# Skript
# Algebra I

WS 2003/04 bei Prof. Zink

Ewald Stamp <stamp@mathematik.hu-berlin.de>

VL-Stand: 16. Februar 2004
Letzte Änderung: 9. März 2008

# Inhaltsverzeichnis

# Kapitel 1

# Ringe

## 1.1 Definition & Grundlagen

*1. Vorlesung vom 20.10.2003*

**1.1.1 Definition** (Ring). *Ein* Ring $R$ *ist eine Menge mit 2 Operationen:*

$$+\colon R \times R \xrightarrow{+} R, \quad (a,b) \mapsto a+b \in R$$
$$\cdot\colon R \times R \xrightarrow{\cdot} R, \quad (a,b) \mapsto a \cdot b \in R$$

*und den Eigenschaften:*

*(i)* $(R,+)$ *soll* kommutative Gruppe *sein*
*neutrales Element:* $0_R = 0$
*inverses Element:* $a \in R \mapsto -a \in R$

*(ii) Multiplikation soll* assoziativ *sein:* $a(bc) = (ab)c$

*(iii) Distributivität:* $(a+b)c = ac + bc$ *und* $a(b+c) = ab + ac$

**Zusatz.**

- Ring mit *Einselement* „$1_R$“, d.h. es existiert ein Element:
$$1 \cdot r = r \cdot 1 = r \qquad \forall \quad r \in R$$
- *kommutativer* Ring: $ab = ba, \forall a,b \in R$
- Ring heißt *nullteilerfrei*, falls $ab = 0 \Leftrightarrow a = 0$ oder $b = 0$, d.h. mindestens ein Faktor ist Null. Dann gilt die *Kürzungsregel*:
$$ac = bc, c \neq 0 \Rightarrow a = b$$

**Beispiel** (Matrizenring über Körper). $K^{n\times n}$ sind Matrizen vom quadrarischem Format $n \times n$ mit Einträgen im Körper $K$.

- nicht kommutativ
- hat Nullteiler: $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$
- Einselement: $I_n = \begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}$, Einträge $= \delta_{ij}$
  Kronecker-Symbol: $\delta_{ij} := \begin{cases}1 & \text{für } i = j\\ 0 & \text{sonst}\end{cases}$

**1.1.2 Satz** (Rechenregeln). *Sei $R$ ein Ring. Dann gilt:*

*(i)* $0 \cdot a = a \cdot 0 = 0, \forall a \in R$

*(ii)* $a(-b) = (-a)b = -(ab)$

*(iii)* $(-a)(-b) = ab$

*(iv)* *Wenn $1_R$ existiert, dann ist es eindeutig bestimmt, und:*
$(-1)a = -a$
$(-1)(-1) = 1$

*Beweis. (i)/(ii)*: Fixiere $a \in R$. $x \in R \mapsto ax \in R$ ist ein Homomorphismus von $(R, +)$ in sich. (Für Hom. von Gruppen gilt: $0 \mapsto 0$ und vertauschbar mit Inversenbildung)
*(ii)* $\Rightarrow$ *(iii)* $-(-a) = a$
*(iv)* Annahme: $1, 1' \in R$.

$$\left.\begin{array}{lll} r \cdot 1 = r & \forall r, & r = 1' \\ 1' \cdot r = r & \forall r, & r = 1 \end{array}\right\} \Rightarrow 1' = 1$$

der Rest folgt aus *(ii)*. □

**Definition** (Nullring). *Ein Ring mit einem Element heißt* N u l l r i n g *(0-Ring):*

$$r + r = r, \quad r \cdot r = r, \quad d.h.\ 1 = 0$$

**1.1.3 Definition** (Teilring). *Ein* T e i l r i n g $S \subset R$ *ist eine Teilmenge, so dass*

*(i)* $(S, +)$ *ist Untergruppe von* $(R, +) \Rightarrow 0_S = 0_R$

*(ii)* $a, b \in S \Rightarrow ab \in S$,

**Bemerkung.** D.h. $S$ ist ebenfalls Ring, aber es kann sein, dass:

(i) $1_R$ ex., aber $1_S$ ex. nicht

(ii) $1_R \neq 1_S$

**Beispiel.** $R = \mathbb{Z}$, $S = 2\mathbb{Z}$ ist ein Ring ohne Einselement.

**1.1.4 Beispiel** (Matrizenring über Ring). $R$ ein beliebiger Ring. Dann können wir darüber den Matrizenring $R^{n\times n}$ aufbauen. $A, B \in R^{n\times n}$:

$$\begin{aligned} (A + B)_{ij} &:= A_{ij} + B_{ij} \\ (A \cdot B)_{ij} &:= \sum_k A_{ik} B_{kj} \end{aligned} \qquad (*)$$

Wenn $R$ nicht kommutativ ist, dann in $(*)$ genau auf die Reihenfolge achten.

$$(R^{n\times n})^{m\times m} \xrightarrow{\sim} R^{nm\times nm}$$

$$\text{Blockmultiplikation} \longmapsto \begin{array}{c}\text{vergiss die Blockeinteilung,} \\ \text{benutze Kästchenmultiplikation}\end{array}$$

**1.1.5 Definition** (Zentrum). *Sei $R$ ein nicht kommutativer Ring. Das* Z e n t r u m

$$Z(R) := \{s \in R; sr = rs \,\forall r \in R\}$$

*ist ein kommutativer Teilring von $R$, und es gilt:*

$$\begin{aligned} 1_R \in R &\Rightarrow 1_R \in Z(R) \\ s, s' \in Z &\Rightarrow s + s' \in Z \text{ (Distributivität anwenden!)} \\ &\Rightarrow -s \in Z, \text{ wegen } 1.1.2 \\ &\Rightarrow s \cdot s' \in Z, \text{ da: } ss'r = s(s'r) = s(rs') = (sr)s' = (rs)s' = r(ss') \end{aligned}$$

**1.1.6 Beispiel** (Übung). $R$ = Ring mit 1-Element. Das Zentrum $Z(R^{n\times n})$ des Matrizenringes besteht aus allen Matrizen $z \cdot I_n$, wobei $z \in Z(R)$. Für $n = 2$:

$$\begin{pmatrix} z & \\ & z \end{pmatrix}\begin{pmatrix} a_{ij} \end{pmatrix} = \begin{pmatrix} za_{ij} \end{pmatrix} \overset{z\in Z}{=} \begin{pmatrix} a_{ij}z \end{pmatrix} = \begin{pmatrix} a_{ij} \end{pmatrix}\begin{pmatrix} z & \\ & z \end{pmatrix}$$

*D.h.:* $Z(R) \cdot I_n \subseteq Z(R^{n\times n})$

*Umkehrung:* Betrachte $E_{i_0j_0} = \begin{cases} \text{Eintrag } 1_R & \text{für } (i_0, j_0) \\ \text{Eintrag } 0 & \text{falls } (i,j) \neq (i_0, j_0) \end{cases}$

$A \in R^{n\times n}, (A \cdot E_{i_0j_0})_{ij} = \begin{cases} a_{i,i_0} & \text{falls } j = j_0 \\ 0 & \text{falls } j \neq j_0 \end{cases}$

d.h. Spalte $\begin{aligned} S_{j_0}(A \cdot E_{i_0j_0}) &= S_{i_0}(A) \\ S_j(A \cdot E_{i_0j_0}) &= 0 \text{ für } j \neq j_0 \end{aligned}$

entsprechend Zeile $\begin{aligned} Z_{i_0}(E_{i_0j_0} \cdot A) &= Z_{j_0}(A) \\ Z_i(E_{i_0j_0} \cdot A) &= 0 \text{ sonst} \end{aligned}$

$A$ im Zentrum heißt: $AE_{i_0j_0} = E_{i_0j_0}A \,\forall i_0, j_0$ gilt gdw. $A = \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$

**1.1.7 Definition** (Einheit). *$R$ sei Ring mit 1. $r \in R$ heißt* E i n h e i t, *falls ein $s \in R$ existiert, so dass $rs = sr = 1$.*

**Folgerung.** *Natürlich ist 1 Einheit.*

**Folgerung.** *Die Einheiten eines Ringes $R$ (mit 1-Element) bilden bezüglich Multiplikation eine Gruppe (= $R^\times$, „$R$ mal“).*

*Beweis.* Es ist $1 \in R^\times$. Wenn $r \in R^\times$, dann existiert ein $s$ mit: $sr = rs = 1 \Rightarrow s \in R^\times$, invers zu $r$.

$$r, r' \in R^\times \Rightarrow \left.\begin{aligned} rs = sr = 1 \\ r's' = s'r' = 1 \end{aligned}\right\} \Rightarrow (rr')(s's) = (s's)(rr') = 1$$

Also ist $rr'$ eine Einheit und $(rr')^{-1} = (r')^{-1} \cdot (r^{-1})$. □

**Beispiele.**

- $\mathbb{Z}$ ganze Zahlen, $\mathbb{Z}^\times = \{\pm 1\}$
- $K$ Körper, $K[X]^\times = K - \{0\}$, konstante Polynome
  $1 \in K[X]$ ist das konstante Polynom mit Koeffizienten $= 1$.

- $(K^{n\times n)})^\times = GL_n(K)$ allg. lineare Gruppe, d.h det $\neq 0 \Leftrightarrow$ Rang $= n$

**1.1.8 Definition** (Potenzen im Ring $R$)**.** $r \in R, n \geq 1$*:*

$$r^n := \underbrace{r \cdots r}_{n\text{-mal}} \qquad \textit{und setze} \qquad r^0 := 1_R$$

*Negative Potenzen von r kann man nur bilden, falls* $r \in R^\times$, $n < 0$*:*

$$r^n := (r^{-1})^{-n}$$

### 1.1.1 $K$-Algebren

**Erinnerung.** Ein Ring $R$ heißt *K ö r p e r*, falls:

(i) $R$ ist *kommutativer* Ring mit $1 \neq 0$

(ii) $R^\times = R - \{0\}$, jedes von 0 verschiedene Element hat ein Inverses.

Wenn $R$ wie oben, aber nicht kommutativ, dann spricht man von einem *S c h i e f k ö r p e r*.

**Beispiel** (Schiefkörper der Quaternionen $\mathbb{H}$)**.** Nach WILLIAM R. HAMILTON. [1] $K = \mathbb{C}$, Körper der komplexen Zahlen. $z = a + bi$, $\overline{z} = a - bi$. $\mathbb{C} \ni z \mapsto \overline{z} \in \mathbb{C}$ entspricht Spiegelung an der reellen Achse, und ist verträglich mit allen Körperoperationen. Es ist $\overline{\overline{z}} = z$ (Involution), und $\overline{z} = z \Leftrightarrow z$ reell. Schreibe $\mathbb{H}$ als $2 \times 2$-Matrizen mit Einträgen aus $\mathbb{C}$:

$$\mathbb{H} := \left\{ \begin{pmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{pmatrix} ; z_1, z_2 \in \mathbb{C} \right\}$$

Weil $\mathbb{C}$ = 2-dim. $\mathbb{R}$-Vektorraum $\Rightarrow \mathbb{H}$ = 4-dim. $\mathbb{R}$-Vektorraum.

*Behauptung:* $\mathbb{H}$ ist abgeschlossen bei Addition und Multiplikation von Matrizen. (Die Multiplikation ist aber nicht kommutativ, d.h. $\mathbb{H}$ ist ein Schiefkörper.)

$\begin{pmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{pmatrix} = A \in \mathbb{H}$ hat Inverses, weil $\det A = z_1\overline{z}_1 + z_2\overline{z}_2 =$ Summe von 4 Quadraten, und $\det A = 0 \Leftrightarrow z_1 = z_2 = 0$.

$\begin{pmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{pmatrix}^{-1} = \frac{1}{\det A} \begin{pmatrix} \overline{z}_1 & \overline{z}_2 \\ -z_2 & z_1 \end{pmatrix} \overset{(?)}{=} \begin{pmatrix} x_1 & -\overline{x}_2 \\ x_2 & \overline{x}_1 \end{pmatrix} \Rightarrow x_1 = \overline{\left(\frac{z_1}{\det A}\right)} = \frac{\overline{z}_1}{\det A}$ (da $\det A \in \mathbb{R} \Rightarrow \overline{\det A} = \det A$) und $x_2 = -\frac{z_2}{\det A}$.

*2. Vorlesung vom 27.10.2003*

**1.1.9 Definition** ($K$-Algebra)**.** *Sei K ein Körper. Eine Menge A heißt K - A l g e - b r a, falls:*

*(i) A ist ein K-Vektorraum*

*(ii) A ist ein Ring, d.h. wir können für* 2 *Vektoren ein assoziatives Prdukt bilden.*

*(iii)* $\lambda \in K, a, b \in A \Rightarrow \lambda(ab) = (\lambda a)b = a(\lambda b)$

*Wir nennen die K-Algebra A e n d l i c h d i m e n s i o n a l, falls* $\dim_K A < \infty$*.*

[1] WILLIAM R. HAMILTON(1806-1865), Mathematiker und Physiker in Dublin. Entdecker des Assoziativgesetzes. Er beschrieb die Quaternionen als Erster 1853.

**Beispiele.** a) $K^{n\times n}$ = Matrizenring (nicht-kommutative Algebra)
*(iii)* gilt: $\lambda \in K, A = (a_{ij}) \in K, \lambda A = (\lambda a_{ij})$; $\lambda(AB) = (\lambda A)B = A(\lambda B)$.
$\dim_K(K^{n\times n}) = n^2$

b) Polynomring $K[X]$ (kommutative Algebra): $a = \sum_{i=0}^{m} a_i X^i \in K[X], a_i \in K$
$\lambda \in K : \lambda a = \sum(\lambda a_i)X^i, \dim_K(K[X]) = \infty$.

c) die Quaternionenalgebra $\mathbb{H}$ ist eine 4-dim. $\mathbb{R}$-Algebra:

$$\lambda \in \mathbb{R} \Rightarrow \lambda \begin{pmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{pmatrix} = \begin{pmatrix} \lambda z_1 & -\overline{\lambda z_2} \\ \lambda z_2 & \overline{\lambda z_1} \end{pmatrix} \in \mathbb{H}$$

Sei $h(z_1, z_2) := \left(\begin{smallmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{smallmatrix}\right)$, $a_j, b_j \in \mathbb{R}, z_j = a_j + ib_j$:

$$\begin{aligned} h(a_1 + ib_1, a_2 + ib_2) &= h(a_1 + ib_1, 0) + h(0, a_2 + ib_2) \\ &= a_1 h(1,0) + b_1 h(i,0) + a_2 h(0,1) + b_2 h(0,i) \end{aligned}$$

d.h. $h(1,0), h(i,0), h(0,1), h(0,i)$ ist ein Erzeugendensystem.

**Bemerkung.** Sei $A$ ein endlich-dimensionaler $K$-Vektorraum mit einer Basis $b = (b_1, \ldots, b_n)$. Eine Algebra-Struktur auf $A$ ist erklärt, sobald eine Multiplikation der Basis erklärt werden kann. Wobei die Assoziativität gelten muss, d.h. $(b_i b_j)b_k = b_i(b_j b_k) \in A$. Dann ergibt sich aufgrund der Distribuitivitätsforderung eindeutig eine Algebra-Struktur auf $A$: $(\sum \lambda_i b_i)(\sum \mu_i b_i) \in A$.

**Beispiel** (Basen von $\mathbb{H}$). (Es ist $\bar{i} = -i$.)

$$h(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =: e \qquad h(0,1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} =: j$$
$$h(i,0) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} =: i \qquad h(0,i) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} =: k$$

Multiplikationstafel: (Zeile $\times$ Spalte)

| | $e$ | $i$ | $j$ | $k$ |
|---|---|---|---|---|
| $e$ | $e$ | $i$ | $j$ | $k$ |
| $i$ | $i$ | $-e$ | $-k$ | $j$ |
| $j$ | $j$ | $k$ | $-e$ | $-i$ |
| $k$ | $k$ | $-j$ | $i$ | $-e$ |

**Bemerkung.** Die Elemente $\pm e, \pm i, \pm j, \pm k \in \mathbb{H}$ bilden bezüglich der Multiplikation eine nicht-kommutative Gruppe der Ordnung 8. Sie heißt *Quaternionengruppe* $Q$. Wir kennen bereits eine nicht-kommutative Gruppe der Ordnung 8, nämlich die Diedergruppe $D_4$ (Symmetrien des Quadrats: Drehungen und Spiegelungen). $Q$ und $D_4$ sind nicht isomorph. $Q$ wird durch 2 Elemente der Ordnung 4 erzeugt, $D_4$ durch zwei Elemente der Ordnung 2.

