6.1.5 **Satz** (Jordansche Normalform)

Sei $A \in K^{n \times n}$ eine quadratische Matrix, deren charakteristisches Polynom

$$\chi_A(x) = \det(A - xE_n) \in K[x]$$

vollständig in Linearfaktoren zerfällt. Dann existiert eine Basis von K^n bezüglich der die lineare Abbildung A in Jordannormalform ist, d.h. $\exists S \in GL(n,K)$

$$A \sim SAS^{-1} = J = \begin{pmatrix} J(\lambda_1, \nu_1) & & \\ & \ddots & \\ & & J(\lambda_r, \nu_r) \end{pmatrix}$$

wobei $\lambda_1, \dots, \lambda_r$ die nicht notwendig von einander verschiedene Eigenwerte von A sind und

$$J(\lambda, \nu) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} \in K^{\nu \times \nu} \quad \text{ist.}$$

__Beweis__ Wir fassen $M = K^n$ als ein $K[x]$-Modul auf ~~d~~ auf dem x durch A operiert. Dann gilt für die Basis $e_i = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \leftarrow$ i-te Position

$xe_i = Ae_i$. Wählen wir $e_1, \dots, e_n$ als ein Erzeugendensystem von M $\quad 0 \leftarrow M \leftarrow K[x]^n \xleftarrow{(xE_n - A)} K[x]^n$

dann ist $(xE_n - A)$ die Matrix deren Spalten die Relationen ~~[illegible]~~ als $K[x]$-Modul der e_i beschreiben.

Die Matrix $xE - A$ lässt sich vermöge Zeilen und Spaltenoperation über $K[x]$ in Diagonalgestalt bringen.

$$(xE - A) \sim S(xE - A)T = B \qquad S, T \in GL(n, K[x])$$

$$B = \begin{pmatrix} f_1 & & 0 \\ & \ddots & \\ 0 & & f_n \end{pmatrix} \qquad \det(B) = u \cdot \det(xE - A), \; u \in K^* \text{ eine Einheit}$$

folgt $f_1, \dots, f_n$ zerfallen ebenfalls in Linearfaktoren und mit dem chinesischen Restsatz

$$M \cong \left(K[x]/(x-\lambda_1)^{\nu_1}\right) \oplus \dots \oplus \left(K[x]/(x-\lambda_r)^{\nu_r}\right)$$

$\frac{K[x]}{(x-\lambda)^\nu}$ hat die K-Vektorraumbasis
$$1, (x-\lambda), (x-\lambda)^2, \dots, (x-\lambda)^{\nu-1}$$
Bezüglich dieser Basis operiert $(x-\lambda)$ durch die Matrix

$$\begin{pmatrix} 0 & & & 0 \\ 1 & 0 & & \\ \vdots & 1 & \ddots & \\ \vdots & & \ddots & \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$ also $x = (x-\lambda)+\lambda$ operiert durch die Matrix $\begin{pmatrix} \lambda & & 0 \\ 1 & \ddots & \\ 0 & 1 & \lambda \end{pmatrix}$

Bzgl der Basis in der umgekehrten Reihenfolge
$$(x-\lambda)^{\nu-1}, \dots, (x-\lambda), 1$$
operiert x und damit A auf diesen Summanden von M vermöge
$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$$
Der Satz folgt. □

Wir haben jetzt verschiedene Darstellungen von Präsentationsmatrizen von Modul über Hauptidealringen kennengelernt. Die folgende Wahl ist kanonisch bis auf Einheiten.

6.16 **Satz + Def** (Elementarteilersatz) Sei R ein Hauptidealring und $A \in R^{m\times n}$ eine Präsentationsmatrix. Dann gibt es Matrizen $S \in GL(m,R)$, $T \in GL(n,R)$, sodass
$$SAT = \begin{array}{c} \\ \\ m-r \end{array} \left(\begin{array}{cc|c} d_1 & 0 & \\ & \ddots & 0 \\ 0 & d_r & \\ \hline 0 & & \underbrace{0}_{n-r} \end{array}\right)$$
sodass $d_1 | d_2 | d_3 | \dots | d_n$

Man nennt $d_1, \dots, d_r$ die Elementarteiler von A.

