln M und N.

4. Ist A eine beliebige Menge, so ist R^A ein R-Modul mit werteweiser Addition und Produkt:

   $$R \times R^A \to R^A : (r, f) \mapsto (a \mapsto rf(a)).$$

   Im Falle von $A = \underline{n}$ schreiben wir R^n statt $R^{\underline{n}}$.

Beweis.

1. Klar.

2. Existenz:

   $$\varphi : {}_RR \to M : r \mapsto rm$$

   ist wohldefiniert und hat die gewünschte Eigenschaft.
   Eindeutigkeit: Sei ψ ein weiterer Homomorphismus mit dieser Eigenschaft. Dann gilt für alle $r \in {}_RR$:

   $$\psi(r) = \psi(r1) = r\psi(1) = rm = \varphi_m(r), \text{ also } \psi = \varphi_m.$$

3. Übung.

4. Übung. □

Übung 3.4. Zeige: Sind A und B disjunkte Mengen, so gilt: $R^A \oplus R^B \cong R^{A\cup B}$ als R-Moduln.

Bemerkung 3.7. Sei A eine Menge und für jedes $a \in A$ sei $e_a \in R^A$ die charakteristische Funktion von $\{a\}$, definiert durch

$$e_a(b) := \begin{cases} 0, & b \neq a \\ 1, & b = a \end{cases}$$

Dann ist der von den e_a mit $a \in A$ erzeugte R-Teilmodul von R^A gegeben durch

$$\mathrm{Fr}_R(A) := \langle e_a | a \in A \rangle_R = \{f \in R^A \mid |\{a \in A | f(a) \neq 0\}| < \infty\} \leq R^A.$$

$\mathrm{Fr}_R(A)$ heißt der **freie R-Modul auf** A.

Satz 3.8. *Sei R ein Ring, A eine Menge. Der Modul $\mathrm{Fr}_R(A) := \langle e_a | a \in A \rangle_R \leq_R R^A$ hat folgende Eigenschaft: Für jeden R-Modul M und jede Abbildung $\psi : A \to M$ gibt es genau einen R-Modulhomomorphismus*

$$\begin{array}{rcll} \tilde{\psi} : \mathrm{Fr}_R(A) & \to & M & \textit{mit} \\ \tilde{\psi}(e_a) & = & \psi(a) & \textit{für alle } a \in A. \end{array}$$

Moduln, die isomorph zu $\mathrm{Fr}_R(A)$ sind, heißen **frei** *auf dem Erzeugendensystem, welches $(e_a)_{a \in A}$ entspricht. Ein freies Erzeugendensysteme heißt auch* **Basis**, *genauer R-Modulbasis.*

Beispiel 3.9. ${}_RR$ ist frei auf $\{1\}$.
Der Spaltenmodul $R^{n \times 1}$ ist frei auf den Einheitsspalten $(e_1, \ldots, e_n)$.

Beweis. Jedes Element aus $\mathrm{Fr}_R(A)$ hat eine eindeutige Darstellung als

$$\sum_{a \in A} r_a e_a$$

mit $r_a \in R$ und $r_a = 0$ für alle bis auf endlich viele $a \in A$. Daher ist

$$\tilde{\psi} : \mathrm{Fr}_R(A) \to M : \sum_{a \in A} r_a e_a \mapsto \sum_{a \in A} r_a \psi(a)$$

eine wohldefinierte Abbildung, von der man leicht zeigt, dass sie ein Modulhomomorphismus ist. Sie erfüllt sicher die Bedingung $\tilde{\psi}(e_a) = \psi(a)$ für alle $a \in A$ und ist auch der einzige Modulhomomorphismus mit dieser Eigenschaft. □

Übung 3.5. Sei R ein kommutativer Ring. Dann gilt

$$\mathrm{End}_R(R^n) \cong R^{n \times n},$$

wobei wir $R^{n \times n}$ durch komponentenweise Addition und übliche Multiplikation zu einem Ring machen. Genauer: Identifiziere R^n mit $R^{n \times 1}$. Dann liefert das Heranmultiplizieren von Matrizen aus $R^{n \times n}$ eine eindeutige Darstellung der Endomorphismen von $R^{n \times 1}$ durch Matrizen. Man setzt
$\mathrm{GL}(n, R) := (R^{n \times n})^*$. (Beachte, der Fall $n = 1$ ist schon interessant.)
(Hinweis:

$$\widetilde{A} : R^{n \times 1} \to R^{n \times 1} : X \mapsto AX$$

ist für jedes $A \in R^{n \times n}$ ein R-Modulendomorphismus und jede Matrix induziert einen anderen Endomorphismus, da ein Endomorphismus durch die Bilder der (freien) Erzeuger $e_1, \ldots, e_n$ festgelegt ist, die wie in der linearen Algebra in den Spalten der beschreibenden Matrix stehen. Da diese Bilder beliebig vorgegeben werden können, folgt die Behauptung, wenn man beachtet, dass der Summe und dem Matrixprodukt gerade die Summe und die Hintereinanderausführung der Endomorphismen entsprechen.)

2 Homomorphiesätze und der chinesische Restsatz.

2.1 Der Homomorphiesatz für Moduln

Bemerkung 3.10. Sei R Ring und M ein R-Modul mit Teilmodul $U \leq M$.

1. Für $m \in M$ heißt
$$m + U := \{m + u | u \in U\}$$
die **Restklasse** von m nach U. Die Menge
$$M/U := \{m + U | m \in M\}$$
aller Restklassen nach U in M bilden den **Faktormodul** M/U von M nach U vermöge der folgenden Verknüpfungen:
$$+ : M/U \times M/U \to M/U : (m_1 + U, m_2 + U) \mapsto (m_1 + m_2) + U$$
und
$$\cdot : R \times M/U \to M/U : (r, m + U) \mapsto rm + U.$$

2. Der **natürliche Epimorphismus**
$$\nu = \nu_U : M \to M/U : m \mapsto m + U$$
ist ein R-Modulepimorphismus mit $\mathrm{Kern}(\nu_U) = U$.

Beweis.

1. Wir müssen zeigen, dass $+$ und $\cdot$ wohldefiniert sind. $+$ lassen wir als Übung. Für $\cdot$ sei $m+U = n+U$. Wir zeigen: $rm+U = rn+U$. Aber $m-n \in U$, also auch $r(m-n)$, also $rm + U = rn + U$. Die R-Modulaxiome müssen verifiziert werden. Z. B. ist $U = 0 + U$ das Nullelement von M/U. Den Rest lassen wir als Übung.

2. Dies folgt direkt aus der Definition der Addition von Restklassen. □

Der nächste Schritt in der allgemeinen Modultheorie ist der **Homomorphiesatz**, dessen Beweis genau so einfach ist wie bei Vektorräumen.

Satz 3.11. *Sei $\varphi : M \to N$ ein R-Modulhomomorphismus. Dann faktorisiert φ als*
$$\varphi = \widetilde{\varphi} \circ \nu_{\mathrm{Kern}(\varphi)}$$
über $M/\mathrm{Kern}(\varphi)$ mit $\nu_{\mathrm{Kern}(\varphi)}$ ein R-Modulepimorphismus und den R-Modulmonomorphimus
$$\widetilde{\varphi} : M/\mathrm{Kern}(\varphi) \to N : m + \mathrm{Kern}(\varphi) \mapsto \varphi(m).$$

Bemerkung 3.12. Ist M ein endlich erzeugter R-Modul, so gibt es ein $n \in \mathbb{N}$ und einen R-Modulepimorphismus $\varepsilon : R^{n\times 1} \to M$. Insbesondere $M \cong R^{n\times 1}/\mathrm{Kern}(\varepsilon)$.

Beweis. Sei $\psi : \underline{n} \to M$ gegeben, so dass $\mathrm{Bild}(\psi)$ ein Erzeugendensystem von M ist. Der eindeutige R-Modulhomomorphismus $\varepsilon : R^{n\times 1} \to M$ mit $\varepsilon \circ S = \psi$, wo S die Standardbasis von $R^{n\times 1}$ ist, ist dann ein Epimorphismus. □

Beispiel 3.13.

1. Jede abelsche Gruppe, die von zwei Elementen erzeugt wird, ist von der Form $\mathbb{Z}^2/M$ wobei M ein $\mathbb{Z}$-Teilmodul von $\mathbb{Z}^2 \cong \mathrm{Fr}_{\mathbb{Z}}(\underline{2})$ ist.

2. Sei K ein Körper und $\mathcal{V}$ ein endlich erzeugter K-Vektorraum mit $\varphi \in \mathrm{End}_K(\mathcal{V})$, so dass das Minimalpolynom und das charakteristische Polynom von φ beide gleich $p(x) \in K[x]$ sind, so gilt (vgl. Begleitmatrix von $p(x)$):
$$\mathcal{V} \cong_{K[x]\ K[x]} K[x]/\langle p(x)\rangle.$$

2.2 Ringe und Ideale

Wir kommen zu dem Homomorphiesatz von Ringen. Zuerst sieht die Definition eines Ideals etwas sonderbar aus, wird aber einsichtig, wenn man sich vorstellt, dass ein Ideal etwas ist, was man gleich Null setzen kann, um einen neuen Ring zu bekommen.

Definition 3.14. Sei R ein Ring.

1. $I \subseteq R$ heißt **Ideal** von R, in Zeichen $I \trianglelefteq R$, falls
   - $I \neq \emptyset$ und
   - $a, b \in I$ und $r, s \in R$ impliziert $ra + bs \in I$.
2. Sind $I_1, I_2 \trianglelefteq R$ so heißt das kleinste Ideal $I_1 + I_2$, welches I_1 und I_2 enthält, die **Summe** von I_1 und I_2.

Beispiel 3.15.

1. Für $R = \mathbb{Z}$ ist $3\mathbb{Z} = \langle 3 \rangle = \{3z \mid z \in \mathbb{Z}\}$ ein Ideal: $\langle 3 \rangle \trianglelefteq \mathbb{Z}$.
2. Ist K ein Körper und $a \in K$, dann ist
$$\{p(x) \in K[x] \mid p(a) = 0\} = \langle x - a \rangle := \{p(x)(x - a) \mid p(x) \in K[x]\} \trianglelefteq K[x].$$
3. Ist R ein kommutativer Ring mit Eins, so sind die Ideale in R genau die R-Teilmoduln von ${}_R R$, sprich die Linksideale.
4. Der Durchschnitt einer Menge von Idealen ist wieder ein Ideal.
5. Ist $M \subseteq R$, so heißt
$$\langle M \rangle := \bigcap_{M \subseteq I \trianglelefteq R} I$$
das von M **erzeugte Ideal**. Ist $M = \{a_1, \ldots a_n\}$ so schreibt man auch $\langle a_1, \ldots, a_n \rangle$ statt $\langle M \rangle$.
6. Ist R ein kommutativer Ring mit Eins, so heißt
$$\langle a \rangle := \{ra \mid r \in R\}$$
das von $a \in R$ erzeugte **Hauptideal**: $\langle a \rangle \trianglelefteq R$.
7. Ist $\varphi : R \to S$ ein Ringhomomorphismus, dann ist
$$\mathrm{Kern}(\varphi) := \{r \in R \mid \varphi(r) = 0\}$$
ein Ideal von R:
$$\mathrm{Kern}(\varphi) \trianglelefteq R.$$

Übung 3.6. Das von M erzeugte Ideal ist

$$\langle M \rangle = \left\{ \sum_{i=1}^{n} a_i m_i b_i \mid n \in \mathbb{N}_0, a_i, b_i \in R, m_i \in M \right\}.$$

Benutze diese Beschreibung um zu zeigen, dass die Ideale von $R = \mathbb{Z}^{n \times n}$ genau die Teilmengen aR sind mit $a \in \mathbb{Z}$.

Bei Ringen können wir Restklassenringe nach Idealen bilden. Der neue Punkt ist die Wohldefiniertheit der vertreterweisen Multiplikation.

Satz 3.16. *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal von R. Dann ist $R/I := \{r + I | r \in R\}$ ein Ring mit den vertreterweisen Verknüpfungen*

$$\begin{aligned} + : R/I \times R/I \to R/I &: (r + I, s + I) \mapsto (r + s) + I, \\ \cdot : R/I \times R/I \to R/I &: (r + I, s + I) \mapsto rs + I, \end{aligned}$$

und $\nu = \nu_I : R \to R/I : r \mapsto r + I$ ist ein Ringepimorphismus mit I als Kern. R/I heißt **Restklassenring** *von R nach I und ν der* **natürliche Epimorphismus**. *(Insbesondere ist jedes Ideal Kern eines Ringepimorphismus.) Ist R kommutativ, so auch R/I.*

Beweis. Da $I \leq R$ ein R-Teilmodul von R ist, ist R/I wieder ein R-Modul und wir brauchen uns nur um die Wohldefiniertheit der Multiplikation zu kümmern. Seien also $r + I = r' + I$ und $s + I = s' + I$ für gewisse $r, r', s, s' \in R$. Dann existieren $a, b \in I$ mit $r' = r + a, s' = s + b$, und wir bekommen

$$\begin{aligned} r's' - rs &= (r + a)(s + b) - rs \\ &= rs + rb + as + ab - rs \\ &= rb + as + ab \in I \end{aligned}$$

d.h. $(r + I)(s + I)$ ist wohldefiniert. Die Assoziativ- und Distributivgesetze übertragen sich von R. Dass ν ein Epimorphismus ist, ist gerade die Definition der Operationen im Restklassenring. □

Folgerung 3.17. *(Homomorphiesatz für Ringe) Seien R, S Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist $I := \mathrm{Kern}(\varphi)$ ein Ideal von R, $B := \mathrm{Bild}(\varphi)$ ein Teilring von S und*

$$\overline{\varphi} : R/I \to B, r + I \mapsto \varphi(r)$$

ein wohldefinierter Ringisomorphismus.

Ende Vorl. 10

Bemerkung 3.18. Sei M ein R-Modul. Dann ist der **Annihilator** von M

$$\mathrm{Ann}_R(M) := \{r \in R \mid rm = 0 \text{ für alle } m \in M\}$$

ein Ideal von R, der Kern des Ringhomomorphismus

$$R \to \mathrm{End}_{\mathbb{Z}}(M), r \mapsto (m \mapsto rm).$$

Weiter ist M ein $R/\mathrm{Ann}_R(M)$-Modul.

Bemerkung 3.19. Seien R und S Ringe, M ein R-Modul und N ein S-Modul. Dann ist $M \oplus N$ ein $R \times S$-Modul durch

$$(r, s) \cdot (m, n) := (rm, sn) \text{ für alle } r \in R, s \in S, m \in M, n \in N.$$

Sei umgekehrt X ein $R \times S$-Modul. Dann sind $M := (1, 0)X$ und $N := (0, 1)X$ Teilmoduln von X, so dass $X = M \oplus N$. Es ist $\mathrm{Ann}_{R\times S}(M) \supseteq \{0\} \times S$ und somit M ein $R \times S/\{0\} \times S \cong R$-Modul und ebenso $(R \times \{0\})N = \{0\}$ und N ist ein S-Modul.
Die $R \times S$-Moduln sind also genau die direkten Summen von R-Moduln und S-Moduln.

Definition 3.20. Sei R ein kommutativer Ring mit Eins. Eine R-**Algebra** A ist ein Ring mit Eins (in unserem Kontext meistens kommutativ), der gleichzeitig R-Modul ist, so dass die Multiplikation ist R-bilinear ist, d.h.

$$(ra)b = a(rb) = r(ab) \text{ für alle } r \in R, a, b \in A.$$

Ein R-Algebrenhomomorphismus ist ein Ringhomomorphismus, der gleichzeitig R-Modulhomomorphismus ist.

Übung 3.7. Sei A eine R-Algebra. Dann ist $R \to A : r \mapsto r1_A$ ein Ringhomomorphismus, sogar ein R-Algebrenhomomorphismus.

Beispiel 3.21.

1. $\mathbb{C}[x]$ ist eine $\mathbb{C}$-Algebra. Sei

   $$^- : \mathbb{C} \to \mathbb{C} : a + bi \mapsto a - bi \qquad a, b \in \mathbb{R},$$

   die **komplexe Konjugation**. Dann ist

   $$\mathbb{C}[x] \to \mathbb{C}[x] : \sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} \overline{a_k} x^k$$

   ein Ringhomomorphismus, jedoch kein $\mathbb{C}$-Algebrenhomomorphismus. (Man kann ihn jedoch als $\mathbb{R}$-Algebrenhomomorphismus auffassen.)

2. Ist A eine R-Algebra und $I \trianglelefteq A$ ein Ideal, so ist A/I eine R-Algebra und ν_I ein R-Algebrenepimorphismus.

3. Jeder Ring ist eine $\mathbb{Z}$-Algebra.

2.3 Euklidische Ringe

Definition 3.22. Sei R ein kommutativer Ring mit Eins.

1. R heißt **Integritätsbereich** oder auch **nullteilerfrei**, falls $1 \neq 0$ in R gilt und für alle $a, b \in R$, $ab = 0 \implies a = 0$ oder $b = 0$.

2. R heißt **Hauptidealbereich**, falls R ein Integritätsbereich ist und jedes Ideal von R ein Hauptideal ist.

3. R heißt **Euklidischer Bereich** oder **Euklidischer Ring**, falls eine Abbildung $\nu : R \longrightarrow \mathbb{Z}_{\geq 0}$ existiert mit folgenden Eigenschaften:

   (i) $\nu(r) = 0$ genau dann, wenn $r = 0$

   (ii) $\nu(r_1 r_2) = \nu(r_1)\nu(r_2)$

   (iii) für $a \in R$ und $b \in R \setminus \{0\}$ existiert ein $q \in R$ und ein $r \in R$, so dass $a = qb + r$ mit $\nu(r) < \nu(b)$.

Beispiel 3.23.

1. Jeder Teilring eines Körpers ist ein Integritätsbereich.

2. Offenbar ist jeder Körper sowohl ein Hauptidealbereich als auch ein EUKLIDischer Ring (mit $\nu(a) = 1$ für alle $a \in K^*$).

3. $\mathbb{Z}$ ist EUKLIDischer Bereich mit dem gewöhnlichen Absolutbetrag:

$$\nu(a) := |a| := \begin{cases} a & a \geq 0 \\ -a & a < 0. \end{cases}$$

4. Sei K ein Körper. Dann ist $K[x]$ ein EUKLIDischer Bereich mit einer multiplikativen Variante des Grades:

$$\nu(a) := \begin{cases} 0 & a = 0 \\ 2^{\mathrm{Grad}(a)} & a \neq 0. \end{cases}$$

5. $\mathbb{Z}[x] := \{p(x) \in \mathbb{Q}[x] \mid p(x) = \sum_{i=0}^{n} a_i x^i \text{ für } n \in \mathbb{N}, a_i \in \mathbb{Z}\}$ ist ein Integritätsbereich, da er ein Teilring des Körpers $\mathbb{Q}(x) = \{p(x)/q(x) \mid p(x), q(x) \in \mathbb{Q}[x], q(x) \neq 0\}$ ist. Jedoch ist $\mathbb{Z}[x]$ kein Hauptidealbereich, da z.B. $\langle 2, x\rangle$ kein Hauptideal ist.

Übung 3.8. Zeige der Ring $\mathbb{Z}[i] := \mathbb{Z}[x]/\langle x^2+1\rangle$ ist EUKLIDischer Bereich mit $\nu(a+bi) := a^2 + b^2$ für $a, b \in \mathbb{Z}$.

Satz 3.24. *Sei R ein Integritätsbereich. Dann gibt es einen Körper K, so dass $R \subseteq K$ Teilring von K ist und*

$$K = \{ab^{-1} | a \in R, b \in R \setminus \{0\}\}.$$

Dieser Körper ist bis auf Isomorphie eindeutig bestimmt und heißt **Quotientenkörper** *von R. Bezeichnung: $K = \mathrm{Quot}(R)$.*

Man beachte: In K sind alle Elemente $\neq 0$ von R zu Einheiten geworden, weshalb es Sinn macht ab^{-1}, $b^{-1}a$, oder a/b zu schreiben.

Beweis.

Existenz: Definiere $\widetilde{K} = \{(a, b) \mid a, b \in R, b \neq 0\}$ und eine Äquivalenzrelation $\approx$ auf $\widetilde{K}$: $(a, b) \approx (c, d)$ genau dann, wenn $ad = cb$. (Zur Veranschaulichung kann man die Tupel (a, b) als ungekürzte Brüche $\frac{a}{b}$ betrachten.) Die Menge der Äquivalenzklassen $\widetilde{K}/\approx =: K$ bildet einen Ring. Definiere nun $\frac{a}{b} :=\approx$ - Klasse von (a, b).
Addition und Multiplikation werden folgendermaßen definiert:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &:= \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &:= \frac{ac}{bd}, \text{ falls } b, d \neq 0. \end{aligned}$$

Zeige, dass die Addition wohldefiniert ist: Da $b, d, bd \neq 0$ sind, sind die Ausdrücke auf beiden Seiten wohldefiniert. Zum Beweis der Vertreterunabhängigkeit sei $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$. Also ist $ab' = ba'$ und $cd' = dc'$. Behauptung: Es ist $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$. Dies gilt aber genau dann, wenn $bd(a'd' + b'c') = (ad + bc)b'd'$. Nach Ausmultiplizieren erhalte: $ba'dd' + bb'c'd = ab'dd' + bb'cd'$ dies gilt, da ja nach Voraussetzung $ba' = ab'$ und $cd' = dc'$. Genauso kann man zeigen, dass die Multiplikation auf K wohldefiniert ist.
Zeige nun, dass $(K, +)$ eine abelsche Gruppe ist: Nullelement: $0 := \frac{0}{1} = \frac{0}{a}, a \neq 0$ ($\frac{0}{a} = \frac{0}{b}$ für alle $a, b \in R$ mit $a, b \neq 0$). Wegen des Assoziativgesetzes in R kann man o.B.d.A. die Nenner als gleich ansehen, also $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$. Dann ist also $\frac{b}{c} + \frac{0}{c} = \frac{b+0}{c} = \frac{b}{c}$. Die Kommutativität von K folgt aus der Kommutativtät von R. Negative: $-\frac{b}{c} := \frac{-b}{c}$.
Zeige, dass $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe bildet: $1 \neq 0$ also $K \setminus \{0\} \neq \emptyset$. Das Assoziativgesetz gilt, da $(R, \cdot)$ für Zähler und Nenner assoziativ ist, ebenso das Kommutativgesetz. Das Einselement ist $1 := \frac{1}{1} = \frac{a}{a}, a \neq 0$, das inverse Element zu $\frac{a}{b} \neq 0$ ist $\left(\frac{a}{b}\right)^{-1} := \frac{b}{a}$. Es bleibt noch zu zeigen, dass auch das Distributivgesetz gilt! (Übung)

Die Abbildung $\mu : R \longrightarrow K : r \to \frac{r}{1}$ ist ein Ringmonomorphismus, denn μ ist Ringhomomorphismus und aus $r \in \operatorname{Kern} \mu$ folgt $\frac{r}{1} = \frac{0}{1}$. Es gilt also: $r = r \cdot 1 = 0 \cdot 1 = 0$. Also identifiziere $r \in R$ mit $\frac{r}{1} \in K$. Beachte: Für $r \in R$ und $0 \neq s \in R$ gilt:

$$\frac{r}{s} = \frac{r}{1} \cdot \left(\frac{s}{1}\right)^{-1} = r \cdot s^{-1}$$

mit dieser Identifikation.

Eindeutigkeit: Sei K' ein weiterer Körper mit $R \subseteq K'$. Dann ist die Abbildung $\varepsilon : K \longrightarrow K' : \frac{a}{b} \mapsto a \cdot b^{-1}$ ein wohldefinierter Homomorphismus: Sei dazu $\frac{a}{b} = \frac{a'}{b'}$. Dann gilt: $ab' = ba'$ in R, also $ab^{-1} = a'b'^{-1}$ in K'. Aus der Homomorphie von ε folgt sofort: ε ist Monomorphismus, also $K \cong \operatorname{Bild} \varepsilon$. □

An dieser Stelle ist auf ein Problem hinzuweisen: Wir haben zwar eine Beschreibung der Elemente des Quotientenkörpers, mit der man Gleichheit testen kann. Man hat aber zunächst und im allgemeinen keine Normalform für die Elemente, die natürlich viel effektiver wäre.

Beispiel 3.25.

1. $\operatorname{Quot}(\mathbb{Z}) = \mathbb{Q}$. Hier lernt man eine Normalform in der Schule kennen.

2. Sei K ein Körper. Dann heißt $K(x) := \operatorname{Quot}(K[x])$ der Körper der **rationalen Funktionen** in einer Variablen.

3. Sei K ein Körper. Dann heißt $K(x_1, \ldots, x_n) := \operatorname{Quot}(K[x_1, \ldots, x_n])$ der Körper der **rationalen Funktionen** in n Variablen. Zum Beispiel ist

$$\frac{x_1^3 - x_2^3}{x_1^2 - x_2^2} = \frac{x_1^2 + x_1 x_2 + x_2^2}{x_1 + x_2}.$$

Wir haben also Integritätsbereiche als die Teilringe von Körpern charakterisiert. Wir werden gleich sehen, dass in Hauptidealbereiche als die Integritätsbereiche größte gemeinsame Teiler stets existiert.

Definition 3.26. Sei R ein Integritätsbereich, $a, b \in R$.

1. $d \in R$ teilt a genau dann, wenn ein $r \in R$ existiert, mit $a = dr$, also genau dann wenn $a \in \langle d \rangle$. Bezeichnung: $d|a$.

2. $a \in R \setminus (R^* \cup \{0\})$ heißt **prim**, falls

$$a|(b_1 b_2) \text{ impliziert } a|b_1 \text{ oder } a|b_2 \text{ für alle } b_1, b_2 \in R.$$

3. Eine Zahl $d \in R$ heißt **größter gemeinsamer Teiler** $\operatorname{ggT}(a, b)$ von a und b genau dann, wenn d ein Teiler von a und ein Teiler von b ist und für jedes $c \in R$, welches a und b teilt, auch gilt, dass c ein Teiler von d ist.

4. Eine Zahl $v \in R$ heißt **kleinstes gemeinsames Vielfaches** $\operatorname{kgV}(a, b)$ von a und b genau dann, wenn sie sowohl durch a als auch durch b teilbar ist und jedes $w \in R$, welches durch a und b teilbar ist, auch durch v teilbar ist.

Satz 3.27. *Sei R ein Hauptidealbereich, $a, b \in R$. Dann existieren $\operatorname{ggT}(a, b) \in R$ und $\operatorname{kgV}(a, b) \in R$ und sind eindeutig bis auf Multiplikation mit Einheiten.*

Beweis. Wir betrachten das Erzeugnis $\langle a\rangle + \langle b\rangle = \langle a, b\rangle \trianglelefteq R$. Da R ein Hauptidealbereich ist, ist dieses Ideal ein Hauptideal, also gibt es ein $d \in R$ mit $\langle a\rangle + \langle b\rangle = \langle d\rangle$. Dann gilt $a \in \langle d\rangle$, also d teilt a und ebenso d teilt b. Ist umgekehrt $c \in R$ ein Teiler von a und von b, so heißt dies, dass $a \in \langle c\rangle$ und $b \in \langle c\rangle$, also

$$\langle d\rangle = \langle a\rangle + \langle b\rangle \subseteq \langle c\rangle$$

und somit gibt es ein $r \in R$ mit $d = cr$.
Für das kleinste gemeinsame Vielfache gilt $\langle \mathrm{kgV}(a, b)\rangle = \langle a\rangle \cap \langle b\rangle$. Der Beweis hierfür und für die Eindeutigkeit bis auf Einheiten ist eine Übungsaufgabe. □

Bemerkung 3.28. Sei R ein EUKLIDischer Bereich. Dann ist R ein Hauptidealbereich.

Ende Vorl. 11

Beweis. Wir zeigen zunächst, dass R nullteilerfrei ist. Seien $a, b \in R$ mit $ab = 0$. Dann ist $0 = \nu(ab) = \nu(a)\nu(b)$ also $\nu(a) = 0$ oder $\nu(b) = 0$, da $\mathbb{Z}$ als Teilring des Körpers $\mathbb{Q}$ nullteilerfrei ist. Somit folgt $a = 0$ oder $b = 0$.
Nun zeigen wir, dass jedes Ideal von R ein Hauptideal ist. Sei $\langle 0\rangle \neq I \trianglelefteq R$. Wähle ein $a \in I \setminus \{0\}$ mit $\nu(a)$ minimal. (Dies ist möglich, da $\mathbb{Z}_{\geq 0}$ wohlgeortnet ist.)
Behauptung: $I = \langle a\rangle$. Ist nämlich $b \in I$, dann folgt: $b = aq + r$ mit $\nu(r) < \nu(a)$ für $q, r \in R$ und $r \in I$. Daraus folgt aber $r = 0$, d.h. $b = aq \in \langle a\rangle$. □

Man kann sagen, dass die EUKLIDischen Ringe besonders konstruktive Versionen der Hauptidealbereiche sind. Man hat nämlich den EUKLIDischen Algorithmus, um den ggT und damit auch Erzeuger von endlich erzeugten Idealen konstruktiv auszurechnen.