**Bemerkung.** Wenn die $K$-Algebra $A$ ein Einselement $1_A$ hat, dann können wir den Skalarkörper $K$ in $A$ einbetten, vermittels $\lambda \mapsto \lambda \cdot 1_A$. Damit haben wir $K$ als einen Teilkörper von $A$, der im Zentrum von $A$ liegen muss.

**Beispiele.** • $K^{n\times n}, K \ni \lambda \mapsto \lambda I_n$ (Skalarmatrizen)

- $A = K[X], 1_A = 1 + \sum 0X^i = 1, \lambda \cdot 1_A = \lambda + \sum 0X^i = \lambda$ (konstante Polynome)

**1.1.10 Satz.** *Sei $A$ eine endlich-dimensionale und nullteilerfreie $K$-Algebra. Dann hat $A$ ein Einselement und ist ein Schiefkörper. (Man spricht auch von einer* D i v i s i o - n a l g e b r a *über $K$.)*

*Beweis.* Betrachte $x \neq 0, \in A$ und die Abbildungen $l_x : A \to A, a \mapsto xa$ und $r_x : A \to A, a \mapsto ax$. Die Abbildungen $l_x$ und $r_x$ sind beide $K$-linear und injektiv, weil $A$ nullteilerfrei ist. Daraus folgt, dass die Abbildungen sogar surjektiv sein müssen, weil $A$ endlichdimensinal ist.

Existenz der 1:

a) Fixiere irgendein $x \neq 0$. Dann gibt es *genau ein* $a_0$ mit $x = xa_0$ und *genau ein* $b_0$ mit $b_0x = x \Rightarrow xa_0x = x^2 = xb_0x \Rightarrow a_0 = b_0$.

   *Zwischenergebnis*: Wenn $xa_0 = x$ dann gilt auch $a_0x = x$ und umgekehrt.

b) Betrachte $xa_0 = x = a_0x$ und $yb_0 = y = b_0y$. Dann zeigt man $a_0 = b_0$, dh. $a_0$ ist gut für alle $x$, also $a_0 = 1_A$. Denn: $x = a_0x \Rightarrow xy = a_0xy \Rightarrow xy = xya_0$, wegen Zwischenergebnis und $xyb_0 = xy = xya_0$.

c) Existenz des Inversen: Gegeben sei $x \neq 0$.

$$\left.\begin{array}{l}\text{finde } y \text{ mit } xy = 1_A \\ \text{finde } z \text{ mit } zx = 1_A\end{array}\right\} \Rightarrow z = z1_A = zxy = 1_Ay = y = x^{-1}$$

□

### 1.1.2 Charakterisierung von $\mathbb{Z}$

**Definition** (geordneter Ring)**.** *Ein Ring $R$ heißt* g e o r d n e t*, wenn es darin eine Teilmenge $R_+$ von so genannten* P o s i t i v e l e m e n t e n *gibt, mit:*

*(i)* $a, b \in R_+ \to a + b, a \cdot b \in R_+$ (Monotonie der Addition/Multiplikation)

*(ii) Für jedes $a \in R$ tritt genau einer der folgenden Fällen ein* (Trichotomie)*:*

$$a \in R_+, \quad a = 0, \quad -a \in R_+$$

**Folgerung.** *$R = R_+ \dot\cup \{0\} \dot\cup -R_+$ ist eine disjunkte Vereinigung.*

**Folgerung** (Eigenschaften)**.** *$R$ sei geordneter Ring. Dann gilt:*

*(i) Für jedes $a \neq 0$ gilt: $a^2 \in R_+$. Insbesondere $1 = 1^2 \in R_+$.*

*(ii) $R$ ist Nullteilerfrei, weil $R_+ \cdot R_+ \subseteq R_+$.*

*(iii) $R$ enthält einen zu $\mathbb{Z}$ isomorphen Teilring, nämlich die Vielfachen der* 1*.*

*(iv) Es kann niemals ein Vielfaches der $1_R$ gleich $0_R$ sein.*

**Folgerung** (Existenz einer Ordnung)**.** *Auf einem geordneten Ring $R$ kann man eine Ordnung einführen mittels:*

$$a > b \quad :\Longleftrightarrow \quad a - b \in R_+$$

*(i)* *für $a, b \in R$ trifft genau einer der Fälle $a < b$, $a > b$, $a = b$ zu.*

*(ii)* $a > b \Leftrightarrow a + c > b + c \quad \forall c \in R$
$a > b, c \in R_+ \Rightarrow ac > bc$

*(iii)* $a \neq 0 \Rightarrow a^2 > 0$

*(iv)* $a > b, b > c \Rightarrow a > c$

*Nach Definition:* $R_+ = \{a \in R, a > 0\}$.

**Definition** (wohlgeordneter Ring)**.** *Ein geordneter Ring heißt* wohlgeordnet, *falls jede nichtleere Teilmenge $M \subset R_+$ ein (eindeutig bestimmtes) kleinstes Element hat.*

**1.1.11 Satz** (Charakterisierung von $\mathbb{Z}$)**.** *Bis auf Isomorphismen ist $\mathbb{Z}$ der einzige wohlgeordnete Ring mit 1-Element.*

*Beweis.* $R$ sei wohlgeordnet $\Rightarrow R_+$ besitzt ein kleinstes Element. Dieses muss notwendigerweise $1_R$ sein (denn $0 < a < 1 \Rightarrow 0 < a^2 < a < 1 \Rightarrow a$ kann nicht kleinstes Element sein). Durch Verschiebung folgt: $1 + a$ ist das kleinste aller Elemente welche größer als $a$ sind. $\Rightarrow$ konstruiere $R$ induktiv, es entsteht $\mathbb{Z}$.

Noch zu zeigen: die positiven Vielfachen der 1 schöpfen $R_+$ aus. Annahme: es gebe positive Elemente, welche nicht Vielfache der 1 sind. Dann folgt: Die Menge $M$ aller dieser Elemente muss ein kleinstes Element $m \neq 1$ haben. Aber: $m > 1 \Rightarrow m - 1 \notin M \Rightarrow m - 1 = n \cdot 1 \Rightarrow m = (n + 1) \cdot 1$ ↯. □

**1.1.12 Folgerung** (Division mit Rest in $\mathbb{Z}$)**.** *Seien $a, b \in \mathbb{Z}$. Dann existiert eine eindeutig bestimmte Darstellung $a = qb + r$ mit $0 \leq r < |b|$.*

*Beweisidee.* Wenn $b \mid a$, dann ist nichts zu zeigen. Wenn $b \nmid a$, dann betrachte die Menge $a + b\mathbb{Z} = S$. Zeige $S_+$ (positive Elemnte in $S$) ist $\neq \emptyset$. Wohlordnung $\Rightarrow S_+$ enthält kleinstes Element $r$. □

## 1.2 Ideale, Faktorringe und Homomorphiesatz

**1.2.1 Definition** (Ring-Homomorphismus)**.** *Eine Abbildung $f : R \to S$ zwischen zwei Ringen heißt* Homomorphismus, *falls:*

$$\begin{aligned} f(r_1 +_R r_2) &= f(r_1) +_S f(r_2) \\ f(r_1 \cdot_R r_2) &= f(r_1) \cdot_S f(r_2) \end{aligned}$$

$\Rightarrow f(0_R) = 0_S$, weil $f$ Homomorphismus zwischen den additiven Gruppen ist. In Bezug auf die Einselemente, falls sie überhaupt existieren, kann man nur sagen: $1_R \cdot 1_R = 1_R \Rightarrow f(1_R) \cdot f(1_R) = f(1_R)$, d.h. $s = f(1_R)$ ist ein sogennantes *Idempotent* (d.h. $s^2 = s$).

**Anwendung.** Betrachte $R = \mathbb{Z}/n\mathbb{Z} \ni [a]_n$ und $S = \mathbb{Z}/m\mathbb{Z} \ni [a]_m$. Wann kann ein Homomorphismus $[a]_n \mapsto [a]_m$ existieren?

Notwendig ist:

$$\underbrace{0\text{-Klasse}}_{\substack{\text{alle Zahlen, welche} \\ \text{durch } n \text{ teilbar sind}}} \quad \mapsto \quad \underbrace{0\text{-Klasse}}_{\substack{\text{alle Zahlen, welche} \\ \text{durch } m \text{ teilbar sind}}}$$

Also muss gelten: $n \mid x \Rightarrow m \mid x \quad \forall x \in R$. Das ist genau dann wenn $m \mid n$.

**Folgerung.** *Der natürliche Homomorphismus $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ existiert gdw. $m \mid n$.*

**1.2.2 Definition** (Ring-Isomorphismus)**.** *Ein Homomorphismus $f : R \to S$ sei zusätzlich bijektiv. Dann gilt:*

*(i) die Umkehrabbildung $f^{-1}(s) = r$ ist wohldefiniert, und*

*(ii) $f^{-1}$ ist ein Ringhomomorphismus von $S \to R$ mit $f^{-1} \circ f = \mathrm{id}_R$ und $f \circ f^{-1} = \mathrm{id}_S$.*

*Dann nennen wir die Ringe R und S* i s o m o r p h *und f einen* I s o m o r p h i s m u s*. Schreibweise: $R \cong S$, $R \xrightarrow{\sim} S$.*

Die Isomorphie von Ringen ist eine Äquivalenzrelation (d.h. Existenz von Isomorphismen).

(i) *(Reflexivität)* $R \cong R, \quad f = \mathrm{id}_R$

(ii) *(Symmetrie)* $f : R \xrightarrow{\sim} S \Rightarrow f^{-1} : S \xrightarrow{\sim} R$

(iii) *(Transitivität)* $R \xrightarrow[f]{\sim} S \xrightarrow[g]{\sim} T \Rightarrow g \circ f : R \xrightarrow{\sim} T$

*3. Vorlesung vom 03.11.2003*

**Beispiel** (Chinesischer Restsatz)**.** Der chinesische Restsatz gibt ein nicht triviales Beispiel für einen Isomorphismus. Sei $a = a_1 \cdots a_n$ Produkt von paarweise teilerfremden ganzen Zahlen:

$$\phi : \mathbb{Z}/a\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

**1.2.3 Satz** (Eigenschaften von Kern und Bild)**.** *Sei $f : R \to S$ Homomorphismus von Ringen. Dann gilt:*

*(i)* Bild $f$ *ist Teilring von S*

*(ii)* $\ker f$ *ist Teilring von R*

*(iii) Sei* $I := \ker f$*. Dann gilt:* $R \cdot I \subseteq I$, $I \cdot R \subseteq I$.

*(iv) $f$ ist injektiv gdw.* $\ker f = \{0\}$.

*Beweis.* $f$ ist Homomorphismus von Ringen. Insbesondere ist $f\colon (R,+) \to (S,+)$ ein Homomorphismus von kommutativen Gruppen. $\Rightarrow$ *(iv)*. Außerdem ist Bild$(f,+)$ eine Untergruppe von $(S,+)$ und $f(r_1)f(r_2) = f(r_1r_2) \in$ Bild $f$, also ist das Bild stabil bei Multiplikation. Die Distributivgesetze übertragen sich $\Rightarrow$ Bild $f$ ist Teilring von $S$ $\Rightarrow$*(i)*.

*(ii)/(iii):* Zunächst haben wir $(I,+) := (kerf,+)$ Untergruppe von $(R,+)$. Behauptung: $R \cdot I \subseteq I \supseteq I \cdot R$. Sei $x \in I, f(x) = 0, r \in R$ beliebig $\Rightarrow f(xr) = 0_S \cdot f(r) = 0 \Rightarrow xr \in I$; ebenso rx. (Es folgt natürlich $I \cdot I \subset I$). □

**1.2.4 Definition** (Ideal)**.** *Eine Teilmenge I eines Ringes R heißt* I d e a l *falls:*

*(i) $(I,+)$ ist Untergruppe von $(R,+)$*

*(ii) Es gilt: $R \cdot I \subseteq I$ (Linksideal)*
*$I \cdot R \subseteq I$ (Rechtsideal)*
*$I \cdot R \subseteq I \supseteq R \cdot I$ (Zweiseitiges Ideal)*

Im kommutativen Fall gibt es nur einen Idealbegriff, im nicht kommutativen drei.

**Beispiel** (Hauptideale)**.** Einfachstes Beispiel eines Ideals: sei $a \in R$ beliebig. Dann ist:

- $R \cdot a$ das von $a$ erzeugte Linksideal
- $a \cdot R$ das von $a$ erzeugte Rechtsideal
- $RaR$ das von $a$ erzeugte zweiseitige Ideal. (*Vorsicht im nicht kommutativen Fall*: Nicht alle Elemente aus $RaR$ haben die Form $r_1 a r_2$. Beispiel: $r_1 a r_2 + s_1 a s_2$ liegt in dem von $a$ erzeugten zweiseitigen Ideal, *ohne* dass eine Relation $r_1 a r_2 + s_1 a s_2 = t_1 a t_2$ gelten muss.)

Die von einem Element erzeugten Ideale heißen *H a u p t i d e a l e*.
$(Ra, +)$ ist Gruppe wegen Distributivität:

$$r_1 a + r_2 a = (r_1 + r_2)a$$

Es gilt $R \cdot (Ra) \subset Ra$ wegen Assoziativität der Multiplikation:

$$r_1(r_2 a) = (r_1 r_2)a$$

**Hilfssatz.** *Im Ring $\mathbb{Z}$ sind alle Ideale Hauptideale.*

*Beweisskizze.* Sei $I \subseteq \mathbb{Z}$ ein Ideal:

$$x \in I \Rightarrow -x = (-1)x \in I$$

Wir betrachten in $I$ das kleinste positive Element $a$. Dann ist $I = \mathbb{Z}a$ wegen der Division mit Rest (Rest wäre kleiner als $a$). □

Charakterisierende Eigenschaft des 2-seitigen Ideals $I \subset R$ ist die Tatsache, dass die Faktorgruppe $(R/I, +)$ von $R$ die Ringstruktur erbt. Genauer:

**1.2.5 Satz.** *Sei $R$ ein Ring, $I \subset R$ ein zweiseitiges Ideal. Äquivalenzrelation:*

$$r_1 \sim r_2 \quad :\Leftrightarrow \quad r_1 - r_2 \in I$$

*$R/I$ bezeichne die Menge der Äquivalenzklassen.*

$$a \in R \mapsto [a] \in R/I, \qquad [a] = a + I$$

*Dann erbt $R/I$ von $R$ die Ringstruktur und die Multiplikation $[a][b] := [ab]$ ist wohldefiniert.*

*Beweis.* Zunächst ist $(R/I, +)$ wieder kommutative Gruppe.
Zu zeigen: $a \sim a', b \sim b' \Rightarrow ab \sim a'b'$:

$$ab - a'b' = (a - a')b + a'(b - b') \in I$$

weil $I$ ein 2-seitiges Ideal. □

**Definition** (Faktorring)**.** *Ist $R$ ein Ring, und $I \subset R$ ein zweiseitiges Ideal, so nennt man $R/I := \{a + I; a \in R\}$ (wie oben) den* F a k t o r r i n g $R$ m o d u l o $I$.

**1.2.6 Satz** (Homomorphiesatz in der Ringtheorie)**.** *Sei $f : R \to S$ ein Homomorphismus von Ringen, und sei $I$ der* ker $f$*. Dann induziert $f$ einen Isomorphismus zwischen dem Faktorring $R/I$ und* Bild $f$*, d.h.*

$$f_* : R/I \xrightarrow{\sim} \text{Bild } f$$

*Beweis.* Betrachte $f : R \to S$ als Abbildung von Mengen. Führe auf $R$ folgende Äquivalenzrelation ein:

$$r_1 \sim r_2 \quad :\Leftrightarrow \quad f(r_1) = f(r_2)$$

$\Rightarrow f$ induziert Bijektion $f_* : R/\sim \longleftrightarrow$ Bild $f$.