Beweis. Dass wir A in Diaggestalt bringen können
$$A \sim \left(\begin{array}{c|c} a_1 \cdots a_r & 0 \\ \hline 0 & 0 \end{array}\right)$$
haben wir schon gezeigt.

Für 2x2-Matrizen $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} a & b \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}$ wobei $d = ggT(a,b)$. Wegen $\det\begin{pmatrix} a & \\ & b \end{pmatrix} = ab \sim \det\begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix} = de$ und $ggT(a,b) \cdot kgV(a,b) = ab$ folgt $e \sim kgV(a,b)$. Insbesondere gilt $d | e$.

Wenden wir dies iterativ an, so erhalten wir schließlich

$$\left(\begin{array}{ccc|c} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \text{ mit } d_1 | d_2 | d_3 \dots | d_r$$

Bem: 1) Es gilt $d_1 \sim ggT(a_{11}, \dots, a_{mn})$

$A = d_1 A'$, $\quad f_1 = ggT(a_{11}', \dots, a_{mn}')$ so ergibt sich

$d_2 = d_1 f_1$ usw.

2) Eine andere Möglichkeit $d_1 | \dots | d_r$ zu bestimmen ist die Fittingideale

F_k = Ideal erzeugt von sämtlichen $k \times k$ Minoren zu bestimmen

$$R \supset F_1 \supset F_2 \supset \dots \supset F_r$$

Dann gilt, da SAT und A die gleichen Fittingideale haben (ohne Beweis) dass $F_1 = (d_1)$, $F_2 = (d_1 d_2)$, $\dots$, $F_r = (d_1 \cdots d_r)$

Beispiel: Betrachte $\begin{pmatrix} 2 & 6 & 8 \\ 3 & 1 & 2 \\ 9 & 5 & 4 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$

$F_1 = (1)$, $F_2 = (-14, -20, 4, -44, -64, -16, 6, -6, 6) = (2)$

$F_3 = (2(-6) - 6(-6) + 8 \cdot 6) = (6\ (-2 + 6 + 8)) = 2 \cdot 36$

$$A \sim \begin{pmatrix} 1 & & 0 \\ & 2 & \\ 0 & & 36 \end{pmatrix}$$

□

Um die Algorithmen in diesem Paragraphen anzuwenden, müssen wir die ggT's berechnen. Faktorisieren ist keine gute Idee.

6.17 Def Ein euklidischer Ring ist ein Paar (R, δ), wobei $\delta : R \setminus \{0\} \to \mathbb{N} = \mathbb{Z}_{\geq 0}$ und R Integritätsring sodass für jedes Element $a, b \in R \setminus \{0\}$ ein Quotient q und ein Rest r existiert $a = qb + r$, wobei $\delta(r) < \delta(b)$ oder $r = 0$

Beispiele 1) $(\mathbb{Z}, |\,|)$ ist euklidisch

2) $(K[x], \deg)$ K Körper "

3) $\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\} \subset \mathbb{C}$ ist ein euklidischer

Ring mit $\delta(m+in) = |m+in|^2 = m^2+n^2$

Beweis: $a, b \in \mathbb{Z}[i]$, $b \neq 0$

$$\frac{a}{b} = \frac{a\cdot\overline{b}}{|b|^2} \in \mathbb{Q}[i]$$

Wir wählen $x, y \in \mathbb{Z}$ mit $|\mathrm{Re}\,(\frac{a}{b}) - x| \leq 1/2$, $|\mathrm{Im}\,\frac{a}{b} - y| \leq \frac{1}{2}$.

Dann gilt: $\left|\frac{a}{b} - (x+iy)\right|^2 \leq \frac{1}{2}\sqrt{2} < 1$

Für $q = x+iy$ gilt dann

$$|r|^2 = |a-qb|^2 = \underbrace{\left|\frac{a}{b} - q\right|^2}_{\leq \frac{1}{2}} \cdot |b|^2 < |b|^2$$

Also $a = qb + r$ hat die gewünschte Eigenschaft.