Übung 3.9. Man formuliere den EUKLIDischen Algorithmus (inklusive der Darstellung des größten gemeinsamen Teilers) für EUKLIDische Bereiche und zeige, wie man ihn zur Beschreibung von endlich erzeugten Idealen als Hauptideale benutzen kann.

2.4 Der chinesische Restsatz

Wenn nicht anders angekündigt, bedeutet Ring ein kommutativer Ring mit Eins.

Satz 3.29. *(**Chinesischer Restsatz**) Sei R ein Ring und $I_1, \ldots, I_n$ paarweise* **teilerfremde** *Ideale von R, d.h. $I_i \trianglelefteq R$ und $I_i + I_j = R$ für $i, j = 1, \ldots, n$ mit $i \neq j$. Dann gilt:*

$$\begin{aligned} R/\bigcap_{i=1}^{n} I_i &\xrightarrow{\sim} R/I_1 \times R/I_2 \times \ldots \times R/I_n \\ r + \bigcap_{i=1}^{n} I_i &\mapsto (r + I_1, r + I_2, \ldots, r + I_n) \end{aligned}$$

ist ein Isomorphismus.

Bei Anwendungen will man häufig den zu dem obigen Isomorphismus inversen Isomorphismus ausrechnen. Man nennt den Satz auch den **Hauptsatz über das Lösen von simultanen Kongruenzen**. Dies ist wie folgt zu verstehen: Für $I \trianglelefteq R$ schreibt man für Elemente $r, s \in R$ statt $r + I = s + I$ auch schon mal $r \equiv s \pmod{I}$. Der obige Satz sagt also: Für beliebige $r_1, \ldots, r_n \in R$ gibt es ein $x \in R$ mit

$$x \equiv r_i \pmod{I_i} \qquad \text{für alle } i = 1, \ldots n$$

und die Lösungen sind eindeutig $\pmod{\bigcap_{i=1}^{n} I_i}$.

Beweis. Der Fall $n = 2$ ist klar: Der offensichtliche Homomorphismus

$$R \to R/I_1 \times R/I_2 : r \mapsto (r + I_1, r + I_2)$$

hat Kern $I_1 \cap I_2$ und ist wegen $I_1 + I_2 = R$ surjektiv (leichte Übung: Zeige, dass insbesondere $(1, 0)$ und $(0, 1)$ im Bild sind). Die Behauptung folgt aus dem Homomorphiesatz.
Der allgemeine Beweis erfolgt nun durch Induktion, die wir als Übung lassen. Der wesentliche Schritt steckt schon im Fall $n = 3$:
Behauptung: $I_1 + (I_2 \cap I_3) = R$. Zum Beweis beachte: Es existieren $e_1, e_1' \in I_1, e_2 \in I_2, e_3 \in I_3$ mit

$$1 = e_1 + e_2 = e_1' + e_3, \text{ also } 1 = 1 \cdot 1 = \underbrace{e_1 e_1' + e_1 e_3 + e_2 e_1'}_{=:e_{11} \in I_1} + \underbrace{e_2 e_3}_{=:e_{12} \in I_2 \cap I_3}.$$

Damit ist klar: $R = Re_{11}R + Re_{12}R \subseteq I_1 + (I_2 \cap I_3)$. Wir wenden den Fall $n = 2$ nun zweimal an:

$$R/(I_1 \cap I_2 \cap I_3) \cong R/I_1 \times R/(I_2 \cap I_3) \cong R/I_1 \times R/I_2 \times R/I_3$$

mit den entsprechenden Isomorphismen. □

Beispiel 3.30. Durch Kombination der Neunerprobe mittels Quersumme $\pmod 9$, der Zehnerprobe mittels letzter Stelle $\pmod{10}$ und der Elferprobe vermöge der alternierenden Quersumme $\pmod{11}$ kann man Rechnungen mit ganzen Zahlen, die nur Multiplikationen und Additionen involvieren $\pmod{990}$ überprüfen.
Sei $s := 124$, $t := 351$. Wir wollen $(s + t)t = 166275$ verifizieren. Mod 10 ist diese Rechnung richtig (letzte Ziffer stimmt).
Sei q die Quersumme und a die alternierende Quersumme.
Dann gilt für jedes $n \in \mathbb{N}$: $n \equiv q(n) \pmod 9$ und $n \equiv a(n) \pmod{11}$ (Übung für alle Lehramtsstudierenden !!)
Modulo 9: $q(s) = 7$, $q(t) = 0$ also auch $q((s + t)t) = 0$ auch das stimmt.
Mod 11: $a(s) = 3$, $a(t) = -1$, also $a((s+t)t) = -2$. Es ist aber $a(166275) = 5-7+2-6+6-1 = -1$ also ist an der Rechnung etwas falsch. Die richtige Antwort ist $(s + t)t = 166725$ mit $a(166725) = 5 - 2 + 7 - 6 + 6 - 1 = 9 \equiv -2 \pmod{11}$.

Der Chinesische Restsatz 3.29 kann für Euklidische Ringe wie folgt formuliert und auch bewiesen werden:

Satz 3.31. *(***Chinesischer Restsatz für Euklidische Ringe***) Sei R ein Euklidischer Ring und $a_1, \ldots, a_n$ paarweise* **teilerfremde** *Elemente von R, d.h. $\mathrm{ggT}(a_i, a_j) = 1$ für $i, j = 1, \ldots, n$ mit $i \neq j$. Dann gilt:*

$$\begin{aligned} \bigcap_{i=1}^{n} \langle a_i \rangle &= \left\langle \prod_{i=1}^{n} a_i \right\rangle \\ \varphi : R/\left\langle \prod_{i=1}^{n} a_i \right\rangle &\xrightarrow{\sim} R/\langle a_1 \rangle \times R/\langle a_2 \rangle \times \ldots \times R/\langle a_n \rangle \\ r + \left\langle \prod_{i=1}^{n} a_i \right\rangle &\mapsto (r + \langle a_1 \rangle, r + \langle a_2 \rangle, \ldots, r + \langle a_n \rangle) \end{aligned}$$

ist ein Isomorphismus dessen Umkehrabbildung mit dem Euklidischen Algorithmus berechnet werden kann.

Beweis. Da $\langle a_i \rangle + \langle a_j \rangle = \langle 1 \rangle = R$ für alle $i \neq j$ gilt, ist $\mathrm{kgV}(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_i$ und somit $\cap_{i=1}^{n} \langle a_i \rangle = \langle \prod_{i=1}^{n} a_i \rangle$. Es genügt also den Algorithmus anzugeben. Ein allgemeines Element von $R/\langle a_1 \rangle \times R/\langle a_2 \rangle \times \ldots \times R/\langle a_n \rangle$ ist von der Form $X := (r_1 + \langle a_1 \rangle, \ldots, r_n + \langle a_n \rangle)$. Setze

$A := \langle \prod_{i=1}^n a_i \rangle$. Gesucht ist ein $r \in R$ mit $r + \langle a_i \rangle = r_i + \langle a_i \rangle$ für alle $i = 1, \ldots, n$, also $\varphi(r + A) = X$.
Dazu setze $B_i := \prod_{j \neq i} a_j$. Da $\mathrm{ggT}(a_i, a_j) = 1$ für alle $i \neq j$ gilt, folgt auch $\mathrm{ggT}(a_i, B_i) = 1$, es gibt also $x_i, y_i \in R$ mit

$$1 = x_i a_i + y_i B_i.$$

Setze $e_i := y_i B_i$. Dann ist

$$e_i + \langle a_j \rangle = 0 \text{ für alle } i \neq j \text{ und } e_i + \langle a_i \rangle = 1$$

also $\varphi(e_i + A) = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit 1 an der i-ten Stelle. Da φ ein R-Ringhomomorphismus ist, ergibt sich

$$\varphi^{-1}(X) = \sum_{i=1}^n r_i e_i + A. \qquad \square$$

Beispiel 3.32. Wir wollen das simultane Kongruenzensystem

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

lösen. Wir haben den Isomorphismus

$$\varphi : \mathbb{Z}/\langle 60 \rangle \xrightarrow{\sim} \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 4 \rangle \times \mathbb{Z}/\langle 5 \rangle$$

und haben das Problem gelöst, wenn wir

$$\begin{aligned} e_1 + \langle 60 \rangle &:= \varphi^{-1}((\overline{1}, \overline{0}, \overline{0})), \\ e_2 + \langle 60 \rangle &:= \varphi^{-1}((\overline{0}, \overline{1}, \overline{0})), \\ e_3 + \langle 60 \rangle &:= \varphi^{-1}((\overline{0}, \overline{0}, \overline{1})) \end{aligned}$$

kennen, denn die Lösungsmenge ist dann $e_1 + 2e_2 + 3e_3 + \langle 60 \rangle$. Mit Hilfe des EUKLIDischen Algorithmus für 3 und $4 \cdot 5$ etc. bekommen wir dann e_1 etc. :

$$\begin{aligned} 1 &= 7 \cdot 3 + (-1) \cdot 20, \quad \text{also} \quad e_1 = -20, \\ 1 &= 4 \cdot 4 + (-1) \cdot 15, \quad \text{also} \quad e_2 = -15, \\ 1 &= 5 \cdot 5 + (-2) \cdot 12, \quad \text{also} \quad e_3 = -24. \end{aligned}$$

Also $x \in -122 + \langle 60 \rangle = -2 + \langle 60 \rangle$.

Beispiel 3.33 (Lagrangeinterpolation). Sei K ein Körper und $p(x) \in K[x]$. Wie wir schon wissen gilt für $a \in K$

$$p(a) = 0 \text{ genau dann, wenn } p(x) \in \langle x - a \rangle \trianglelefteq K[x],$$

(was man auch durch Entwickeln nach Potenzen von $x - a$ sehen kann). Dies liefert auch

$$p(x) \equiv p(a) \pmod{\langle x - a \rangle}.$$

Sind nun $a_1, \ldots, a_n \in K$ paarweise verschiedene Elemente, so sind die Ideale $\langle x - a_i \rangle$ paarweise teilerfremd und der Chinesische Restsatz liefert

$$K[x] / \left\langle \prod_{i=1}^n (x - a_i) \right\rangle \cong \bigtimes_{i=1}^n \underbrace{K[x]/\langle x - a_i \rangle}_{\cong K}.$$

Die Restklassen der Elemente $\tilde{e}_i(x) := \prod_{j\neq i}(x-a_j) \in K[x]$ liefern auf der rechten Seite Tupel, deren Komponenten alle Null sind, außer der i-ten, welche gleich $\tilde{e}_i(a_i) = \prod_{j\neq i}(a_i - a_j)$ ist. Hieraus ergibt sich sofort die LAGRANGEsche Interpolationsformel: Eine Abbildung $f : K \to K$ wird interpoliert an den Stützstellen a_i durch das Polynom (vom Grad $< n$):

$$\sum_{i=1}^{n} f(a_i)\frac{\tilde{e}_i(x)}{\tilde{e}_i(a_i)}.$$

Wenn man im Falle $K = \mathbb{R}$ auch noch Ableitungen an den Stellen a_i vorgeben will, muss man mit $\langle (x-a_i)^k\rangle \trianglelefteq K[x]$ arbeiten statt mit $\langle x-a_i\rangle$ und kommt zur **Hermiteinterpolation**.

Die ringdirekten Summen enthalten etwas suspekte Elemente, die sich aber oben schon als sehr nützlich erwiesen haben.

Definition 3.34. Sei R ein Ring (kmE) und $a \in R$ mit $a \neq 0$. Man nennt a einen **Nullteiler**, wenn ein $b \in R$ existiert mit $b \neq 0$ und $ab = 0$. Weiter heißt a **nilpotent**, falls ein $n \in \mathbb{N}$ existiert mit $a^n = 0$.

Klar, nilpotente Elemente sind Nullteiler, aber oben haben wir schon Nullteiler gesehen, die nicht nilpotent sind.

Beispiel 3.35.

1. Seien $n, k \in \mathbb{Z}$ beide größer als 1. Dann ist $n + \langle n^k\rangle \in \mathbb{Z}/\langle n^k\rangle$ nilpotent.
2. (Wurzel ziehen). Aus dem Chinesischen Restsatz bekommen wir

$$\begin{aligned} \pi_1 \times \pi_2 : \mathbb{R}[x]/\langle x^2-2\rangle &\xrightarrow{\sim} \underbrace{\mathbb{R}}_{\cong \mathbb{R}[x]/\langle x-\sqrt{2}\rangle} \times \underbrace{\mathbb{R}}_{\cong \mathbb{R}[x]/\langle x+\sqrt{2}\rangle} : \\ \overline{x} := x + \langle x^2-2\rangle &\mapsto (\sqrt{2}, -\sqrt{2}) = (\pi_1(\overline{x}), \pi_2(\overline{x})). \end{aligned}$$

   Wir wollen auf der rechten Seite rechnen, können aber nur auf der linken Seite Nullteiler erkennen. Unser Ziel ist eine numerische Approximation von $\sqrt{2}$ zu bestimmen. Klar: Die einzigen Nullteiler der Form $a + \overline{x}$ mit $a \in \mathbb{R}$ sind $\sqrt{2} + \overline{x}$ und $-\sqrt{2} + \overline{x}$. Die Idee ist nun so: Sei $b \in \mathbb{Q}$ so gewählt, dass $a := \overline{x} - b$ auf der rechten Seite einem (a_1, a_2) entspricht mit $|a_1| < 1$ und $|a_2| > 1$. (Betragstriche markieren Absolutbeträge.) Es ist $a^2 = 2 - 2b\overline{x} + b^2$. Dann ist $|a_1^2| < |a_1| < 1$, und $\pi_1(a^2/(-2b))$ hat einen noch kleineren Absolutbetrag, so dass $(b^2+2)/(2b)$ eine noch bessere Näherung an $\sqrt{2}$ ist als b. Durch fortgesetztes Quadrieren verdoppelt sich immer die Anzahl der signifikanten Dezimalstellen, wir haben quadratische Konvergenz. Fängt man also mit $b = 1$ an, so erhält man die folgende Folge die gegen $\sqrt{2}$ konvergiert:

$$1, \frac{3}{2}, \frac{17}{12} = 1.416666667, \frac{577}{408} = 1.414215686, \frac{665857}{470832} = 1.414213562, ...$$

Übung 3.10. Vergleiche obige Methode des Wurzelziehens mit dem NEWTONverfahren aus der Numerik.

2.5 Der chinesische Restsatz und die Hauptraumzerlegung.

Die Hauptraumzerlegung aus Bemerkung 2.34 erinnert stark an den chinesischen Restsatz. Sei dazu K ein Körper, $\mathcal{V}$ ein e.e. K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$ mit Minimalpolynom

$$\mu_\alpha = p_1^{n_1} \cdots p_k^{n_k}$$

wobei die p_i paarweise verschiedene irreduzible Polynome in $K[x]$ sind und $n_i \in \mathbb{N}$. Unter den obigen Voraussetzungen läßt sich $\mathcal{V}$ eindeutig schreiben als direkte Summe α-invarianter Teilräume $\mathcal{U}_i$:

$$\mathcal{V} = \bigoplus_{i=1}^{k} \mathcal{U}_i,$$

so dass das Minimalpolynom der Einschränkung von α auf $\mathcal{U}_i$ genau $p_i^{n_i}$ ist. Setzt man $q_i := \prod_{j \neq i} p_j^{n_j}$ so ist $\mathcal{U}_i = \mathrm{Bild}(q_i(\alpha))$.

Ende Vorl. 12

Bemerkung 3.36.

1. Das Minimalpolynom von α war definiert als normierter Erzeuger des Kerns des Einsetzungshomomorphismus

   $$\varepsilon_\alpha : K[x] \to \mathrm{End}(\mathcal{V}), p \mapsto p(\alpha)$$

   $\mathrm{Kern}(\varepsilon_\alpha) = \langle \mu_\alpha \rangle$, $\mathrm{Bild}(\varepsilon_\alpha) = K[\alpha]$. Also ist nach dem Homomorphiesatz für Ringe $K[x]/\langle \mu_\alpha \rangle \cong K[\alpha]$.

2. Setzt man $R := K[x]/\langle \mu_\alpha \rangle$, so wird $\mathcal{V}$ ein R-Modul durch

   $$(p + \langle \mu_\alpha \rangle)V := \varepsilon_\alpha(p)(V) = p(\alpha)(V).$$

3. Die Struktur von R bekommen wir aus dem Chinesischen Restsatz:

   $$R \cong K[x]/\langle p_1^{n_1} \cdots p_k^{n_k} \rangle \cong K[x]/\langle p_1^{n_1} \rangle \times K[x]/\langle p_2^{n_2} \rangle \times \ldots \times K[x]/\langle p_k^{n_k} \rangle$$

   und Urbilder e_i der **Idempotente** $\pi_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (mit 1 an der i-ten Stelle) können mit dem Algorithmus in 3.31 ermittelt werden, indem wir für alle i mit dem Euklidischen Algorithmus $1 = x_i p_i^{n_i} + y_i q_i$ schreiben, und $e_i = \varepsilon_\alpha(y_i q_i) \in K[\alpha]$ setzen. Aus einer Übung wissen wir, dass das Bild von e_i gleich dem von $q_i(\alpha)$ ist.

4. Also ist $\mathcal{V}$ ein Modul für dem Produktring $K[x]/\langle p_1^{n_1} \rangle \times K[x]/\langle p_2^{n_2} \rangle \times \ldots \times K[x]/\langle p_k^{n_k} \rangle$.

3 Elementare Teilbarkeitstheorie für Ringe

Definition 3.37. Sei R Ring (kmE) und $a, b \in R$.

1. a **teilt** b (in R) oder b ist ein **Vielfaches** von a, in Zeichen $a \mid b$, falls ein $r \in R$ existiert mit $ar = b$.

2. a ist **assoziiert** zu b (in R), in Zeichen $a \sim b$, falls $a \mid b$ und $b \mid a$.

Klar: Die Vielfachen von a bilden gerade das Hauptideal $\langle a \rangle$. Teilen ist eine transitive Relation auf R und $\sim$ ist eine Äquivalenzrelation auf R. Auch klar: Seien $a, b \in R$. Falls ein $e \in R^*$ existiert mit $a = eb$, dann gilt $a \sim b$. Wenn wir versuchen die Umkehrung zu beweisen, stoßen wir auf eine kleine Schwierigkeit. Diese verschwindet, wenn wir verlangen, dass R ein Integritätsbereich ist.

Bemerkung 3.38. In einem Integritätsbereich sind die Assoziertenklassen der Elemente gegeben durch R^*a mit $a \in R$.

Beweis. Es ist klar, dass jedes Element der Form ua mit $u \in R^*$ zu $a = u^{-1}ua$ assoziiert ist. Sei nun $b \in R$ mit $b \mid a$ und $a \mid b$. Dann gibt es $r, s \in R$ mit $a = br$ und $b = as$.
Ist $a = 0$, so ist $b = as = 0 \in R^*a = \{0\}$.
Sei also $a \neq 0$. Wir wollen zeigen, dass r und s Einheiten sind, sogar $r = s^{-1}$ also $rs = 1$: Denn es ist $a = br = asr$ also $a(1-sr) = 0$. Da $a \neq 0$ und R nullteilerfrei, folgt jetzt $1-sr = 0$ also $sr = 1$. □

Bemerkung 3.39. Ist R ein Integritätsbereich, so ist der Polynomring $R[x_1, \ldots, x_n]$ auch ein Integritätsbereich. Zum Beweis definieren wir den **Grad** eines Polynoms

$$p = p(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \in R[x_1, \ldots, x_n], p \neq 0$$

als

$$\operatorname{Grad} p := \max\{i_1 + \cdots + i_n | a_{i_1 \ldots i_n} \neq 0\}.$$

Für $p, q \in R[x_1, \ldots, x_n]$ mit $p \neq 0 \neq q$ gilt offenbar

$$\operatorname{Grad} pq = \operatorname{Grad}(p) + \operatorname{Grad}(q),$$

woraus man leicht sieht, dass man keine Nullteiler hat.

Unsere nächste Frage lautet: Welche Restklassenringe sind Integritätsbereiche?

Definition 3.40. Sei R ein Ring (kmE).

1. Ein Ideal $I \trianglelefteq R$ mit $I \neq R$ heißt **Primideal**, falls für alle $r, s \in R$ gilt:

$$r, s \notin I \text{ impliziert } rs \notin I.$$

2. Ein Ideal I heißt **maximales Ideal**, falls $I \neq R$ und für jedes Ideal J von R, welches I enthält gilt $J = I$ oder $J = R$.

Bemerkung 3.41. Sei R Ring (kmE) und $I \trianglelefteq R$.

1. R/I ist genau dann Integritätsbereich, wenn I Primideal ist.
2. R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.

Beweis.

1. R/I ist Integritätsbereich, genau dann wenn für alle $r, s \in R$ mit $(r + I)(s + I) = 0$ gilt, dass entweder $r + I = 0$ ist oder $s + I = 0$, also entweder $r \in I$ oder $s \in I$. Da $(r + I)(s + I) = rs + I$ ist dies gleichbedeutend mit ($rs \in I \iff r \in I$ oder $s \in I$), also damit, dass I ein Primideal ist.
2. R/I ist ein Körper, genau dann wenn jedes $r + I \in R/I \setminus \{0 + I\}$ ein multiplikatives Inverses hat. Sei also $r \in R \setminus I$. Dann ist $\langle r, I\rangle = \langle r\rangle + I$ ein Ideal von R, welches I echt enthält. Ist I ein maximales Ideal, so ist $\langle r\rangle + I = R$ und es gibt $a \in R$, $i \in I$ mit $ar + i = 1$. Dann ist $(a + I)(r + I) = 1 + I$ und $(a + I)$ ein multiplikatives Inverses von $r + I$. Die Umkehrung geht genauso. □

Beispiel 3.42.

1. Sei R Integritätsbereich. $\langle y\rangle \trianglelefteq R[x, y]$ ist Primideal, da $R[x, y]/\langle y\rangle \cong R[x]$ Integritätsbereich.
2. R ein Ring (kmE), $I \trianglelefteq R$ maximal, dann ist I prim.

3. Sei ein R Ring (kmE). Genau dann ist $\{0\}$ Primideal, wenn R Integritätsbereich ist.

Nun kommen wir zur Teilbarkeitstheorie in Integritätsbereichen. Es wird ganz elementar in dem Sinne, dass wir wieder mehr von Elementen als von Idealen sprechen. Zuerst eine Ernüchterung: Die Begriffe "prim" und "irreduzibel" für Elemente in einem Integritätsbereich fallen im allgemeinen auseinander:

Definition 3.43. Sei R ein Integritätsbereich.

1. Ein Element $a \in R \setminus (R^* \cup \{0\})$ heißt **irreduzibel** oder **unzerlegbar**, falls jede Faktorisierung von a in R trivial ist, das heißt, falls gilt:
$$a = a_1 a_2 \text{ für } a_i \in R \text{ impliziert } a_1 \in R^* \text{ oder } a_2 \in R^*.$$
2. Ein Element $a \in R \setminus (R^* \cup \{0\})$ heißt **prim**, falls
$$a|(b_1 b_2) \text{ impliziert } a|b_1 \text{ oder } a|b_2 \text{ für alle } b_i \in R.$$

Beispiel 3.44.

1. In $R = \mathbb{Z}$ ist 2 prim und irreduzibel.
2. Sei K ein Integritätsbereich und $R = K[x]$. Dann ist x prim (vom Grad 1) und unzerlegbar. (Falls $x|(a(x)b(x))$ und $x \nmid a(x)$, so folgt: $a(0) \neq 0$, also $b(0) = 0$ und $x|b(x)$.)

Bemerkung 3.45.

1. Ist a prim, so ist a auch unzerlegbar.
2. a ist prim genau dann, wenn $\langle a \rangle \trianglelefteq R$ ein Primideal $\neq 0$ ist.

Beweis.

1. Sei a prim und $a = a_1 a_2$ mit $a_i \in R \setminus R^*$. Dann gilt: $a|a_1 a_2$ und $a \nmid a_1$ (sonst wäre $a_2 \in R^*$) und $a \nmid a_2$ (sonst wäre $a_1 \in R^*$). Dies ist aber ein Widerspruch zu der Voraussetzung : a prim.
2. Sei $a \in R$ prim. Dann ist $\langle a \rangle \neq 0$. Weiter gilt für $r, s \in R$:
$$rs \in \langle a \rangle \Leftrightarrow a \mid rs \Leftrightarrow a \mid r \text{ oder } a \mid s \Leftrightarrow r \in \langle a \rangle \text{ oder } s \in \langle a \rangle.$$
Die Umkehrung folgt ebenso. □

Übung 3.11. Es gibt unzerlegbare Elemente, die nicht prim sind:
Sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Es gilt: $3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Zeige: Die Elemente $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ sind allesamt in R unzerlegbar, aber nicht prim.
Hinweis: Betrachte die multiplikative Norm $\nu(a + b\sqrt{-5}) := a^2 + 5b^2$.

An dieser Stelle sei angemerkt, dass DEDEKIND, der sicher als einer der Urväter der modernen Algebra einzuschätzen ist, wegen der schlechten Eigenschaften des Teilbarkeitsbegriffes für Elemente, den Idealbegriff erfunden hat, um in bestimmten Situationen der Zahlentheorie doch noch zu einer befriedigenden Teilbarkeitstheorie, diesmal aber für Ideale (sprich ideale Zahlen) zu kommen. Im obigen Beispiel kann man nämlich alle vier Zahlen als Ideale noch weiter zerlegen:

$$\begin{aligned}
\langle 3 \rangle &= \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle \\
\langle 2 \rangle &= \langle 2, 1 + \sqrt{-5} \rangle \langle 2, 1 - \sqrt{-5} \rangle \\
\langle 1 + \sqrt{-5} \rangle &= \langle 3, 1 + \sqrt{-5} \rangle \langle 2, 1 + \sqrt{-5} \rangle \\
\langle 1 - \sqrt{-5} \rangle &= \langle 3, 1 - \sqrt{-5} \rangle \langle 2, 1 - \sqrt{-5} \rangle
\end{aligned}$$

Satz 3.46. *Ist R Hauptidealbereich, so ist jedes unzerlegbare Element prim.*

Beweis. Sei $a \in R \setminus (R^* \cup \{0\})$ unzerlegbar. Wir wissen, dass a genau dann prim ist, wenn $\langle a \rangle$ ein Primideal ist. Wir können sogar zeigen, dass $\langle a \rangle$ ein maximales Ideal ist, denn sei $\langle a \rangle \subseteq I \trianglelefteq R \neq I$. Da R Hauptidealbereich ist, folgt $I = \langle d \rangle$ für ein $d \in R \setminus (R^* \cup \{0\})$. Somit $a \in \langle d \rangle$, also $a = dd'$ für ein $d' \in R$. Das bedeutet $d' \in R^*$, denn a ist unzerlegbar und $d \notin R^*$. Da $a \sim d$ ist, haben wir $I = \langle a \rangle$. □

Übung 3.12. Sei R Hauptidealbereich und $a, b \in R \setminus \{0\}$. Zeige $\langle a \rangle + \langle b \rangle = \langle a, b \rangle = (\mathrm{ggT}(a, b))$ und $\langle a \rangle \cap \langle b \rangle = \langle \mathrm{kgV}(a, b) \rangle$ und schließlich $\langle a \rangle \langle b \rangle = \langle ab \rangle$.