Jetzt sei $f$ ein Homomorphismus von Ringen. Dann folgt:

$$\begin{aligned} r_1 \sim r_2 &\Leftrightarrow f(r_1) = f(r_2) \Leftrightarrow f(r_1) - f(r_2) = 0_S \\ &\Leftrightarrow f(r_1 - r_2) = 0_s \\ &\Leftrightarrow r_1 - r_2 \in I \end{aligned}$$

In diesem Fall bekommen wir $R/\sim \; = R/I$ als Ring. Also: $f_*$ ist bijektiv zwischen 2 Ringen. Noch zu zeigen: $f_*$ ist Homomorphismus.

$$\begin{aligned} f_*([a] + [b]) = f_*([a + b]) &= f(a + b) = f(a) + f(b) \\ &= f_*([a]) + f_*([b]) \end{aligned}$$

Entsprechend $f_*([a][b])$. □

**1.2.7 Bemerkung.** Sei $I$ ein Ideal im *kommutativen* Ring $R$. Dann hat man eine natürliche Bijektion:

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Ideale von } R \\ \text{welche } I \text{ enthalten} \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{Ideale im} \\ \text{Faktorring } R/I \end{array} \right\} \\ I \subseteq J & \longmapsto & \overline{J} := J/I \end{array}$$

Sei $\phi : R \to R/I, a \mapsto [a]$ die natürliche Abbildung. Wir definieren zwei Abbildungen: Sei $J$ Ideal in $R$ mit $J \supseteq I$. Dann bilde dazu $\overline{J} = J/I$ (Ideal in $R/I$). Umgekehrt sei $\Lambda$ ein Ideal in $R/I$. Dann bilde dazu $\phi^{-1}(\Lambda) := \{a \in R; [a] \in \Lambda\}$. Dies ist ein Ideal von $R$, welches $I = \Lambda^{-1}(0)$ enthält. Die Abbildungen $J \mapsto \overline{J}$ und $\Lambda \mapsto \phi^{-1}(\Lambda)$ sind zueinander invers.

**1.2.8 Satz.** *$R$ sei ein kommutativer Ring mit* 1*. Dann ist folgendes äquivalent:*

*(i) $R$ hat außer $\{0\}$ und $R$ keine weiteren Ideale.*

*(ii) $R$ ist ein Körper.*

*Beweis. (i)⇒(ii):* Sei $x \neq 0 \in R$. Betrachte $Rx$. Dann ist $x = 1x \in Rx \neq \{0\} \Rightarrow Rx = R \Rightarrow yx = 1$ ist lösbar $\Rightarrow R$ ist Körper.

*(ii)⇒(i):* Sei $x \neq 0, \in R =$ Körper. Betrachte $Rx$. Finde $y$ mit $yx = 1 \Rightarrow 1 \in Rx \Rightarrow R = R1 \subseteq Rx \Rightarrow R = Rx$. □

**1.2.9 Satz.** *Sei $R$ kommutativ mit Eins und $I \subset R$ ein echtes Ideal, d.h. $I \neq R$ und $I \neq \{0\}$. Dann ist $I$ maximal (im Sinne von Inklusion) genau dann, wenn $R/I$ ein Körper ist.*

*Beweis.* Zwischen $I$ und $R$ gibt es keine weiteren Ideale $\Leftrightarrow$ $I$ maximal ist $\Leftrightarrow$ in $R/I$ gibt es keine nicht trivialen Ideale $\Leftrightarrow$ $R/I$ ist Körper (1.2.7 anwenden). $\square$

**Bemerkung.** Durch Anwendung des Zornschen Lemmas folgt: zu jedem Ideal $I \subset R, I \neq R$ existiert ein maximales Ideal $J$ mit der Eigenschaft: $I \subseteq J \subsetneq R$.

## 1.3 Teilbarkeit in Ringen

$R$ sei immer kommutativ mit Eins.

**1.3.1 Definition** (Teiler, Vielfaches)**.** *Für zwei Elemente $a, b \in R$ sagen wir „$a$ teilt $b$“ oder „$b$ ist Vielfaches von $a$“, „$a \mid b$“ falls ein $c \in R$ existiert mit $b = ca$.*

**Spezialfälle.** (i) $a \mid b, b \nmid a$ ($b$ teilt nicht $a$). Dann nennen wir $a$ einen *echten Teiler* von $b$.

(ii) $a \mid b, b \mid a$. Dann nennen wir die Elemente $a, b$ *assoziert* und schreiben $a \sim b$, weil das eine Äquivalenz-Relation ist.

**1.3.2 Satz** (Mengentheoretische Charakterisierung der Teilbarkeit)**.** *Für $a, b \in R$ gilt: $a \mid b \iff Rb \subseteq Ra$. (Umgekehrte Inklusion für die Hauptideale.)*

*Beweis.* „$\Rightarrow$“: $a \mid b, b = ca \in Ra \Rightarrow Rb \subseteq Ra$. „$\Leftarrow$“: $Rb \subseteq Ra$. Dann gilt insbesondere: $b = 1b \in Rb \subseteq Ra \Rightarrow b = ca \Rightarrow a \mid b$. $\square$

**Sonderfälle.** (i) $0 \mid a \iff a = 0$, sonst $R0 = 0 \subseteq Ra$, andererseits $a \mid 0$ ist immer richtig, weil $Ra \supset R0 = 0$.

(ii) $a \mid x$ für alle $x \in R \Leftrightarrow a \mid 1 \Leftrightarrow a \in R^\times$ eine Einheit $\iff Ra = R$, d.h. die Einheiten eines Ringes sind genau die Elemente, welche jedes Ringelement teilen. $\Rightarrow$ Die Teilbarkeitslehre in einem Ring ist umso uninteressanter, je mehr Einheiten der Ring hat.

Es folgt: $x$ ist *gemeinsamer Teiler* von

$$a_1, \ldots, a_n \Leftrightarrow Rx \supseteq Ra_1 + \cdots + Ra_n$$

$x$ ist *gemeinsames Vielfaches* von

$$a_1, \ldots, a_n \Leftrightarrow Rx \subset Ra_1 \cap \cdots \cap Ra_n$$

.

*4. Vorlesung vom 10.11.2003*

**1.3.3 Ein Ziel.** In $\mathbb{Z}$ gilt der Hauptsatz der Arithmetik: Jede ganze Zahl $n$ schreibt sich eindeutig als

$$n = \operatorname{sgn}(n) \cdot \text{Produkt von Primzahlen}$$

## Thema I: Irreduzible Elemente & Primelemente

**1.3.4 Definition** (Irreduzibles Element, Primelement). *$a \in R$, a keine Einheit, d.h. $Ra \neq R$.*

*(i) a heißt* irreduzibles Element, *falls a keine echten Teiler hat (d.h. wenn $b \mid a \Rightarrow b \sim a$ (assoziert) oder b ist Einheit).*

*(ii) Nenne $a \in R$* Primelement, *falls $a \mid bc$ bedeutet $\Rightarrow$ a teilt wenigstens einen Faktor.*

**1.3.5 Hilfssatz.** *(i) $a \in R$ ist irreduzibel $\Leftrightarrow$ $Ra$ ist ein maximales Hauptideal in $R$.*

*(ii) $0 \in R$ ist irreduzibel $\Leftrightarrow$ $R$ ist Körper.*

*(iii) $0 \in R$ ist Primelement $\Leftrightarrow$ $R$ ist nullteilerfrei.*

*(iv) $a \in R$ ist Primelement $\Leftrightarrow$ $R/Ra$ ist ein nullteilerfreier Ring.*

*Beweis.* (i) 0 irreduzibel $\Leftrightarrow R0 = \{0\} \subset R$ ist maximales Hauptideal $\Leftrightarrow b \neq 0, Rb = R \Leftrightarrow b$ ist Einheit $\Leftrightarrow R$ Körper.

(ii) $a$ ist irreduzibel $\Leftrightarrow a$ hat keine echten Teiler $\Leftrightarrow$ es existieren keine Hauptideale $Rb$ mit $R \supsetneq Rb \supsetneq Ra \Leftrightarrow Ra$ ist maximales Hauptideal

(iii) 0 prim $\Leftrightarrow (0 \mid ab \Leftrightarrow a = b = 0) \Leftrightarrow 0 \mid a \vee 0 \mid b \Leftrightarrow a = 0 \vee b = 0 \Leftrightarrow R$ ist nullteilerfrei. $a \mid 0$ gilt immer, weil $0 = 0a$; $a$ Nullteiler bedeutet: $0 = ba$ mit $b \neq 0$ (0 ist echtes Vielfaches von $a$).

(iv) $a$ Primelement heißt: $a \mid bc \Leftrightarrow a \mid b \vee a \mid c$. In $R/aR$: $Ra \supset Rbc$, d.h. $[b][c] = [bc] = [a] = [0]$.

$$a \mid b \Leftrightarrow b \in Ra \Leftrightarrow [b] = [0]$$
$$a \mid c \Leftrightarrow c \in Ra \Leftrightarrow [c] = [0]$$

Also $a \mid bc \Leftrightarrow a \mid b$ oder $a \mid c$. Bedeutet im Restklassenring $R/Ra$:

$$[b][c] = [0] \Leftrightarrow [b] = [0] \quad \text{oder} \quad [c] = [0]$$

d.h. $R/Ra$ ist nullteilerfreier Ring.

□

**Bemerkung.** Die Eigenschaft $a$ ist irreduzibel bzw. Primelement kann ausgedrückt werden nur unter Benutzung von Ideal $Ra$. D.h.:

(i) $a$ irreduzibel $\Longleftrightarrow$ alle assoziierten Elemente irreduzibel

(ii) $a$ Primelement $\Longleftrightarrow$ alle assoziierten Elemente Primelemente

**1.3.6 Satz.** *(i) Ring $R$ sei nullteilerfrei. Dann ist jedes Primelement ($\neq 0$) auch irreduzibel.*

*(ii) $R$ sei Haupidealring (d.h. jedes Ideal hat die Form $J = Ra$). Dann ist jedes irreduzible Element auch Primelement.*

*Beweis.* (i) Sei $a \neq 0$ Primelement. Annahme: $a$ ist reduzibel (= nicht irreduzibel) $\Rightarrow$ $a$ hat echten Teiler $b$, d.h. $R \supsetneq Rb \supseteq Ra$. Schreibe $a = bc$, $a$ Primelement und $a \mid bc \Rightarrow b$ ist echter Teiler von $a$ oder $a \mid c$. Also folgt $a \mid c \Rightarrow c = ad \Rightarrow a = bc = bad \Rightarrow a(1 - bd) = 0$. Wegen Nullteilerfreiheit und $a \neq 0 \Rightarrow 1 - bd = 0 \Rightarrow bd = 1$, d.h. $b$ Einheit ↯(weil $b$ echter Teiler)

(ii) $a$ sei irreduzibel ($\neq 0$) $\Rightarrow R \supset Ra$ ist echtes Maximalideal $\Rightarrow R/Ra$ ist ein Körper $\Rightarrow$ nullteilerfrei $\Rightarrow$ $a$ ist Primelement

□

**Bemerkung.** $\mathbb{Z}$ ist nullteilerfrei und Hauptidealring. Also gelten in $\mathbb{Z}$ beide Richtungen des Satzes. D.h. Für $a \neq 0, \in \mathbb{Z}$ : $a$ irreduzibel $\Leftrightarrow$ $a$ prim.

## Thema II: Teilerketten

Absteigende *Teilerkette* im Ring $R$ ist eine Kette der Form:

$$a_1 \mid a, \quad a_2 \mid a_1, \quad a_3 \mid a_2, \quad \ldots$$

Idealtheoretisch bedeutet das:

$$Ra \subseteq Ra_1 \subseteq Ra_2 \subseteq Ra_3 \subseteq \ldots$$

ist eine aufsteigende Kette von Hauptidealen.

**1.3.7 Definition** (Teilerkettensatz). *(i) Wir sagen im Ring $R$ gilt der* Teilerkettensatz für Elemente, *falls es keine unendlichen echten absteigenden Teilerketten gibt.*

*(ii) Wir sagen, dass in $R$ der* Teilerkettensatz für Ideale *gilt, falls es keine unendlichen echt aufsteigenden Idealketten in $R$ gibt.*

**Folgerung.** *Offensichtlich: Wenn in $R$ der Teilerkettensatz für Ideale gilt, dann erst recht für Elemente.*

**1.3.8 Satz** (Satz von Euklid[2]). *Wenn im Ring $R$ der Teilerkettensatz für Elemente gilt, dann kann man jedes $a \in R, a \neq 0, a \notin R^\times$, $a$ kein Nullteiler, als Produkt von endlich vielen irreduziblen Elementen schreiben.*

*Beweis.* Wenn $a$ irreduzibel, dann $a = a$, trivial. Betrachte

$$M = \left\{ \begin{array}{c} x \in R; \quad x \neq 0; \quad x \text{ kein Nullteiler}; \quad x \notin R^\times \\ \text{nicht darstellbar als Produkt endlich vieler irreduzibler Faktoren} \end{array} \right\}$$

Behauptung: $M = \emptyset$. Annahme: Es existiert $r \in M$, dann existiert auch ein solches $r$, dass alle echten Teiler von $r$ nicht mehr in $M$ liegen ($*$). Sei nämlich $a \mid r$ echt, $a \in M$, und $a$ wieder echter Teiler in $M$, $b \mid a$ usw. Wir würden eine unendliche Teilerkette finden ↯.

[2] griechischer Mathematiker und Philosoph, 365-300 v. Chr. in Alexandria. *Die Elemente*: 13 Kapitel Geometrie und Zahlentheorie, ca. 325 v. Chr.

Sei $r \in M$ mit Eigenschaft $(*)$. $r$ kann nicht irreduzibel sein $\Rightarrow r = r_1 r_2$, wobei $r_1$ ein echter Teiler von $r$ ist. Behauptung: $r_2$ ist ebenfalls echter Teiler von $r$. Anderenfalls: $r_2 \mid r$ und $r \mid r_2$, $r_2 = ar$

$$r = r_1 r_2 = a r_1 r \Rightarrow r(1 - a r_1) = 0$$

aber $r_1$ ist keine Einheit, d.h. $1 - ar_1 \neq 0 \Rightarrow r$ ist Nullteiler $\lightning$.

Also sind in $r = r_1 r_2$ beide Faktoren echte Teiler von $r \Rightarrow$ beide Faktoren $\notin M \Rightarrow$ jedes $r_i$ ist Produkt endlich vieler irreduzibler Faktoren $\Rightarrow r = r_1 r_2$ ist ebenfalls eine Widerspruch $\lightning$. □

**Folgerung.** *Euklid folgend: In $\mathbb{Z}$ gibt es unendlich viele irreduzible Zahlen.*

*Beweis.* Annahme: $p_1, \ldots, p_n$ seien alle irreduziblen Zahlen. Bilde $p_1 \cdot p_2 \cdots p_n + 1 = q_1 \cdots q_n$, ein Produkt von endlich vielen irreduziblen Teiler (Teilerkettensatz, also ist 1.3.8 anwendbar). Annahme: $q_i = p_i = p$ für ein $i \Rightarrow p \mid n$ und $p \mid (n+1) \Rightarrow p \mid 1$ $\lightning$ □

## Thema III: Faktorielle Ringe

**1.3.9 Definition** (Faktorieller Ring)**.** *Sei $x \in R$, seien $x = p_1 \cdots p_r = q_1 \cdots q_s$ zwei Zerlegungen von $x$ in irreduzible Faktoren.*

*(i) Wir nennen beiden Zerlegungen* ä q u i v a l e n t, *falls $r = s$ und bei geeigneter Nummerierung der Faktoren $p_i \sim q_i$ (d.h. $p_i \mid q_i$ und $q_i \mid p_i$) gilt.*

*(ii) Wir sagen, dass $x \in R$ eine* e i n d e u t i g e Z e r l e g u n g i n i r r e d u z i b l e F a k t o r e n *erlaubt, falls je zwei Zerlegungen von $x$ äquivalent sind.*

*(iii) Wir nennen den Ring $R$* f a k t o r i e l l, *falls $R$ nullteilerfrei ist und jedes $x \in R, \neq 0, \notin R^\times$ eine eindeutige Zerlegung in irreduzible Faktoren besitzt.*

**1.3.10 Hauptsatz.** *Sei $R$ nullteilerfreier Ring. Dann ist $R$ faktoriell (d.h. Eindeutigkeit der Zerlegung) genau dann, wenn in $R$ der Teilerkettensatz für Elemente gilt, und jedes irreduzible Element ($\neq 0$) auch automatisch Primelement ist.*

*5. Vorlesung vom 17.11.2003*

*Beweis.* „⇒": $R$ sei faktoriell. Betrachte $r = p_1 \cdots p_n \in R$. Sei $s$ echter Teiler von $r \Rightarrow r = st$ und $t$ ebenfalls echter Teiler ($s$ keine Einheit).

$$\begin{aligned} \text{faktoriell} \quad &\Rightarrow \quad s = q_1 \cdots q_m, \qquad t = q_1' \cdots q_k' \\ &\Rightarrow \quad r = p_1 \cdots p_n = q_1 \cdots q_m \cdot q_1' \cdots q_k' \\ &\Rightarrow \quad \text{Eindeutigkeit: } n = m + k \end{aligned}$$

Also: Wenn $s$ echter Teiler von $r \Rightarrow s$ hat weniger irreduzible Faktoren als $r \Rightarrow$ echte Teilerketten müssen abbrechen.