6.18 Satz Euklidische Ringe sind Hauptidealringe.

Beweis Sei $I \subseteq R$ ein Ideal $\neq (0)$ und $b \in I \setminus \{0\}$ ein Element für das $\delta(b) \in \mathbb{N}$ minimal ist unter allen $\delta(a)$, $a \in I \setminus \{0\}$. Ist $a \in I$ und

$$a = qb + r \quad \text{mit } \delta(r) < \delta(b) \text{ oder } r = 0$$

so folgt $r \in I$ und daher $r = 0$ nach Wahl von b.
Also $I = (b)$

□

6.19 Erweiterter euklidischer Algorithmus

Input (R, δ) euklidischer Ring.
$a, b \in R \setminus \{0\}$

Output $d = ggT(a,b)$ und eine Darstellung
$d = ua + vb$ mit $u, v \in R$
(Bézout-Darstellung) u, v: Bézoutkoeffizienten.

```
1. Initialisierung
     $a_0 = a$     $u_0 = 1$     $u_1 = 0$
     $a_1 = b$     $v_0 = 0$     $v_1 = 1$     $n = 1$
2. Schleife while $a_n \neq 0$ do (
        Berechne $a_{n+1} = a_{n-1} - q_n a_n$ mit $\delta(a_{n+1}) < \delta(a_n)$
                                                  oder $a_{n+1} = 0$
```

2) $u_{n+1} = u_{n-1} - q_n u_n$ $\qquad n = n+1 \qquad)$

$v_{n+1} = v_{n-1} + q_n v_n$

3. Return $\ell = n-1$; $d = a_\ell$ und $u = u_\ell$, $v = v_\ell$

Beweis der Korrektheit

1) Terminierung: Da für $a_{n+1} \neq 0$ $\delta(a_{n+1}) < \delta(a_n)$ und die Werte in $\mathbb{Z}_{\geq 0}$ sind bricht das Verfahren ab mit

$a_\ell \neq 0$ und $a_{\ell+1} = 0$

2) a_ℓ ist der ggT(a, b).

- Sei $d = \text{ggT}(a,b)$ $\quad d \mid a_0,\ d \mid a_1 \Rightarrow d \mid a_2, \ldots d \mid a_n\ \forall n$ also insbesondere $d \mid a_\ell$. Umgekehrt, aus $a_{\ell+1} = 0$ folgt $a_\ell \mid a_{\ell-1} \Rightarrow a_\ell \mid a_{\ell-2}$ usw $a_\ell \mid a_1 = b$ und $a_\ell \mid a_0 = a$

$\text{ggT}(a,b) \mid a_\ell \mid \text{ggT}(a,b) \Rightarrow a_\ell \sim \text{ggT}(a,b)$

Gleich bis auf eine Einheit

3) Für die Bézout Darstellung zeigen wir, dass

$a_n = u_n\, a + v_n\, b \quad \forall\ n$ gilt.

Das ist richtig für $n=0$ und $n=1$

$$\begin{aligned} a_{n+1} &= a_{n-1} - q_n a_n \\ &\overset{IV}{=} (u_{n-1} a + v_{n-1} b) - q_n (u_n a + v_n b) \\ &= (u_{n-1} - q_n u_n) a + (v_{n-1} - q_n v_n) b \\ &= u_{n+1} a + v_{n+1} b \qquad \square \end{aligned}$$

Beispiel ggT(369, 192) = ?

n	a_n	q_n	u_n	v_n
0	369	–	1	0
1	192	1	0	1
2	177	1	1	-1
3	15	11	-1	2
4	12	1	12	23
5	3	4	-13	25
	0	–	64	-123