Folgerung 3.47. *Ist R ein Hauptidealbereich, so ist jedes Primideal, das ungleich dem 0-Ideal ist, ein maximales Ideal.*

Satz 3.48. *Sei R ein Hauptidealbereich, $a \in R \setminus \{0\}$ keine Einheit. Dann gibt es im wesentlichen eindeutige Primelemente $a_1, \ldots, a_n \in R$ mit $a = a_1 \cdots a_n$. Die Eindeutigkeit bedeutet: Falls $a = a_1 \cdots a_n = b_1 \cdots b_m$ mit $a_i, b_j \in R$ unzerlegbar, so folgt $n = m$ und nach Umnumerierung $a_i \sim b_i$ für $i = 1, \ldots, n$.*

Beweis. Wir können zunächst genauso vorgehen wie für $R = \mathbb{Z}$: Ist a unzerlegbar, so ist a schon prim und wir sind fertig. Ist a nicht irreduzibel, so können wir $a = bc$ schreiben mit $b, c \in R \setminus R^*$ und dann mit b und c weitermachen. Wieso hört dieser Prozess auf? Falls nicht, so konstruiert man eine Folge von echten Teilern $\ldots b_{i+1} \mid b_i \mid \ldots \mid b_1 = b \mid a$, so dass

$$\langle a \rangle \subsetneq \langle b_1 \rangle \subsetneq \langle b_2 \rangle \ldots$$

Sei $I := \bigcup_{i \in \mathbb{N}} \langle b_i \rangle$. Da die Ideale $\langle b_i \rangle$ eine Kette bilden, ist I ein Ideal von R. Nun ist R ein Hauptidealbereich also gibt es ein $d \in R$ mit $I = \langle d \rangle$. Da $d \in I = \bigcup_{i \in \mathbb{N}} \langle b_i \rangle$ existiert also ein $i \in \mathbb{N}$ mit $d \in \langle b_i \rangle$. Aber dann ist $\langle b_j \rangle = \langle b_i \rangle = I$ für alle $j \geq i$ ein Widerspruch dazu, dass b_{i+1} ein echter Teiler von b_i ist.
Die Eindeutigkeit zeigt man genauso wie für $\mathbb{Z}$: Sei $a = a_1 \cdots a_n = b_1 \cdots b_m$ mit $a_i, b_j \in R$ unzerlegbar. Dann ist a_1 prim, $a_1 \mid a = b_1 \cdots b_m$, also gibt es ein i mit $a_1 \mid b_i$. Da b_i irreduzibel ist, gilt also $a_1 \sim b_i$, usw. mit Induktion über die Anzahl m von Faktoren. □

Beispiel 3.49.

1. $\mathbb{Z}[x]$ ist kein Hauptidealbereich, denn das Primideal $\langle x \rangle$ ist kein maximales Ideal.
2. $K[x, y]$ (K sei ein Körper) ist ebenfalls kein Hauptidealbereich.

Ende Vorl. 13

3. $\mathbb{Z}$ ist ein Hauptidealbereich. Die Primzahlen sind bis auf Multiplikation mit Einheiten $\{\pm 1\}$ die unzerlegbaren Elemente von $\mathbb{Z}$. Die $\mathbb{F}_p := \mathbb{Z}/\langle p \rangle$ für Primzahlen p sind die einzigen Restklassenkörper von $\mathbb{Z}$.
4. Für jeden Körper K ist $K[x]$ ein Hauptidealbereich. Die irreduziblen Polynome in $K[x]$ sind gleich den Primelementen in $K[x]$ und den unzerlegbaren Elementen in $K[x]$. Die Restklassenkörper von $K[x]$ sind alle von der Form $K[x]/\langle p(x) \rangle$, wo $p(x) \in K[x]$ irreduzibel ist.

4 Moduln über Hauptidealbereichen.

4.1 Der Struktursatz

Endlich erzeugte Moduln über Hauptidealbereichen haben eine sehr schöne Struktur. Um algorithmisch einen solchen Modul auf Normalform zu bringen benötigt man lediglich die algorithmische Berechenbarkeit der Bézout Identität. Die „algorithmisch zugänglichen“ HIB sind also die Euklidischen Ringe.

Definition 3.50. Sei R ein Integritätsbereich und M ein R-Modul. Ein $m \in M$ heißt **Torsionselement**, falls das **Annullatorideal**[1]

$$\mathrm{Ann}_R(m) := \{r \in R \mid rm = 0\}$$

von $\langle 0\rangle$ verschieden ist. Der **Torsionsteilmodul**, also der Teilmodul aller Torsionselemente von M, wird mit $T(M)$ bezeichnet. M heißt **torsionsfrei**, falls $T(M) = \{0\}$ und ein **Torsionsmodul**, falls $T(M) = M$.

Man konkretisiert sich die Begriffe mit Hilfe der folgenden Beispiele, wobei man $R = \mathbb{Z}$ und $R = K[x]$ betrachte.

Beispiel 3.51. Sei R ein Hauptidealbereich mit $K := \mathrm{Quot}(R) \neq R$.

1. K ist ein nicht endlich erzeugter, torsionsfreier R-Modul. (später)
2. K/R ist ein nicht endlich erzeugter R-Torsionsmodul. (zu kompliziert für uns.)
3. Jeder freie R-Modul ist torsionsfrei, insbesondere ${}_RR = R$ selbst.
4. Ist M beliebiger R-Modul, so ist $M/T(M)$ torsionsfrei (Übung).
5. Jeder **zyklische Modul** (sprich, von einem Element erzeugt), ist entweder isomorph zu ${}_RR \equiv R$ oder zu ${}_RR/Ra \equiv R/\langle a\rangle$ für ein $a \in R \setminus \{0\}$. Im letzteren Fall haben wir einen Torsionsmodul. (Obwohl ${}_RR/Ra$ und $R/\langle a\rangle$ als abelsche Gruppen identisch sind und auch als R-Moduln, wenn man die R-Modulstruktur auf $R/\langle a\rangle$ wie erwartet definiert, wollen wir doch im Kontext von Moduln lieber die erste und im Kontext von Restklassenringen die zweite Notation benutzen; also, da $\mathrm{Ann}_R({}_RR/Ra) := \cap_{x\in {}_RR/Ra}\mathrm{Ann}_R(x) = \langle a\rangle$ können wir den R-Modul ${}_RR/Ra$ auch als $R/\langle a\rangle$-Modul auffassen. Als letzter ist er sogar frei.)
6. Endliche direkte Summen der Moduln aus 5. sind typische endlich erzeugte R-Moduln. Nur scheinbar allgemeiner sind die folgenden:
7. Faktormoduln von $R^{n\times 1}$ (freier Modul auf n Erzeugern) nach Teilmoduln.

Unser Ziel wird sein, zu zeigen, dass die Moduln aus 7. nicht allgemeiner sind als die Moduln aus 6. Hier zwei kleine Schritte in diese Richtung.

Lemma 3.52. *Sei R Integritätsbereich und $(e_1 = (1,0,\ldots,0)^{tr}, e_2, \ldots, e_n)$ die Standardbasis von $R^{n\times 1}$, also freies Erzeugendensystem des freien R-Moduls $\mathrm{Fr}_R(\underline{n}) \equiv R^{n\times 1}$. Sei $k \leq n$ und $d_1, \ldots, d_k \in R \setminus \{0\}$. Dann gilt*

$$\begin{aligned} R^{n\times 1}/\langle d_1e_1, \ldots, d_ke_k\rangle_R &= (\bigoplus_{i=1}^{n} Re_i)/(\bigoplus_{i=1}^{k} Rd_ie_i) \\ &\cong \bigoplus_{i=1}^{k} Re_i/Rd_ie_i \oplus \bigoplus_{i=k+1}^{n} Re_i \\ &\cong \bigoplus_{i=1}^{k} {}_RR/Rd_i \oplus R^{(n-k)\times 1}. \end{aligned}$$

Falls in dieser Situation noch zusätzlich d_i teilt d_{i+1} für $i = 1, \ldots, k-1$ gilt, so nennt man $(e_1, \ldots, e_n)$ und $(d_1e_1, \ldots, d_ke_k)$ **kompatible Basen**, *genauer ein Paar kompatibler Basen. (Den Begriff* **Basis** *benutzen wir als Synonym für freies Erzeugendensystem.)*

[1] Es gilt: $\mathrm{Ann}_R(M) = \cap_{m\in M}\mathrm{Ann}_R(m)$.

Beweis. Übung. Hinweis: Bestimme den offensichtlichen Epimorphismus

$$R^{n\times 1} \to \bigoplus_{i=1}^{k} {}_R R/Rd_i \oplus R^{(n-k)\times 1}$$

und wende den Homomorphiesatz für Moduln an. Beachte:

$$R^{k\times 1} \to \bigoplus_{i=1}^{k} Rd_ie_i : (a_1, \ldots, a_k)^{tr} \mapsto (a_1d_1, \ldots, a_kd_k, 0, \ldots, 0)^{tr}$$

ist ein R-Modulisomorphismus. □

Bislang wissen wir nicht einmal, dass Teilmoduln freier endlich erzeugter Moduln über Hauptidealbereichen frei sind, geschweige denn, ob kompatible Basen existieren. Hier ein erstes Indiz.

Lemma 3.53. *Sei R ein Hauptidealbereich und $M \cong R^{n\times 1}$ ein freier R-Modul von Rang n. Dann ist jeder R-Teilmodul von M endlich erzeugter freier R-Modul auf $k \leq n$ freien Erzeugern.*

Beweis. Wir führen den Beweis durch Induktion über n. Für $n = 1$ ist die Sache klar, da Teilmoduln von ${}_R R$ Ideale von R sind, also Hauptideale. Sei nun $T \leq_R M$ und $(e_1, \ldots, e_n)$ die Standard-R-Basis von M. Zu der Zerlegung

$$M = Re_1 \oplus \langle e_2, \ldots, e_n\rangle_R$$

gehört die Projektion $\pi : M \to Re_1$. Dann ist $\pi(T) \leq Re_1$. Im Falle $\pi(T) = \{0\}$ greift die Induktionsvoraussetzung sofort. Sonst ist $\pi(T) = Rde_1$ für ein $d \in R \setminus \{0\}$. Beachte, $\pi(T)$ ist frei auf de_1. Wähle $t \in T$ mit $\pi(t) = de_1$. Dann definiert

$$\iota : Rde_1 \to T : de_1 \mapsto t$$

einen R-Modulmonomorphismus und es gilt (Übung)

$$T = Rt \oplus \operatorname{Kern} \pi_{|T}.$$

Wegen $\operatorname{Kern} \pi_{|T} \leq \langle e_2, \ldots, e_n\rangle_R$ können wir die Induktionsvoraussetzung benutzen und bekommen unsere Behauptung. □

Wir wollen jetzt die Existenz kompatibler Basen beweisen, indem wir sowohl beim Teilmodul $R^{k\times 1}$ als auch bei $R^{n\times 1}$ Basistransformationen vornehmen.

Bemerkung 3.54. Sei R ein Hauptidealbereich.

1. Die Beschreibung von Homomorphismen von freien R-Moduln in freie R-Moduln (alle endlich erzeugt) geschieht wie bei Vektorräumen durch Matrizen bezüglich Basen. (Alle relevanten Formeln aus der linearen Algebra bleiben gültig.)

2. Automorphismen von freien R-Moduln (vom Rang n) und Basistransformationen werden beschrieben durch Matrizen aus

$$(R^{n\times n})^* = \mathrm{GL}(n, R) = \{g \in R^{n\times n} \mid \det(g) \in R^*\}.$$

3. Für $a, b \in R \setminus \{0\}$ mit $\mathrm{ggT}(a, b) = d$ gibt es $s, t \in R$ mit $sa + tb = d$. Es gilt

$$U_{(a,b)} := \begin{pmatrix} s & t \\ -\frac{b}{d} & \frac{a}{d} \end{pmatrix} \in \mathrm{GL}(2, R) \text{ und } U_{(a,b)} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Satz 3.55. *Sei R Hauptidealbereich und $C \in R^{k\times n}$. Dann existieren Matrizen $A \in \mathrm{GL}(k,R)$ und $B \in \mathrm{GL}(n,R)$, so dass*

$$ACB = \begin{pmatrix} \mathrm{Diag}(d_1,\ldots,d_l) & 0 \\ 0 & 0 \end{pmatrix}$$

mit $d_i \in R\setminus\{0\}, l \le \min(k,n)$ und $d_i \mid d_{i+1}$ für $i = 1,\ldots,l-1$. Die Matrix ACB nennt man die **Smith-Form** *von C.*

Ende Vorl. 14

Beweis. Setze $C_1 := C$. Wir führen reversible Zeilenoperationen durch, und erhalten $C_2 := A_1C_1, C_3 := A_2C_2, \ldots, C_r := A_{r-1}C_{r-1}$, so dass die erste Spalte von C_r gleich $(d,0,\ldots,0)^{tr}$. Dabei sind die A_i Permutationsmatrizen oder von der Form $\mathrm{Diag}(U_{(a,b)}, I_{k-2})$, wenn die obersten zwei Einträge a,b der jeweils ersten Spalte von C_i von Null verschieden sind. Beachte, d ist der grösste gemeinsame Teiler der Einträge der ersten Spalte von C.
Danach führen wir reversible Spaltenoperationen durch und erhalten $C_{r+1} := C_rB_1$, …, $C_{r+s} := C_{r+s-1}B_s$, so dass die erste Zeile von C_{r+s} gleich $(d',0,\ldots,0)$ ist. Dabei sind die B_i Permutationsmatrizen oder von der Form $\mathrm{Diag}(U^{tr}_{(a,b)}, I_{n-2})$, wenn die ersten zwei Einträge a,b der jeweils ersten Zeile von C_i von Null verschieden sind. Klar: $d' \mid d$. Aber leider ist jetzt die erste Spalte nicht mehr notwendig ausgeräumt, so dass man den ersten Schritt wiederholen muss. Da aber R keine echten unendlichen Teilerketten zulässt hat man nach endlich vielen Wiederholungen die Matrix $C_t := \mathrm{Diag}(d_1, C')$.
Rekursives Anwenden der Methode auf C' liefert nach endlich vielen Schritten schliesslich Matrizen $A' \in \mathrm{GL}(n,R), B' \in \mathrm{GL}(k,R)$, so dass

$$C' := A'CB' = \begin{pmatrix} \mathrm{Diag}(d_1,\ldots,d_l) & 0 \\ 0 & 0 \end{pmatrix}$$

mit $d_i \in R\setminus\{0\}$. Sollte für ein i noch die Bedingung $d_i \mid d_{i+1}$ verletzt sein, sind noch weitere Umformungen durchzuführen. Es genügt, diese für 2×2-Matrizen zu demonstrieren:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mathrm{Diag}(d_i, d_{i+1}) = \begin{pmatrix} d_i & d_{i+1} \\ 0 & d_{i+1} \end{pmatrix}$$

also eine Matrix, die man mit den anfänglichen Methoden wieder auf die Form

$$\mathrm{Diag}(\mathrm{ggT}(d_i,d_{i+1}), \mathrm{kgV}(d_i,d_{i+1}))$$

transformieren kann. Nach endlich vielen Schritten hat man die geforderte Gestalt. □

Übung 3.13. Gib ein effektives Verfahren für Matrizen über EUKLIDischen Bereichen an, welches versucht, immer das Matrixelement einer festen Spalte bzw. einer festen Zeile mit dem größten ν-Wert abzubauen, bis die Spalte oder Zeile ausgeräumt ist.

Beispiel 3.56. Sei $R := \mathbb{Z}$ und $A := \begin{pmatrix} 6 & 2 \\ 8 & 7 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$.

Mit $U_1 := \begin{pmatrix} -1 & 1 \\ 4 & -3 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$ folgt $U_1A = \begin{pmatrix} 2 & 5 \\ 0 & -13 \end{pmatrix}$.

Mit $W_1 := \begin{pmatrix} 3 & 5 \\ -1 & -2 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$ folgt $U_1AW_1 = \begin{pmatrix} 1 & 0 \\ 13 & 26 \end{pmatrix}$.

Mit $U_2 := \begin{pmatrix} 1 & 0 \\ -13 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$ folgt $U_2U_1AW_1 = \mathrm{Diag}(1,26)$.

Beispiel 3.57. Simultane Kongruenzen

$$\begin{aligned} x_1 + x_2 &\equiv 0 \pmod{\mathbb{Z}} \\ x_1 - x_2 &\equiv 1/4 \pmod{\mathbb{Z}} \end{aligned}$$

sind für $x_1, x_2 \in \mathbb{R}$ zu lösen. Wir schreiben dies als Matrix:

$$\left(\begin{array}{cc|c} 1 & 1 & 0 \\ 1 & -1 & 1/4 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & -2 & 1/4 \end{array}\right) \xrightarrow{W:=\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}} \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 2 & 1/4 \end{array}\right)$$

Aus der letzten Matrix lesen wir die Zwischenlösung

$$y = \begin{pmatrix} z_1 \\ 1/8 + 1/2 z_2 \end{pmatrix} \qquad \text{mit } z_1, z_2 \in \mathbb{Z}$$

ab und erhalten als endgültige Lösung durch Multiplikation mit W:

$$x = \begin{pmatrix} 1/8 + z_1 + 1/2 z_2 \\ -1/8 - 1/2 z_2 \end{pmatrix} \qquad \text{mit } z_1, z_2 \in \mathbb{Z}$$

Lineare Differentialgleichungssysteme mit konstanten Koeffizienten erweisen sich auch als Kongruenzsysteme über $\mathbb{R}[x]$ oder $\mathbb{C}[x]$. Solange die rechte Seite Null ist, sind keine Probleme der Analysis involviert. Im inhomogenen Fall braucht man aus der Analysis die Methode der Variation der Konstanten. Wir beschränken uns auf den homogenen Fall.

Beispiel 3.58. Seien x_1, x_2, x_3 unendlich oft differenzierbare Funktionen auf $\mathbb{R}$ oder Elemente von $\mathbb{R}[[t]]$. Gesucht sind die Lösungen des Differentialgleichungssystems

$$\begin{aligned} x_1' - x_2' + x_3'' &= b_1 \\ x_1 + x_2'' + x_3' &= b_2 \end{aligned}$$

mit $b_1 = b_2 = 0$. In Matrizen, wobei D dann die Ableitung induzieren soll:

$$M \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 0 \text{ mit } M := \begin{pmatrix} D & -D & D^2 \\ 1 & D^2 & D \end{pmatrix},$$

Zeilenumformungen:

$$\left(\begin{array}{ccc|c} D & -D & D^2 & b_1 \\ 1 & D^2 & D & b_2 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & D^2 & D & b_2 \\ 0 & D^3 + D & 0 & -b_1 + D b_2 \end{array}\right)$$

Spaltenumformungen mit

$$W := \begin{pmatrix} 1 & -D^2 & -D \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ liefert } \begin{pmatrix} 1 & 0 & 0 \\ 0 & D^3 + D & 0 \end{pmatrix}$$

als Matrix der linken Seite. Wegen $x^3 + x = x(x^2 + 1)$ löst sich dieses System sehr leicht:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 \\ a + b\sin(t) + c\cos(t) \\ f(t) \end{pmatrix}$$

mit $a, b, c \in \mathbb{R}$ und f eine unendlich oft differenzierbare Funktion $\mathbb{R} \to \mathbb{R}$. Durch Heranmultiplizieren von W erhalten wir die Lösungen des ursprünglichen Systems:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} b\sin(t) + c\cos(t) - f'(t) \\ a + b\sin(t) + c\cos(t) \\ f(t) \end{pmatrix}$$

Hauptsatz 3.59. *Sei R ein Hauptidealbereich.*

1. *Ist M ein endlich erzeugter R-Modul, so gibt es $s, t \in \mathbb{Z}_{\geq 0}$ und $d_1, \ldots, d_t \in R \setminus (R^* \cup \{0\})$ mit $d_i \mid d_{i+1}$ für alle i, so dass*

$$M \cong_R R^{s\times 1} \oplus \bigoplus_{i=1}^{t} {}_R R/Rd_i.$$

2. *Gilt*

$$R^{s\times 1} \oplus \bigoplus_{i=1}^{t} {}_R R/Rd_i \cong_R R^{s'\times 1} \oplus \bigoplus_{i=1}^{t'} {}_R R/Rd'_i$$

mit $s, t, s', t' \in \mathbb{Z}_{\geq 0}$ und $d_1, \ldots, d_t, d'_1, \ldots, d'_{t'} \in R\setminus(R^*\cup\{0\})$ mit $d_i \mid d_{i+1}$ für $i = 1, \ldots, t-1$ und $d'_i \mid d'_{i+1}$ für $i = 1, \ldots, t'-1$, so gilt $s = s', t = t'$ und $d_i \sim d'_i$ für $i = 1, \ldots, t$. Man nennt s den **Rang** *(genauer torsionsfreien Rang) von M und d_i den i-ten* **Elementarteiler** *von M.*

Beweis.

1. Folgt sofort aus den vorangegangenen Lemmata und dem Satz.

2. Bezeichne die linke Seite mit M und die rechte mit N. Aus $M \cong N$ folgt

$$R^{s\times 1} \cong M/T(M) \cong N/T(N) \cong R^{s'\times 1}.$$

Sei $p \in R$ ein Primelement und $F := R/\langle p\rangle$ der zugehörige Restklassenkörper. Dann gilt:

$$s = \dim_F(\underbrace{R^{s\times 1}/pR^{s\times 1}}_{\cong (R/\langle p\rangle)^{s\times 1} = F^{s\times 1}}) = \dim_F(R^{s'\times 1}/pR^{s'\times 1}) = s'.$$

Weiter folgt $T(M) \cong T(N)$, also auch

$$\langle d_t\rangle = \mathrm{Ann}_R(T(M)) = \mathrm{Ann}_R(T(N)) = \langle d_{t'}\rangle \text{ d.h. } d_t \sim d'_{t'}.$$

Um die d_i zu rekonstruieren, brauchen wir nur die p-Potenzen zu testen, welche in den d_i aufgehen, wobei die p die Primteiler von d_t durchläuft. Man betrachtet hierzu die Zahlenfolge

$$\dim_F p^i T(M)/p^{i+1}T(M) = \dim_F p^i T(N)/p^{i+1}T(N)$$

für $i = 0, 1, \ldots k(p)$, wo $p^{k(p)}$ die höchste p-Potenz ist, die in d_t aufgeht. Es ist klar, wie man (durch Übergang zur sogenannten assoziierten Partition) die p-Potenzanteile der d_i und der d'_i rekonstruieren kann und so $d_i \sim d'_i$ und $t = t'$ beweist. Beachte: $t = t'$ ist die minimale Erzeugendenzahl von $T(M) \cong T(N)$ und gleich dem Maximum der Dimensionen der $T(M)/pT(M) \cong T(N)/pT(N)$ als $R/\langle p\rangle$-Vektorräume, wo p die Primteiler von d_t durchläuft. □

Ende Vorl. 15

Folgerung 3.60. *Sei $M = T(M)$ ein endlich erzeugter R-Torsionsmodul mit $\mathrm{Ann}(M) = \langle d \rangle$. Ist $d \sim \prod_i p_i^{n_i}$ die Faktorisierung in Potenzen von Primelementen, so zerlegt sich nach dem Chinesischen Restsatz*

$$R/\langle d \rangle \cong \bigtimes_i R/\langle p_i^{n_i} \rangle \text{ und entsprechend } M \cong \bigoplus_i M/p_i^{n_i} M$$

und $M/p_i^{n_i} M$ ist $R/\langle p_i^{n_i} \rangle$-Modul.
Ist $p \in R$ prim, so sind die endlich erzeugten $R/\langle p^n \rangle$-Moduln durch endliche monoton steigende Folgen a natürlicher Zahlen $\leq n$ charakterisiert: a liefert den Modul

$$\bigoplus_i {}_R R/Rp^{a_i}.$$

Folgerung 3.61. *Sei M ein e.e. torsionsfreier R-Modul. Dann ist M frei.*

Achtung: Dies ist falsch für nicht e.e. torsionsfreie R-Moduln. Ist z.B. $R = \mathbb{Z}$, so ist $\mathbb{Q}$ ein torsionsfreier $\mathbb{Z}$-Modul. Jedoch ist $\mathbb{Q}$ nicht frei, denn für je zwei Elemente $a/b, c/d \in \mathbb{Q}$ gilt $(bc)a/b - (ad)c/d = 0$.

Folgerung 3.62. *Sei R ein Hauptidealbereich mit $K := \mathrm{Quot}(R) \neq R$. Dann ist K ist ein nicht endlich erzeugter, torsionsfreier R-Modul. (Übung)*

4.2 Der Hauptsatz über endlich erzeugte abelsche Gruppen

Wir wenden unsere Erkenntnisse jetzt speziell für den Ring $R = \mathbb{Z}$ an. Die $\mathbb{Z}$-Moduln sind genau die abelschen Gruppen, endlich erzeugte $\mathbb{Z}$-Moduln also endlich erzeugte abelsche Gruppen und wir erhalten den folgenden Struktursatz.

Folgerung 3.63. *(Hauptsatz über endlich erzeugte abelsche Gruppen) Sei $G = \langle g_1, \ldots, g_n \rangle$ eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, s \in \mathbb{Z}_{\geq 0}$, $h_1, \ldots, h_r \in G$, $t_1, \ldots, t_s \in G$, $d_1, \ldots, d_s \in \mathbb{Z}$ mit $d_1 | d_2 | \ldots | d_s$, so dass*

$$G = \langle h_1 \rangle \times \ldots \langle h_r \rangle \times \langle t_1 \rangle \times \ldots \times \langle t_s \rangle \cong \mathbb{Z}^r \oplus \mathbb{Z}/(d_1\rangle \oplus \ldots \oplus \mathbb{Z}/(d_s\rangle$$

Folgerung 3.64.

1. *Sei G eine endliche abelsche Gruppe von Ordnung $|G| = p_1^{n_1} \ldots p_s^{n_s}$. Dann ist G ein $\mathbb{Z}/\langle \prod_{i=1}^s p_i^{n_i} \rangle$-Modul. Dieser Ring ist nach dem chinesischen Restsatz isomorph zu $\bigtimes_{i=1}^s \mathbb{Z}/\langle p_i^{n_i} \rangle$. Dementsprechend läßt sich G eindeutig schreiben als*

$$G = \bigoplus_{i=1}^s P_i$$

   wo $|P_i| = p_i^{n_i}$ ist. (P_i nennt man auch die p_i-Sylowgruppe von G).

2. *Sei P eine abelsche Gruppe von Primzahlpotenzordnung $|P| = p^n > 1$ (p-Gruppe). Dann gibt es eindeutiges $t \in \mathbb{N}$, $a_1 \leq \ldots \leq a_t \in \mathbb{N}$ mit $P \cong \mathbb{Z}/\langle p^{a_1} \rangle \oplus \ldots \oplus \mathbb{Z}/\langle p^{a_t} \rangle$.*

Beispiel 3.65. Die abelschen Gruppen der Ordnung $24 = 2^3 \cdot 3$ sind: $\mathbb{Z}/\langle 24 \rangle = \mathbb{Z}/\langle 8 \rangle \oplus \mathbb{Z}/\langle 3 \rangle$, $\mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 4 \rangle \oplus \mathbb{Z}/\langle 3 \rangle$, $\mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 3 \rangle$.

Folgerung 3.66. *Sei G eine endliche abelsche Gruppe, $a \in G$. Das $n \in \mathbb{N}$ mit $n\mathbb{Z} = \mathrm{Ann}_{\mathbb{Z}}(a)$ nennt man auch die* **Ordnung** *von a. Es gilt $\mathrm{ord}(a) = |\langle a \rangle|$ und $\mathrm{ord}(a)$ teilt $|G|$.*
Existiert ein $a \in G$, so dass $\langle a \rangle = G$, so heißt G **zyklische Gruppe**. *Von Ordnung $m \in \mathbb{Z}_{\geq 0}$ ist $C_m := (\mathbb{Z}/m\mathbb{Z}, +)$ bis auf Isomorphie die einzige zyklische Gruppe von Ordnung m.*

Wir wollen unsere Ergebnisse jetzt auf Einheitengruppen von Restklassenringen von $\mathbb{Z}$ anwenden. $(\mathbb{Z}/m\mathbb{Z})^* = \{a + m\mathbb{Z} \in \{1, \ldots, m-1\} \mid \mathrm{ggT}(a, m) = 1\}$.

Definition 3.67. Die Eulersche φ-Funktion:

$$\varphi : \mathbb{N} \implies \mathbb{N};\ \ \varphi(m) := |(\mathbb{Z}/m\mathbb{Z})^*|$$

Bemerkung 3.68.

1. (Kleiner Satz von Fermat) Ist p eine Primzahl und $a \in \mathbb{Z}$, dann $a^p \equiv a \pmod p$, denn $\varphi(p) = p - 1$.

2. Ist p eine Primzahl, so ist $(\mathbb{Z}/p^a\mathbb{Z})^* = \mathbb{Z}/p^a\mathbb{Z} \setminus p(\mathbb{Z}/p^a\mathbb{Z})$ also $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.