Noch zu zeigen: Irreduzible Elemente $p$ sind prim. Sei $p$ Teiler des Produkts $ab \Rightarrow pr = ab$. Zerlege $r, a, b$ in irreduzible Faktoren. Dann:

$$p \cdot p_1 \cdots p_n = q_1 \cdots q_m q_1' \cdots q_k'$$

Eindeutigkeit $\Rightarrow$ der Faktor $p$ muss bis auf Äquivalente auf der rechten Seite vorkommen $\Rightarrow p \mid a$ oder $p \mid b$. Also: $p$ ist Primelement.

„⇐“: Voraussetzung: in $R$ gelte der Teilerkettensatz, und jedes irreduzible Element ist prim. Satz von Euklid: *Jedes $x \in R, x \neq 0, x \notin R^\times$ lässt sich zerlegen in ein Produkt $x = p_1 \cdots p_n$ irreduzibler Faktoren.*

Nun zur Eindeutigkeit: Sei $x = q_1 \cdots q_m$ eine zweite Zerlegung. Dann ist:

$$p_1 \cdots p_n = q_1 \cdots q_n \qquad (*)$$

Nach Voraussetzung sind alle $p_i, q_j$ Primelemente. $\Rightarrow$ Finde $q_i$ mit $p_1 \mid q_i$. Da $p_1$ und $q_i$ beide irreduzibel sind, folgt dann $p_1 \sim q_i$. O.B.d.A.: $p_1 \sim q_1$.

**Hilfssatz.** *In einem nullteilerfreien Ring $R$ können sich assozierte Elemente nur um (vielfache) Einheiten unterscheiden.*

*Beweis.* $p_1 \mid q_1$ und $q_1 \mid p_1 \Rightarrow q_1 = ap_1 \wedge p_1 = bq_1 \Rightarrow q_1 = abq_1$. Weil $R$ nullteilerfrei ist, darf man kürzen $\Rightarrow 1 = ab \Rightarrow a, b \in R^\times$. (Umkehrung gilt immer: $q = ap, e \in R^\times \Rightarrow q = e^{-1}p \Rightarrow p \sim q$) □

Mit dem Hilfssatz folgt aus $(*)$: $p_2 \cdots p_n = eq_2 \cdots q_m =: \tilde{q_2} q_3 \cdots q_m$. Durch Iteration bekommen wir schließlich $n = m$, und die Faktoren sind paarweise assoziert. □

**Bemerkung.** Variante der Zerlegung in irreduzible Faktoren: $R$ faktorieller Ring, $P$ Menge der irreduziblen Elemente von $R$. Auf $P$ haben wir die Äquivalenzrelation „assoziert“. Wir wählen einen Schnitt $S$ und können dann jedes $x \in R, \neq 0$ eindeutig schreiben als $x = e \cdot p_1 \cdots p_n$, mit $e \in R^\times$ und $p_i \in S$.

**Beispiel.** Beispiel: $R = \mathbb{Z}$, $\mathbb{Z}^\times = \{\pm 1\}$. Wir nehmen für $S$ die Menge der positiven Primzahlen $\Rightarrow n \in \mathbb{Z}, n = \operatorname{sgn}(n) \cdot \prod_{i=i}^{m} p_i$ (mit $e = \operatorname{sgn}(n)$)

## Thema IV: Ringe mit Teilerkettensatz

Einfacher ist die Charakterisierung der Ringe mit Teilerkettensatz für Ideale (sonst nur für Elemente).

**1.3.11 Satz.** *$R$ sei kommutativer Ring mit 1. Dann ist folgendes äquivalent:*

*(i) Jedes Ideal $I$ von $R$ lässt sich endlich erzeugen. Konkret: finde $a_1, \ldots, a_n \in R$, so dass $I = Ra_1 + \cdots + Ra_n$*

*(ii) In $R$ gilt der Teilerkettensatz für Ideale*

*(iii) In $R$ gilt die Maximalbedingung für Ideale. D.h.: in jeder nichtleeren Teilmenge von Idealen aus $R$ findet man bezüglich Inklusion ein maximales Element.*

*Beweis. (i)⇒(ii):* Sei $I_1 \subset I_2 \subset I_3 \subset \ldots$ eine aufsteigende Idealkette. Z.z.: Kette bricht ab. Betrachte $I = \bigcup_{v \geq 1} I_v$. Beh.: $I$ ist wieder ein Ideal.

$$\begin{aligned} a, b \in I &\Rightarrow a \in I_v, b \in I_{v'} \quad (\text{oBdA: } v \leq v' \\ &\Rightarrow a, b \in I_{v'} \Rightarrow a \pm b \in I_{v'} \subset \\ &\quad \forall r \in R : ra \in I_v \subset I \end{aligned}$$

Nach Voraussetzung ist jedes Ideal endlich erzeugt $\Rightarrow I = Ra_1 + \cdots + Ra_n$. Nach Konstruktion: $\forall i : a_i \in I_{v_i} \Rightarrow m = \max_i v_i \Rightarrow I_{v_m} = I$, weil $I_{v_i} \subseteq I_{v_m}\, \forall i$ und $a_i \in I_{v_i}$. Abbruch ($I_{v_n} = I_{v_m}, n \geq m$).

*(ii)⇒(iii):* klar. Sei $M$ nichtleere Teilmenge von Idealen. $I \in M \Rightarrow$ Entweder $I$ maximal oder finde $I' \in M$ mit $I \subset I'$. Dieses kann man nur endlich oft wiederholen wegen Teilerkettensatz $\Rightarrow$ *(iii)*.

*(iii)⇒(i):* Sei $I$ ein Ideal aus $R$. Sei $M$ die Menge der endlich erzeugten Ideale $J$, mit $J \subset I$. $M \neq \emptyset$, denn $a \neq 0, \in I \Rightarrow Ra \subset I$ und $Ra \in M$. Nach Voraussetzung: $M$ hat einen maximalen Vertreter $J$ und $J \subseteq I$. Annahme: $J \neq I \Rightarrow \exists a \in I : a \notin J \Rightarrow J + Ra$ ist maximal endlich erzeugt und $J + Ra \subset M \Rightarrow J + Ra \in M \Rightarrow J = J + Ra \Rightarrow a + J \lightning$. Also: $I = J$ endlich erzeugt. □

**1.3.12 Definition** (Noetherscher[3] Ring)**.** *Ein Ring mit den äquivalenten Eigenschaften (i) bis (iii) heißt* noetherscher Ring.

## 1.4 Euklidische Ringe

Generelle Voraussetzung: $R$ ist kommutativer Ring mit 1 und nullteilerfrei. Ein solcher Ring heißt *Integritätsbereich* (Vorbild $\mathbb{Z}$).

**1.4.1 Definition** (Euklidischer Ring)**.** *Ein Integritätsbereich $R$ heißt ein* euklidischer Ring*, falls es in $R$ eine Division mit Rest gibt. Das bedeutet genauer: es gibt eine Gewichtsfunktion $g : R - \{0\} \to \mathbb{N}_0 = \{0, 1, 2, \dots\}$ (nicht unbedingt surjektiv) mit:*

*(i) Wenn $a, b \in R - \{0\}$:*

$$g(ab) \geq g(a)$$

*(ii) Seien $a, b \in R, b \neq 0$. Dann besitzt $a$ immer eine Darstellung*

$$a = qb + r$$

*mit $r = 0$ oder $g(r) < g(b)$.*

**1.4.2 Beispiele.** a) $R = \mathbb{Z}$, $a \in \mathbb{Z} - \{0\} \mapsto g(a) = |a|$. Mit $g(ab) \geq g(a)$. Division mit Rest: $b \neq 0, a = qb + r, r = 0$ oder $0 < r < |b|$.

b) $R = K[X]$, Polynome mit Koeffizienten im Körper $R$ (dies ist sogar eine $K$-Algebra). $a = \sum a_i X^i \in R : g(a) = \deg(a) = max\{i | a_i \neq 0\}$ mit $g(ab) = g(a) + g(b) \geq g(a)$. Ist $b \neq 0, \in K[X]$, so gibt es $q, r \in K[X]$ mit $a = qb + r$, und $r = 0$ oder $\deg(r) < \deg(b)$.

**1.4.3 Satz.** *Sei $(R, g)$ ein euklidischer Ring. $a, b \in R, b \neq 0$. Dann gilt:*

*(i)* $b \mid a \Rightarrow g(b) \leq g(a)$

*(ii)* $b \mid a$ *echt* $\Rightarrow g(b) < g(a)$

*(iii)* $g(1_R) \leq g(a) \; \forall a \in R$

*(iv)* $g(a) = g(1_R) \Leftrightarrow a \in R^\times$*, also $a$ ist Einheit*

[3] EMMY NOETHER (1882-1935), Professorin in Göttingen, Begründerin der modernen Ringtheorie. Ihr Schüler BARTEL L. VAN DER WAERDEN veröffentliche 1930 *Moderne Algebra*, das auf den Göttinger Vorlesungen basiert.

*Beweis.* (i) klar nach Definition, dann $b \mid a \Rightarrow a = bq \Rightarrow g(a) \geq g(b)$

(ii) Sei $b \mid a$ echt $\Rightarrow a \nmid b \Rightarrow b = aq + r, r \neq 0$, mit $g(r) < g(a)$. Weiter ist $a = cb$, da $b \mid a \Rightarrow r = b - qa = b - qcb = (1 - qc)b \Rightarrow q(r) \geq g(b)$. Also folgt: $g(b) < g(a)$.

(iii) Denn $1 \mid a \; \forall a \in R$.

(iv) „$\Rightarrow$“: $g(a) \leq g(b), g(a) \geq g(b) \Rightarrow a \mid 1, 1 \mid a \Rightarrow a \in R^\times$.
„$\Leftarrow$“: $a \notin R^\times \Rightarrow 1 \mid a$ und $a \nmid b \overset{(ii)}{\Rightarrow} g(1) \neq g(a)$

□

**1.4.4 Hauptsatz.** *Jeder euklidische Ring ist nullteilerfreier Hauptring, und jeder nullteilerfreier Hauptidealring ist faktoriell.*

*Beweis.* $(R, g)$ sei euklidischer Ring, und $I$ ein Ideal von $R$. Suche $a \in I$ mit $g(a) = m$ ist minimal in $I$. Behauptung $I = Ra$. Sei $x \in I$ beliebig $\Rightarrow x = qa + r$. Annahme: $x \notin Ra \Rightarrow r \neq 0$ und $g(x) < g(a)$. Jedoch ist $r = x - qa \in I$, weil $x \in I$ und $qa \in I$. Dann ist $g(x) < m = g(a)$. Aber $g(a)$ ist minimal. ↯.

Sei nun $R$ nullteilerfreier Hauptring $\Rightarrow R$ ist noethersch $\Rightarrow$ Teilerkettenbedingung und jedes irreduzible Element ist prim (1.3.6) $\Rightarrow R$ faktoriell. □

*6. Vorlesung vom 24.11.2003*

Euklidische Ringe $\subset$ nullteilerfreier Hauptidealring $\subset$ faktorielle Ringe

**Zusatz.** $R$ sei nullteilerfreier Hauptidealring, $a_1, \ldots, a_n \in R$. Dann existieren $\mathrm{ggT}(a_1, \cdots, a_n)$ und $\mathrm{kgV}(a_1, \ldots, a_n)$ und sind eindeutig bis auf Assoziierte bestimmt.

$$\begin{aligned} d &= \mathrm{ggT}(a_1, \cdots, a_n) = \text{Linearkombination von } a_1, \ldots, a_n \\ d &\in Rd = Ra_1 + \cdots + Ra_n \end{aligned}$$

Wenn zusätzlich $(R, g)$ ein euklidischer Ring ist, dann können wir $g$ benutzen, um $d$ und eine Linearkombination $d = \alpha_1 a_1 + \cdots + \alpha_n a_n$ explizit mit dem euklidischen Algorithmus auszurechnen.

Für einen beliebigen Hauptidealring $R$ ist die Existenz einer Gewichtsfunktion $g$, so dass $(R, g)$ ein euklidischer Ring wird, ein offenes Problem.

## 1.5 Quotientenkörper und der Satz von Gauß

**1.5.1 Definition und Satz** (Konstruktion des Quotientenkörpers)**.** *Voraussetzung: $R$ sei ein Integritätsbereich, d.h. ein kommutativer, nullteilerfreier Ring mit* 1.

*Betrachte alle Paare $\frac{a}{b} := (a, b) \in R \times R \setminus \{0\}$ (d.h. $b \neq 0$). Dann ergibt sich eine Äquivalenzrelation:*

$$\frac{a}{b} \sim \frac{c}{d} \quad \Leftrightarrow \quad ad = bd \in R \qquad (b, d \neq 0)$$

*Die Menge der Äquivalenzklassen wird mit* $\mathrm{Quot}(R)$ *bezeichnet. Also ist $\left[\frac{a}{b}\right] = \{(c, d) \mid (c, d) \sim (a, b)\} \in \mathrm{Quot}(R)$ die Menge der Quotienten. Es gelten folgende*

*Operationen, und diese sind wohldefiniert (d.h. unabhängig von der Wahl der Repräsentanten) so dass $K = \mathrm{Quot}(R)$ ein Körper wird:*

$$\begin{aligned}
\left[\frac{a}{b}\right] \pm \left[\frac{c}{d}\right] &:= \left[\frac{ad \pm bc}{bd}\right] \\
\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] &:= \left[\frac{ac}{db}\right] \\
0_K := \left[\frac{0_R}{1_R}\right] & \qquad 1_K := \left[\frac{1_R}{1_R}\right] \\
\left[\frac{a}{b}\right]^{-1} := \left[\frac{b}{a}\right] \text{ ex.} &\quad \Leftrightarrow \quad a \neq 0
\end{aligned}$$

*Außerdem existiert eine natürliche Einbettung von $R$ in $\mathrm{Quot}(R)$, die verträglich ist mit allen Operationen:*

$$R \ni a \mapsto \left[\frac{a}{1_R}\right] \in \mathrm{Quot}(R)$$

*Beweis (nur zum Teil).* Die Relation ist transitiv:

$$\begin{aligned}
\frac{a}{b} \sim \frac{c}{d}, \frac{c}{d} \sim \frac{e}{f} &\Rightarrow ad = cb, cf = de \\
&\Rightarrow fad = fcb = deb \\
&\Rightarrow fa = be \quad \text{(da nullteilerfrei)} \\
&\Rightarrow \frac{a}{b} \sim \frac{e}{f}
\end{aligned}$$

Reflexivität und Symmetrie sind klar. □

**1.5.2 Satz** (Der Satz von Gauß)**.** *$R$ sei ein faktorieller Ring und $R[X]$ sei der Ring aller Polynome mit Koeffizienten aus $R$. Dann ist $R[X]$ ebenfalls ein faktorieller Ring.*

*Beweis.* 1. $R$ ist Integritätsbereich $\Rightarrow$ $R[X]$ ist ebenfalls Integritätsbereich.

$$\underbrace{\left(\sum_{i=1}^{n} a_i X^i\right)}_{\deg = n} \underbrace{\left(\sum_{j=1}^{m} b_j X^j\right)}_{\deg = m} = \underbrace{\cdots + a_n b_m X^{n+m}}_{\deg = n+m} \neq 0$$

denn $a_n \neq 0, b_m \neq 0 \Rightarrow a_n b_m \neq 0 \Rightarrow R[X]$ ist auch nullteilerfrei. ($\overset{1.3.6}{\Rightarrow}$ jedes Primelement ist irreduzibel)

2. $R$ faktoriell. Also ist $p \neq 0$ irreduzibel $\Leftrightarrow$ $p$ ist prim.

   *Behauptung:* $p$ hat als Element von $R[X]$ (als konstantes Polynom betrachtet) ebenfalls diese Eigenschaft.

   *Beweis:* Sei $(p) := R[X] \cdot p$ Ideal der Vielfachen von $p$, d.h. Polynome, deren Koeffizienten alle durch $p$ teilbar sind. $\Rightarrow$ Faktorring $R[X]/(p) \simeq (R/pR)[X]$. $p$ Primelement $\Rightarrow$ $R/pR$ ist nullteilerfrei $\Rightarrow$ $(R/pR)[X]$ ebenfalls nullteilerfrei $\Rightarrow$ $p$ ist Primelement in $R[X]$ und damit irreduzibel.

3. In einem faktoriellen Ring $R$ existieren (eindeutig bis auf Assozierte) das ggT und kgV von endlich vielen Elementen.

   *Beweis:* $a_1 = p_1 \cdots p_n, a_2 = q_1 \cdots q_m$ Zerlegung in Primfaktoren. Sei $p$ irgendein Primelement von $R$.