$369 = 3 \cdot 123$

$192 = 3 \cdot 64$

$3 = -13(369) + 25 \cdot 192$

$$\begin{pmatrix} 2&6&8\\ 3&1&2\\ 9&5&4 \end{pmatrix} \sim \begin{pmatrix} 1&3&2\\ 6&2&8\\ 5&9&4 \end{pmatrix} \sim \begin{pmatrix} 1&0&0\\ 6&-16&-4\\ 5&-6&-6 \end{pmatrix} \sim \begin{pmatrix} 1&0&0\\ 0&4&16\\ 0&6&6 \end{pmatrix} \sim \begin{pmatrix} 1&0&0\\ 0&4&0\\ 0&6&-18 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1&0&0\\ 0&2&*\\ 0&0&36 \end{pmatrix}$$

§ Körpererweiterungen

7.1 Def Eine Körpererweiterung ist eine Inklusion, ~~da~~ $K \subset L$ von zwei Körpern.

K heißt Unterkörper von L, L Oberkörper von K

L ist dann ein K-Vektorraum der Grad der Körpererweiterung

$$[L:K] = \dim_K L$$

Ist $[L:K] < \infty$, dann spricht man von einer endlichen Körpererweiterung

<u>Beispiele</u> $\mathbb{R} \subset \mathbb{C}$, $[\mathbb{C}:\mathbb{R}] = 2$

$[\mathbb{R}:\mathbb{Q}] = \infty$, da $\mathbb{R}$ überabzählbar ist

2) $\sqrt{2}$, $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$

$\shortparallel$

$2a+b\sqrt{2} \mid a,b \in \mathbb{Q}$

$[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = 2$.

7.2 <u>Satz</u> Seien K ~~und~~ $\subset L \subset M$ Körpererweiterungen

Dann gilt $[M:K] = [M:L] \cdot [L:K]$

<u>Beweis</u> Ist $[M,L] = \infty$ oder $[L:K] = \infty$ dann ist auch $[M:K] = \infty$. Sei also $[M,L] = n < \infty$, $[L:K] = m < \infty$ etwa $y_1, \dots, y_n \in M$ eine Basis von M als L-Vektorraum und $x_1, \dots, x_m \in L$ eine Basis von L als K-Vektorraum. Wir zeigen $x_i y_j$ bilden eine Basis von M.

<u>Erzeugung</u> Sei $z \in M$ dann ist $z = \cancel{\Sigma}\, c_1 y_1 + \dots + c_n y_n$ mit $c_i \in L$ und jedes c_i ist eine Linearkombination der x_j also $c_i = \sum_{j=1}^{n} c_{ij} x_j$

Also $z = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} x_j y_i$

Lineare Unabhängigkeit:

$$0 = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} c_{ij} x_j \right) y_i$$

Dann folgt aus Linearen Unabhängigkeit der y_i

$$0 = \sum_{j=1}^{m} c_{ij} x_j \quad \forall i$$

Unabhängigkeit von $x_1, \dots, x_n \in L$ über K gibt

$$c_{ij} = 0 \quad \forall i, j$$

□

7.3 **Def** Sei $K \subset L$ eine Körpererweiterung und $a \in L$. a heißt algebraisch über K, wenn a einer algebraischen Gleichung $a^n + c_1 a^{n-1} + \dots + c_n = 0$ genügt mit $c_1, \dots, c_n \in K$. Mit anderen Worten, wenn der Substitutionshomomorphismus $\varphi : K[x] \to L$

$$x \mapsto a$$

einen nicht trivialen Kern hat. Der normierte Erzeuger f von $\ker \varphi$ heißt das Minimalpolynom a über K. Ist $a \in L$ nicht algebraisch, dann nennt man a transzendent über K. Ist jedes Element von L algebraisch über K, dann nennt man $K \subset L$ eine algebraische Körpererweiterung.

7-4 **Satz** Sei $a \in L \supset K$ algebraisch über K. Dann ist

$$K[a] \cong K[x]/(f)$$, wobei f Minimalpolynom

ein Körper. Insbes. ist f irreduzibel.