3. Ist $m = \prod_{j=1}^s p_j^{\alpha_j}$ mit paarweise verschiedenen Primzahlen p_j und $\alpha_j \geq 1$, dann ist $\mathbb{Z}/m\mathbb{Z} = \bigtimes_j \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$ nach dem chinesischen Restsatz, also auch $(\mathbb{Z}/m\mathbb{Z})^* = \times_j (\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^*$.

4. Es ist $\varphi(m) = \prod_{j=1}^s p_j^{\alpha_j - 1}(p_j - 1)$.

Lemma 3.69. $\sum_{d|m} \varphi(d) = m$.

Beweis. Sei $m = \prod_{j=1}^s p_j^{\alpha_j}$. Induktion über $\sum_{j=1}^s \alpha_j =: n$.
$n = 1$: Klar.
Induktionsschritt:

$$\sum_{d|m} \varphi(d) = \sum_{d|m/p_1} \varphi(d) + \sum_{d|m/(p_1^{\alpha_1})} \varphi(p_1^{\alpha_1} d) =$$

$$m/p_1 + p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2} \ldots p_s^{\alpha_s} = m. \qquad \square$$

Satz 3.70. *Sei K ein endlicher Körper. Dann ist seine Einheitengruppe zyklisch.*

Beweis. Betrachte $(K^*, \cdot)$ als $\mathbb{Z}$-Modul über $za = a^z$ für $z \in \mathbb{Z}$ und $a \in K^*$. Zeigen: Für jeden Teiler d von $|K| - 1$ hat K^* genau $\varphi(d)$ Elemente der Ordnung d.
Denn: Sei $\psi(d) := |\{a \in K^* \mid \mathrm{ord}(a) = d\}|$. Dann gilt $d \nmid |K| - 1 \implies \psi(d) = 0$.
Ist $a \in K^*$, $\mathrm{ord}(a) = d$, so ist $\langle a \rangle$ die Menge der d verschiedenen Nullstellen von $X^d - 1$. Die Elemente der Ordnung d in $\langle a \rangle$ sind genau die a^m mit $\mathrm{ggT}(m, d) = 1$, also ist ihre Anzahl genau $\varphi(d)$ und $\psi(d) \leq \varphi(d)$. Deshalb ist

$$|K| - 1 = |K^*| = \sum_{d||K|-1} \psi(d) \leq \sum_{d||K|-1} \varphi(d) = |K| - 1.$$

Also $\psi(d) = \varphi(d)$. Insbesondere ist $\psi(|K| - 1) \neq 0$ und $K^* = \langle a \rangle$ für jedes Element $a \in K^*$ mit $\mathrm{ord}(a) = |K| - 1$. $\square$

Ende Vorl. 16

Satz 3.71. *Sei p eine Primzahl, $\alpha \geq 1$.*

1. *Ist $p > 2$, so ist $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong (\mathbb{Z}/p^{\alpha-1}\mathbb{Z}, +) \oplus (\mathbb{Z}/(p-1)\mathbb{Z}, +)$.*

2. *Ist $\alpha \geq 2$, so ist $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}, +) \oplus (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}, +)$.*

Beweis.

1. Zeige: Die Gruppe ist zyklisch. Mit Hilfe des binomischen Lehrsatzes zeigt man: Ist $\beta \geq 1$, $b \in \mathbb{Z}$, $p \nmid b$, dann ist
$$(1 + p^\beta b)^p = 1 + p^{\beta+1} c$$
für ein $c \in \mathbb{Z}$ mit $p \nmid c$.
Ist $a \in \mathbb{Z}$ mit $\langle a + p\mathbb{Z}\rangle = (\mathbb{Z}/p\mathbb{Z})^*$, so ist $a^{p-1} = 1 + pb$ für ein $b \in \mathbb{Z}$. Gilt $p \nmid b$, so ist $\langle a + p^\alpha \mathbb{Z}\rangle = (\mathbb{Z}/p^\alpha\mathbb{Z})^*$. Falls $p \mid b$, dann ersetze a durch $a+p$ und erhalte $\langle a+p+p^\alpha\mathbb{Z}\rangle = (\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

2. als Übung. □

Damit haben wir die Struktur der Einheitengruppe von $\mathbb{Z}/m\mathbb{Z}$ bestimmt, denn dieser Ring ist nach dem chinesischen Restsatz isomorph zu

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z},$$

falls $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ eine Primfaktorzerlegung von m ist. Also ist seine Einheitengruppe das direkte Produkt der Einheitengruppen

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^*.$$

Kapitel 4

Normalformen für Matrizen.

1 Ähnlichkeit von Matrizen

Wir wollen über das Klassifikationsproblem der Endomorphismen eines endlich dimensionalen K-Vektorraumes sprechen oder, was äquivalent hierzu ist, über eine Normalform der Matrizen des Endomorphismus, die durch eine gewisse Basiswahl erreicht wird.

Definition 4.1. Sei $\mathcal{V}$ ein endlich erzeugter Vektorraum über dem Körper K der Dimension $n \in \mathbb{N}$.

1. Zwei Endomorphismen $\alpha, \beta \in \mathrm{End}(\mathcal{V})$ heißen **ähnlich** oder **konjugiert** unter $\mathrm{GL}(\mathcal{V})$, falls ein $\gamma \in \mathrm{GL}(\mathcal{V})$ existiert mit $\alpha = \gamma \circ \beta \circ \gamma^{-1}$.

2. Zwei Matrizen $A, B \in K^{n\times n}$ heißen **ähnlich** oder **konjugiert** unter $\mathrm{GL}(n, K)$, falls ein $g \in \mathrm{GL}(n, K)$ existiert mit $A = gBg^{-1}$.

3. Sei R ein Integritätsbereich. Zwei Matrizen $A, B \in R^{n\times m}$ heißen **äquivalent** (über R), wenn es $g \in \mathrm{GL}_n(R)$, $h \in \mathrm{GL}_m(R)$ gibt mit $gAh = B$.

Klar: Äquivalenz von Matrizen ist eine Äquivalenzrelation.
Den Struktursatz 3.55 kann man auch so formulieren: Ist R ein Hauptidealbereich, so ist jede Matrix äquivalent zu einer Diagonalmatrix.
Ähnliche Matrizen sind äquivalent über K. Die Umkehrung gilt jedoch nicht. Z.B. ist jede Matrix in $\mathrm{GL}_n(K)$ ist äquivalent über K zur Einheitsmatrix, aber dies ist nicht richtig für Ähnlichkeit.
Die Matrizen, die einen festen Endomorphismus beschreiben, bilden eine Ähnlichkeitsklasse, wenn man die Basis variieren lässt. Umgekehrt sind zwei Endomorphismen genau dann durch dieselbe Matrix beschreibbar, wenn sie konjugiert sind.

Bemerkung 4.2. μ_α, χ_α sind Invarianten (aus denen man Spur und Determinante ablesen kann). Für jedes Polynom $p(x) \in K[x]$ ist

$$\mathrm{End}(\mathcal{V}) \to \mathbb{Z}_{\geq 0} : \alpha \mapsto \mathrm{Dim}(\mathrm{Kern}(p(\alpha)))$$

eine Invariante.

Wir wollen in diesem Abschnitt für einen gegebenen Endomorphismus $\alpha \in \mathrm{End}(\mathcal{V})$ eine möglichst einfache Form für die Matrix ${}^B\alpha^B$ finden. Bislang haben wir nur Teilergebnisse und Spezialfälle erledigt, an die wir uns kurz erinnern wollen. Für den ganzen Abschnitt sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum. Hier ist eine Zusammenfassung einiger relevanter Ergebnisse aus dem ersten Semester.

Bemerkung 4.3. Ist $\mu_\alpha(x) = \prod_{i=1}^{\ell} p_i^{m_i}$ die Zerlegung des Minimalpolynoms in normierte irreduzible und paarweise verschiedene Polynome p_i, dann gilt:

1. Das charakteristische Polynom ist gegeben durch $\chi_\alpha(x) = \prod_{i=1}^{\ell} p_i^{c_i}$ mit $c_i \geq m_i$.
2. Man hat eine kanonische Zerlegung von $\mathcal{V}$ in die p_i-**Haupträume** $\mathcal{V}_i := \mathrm{Kern}(p_i^{m_i}(\alpha))$, die alle α-invariant sind:
$$\mathcal{V} = \bigoplus_{i=1}^{\ell} \mathcal{V}_i.$$
Man hat $\mathcal{V}_i = \mathrm{Kern}(p_i^{m_i}(\alpha)) = \mathrm{Bild}(q_i(\alpha))$ mit $q_i := \prod_{j\neq i}^{\ell} p_j^{m_j}$.
3. Die Projektionen der Zerlegung sind gegeben durch $\pi_i = (a_i q_i)(\alpha)$ wobei $a_i \in K[x]$ mit
$$1 = a_1 q_1 + \ldots + a_\ell q_\ell$$
gegeben sind.
4. Für die Dimension der Haupträume gilt
$$\mathrm{Dim}(\mathrm{Kern}(p_i^{m_i}(\alpha))) = c_i \,\mathrm{Grad}(p_i).$$
5. Im Falle $m_i = 1$ ist $\mathrm{Kern}(p_i^{m_i}(\alpha))$ ein $K[x]/\langle p_i\rangle$-Vektorraum der Dimension c_i, und aus einer $K[x]/\langle p_i\rangle$-Basis konstruiert man leicht eine K-Basis, die für die Einschränkung von α auf $\mathrm{Kern}(p_i^{m_i}(\alpha))$ die Matrix $\mathrm{Diag}(M_{p_i}, \ldots, M_{p_i})$ liefert, wobei M_{p_i} die Begleitmatrix von p_i ist. (Wichtiger Spezialfall: $p_i(x) = x - a$ für ein $a \in K$. Dann ist $M_{p_i} = (a)$ und wir haben ($m_i = 1$ vorausgesetzt) eine Basis aus Eigenvektoren für den Hauptraum.)

Übung 4.1. Sei $\mu_\alpha = p^r$ für ein irreduzibles normiertes Polynom $p \in K[x]$. Zeige, dass der Algorithmus zur Berechnung des Minimalpolynoms einen Vektor $V \in \mathcal{V}$ als Nebenprodukt produziert, für dessen Minimalpolynom gilt: $\mu_{\alpha,V} = \mu_\alpha$.

Mit diesen Vorbemerkungen wollen wir zunächst einen kurzen Blick auf den Zentralisator eines Endomorphimus werfen.

Definition 4.4. Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum der Dimension n und $\alpha \in \mathrm{End}(\mathcal{V})$. Dann heißt
$$C_{\mathrm{End}(\mathcal{V})}(\alpha) := \{\beta \in \mathrm{End}(\mathcal{V}) | \alpha \circ \beta = \beta \circ \alpha\} \leq \mathrm{End}(\mathcal{V})$$
der **Zentralisator** oder die **Zentralisatoralgebra** von α (in $\mathrm{End}(\mathcal{V})$).
Für $A \in K^{n\times n}$ ist die Zentralisatoralgebra von A definiert als $C_{K^{n\times n}}(A) := \{X \in K^{n\times n} \mid AX = XA\}$

Bemerkung 4.5. $C_{\mathrm{End}(\mathcal{V})}(\alpha)$ ist der Kern der linearen Abbildung
$$\mathrm{End}(\mathcal{V}) \to \mathrm{End}(\mathcal{V}) : \gamma \mapsto \alpha \circ \gamma - \gamma \circ \alpha$$
und somit ein Teilraum des K-Vektorraums $\mathrm{End}(\mathcal{V})$. Da $C_{\mathrm{End}(\mathcal{V})}(\alpha)$ auch abgeschlossen ist unter Komposition von Abbildungen, ist $C_{\mathrm{End}(\mathcal{V})}(\alpha)$ eine Teilalgebra von $\mathrm{End}(\mathcal{V})$.

Beispiel 4.6. Ist $A = \mathrm{Diag}(0, 1) \in K^{2\times 2}$ so ist $C_{K^{2\times 2}}(A) = \{\mathrm{Diag}(a, b) \mid a, b \in K\} = K[A]$. Für $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{2\times 2}$ ist $C_{\mathbb{F}_2^{2\times 2}}(A) = \mathbb{F}_2[A] \cong \mathbb{F}_4$. Betrachtet man die Blockdiagonalmatrix $\mathrm{Diag}(A, A) \in \mathbb{F}_2^{4\times 4}$ so ist ihr Zentralisator isomorph zu $\mathbb{F}_4^{2\times 2}$ (Übung).

Satz 4.7. *Sei $\alpha \in \mathrm{End}(\mathcal{V})$ etc. wie in Bemerkung 4.3. Setze $\mathcal{V}_i = \pi_i(\mathcal{V})$, $\alpha_i := \alpha_{|\mathcal{V}_i} : \mathcal{V}_i \to \mathcal{V}_i$.*

1. *Für $\beta \in C_{\mathrm{End}(\mathcal{V})}(\alpha)$ und $1 \leq i < j \leq \ell$ gilt $\pi_i \circ \beta \circ \pi_j = 0$, d.h. β respektiert die Zerlegung von $\mathcal{V}$ in seine Haupträume, und somit gilt insbesondere*

$$\beta = \sum_{i=1}^{\ell} \underbrace{\pi_i \circ \beta \circ \pi_i}_{\in C_{\mathrm{End}(\mathcal{V}_i)}(\alpha_i)}$$

und

$$C_{\mathrm{End}(\mathcal{V})}(\alpha) = \bigtimes_{i=1}^{\ell} C_{\mathrm{End}(\mathcal{V}_i)}(\alpha_i)$$

2. *Sei $\mu_\alpha(x) = \chi_\alpha(x)$, also das Minimalpolynom und das charakteristische Polynom seien gleich. Dann ist*

$$(\mathrm{id}_\mathcal{V}, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

mit $n = \mathrm{Dim}(\mathcal{V})$ eine K-Vektorraumbasis von $C_{\mathrm{End}(\mathcal{V})}(\alpha)$.

Beweis.

1. Da $\beta \in C_{\mathrm{End}(\mathcal{V})}(\alpha)$ mit α vertauschbar ist, ist es auch mit jedem Polynom in α vertauschbar, insbesondere mit den π_i. Damit folgen die ersten Aussagen. Weiter ist $\pi_i \in C_{\mathrm{End}(\mathcal{V})}(\alpha)$ für jedes i und als Polynom in α ist π_i mit jedem Element in $C_{\mathrm{End}(\mathcal{V})}(\alpha)$ vertauschbar. Daher ist jedes

$$C_{\mathrm{End}(\mathcal{V})}(\alpha) = \bigoplus_i \pi_i C_{\mathrm{End}(\mathcal{V})}(\alpha)$$

und $\pi_i C_{\mathrm{End}(\mathcal{V})}(\alpha) = C_{\mathrm{End}(\mathcal{V}_i)}(\alpha_i)$.

Ende Vorl. 17

2. Aus der Vorübung schließen wir, dass jeder Hauptraum $\mathcal{V}_i$ einen Vektor enthält, dessen Minimalpolynom gleich p^{m_i} ist. Wegen $\mu_\alpha(x) = \chi_\alpha(x)$ liefert die Summe dieser Vektoren uns einen Vektor $V \in \mathcal{V}$ mit mit Minimalpolynom $\mu_{\alpha,V}(x) = \mu_\alpha(x)$.
Unter den gegebenen Voraussetzungen ist

$$(V, \alpha(V), \ldots, \alpha^{n-1}(V))$$

eine Basis von $\mathcal{V}$. Sei nun $\beta \in C_{\mathrm{End}(\mathcal{V})}(\alpha)$ und

$$\beta(V) = V' = \sum a_i \alpha^i(V) \text{ für geeignete } a_i \in K.$$

Dann ist $\beta(\alpha(V)) = \alpha(\beta(V)) = \alpha(V')$ und allgemeiner $\beta(\alpha^j(V)) = \alpha^j(V')$, also

$$\beta(\alpha^j(V)) = (\sum_i a_i \alpha^i)(\alpha^j(V)).$$

Also hat β denselben Effekt auf unsere Basis wie $\sum a_i \alpha^i$, somit ist $\beta = \sum a_i \alpha^i$. □

Übung 4.2. Zeige: Im Falle $\mu_\alpha = \chi_\alpha$ ist $C_{\mathrm{End}(\mathcal{V})}(\alpha)$ als K-Algebra isomorph zu $K[x]/\langle \mu_\alpha \rangle$.

Übung 4.3. Man formuliere den letzten Satz und die zugehörigen Übungen in der Sprache der Matrizen. (Sehr wichtig!)

Die Situation aus Satz 4.7 hat einen Namen:

Definition 4.8. Sei $\alpha \in \mathrm{End}(\mathcal{V})$. Jeder Vektor $V \in \mathcal{V}$ mit $\langle V \rangle_\alpha := K[\alpha](V) = \mathcal{V}$ heißt ein **zyklischer Vektor** von $\mathcal{V}$ (bezüglich α). Falls ein solcher existiert, heißt $\mathcal{V}$ ein **zyklischer Vektorraum** bezüglich α.

Beispiel 4.9. Sei $A = \mathrm{Diag}(0,1) \in K^{2\times 2}$. Ist $K^{2\times 1}$ ein zyklischer Vektorraum bezüglich $\widetilde{A}$?

Sei $B = \mathrm{Diag}(1,1) = I_2 \in K^{2\times 2}$. Ist $K^{2\times 1}$ ein zyklischer Vektorraum bezüglich $\widetilde{B}$?

Klar: $\mathcal{V}$ ist genau dann ein zyklischer Vektorraum bezüglich $\alpha \in \mathrm{End}(\mathcal{V})$ wenn $\mu_\alpha = \chi_\alpha$ gilt, denn für jeden zyklischen Vektor V hat $\mu_{\alpha,V}$ den Grad $\dim(\mathcal{V})$. Die Umkehrung ist eine Übungsaufgabe.

2 Normalformen für Matrizen

2.1 Die rationale kanonische Form

In diesem Abschnitt möchten wir den Struktursatz für Moduln über Hauptidealbereichen anwenden, um eine Normalform für Ähnlichkeitsklassen von Matrizen zu erhalten. Sei dazu K ein Körper.

Satz 4.10.

1. *Jede Matrix $A \in K^{n\times n}$ macht $K^{n\times 1}$ zu einem $K[x]$-Modul durch $p(x)V = p(A)V$ für alle $V \in K^{n\times 1}$, $p(x) \in K[x]$. Diesen $K[x]$-Modul bezeichnen wir mit M_A.*
2. *Es ist $\mathrm{Ann}_{K[x]}(M_A) = \langle \mu_A \rangle \lhd K[x]$ das vom Minimalpolynom von A erzeugte Ideal.*
3. $\mathrm{End}_{K[x]}(M_A) \cong C_{K^{n\times n}}(A) = \{X \in K^{n\times n} \mid XA = AX\}$.
4. *Für $A, B \in K^{n\times n}$ gilt $M_A \cong M_B$ genau dann, wenn es ein $g \in \mathrm{GL}_n(K)$ gibt mit $A = g^{-1}Bg$, also genau dann wenn A und B ähnlich sind.*

Beweis.

1. & 2. hatten wir schon früher bemerkt.
3. Der $K[x]$-Modul M_A wird durch Einschränkung zu einem K-Modul, also einem K-Vektorraum. Insbesondere sind alle $K[x]$-Modulhomomorphismen auch K-lineare Abbildungen und somit gegeben durch Multiplikation mit einer Matrix. Für $X \in K^{n\times n}$ ist die K-lineare Abbildung $\widetilde{X} \in \mathrm{End}_{K[x]}(M_A)$ genau dann, wenn $\widetilde{X}(xV) = x\widetilde{X}(V)$ für alle $V \in K^{n\times 1}$, also genau dann wenn $XAV = AXV$ für alle $V \in K^{n\times 1}$, d.h. $XA = AX$ und somit $X \in C_{K^{n\times n}}(A)$.
4. Sei $\widetilde{X} : M_A \to M_B$ ein Isomorphismus. Dann ist insbesondere die lineare Abbildung $\widetilde{X}$ bijektiv, also $X \in \mathrm{GL}_n(K)$. Weiter erfüllt $\widetilde{X}$ die Bedingung $\widetilde{X}(AV) = B\widetilde{X}(V)$ für alle $V \in K^{n\times 1}$, also $XA = BX$ und somit $A = X^{-1}BX$. □

Übung 4.4. Formulieren Sie obigen Satz und alle weiteren Ergebnisse dieses Abschnitts in der Sprache der Endomorphismen.

Definition 4.11. Sei $A \in K^{n\times n}$. Die **charakteristische Matrix** $\mathfrak{X}(A)$ ist definiert als $\mathfrak{X}(A) = xI_n - A \in K[x]^{n\times n}$.

Satz 4.12. *Sei $A \in K^{n\times n}$. Der Kern des $K[x]$-Modulepimorphismus*

$$f_A : K[x]^{n\times 1} = \mathrm{Fr}_{K[x]}(\underline{n}) \to M_A, f_A(e_i) := e_i$$

ist der Teilmodul $S(\mathfrak{X}(A)) \leq K[x]^{n\times 1}$, der frei auf den Spalten von $\mathfrak{X}(A)$ ist.

Beachten Sie: e_i hat in diesem Kontext zwei verschiedene Bedeutungen: Als Argument von f_A lebt e_i in $K[x]^{n\times 1}$ und bezeichnet die i-te Einheitsspalte in diesem freien $K[x]$-Modul. Als Wert von f_A lebt e_i in M_A und bezeichnet die i-te Einheitsspalte in $K^{n\times 1}$.

Beweis. Für $p = (p_1, \ldots, p_n)^{tr} \in K[x]^{n\times 1}$ ist

$$f_A(p) = f_A(\sum_{i=1}^{n} p_i e_i) = \sum_{i=1}^{n} p_i(A) \cdot f_A(e_i) = \sum_{i=1}^{n} p_i(A) e_i.$$

Insbesondere haben wir für alle $1 \leq j \leq n$:

$$f_A(xe_j) = Ae_j = A_{-j} \text{ und } f_A(e_j) = e_j$$

und somit $f_A(xe_j - A_{-j}) = f_A(xe_j - \sum_{i=1}^{n} A_{ij}e_i) = A_{-j} - A_{-j} = 0$. Somit ist der von den Spalten $xe_j - A_{-j}$ der charakteristischen Matrix erzeugte Teilmodul von $K[x]^{n\times 1}$ enthalten im Kern von f_A. Bezeichne $N_A := S(\mathfrak{X}(A))$ diesen Spaltenraum. Da N_A im Kern von f_A liegt, ist die Abbildung $\overline{f}_A : K[x]^{n\times 1}/N_A \to M_A$ wohldefiniert und wie die Ausgangsabbildung f_A ist auch $\overline{f}_A$ K-linear und surjektiv. Die K-Dimension von M_A ist n.
Behauptung: $(e_1+N_A, \ldots, e_n+N_A)$ ist ein K-Erzeugendensystem von $K[x]^{n\times 1}/N_A$. Dazu sei $p = (p_1, \ldots, p_n)^{tr} \in K[x]^{n\times 1}$. Wir zeigen durch Induktion über $\mathrm{Grad}(p) := \max\{\mathrm{Grad}(p_i) \mid 1 \leq i \leq n\}$ dass es ein $c \in K^{n\times 1}$ und ein $C \in N_A$ gibt mit $p = c + C$. Dies ist klar, falls $\mathrm{Grad}(p) = 0$, da dann schon $p = c \in K^{n\times 1}$. Ansonsten dividiere alle p_i mit $\mathrm{Grad}(p_i) = \mathrm{Grad}(p)$ sukzessive mit Rest durch $(x - A_{ii})$ und ersetze p durch $p - q_i\mathfrak{X}(A)_{-i}$. Da $\mathrm{Grad}(q_i) = \mathrm{Grad}(p_i) - 1$ ist, verringert sich der Grad von p danach um mindestens 1.
Also ist die K-Dimension von $K[x]^{n\times 1}/N_A$ höchstens n und somit $\overline{f}_A$ auch injektiv.
Dass N_A frei auf den Spalten von $\mathfrak{X}(A)$ ist, folgt da $\det(\mathfrak{X}(A)) = \chi_A \neq 0$. □

Folgerung 4.13. *Als $K[x]$-Modul ist M_A isomorph zu $K[x]^{n\times 1}/S(\mathfrak{X}(A))$. Nach dem Struktursatz 3.55 gibt es $\mathfrak{g}, \mathfrak{h} \in \mathrm{GL}_n(K[x])$ mit*

$$\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(f_1(x), \ldots, f_n(x))$$

so dass $f_i(x) \in K[x]$ normiert, $f_1(x) \mid f_2(x) \mid \ldots \mid f_n(x)$. Die $f_i(x)$ sind nach Satz 3.59 durch A eindeutig bestimmt (die Elementarteiler von $\mathfrak{X}(A)$). Es gilt $\chi_A = \det(\mathfrak{X}(A)) = \prod_{i=1}^{n} f_i(x)$, $\mu_A = f_n(x)$ und

$$M_A \cong_{K[x]} K[x]/\langle f_1(x)\rangle \oplus \ldots \oplus K[x]/\langle f_n(x)\rangle \cong M_F$$

mit $F = \mathrm{Diag}(M_{f_1}, \ldots, M_{f_n})$. Ist $d_i := \mathrm{Grad}(f_i)$ und $s = \min\{i \in \underline{n} \mid d_i > 0\}$, so ist A ähnlich zur Blockdiagonalmatrix

$$\mathrm{RKF}(A) := \mathrm{Diag}(M_{f_s}, \ldots, M_{f_n})$$

wo $M_{f_i} \in K^{d_i\times d_i}$ die Begleitmatrix von f_i bezeichnet (die leere Matrix, falls $d_i = 0$ ist). $\mathrm{RKF}(A)$ heißt **rationale kanonische Form** *oder auch* **Frobenius-Normalform** *von $A \in K^{n\times n}$.*

Bemerkung 4.14. Sei $\mathrm{RKF}(A) := \mathrm{Diag}(M_{f_s}, \ldots, M_{f_n})$. Dann ist M_A die direkte Summe von $n - s + 1$ zyklischen $K[x]$-Moduln $K[x]/(f_i)$. Jede andere solche Zerlegung von M_A hat mindestens ebensoviele zyklische Summanden. Ende Vorl. 18

Achtung: Im Gegensatz zur Hauptraumzerlegung ist die Zerlegung in Bemerkung 4.14 nur bis auf Isomorphie eindeutig:

Bemerkung 4.15. Die direkte Zerlegung in zyklische Summanden ist nicht eindeutig. Ist $\alpha = \widetilde{A}$ und sind B, B' Basen von $\mathcal{V} = K^{n\times 1}$ mit

$${}^{B}\alpha^{B} = \mathrm{Diag}(M_{f_s}, \ldots, M_{f_n}) = {}^{B'}\alpha^{B'}.$$

so ist der Endomorphismus $\beta \in \mathrm{End}(\mathcal{V})$ definiert durch $\beta(B_i) := B'_i$ für alle $1 \leq i \leq n = \mathrm{Dim}(\mathcal{V})$ eine Einheit im Zentralisator von α:

$$\beta \in C_{\mathrm{End}(\mathcal{V})}(\alpha)^* = C_{\mathrm{End}(\mathcal{V})}(\alpha) \cap \mathrm{GL}(\mathcal{V}) =: \mathrm{Aut}_\alpha(\mathcal{V}).$$

Folgerung 4.16. *Seien $A, B \in K^{n\times n}$. Äquivalent sind:*

1. *A und B sind ähnlich.*
2. *$\mathfrak{X}(A)$ und $\mathfrak{X}(B)$ sind ähnlich.*
3. *$\mathfrak{X}(A)$ und $\mathfrak{X}(B)$ sind äquivalent über $K[x]$.*
4. *M_A und M_B sind isomorphe $K[x]$-Moduln.*
5. *A und B haben dieselbe rationale kanonische Form.*

Durch eine Kombination von Hauptraumzerlegung und rationaler kanonischer Form erhält man die sogenannte primäre rationale Form einer Matrix A, mit der man M_A in die maximal mögliche Anzahl nicht-trivialer zyklischer $K[X]$-Moduln zerlegt. Diese hat den Vorteil, dass die Blockdiagonalmatrizen kleiner sind als bei der rationalen kanonischen Form.