   Setze $\nu_p(a_i) =$ Anzahl der Faktoren in der Zerlegung, welche zu $p$ assoziert sind. Dann ist:

$$\begin{aligned} \mathrm{ggT}(a_1, a_2) &= \prod_{p \in \text{ Primelemente}/\sim} p^{\min(\nu_p(a_1), \nu_p(a_2))} \\ \mathrm{kgV}(a_1, a_2) &= \prod_{p \in \text{ Primelemente}/\sim} p^{\max(\nu_p(a_1), \nu_p(a_2))} \end{aligned}$$

   **Bemerkung.** Wenn $R$ kein Hauptidealring ist, dann wird im Allgemeinen $d = ggT(a_1, a_2)$ nicht aus $a_1$, $a_2$ linear kombinierbar sein, weil der Fall $Rd \subsetneq Ra_1 + Ra_2$ möglich ist.

4. **Definition (Inhalt, primitives Polynom).** Sei $a = \sum a_i X^i \in R[X]$. Dann ist

$$c(a) := \mathrm{ggT}(a_0, \ldots, a_n) \in R$$

   der *Inhalt*. Dann bekommen wir die Zerlegung

$$a = c(a) \frac{a}{c(a)}$$

   mit $\frac{a}{c(a)}$ ein Polynom mit Inhalt $\sim 1$. Es heißt dann *primitiv*. Die Zerlegung ist eindeutig bis auf Assozierte (also bis auf Einheiten).

5. **Bemerkung.** $a, b \in R[X] \Rightarrow c(ab) \sim c(a) \cdot c(b) \in R$. Insbesondere: wenn $a, b$ beide primitiv, dann ist auch $ab$ primitiv.

   Zum Beweis benutzt man: Ein Primelement $p \in R \subset R[X]$ teilt (in $R[X]$) das Polynom $a$ gdw. $p$ teilt (in $R$ den Inhalt $c(a)$.

6. Sei $R \subset K = \mathrm{Quot}(R) \Rightarrow R[X] \subset K[X]$ Einbettung der Polynomringe. Sei jetzt $f \in K[X]$. Dann gibt es ebenfalls eine „eindeutige“ Faktorisierung $f = c(f) \cdot \varphi$, wobei $c(f) \in K$ und $\varphi \in R[X]$ primitv.

$$\begin{aligned} f = \sum a_i X^i, a_i \in K \quad &\Rightarrow \quad a_i = \left[\frac{\alpha_i}{\beta_i}\right], \quad \alpha_i, \beta_i \in R \\ d := \prod_i \beta_i \quad &\Rightarrow \quad f = \frac{1}{d} \underbrace{df}_{\in R[X]} = \frac{c(df)}{d} \underbrace{\frac{df}{c(df)}}_{=:\varphi} \\ \Rightarrow c(f) \quad &= \quad \frac{c(df)}{d} \in K \end{aligned}$$

7. Die irreduziblen Elemente in $R[X]$. Sei $a = \sum a_i X^i \in R[X]$ irreduzibel. Dann gibt es folgende Möglichkeiten:

   - Typ I: $a = a_0$ eine Konstante, $a_0 \in R$ ist prim.

- Typ II: $\deg(a) > 0$, dann ist $a \in R[X]$ primitiv, und $a \in K[X]$ irreduzibel.

*Bemerkung.* $K[X]$ ist faktoriell, weil sogar ein euklidischer Ring.

*Beweis.* Für Typ I, trivial.

Typ II: $\deg(a) > 0 \Rightarrow a$ keine Konstante $\Rightarrow a = c(a) \cdot \varphi$ mit $\varphi$ primitiv. Falls nicht $c(a) \sim 1$, dann hätte $a$ echte Teiler in $R$ $\lightning\Rightarrow$ $a$ muss primitiv sein. Betrachte nun $a \in K[X]$. Annahme: $a = f \cdot g$ ist in $\mathbb{K}[X]$ reduzibel. Schreibe

$$\begin{aligned} f &= c(f)\varphi_f & c(f), c(g) &\in K \\ g &= c(g)\varphi_g & \varphi_f, \varphi_g &\in R[X] \end{aligned}$$

$$\begin{aligned} \Rightarrow \quad a &= fg = c(f)c(g)\varphi_f\varphi_g \\ c(a) &= c(fg) = c(f)c(g) \sim 1 \\ \Rightarrow \quad a &= \epsilon\varphi_f\varphi_g \in R[X] \text{ zerlegbar } \lightning \end{aligned}$$

*Also:* Irreduzible Elemente müssen vom Typ I oder II sein. Umgekehrt Jedes $a \in R[X]$ von Typ I oder II ist auch wirklich irreduzibel. □

8. Jedes irreduzible Element aus $R[X]$ ist Primelement.

*Beweis.* Für Typ I schon klar. Also sei $a \in R[X]$ irreduzibel vom Typ II. Dann ist $a \in K[X]$ ebenfalls irreduzibel, also Primelement von $K[X]$ (weil dieser Ring faktoriell ist). Seien nun $g, h \in R[X]$ und sei $a \mid gh$ in $R[X]$. $\Rightarrow a|gh$ in $K[X] \Rightarrow$ In $K[X]$ gilt $a \mid g$ oder $a \mid h$.

O.B.d.A $g = ab$ mit $b \in K[X] \Rightarrow g = a \cdot c(b) \cdot \beta$ mit $\beta \in R[X]$ primitiv. Jedoch $a$ ist primitiv(!) $\Rightarrow c(b) \sim c(g) \in R \Rightarrow b \in R[X]$. □

9. Um zu zeigen, dass $R[X]$ faktorieller Ring ist, müssen wir schließlich noch zeigen, dass der Teilerkettensatz für Elemente gilt. Das folgt aus: $a \in R[X]$, $a = c(a)\varphi$, $c(a) \in R$, $\varphi$ primitiv. $\Rightarrow$ Teiler sind inneres Produkt aus Teilern der Inhalts $c(a)$ in $R$ und Teilern des primitiven Polynoms $\varphi(X)$ in $R[X] \Rightarrow$ Endlich viele Möglichkeiten für eine Teilerkette.

□

*7. Vorlesung vom 01.12.2003*

**Beispiel.** $R = \mathbb{Z} \Rightarrow$ der Ring $\mathbb{Z}[X]$ ist ebenfalls faktoriell. Die irreduziblen Elemente in $\mathbb{Z}[X]$ sind für Typ I die Primzahlen $p$ = konstante Polynome. Für Typ II die Polynome $a = \sum_{i=1}^{n} a_i X^i, n > 0, a_n \neq 0$, die primitiv sind, d.h. $\mathrm{ggT}(a_0, \ldots, a_n) = 1$. In $\mathbb{Q}[X]$ ist $a$ irreduzibel.

$\mathbb{Z}[X]$ ist ein Beispiel für einen faktoriellen Ring, welcher kein Hauptidealring ist.

**Beispiel.** Sei $p$ eine Primzahl. Dann ist das Ideal $(p, X) := \mathbb{Z}[X] \cdot p + \mathbb{Z}[X] \cdot X$ kein Hauptideal.

*Beweis.* Wir wissen: $p$ ist irreduzibel vom Typ I $\Rightarrow$ Das Hauptideal $\mathbb{Z}[X]p$ ist ein maximales Hauptideal. Jedoch:

$$\underbrace{\mathbb{Z}[X] \supset (p, X)}_{\substack{\text{Quotient ist der Körper} \\ \text{mit } p \text{ Elementen}}} \supsetneq \mathbb{Z}[X]p$$

Noch zu zeigen: $(p, X)$ ist echtes Ideal.

$$\begin{aligned} & \mathbb{Z}[X]/\mathbb{Z}[X]p \cong \mathbb{F}_p[X] \\ \text{Ideal: } & (p, X)/\mathbb{Z}[X]p = I \to \mathbb{F}_p[X] \cdot X \\ \text{da} \quad & p \mapsto 0 \\ \Rightarrow \quad & \mathbb{Z}[X]/(p, X) \cong \mathbb{F}_p[X]/\mathbb{F}_p[X]X \\ & \cong \mathbb{F}_p \end{aligned}$$

Kriterium: Ideal $m$ in einem kommutativen Ring $R$ ist maximal genau dann, wenn $R/m$ ein Körper ist. Also: $\mathbb{Z}[X]p$ ist ein maximales Hauptideal, weil $p$ irreduzibel ist. $(p, X)$ ist ein maximales Ideal im „absoluten“ Sinne, weil der Quotientenring ein Körper ist. □

## 1.6 Polynomring in mehreren Variablen und Universalität

$R$ sei kommutativer Ring mit 1. Wir wollen den Polynomring $R[X_1, \ldots, X_n]$ in $n$ Variablen erklären. Dabei sei:

$$\begin{aligned} \mathbb{N}_0 &:= \{0, 1, 2, \ldots\} \\ \mathbb{N}_0^n \ni i &:= (i_1, \ldots, i_n) \quad \forall i_\nu \in \mathbb{N}_0 \\ \text{und} \quad |i| &:= \sum_{\nu=1}^{n} i_\nu \end{aligned}$$

**1.6.1 Definition** (Multipotenz, Grad)**.** *Die zu $i \in \mathbb{N}_0^n$ gehörige* Multipotenz *in $n$ Variablen sei:*

$$X^i := X_1^{i_1} \cdot X_2^{i_2} \cdots X_n^{i_n}$$

*Wir vereinbaren den* Grad *der Multipotenz:*

$$\deg(X^i) := |i| := \sum_{\nu=1}^{n} i_\nu$$

**1.6.2 Definition** (Polynomring $R[X_1, \ldots, X_n]$)**.** *Sei $R$ wie zu Anfang. Der Polynomring $R[X_1, \ldots, X_n]$ ist durch folgende Daten erklärt:*

*$R[X_1, \ldots, X_n]$ ist der $\infty$-dimensionale „$R$-Vektorraum“ ($R$ ist kein Körper!) mit den Multipotenzen $X^i$ als* Basen.

$$a \in R[X_1, \ldots, X_n] : a = \sum_{i \in \mathbb{N}_0^n} a_i X^i$$

*(nur endlich viele beteiligte Summanden $\neq 0$)*

*Addition:* $(a = \sum a_i X^i, b = \sum b_i X^i)$

$$a + b := \sum (a_i + b_i) X^i$$

*Skalar-Multiplikation:* $(\lambda \in R)$

$$\lambda a := \sum (\lambda a_i) X^i$$

*Multiplikation:*

$$X^i \cdot X^j := X^{i+j}$$

*mit*

$$\begin{aligned} i + j &= (i_1, \ldots, i_n) + (j_1, \ldots, j_n) \\ &:= (i_1 + j_1, \ldots, i_1 + j_n) \end{aligned}$$

*also*

$$X^{i+j} = X_1^{i_1+j_1} \cdots X_n^{i_n+j_n}$$

*Aus der Forderung der Distributivität ergibt sich dann notwendig:*

$$(\sum a_i X^i)(\sum b_i X^i) = \sum_{k \in \mathbb{N}_0^n} c_k X^k$$

*wobei* $c_k = \sum_{i+j=k \in \mathbb{N}_0^n} a_i b_i$

*Damit wird* $R[X]$ *zu einer „R-Algebra“ (wie K-Algebra, nur mit Ring).*

| | |
|---|---|
| *Nullelement* | $0 = \sum_i 0 X^i$ |
| *Einselement* | $1 = X^0 = X^{(0,\ldots,0)}$ |
| *R-Basis* | $X^i, i \in \mathbb{N}_0^n$ |

**Definition** ($m$-Form)**.** *Sei* $m \in \mathbb{N}_0$*. Als* $m$-Form *in n Variablen* $X_1, \ldots, X_n$ *bezeichnen wir ein Polynom* $\sum a_i X^i$*, wobei stets* $|i| = m$*, falls* $a_i \neq 0$*.*

**Folgerung.** *Jedes* $a \in R[X_1, \ldots, X_n]$ *lässt sich schreiben als Summe von Formen:*

$$a = \sum_{m \in \mathbb{N}_0} \Big( \sum_{\substack{i \in \mathbb{N}_0^n \\ |i| = m}} a_i X^i \Big)$$

**Beispiel.** Quadratische Polynome in $n$ Variablen = 2-Form + 1-Form + Konstante.

**1.6.3 Definition** ($R$-Modul, $R$-Aktion)**.** *Sei R kommutativer Ring mit* 1*.*

*Ein* $R$-Modul $M$ *ist eine Menge mit zwei Operationen:*

$$\begin{aligned} +&: M \times M \to M & (m_1, m_2) &\mapsto m_1 + m_2 \\ \cdot&: R \times M \to M & (r, m) &\mapsto rm \end{aligned}$$

*mit der Eigenschaft, dass* $(M, +)$ *eine abelsche Gruppe ist und die die Distributivgesetze gelten:*

$$(r_1 + r_2)m = r_1 m + r_2 m \quad \textit{und} \quad r(m_1 + m_2) = rm_1 + rm_2$$

$R$-Aktion*:*

$$(r_1 r_2)m = r_1(r_2 m) \quad \textit{und} \quad 1_R \cdot m = m$$

Ein Modul ist wie ein Vektorraum aufgebaut, hat aber als Skalarbereich einen kommutativen Ring mit Einselement statt einem Körper. Hauptunterschied zur Theorie der Vektorräume: *R-Moduln M haben im Allgemeinen keine Basis*. $R$-Moduln welche eine Basis besitzen heißen $frei$ (z.B. $R[X_1, \ldots, X_n]$).

**Beispiel** (nicht freier Modul)**.** Sei $I \subset R$ ein nicht triviales Ideal. Dann ist $R/I$ ein $R$-Modul, welches nicht frei ist. Offensichtlich ist $[1_R] \in R/I$ ein erzeugendes Element, denn für $r \in R$ gilt: $r[1_R] = [r \cdot 1_R] = [r]$. Es ergeben sich alle Elemente aus $R/I$. Aber $[1_R] \in R/I$ ist kein linear unabhängiges Element:

$$r \in I, r \neq 0 \quad \Rightarrow \quad r[1_R] = [r] = [0]$$

$[1_R]$ ist also erzeugendes Element, aber kein Basiselement.

**Definition** ($R$-Algebra $A$)**.** *(i) A ist ein R-Modul.*

*(ii) In A gibt es eine Multiplikation, wodurch A ein Ring wird.*

*(iii) Verträglichkeit der Multiplikation in A und der Multiplikation mit Skalaren $r \in R$:*

$$r(a \cdot_A b) = (ra) \cdot_A b = a \cdot_A (rb)$$

$R$-Modul = Verallgemeinerung des $K$-Vektoraums:

$$R\text{-Modul} \supset K\text{-Vektorraum}$$
$$R\text{-Algebra} \supset K\text{-Algebra}$$

**Beispiel.** $R[X_1, \ldots, X_n]$ ist Beispiel einer $R$-Algebra.

**Definition** (Kategorie, Morphismus)**.** *Wir betrachten zu unserem Ring R die* Kategorie $C_n(R)$ *aller kommutativen R-Algebren mit* 1 *und n markierten Elementen:*

$$C_n(R) \ni O = (A, a_1, \ldots, a_n)$$

*wobei A eine kommutative R-Algebra mit 1 und $a_1, \ldots, a_n \in A$ ein geordneten n-Tupel von Elemente sind. Sie müssen nicht einmal verschieden sein. Sei $O' = (B, b_1, \ldots, b_n)$. Ein* Morphismus $\phi : O \to O'$ *ist eine Abbildung $\phi : A \to B$ mit folgenden Eigenschaften:*

*(i) $\phi$ ist Homomorphismus von R-Algebren.*

*(ii) $\phi(1_A) = 1_B$*

*(iii) $\phi(a_i) = b_i \, \forall i \in \{1, \ldots, n\}$*

**1.6.4 Hauptsatz** (für Kategorien)**.** *Das Objekt $U = (R[X_1, \ldots, X_n], X_1, \ldots, X_n)$ ($X_1, \ldots, X_n$ = Elementvektor) ist* universelles Anfangsobjekt*, d.h. zu jedem beliebigen Objekt $O = (A, a_1, \ldots, a_n)$ gibt es genau einen Morphismus $\phi : U \to O$. Konkret ist $\phi$ die* Einsetzabbildung*:*

$$\phi(\sum r_i X^i) = \sum r_i a^i \in A$$

*wobei $a^i = a_1^{i_1} \cdots a_n^{i_n} \in A$.*

*Beweis.* $\phi$ existiert als Abbildung von $R$-Moduln, weil $R[X_1, \ldots, X_n]$ ein freier $R$-Modul ist, mit der Basis $X_i, i \in \mathbb{N}_0^n$. (Satz aus der linearen Algebra: Eine $R$-lineare Abbildung ist voll bestimmt, sobald die Werte der Basis-Vektoren gegeben sind, und hierfür hat man freie Wahl.) Wir benötigen:

$$1_{R[X_1,\ldots,X_n]} = X^{(0,\ldots,0)} \mapsto 1_A$$
$$X_\nu \mapsto a_\nu \quad \nu \in \{1, \ldots, n\}$$

Verträglichkeit mit Multiplikation:

$$X^i = X_1^{i_1} \cdots X_n^{i_n} \mapsto a^i = a_1^{i_1} \ldots a_n^{i_n} \qquad (*)$$

Damit wird $\phi : R[X_1, \ldots, X_n] \to A$ ein Morphismus von $R$-Moduln. Durch Zurückführung auf $(*)$ zeigt man, dass $\phi : R[X_1, \ldots, X_n] \to A$ ein Morphismus von $R$-Algebren ist, d.h. verträglich mit Multiplikation. □

*8.,9. Vorlesung vom 05.01.2004*

**Hauptsatz.** *(in anderer Formulierung) Der Polynomring $R[X1, \cdots, X_n]$ ist universales Anfangsobjekt in der Kategorie $C_n(R)$ aller kommutativen $R$-Algebren $A$ mit 1 und $n$ Markierungen.*

*Explizit: Sei $A$ eine $R$-Algebra mit 1, und seien $a_1, \cdots, a_n \in A$ fixiert (nicht notwendig verschieden). Dann gibt es genau einen Homomorphismus*

$$R[X_1, \ldots, X_n] \to A \quad \textit{so dass} \quad \begin{array}{l} 1 \mapsto 1 \\ x_i \mapsto a_i \quad \forall i = 1, \cdots, n \end{array}$$

*Man nennt diese Abbildung auch* E i n s e t z a b b i l d u n g.