Beweis: Angenommen $f = g \cdot h \Rightarrow 0 = f(a) = g(a) \cdot h(a) \in L$

$\Rightarrow g(a) = 0$ oder $h(a) = 0$, etwa $g(a) = 0$

Dann liegt $g \in \ker \varphi = (f)$

also $f | g | h \Rightarrow f \sim g$ gleich bis auf eine Einheit

$\Rightarrow h \in K^\times$ also f ist irreduziebel.

in Hauptidealringen erzeugen irreduzible Elemente maximale ideale

$$(f) \subset \mathfrak{M} = (g) \subsetneq K[x]$$

$g | f \Rightarrow (f) = (g)$ also (f) maximales Ideal

und deshalb $K[a] = K[x]/_{(f)}$ ein Körper

Beispiel: 1) $\sqrt{2} / \mathbb{Q}$ $f = x^2 - 2$ ist das Minimalpolynom da $\sqrt{2} \neq \mathbb{Q}$. $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(f)$ ein Körper.

2): p Primzahl, $\mathbb{Q}[\sqrt[n]{p}]$ ist ein Körper von Grad n über $\mathbb{Q}$ $x^n - p \in \ker \varphi \subset \mathbb{Q}[x]$ und ist irreduzibel nach Eisenstein

$\mathbb{Q}[\sqrt[n]{p}] \ni \mathbb{Q}[x]/_{(f)}$ hat als Basis $1, x, \dots, x^{n-1}$

7.5 Corollar $a \in L$ algebraisch über K und f sein Minimalpolynom. Dann gilt $[K[a] : K] = \deg f$.

Bew $1, x, .., x^{n-1}$, $n = \deg f$ werden aus einer Basis von $K[a] \cong K[x]/(f)$ abgebildet □

Bem. Für das Rechnen in $K[a] \cong \frac{K[x]}{(f)}$ reicht es f zu kennen. Um das Inverse in $g(a)$ zu bestimmen für $g \in K[x]$ polynom von $\deg g < \deg f$ zu bestimmen berechnen wir den ggT $(f, g) = 1$ und dessen Bezoutdarstellung

$$1 = uf + vg$$

$\Rightarrow v(a) \cdot g(a) = 1$ also $v(a) = g(a)^{-1}$ □

7.6 Satz Jede endliche Körpererweiterung $K \subset L$ ist algebraisch.

Bew $n = [L : K] < \infty$ und $a \in L$. Dann sind die Elemente $1, a, a^2, \dots, a^n$ linear abhängig über K, Eine normierte Abhängigkeitsrelation zeigt a ist algebraisch über K □

7.7 **Def** Sei $K \subset L$ eine Körpererweiterung und $a_1,\dots,a_n \in L$. Dann bezeichnet

$$K(a_1,\dots,a_n) \subset L$$

den kleinsten Unterkörper in L, der K und $a_1,\dots,a_n$ enthält, den von $a_1..a_n$ erzeugte Unterkörper. Erinnerung:

$K[a_1,\dots,a_n]$ ist das Bild von $k[x_1,\dots,x_n]$ unter dem Substitutionshomo $x_i \mapsto a_i$

Es gilt $K(a_1,\dots,a_n) \cong Q(K[a_1,\dots,a_n])$

in der Tat

$$\begin{tikzcd} k[a_1,\dots,a_n] \arrow[r, phantom, "\subset"] \arrow[d, phantom, "\cap"] & L \\ QK[a_1,\dots,a_n] \arrow[ur, bend right] & \end{tikzcd}$$

Also: $QK(a_1,\dots a_n)$ wird auf einen Unterkörper in L inj. abgebildet. Dieser ist der kleinste Körper der K ~~auch~~ und $a_1,\dots,a_n$ enthält.