Bemerkung 4.17. Sei $A \in K^{n\times n}$ mit Minimalpolynom $\mu_A = \prod_{i=1}^{\ell} p_i^{m_i}$, charakterisitischem Polynom $\chi_A = \prod_{i=1}^{\ell} p_i^{c_i}$ und $\mathcal{V}_i := \mathrm{Kern}(p_i^{m_i}(A))$ der p_i-Hauptraum. Dann ist $K^{n\times 1} = \bigoplus_{i=1}^{\ell} \mathcal{V}_i$ eine $\widetilde{A}$-invariante Zerlegung. Bezüglich einer an diese Zerlegung angepassten Basis hat $\widetilde{A}$ also eine Matrix $\mathrm{Diag}(A_1, \ldots, A_\ell)$ in Blockdiagonalgestalt. Ist $\mathrm{RKF}(A_i) = \mathrm{Diag}(M(p_i^{a_{i1}}), \ldots, M(p_i^{a_{is_i}}))$ die rationale kanonische Form von A_i (also $0 < a_1 \leq a_2 \leq \ldots \leq a_s$, $c_i = a_1 + \ldots + a_s$, $a_s = m_i$) so ist A ähnlich zu

$$\mathrm{PRF}(A) = \mathrm{Diag}(\mathrm{RKF}(A_1), \ldots, \mathrm{RKF}(A_\ell)) = \mathrm{Diag}(M_{p_1^{a_{11}}}, \ldots, M_{p_\ell^{a_{\ell s_\ell}}}).$$

$\mathrm{PRF}(A)$ heißt die **primäre rationale Form** oder **Weierstraß Form** von A.

Übung 4.5. Die a_{ij} lassen sich aus der Primfaktorzerlegung der Elementarteiler von $\mathfrak{X}(A)$ bestimmen.

Beispiel 4.18. Sei $K := \mathbb{Q}$ und

$$A := \begin{pmatrix} -6 & 6 & 0 & 6 \\ -4 & 6 & -1 & 3 \\ -6 & 12 & -3 & 3 \\ -6 & 12 & -3 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$$

Dann ist

$$\mathfrak{X}(A) = \begin{pmatrix} x+6 & -6 & 0 & -6 \\ 4 & x-6 & 1 & -3 \\ 6 & -12 & x+3 & -3 \\ 6 & -12 & 3 & x-3 \end{pmatrix} \in \mathbb{Q}[x]^{4\times 4}$$

und $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(1, 1, x, x^3)$, wobei

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/24x + 1/4 & -3/4 & 0 & 1/4 \\ 1/6x^2 - x - 4 & x + 12 & -4 & x \end{pmatrix}, \ \mathfrak{h} = \begin{pmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & -1 & 1/4x + 3 \\ -1/2 & 1 & x-3 & -1/4x^2 + 3/4x + 3 \\ -1/6 & 0 & 1 & 3/4x + 3 \end{pmatrix}.$$

Also erhält man

$$\mathrm{RKF}(A) = \mathrm{PRF}(A) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Beispiel 4.19. Sei

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 3}.$$

Dann findet man $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(1, 1, x^3 + x^2 - x - 1)$ wobei

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x & x^2 & 1 \end{pmatrix}, \ \mathfrak{h} = \begin{pmatrix} 0 & -1 & x+1 \\ 0 & 0 & 1 \\ -1 & -x & x^2+x-1 \end{pmatrix}$$

Also ist $p = x^3 + x^2 - x - 1 = \mu_A = \chi_A = (x+1)^2(x-1)$, $\mathrm{RKF}(A) = M_p$ und $\mathrm{PRF}(A) = \mathrm{Diag}(1, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix})$.

2.2 Trennende Invarianten

Definition 4.20.

1. Eine **Partition der natürlichen Zahl** c ist ein k-Tupel $a = (a_1, \ldots, a_k) \in \mathbb{N}^k$ für ein $k \in \mathbb{N}$ mit $a_1 \geq a_2 \geq \ldots \geq a_k$ und $a_1 + a_2 + \cdots + a_k = c$.
2. Ist $a = (a_1, \ldots, a_k) \in \mathbb{N}^k$ eine Partition von $c \in \mathbb{N}$, so ist die **konjugierte Partition** a' von a definiert durch $a'_i := |\{j | a_j \geq i\}|$.

Man visualisiert üblicherweise die Partition durch Kästchen, die man linksbündig in Zeilen untereinander anordnet mit a_i Kästchen in der i-ten Zeile. Dies nennt man das **Young-Diagramm** der Partition. Die YOUNG-Diagramme von a und a' sind transponiert zueinander.

Definition 4.21. Sei $\mathcal{V}$ ein K-Vektorraum und $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\chi_\alpha = p^c$, $p \in K[x]$ irreduzibel. Dann gibt es eine Basis B von $\mathcal{V}$ mit

$${}^B\alpha^B = \mathrm{Diag}(M_{p^{a_1}}, \ldots, M_{p^{a_k}})$$

für eine eindeutig durch α definierte Partition $(a_k, \ldots, a_1)$ von c. Diese Partition heißt die durch α definierte Partition.

Satz 4.22. *Sei $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\mu_\alpha = p^m$ mit $p \in K[x]$ irreduzibel. Setze $\nu := p(\alpha)$, $d := \mathrm{Grad}(p)$.*
Folgende Aussagen sind äquivalent:

1. *$\mathcal{V}$ ist zyklisch bezüglich α.*
2. *$\mathrm{Kern}(\nu)$ hat Dimension d über K.*
3. *ν hat Rang $\dim(\mathcal{V}) - d$.*
4. *$\mu_\alpha = \chi_\alpha$.*
5. *Sämtliche α-invarianten Teilräume von $\mathcal{V}$ sind gegeben durch*

$$\langle \nu^i(\mathcal{V}) \rangle_\alpha = \mathrm{Bild}(\nu^i)$$

für $i = 0, 1, \ldots m$.

Beweis. Zunächst eine allgemeine Vorbemerkung: Setze $\mathcal{V}_i := \mathrm{Bild}(\nu^i)$. Nach Definition des Minimalpolynoms ist $\mathcal{V}_{m-1} \neq \{0\}$ und $\mathcal{V}_m = \{0\}$. Weiter sind die $\mathcal{V}_i$ α-invariant, d.h. $\alpha(\mathcal{V}_i) \subseteq \mathcal{V}_i$. Es ist

$$(\star)\ \ \mathcal{V} = \mathcal{V}_0 > \mathcal{V}_1 > \ldots > \mathcal{V}_{m-1} > \mathcal{V}_m = \{0\}.$$

wobei die Faktoren $\mathcal{V}_i/\mathcal{V}_{i+1} = \nu(\mathcal{V}_{i-1}/\mathcal{V}_i)$ epimorphe Bilder voneinander sind, also

$$\mathrm{Dim}(\mathcal{V}_{m-1}) \leq \mathrm{Dim}(\mathcal{V}_i) - \mathrm{Dim}(\mathcal{V}_{i+1}) \leq \mathrm{Dim}(\mathcal{V}_{i-1}) - \mathrm{Dim}(\mathcal{V}_i) \leq \ldots \mathrm{Dim}(\mathcal{V}) - \mathrm{Dim}(\mathcal{V}_1) = \mathrm{Dim}(\mathrm{Kern}(\nu))$$

Das Minimalpolynom des von α auf $\mathcal{V}_i/\mathcal{V}_{i+1}$ induzierten Endomorphismus α_i ist $\mu_{\alpha_i} = p$. Insbesondere die Dimension $\mathrm{Dim}(\mathcal{V}_i/\mathcal{V}_{i+1})$ ein Vielfaches von d.
2. $\Leftrightarrow$ 3. folgt aus dem Homomorphiesatz.
Die Äquivalenz von 1. und 4. folgt aus dem Struktursatz für Moduln über Hauptidealbereichen .
4. $\Rightarrow$ 2.: Ist $\mu_\alpha = \chi_\alpha$, so ist $md = \mathrm{Grad}(\mu_\alpha) = \mathrm{Grad}(\chi_\alpha) = n$ und die echt absteigende Kette von Teilräumen oben hat Länge n/d. Damit muss aber $\mathrm{Dim}(\mathcal{V}_i) - \mathrm{Dim}(\mathcal{V}_{i+1}) = d$ sein für alle i, also auch $\mathrm{Dim}(\mathrm{Kern}(\nu)) = d$.
2. $\Rightarrow$ 4.: Ist $\mathrm{Dim}(\mathrm{Kern}(\nu)) = d$, so folgt $\mathrm{Dim}(\mathcal{V}_i) = \mathrm{Dim}(\mathcal{V}_{i+1}) + d$ für alle i und daher $m = n/d$.
1. $\Rightarrow$ 5.: Ist $\mathcal{W} \leq \mathcal{V}$ ein α-invarianter Teilraum, so gibt es ein größtes i mit $\mathcal{W} \leq \mathcal{V}_i$. Aber jedes $W \in \mathcal{W} \setminus \mathcal{V}_{i+1}$ erfüllt bereits $\langle W \rangle_\alpha = \mathcal{V}_i$, da auch $\mathcal{V}_i$ ein zyklischer Modul für α_i ist.
5. $\Rightarrow$ 1.: klar. □

Folgerung 4.23. *Seien α und p wie in Definition 4.21, $d := \mathrm{Grad}(p)$ und $a := (a_k, \ldots, a_1)$ die durch α definierte Partition. Sei $\mathcal{V}_i := \mathrm{Bild}(p(\alpha)^i)$ für $i = 0, \ldots, a_k$. Dann gilt*

$$\mathcal{V} = \mathcal{V}_0 > \mathcal{V}_1 > \ldots > \mathcal{V}_{a_k - 1} > \mathcal{V}_{a_k} = \{0\}$$

und $\dim(\mathcal{V}_i/\mathcal{V}_{i+1}) = a'_i d$, wobei a' die zu a konjugierte Partition ist.

Beweis. Wende Satz 4.22 auf jeden zyklischen Summanden an. □

Beispiel 4.24. Sie $p \in K[x]$ normiert, irreduzibel von Grad d und $A \in K^{5d \times 5d}$ mit $\mu_A = p^3$. Dann ist $\chi_A = p^5$ und man hat 2 Möglichkeiten für die Ähnlichkeitsklasse von A:

$$A \sim \mathrm{Diag}(M_p, M_p, M_{p^3}) \text{ oder } A \sim \mathrm{Diag}(M_{p^2}, M_{p^3})$$

Im ersten Fall ist $\dim(\mathrm{Kern}(p(A)) = 3d$ und im zweiten Fall gleich $2d$. Man kann also entscheiden, zu welcher Ähnlichkeitsklasse die Matrix A gehört, indem man nur den Rang von $\nu = p(A)$ berechnet.

Ende Vorl. 19

Es stellt sich abschließend die Frage nach trennenden Invarianten für die Konjugationsoperation.

Satz 4.25. *Zwei Endomorphismen $\alpha, \beta \in \mathrm{End}(\mathcal{V})$ sind genau dann unter $\mathrm{GL}(\mathcal{V})$ konjugiert, wenn gilt*

1. *die Minimalpolynome sind gleich: $\mu_\alpha(x) = \mu_\beta(x)$ und*
2. *für jeden normierten irreduziblen Teiler $p \in K[x]$ des Minimalpolynoms sind die Partitionen des p-Hauptraumes von $(\mathcal{V}, \alpha)$ und von $(\mathcal{V}, \beta)$ gleich.*

In anderen Worten: Das Minimalpolynom zusammen mit den Partitionen bilden ein System trennender Invarianten für die Ähnlichkeitsklassen.

Beispiel 4.26. Ähnlichkeitsklassen in $\mathbb{C}^{4\times 4}$: (in der Vorlesung nur 3x3)

$\chi_A(x)$	$\mu_A(x)$	Partitionen	Vertreter
$(x-a)^4$	$x-a$	$(1,1,1,1)$	$\mathrm{Diag}(a,a,a,a)$
	$(x-a)^2$	$(2,1,1)$	$\mathrm{Diag}(M((x-a)^2),a,a)$
	$(x-a)^2$	$(2,2)$	$\mathrm{Diag}(M((x-a)^2),M((x-a)^2))$
	$(x-a)^3$	$(3,1)$	$\mathrm{Diag}(M((x-a)^3),a)$
	$(x-a)^4$	(4)	$J_4(a)$
$(x-a)^3(x-b)$	$(x-a)(x-b)$	$(1,1,1),(1)$	$\mathrm{Diag}(a,a,a,b)$
	$(x-a)^2(x-b)$	$(2,1),(1)$	$\mathrm{Diag}(M((x-a)^2),a,b)$
	$(x-a)^3(x-b)$	$(3),(1)$	$\mathrm{Diag}(M((x-a)^3),b)$
$(x-a)^2(x-b)^2$	$(x-a)(x-b)$	$(1,1),(1,1)$	$\mathrm{Diag}(a,a,b,b)$
	$(x-a)^2(x-b)$	$(2),(1,1)$	$\mathrm{Diag}(M((x-a)^2),b,b)$
	$(x-a)^2(x-b)^2$	$(2),(2)$	$\mathrm{Diag}(M((x-a)^2),M((x-b)^2))$
$(x-a)^2(x-b)(x-c)$	$(x-a)(x-b)(x-c)$	$(1,1),(1),(1)$	$\mathrm{Diag}(a,a,b,c)$
	$(x-a)^2(x-b)(x-c)$	$(2),(1),(1)$	$\mathrm{Diag}(M((x-a)^2),b,c)$
$\prod_{w=a,b,c,d}(x-w)$	$\prod_{w=a,b,c,d}(x-w)$	$(1),(1),(1),(1)$	$\mathrm{Diag}(a,b,c,d)$

Übung 4.6. Gib ein Vertretersystem aller Konjugiertenklassen von Endomorphismen von $\mathbb{F}_2^{3\times 1}$ und von $\mathbb{R}^{3\times 1}$ an.

2.3 Die JORDAN Normalform

Aus der primären rationalen Form erhält man durch eine etwas andere Basiswahl leicht die JORDAN Normalform. Dazu genügt es, die zyklischen Moduln innerhalb eines Hauptraums zu behandeln.

Satz 4.27. *Sei $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\mu_\alpha = \chi_\alpha = p^m$ mit $p \in K[x]$ irreduzibel. Setze $\nu := p(\alpha)$, $d := \mathrm{Grad}(p)$.*
Jedes $V \in \mathcal{V} - \nu(\mathcal{V})$ liefert eine Basis

$$B := (\underbrace{V, \alpha(V), \ldots, \alpha^{d-1}(V)}, \underbrace{\nu(V), \alpha(\nu(V)), \ldots \alpha^{d-1}(\nu(V))}, \ldots, \underbrace{\nu^{m-1}(V), \ldots, \alpha^{d-1}(\nu^{m-1}(V))})$$

von $\mathcal{V}$, so dass die Matrix von α gegeben ist durch

$${}^B\alpha^B = J_m(p) := \begin{pmatrix} M_p & 0 & 0 & \ldots & 0 & 0 \\ N_d & M_p & 0 & \ldots & 0 & 0 \\ 0 & N_d & M_p & \ldots & 0 & 0 \\ 0 & 0 & N_d & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & N_d & M_p \end{pmatrix}$$

wobei $N_d = \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 0 & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & 0 \end{pmatrix} \in K^{d\times d}$.

Beweis. Nachrechnen. □

Folgerung 4.28. *Sei $A \in K^{n\times n}$ mit $\mathrm{PRF}(A) = \mathrm{Diag}(M_{p_1^{a_{11}}}, \ldots, M_{p_\ell^{a_{\ell s_\ell}}})$. Dann ist A ähnlich zu $\mathrm{JNF}(A) = \mathrm{Diag}(J_{a_{11}}(p_1), \ldots, J_{a_{\ell s_\ell}}(p_\ell))$. $\mathrm{JNF}(A)$ heißt die* **Jordan-Normalform** *von A.*

Im Beispiel 4.18 ist $\mathrm{RKF}(A) = \mathrm{PRF}(A) = \mathrm{JNF}(A)$. Im Beispiel 4.19 erhält man

$$\mathrm{JNF}(A) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -1 & 0 \\ 0 & 1 & -1 \end{array}\right)$$

2.4 Transformationsmatrizen

Bemerkung 4.29. (ohne Beweis) Sei $S = \mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(f_1, \ldots, f_n)$ die SMITH-Form von $\mathfrak{X}(A)$, wobei die f_i normiert seien. Seien $f_1 = \ldots = f_{s-1} = 1$ und $\mathrm{Grad}(f_i) = d_i \geq 1$ für alle $i \geq s$. Dann gilt $d_s + \ldots + d_n = n$. Für $i \geq s$ und $1 \leq j \leq n$ sei

$$\mathfrak{g}_{ij} \equiv c_{i,j,0} + c_{i,j,1}x + \ldots + c_{i,j,d_i-1}x^{d_i-1} \pmod{f_i}.$$

Setze

$$P_j^{(i)} := \begin{bmatrix} c_{i,j,0} \\ \vdots \\ c_{i,j,d_i-1} \end{bmatrix} \in K^{d_i}$$

und

$$P_j := \begin{bmatrix} P_j^{(s)} \\ \vdots \\ P_j^{(n)} \end{bmatrix} \in K^n.$$

Dann ist die Matrix $P = [P_1, \ldots, P_n] \in K^{n\times n}$ invertierbar und es gilt $PAP^{-1} = \mathrm{RKF}(A)$, wobei $\mathrm{RKF}(A)$ die rationale kanonische Form von A ist.

Beispiel 4.30. Ist A wie in Beispiel 4.19, so kann $\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x & x^2 & 1 \end{pmatrix}$ gewählt werden und es ergibt sich gemäß obiger Vorschrift

$$P := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

und erhält

$$PAP^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} = \mathrm{RKF}(A)$$

wie gewünscht.
Die Berechnung der SMITH-Form von $\mathfrak{X}(A)$ ist viel zu aufwendig. Eine Transformationsmatrix P erhält man einfacher durch direktes Rechnen mit Matrizen über K: Da $\mu_A = \chi_A$ gilt, ist $\mathbb{R}^{3\times 1}$ ein zyklischer Modul. Beginnt man mit $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $Ae_1 = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $A^2e_1 = Ae_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, so erhält man direkt eine Basis $B = (e_1, e_2, Ae_2)$ mit ${}^B\widetilde{A}^B = M_{\mu_A}$, in Matrizen $T := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ erfüllt $T^{-1}AT = M_{\mu_A}$.

Beispiel 4.31. Sei nun A wie in Beispiel 4.18, also $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(1, 1, x, x^3)$, wobei

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/24x + 1/4 & -3/4 & 0 & 1/4 \\ 1/6x^2 - x - 4 & x + 12 & -4 & x \end{pmatrix}.$$

Dann erhält man

$$P = \begin{pmatrix} 1/4 & -3/4 & 0 & 1/4 \\ -4 & 12 & -4 & 0 \\ -1 & 1 & 0 & 1 \\ 1/6 & 0 & 0 & 0 \end{pmatrix}$$

und berechnet $PAP^{-1} = \mathrm{Diag}(M_x, M_{x^3})$.

Diese Methode ist sehr aufwendig, da es i.a. nicht so leicht ist, die SMITH-Form der charakteristischen Matrix zu bestimmen. Dazu werden Rechnungen im Polynomring benötigt. Im folgenden wollen wir uns überlegen, wie wir eine geeignete Basis finden, so dass ${}^B\alpha^B$ in Normalform ist, wobei wir ab jetzt mit der JORDAN-Normalform arbeiten werden.

Beispiel 4.32. Sei $K := \mathbb{Q}$ und

$$A := \begin{pmatrix} -6 & 6 & 0 & 6 \\ -4 & 6 & -1 & 3 \\ -6 & 12 & -3 & 3 \\ -6 & 12 & -3 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$$

mit Minimalpolynom $\mu_A(x) = x^3$. Der erste Standardbasisvektor E_1 hat x^3 als Minimalpolynom:

$$(E_1, AE_1, A^2E_1) = \begin{pmatrix} 1 & -6 & -24 \\ 0 & -4 & -12 \\ 0 & -6 & -12 \\ 0 & -6 & -12 \end{pmatrix},$$

Es ist $\langle E_1\rangle_A = \langle E_1, E_2, E_3 + E_4\rangle$ (etwa mit Spalten-Gauß nachrechnen). Dieser Raum enthält also nicht E_3. Es ist $AE_3 = AE_1 - 1/4A^2E_1$ also setzen wir $F := 2E_1 - 1/2AE_1 - 2E_3 = (5, 2, 1, 3)^{tr}$ damit $AF = 0$ wird. Dann ist (E_1, AE_1, A^2E_1, F) eine Basis von $\mathbb{Q}^{4\times 1}$, bezüglich der $\widetilde{A}$ die Matrix $\mathrm{Diag}(M_{x^3}, M_x)$ bekommt.

Ende Vorl. 20

Unsere Aufgabe ist es, diese Normierung auf den Fall von mehr als zwei Summanden zu übertragen. Der Einfachheit halber nehmen wir an, dass $\mu_\alpha = (x-a)^m$ gilt, also nur ein Hauptraum vorliegt (die Zerlegung in Haupträume haben wir also schon erledigt) und (nur um das Verfahren klarer zu machen) dass der irreduzible Faktor Grad 1 hat.

Bemerkung 4.33. Algorithmus zur Bestimmung der Jordan-Normalform, der mit Kernen arbeitet
Sei $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\mu_\alpha = p^m = (x-a)^m$ und setze $\nu := p(\alpha) = \alpha - a\,\mathrm{id}_\mathcal{V}$. Sei $\mathcal{W}_i := \mathrm{Kern}(\nu^i)$. Dann ist

$$\mathcal{W}_0 = \{0\} < \underbrace{\mathcal{W}_1}_{=E_\alpha(a)} < \ldots < \mathcal{W}_{m-1} < \mathcal{W}_m = \mathcal{V}.$$

Vorbemerkungen: Für die Elemente $V \in \mathcal{W}_j \setminus \mathcal{W}_{j-1}$ gilt $\nu^j(V) = 0$, aber $\nu^{j-1}(V) \neq 0$. Außerdem ist $\nu : \mathcal{W}_j/\mathcal{W}_{j-1} \to \mathcal{W}_{j-1}/\mathcal{W}_{j-2}$ injektiv, da $\nu^{-1}(\mathcal{W}_{j-2}) \leq \mathcal{W}_{j-1}$ ist.

1. Ergänze eine Basis von $\mathcal{W}_{m-1}$ durch $V_1, \ldots, V_k$ zu einer Basis von $\mathcal{W}_m = \mathcal{V}$. Dann bilden die Restklassen $(V_1 + \mathcal{W}_{m-1}, \ldots, V_k + \mathcal{W}_{m-1})$ eine Basis von $\mathcal{W}_m/\mathcal{W}_{m-1}$. Da $\nu : \mathcal{W}_m/\mathcal{W}_{m-1} \to \mathcal{W}_{m-1}/\mathcal{W}_{m-2}$ injekitiv ist, sind auch $(\nu(V_1)+\mathcal{W}_{m-2}, \ldots, \nu(V_k)+\mathcal{W}_{m-2})$ linear unabhängig und man erhält induktiv, dass

$$B_m := (V_1, \nu(V_1), \ldots, \nu^{m-1}(V_1), V_2, \nu(V_2), \ldots, \nu^{m-1}(V_2), \ldots, V_k, \nu(V_k), \ldots, \nu^{m-1}(V_k))$$

eine Basis eines α-invarianten Teilraums ist mit ${}^{B_m}\alpha^{B_m} = \mathrm{Diag}(\underbrace{J_m(a), \ldots, J_m(a)}_{k})$.

2. Ergänze eine Basis von

$$\mathcal{W}_{m-2} \oplus \langle \nu(V_1), \ldots, \nu(V_k) \rangle \leq \mathcal{W}_{m-1}$$

durch Vektoren $W_1, \ldots, W_\ell$ zu einer Basis von $\mathcal{W}_{m-1}$. Die Zahl ℓ kann 0 sein.

$$B_{m-1} := (W_1, \nu(W_1), \ldots, \nu^{m-2}(W_1), W_2, \ldots, \nu^{m-2}(W_2), \ldots, W_\ell, \ldots, \nu^{m-2}(W_\ell))$$

ist dann eine Basis eines α-invarianten Teilraums,

$${}^{B_m, B_{m-1}}\alpha^{B_m, B_{m-1}} = \mathrm{Diag}(\underbrace{J_m(a), \ldots, J_m(a)}_{k}, \underbrace{J_{m-1}(a), \ldots, J_{m-1}(a)}_{\ell}).$$

3. Wiederhole 2. mit $m-1$ anstelle von m, dann mit $m-2$ etc..

Beispiel 4.34.

$$A := \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 2 & 0 & 2 \\ 1 & 2 & 2 & 1 \\ 2 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{4\times 4}$$

hat Minimalpolynom $\mu_A = (x-2)^3$. Es gilt

$$(A - 2I_4)^2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Der Rang ist 1, wir werden also den ersten JORDAN-Block aus dem zweiten Standardbasisvektor $V = E_2$ bekommen. $(A-2I_4)^2 V$ wird offenbar durch den dritten Standardbasisvektor $W = E_3$ zur Basis von $\mathcal{W} := \mathrm{Kern}(A - 2I_4) =: E_A(2)$ ergänzt. Also ist unsere neue Basis $B = (V, (A-2I_4)V, (A-2I_4)^2 V, W)$ und die transformierte Matrix ist

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \in \mathbb{F}_3^{4\times 4}.$$

2.5 Eine Anwendung: lineare Differentialgleichungssysteme.

In diesem Abschnitt wollen wir eine Anwendung der Jordan-Normalform sehen. Im Wesentlichen geht es um die Berechnung der Matrix-Exponentialfunktion.

Definition 4.35. Sei $A \in \mathbb{R}^{n\times n}$. Sind $u_i(t)$ reelle Funktionen so setze

$$u(t) := \begin{pmatrix} u_1(t) \\ \vdots \\ u_n(t) \end{pmatrix} \text{ und } u'(t) := \begin{pmatrix} u_1'(t) \\ \vdots \\ u_n'(t) \end{pmatrix}$$

Dann heißt

$$u'(t) = Au(t) \qquad (\star)$$

ein **lineares Differentialgleichungssystem** (mit konstanten Koeffizienten). Die **Lösungsmenge** von $(\star)$ ist

$$L(\star) = \{u(t) \mid u_i(t) \text{ reelle, differenzierbare Funktionen und } u'(t) = Au(t)\}.$$

Satz 4.36 (Aus der Analysis). *Sei $A \in \mathbb{R}^{n\times n}$. Dann ist die* **Exponentialreihe**

$$\exp(A) := \sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

konvergent und die Abbildung $\mathbb{R} \to \mathbb{R}^{n\times n}$, $t \mapsto \exp(tA)$ auf jedem beschränkten Intervall gleichmäßig stetig (bzgl. der Maximumsnorm $||A|| := \max\{|a_{ij}| \mid 1 \le i, j \le n\}$*).*

Bemerkung 4.37. Seien $A, B \in \mathbb{R}^{n\times n}$.

1. Aus $AB = BA$ folgt $\exp(A)\exp(B) = \exp(B)\exp(A) = \exp(A + B)$.
2. $\exp(0) = I_n$.
3. $\exp(A)$ ist invertierbar mit $\exp(A)^{-1} = \exp(-A)$.
4. $\frac{d}{dt}(\exp(tA)) = A\exp(tA) = \exp(tA)A$ für alle $t \in \mathbb{R}$.

Beweis. Wir zeigen 1: Sei $AB = BA$. Dann ist

$$\begin{aligned}&\exp(A + B) = \textstyle\sum_{k=0}^{\infty} \frac{1}{k!}(A + B)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} A^j B^{k-j} \\ &= \textstyle\sum_{j=0}^{\infty} \sum_{k=j}^{\infty} \frac{1}{j!} A^j \frac{1}{(k-j)!} B^{k-j} = \sum_{j=0}^{\infty} \sum_{m=0}^{\infty} \frac{1}{j!} A^j \frac{1}{m!} B^m = \exp(A)\exp(B)\end{aligned}$$

Behauptung 2 ist klar, 3 folgt direkt aus 1 und 2 und 4 ist durch gliedweises Differenzieren eine leichte Übung. □

Satz 4.38 (Aus der Analysis). *Sei $A \in \mathbb{R}^{n\times n}$. Das lineare Differentialgleichungssystem $u'(t) = Au(t)$ hat die Lösungsmenge $L = \{u : \mathbb{R} \to \mathbb{R}^n \mid u(t) = \exp(tA)c$ mit $c \in \mathbb{R}^n\}$. Die eindeutig bestimmte Lösung des Anfangswertproblems $u'(t) = Au(t), u(t_0) = u_0 \in \mathbb{R}^n$ ist $u(t) = \exp((t - t_0)A)u_0$.*

Diese Lösungsmenge L ist ein Vektorraum der Dimension n. Ist $(b_1, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$, so ist $(\exp(tA)b_1, \ldots, \exp(tA)b_n)$ eine Basis von L. Die Jordan-Normalform von A wird benutzt, um eine solche schöne Basis von L zu finden. Wir formulieren dies nur für zyklische Vektorräume und den Fall dass $\mu_A = \chi_A = (x - \lambda)^n$ ist. Der allgemeine Fall folgt durch einfaches Zusammensetzen.