**1.6.5 Hilfssatz.** *Sind $U, U'$ zwei universelle Anfangsobjekte in einer Kategorie $C$ dann folgt $U \simeq U'$ in $C$.*

*Beweis.* Weil $U$ universell ist, gibt es *genau eine* Abbildung $U \to U$ (Identität ist die einzige Möglichkeit). $U'$ sei ein zweites universelles Objekt

$$\Rightarrow \qquad \begin{array}{ll} U \to U' & \text{weil } U \text{ universell ist} \\ U' \to U & \text{weil } U' \text{ universell ist} \end{array}$$

Die Kombination beider Abbildungen muss jeweils die Indentität sein:

$$\Rightarrow U \simeq U'$$

□

**1.6.6 Folgerung.** *Für $n \geq 2$ ist*

$$(\cdots(R[X_1])[X_2])\cdots)[X_n]) \xrightarrow{\sim} R[X_1, \ldots, X_n]$$

*ein natürlicher Isomorphismus, welcher durch das Weglassen der Klammerung entsteht.*

*Beweis.* Zu Zeigen: Die Abbildung ist verträglich mit den Ringoperationen $(+, \cdot)$. Beweis durch Iteration, dann genügt es zu zeigen:

$$(R[X_1, \ldots, X_{n-1}])[X_n] \xrightarrow{\sim} R[X_1, \ldots, X_n] \tag{1}$$

Betrachte die Kategorie $C_1(R[X_1, \ldots, X_{n-1}])$ aller $R[X_1, \ldots, X_{n-1}]$-Algebren mit einer Markierung. Die linke Seite von (1) ist per Definition ein universelles Anfangsobjekt in dieser Kategorie. Es genügt zu zeigen, dass $(R[X_1, \ldots, X_n], X_n)$ ebenfalls ein universelles Anfangsobjekt ist.

Sei $(A, a) \in C_1(R[X_1, \ldots, X_{n-1}]$. Behauptung: Es gibt genau einen Homomorphismus $R[X_1, \ldots, X_n] \to A$ von $R[X_1, \ldots, X_{n-1}]$-Algebren mit der Eigenschaft $X_n \mapsto a$ und $1 \mapsto 1$. Höchstens eine Möglichkeit, nämlich ordne $f(X_1, \ldots, X_n)$ nach Potenzen von $X_n$, d.h.

$$\begin{aligned} f(X_1, \ldots, X_n) =& f_0(X_1, \ldots, X_{n-1}) + f_1(X_1, \ldots, X_{n-1}) X_n \\ &+ \cdots + f_r(X_1, \ldots, X_{n-1}) X_n^r \end{aligned}$$

Dann gibt es nur die Möglichkeit:

$$\begin{aligned} f(X_1, \ldots, X_n) \mapsto& f_0(X_1, \ldots, X_n) \cdot_A 1_A + f_1(X_1, \ldots, X_n) \cdot_A a \\ &+ \cdots + f_r(X_1, \ldots, X_n) \cdot_A a^r \\ =:& f(X_1, \ldots, X_n, a) \in A \end{aligned}$$

Behauptung: diese Abbildung ist tatsächlich ein Homomorphismus von $R[X_1, \ldots, X_n]$-Algebren. Setze: $\Lambda_n := R[X_1, \ldots, X_n]$. Dann ist zu zeigen:

$$(f \cdot_{\Lambda_n} g)(X_1, \ldots, X_n, a) = f(X_1, \ldots, X_n, a) \cdot_{\Lambda_n} g(X_1, \ldots, X_n, a)$$

$\Rightarrow (R[X_1, \ldots, X_{n-1}])[X_n] \simeq R[X_1, \ldots, X_n]$ (wegen Eindeutigkeit, siehe letzte Bemerkung) sogar als $R[X_1, \ldots, X_{n-1}]$-Algebren $\Rightarrow$ auch als $R$-Algebren. □

**1.6.7 Hilfssatz.** *(i) Wenn $R$ ein nullteilerfreier Ring, dann ist $R[X_1, \ldots, X_n] \simeq (\cdots (R[X_1])[X_2] \cdots)$ ebenfalls nullteilerfrei*

*(ii) Wenn $R$ faktoriell, dann ist $R[X_1, \ldots, X_n]$ auch faktoriell.*

*Beweis.* Durch Zurückführung auf Adjunktion einer Variablen. □

**1.6.8 Definition.** *Man nennt eine $R$-Algebra $A$ (mit 1)* erzeugt *durch die Elemente $a_1, \ldots, a_n$ falls die Einsetzabbildung* ev $: R[X_1, \ldots, X_n] \to A$, *mit $1 \mapsto 1$ und $X_i \mapsto a_i$, surjektiv ist.*

*Die Abbildung* ev *hat im Allgemeinen einen Kern, welcher ein Ideal im Polynomring $R[X_1, \ldots, X_n]$ ist. Man nennt es* Relationenideal, *und erzeugende Elemente dieses Ideals werden als* erzeugende Relationen *bezeichnet.*

**Folgerung.** *Wenn $I = \ker(\text{ev}) = (f_1(X_1, \ldots, X_n), \ldots, f_r(X_1, \ldots, X_n))$, dann sind*

$$\begin{aligned} f_1(a_1, \ldots, a_n) &= 0 \qquad \in A \\ &\vdots \\ f_n(a_1, \ldots, a_n) &= 0 \qquad \in A \end{aligned}$$

*die erzeugenden Relationen der Algebra $A$.*

**Bemerkung.** Fall $R = \mathbb{Z}$. Dann ist jede kommutative Gruppe ein $\mathbb{Z}$-Modul, und jeder kommutative Ring mit 1 ist eine $\mathbb{Z}$-Algebra. $(G, +)$ kommutative Gruppe:

$$\left.\begin{array}{ll} \mathbb{Z} \ni n > 0: & n \cdot g := \underbrace{g + \cdots + g}_{n\text{-mal}} \\ \mathbb{Z} \ni n < 0: & n \cdot g := (-n) \cdot (-g) \end{array}\right\} \Rightarrow G \text{ ist } \mathbb{Z}\text{-Modul}$$

# 1.7 Moduln über Hauptidealringen

## 1.7.1 Die Smithsche Normalform einer Matrix.

Wir betrachten folgende Typen von Ringen:

a) Integritätsbereich (nullteilerfrei, kommutativ, mit 1)

b) Integritätsbereich und Hauptidealring (jedes Ideal ist Hauptideal)

Wir analysieren Matrizen $A \in R^{m \times n}$. Spezialfall $m = n \Rightarrow R^{n \times n}$ ist ein nichtkommutativer Ring mit üblicher Matrizenmultiplikation. $\mathrm{GL}_n(R) := (R^{n \times n})^\times$ ist die Einheitengruppe dieses Ringes.

**1.7.1 Hilfssatz.** *Sei $A \in R^{n \times n}$ eine quadratische Matrix. Dann ist $A$ genau dann invertierbar (d.h. $A \in \mathrm{GL}_n(R)$), wenn* $\det(A) \in R^\times$ *(Einheit im Ring $R$).*

*Beweis.* Wenn $A$ invertierbar ist, dann finde $B \in R^{n \times n}$ so dass

$$A \cdot B = B \cdot A = I_n = \begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix}$$

$$\Rightarrow \det(A) \cdot \det(B) = \det(A \cdot B) = \det I_n = 1_R$$

$$\Rightarrow \det(A), \det(B) \text{ ist Einheit}$$

Umgekehrt sei $\det(A) \in R^\times$. Wir bilden die Adjunkte Matrix $A^\#$ (Transponierte der Kofaktormatrix, Bildung ohne Division). Wie üblich gilt dann:

$$A \cdot A^\# = A^\# \cdot A = \det(A) \cdot I_n$$

$\Rightarrow$ wenn $\det(A) \in R^\times$ dann können wir $\det(A)$ ausdividieren:

$$A^{-1} = \frac{1}{\det(A)} \cdot A^\#$$

□

**Beispiele.** (i) $R = \mathbb{Z}, A \in \mathbb{Z}^{n \times n}$. $A$ ist genau dann invertierbar, wenn $\det A = \pm 1$. Falls $\det A \neq 0$, dann ist $A$ invertierbar als $A \in \mathbb{Q}^{n \times n}$.

(ii) Wenn $R$ ein Körper, dann ist $R^\times = R \setminus \{0\} \Rightarrow A$ invertierbar $\Leftrightarrow \det A \neq 0$.

(iii) $A \in R^{n \times n}$: dann bedeutet $\det A \neq 0$, dass die Abbildung $R^{n \times 1} \to R^{n \times 1}$, $v \mapsto Av$ injektiv, aber im Allgemeinen nicht surjektiv ist (Übung).

**1.7.2 Definition** (Äquivalenzrelationen auf $R^{m\times n}$)**.** *Wir nennen $A, B \in R^{m\times n}$ ä q u i v a l e n t, falls invertierbare Matrizen $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ existieren mit*

$$B = PAQ$$

*Beweis.* Dies ist eine Äquivalenzrelation:

(i) *Reflexivität:* $A \sim A$, dann $P = I_m$, $Q = I_n$

(ii) *Symmetrie:* $A \sim B \Rightarrow B = PAQ \Rightarrow A = P^{-1}BQ^{-1} \Rightarrow B \sim A$

(iii) *Transitivität:* $C \sim B \sim A \Rightarrow C = P'BA', B = PAQ \Rightarrow C = P'PAQQ' = P''AQ'' \Rightarrow C \sim A$

□

Die Smithsche Normalform ist ein ausgezeichneter Vertreter in einer Äquivalenzklasse.

**1.7.3 Hauptsatz** (Smithsche[4] Normalform)**.** *Es sei $R$ ein Hauptidealring, und $A \in R^{m\times n}$. Dann ist $A$ stets äquivalent zu einer Diagonalmatrix*

$$D = (d_1, \ldots, d_r) := \begin{pmatrix} d_1 & & & & & 0 \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix} \in R^{m\times n}$$

*mit $d_1 \mid d_2 \mid \cdots \mid d_r$. Dabei sind die Zahlen $d_1, \ldots, d_r$ eindeutig bis auf Assoziierte bestimmt. Insbesondere ist $r$ (Anzahl der von 0 verschiedenen Einträgen) eindeutig bestimmt und heißt* R a n g *von $A$.*

Zur Charakterisierung der Einträge $d_i$:

**Definition** (Minor)**.** *Sei $A \in R^{m\times n}$, und $k \leq \min\{m, n\}$. Wähle in $A$ $k$ Zeilen und $k$ Spalten aus, und bilde die $k \times k$-Matrix der zugehörigen Kreuzungspunkte. Die Determinante dieser Matrix heißt* $k$ - M i n o r *von $A$.*

Sei $D_k = D_k(A)$ der ggT aller $k$-Minore der Matrix $A$ (eindeutig bis auf Assoziierte). Dann gilt: $d_1 = D_1$ und $d_1 \cdots d_k = D_k (\forall k \geq 2)$

$$\begin{aligned} \Rightarrow d_1 &= \mathrm{ggT}(\text{alle Koeffizienten von } A) \\ d_k &= \frac{D_k(A)}{D_{k-1}(A)} \end{aligned}$$

**Bemerkung.** Jeder $k$-Minor ist Linearkombination von $(k-1)$-Minore. Jede Zahl, welche alle $(k-1)$-Minore teilt, teilt auch alle $k$-Minore. Der Rang $r$ ist charakterisiert als Maximum aller $k$, so dass $A$ einen von 0 verschiedenen $k$-Minor besitzt.

[4] HENRY JOHN STEPHEN SMITH (1826-83), Professor in Oxford

**1.7.4 Definition** (Invariante Teiler, Determinantenteiler)**.** *Man nennt $d_1, \ldots, d_r$ die* invarianten Teiler *von $A$ (manchmal auch* Elementarteiler*) und $D_1, \ldots, D_k$ die* Determinantenteiler *von $A$. (Denn wenn $A \in R^{n\times n} \Rightarrow D_n(A) = \det(A)$.)*

*Beweis des Hauptsatzes im Fall, dass $(R, g)$ ein euklidischer Ring ist.* Für allgemeine Hauptidealringe ist unklar, ob eine Gewichtsfunktion existiert. Deswegen braucht man dann eine Variante (folgt später).

Wir müssen $A \in R^{m\times n}$ durch eine Folge elementarer Zeilen- und Spaltenoperationen auf die gewünschte Form bringen. Elementare Zeilenoperationen sind:

(i) Multiplikation einer Zeile von $A$ mit einer Konstante $\lambda \in R^\times$ (so dass inverse Operation existiert)

(ii) Vertauschung von zwei Zeilen

(iii) Zeile $i$ ersetzten durch Zeile $i + \lambda \cdot$ Zeile $j$ ($i \neq j, \lambda \in R$)

Elementare Spaltenoperationen entsprechen (i), (ii) und (iii). Sind $Z$ und $S$ Zeilen– bzw. Spaltenoperationen, dann gilt:

$$Z(A) = Z(I_m) \cdot A \qquad\qquad S(A) = A \cdot S(I_n)$$

**Verfahren.** $A =$ Nullmatrix ist trivial. Also sei $A \neq 0$. Strategie zum Erreichen der Form:

$$P_0 A Q_0 = \left(\begin{array}{c|ccc} a_1 & 0 & \ldots & 0 \\ \hline 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{array}\right), \quad a_1 \neq 0$$

**1. Schritt.** Suche unter Einträgen $a_{i,j} \neq 0$ eines mit Minimalgewicht $g$ und bringe dieses Element durch Vertauschung der Zeile und Spalte auf Platz $(1, 1)$.

Also nun: $a_{1,1} \neq 0$, und das Gewicht von $a_{1,1}$ ist minimal.

**2. Schritt.** Eintrag in erster Spalte: $a_{i,1} \neq 0, i \geq 2$ (sonst fertig mit Spalte). Division mit Rest ergibt: $a_{i,1} = q a_{1,1} + r$ mit

$$r = 0 \tag{a}$$
$$\text{oder } g(r) < g(a_{1,1}) \tag{b}$$

Im Fall (a) nutze Zeilenoperation (iii) um $a_{i,1}$ zu löschen

(b) nutze (iii) um $a_{i,1}$ mit $g(a_{i,1}) < g(a_{1,1})$ zu erzeugen. Dann zurück zu Schritt 1.

Da $g$ nach unten beschränkt ist, entfällt spätestens bei $a_{1,1} = 1$ Fall (b).

**3. Schritt.** Entsprechend mit erster Zeile.

Schwierigkeit: bei (b) mus man eine Spalte ganz nach vorne bringen, und dabei kann man die erste Spalte wieder zerstören. Aber trotzdem wird das Gewicht von $a_{1,1}$ stetig kleiner, so dass irgendwann für Spalten– und Zeilenoperationen Alternative (b) entfällt. (Wenn $R$ ein Körper ist, dann benutze Division ohne Rest, d.h. (b) entfällt immer.)