Beispiel: $a \in L$ alg. über K dann $K[a]=K(a)$
ist $a \in L$ transzendent dann $K[a] \cong K[x]$ also kein Körper ist und $K[a] \subsetneq K(a) \cong Q(K[x])$

7.6 Satz $K \subset L$ Körpererweiterung, $a_1,\dots,a_n \in L$ algebraisch über K. Dann gilt

1) $K[a_1,\dots,a_n] = K(a_1,\dots,a_n)$ und

2) $[K[a_1,\dots,a_n] : K] < \infty$

Beweis: 1) Induktion nach n.

a_1 algebraisch $\Rightarrow K[a_1]=K(a_1)$ haben wir gesehen.

$$K[a_1,a_2] = K[a_1][a_2] \cong K(a_1)[a_2] \cong K(a_1)(a_2) = K(a_1,a_2)$$

Allgemeiner $K[a_1,\dots,a_i] = K(a_1,\dots,a_i)$ schon gezeigt

$$K[a_1,\dots a_i,a_{i+1}] = K[\ ][a_{i+1}] \cong K(a_1 \dots a_i)[a_{i+1}]$$
$$= K(a_1,\dots,a_{i+1})$$

Also $K[a_1,\dots a_n] \supset K[a_1\dots a_{n-1}] \supset \dots \supset K[a_1] \supset K$
ist ein Turm von endlichen Körpererweiterungen und damit eine

endliche Körpererweiterung vom Grad

$$\prod_{i=1}^{n} [K[a_1,\dots,a_i] : K[a_1,\dots,a_{i-1}]]$$

7.8 Satz (Turmsatz) $K \subset L \subset M$ Körpererweiterungen, $M \supset K$ ist algebraisch genau dann, wenn $L \subset M$ und $K \subset L$ algebraische Körpererweiterungen sind.

Beweis: „$\Rightarrow$" trivial

„$\Leftarrow$" Sei $z \in M$, z algebraisch über L

$\Rightarrow \exists\ z^n + c_1 z^{n-1} + \dots + c_n = 0$ mit $c_i \in L$

$\Rightarrow z$ ist algebraisch über $K[c_1,\dots,c_n]$. Also z ist in der endlichen Körpererweiterung $K \subset K[c_1,\dots,c_n,z]$ enthalten also z ist algebraisch über K □

7.8 Def und Satz Sei $K \subset L$ eine Körpererweiterung. Dann ~~heißt~~

$$\overline{K}^L = \{a \in L \mid a \text{ ist algebraisch über } K\}$$

algebraischer Abschluss von K in L. Dies ist ein Unterkörper.

Beweis $a, b \in \overline{K}^L \Rightarrow a+b, a\cdot b, \frac{a}{b} \in K[a,b]$ also $\overline{K}^L$ ist ein Körper □

Ein Körper L heißt algebraisch abgeschlossen, wenn jedes nicht konstante Polynom $f \in L[x]$ eine Nullstelle in L hat.

Äquivalent, wenn jedes nicht konstante Polynom f in Linearfaktoren in $L[x]$ zerfällt.

Fundamentalsatz der Algebra. $\mathbb{C}$ ist ein algebraisch abgeschlossener Körper (ein Satz aus der Funktionentheorie)

7.10 Satz Sei $K \subset L$ eine Körpererweiterung, ~~wobei~~ und L ein algebraisch abgeschlossener Körper. Dann ist auch $\overline{K}^L$ ein algebraisch abgeschlossener

Körper.

Beispiel $\overline{\mathbb{Q}} = \overline{\mathbb{Q}}^{\mathbb{C}}$ ist algebraisch abgeschlossen

$\{a \in \mathbb{C} \mid a$ ist algebraisch über $\mathbb{Q}\}$

Satz (Cantor) $\overline{\mathbb{Q}}$ ist abzählbar. Insbesondere gibt es transzendente Zahlen in $\mathbb{R}$ und $\mathbb{C}$ da $\mathbb{R}$ überabzählbar ist.

Beweis: ~~Sei~~ $\mathbb{Q}[x] = \bigcup_{n=0}^{\infty} \underbrace{\{f \in \mathbb{Q}[x] \mid \deg f = n\}}_{\cong \mathbb{Q}^{n+1}}$

ist als abzählbare Vereinigung von abzählbaren Mengen abzählbar.

$\overline{\mathbb{Q}} = \bigcup_{f \in \mathbb{Q}[x]} \{a$ Nullstelle von $f\}$ eine abzählbare Vereinigung von endlichen Mengen, also auch abzählbar.