Satz 4.39. *Sei $A \in \mathbb{R}^{n\times n}$, $\chi_A = \mu_A = (x - \lambda)^n$. Sei $b_1 \in \mathbb{R}^n$ ein zyklischer Vektor, also $b_2 := (A - \lambda I_n)b_1, \ldots, b_n := (A - \lambda I_n)^{n-1}b_1 \in \mathbb{R}^n \setminus \{0\}$ und $Ab_n = \lambda b_n$. Dann ist $(b_1, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$ und $(\exp(tA)b_1, \ldots, \exp(tA)b_n)$ eine Basis von L. Es gilt für $1 \le \ell \le n$ und alle $k \in \mathbb{N}$:*

$$A^k b_\ell = \sum_{j=0}^{n-\ell} \lambda^{k-j} \binom{k}{j} b_{j+\ell}$$

und

$$\exp(tA)b_\ell = \exp(\lambda t) \left(\sum_{j=0}^{n-\ell} \frac{t^j}{j!} b_{j+\ell} \right)$$

für alle $t \in \mathbb{R}$.

Beweis. Wir zeigen

$$A^k b_1 = \sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} b_{j+1}.$$

Die Aussage für $\ell > 1$ ergibt sich dann analog. Dazu wenden wir Induktion über k an. Für $k = 0$ liest sich die Behauptung als $b_1 = b_1$, da $\binom{k}{j} = 0$ für $j > k$. Der Induktionsschluss ist nicht schwerer:

$$\begin{aligned} A^{k+1} b_1 &= A \left(\sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} b_{j+1} \right) = \sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} (b_{j+2} + \lambda b_{j+1}) \\ &= \sum_{j=0}^{n-1} \lambda^{k-j+1} \binom{k}{j-1} b_{j+1} + \sum_{j=0}^{n-1} \lambda^{k-j+1} \binom{k}{j} b_{j+1} = \sum_{j=0}^{n-1} \lambda^{k-j+1} \left(\binom{k}{j-1} + \binom{k}{j} \right) b_{j+1} \\ &= \sum_{j=0}^{n-1} \lambda^{k+1-j} \binom{k+1}{j} b_{j+1}, \end{aligned}$$

wobei wir der Einfachheit halber $b_{n+1} := 0$ setzen. Mit dieser Formel gilt

$$\begin{aligned} \exp(tA) b_\ell &= \sum_{k=0}^{\infty} \frac{t^k}{k!} \sum_{j=0}^{n-\ell} \lambda^{k-j} \binom{k}{j} b_{j+\ell} = \sum_{k=0}^{\infty} \sum_{j=0}^{n-\ell} \frac{t^{k-j}}{(k-j)!} \lambda^{k-j} \frac{t^j}{j!} b_{j+\ell} \\ &= \exp(\lambda t) \left(\sum_{j=0}^{n-\ell} \frac{t^j}{j!} b_{j+\ell} \right). \end{aligned}$$

□

Beispiel 4.40. Gesucht ist die Lösungsmenge des Differentialgleichungssystems

$$\begin{aligned} u_1' &= -u_1 - u_2 - 3u_2' \\ u_2'' &= -u_2 - 2u_2' \end{aligned}$$

Um daraus ein DGL-System erster Ordnung zu machen, setzen wir $u_2' =: u_3$ und erhalten

$$\begin{aligned} u_1' &= -u_1 - u_2 - 3u_3 \\ u_2' &= u_3 \\ u_3' &= -u_2 - 2u_3 \end{aligned}$$

also $u' = Au$, wobei

$$A = \begin{pmatrix} -1 & -1 & -3 \\ 0 & 0 & 1 \\ 0 & -1 & -2 \end{pmatrix}$$

gilt. Das Minimalpolynom von A ist $(x+1)^3$, also ist -1 der einzige Eigenwert von A und A ist ähnlich zum Jordan-Block

$$J := \begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

Ende Vorl. 21

Der Kern von $(A+1)^2$ ist hier[1] gleich dem Bild von $A+1$ und

$$\mathrm{Kern}((A+1)^2) = \mathrm{Bild}(A+1) = \langle (1,0,0)^{tr}, (0,1,-1)^{tr} \rangle$$

[1] Da es genau einen Jordan-Block gibt, allgemeiner, da alle Jordan-Blöcke zum gegebenen Eigenwert gleich groß sind.

und enthält nicht den 2. Basisvektor. Wir bilden also

$$b_1 = (0,1,0)^{tr}, b_2 = (A+1)b_1 = (-1,1,-1)^{tr}, b_3 = (A+1)b_2 = (2,0,0)^{tr}$$

und erhalten mit

$$B = \begin{pmatrix} 0 & -1 & 2 \\ 1 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

dass $B^{-1}AB = J$ gilt. Die Lösungsmenge des DGL-Systems ergibt sich also als Erzeugnis von

$$\exp(tA)b_1 = \begin{pmatrix} \exp(-t)(t^2-t) \\ \exp(-t)(t+1) \\ \exp(-t)(-t) \end{pmatrix}, \exp(tA)b_2 = \begin{pmatrix} \exp(-t)(2t-1) \\ \exp(-t) \\ -\exp(-t) \end{pmatrix}, \exp(tA)b_3 = \begin{pmatrix} 2\exp(-t) \\ 0 \\ 0 \end{pmatrix}.$$

Kapitel 5

Gruppen und Operationen

1 Operationen von Gruppen auf Mengen.

1.1 Wiederholung und erste Beispiele

Eine Gruppe G ist eine Menge G mit einer Verknüpfung $\cdot : G \times G \to G$, die das Assoziativgesetz erfüllt, ein Einselement enthält und für jedes $g \in G$ ein inverses Element.

Die **Ordnung** der Gruppe G ist die Anzahl der Elemente der Menge G, also eine natürliche Zahl, falls G **endlich** ist und ∞ falls G nicht endlich ist.

Die Gruppe heißt **Abelsch**, falls zusätzlich das Kommutativgesetz gilt, also $gh = hg$ für alle $g, h \in G$.

Eine Gruppe G heißt **zyklisch**, falls es ein $g \in G$ gibt mit $G = \{g^z \mid z \in \mathbb{Z}\} =: \langle g \rangle$. Die **Ordnung eines Elementes** $g \in G$ ist die Ordnung der davon erzeugten zyklischen Gruppe: $\mathrm{ord}(g) := |\langle g \rangle|$. Die zyklische Gruppe der Ordnung n bezeichnen wir auch mit $C_n = (\mathbb{Z}/n\mathbb{Z}, +)$. Zyklische Gruppen sind Abelsch und nach dem Hauptsatz über endlich erzeugte Abelsche Gruppen ist jede e.e. Abelsche Gruppe das **direkte Produkt** zyklischer Gruppen.

Weitere Beispiele für Gruppen sind

- die symmetrische Gruppe

$$S_n := S_{\underline{n}} := \{\pi : \underline{n} \to \underline{n} \mid \pi \text{ bijektiv } \}$$

  mit $|S_n| = n!$,

- die volle lineare Gruppe eines Vektorraums $\mathrm{GL}(\mathcal{V})$,

- die Gruppe $\mathrm{GL}_n(R)$ der invertierbaren $n \times n$-Matrizen über einem (kommutativen) Ring R.

Definition 5.1 (Operation)**.** Die Gruppe G **operiert** auf der Menge M (von links), falls es eine Abbildung $G \times M \to M, (g, m) \mapsto gm$ gibt mit

- $1m = m$ für alle $m \in M$;

- $(gh)m = g(hm)$ für alle $m \in M$, $g, h \in G$.

Eine Menge M mit einer **Operation** von G nennt man auch G**-Menge**.

Bemerkung 5.2. Die Gruppe G operiere auf der Menge M. Die **Bahn** von $m \in M$ unter G ist definiert als die Teilmenge

$$Gm := \{gm \mid g \in G\} \subset M.$$

Die Menge aller **Bahnen** in M unter G bilden eine **Partition**[1]

$$G\backslash M = \{Gm \mid m \in M\}$$

auf M.

Beweis. Erinnerung: Eine Partition $\mathcal{P}$ ist eine Teilmenge $\mathcal{P} \subset \mathrm{Pot}(M)$ der Potenzmenge von M mit den Eigenschaften:

- $\emptyset \notin \mathcal{P}$.
- Für $X, Y \in \mathcal{P}$ gilt entweder $X = Y$ oder $X \cap Y = \emptyset$.
- $M = \bigcup_{X \in \mathcal{P}} X$.

Diese Eigenschaften sind nun für $G\backslash M$ zu überprüfen:

- $Gm \neq \emptyset$, da $m = 1m \in Gm$.
- Seien $Gm, Gn \in G\backslash M$. Angenommen $Gm \cap Gn \neq \emptyset$. Dann gibt es $x \in Gm \cap Gn$, also $x = gm = hn$ für geeignete $g, h \in G$. Dann ist aber

  $$m = g^{-1}x = g^{-1}(hn) = (g^{-1}h)n \in Gn$$

  und daher $Gm \subseteq Gn$, denn jedes $um \in Gm$ ist von der Form $um = (ug^{-1}h)n \in Gn$. Aus Symmetriegründen gilt dann auch $Gn \subseteq Gm$ also sind die beiden Bahnen gleich.

  Zwei Bahnen sind entweder gleich oder disjunkt.

- $M = \bigcup_{m \in M} Gm$, da die rechte Seite eine Teilmenge von M ist und umgekehrt jedes $m \in M$ in seiner Bahn Gm liegt und daher auch in der Vereinigung auf der rechten Seite. □

Folgerung 5.3. *G operiere auf M. Dann ist $\sim_G \subset M \times M$ definiert durch $a \sim_G b$ genau dann, wenn a und b in derselben Bahn liegen, also genau dann wenn ein $g \in G$ existiert mit $a = gb$ eine Äquivalenzrelation auf M ist.*

Definition 5.4. Sei G eine Gruppe.

1. $U \subseteq G$ heißt **Untergruppe** von G, kurz $U \leq G$, falls
   (a) $U \neq \emptyset$,
   (b) $g, h \in U$ impliziert $gh^{-1} \in U$.
2. G operiere auf der Menge M. Für $m \in M$ heißt

   $$\mathrm{Stab}_G(m) := \{g \in G | gm = m\}$$

   der **Stabilisator** von m in G.

Bemerkung 5.5. G operiere auf M.

1. Für $m \in M$ gilt $\mathrm{Stab}_G(m) \leq G$.
2. Ist $m \in M$ und $g \in G$, so gilt $\mathrm{Stab}_G(gm) = g\,\mathrm{Stab}_G(m)g^{-1}$.

[1] Nicht zu verwechseln mit dem Komplementzeichen!

Beweis.

1. $1m = m$ also ist $1 \in \mathrm{Stab}_G(m)$ und somit $\mathrm{Stab}_G(m) \neq \emptyset$. Sind $g, h \in \mathrm{Stab}_G(m)$, so gilt $hm = m$ und somit auch $h^{-1}m = h^{-1}(hm) = (h^{-1}h)m = 1m = m$ und ebenso
$$(gh^{-1})m = g(h^{-1}m) = gm = m \text{ also } gh^{-1} \in \mathrm{Stab}_G(m).$$
2. Es gilt $h \in \mathrm{Stab}_G(gm)$ genau dann, wenn $h(gm) = gm$, also $g^{-1}hgm = m$, d. h. $g^{-1}hg \in \mathrm{Stab}_G(m)$ oder äquivalent $h \in g\,\mathrm{Stab}_G(m)g^{-1}$. □

Bemerkung 5.6. Sei G eine beliebige Gruppe und $U \leq G$ eine Untergruppe. Dann operiert U auf G durch inverse Rechtsmultiplikation:
$$U \times G \to G, (u, g) \mapsto gu^{-1}$$
Die Bahnen heißen auch **Linksrestklassen** von U in G,
$$gU = \{gu^{-1} \mid u \in U\} = \{gu \mid u \in U\}$$
Die Menge der Linksrestklassen von G nach U bezeichnen wir mit G/U. Die Anzahl der Linksrestklassen von U in G heißt der **Index** $[G : U]$ von U in G.

Folgerung 5.7. *(**Lagrange**) Sei G eine endliche Gruppe und $U \leq G$. Dann teilt die Ordnung von U die Ordnung von G:*
$$|U| \mid |G|.$$
Der Quotient $\frac{|G|}{|U|}$ ist gleich dem Index von U in G.

Beweis. Die Abbildung $U \to gU, u \mapsto gu$ ist eine Bijektion. Also haben je zwei Restklassen aus der Partition G/U von G genau $|U|$ Elemente. Nun ist $G = g_1U \dot\cup g_2U \ldots \dot\cup g_sU$ mit $s = [G : U]$ und somit $|G| = \sum_{i=1}^{s} |g_iU| = s|U|$. □

Ende Vorl. 22

Definition 5.8. Die Operation der Gruppe G auf dem K-Vektorraum $\mathcal{V}$ heißt **linear**, falls für jedes $g \in G$ die Abbildung
$$\widehat{g} : \mathcal{V} \to \mathcal{V} : V \mapsto gV$$
linear ist.

Beispiel 5.9. Sei $M := \mathbb{F}_2^3$. Die symmetrische Gruppe $G = S_3$ operiert auf M durch $(\pi, (a_1, a_2, a_3)) \mapsto (a_{\pi^{-1}(1)}, a_{\pi^{-1}(2)}, a_{\pi^{-1}(3)})$.
Bahnen: $\{(0,0,0)\}$, $\{(1,1,1)\}$, $\{(1,0,0),(0,1,0),(0,0,1)\}$, $\{(1,1,0),(0,1,1),(1,0,1)\}$. Stabilisatoren: $\mathrm{Stab}_{S_3}((1,0,0)) = \left\{\mathrm{id}, \pi := \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 1 & 3 & 2 \\ \hline \end{array}\right\}$. $\mathrm{Stab}_{S_3}(1,1,1) = S_3$.

Diese Operation ist linear, z.B. ist bzgl. der Standardbasis S
$${}^S\widehat{\pi}^S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Bemerkung 5.10.

1. Operiert G auf der Menge M, so erhält man einen Gruppenhomomorphismus
$$G \to S_M, g \mapsto \widehat{g}.$$
Umgekehrt definiert jeder Gruppenhomomorphismus in S_M eine Operation auf M.

2. Operiert G linear auf dem Vektorraum $\mathcal{V}$, so liefert dies einen Gruppenhomomorphismus
$$G \to \mathrm{GL}(\mathcal{V}) \leq S_{\mathcal{V}}.$$
Umgekehrt definiert jeder Gruppenhomomorphismus in $\mathrm{GL}(\mathcal{V})$ eine lineare Operation auf M.

Definition 5.11. Die Operation von G auf M heißt

1. **transitiv**, falls M eine Bahn bildet, d. h. $M = Gm$ für ein $m \in M$ (und somit $M = Gm$ für jedes $m \in M$).
2. **regulär** oder **scharf transitiv**, falls sie transitiv ist und $\mathrm{Stab}_G(m) = \{1\}$ für ein und somit alle $m \in M$.
3. **treu**, falls $gm = m$ für alle $m \in M$ impliziert $g = 1$.

Satz 5.12. *Die Gruppe G operiere auf der Menge M. Folgende Aussagen sind äquivalent:*

1. *G operiert regulär auf M.*
2. *Zu je zwei $m, n \in M$ gibt es genau ein $g \in G$ mit $gm = n$. (Man ist versucht dieses $g \in G$ mit $\overrightarrow{mn}$ zu bezeichnen.)*
3. *Für jedes feste $m_0 \in M$ ist die Abbildung*
$$G \to M : g \mapsto gm_0$$
bijektiv.
4. *Es existiert ein $m_0 \in M$, so daß die Abbildung*
$$G \to M : g \mapsto gm_0$$
bijektiv ist.

Beweis.

1 $\Rightarrow$ 2: Wegen der Transitivität existiert ein $g \in G$ mit $gm = n$. Angenommen es gibt ein weiteres $h \in G$ mit $hm = n$. Dann ist $h^{-1}g \in \mathrm{Stab}_G(m) = \{1_G\}$, also $h = g$.

2 $\Rightarrow$ 3: Definiert ist die Abbildung immer. Sie ist surjektiv, da G transitiv operiert. Sie ist injektiv wegen der Eindeutigkeit in 2.

3 $\Rightarrow$ 4: Klar.

4 $\Rightarrow$ 1: $\mathrm{Stab}_G(m_0) = \{1_G\}$ wegen der Injektivität in 4. Wegen der Surjektivität in 4 ist die Operation auch transitiv. Ist $m \in M$ beliebig, so haben wir ein $g \in G$ mit $gm_0 = m$. Also $\mathrm{Stab}_G(m) = \mathrm{Stab}_G(gm_0) = g\,\mathrm{Stab}_G(m_0)g^{-1} = \{1_G\}$ □

Beispiel 5.13. Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum und $\mathcal{B}(\mathcal{V}) \subset \mathcal{V}^n$ die Menge der Basen von $\mathcal{V}$. Dann ist die Operation
$$\mathrm{GL}(\mathcal{V}) \times \mathcal{B}(\mathcal{V}) \to \mathcal{B}(\mathcal{V}) : (g, B) \mapsto gB := (g(B_1), \ldots, g(B_n))$$
regulär, da jede lineare Abbildung durch die Bilder einer Basis festgelegt ist.

Beispiel 5.14. Sei $M = \{x \in K^n \mid Ax = b\} \neq \emptyset$ die Lösungsmenge eines linearen GLS und $\mathcal{U} = \{x \in K^n \mid Ax = 0\}$ die Lösungsmenge des zugehörigen homogenen Systems. Dann ist $\mathcal{U}$ ein K-Vektorraum, also insbesondere eine Gruppe, die regulär auf M durch Addition operiert.

Bemerkung 5.15. Ist $\varphi : \mathcal{V} \to \mathcal{W}$ eine lineare Abbildung von K-Vektorräumen und $W \in \mathrm{Bild}(\varphi)$, so operiert $\mathrm{Kern}(\varphi)$ regulär auf der Faser $\varphi^{-1}(\{W\})$.
Dies haben wir schon bei den Lösungsmengen linearer Gleichungssysteme gesehen: Die Lösungsmenge des homogenen Systems ist ein Teilraum und operiert regulär auf der Lösungsmenge des inhomogenen Systems. Hat man eine partikuläre Lösung x_0 des inhomogenen Systems gefunden, so ist $\{x_0 + y \mid y \text{ Lösung des homogenen Systems}\}$ die Lösungsmenge des inhomogenen Systems. Die Beobachtung wird auch der Ausgangspunkt für die affine Geometrie sein.

1.2 Die Konjugationsoperation

Definition 5.16. Sei G eine Gruppe. Dann operiert G auf sich selbst durch **Konjugation**,

$$G \times G \to G, (g, m) \mapsto \kappa_g(m) := gmg^{-1}.$$

Die Bahnen unter dieser Operation heißen **Konjugiertenklassen**. Der Stabilisator von $m \in G$ wird auch als **Zentralisator** bezeichnet

$$C_G(m) = \{g \in G \mid gmg^{-1} = m\} = \{g \in G \mid gm = mg\}.$$

Bemerkung 5.17. Für $g \in G$ ist die Abbildung $\kappa_g : G \to G, m \mapsto gmg^{-1}$ ein bijektiver Gruppenhomomorphismus von G in sich selbst, also ein Gruppenautomorphismus mit $(\kappa_g)^{-1} = \kappa_{g^{-1}}$.

Übung 5.1.

1. Die Menge aller Gruppenautomorphismen von G bildet (zusammen mit der Komposition) eine Gruppe $\mathrm{Aut}(G)$.
2. Die Abbildung $\kappa : G \to \mathrm{Aut}(G), g \mapsto \kappa_g$ ist ein Gruppenhomomorphismus von G in ihre **Automorphismengruppe**.
3. Der Kern von κ ist das **Zentrum** $Z(G)$ von G:

$$Z(G) = \{g \in G \mid gh = hg \text{ für alle } h \in G\}.$$

Das Bild von κ wird auch mit $\mathrm{Inn}(G)$ bezeichnet und heißt die Gruppe der **inneren Automorphismen** von G.

Übung 5.2. Betrachte die Diedergruppe $D_8 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$ der Ordnung 8 als Symmetriegruppe eines Quadrats. Bestimme alle Untergruppen, Konjugierten, Zentrum, etc.

1.3 Parametrisierung aller transitiver G-Mengen.

Definition 5.18. (Ähnlichkeit von G-Mengen) Sei G eine Gruppe, M, N zwei G-Mengen. Eine Abbildung $\varphi : M \to N$ heißt G**-äquivariant**, genau dann, wenn $\varphi(gm) = g\varphi(m)$ für alle $g \in G, m \in M$.

M und N heißen **ähnlich**, falls es eine G-äquivariante Bijektion $\varphi : M \to N$ gibt (in Zeichen $M \cong_G N$). φ heißt auch eine **Ähnlichkeit** der G-Mengen M und N.

Beispiel 5.19. Sind $U \leq S \leq G$ Untergruppen von G, so ist die Abbildung $G/U \to G/S, gU \mapsto gS$ eine G-äquivariante Abblidung.

Satz 5.20. *Die Gruppe G operiere transitiv auf der Menge M, sei $m \in M$. Dann sind M und $G/\operatorname{Stab}_G(m)$ als G-Mengen ähnlich:*

$$\varphi : G/\operatorname{Stab}_G(m) \to M : g \operatorname{Stab}_G(m) \mapsto gm$$

ist eine G-Ähnlichkeit.

Beweis. Offenbar ist $\Phi : G \to M : g \mapsto gm$ eine surjektive G-äquivariante Abbildung, wobei G durch Linksmultiplikation auf sich operiert. Die Fasern dieser Abbildung sind gerade die Linksrestklassen von G nach $S := \operatorname{Stab}_G(m)$:

$$\Phi^{-1}(\{gm\}) = gS \qquad \text{für alle } g \in G.$$

Also (nach dem Homomorphiesatz für Mengen) faktorisiert Φ über G/S mit einer Bijektion

$$\varphi : G/S \to M : gS \mapsto gm,$$

die offensichtlich G-äquivariant ist. □

Folgerung 5.21. *Die Gruppe G operiere auf der Menge M. Sei $m \in M$ mit $|Gm| < \infty$. Dann gilt: Die* **Länge der Bahn** *ist gleich dem Index des Stabilisators:*

$$|Gm| = [G : \operatorname{Stab}_G(m)] \qquad (:= |G/\operatorname{Stab}_G(m)|).$$

Insbesondere, falls $|G| < \infty$, so gilt:

$$|Gm| = \frac{|G|}{|\operatorname{Stab}_G(m)|}.$$

Beispiel 5.22 (Bestimmung der Ordnung der **vollen linearen Gruppe**)**.** Sei $\mathbb{F}_q$ ein Körper mit $q = p^n$ Elementen. Es gilt

$$|\operatorname{GL}_n(\mathbb{F}_q)| = (q^n - 1) \cdot (q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}),$$

wobei

$$\operatorname{GL}(n, q) := \operatorname{GL}_n(\mathbb{F}_q) = \{X \in \mathbb{F}_q^{n \times n} \mid \det X \neq 0\}$$

mit $\mathbb{F}_q$ ein endlicher Körper mit q Elementen.

Beweis. $\operatorname{GL}(n, q)$ operiert transitiv auf $\mathbb{F}_q^{n \times 1} \backslash \{0\}$ mit Bahnlänge $q^n - 1$. Der Stabilisator von $(1, 0, \ldots, 0)^{tr} \in \mathbb{F}_q^{n \times 1}$ in $\operatorname{GL}(n, q)$ ist

$$\operatorname{Stab}_{\operatorname{GL}(n,q)}\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = \left\{ \begin{pmatrix} 1 & * \cdots * \\ 0 & \\ \vdots & X \\ 0 & \end{pmatrix} \mid * \in \mathbb{F}_q, X \in \operatorname{GL}(n-1, q) \right\}$$

und hat die Ordnung

$$|\operatorname{Stab}_{\operatorname{GL}(n,q)}(1, 0, \ldots, 0)^{tr}| = q^{n-1} \cdot |\operatorname{GL}(n-1, q)|.$$

Nach dem Hauptsatz 5.20 gilt also

$$|\operatorname{GL}(n, q)| = (q^n - 1) \cdot q^{n-1} \cdot |\operatorname{GL}(n-1, q)|.$$

Mit $|\operatorname{GL}(1, q)| = q - 1$ folgt die Behauptung durch Induktion. □

Übung 5.3. (**Gaußsche Binomialkoeffizienten**) Betrachte die Menge

$$\mathcal{U}(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q) := \{X \mid X \leq_{\mathbb{F}_q} \mathbb{F}_q^{n\times 1}\}$$

der $\mathbb{F}_q$-Teilräume von $\mathbb{F}_q^{n\times 1}$ bzw. die Teilmenge $\mathcal{U}_k(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q)$ der k-dimensionalen Teilräume von $\mathbb{F}_q^{n\times 1}$. Zeige:

$$|\mathcal{U}_k(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q)| = \frac{|\operatorname{GL}_n(\mathbb{F}_g)|}{|\operatorname{GL}_k(\mathbb{F}^q)| \cdot |\operatorname{GL}_{n-k}(\mathbb{F}^q)| \cdot q^{k(n-k)}} =: \begin{bmatrix} n \\ k \end{bmatrix}_q$$

Übung 5.4. $\operatorname{GL}_n(\mathbb{F}_q)$ operiert auf $\mathbb{F}_q^{n\times n}$ durch Konjugation. Die Bahnen sind die Ähnlichkeitsklassen von Matrizen, von denen wir eine Parametrisierung im vorherigen Kapitel kennengelernt haben. Der Stabilisator einer Matrix A ist $C_{\mathbb{F}_q^{n\times n}}(A)^*$, die Einheitengruppe des Zentralisators. Ihr Index gibt an, wieviele Matrizen zu A ähnlich sind. Der Fall $n = 2, p = 2$ kann man wie folgt zusammenfassen:

μ_A	χ_A	Vertreter	$\lvert C^*\rvert$	Anzahl
x	x^2	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	6	1
$x+1$	$(x+1)^2$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	6	1
x^2	x^2	$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$	2	3
$(x+1)^2$	$(x+1)^2$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2	3
$x(x+1)$	$x(x+1)$	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	1	6
x^2+x+1	x^2+x+1	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	3	2

Behandle den Fall $n = 3, p = 2$.

1.4 Anzahl der Bahnen des Stabilisators

Für unsere geometrischen Anwendungen der Gruppentheorie ist die folgende Bemerkung grundlegend.

Bemerkung 5.23. Die Gruppe G operiere auf den Menge M und N.

1. G operiert auf $M \times N$ durch

$$G \times (M \times N) \to M \times N : (g, (m, n)) \mapsto (gm, gn).$$

   Diese Operation heißt **diagonale Operation**.

2. Ist die Operation von G auf M transitiv, dann gibt es eine Bijektion zwischen der Menge der Bahnen von G auf $M \times N$ und der Menge der $\operatorname{Stab}_G(m)$-Bahnen auf N für jedes (feste) $m \in M$:

$$G\backslash(M \times N) \to N/\operatorname{Stab}_G(m) : G(m, n) \mapsto \operatorname{Stab}_G(m)n.$$

$$\boxed{G\backslash(M \times N) \xrightarrow{\sim} N/\operatorname{Stab}_G(m)}$$

Ende Vorl. 23

Beweis.

1. Übung.