Nun: $A_1$ = Nullmatrix, dann fertig. $A_1 \neq 0$, dann finde:

$$P_1 A_1 Q_1 = \left(\begin{array}{c|ccc} a_2 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{array}\right)$$

denn

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P_1 \end{array}\right) P_0 A Q_0 \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q_1 \end{array}\right) = \left(\begin{array}{cc|c} a_1 & & \\ & a_2 & \\ \hline & & A_2 \end{array}\right)$$

usw. So wird also Diagonalform erreicht:

$$P' A Q' = \begin{pmatrix} a_1 & & & & & 0 \\ & \ddots & & & & \\ & & a_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$$

Jetzt brauchen wir noch $a_1 \mid a_2 \mid \cdots \mid a_r$. Alternativen:

(a) $a_1$ teilt alle übrigen Einträge $a_i$

(b) Reduziere durch Vertauschung $a_1$ mit kleinerem Gewicht

Sei z.B.: $a_1 \nmid a_2$. Durch Vertauschung können wir erst

$$g(a_1) \leq g(a_2) \leq \cdots \leq g(a_r)$$

erreichen. Betrachte

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \sim \begin{pmatrix} a_1 & a_2 \\ 0 & a_2 \end{pmatrix} \overset{q-II}{\sim} \begin{pmatrix} a_1 & r \\ 0 & a_2 \end{pmatrix} \overset{\text{Sp.}}{\sim} \begin{pmatrix} r & a_1 \\ a_2 & 0 \end{pmatrix}$$

mit $a_2 = q a_1 + r, g(r) < g(a_1)$. Das vorherige Verfahren ergibt:

$$\sim \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}, \quad g(a_1') \leq g(r) < g(a_1)$$

$\Rightarrow$ Gewicht von $a_{1,1}$ wird immer kleiner
$\Rightarrow$ irgendwann teilt $a_{1,1}$ alle $a_{i,i}$
Wiederhole für $a_2$, für $a_3$, ... (Dabei bleibt $a_1 \mid a_i$ erhalten, da Linearkombination)

Schließlich: $\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_r \end{pmatrix} \sim \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ mit $d_1 \mid d_2 \mid \cdots d_r$.

Also $A \sim \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ 0 & & & & \ddots \end{pmatrix}$ eine Smith-Normalform

□

**Beispiel** (H.J.S. Smith 1861: $R = \mathbb{Z}$)**.**

$$\begin{pmatrix} -14 & 10 \\ 24 & -24 \end{pmatrix} \overset{\text{1) Sp.}}{\sim} \begin{pmatrix} 10 & -14 \\ -24 & 24 \end{pmatrix} \overset{\text{b) Sp. rest}}{\sim} \begin{pmatrix} 10 & -4 \\ -24 & 0 \end{pmatrix} \overset{\text{1) Sp.}}{\sim} \begin{pmatrix} 4 & 10 \\ 0 & -24 \end{pmatrix}$$
$$\sim \begin{pmatrix} 4 & 2 \\ 0 & -24 \end{pmatrix} \overset{1)}{\sim} \begin{pmatrix} 2 & 4 \\ -24 & 0 \end{pmatrix} \overset{\text{1) Div. Sp.}}{\sim} \begin{pmatrix} 2 & 0 \\ -24 & 48 \end{pmatrix}$$
$$\overset{\text{a) Div. Z.}}{\sim} \begin{pmatrix} 2 & 0 \\ 0 & 48 \end{pmatrix}$$

Im Fall $R = \mathbb{Z}$, $PAQ = D$ und $\det P = \det Q \in \{\pm 1\}$. Im quadratischen Fall ist dann $\det A = \pm \det D$. Im Beispiel:

$$\begin{aligned} d_1 &= \mathrm{ggT}(-14, 10, 24, -24) = 2 \\ d_1 d_2 &= \det \begin{pmatrix} -14 & 10 \\ 24 & -24 \end{pmatrix} = 4 \cdot 24 \\ \Rightarrow d_2 &= 2 \cdot 24 = 48 \end{aligned}$$

**Variante.** Wenn $R$ ein Hauptidealring ohne geeignete Gewichtsfunktion ist. Sei $x \in R$. Als Ersatz für die Gewichtsfunktion nehmen wir:

$$d(x) := \begin{cases} 0 & \text{wenn } x \in R^\times \\ \text{Anzahl der irreduziblen Faktoren von } x & x \notin R^\times, \neq 0 \end{cases}$$

*Spezialfall:* $A = (u, v) \in R^{1\times 2}$ mit der Eigenschaft $u \nmid v$ *Behauptung:* Wir können $(u, v) \cdot Q = (t, 0), t = \mathrm{ggT}(u, v)$ erreichen.

Benutze: Ideal $(u, v) = Ru + Rv = Rt$ ist Hauptidealring. $u = ta, v = tb$ und $t$ ist Linearkombination von $u$ und $v$:

$$\begin{aligned} \Rightarrow \quad & t = ud - vc \qquad d, c \in R \\ \Rightarrow \quad & t = tad - tbc \\ \Rightarrow \quad & 1 = ad - bc \end{aligned}$$

$R$ ist nullteilerfrei. Offensichtlich ist $(u, v) = (t, 0) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) =: (t, 0) \cdot Q'$ und $\det Q' = 1$. Also ist $Q'$ in $R$ invertierbar.

*Verallgemeinerung:* $(u, *, \ldots, *, v, *, \ldots, *) \cdot Q = (t, *, \ldots, *, 0, *, \ldots, *)$, wobei $t = \mathrm{ggT}(u, v)$ und wiederum $\det Q = 1$. Schließlich betrachte anstelle der Zeile $(u, *, \ldots, *, v, *, \ldots, *)$ eine Matrix $A$ weelche $(u, *, \ldots, *, v, *, \ldots, *)$ als

*erste* Zeile hat. Dann erreichen wir durch $AQ$ eine Matrix mit der erste Zeile $(t, *, \ldots, *, 0, *, \ldots, *)$, denn es gilt:

$$\text{Zeile1}(AQ) = \text{Zeile1}(A) \cdot Q$$

Wir können dann noch eine vierte Elementaroperation einführen:

(iv) ersetze die erste Zeile von $A$ $(a_{1,1}, *, a_{1,i}, *)$ durch $(\text{ggT}(a_{1,1}, a_{1,i}), *, 0, *)$

Entsprechend kann man auch eine Sptaltenoperation (iv) einführen. Sie wird realisiert durch geeignete Multiplikation $P \cdot A$.

Nun Alternative: benutze Operation (iii) für Einträge $a_{i,1}$ bzw. $a_{i,1}$ (wenn $a_{1,1} \mid a_{i,1}$ bzw. $a_{1,1} \mid a_{1,i}$) oder wir benutzen Operation (iv), dabei wird $d(a_{1,1})$ kleiner. Strategie: Verkleinere $d(a_{1,1})$ bis Operation (iv) nicht mehr gebraucht wird $\Rightarrow$ es liegt Teilbarkeit vor.

Bemerkung: Wir haben nur die Operationen (ii), (iii) und (iv) benutzt.

$\Rightarrow$ Wir erreichen die Smithsche Form bereits mit Matrizen $P, Q$, welche die Determinante $\pm 1$ haben: $D = PAQ$.

*10.,11. Vorlesung vom 12.01.2004*

Noch zu zeigen: Die Einträge $d_1, d_2, \ldots$ sind bis auf Assozierte eindeutig:

$\epsilon_1, \ldots, \epsilon_m \in R^\times, P = \begin{pmatrix} \epsilon_1 & & \\ & \ddots & \\ & & \epsilon_m \end{pmatrix} \in R^{m \times m}$

$$PA = \begin{pmatrix} \epsilon_1 d_1 & & & 0 \\ & \ddots & & \\ & & \epsilon_r d_r & \\ 0 & & & 0 \end{pmatrix}$$

**1.7.5 Hilfssatz.** *Sei $AB \in R^{l \times n}$ Produkt von 2 Matrizen (beachte Formatregel). Behauptung: Jeder k-Minor lässt sich schreiben als Linearkombination von k-Minoren des ersten oder auch des zweiten Faktors.*

$k$-Minor von $M$ = Matrix. Wähle $k$ Zeilen und $k$ Spalten. Betrachte die Matrix, welche aus den Kreuzungspunkten besteht. $k$-Minor := Determinante einer solchen Matrix. Anwendung des Lemmas: $D = PAQ$.

$$\begin{aligned} k\text{-Minor von P(AQ)} &= \text{Linearkombination von } k\text{-Minoren von } AQ \\ k\text{-Minor von AQ} &= \text{Linearkombination von } k\text{-Minoren von } A \\ \Rightarrow \quad k\text{-Minor von D} &= R\text{-Linearkombination von } k\text{-Minoren von } A \end{aligned}$$

da: $A = P^{-1}DQ$

$$\Rightarrow \quad k\text{-Minor von } A = R\text{-Linearkombination von } k\text{-Minoren von } D$$

Also: Die $k$-Minoren von $A$ und die $k$-Minoren von $D$ erzeugen im Ring $R$ dasselbe Ideal $(D_k) = R \cdot D_k$. $D_k$ ist eindeutig bis auf Assozierte und hat die Eigenschaft:

$$\begin{aligned} D_k &= \text{ggT der } k\text{-Minoren von } A \\ &= \text{ggT der } k\text{-Minoren von } D \end{aligned}$$

Wenn der $k$-Minor von $D$ zu einer Matrix gehört, welche eine von $D$ abweichende Hauptdiagonale hat, dann muss er $= 0$ sein.

**Beispiel.** 2-Minor von $D$, Spalten 1 und 3, Zeile 1 und 2.

$$D = \begin{pmatrix} d_1 & & \\ & d_2 & \\ & & d_3 \end{pmatrix} \qquad \begin{vmatrix} d_1 & 0 \\ 0 & 0 \end{vmatrix} = 0$$

Es bleiben diejenigen Fälle, wo der $k$-Minor dieselbe Hauptdiagonale hat wie $D$:

$$\Rightarrow \qquad k\text{-Minor} = \det \begin{pmatrix} d_{i_1} & & 0 \\ & \ddots & \\ 0 & & d_{i_k} \end{pmatrix} = d_{i_1} \cdots d_{i_k}$$

$$\Rightarrow \qquad D_k = D_k(A) = \mathrm{ggT}(d_{i_1}, \ldots, d_{i_k}$$

mit $k$ ausgewählten Indizes $i_1 < \cdots < i_k$. Jedoch:

$$d_1 \mid d_2 \mid \cdots \mid d_r \Rightarrow d = d_1 \cdots d_k \text{ teilt alle } k\text{-fachen Produkte}$$

Ergebnis: $D_k \sim d_1 \cdots d_k \sim D_k(A)$

$$d_1 \sim D_1(A) \qquad\qquad d_k \sim \frac{D_k(A)}{D_{k-1}(A)}$$

eindeutig durch $A$ bestimmt.

Ist $R$ ein Körper $\Rightarrow$ Wenn $d_i \neq 0$ dann ist $d_i \sim 1$

$$\Rightarrow D = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & & 1 \\ 0 & & 0 \end{pmatrix}$$

**1.7.6 Folgerung.** *$A \in R^{m\times n}$ und $m < n$, dann hat das System $AX = 0$ nicht triviale Lösungen $X \in R^{n\times 1}$.*

*Beweis.* Finde $P, Q$ invertierbar, mit

$$PAQ = D = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ 0 & & & \ddots \end{pmatrix}$$

Es gilt $r < \min(m, n) < n$. Deshalb folgt:

$$\begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ 0 & & & \ddots \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ * \\ \vdots \\ * \end{pmatrix} \begin{matrix} \\ \\ \}m \\ \\ \\ \\ \end{matrix} = D \cdot Y = 0$$

hat offensichtlich nicht triviale Lösungen

$$\begin{aligned} P^{-1}| \qquad & PAQY = 0 \\ & AQY = 0 \\ \Rightarrow \qquad & AX = 0 \end{aligned}$$

mit $X = QY$. $QY \neq 0$, weil $Y \neq 0$ und $Q$ invertierbar ist. □

### 1.7.2 Moduln über Hauptidealringen

Ziele: a) Smithsche NF $\Rightarrow$ Informationen über $R$-Moduln (Anwendung)

b) Wir betrachten die Spezialfälle:

- $R = \mathbb{Z}$: Informationen über $\mathbb{Z}$-Moduln = kommutative Gruppen
- $R = K[X]$: Aussagen über NF von Matrizen (insbesondere Jordansche NF)

**1.7.7 Grundbegriffe über $R$-Moduln.** Zunächst sei $R$ kommutativer Ring mit 1.

1) $R$-*Modul* ist das Analogon eines $K$-Vektorraumes
2) $M$ ein $R$-Modul $\Rightarrow$ Begriffe wie:
   - *Untermodul* $N \subset M$
   - *Faktormodul* $M/N$
     ($N \subset M, m\ m' \Rightarrow m - m' \in N$, dann: $M/N$ = Menge der Äquivalenzklassen ist in natürlicher Weise ein $R$-Modul)
3) Wir können den Ring selbst als $R$-(Links)Modul betrachten $\Rightarrow$ Untermodule von $R$ sind dasselbe wie *Ideale* von $R$.
4) Sei $S \subset M$ eine Teilmenge eines $R$-Moduls $M$:
   - Man kann wie üblich den *Spann* von $S$, bilden. Das ist der von $S$ erzeugt Untermodul.
   - Die Menge $S$ heißt *linear unabhängig*, falls sich $0 \in M$ nur als die triviale Linearkombination von $S$ realisieren lässt, anderenfalls linear abhängig.
   - $S$ heißt *Basis* von $M$, falls $S$ ein *Erzeugendensystem* aus linear unabhängigen Elementen ist.
   - Im Allgemeinen besitzt ein $R$-Modul keine Basis.
     Beispiel: $R \supset I =$ Ideal, $R/I$ betrachtet als $R$-Modul hat keine Basis. $[1] \in R/I$ ist zwar erzeugendes Element, aber $[1]$ ist nicht linear unabhängig: $\lambda \in I, \lambda \neq 0 \Rightarrow \lambda[1] = [0]$

**Definition.** *$R$-Moduln $M$, welche eine Basis besitzen nennt man* frei.

**Bemerkung.** Wenn $M$ frei ist, mit Basis $S$, dann ist $M \cong R^{n\times 1}$, wobei $n = \#S$, und $m \mapsto [m]_S = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$ ist der Koordinatenvektor, falls $m = \lambda_1 s_1 + \cdots + \lambda_n s_n$.

**1.7.8 Satz.** *Sei $R$ ein Hauptidealring, und der $R$-Modul $M$ habe $n$ Erzeugende $\nu_1, \ldots, \nu_n$. Dann sind $n+1$ Elemente stets linear abhängig.*

*Beweis.* $A \in R^{n\times(n+1)} \Rightarrow \exists X \neq 0 : AX = 0$

$$\begin{aligned} (w_1, \ldots, w_{n+1}) &= (\nu_1, \ldots, \nu_n) \cdot A \qquad | \cdot X \\ \Rightarrow (w_1, \ldots, w_{n+1}) \cdot X &= (\nu_1, \ldots, \nu_n) \cdot A \cdot X \\ &= 0 \end{aligned}$$

□

**1.7.9 Folgerung** (Rang). *Sei $M$ ein endlich erzeugter freier $R$-Modul. Dann haben alle Basen $S$ von $M$ die selbe Kardinalzahl.* $\mathrm{Rang}(M) =$ *Kardinalzahl*

Unterschied zur Theorie der $K$-Vektorräume: Sei $V$ ein $K$-VR, $\dim_K(V) = m$. Dann haben alle Unterräume eine echt kleinere Dimension.

**Beispiel.** $\mathbb{Z}$-Moduln:

$$\begin{array}{c} \mathbb{Z} \times \mathbb{Z}\text{– freier Modul von Rg} = 2 \\ \Downarrow \\ (5\mathbb{Z}) \times (7\mathbb{Z})\text{– freier Modul von Rg} = 2 \end{array}$$

**1.7.10 Satz.** *Sei $R$ ein Hauptidealring, und seien $V, W$ zwei endlich erzeugte freie $R$-Moduln. Dann gilt:*

*(i) sind $B = (b_1, \ldots, b_n)$ von $V$ und $C = (c_1, \ldots, c_m)$ von $W$ zwei* fixierte Basen*, dann können wir jeder $R$-linearen Abbildung $\phi\colon V \to W$* eindeutig *eine Koordinatenmatrix $[\phi]_{C,B}$ zuordnen. Charakterisierung von $[\phi]_{C,B}$:*

$$[\phi]_{C,B} \cdot [v]_b = [\phi(v)]_C \quad \forall v \in V$$

*d.h.: j-te Spalte $[\phi]_{C,B} = [\phi(b_j)]_C$*

*(ii) zu gegebenen $\phi \in \mathrm{Hom}_R(V, W)$ kann man die Basen $B, C$ immer so finden, dass*

$$[\phi]_{C,B} = D = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_{m'} & \\ 0 & & & 0 \end{pmatrix} \qquad m' \leq min\{m, n\}$$

*d.h.*

$$\phi(b_i) = \begin{cases} d_i e_i & \text{falls } i \leq m' \\ 0 & \text{falls } i > m' \end{cases}$$

*(iii) Sei $A = [\phi]_{C',B'}$, $B', C'$ Basen von $V$ bzw. $W$, und sei $P \in \mathrm{GL}_m(R), Q \in \mathrm{GL}_n(R) \Rightarrow$*

$$\begin{array}{c} P \cdot [\phi]_{C',B'} \cdot Q = [\phi]_{C'P^{-1},B'Q} \\ C' = (c'_1, \ldots, c'_m) \mapsto C'P^{-1} \end{array}$$

*Beweis.* (i) klar.