2. Wir zeigen, daß diese Abbildung wohldefiniert ist:
   Wegen der Transitivität von G auf M ist jede Bahn von G auf $M \times N$ von der Form $G(m,n) = \{(gm, gn) | g \in G\}$. Gilt $G(m,n) = G(m,n')$ für ein $n' \in N$, so sind offenbar n und n' in derselben Bahn unter $\mathrm{Stab}_G(m)$. Also ist die Abbildung wohldefiniert.
   Offenbar ist die Abbildung surjektiv. Wir zeigen die Injektivität:
   $\mathrm{Stab}_G(m)n = \mathrm{Stab}_G(m)n'$ impliziert offenbar $G(m,n) = G(m,n')$. Also haben wir insgesamt eine Bijektion. □

Beispiel 5.24. Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum. Dann operiert $G := \mathrm{GL}(\mathcal{V})$ auf $\mathcal{V} \setminus \{0\}$ transitiv. Der Stabilisator eines $V \in \mathcal{V} \setminus \{0\}$ hat dann jedes Vielfache $\neq 0$ von V als Bahn, sowie die Menge aller Vektoren, die linear unabhängig von V sind. Die Bahnen von $\mathrm{GL}(\mathcal{V})$ auf $(\mathcal{V} \setminus \{0\}) \times (\mathcal{V} \setminus \{0\})$ sind also gegeben durch $\{(V, aV) \mid 0 \neq V \in \mathcal{V}\}, a \in K$ und $\{(V,W) \mid (V,W)$ linear unabhängig $.\}$.
In Matrizen: $\mathcal{V} = K^{n\times 1}$, $G = \mathrm{GL}(n,K)$, Operation durch Linksmultiplikation. Der Stabilisator des ersten Standardbasisvektors $E_1 := (I_n)_{-,1}$ ist

$$\mathrm{Stab}_G(E_1) := \left\{ \left(\begin{array}{c|c} 1 & a \\ \hline 0 & A \end{array} \right) | a \in K^{1\times(n-1)}, A \in \mathrm{GL}(n-1,K) \right\}$$

und hat die folgenden Bahnen auf $\mathcal{V}$:

$$\{aE_1\} \text{ mit } a \in K \setminus \{0\} \text{ und } \mathcal{V} \setminus \{aE_1 | a \in K\}.$$

Beispiel 5.25. Sei $\mathcal{V}$ ein endlich erzeugter K-Vektorraum. Dann operiert $G := \mathrm{GL}(\mathcal{V})$ auf dem Dualraum $\mathcal{V}^*$ linear und treu durch

$$G \times \mathcal{V}^* \to \mathcal{V}^* : (g, \varphi) \mapsto (g^{-1})^{tr}(\varphi) = \varphi \circ g^{-1}.$$

Der Stabilisator eines $\varphi \in \mathcal{V}^* \setminus \{0\}$ operiert auf jeder Faser $\varphi^{-1}(\{a\})$ mit $a \in K$, also auf jeder Restklasse nach $\mathrm{Kern}(\varphi)$. Das Studium der Operation von $\mathrm{Stab}_G(\varphi)$ auf $\varphi^{-1}(\{1\})$ heitßt affine Geometrie und wird uns noch ausführlich beschäftigen.
In Matrizen: $\mathcal{V} = K^{n\times 1}$, $G = \mathrm{GL}(n,K)$, die Operation auf $K^{1\times n}$, dem bekanntlich $\mathcal{V}^*$ entspricht, ist gegeben durch

$$G \times K^{1\times n} \to K^{1\times n} : (g, Z) \mapsto Zg^{-1}.$$

Der Stabilisator des letzten Standardbasisvektors $Z_n := (I_n)_{n,-}$ ist

$$\mathrm{Stab}_G(Z_n) := \left\{ \left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) | a \in K^{(n-1)\times 1}, A \in \mathrm{GL}(n-1,K) \right\}.$$

Die Operation dieser Gruppe auf

$$\left\{ \left(\frac{S}{1} \right) | S \in K^{(n-1)\times 1} \right\}$$

wird also affine Geometrie sein. Man beachte:

$$\left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) \left(\frac{S}{1} \right) = \left(\frac{AS + a}{1} \right).$$

2 Homomorphismen und Normalteiler

Definition 5.26. Seien G und H Gruppen. Eine Abbildung $\varphi : G \to H$ heißt ein **Gruppenhomomorphismus** genau dann wenn $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ für alle $g_1, g_2 \in G$.

Beispiel 5.27. G operiere auf M. Dann ist $\varphi : G \to S_M, g \mapsto (m \mapsto gm)$ ein Gruppenhomomorphismus.
Ist $M = \mathcal{V}$ ein K-Vektorraum, so ist die Operation genau dann linear, wenn das Bild dieses Gruppenhomomorphismus in der linearen Gruppe $\mathrm{GL}(\mathcal{V}) \leq S_{\mathcal{V}}$ liegt.

Satz 5.28. *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist $\mathrm{Bild}(\varphi) = \{\varphi(g) : g \in G\}$ eine Untergruppe von H und $K := \mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = 1\}$ eine Untergruppe von G. Es gilt sogar $gKg^{-1} = K$ für alle $g \in G$. Eine Untergruppe $U \leq G$ mit $gUg^{-1} = U$ für alle $g \in G$ heißt* **Normalteiler** *von G. Wir schreiben dann auch $U \trianglelefteq G$.*

Beweis. Für $n \in \mathrm{Kern}(\varphi)$, $g \in G$ ist

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$$

also auch $gng^{-1} \in \mathrm{Kern}(\varphi)$. □

Beispiel 5.29 (Konkrete Beispiele für Normalteiler)**.**

1. Ist G beliebige Gruppe, so sind $\{1\}$ und G Normalteiler von G. Man nennt sie **triviale Normalteiler**.

2. $\det : \mathrm{GL}(n, K) \to K^* := (K \setminus \{0\}, \cdot)$ ist ein Homomorphismus für jeden Körper K. Also ist sein Kern ein Normalteiler von $\mathrm{GL}(n, K)$. Dieser wird mit $\mathrm{SL}(n, K)$ bezeichnet und heißt **spezielle lineare Gruppe** vom Grad n.

3. : Sei $U \leq G$ eine Untergruppe von G. Dann ist $\mathrm{Core}(U) := \bigcap_{g \in G} gUg^{-1}$ der größte Normalteiler von G, der in U enthalten ist. Es gilt $\mathrm{Core}(U) = \mathrm{Kern}(G \to S_{G/U})$.

4. Ist G eine abelsche Gruppe (also $gh = hg$ für alle $g, h \in G$), so ist jede Untergruppe von G ein Normalteiler.

Bemerkung 5.30. Eine Untergruppe $N \leq G$ ist genau dann ein Normalteiler von G, wenn sie Vereinigung von Konjugiertenklassen ist.

Satz 5.31. *Sei N ein Normalteiler von G. Dann bildet die Menge der Restklassen $G/N = \{gN \mid g \in G\}$ eine Gruppe unter vertreterweiser Multiplikation*

$$G/N \times G/N \to G/N, (gN)(hN) := (gh)N.$$

Beweis. Es ist klar, dass wir eine Gruppe vorliegen haben, sobald die Verknüpfung wohldefiniert ist, da die Rechenregeln dann aus denen von G folgen.
Zur Wohldefiniertheit:
Sei $g' = gn \in gN$ und $h' = hm \in hN$. Dann gilt

$$(g'h')N = (gnhm)N = (gh)(h^{-1}nh)mN = (gh)N.$$ □

Normalteiler sind genau die Untergruppen N für die die Faktorgruppe G/N wieder eine Gruppe ist.

Bemerkung 5.32. Eine Untergruppe N ist genau dann ein Normalteiler von G, wenn $gN = Ng$ ist für alle $g \in G$. Insbesondere sind Untergruppen von Index 2 immer Normalteiler, denn es ist $G = N \cup gN = N \cup Ng$, also $gN = G \setminus N = Ng$.

Die Bausteine aller endlichen Gruppen sind die endlichen einfachen Gruppen, das sind die endlichen Gruppen, die nur sich selbst und $\{1\}$ als Normalteiler haben.

Hauptsatz 5.33. *(**Homomorphiesatz für Gruppen**)*

1. *Ist G Gruppe und $N \trianglelefteq G$ ein Normalteiler von G, dann bildet die Menge G/N der Restklassen von G nach N eine Gruppe mit vertreterweiser Multiplikation:*

$$gN \cdot hN := ghN \text{ für alle } g, h \in G$$

und der **natürliche Epimorphismus**

$$\nu = \nu_N : G \to G/N : g \mapsto gN$$

ist ein surjektiver Homomorphismus mit Kern N.

2. *Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so ist $\operatorname{Kern}\varphi$ ein Normalteiler von G und $\operatorname{Bild}\varphi$ eine Untergruppe von H. Weiter definiert*

$$\tilde{\varphi} : G/\operatorname{Kern}\varphi \to H : g \operatorname{Kern}\varphi \mapsto \varphi(g)$$

einen Monomorphismus und φ faktorisiert

$$\varphi = \tilde{\varphi} \circ \nu_{\operatorname{Kern}\varphi},$$

d. h. das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle \nu_{\operatorname{Kern}\varphi}}\searrow & & \nearrow{\scriptstyle \tilde{\varphi}} \\ & G/\operatorname{Kern}\varphi & \end{array}$$

kommutiert. Insbesondere sind $G/\operatorname{Kern}\varphi$ und $\operatorname{Bild}\varphi \leq H$ isomorph.

Beweis.

1. Diesen Teil haben wir bereits bewiesen in Satz 5.31.

2. Genauso wie im Homomorphiesatz für Mengen zeigt man, dass $\tilde{\varphi}$ wohldefiniert und injektiv ist. Es bleibt die Homomorphieeigenschaft von $\tilde{\varphi}$ zu überprüfen: Setze $N := \operatorname{Kern}\varphi$ und seien $g, h \in G$. Dann gilt:

$$\tilde{\varphi}(gNhN) = \varphi(gh) = \varphi(g)\varphi(h) = \tilde{\varphi}(gN)\tilde{\varphi}(hN).$$

Dass $\nu_{\operatorname{Kern}\varphi}$ ein Epimorphismus ist, wissen wir bereits. Die Komposition $\tilde{\varphi} \circ \nu_{\operatorname{Kern}\varphi} = \varphi$ rechnet man leicht nach. □

Satz 5.34. *(**Noetherscher Isomorphiesatz**) Sei N ein Normalteiler von G und $U \leq G$. Dann ist $UN \leq G$, und $N \cap U \trianglelefteq U$ und es gilt*

$$UN/N \cong U/U \cap N.$$

Beweis. Wegen $NU = UN$ folgt $UN \leq G$. Offenbar ist N auch ein Normalteiler von UN und somit

$$\mu : U \to UN/N : u \mapsto uN$$

ein Homomorphismus mit Kern $U \cap N$ und Bild UN/N. Die Behauptung folgt aus dem Homomorphiesatz. □

Definition 5.35. Eine Gruppe G heißt **semidirektes Produkt**, falls es einen Normalteiler $N \trianglelefteq G$ und eine Untergruppe $U \leq G$ gibt mit

1. $NU = G$ und
2. $N \cap U = \{1\}$.

In Zeichen $G = N \rtimes U$.

Beispiel 5.36.

$$\mathrm{Aff}_n(K) := \left\{ \left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) | a \in K^{n\times 1}, A \in \mathrm{GL}(n,K) \right\} = K^{n\times 1} \rtimes \mathrm{GL}_n(K)$$

Dabei ist $K^{n\times 1} = \left\{ \left(\begin{array}{c|c} I_n & a \\ \hline 0 & 1 \end{array} \right) \mid a \in K^{n\times 1} \right\}$ der Kern des Gruppenhomomorphismus

$$\mathrm{Aff}_n(K) \to \mathrm{GL}_n(K), \left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) \mapsto A$$

und $\mathrm{GL}_n(K)$ die Untergruppe $\mathrm{GL}_n(K) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 1 \end{array} \right) \leq \mathrm{Aff}_n(K)$.

Bemerkung 5.37. In einem semindirekten Produkt $G = N \rtimes U$ hat jedes Element eine eindeutige Darstellung als nu mit $n \in N$, $u \in U$. Es gilt

$$n_1u_1n_2u_2 = n_1(u_1n_2u_1^{-1})u_1u_2$$

Ende Vorl. 24

Kapitel 6

Geometrie

1 Affine Geometrie

1.1 Der affine Raum

In der affinen Geometrie hat man einen Punktraum, dessen Punkte in Bijektion zu einem Vektorraum stehen, welcher in bestimmter Weise auf dem Punktraum (durch Translationen oder Verschiebungen) operiert. Der wesentliche Unterschied zum Vektorraum besteht darin, dass kein Punkt (Nullpunkt) mehr ausgezeichnet ist. Begriffe wie Geraden, Ebenen etc. lassen sich leicht als sogenannte affine Unterräume definieren.

Definition 6.1. Sei $\mathcal{V}$ ein K-Vektorraum. Ein **affiner Raum** über $\mathcal{V}$ ist eine nicht leere Menge $\mathscr{A}$, genannt Punktmenge, auf der $\mathcal{V}$ regulär [1] operiert. Genauer ist ein affiner Raum ein Tripel $(\mathscr{A}, \mathcal{V}, \tau)$, wobei

$$\tau : \mathcal{V} \times \mathscr{A} \to \mathscr{A} : (V, P) \mapsto \tau_V(P)$$

eine reguläre Operation des Vektorraumes $\mathcal{V}$ auf dem Punktraum $\mathscr{A}$ ist. Die Abbildung $\tau_V : \mathscr{A} \to \mathscr{A}$ heißt die **Translation** um den Vektor V von $\mathscr{A}$. Der Vektorraum $\mathcal{V}$ wird auch als **Translationsraum** von $\mathscr{A}$ bezeichnet: $\mathcal{T}(\mathscr{A}) := \mathcal{V}$. (Bezeichnung: Oft schreiben wir $V+P$ oder $P+V$ anstatt $\tau_V(P)$. Diese Schreibweise soll nicht implizieren, dass $\mathscr{A} = \mathcal{V}$ ist.)

Jeder Vektorraum $\mathcal{V}$ ist ein affiner Raum mit Translationsraum $\mathcal{V}$. Das Modell $\mathscr{A} = \mathcal{V} = \mathcal{T}(\mathscr{A})$ hat den Nachteil, dass nicht zwischen den Punkten (Elementen von $\mathscr{A}$) und den Vektoren[2] unterschieden wird. Daher bevorzugen wir das folgende Modell:

Beispiel 6.2. (Standardbeispiel) Ist $\widetilde{\mathcal{V}}$ ein K-Vektorraum mit nicht verschwindender Linearform $\varphi : \widetilde{\mathcal{V}} \to K$. Setze $\mathcal{V} := \mathrm{Kern}(\varphi)$ und $\mathscr{A}(\varphi) := \varphi^{-1}(\{1\})$. Dann ist $(\mathscr{A}(\varphi), \mathcal{V}, \tau)$ mit

$$\tau : \mathcal{V} \times \mathscr{A}(\varphi) \to \mathscr{A}(\varphi) : (V, P) \mapsto V + P \text{ in } \widetilde{\mathcal{V}} \text{ gerechnet}$$

ein affiner Raum.
Wir setzen speziell für $\widetilde{\mathcal{V}} = K^{(n+1)\times 1}$ und $\varphi \in (K^{(n+1)\times 1})^*$ die Projektion auf die letzte Komponente:

$$\mathscr{A}_n(K) := \mathscr{A}(\varphi) = \left\{ \begin{pmatrix} X \\ 1 \end{pmatrix} | X \in K^{n\times 1} \right\}$$

und nennen ihn den n-dimensionalen affinen Standardraum. Genau genommen ist

$$\mathcal{T}(\mathscr{A}_n(K)) = \left\{ \begin{pmatrix} X \\ 0 \end{pmatrix} | X \in K^{n\times 1} \right\},$$

[1] Da $\mathcal{V}$ eine abelsche Gruppe ist, sind die Begriffe „reguläre Operation“ einerseits sowie „treue und transitive Operation“ andererseits äquivalent.

[2] vector (lat.): jemand, der trägt, zieht oder befördert

was wir aber mit dem Vektorraum $K^{n\times 1}$ identifizieren.

Bemerkung 6.3. Sei $\mathscr{A}$ ein affiner Raum über dem K-Vektorraum $\mathcal{V}$.

1. Für jeden Punkt $P_0 \in \mathscr{A}$ ist
$$\mathcal{V} \to \mathscr{A} : V \mapsto \tau_V(P_0)$$
eine Bijektion.

2. Für jedes Punktepaar $(P, Q) \in \mathscr{A}^2$ gibt es genau einen Vektor $V \in \mathcal{V}$ mit $\tau_V(P) = Q$. Bezeichnung: $V =: \overrightarrow{PQ}$.

Beweis. Spezialfall von Satz 5.12 □

Übung 6.1. Zeige für $P, Q, P', Q' \in \mathscr{A}$ gilt $\overrightarrow{PQ} = \overrightarrow{P'Q'}$ genau dann, wenn $\overrightarrow{PP'} = \overrightarrow{QQ'}$. (Hinweis: Skizze!)

Wir kommen zur Definition affiner Teilräume.

Definition 6.4. Sei $(\mathscr{A}, \mathcal{V}, \tau)$ affiner Raum über dem K-Vektorräum $\mathcal{V}$. $\mathscr{A}' \subseteq \mathscr{A}$ heißt **affiner Teilraum** von $\mathscr{A}$, falls ein Teilvektorraum $\mathcal{W} \leq \mathcal{V}$ existiert, so dass $(\mathscr{A}', \mathcal{W}, \tau_{|\mathcal{W}\times\mathscr{A}'})$ ein affiner Raum über $\mathcal{W}$ ist.

Bemerkung 6.5. Sei $\mathscr{A}$ affiner Raum über $\mathcal{V} := \mathcal{T}(\mathscr{A})$.

1. Der Translationsraum eines affinen Teilraums $\mathscr{A}'$ von $\mathscr{A}$ ist eindeutig bestimmt. $\mathcal{T}(\mathscr{A}') = \{\overrightarrow{PQ} \mid P, Q \in \mathscr{A}'\}$.

2. Zu jedem $\mathcal{W} \leq \mathcal{V}$ und jedem $P \in \mathscr{A}$ gibt es genau einen affinen Teilraum $\mathscr{A}'$ von $\mathscr{A}$ mit $P \in \mathscr{A}'$ und Translationsraum $\mathcal{T}(\mathscr{A}') = \mathcal{W}$, nämlich $P + \mathcal{W} = \mathcal{W} + P := \tau(\mathcal{W} \times \{P\})$, die Bahn von P unter $\mathcal{W}$.

Beweis.

1. Sofort aus 6.3.

2. Existenz: Verifiziere Eigenschaften für $P + \mathcal{W}$. Eindeutigkeit analog zu 1. □

Bemerkung 6.6. Der Schnitt affiner Teilräume eines affinen Raumes $\mathscr{A}$ ist entweder leer oder wieder ein affiner Teilraum.
Sind $\mathscr{A}_i$ $(i \in I)$ affine Teilräume von $\mathscr{A}$ und ist $P \in \cap_{i\in I}\mathscr{A}_i$, so ist
$$\cap_{i\in I}\mathscr{A}_i = P + \cap_{i\in I}\mathcal{T}(\mathscr{A}_i) = \{\tau_V(P) \mid V \in \cap_{i\in I}\mathcal{T}(\mathscr{A}_i)\}.$$

Ist $\emptyset \neq M \subset \mathscr{A}$ eine Teilmenge, so sei das **affine Erzeugnis** von M der kleinste affine Teilraum, der M enthält: $\langle M\rangle_a := \bigcap_{M\subset\mathcal{B}\leq\mathscr{A}} \mathcal{B}$.

Wie sieht das affine Erzeugnis einer zweipunktigen Teilmenge von $\mathscr{A}$ aus?

1.2 Affine Abbildungen

Nun kommen wir zur Definition affiner Abbildungen. Diese bilden einen ganz wesentlichen Bestandteil der Definition des affinen Raumes, weil wir sonst nicht wissen, wie wir vergleichen können. Es liefert auch eine neue Charakterisierung der affinen Teilräume: Die nicht leeren Fasern affiner Abbildungen werden die affinen Teilräume sein.

Definition 6.7. Seien $\mathscr{A}, \mathscr{A}'$ affine Räume über den K-Vektorräumen $\mathcal{V}, \mathcal{V}'$.
$f : \mathscr{A} \to \mathscr{A}'$ heißt **affine Abbildung**, falls eine lineare Abbildung $\overline{f} : \mathcal{V} \to \mathcal{V}'$ existiert mit $\overrightarrow{f(P)f(Q)} = \overline{f}(\overrightarrow{PQ})$ für alle $P, Q \in \mathscr{A}$. $\overline{f}$ heißt auch der **lineare Anteil** von f.

Bemerkung 6.8. Seien $\mathscr{A}, \mathscr{A}'$ affine Räume mit Translationsvektorraum $\mathcal{V} = \mathcal{T}(\mathscr{A})$ und $\mathcal{V}' = \mathcal{T}(\mathscr{A}')$. Sei $P_0 \in \mathscr{A}$ fest gewählt.

1. Jede affine Abbildung $f : \mathscr{A} \to \mathscr{A}'$ ist eindeutig festgelegt durch ihren linearen Anteil $\overline{f}$ und $f(P_0)$: Ist nämlich $f(P_0) =: Q_0 \in \mathscr{A}'$ so ist für $P \in \mathscr{A}$ und $V := \overrightarrow{P_0P} \in \mathcal{V}$ (so, dass $P = \tau_V(P_0)$)

$$\overrightarrow{Q_0 f(P)} = \overrightarrow{f(P_0)f(P)} = \overline{f}(V) \text{ also } f(P) = \tau_{\overline{f}(V)}(Q_0).$$

2. Für jeden Punkt $Q_0 \in \mathscr{A}'$ und jede lineare Abbildung $\varphi : \mathcal{V} \to \mathcal{V}'$ gibt es genau eine affine Abbildung $f : \mathscr{A} \to \mathscr{A}'$ mit $f(P_0) = Q_0$ und $\overline{f} = \varphi$.
Es ist f injektiv (surjektiv, bijektiv), genau dann wenn $\overline{f}$ injektiv (surjektiv, bijektiv) ist.

Übung 6.2. Translationen sind affine Abbildungen, deren linearer Anteil die Identität des Translationsraumes ist. Sie sind auch die einzigen affinen Abbildungen eines affinen Raumes in sich mit dieser Eigenschaft.

Beispiel 6.9. Affine Abbildungen von $\mathscr{A}_n(K)$. Wähle $P_0 = (0, \ldots, 0|1)^{tr} \in \mathscr{A}_n(K)$. Die affine Abbildung f mit linearem Anteil ${}^S\overline{f}^S = A$ (bzgl. der Standardbasis S von $\mathcal{T}(\mathscr{A}_n(K)) = K^{n\times 1}$) und $f(P_0) = Q_0 = (b_1, \ldots, b_n|1)^{tr}$ ist gegeben durch Matrixmultiplikation mit $\left(\begin{array}{c|c} A & b \\ \hline 0 & 1 \end{array}\right)$.

Satz 6.10.

1. *Kompositionen affiner Abbildungen sind affin: Sind $\mathscr{A}, \mathscr{A}', \mathscr{A}''$ affine Räume über K-Vektorräumen mit affinen Abbildungen $f : \mathscr{A} \to \mathscr{A}'$ und $f' : \mathscr{A}' \to \mathscr{A}''$, so ist $f' \circ f : \mathscr{A} \to \mathscr{A}''$ affin mit $\overline{f' \circ f} = \overline{f'} \circ \overline{f}$.*

2. *Ist $f : \mathscr{A} \to \mathscr{A}'$ affin und bijektiv, so ist $f^{-1} : \mathscr{A}' \to \mathscr{A}$ ebenfalls affin mit $\overline{f^{-1}} = \overline{f}^{-1}$. (Man sagt, f ist ein* **affiner Isomorphismus**.*) Insbesondere ist*

$$\mathrm{Aff}(\mathscr{A}) := \{f : \mathscr{A} \to \mathscr{A} | f \text{ affin und bijektiv } \}$$

eine Gruppe (Untergruppe von $S_{\mathscr{A}}$, der symmetrischen Gruppe von $\mathscr{A}$), genannt die **affine Gruppe** *von $\mathscr{A}$, und*

$$\mathrm{Aff}(\mathscr{A}) \to \mathrm{GL}(\mathcal{T}(\mathscr{A})) : f \mapsto \overline{f}$$

ein Homomorphismus von Gruppen.

3. *Ist $f : \mathscr{A} \to \mathscr{A}'$ affin und $\mathscr{A}''$ ein affiner Teilraum von $\mathscr{A}$, so ist $f(\mathscr{A}'')$ ein affiner Teilraum von $\mathscr{A}'$ mit $\mathcal{T}(f(\mathscr{A}'')) = \overline{f}(\mathcal{T}(\mathscr{A}''))$.*

4. *Ist $f : \mathscr{A} \to \mathscr{A}'$ affin und $\mathscr{A}''$ ein affiner Teilraum von $\mathscr{A}'$, so ist $f^{-1}(\mathscr{A}'')$ leer oder ein affiner Teilraum von $\mathscr{A}$ mit $\mathcal{T}(f^{-1}(\mathscr{A}'')) = \overline{f}^{-1}(\mathcal{T}(\mathscr{A}''))$.*

Beweis.

1. Für $P, Q \in \mathscr{A}$ ist

$$\overrightarrow{(f' \circ f)(P)(f' \circ f)(Q)} = \overrightarrow{f'(f(P))f'(f(Q))} =$$

$$\overline{f'}(\overrightarrow{f(P)f(Q)}) = (\overline{f'} \circ \overline{f})(\overrightarrow{PQ}).$$

2. Wegen der Identifikation von $\mathscr{A}$ mit $\mathcal{T}(\mathscr{A})$ und $\mathscr{A}'$ mit $\mathcal{T}(\mathscr{A}')$ ist klar, dass $\overline{f} : \mathcal{T}(\mathscr{A}) \to \mathcal{T}(\mathscr{A}')$ bijektiv ist. (Genauer Beweis: Übung!). Zeige nur noch

$$\overrightarrow{f^{-1}(P')f^{-1}(Q')} = \overline{f}^{-1}(\overrightarrow{P'Q'})$$

für alle $P', Q' \in \mathscr{A}'$. Dies ist aber äquivalent zu

$$\overline{f}(\overrightarrow{f^{-1}(P')f^{-1}(Q')}) = \overrightarrow{P'Q'}.$$

3. Übung.

4. Leicht mit 6.5 Teil 2. □

Wir können etwas unscharf sagen, dass affine Geometrie das Studium von Eigenschaften ist, welche unter affinen Isomorphismen erhalten bleiben, oder auch das Studium der Invarianten der affinen Gruppe bei diversen Operationen. Hier ein Anfang: Die Dimension.

Satz 6.11. *Zwei affine Räume $\mathscr{A}$ und $\mathscr{A}'$ über demselben Körper K sind genau dann affin isomorph, wenn $\operatorname{Dim}\mathcal{T}(\mathscr{A}) = \operatorname{Dim}\mathcal{T}(\mathscr{A}')$. Man nennt $\operatorname{Dim}\mathscr{A} := \operatorname{Dim}\mathcal{T}(\mathscr{A})$ die* **Dimension** *des affinen Raumes $\mathscr{A}$. Insbesondere ist $\mathscr{A}$ affin isomorph zu $\mathcal{A}_n(K)$ für $n = \operatorname{Dim}\mathscr{A}$. Ein affiner Isomorphismus $\mathscr{A} \to \mathcal{A}_n(K)$ heißt* **affines Koordinatensystem**.

Ende Vorl. 25

Die Idee des Koordinatensystems geht zurück auf DESCARTES,1596-1650, der hierdurch die Algebra und Analysis als Hilfsmittel der Geometrie zugänglich machte.

Beweis. Ist $f : \mathscr{A} \to \mathscr{A}'$ ein affiner Isomorphismus, so ist $\overline{f} : \mathcal{T}(\mathscr{A}) \to \mathcal{T}(\mathscr{A}')$ ein Vektorraumisomorphismus, also $\operatorname{Dim}\mathcal{T}(\mathscr{A}) = \operatorname{Dim}\mathcal{T}(\mathscr{A}')$. Umgekehrt, sei $\varphi : \mathcal{T}(\mathscr{A}) \to \mathcal{T}(\mathscr{A}')$ ein Vektorraumisomorphismus. Offenbar ist für jedes beliebige, fest gewählte $P_0 \in \mathscr{A}$ die Abbildung $\mathscr{A} \to \mathcal{T}(\mathscr{A}) : P \mapsto \overrightarrow{P_0P}$ ein affiner Isomorphismus (Beweis: Übung). Also erhält man durch Komposition einen affinen Isomorphismus von $\mathscr{A}$ auf $\mathscr{A}'$. (Man zeige als Übungsaufgabe: Dieser Isomorphismus ist gegeben durch $P \mapsto P'_0 + \varphi(\overrightarrow{P_0P})$, wo $P'_0 \in \mathscr{A}'$ beliebig, aber fest gewählt ist.) □

Somit ist die Dimension eine affine Invariante. Wir wollen uns ansehen, wie in den verschiedenen Modellen für affine Räume, die wir gesehen haben, die affinen Abbildungen aussehen und dargestellt werden.

Definition 6.12. Sei $\mathscr{A}$ ein affiner Raum über $\mathcal{T}(\mathscr{A}) = \mathcal{V}$ mit affinen Teilräumen $\mathscr{A}', \mathscr{A}''$.

1. Die Teilräume heißen **parallel**, falls $\mathcal{T}(\mathscr{A}') = \mathcal{T}(\mathscr{A}'')$.

2. Sie heißen **schwach parallel**, falls $\mathcal{T}(\mathscr{A}') \subseteq \mathcal{T}(\mathscr{A}'')$ oder $\mathcal{T}(\mathscr{A}'') \subseteq \mathcal{T}(\mathscr{A}')$.

3. Sie heißen **windschief**, falls $\mathscr{A}' \cap \mathscr{A}'' = \emptyset$ und $\mathcal{T}(\mathscr{A}'') \cap \mathcal{T}(\mathscr{A}') = \{0\}$.

Übung 6.3. Sei $\mathscr{A}$ ein affiner Raum über dem Vektorraum $\mathcal{V}$. Zeige, dass Parallelität eine Äquivalenzrelation auf der Menge aller affinen Teilräume von $\mathscr{A}$ ist. Zeige weiter, dass die Äquivalenzklasse mit zugehörigem Teilraum $\mathcal{W} \leq \mathcal{T}(\mathscr{A})$ wiederum einen affinen Raum $\mathscr{A}/\mathcal{W}$ bildet, und zwar mit Translationsraum $\mathcal{V}/\mathcal{W}$. Man nennt $\mathscr{A}/\mathcal{W}$ auch den Bahnenraum von $\mathscr{A}$ mod $\mathcal{W}$. (Beachte: $\mathcal{V}$ operiert zwar auch transitiv auf $\mathscr{A}/\mathcal{W}$, aber nicht treu, es sei denn $\mathcal{W} = \{0\}$.)

Übung 6.4. Ist $\mathscr{A}$ ein affiner Raum über dem K-Vektorraum $\mathcal{V}$, und sind $\mathcal{U}, \mathcal{W} \leq \mathcal{V}$ Teilräume, so gilt für die Abbildung

$$\varphi : \mathscr{A} \to \mathscr{A}/\mathcal{U} \times \mathscr{A}/\mathcal{W} : P \mapsto (P + \mathcal{U}, P + \mathcal{W}),$$

1. φ ist injektiv genau dann, wenn $\mathcal{U} \cap \mathcal{W} = \{0\}$.

2. φ ist surjektiv genau dann, wenn $\mathcal{U} + \mathcal{W} = \mathcal{V}$.

Bemerkung 6.13. Parallelität und schwache Parallelität von affinen Teilräumen bleiben unter affinen Abbildungen erhalten. Die Eigenschaft, windschief zu sein, bleibt unter injektiven affinen Abbildungen erhalten. Wie steht es mit Urbildern?

Beispiel 6.14. Sei $\widetilde{\mathcal{V}}, \varphi, \mathrm{Kern}(\varphi) = \mathcal{V}, \mathcal{A}(\varphi) = \varphi^{-1}(\{1\})$ wie in Beispiel 6.2. Entsprechend nehmen wir einen zweiten affinen Raum mit den Daten $\widetilde{\mathcal{W}}, \psi, \mathrm{Kern}(\psi) = \mathcal{W}, \mathcal{A}(\psi) = \psi^{-1}(\{1\})$. Dann ist eine affine Abbildung $f : \mathcal{A}(\varphi) \to \mathcal{A}(\psi)$ nichts anderes als die Einschränkung einer linearen Abbildung $\alpha : \widetilde{\mathcal{V}} \to \widetilde{\mathcal{W}}$, welche $\mathcal{A}(\varphi)$ in $\mathcal{A}(\psi)$ abbildet, d.h. für die $\psi \circ \alpha = \varphi$. Wir haben also das folgende kommutative Diagramm:

$$\begin{array}{ccc} \mathcal{A}(\varphi) & \stackrel{f}{\to} & \mathcal{A}(\psi) \\ \downarrow & & \downarrow \\ \widetilde{\mathcal{V}} & \stackrel{\alpha}{\to} & \widetilde{\mathcal{W}} \\ \varphi \downarrow & & \downarrow \psi \\ K & = & K \end{array}$$

Übung 6.5. α legt f eindeutig fest und umgekehrt.
Wichtiger Spezialfall: $\mathrm{Aff}(\mathcal{A}_n(K))$ kann mit der Matrixgruppe

$$\mathrm{Aff}_n(K) := \left\{ \left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array} \right) | a \in \mathrm{GL}_n(K), t \in K^{n \times 1} \right\} \leq \mathrm{GL}_{n+1}(K)$$

identifiziert werden, die durch Linksmultiplikation auf $\mathcal{A}_n(K)$ operiert (ähnliche Operationen!). Man beachte, dass $\mathrm{Aff}_n(K)$ schon als Stabilisator eines Kovektors als Untergruppe von $\mathrm{GL}_{n+1}(K)$ früher vorkam.

Bemerkung 6.15. In $\mathrm{Aff}_n(K)$ gelten:

$$\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} b & s \\ \hline 0 & 1 \end{array} \right) = \left(\begin{array}{c|c} ab & as + t \\ \hline 0 & 1 \end{array} \right)$$

$$\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array} \right)^{-1} = \left(\begin{array}{c|c} a^{-1} & -a^{-1}t \\ \hline 0 & 1 \end{array} \right)$$

und

$$\boxed{\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} I_n & s \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array} \right)^{-1} = \left(\begin{array}{c|c} I_n & as \\ \hline 0 & 1 \end{array} \right)}$$

Der Homomorphismus "linearen Anteil nehmen" ist gegeben durch

$$\mathrm{Aff}_n(K) \to \mathrm{GL}_n(K) : \left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array} \right) \mapsto a$$

1.3 Das Invarianzprinzip der affinen Geometrie

Bemerkung 6.16. $\mathrm{Aff}(\mathscr{A})$ operiert transitiv auf $\mathscr{A}$ und hat genau 2 Bahnen auf $\mathscr{A} \times \mathscr{A}$.

Beweis. $\mathcal{T}(\mathscr{A}) \leq \mathrm{Aff}(\mathscr{A})$ operiert regulär, also insbesondere transitiv auf $\mathscr{A}$, daher auch $\mathrm{Aff}(\mathscr{A})$. Ist $P_0 \in \mathscr{A}$, so ist der Stabilisator $\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})}(P_0)$ isomorph zu $\mathrm{GL}(\mathcal{T}(\mathscr{A}))$, vermöge der Abbildung

$$\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})}(P_0) \ni s \mapsto \left(\overline{s} : \overrightarrow{P_0P} \mapsto \overrightarrow{P_0 s(P)}\right) \in \mathrm{GL}(\mathcal{T}(\mathscr{A})).$$

Also hat $\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})}(P_0)$ zwei Bahnen auf $\mathscr{A}$, nämlich $\{P_0\}$ und $\mathscr{A} \setminus \{P_0\}$. □

In unserem Standardmodell $\mathscr{A}_n(K)$ kann man Œ annehmen, dass $P_0 = (0, ..., 0, 1)^{tr}$. Dann ist

$$\mathrm{Stab}_{\mathrm{Aff}_n(K)}(P_0) = \left\{ \left(\begin{array}{c|c} a & 0 \\ \hline 0 & 1 \end{array} \right) | a \in \mathrm{GL}_n(K) \right\} \cong \mathrm{GL}_n(K)$$

Bei der Operation auf Tripeln bekommen wir die ersten geometrischen Invarianten.

Definition 6.17.

1. $P \in \mathscr{A}^n$ heißt **affin unabhängig**, falls für jeden affinen Raum $\mathscr{A}'$ über K und jedes Tupel $Q \in (\mathscr{A}')^n$ eine affine Abbildung $f : \mathscr{A} \to \mathscr{A}'$ existiert, mit $f \circ P = Q$, d.h. $f(P_i) = Q_i$ für $i = 1, \ldots, n$. Ein maximal affin unabhängiges System P in $\mathscr{A}$ heißt auch **affine Basis** von $\mathscr{A}$.

2. $P \in \mathscr{A}^n$ heißt **kollinear** bzw. **komplanar**, falls $\mathrm{Dim}\langle P\rangle_a \leq 1$ bzw. ≤ 2 gilt.

Bemerkung 6.18. Für $P \in \mathscr{A}^n$ sind folgende Aussagen äquivalent:

1. P ist affin unabhängig.
2. $\mathrm{Dim}\langle P\rangle_a = n - 1$.
3. $(\overrightarrow{P_nP_1}, \ldots, \overrightarrow{P_nP_{n-1}}) \in \mathcal{T}(\mathscr{A})^{n-1}$ ist linear unabhängig.
4. Die affine Abbildung $\mathscr{A}_{n-1}(K) \to \langle P\rangle_a : \widetilde{E_i} := \left(\frac{E_i}{1}\right) \mapsto P_i, \widetilde{E_n} := \left(\frac{0}{1}\right) \mapsto P_n$ definiert einen affinen Isomorphismus.

Beweis.

1 ⇒ 4: Dass eine affine Abbildung vorliegt, ist klar. Aus Definition der affinen Unabhängigkeit bekommt man eine affine Abbildung $\mathscr{A} \to \mathscr{A}_{n-1}(K)$, die P_i auf $\widetilde{E_i}$ abbildet. Die Einschränkung dieser Abbildung auf $\langle P\rangle_a$ liefert die Inverse, d.h. es liegt ein affiner Isomorphismus vor.

4 ⇒ 2: Die Dimension ist eine Invariante für affine Isomorphismen.

2 ⇒ 3: Es gilt $\mathcal{T}(\langle P\rangle_a) = \langle \overrightarrow{P_nP_1}, \ldots, \overrightarrow{P_nP_{n-1}}\rangle$. Also $n-1 = \mathrm{Dim}\langle P\rangle_a = \mathrm{Dim}\langle \overrightarrow{P_nP_1}, \ldots, \overrightarrow{P_nP_{n-1}}\rangle$.

3 ⇒ 1: Sei $\mathscr{A}'$ irgendein affiner Raum über dem K-Vektorraum $\mathcal{V}'$ und $Q \in (\mathscr{A}')^n$. Es existiert eine lineare Abbildung $\varphi : \mathcal{V} \to \mathcal{V}'$ mit $\varphi(\overrightarrow{P_nP_i}) = \overrightarrow{Q_nQ_i}$ für $i = 1, \ldots, n-1$. Also gibt es genau eine affine Abbildung $f : \mathscr{A} \to \mathscr{A}'$ mit $\overline{f} = \varphi$ und $f(P_n) = Q_n$. Für diese gilt offenbar $f(P_i) = Q_i$ für $i = 1, \ldots, n$. □

Ende Vorl. 26

Bemerkung 6.19. Ist $\mathscr{A} = \varphi^{-1}(1)$ für $\varphi \in \widetilde{\mathcal{V}}^*$, so ist $P \in \mathscr{A}^n$ affin unabhängig genau dann wenn $P \in \widetilde{\mathcal{V}}^n$ linear unabhängig ist. Die affinen Basen von $\mathscr{A}$ sind also genau die Basen von $\widetilde{\mathcal{V}}$, die in $\mathscr{A}$ enthalten sind.

Sofort klar, etwa mit 3. aus Bemerkung 6.18, ist nun die folgende Bemerkung:

Bemerkung 6.20.

1. Affine Abhängigkeit von Tupeln bleibt erhalten unter beliebigen affinen Abbildungen.
2. Affine Unabhängigkeit bleibt unter injektiven affinen Abbildungen erhalten.

Satz 6.21. *Sei $\mathscr{A}$ ein affiner Raum über einem endlich erzeugten K-Vektorraum. Dann operiert $\mathrm{Aff}(\mathscr{A})$ regulär auf der Menge der affinen Basen von $\mathscr{A}$. Letztere bilden eine der Bahnen von $\mathrm{Aff}(\mathscr{A})$ auf $\mathscr{A}^{n+1}$, wo $n = \mathrm{Dim}\,\mathscr{A}$.*

Beweis. Sofort aus Satz 6.11 und Bemerkung 6.18. □

Satz 6.22.

1. *$\mathrm{Aff}(\mathscr{A})$ operiert transitiv auf der Menge $\mathscr{A}^3_{generisch}$ der affin unabhängigen Tripel in $\mathscr{A}^3$ (nicht entartete Dreiecke), falls $\mathrm{Dim}(\mathscr{A}) \geq 2$.*
2. *Eine trennende Invariante für die Operation von $\mathrm{Aff}(\mathscr{A})$ auf der Menge $\mathscr{A}^3_{spez} := \{P = (P_1, P_2, P_3) \in \mathscr{A}^3 | P_1 \neq P_2, P \text{ kollinear }\}$ ist das* **Teilverhältnis**. *Dabei ist das Teilverhältnis $\mathrm{TV}(P_1, P_2, P_3)$ definiert als das eindeutige $a \in K$ mit $\overrightarrow{P_1P_3} = a\overrightarrow{P_1P_2}$.*

Beweis.

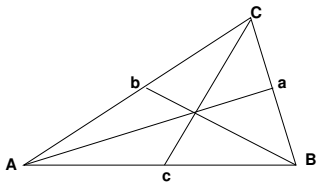
1. Wir können oBdA in $\mathscr{A} = \mathscr{A}(\varphi) \subset \widetilde{\mathcal{V}}$ arbeiten. Offenbar hat $\widetilde{\mathcal{V}}$ eine Basis $B \in \mathscr{A}^{n+1}$ und jedes affin unabhängige Tripel $P \in \mathscr{A}^3$ kann seinerseits zu einer Basis $\widehat{P} \in \mathscr{A}^{n+1}$ von $\widetilde{\mathcal{V}}$ ergänzt werden. Es genügt nun zu zeigen, dass ein $f \in \mathrm{Aff}(\mathscr{A})$ existiert, mit $f((B_1, B_2, B_3)) = P$. Dies ist aber klar, denn ein solches f wird induziert von der eindeutigen linearen Abbildung von $\widetilde{\mathcal{V}}$, die B auf $\widehat{P}$ abbildet.
2. Dass eine Invariante vorliegt, ist sofort klar aus der Definition einer affinen Abbildung. Um zu zeigen, dass sie die Bahnen trennt, gehen wir wieder von der Situation des Beweises von 1 aus mit der Basis B. Sei $P \in \mathscr{A}^3_{spez}$ mit Teilverhältnis $a \in K$. Es genügt zu zeigen, dass ein $f \in \mathrm{Aff}(\mathscr{A})$ existiert mit $f((B_1, B_2, B_1 + a(B_2 - B_1))) = P$. Zu diesem Zweck ergänzt man (P_1, P_2) zu einer Basis $\widehat{P} \in \mathscr{A}^{n+1}$ von $\widetilde{\mathcal{V}}$. Die lineare Abbildung, die B auf $\widehat{P}$ abbildet, induziert den gewünschten affinen Automorphismus. □

Aus dem letzten Beweis erhalten wir eine Folgerung, die eine sehr anschauliche Vorstellung von der affinen Gruppe liefert.

Folgerung 6.23. *Sei $\mathrm{Dim}(\mathscr{A}) = n$. Dann operiert $\mathrm{Aff}(\mathscr{A})$ transitiv auf $\mathscr{A}^k_{generisch} := \{P \in \mathscr{A}^k | P \text{ affin unabhängig}\}$, der Menge der affin unabhängigen k-Tupel ($(k-1)$-Simplizes) für $1 \leq k \leq n+1$. Im Falle $k = n+1$ ist der Stabilisator eines solchen Tupels trivial, d.h. in diesem Falle ist die Operation regulär, vgl. Satz 6.21.*

Wir wollen jetzt als Beispiel einen geometrischen Satz beweisen.

Satz 6.24. *Sei K ein Körper mit $6 \cdot 1 \neq 0$, $\mathscr{A}$ ein affiner Raum über K, $(A, B, C) \in \mathscr{A}^3_{gen}$. Dann schneiden sich die Seitenhalbierenden des nicht-entarteten Dreiecks (A, B, C) in einem Punkt S, so dass das Teilverhältnis $\mathrm{TV}(A, a, S) = 2/3$ ist, wo a der Mittelpunkt der Seite (C, B) ist.*



Beweis. Zunächst einmal definieren wir Seitenhalbierende:

$$s_a = \langle A, a\rangle_a, s_b = \langle B, b\rangle_a, s_c = \langle C, c\rangle_a$$

wobei $c = A + \frac{1}{2}\overrightarrow{AB}$, $a = B + \frac{1}{2}\overrightarrow{BC}$, $b = A + \frac{1}{2}\overrightarrow{AC}$. Um zu rechnen wählen wir Koordinaten für die Eckpunkte (A, B, C) des Dreiecks, also einen affinen Isomorphismus $f : \langle A, B, C\rangle_a \to \mathscr{A}_2(K)$ definiert durch

$$f(A) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},\ f(B) = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix},\ f(C) = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

Ein solcher Isomorphismus existiert, da (A, B, C) affin unabhängig ist. Es genügt den Satz für das Bild unter f zu zeigen, da die Aussage invariant ist unter affinen Isomorphismen. Dann ergeben sich die Fußpunkte $f(a) = f(B + \frac{1}{2}\overrightarrow{BC}) = (1, 1, 1)^{tr}$, $f(b) = (0, 1, 1)^{tr}$, $f(c) = (1, 0, 1)^{tr}$. Die Seitenhalbierenden sind dann

$$f(s_a) = \{f(A) + \alpha\overrightarrow{f}(\overrightarrow{Aa}) = \begin{pmatrix} \alpha \\ \alpha \\ 1 \end{pmatrix} \mid \alpha \in K\},\ f(s_b) = \{\begin{pmatrix} 2-2\beta \\ \beta \\ 1 \end{pmatrix} \mid \beta \in K\},$$

$$f(s_c) = \{\begin{pmatrix} \gamma \\ 2-2\gamma \\ 1 \end{pmatrix} \mid \gamma \in K\}$$

Um den Schnittpunkt $\{S\} = s_a \cap s_b \cap s_c$ zu berechnen, suchen wir $\alpha, \beta, \gamma \in K$ mit

$$\begin{pmatrix} \alpha \\ \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} 2-2\beta \\ \beta \\ 1 \end{pmatrix} = \begin{pmatrix} \gamma \\ 2-2\gamma \\ 1 \end{pmatrix}.$$

und finden als Lösung $\alpha = \beta = \gamma = 2/3$ also $f(S) = \begin{pmatrix} 2/3 \\ 2/3 \\ 1 \end{pmatrix}$. Das Teilverhältnis ergibt sich als $\mathrm{TV}(A, a, S) = \mathrm{TV}(f(A), f(a), f(S)) = 2/3 = \mathrm{TV}(B, b, S) = \mathrm{TV}(C, c, S)$. □

Zum Beweis des nächsten Satzes benötigen wir **Streckungen**, also affine Abbildungen der Form

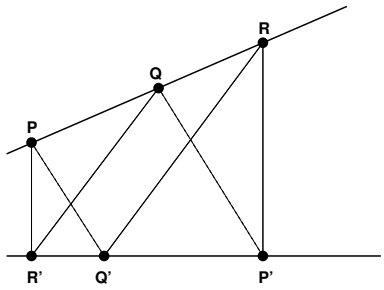
$$\mathscr{A} \to \mathscr{A} : P \mapsto P_0 + a\overrightarrow{P_0P},$$

wobei das feste $P_0 \in \mathscr{A}$ das Streckzentrum ist und das $a \in K^*$ der Streckfaktor.

Übung 6.6. Zeige: Je zwei Streckungen von $\mathscr{A}$ sind konjugiert in $\mathrm{Aff}(\mathscr{A})$ genau dann, wenn sie denselben Streckfaktor haben. Die Streckungen zusammen mit den Translationen bilden einen Normalteiler in $\mathrm{Aff}(\mathscr{A})$ isomorph zur Matrixgruppe

$$\left\{\left(\begin{array}{c|c} aI_n & t \\ \hline 0 & 1 \end{array}\right) | a \in K^*, t \in K^{n\times 1}\right\} \cong K^{n\times 1} \rtimes K^*$$

Satz 6.25. (PAPPOS) *Seien* $\mathrm{Dim}(\mathscr{A}) = 2$ *und* D, D' *zwei Geraden in* $\mathscr{A}$ *mit sechs verschiedenen Punkten* $P, Q, R \in D$, $P', Q', R' \in D'$, *von denen keiner in* $D \cap D'$ *liegt. Gilt* $\langle P, Q' \rangle_a \parallel \langle Q, P' \rangle_a$ *und* $\langle Q, R' \rangle_a \parallel \langle R, Q' \rangle_a$, *so folgt* $\langle P, R' \rangle_a \parallel \langle R, P' \rangle_a$.



Beweis. Wir betrachten zunächst den Fall, dass D und D' sich schneiden. Dann sei $\{P_0\} = D \cap D'$ und f_1 die Streckung mit Zentrum P_0, die P in $Q = P_0 + a\overrightarrow{P_0P}$ überführt, und f_2 die Streckung mit Zentrum P_0, die Q nach R überführt. Es ist $Q' = \tau_V(P)$, also $f_1(Q') = f_1(\tau_V(P)) = \tau_{aV}(f_1(P)) = \tau_{aV}(Q) = P'$ und ebenso $f_2(R') = Q'$. Dann ist $(f_2 \circ f_1)(P) = R$ und $(f_1 \circ f_2)(R') = P'$. Da der lineare Anteil von $f_2 \circ f_1$ gleich dem von $f_1 \circ f_2$ gleich $b\,\mathrm{id}_V$ ist (für ein $b \in K^*$), gilt $b\overrightarrow{PR'} = \overrightarrow{RP'}$ und somit $\langle P, R' \rangle_a \parallel \langle R, P' \rangle_a$.
Falls D und D' sich nicht schneiden, arbeitet man mit Translationen, denn dann sind D und D' parallel. □

Den Rest dieses Abschnitts werden wir nicht in der Vorlesung behandeln. Ende Vorl. 27

Den nächsten Satz kann man als weitgehende Verallgemeinerung einer Version des Strahlensatzes auffassen.

Satz 6.26. *Sei* $\mathrm{Dim}(\mathscr{A}) = n$ *und* H_i *für* $i = 1, 2, 3$ *Hyperebenen in* $\mathscr{A}$, *also affine Teilräume der Dimension* $n - 1$. H_1, H_2, H_3 *seien parallel und* $H_1 \neq H_2$.
1) Jede Gerade (= 1-dimensionaler affiner Teilraum von $\mathscr{A}$*), die nicht schwach parallel zu* H_1 *ist, hat genau einen Schnittpunkt mit* H_i *für* $i = 1, 2, 3$. *(Die Schnittpunkte sind offenbar kollinear.)*
2) Das Teilverhältnis der drei Schnittpunkte aus 1) ist unabhängig von der Wahl der Geraden und legt H_3 *auf Grund der Nebenbedingungen* $\mathrm{Dim}\, H_3 = n - 1, H_3 \parallel H_1$ *eindeutig fest.*

Beweis. 1. Beweis. Sei $\mathcal{W} := \mathcal{T}(H_1) = \mathcal{T}(H_2) = \mathcal{T}(H_3)$. Wir betrachten $\mathscr{A}/\mathcal{W} := \{P + \mathcal{W} | P \in \mathscr{A}\}$ als eindimensionalen affinen Raum und beachten, dass $\nu : \mathscr{A} \to \mathscr{A}/\mathcal{W} : P \mapsto P + \mathcal{W}$ eine affine Abbildung ist. Für jede Gerade G, wie in 1) spezifiziert, ist $\nu_{|G}$ ein affiner Isomorphismus. Klar: Die Schnittpunkte sind $\nu_{|G}^{-1}(H_i)$ und die Behauptung über die Teilverhältnisse folgt auch, da diese bei Anwendung von affinen Isomorphismen fest bleiben.
2. Beweis. Sei G eine Gerade wie in 1) angegeben. Dann gilt $\mathcal{T}(\mathscr{A}) = \mathcal{T}(H_1) \oplus \mathcal{T}(G)$. Entsprechend haben wir eine affine Abbildung, genauer eine **Parallelprojektion**, von $\mathscr{A}$ entlang $\mathcal{T}(H_1)$ auf G, nämlich

$$\pi : \mathscr{A} \to \mathscr{A} : P \mapsto P' \text{ mit } \{P'\} = (P + \mathcal{T}(H_1)) \cap G.$$

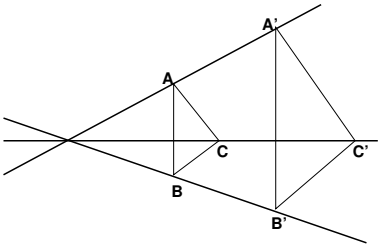
(Man muss nachrechnen, dass dies eine affine Abbildung ist. Die Projektionseigenschaft ist klar.) Jetzt kann der Beweis analog zum ersten Beweis fortgesetzt werden. □

Übung 6.7. Definiere Parallelprojektionen allgemein.

Übung 6.8. Zeige, dass in der affinen Ebene zwei Geraden sich entweder schneiden oder parallel sind. Genauer: Studiere die Bahnen unter der ebenen affinen Gruppe auf der Paarmenge der Geraden in der affinen Ebene.

Eigentlich ist der Satz von PAPPOS ein Satz, der zur projektiven Geometrie gehört. Ähnlich ist es mit dem Satz von DESARGUES, der sich im affinen Raum abspielt. Der Beweis, den ich geben werde, ist vielleicht vom synthetisch-geometrischen Standpunkt aus nicht schön, demonstriert aber die DESCARTESsche Idee, durch Einführung von Koordinaten geometrische Sätze durch algebraische Rechnungen zu beweisen. Für kompliziertere Situationen kann man sogar Computer heranziehen, um derartige Beweise "durchzurechnen".

Satz 6.27. *(*DESARGUES[3]*) Seien* $(A, B, C), (A', B', C') \in \mathscr{A}^3_{generisch}$ *zwei nicht entartete Dreiecke, die keine Eckpunkte gemeinsam haben und für die* $\langle A, B\rangle_a \parallel \langle A', B'\rangle_a$, $\langle B, C\rangle_a \parallel \langle B', C'\rangle_a$, $\langle A, C\rangle_a \parallel \langle A', C'\rangle_a$. *Dann schneiden sich die drei Geraden* $\langle A, A'\rangle_a$, $\langle B, B'\rangle_a$, $\langle C, C'\rangle_a$ *in einem gemeinsamen Punkt oder sind paarweise parallel.*



Beweis. Da die beiden Dreiecke nicht entartet sind, erzeugen sie einen drei- oder zweidimensionalen affinen Raum. Wir behandeln nur den ersten Fall, den zweiten überlasse ich als Übung:
OBdA ist (A, B, C, A') nicht komplanar. Dann können wir affine Koordinaten $\kappa : \langle A, B, C, A', B', C'\rangle_a \to \mathscr{A}_0(K^{3\times 1})$ so wählen (wir arbeiten hier nicht mit $\mathscr{A}_n(K)$, weil es uns nicht weiter hilft!), dass

$$\kappa(A) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \kappa(B) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \kappa(C) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \kappa(A') = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

ist. Wegen der Parallelität der Seiten folgt durch kurze Rechnung

$$\kappa(B') = \begin{pmatrix} a \\ 0 \\ 1 \end{pmatrix}, \kappa(C') = \begin{pmatrix} 0 \\ a \\ 1 \end{pmatrix}$$

für ein $a \in K$. Da (A', B', C') nicht kollinear ist, folgt $a \neq 0$. Im Falle $a = 1$ sind die drei Geraden $\langle A, A'\rangle_a, \langle B, B'\rangle_a, \langle C, C'\rangle_a$ parallel. Anderenfalls schneiden sie sich in dem Punkt mit den Koordinaten $(0, 0, \frac{1}{1-a})^{tr}$. □

[3]Genauer handelt es sich um eine affine Konsequenz der Umkehrung des (projektiven) Satzes von DESARGUES. Die Umkehrung ergibt sich aber durch Dualisieren aus dem ursprünglichen Satz von DESARGUES, wie noch gezeigt werden wird.

Literaturverzeichnis

Index