(ii)/(iii): $\phi\colon V \to W$ gegeben. Finde $P, Q$ mit $PAQ = D$ (Smith. NF). Gehe über von $B', C'$ zu den Basen $B = B'Q$ und $C = C'P^{-1}$. Dann gilt:

$$\begin{array}{cc} Q = [1]_{B',B} & P^{-1} = [1]_{C',C} \Rightarrow P = [1]_{C,C'} \\ \multicolumn{2}{c}{D = PAQ = [1]_{C,C'} \cdot [\phi]_{C',B'} \cdot [1]_{B',B} = [\phi]_{C,B}} \end{array}$$

□

**Bemerkung.** Moduln über Hauptidealringen sind reichhaltiger als Vektorräume:

a) es gibt Moduln, welche nicht frei sind

b) es gibt Inklusionen $N \subset M$ von Moduln desselben Ranges.

Klassifizierung der endlich erzeugten $R$-Moduln unter Benutzung der Smithschen Normalform:

**1.7.11 Folgerung.** *(i) Sei $\phi\colon V \to W$ $R$-linear, und $V$, $W$ seien frei, vom Rang $n$ bzw. $m$. Dann existiert eine Basis $C = (c_1, \ldots, c_m)$ von $W$ und Skalare $d_1 \mid d_2 \mid \cdots \mid d_n \in R$, so dass* Bild$(\phi)$ *ein freier $R$-Modul mit den Erzeugenden $d_1c_1, \ldots, d_{m'}c_{m'}$ ist.*

*(ii) Jeder Untermodul $M$ eines freien Moduls $W$ vom Rang $m$ ist wieder frei und hat einen Rang $\leq m$.*

*Beweis.* (i) Finde Basen $B$ und $C$, so dass

$$[\phi]_{C,B} = D = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_{m'} & \\ 0 & & & 0 \end{pmatrix}$$

$\Rightarrow$ Bild$(\phi)$ wird erzeugt durch $d_1c_1, \ldots, d_{m'}c_{m'}$. Da $c_1, \ldots, c_m$ linear unabhängig $\Rightarrow$ Vielfache $d_1c_1, \ldots, d_{m'}c_{m'}$ sind auch linear unabhängig (weil $R$ nullteilerfrei). □

Zum Beweis von *(ii)* benötigen wir (ohne Beweis):

**1.7.12 Hilfssatz** (E)**.** *Sei $R$ ein noetherscher Ring (jedes Ideal ist endlich erzeugt). Sei $M$ ein $R$-Modul. Dann ist jeder Untermodul $N \subseteq M$ ebenfalls endlich erzeugt.*

**Bemerkung.** Wenn für $R$ die Eigenschaft $(E)$ gilt, dann nimm $M = R$, $N$ ein Ideal in $R$, dann muss $R$ ein noetherscher Ring sein. Umgekehrt, wenn $R$ ein noetherscher Ring ist, dann ist $(E)$ immer richtig. (Hauptidealringe sind noethersch $\Rightarrow$ $(E)$ gilt immer.)

**Anwendung zum Beweis von *(ii)*.** $W$ freier $R$-Modul, $M \subset W$ ein Untermodul $\Rightarrow$ $M$ wieder endlich erzeugt. Also finde $m_1, \ldots, m_n$, so dass

$$\phi\colon R^{n\times 1} \to M \subset W \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_1m_1 + \cdots + x_nm_n$$

surjektiv ist. Nun: $R^{n\times 1}$ und $W$ sind freie $R$-Moduln. $\phi\colon R^{n\times 1} \to W$ ist lineare Abbildung mit Bild$(\phi) = M$. Also könne wir *(i)* anwenden und erhalten: $M$ ist freier Modul und $\mathrm{Rg}(M) \leq \mathrm{Rg}(W)$.

**1.7.13 Hauptsatz.** *$R$ sei HIR. Klassifizierung der endlich erzeugten $R$-Moduln:*

*A) Sei $M$ ein endlich erzeugter $R$-Modul. Dann ist $M$ isomorph zu einer endlichen direkten Summe*

$$M \cong R^r \oplus R/(\delta_1) \oplus \cdots \oplus R/(\delta_s)$$

*(mit $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_s \neq 0$, $\delta_i \notin R^\times$, denn sonst $R/(\delta_i) = 0$) aus einem freien Anteil und einem* Torsionsanteil*. Dabei sind die Zahlen $r$ und die* Strukturinvarianten *$\delta_1, \ldots, \delta_s$ von $M$ eindeutig (bis aus Assoziierte) bestimmt. Man nennt dann $r$ auch den* Rang *von $M$.*

*B) Man kann den Rang und die Struktur von $M$ ausrechnen, sofern eine* Präsentation *von $M$ gegeben ist.*

*D.h. ein Erzeugendensystem $\mathcal{E} = (e_1, \ldots, e_m)$ von $M$ (äquivalent dazu eine surjektive Abbildung) $f : R^{m\times 1} \to M, (x_1, \ldots, x_m)^t \mapsto x_1e_1 + \ldots + x_me_m$ und ein* Relationssystem *$\mathcal{R} = (\rho_1, \ldots, \rho_n)$, das ist ein Erzeugendensystem von $\ker(f)$ als R-Modul.*

Verfahren: *Schreibe $\rho_1, \ldots, \rho_m \in R^{m\times 1}$ als Spaltenvektoren in eine Matrix $A \in R^{m\times n}$, die* Relationenmatrix. *Sei $PAQ = D \in R^{m\times n}$ die Smithsche Normalform der Relationenmatrix mit $m' \leq min(m, n) \Rightarrow$ Rang $r = \mathrm{Rg}(M) = m - m'$.*

*Wenn wir in $d_1 \mid \cdots \mid d_{m'}$ die Einheiten weglassen (alle $d_i, i \leq i_0$), dann bleiben die Strukturinvarianten $\delta_1 = d_{i_0+1}, \ldots, d_s = d_{m'}$ mit $s = m' - i_0$ von $M$ übrig.*

*C) Herstellen der Isomorphie:*

$$M \xrightarrow{\sim} R^r \oplus R/(\delta_1) \oplus \cdots \oplus R/(\delta_s)$$

*Man nehme $P, Q$, sodass $PAQ = D$ ($A$ Relationenmatrix). Sei $C = (c_1, \ldots, c_m)$ die Basis von $R^{m\times 1}$, welche aus den Spaltenvektoren der Matrix $P^{-1}$ entsteht. Dann ist $d_1c_1, \ldots, d_{m'}c_{m'}$ eine Basis von $\mathrm{Bild}(A) = \ker(f)$. Daraus ergibt sich konkret die Isomorphie ($m' + r = m$):*

$$\begin{aligned} R/(d_1) \oplus \cdots \oplus R/(d_{m'}) \oplus R^r &\to M \\ (\bar{\lambda}_1, \ldots, \bar{\lambda}_{m'}, \lambda_{m'+1}, \ldots, \lambda_m) &\mapsto \lambda_1c_1 + \cdots + \lambda_mc_m \end{aligned}$$

*Wenn $d_i \in R^\times$ dann ist mit $d_ic_i$ auch $c_i \in \ker(f) \Rightarrow f(c_i) = 0$, und man kann die entsprechenden $c_i$ weglassen.*

*Beweis.* Da $M$ ein endlich erzeugter $R$-Modul ist, muss eine Präsentation von $M$, d.h. eine exakte Sequenz

$$R^{n\times 1} \xrightarrow{A} R^{m\times 1} \xrightarrow{f} M \to 0$$

existieren.

**Definition** (exakte Sequenz)**.** *An jeder Stelle $\cdots \xrightarrow{\phi_1} R \xrightarrow{\phi_2} \cdots$ ist* $\mathrm{Bild}\,\phi_1 = \ker\phi_2$.

$\ker(f) = \mathrm{Bild}(A)$ ist ein Untermodul, also endlich erzeugt. Es existiert immer eine Relationenmatrix $A$

$$A \mapsto PAQ = D \qquad \text{Smith. NF}$$

$$\begin{array}{c} V = R^{n\times 1} \text{ mit Standardbasis } S_n (\hat{=} B') \\ \overset{A}{\big\downarrow} \\ W = R^{m\times 1} \text{ mit Standardbasis } S_m (\hat{=} C') \end{array}$$

$$A = [A]_{S_m \times S_n} \Rightarrow PAQ = P[A]_{S_m\times S_n}Q = [A]_{S_mP^{-1}, S_nQ}$$

Also müssen wir in $R^{n\times 1} = W$ die Basis $c_1, \ldots, c_m$ nehmen, welche aus den Spaltenvektoren von $P^{-1}$ besteht. Dann folgt:

$$R^{m\times 1} = \{c_1, \ldots, c_m\} \xrightarrow{f} M \to 0$$

Homomorphiesatz $\Rightarrow$

$$\ker(f) = \{d_1 c_1, \ldots, d_m c_m\}$$
$$R^{m\times 1} / \ker(f) \cong M$$

$\Rightarrow$ der Satz (bis auf Eindeutigkeit). Noch zu zeigen: Eindeutigkeit.

□

**Beispiel.** $M = \mathbb{Z}$-Modul = abelsche Gruppe (+). Zwei Erzeugende $(x, y)$, also:

$$\mathbb{Z}^{2\times 1} \xrightarrow{f} M \to 0 \qquad \begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \mapsto \lambda_1 x + \lambda_2 y$$

Eine Relation: $3x + 4y = 0$. Also $\ker(f)$ wird erzeugt durch $\binom{3}{4}$ $(n = 1)$. Präsentation:

$$\mathbb{Z} \to \mathbb{Z}^{2\times 1} \xrightarrow{f} M \to 0 \qquad \lambda \mapsto \binom{3}{4}\lambda = \binom{3\lambda}{4\lambda}$$

$A = \binom{3}{4}$ ist die Relationenmatrix.

$$\binom{3}{4} \to \binom{3}{1} \to \binom{1}{3} \to \binom{1}{0} = D = P\binom{3}{4}$$
$$\begin{pmatrix}1&0\\0&1\end{pmatrix} \to \begin{pmatrix}1&0\\-1&1\end{pmatrix} \to \begin{pmatrix}-1&1\\-1&0\end{pmatrix} \to \begin{pmatrix}-1&1\\-4&3\end{pmatrix} = P \qquad P^{-1} = \begin{pmatrix}3&1\\4&1\end{pmatrix} = (c_1, c_2)$$

Also $\ker(f)$ wird erzeugt durch $\binom{3}{4}$ $(n = 1)$.
$\Rightarrow$ Vielfache von $\binom{1}{1}$ werden isomorph auf $M$ abgebildet.
$\Rightarrow$ Modul $M$ ist frei, vom Rang 1 mit der Erzeugenden $x + y$.

Einfacher: $3x + 4y = 0 \overset{|+x}{\Rightarrow} 4(x + y) = x, \overset{|-y}{\Rightarrow} 3(x + y) = -y$. Beide Erzeugende sind als Vielfache von $x + y$ darstellbar.

*12. Vorlesung vom 19.01.2004*

Bevor wir in 1.7.13 A) die Eindeutigkeit beweisen, werden einige Begriffsbildungen benötigt:

**1.7.14 Vorbemerkung über $R$-Moduln.** Sei $R$ ein Integritätsbreich, $M$ ein $R$-Modul. Betrachte:

a) *Torsionselemente* $M_{tor} := \{m \in M, \exists \lambda \neq 0, \in R : \lambda m = 0\}$ bilden ein Untermodul von $M$. Wenn $M_{tor} = \{0\}$, dann nennt man $M$ einen *torsionsfreien* Modul. Wenn $M = M_{tor}$, dann nennt man $M$ ein *Torsionsmodul*.

b) Im allgemeinen Fall kann man den Faktormodul $N = M/M_{tor}$ bilden. Dann ist $N$ torsionsfrei.

c) Ein freier Modul ist immer torsionsfrei.

*Beweis.* a) $m_1, m_2 \in M; \lambda_1, \lambda_2 \in R : \lambda_1 m_1 = \lambda_2 m_2 = 0 \Rightarrow (\lambda_1\lambda_2)(m_1 + m_2) = 0$ und $\lambda_1\lambda_2 \neq 0$ weil $R$ Integritätsbereich ist. Also $m_1 + m_2 \in M_{tor}$. Wenn $m \in M_{tor}$ und $\mu \in R \Rightarrow \mu m \in M_{tor}$. $\Rightarrow M_{tor}$ ist $R$-Modul. □

**Bemerkung.** In *c)* gilt im Allgemeinen nicht die Umkehrung, d.h. ein torsionsfreier Modul muss nicht unbeding frei sein. Jedoch für endlich erzeugte Moduln über Hauptidealringen ist das richtig, wie wir gleich sehen werden.

**1.7.15 Definition** (Annulator). *Der* A n n u l a t o r *eines R-Moduls M:*

$$\mathrm{Ann}(M) := \{r \in R, rM = 0\}$$

$\mathrm{Ann}(M)$ ist ein Ideal im Ring $R$.

$$r_1M = 0, r_2M = 0 \Rightarrow (r_1 + r_2)M = 0$$

Nun kommen wir zum Beweis der Eindeutigkeisaussage 1.7.13 A). Wir haben

$$\begin{aligned} M &\cong R/\delta_1 \oplus \cdots \oplus R/\delta_s \oplus R^r \qquad (R^r \text{ ist frei}) \\ \Rightarrow M_{tor} &\cong R/\delta_1 \oplus R/\delta_s \\ \Rightarrow M/M_{tor} &\cong R^r \end{aligned}$$

$r$ ist der eindeutig bestimmte Rang des freien Moduls $M/M_{tor}$. Noch zu zeigen: Die Strukturinvarianten $\delta_1, \ldots, \delta_s$ sind eindeutig bis auf Assoziierte.

**1.7.16 Hilfssatz.** *OBdA: $M = M_{tor} \cong R/\delta_1 \oplus \cdots \oplus R/\delta_s$. Dann ist:*

$$\mathrm{Ann}(M) = (\delta_s)$$

*Beweis.* Sei $r \in \mathrm{Ann}(M)$. Betrachte $[1] \oplus \cdots \oplus [1] \in M = M_{tor}$:

$$0 = r([1] \oplus \cdots \oplus [1]) = [r] \oplus \cdots \oplus [r]$$

$\Rightarrow [r] \in R/(\delta_i)$ ist die Nullklasse $\forall i$. D.h. $r \in (\delta_i) \forall i$.

Jedoch $\delta_1 \mid \cdots \mid \delta_s \Rightarrow (\delta_1) \supseteq \cdots \subset (\delta_s)$. Also $r \in (\delta_i)\ \forall i \Rightarrow r \in (\delta_s)$. Die Umkehrung ist offensichtlich. □

**Beispiel.** $M = \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/6\mathbb{Z} + \mathbb{Z}/12\mathbb{Z}$. $2 \mid 6 \mid 12 \Rightarrow \mathrm{Ann}(M) = 12\mathbb{Z}$.

*Beweis der Eindeutigkeit der Zerlegung im Hauptsatz.* Annahme:

$$M \cong R/(\delta_1) \oplus \cdots \oplus R/(\delta_s) \cong R/(d_1) \oplus \cdots \oplus R/(d_t)$$

$\delta_1 \mid \cdots \mid \delta_s$ und $d_1 \mid \cdots \mid d_t$ keine Einheiten. Behauptung: $\mathrm{Ann}(M) = (\delta_s) = (d_t) \Rightarrow \delta_s \sim d_t$.

$l = l(\delta_s) = l(d_t)$ sei die Anzahl der irreduziblen Faktoren in $\delta_s$ bzw. $d_t$. Beweis durch Induktion über $l$:

$l = 1$: $\delta_s \sim d_t$ sind irreduzibel $\Rightarrow$ alle $\delta_i \sim \delta_s$ und alle $d_j \sim d_t \sim d_s$. OBdA: $\delta_i = d_j = p \forall i, j$, $p \in R$ irreduzibel $\Rightarrow R/(p) = K$ ist ein Körper.

$$s = \dim_K(M) = t$$

Das beweist den Fall $l = 1$.

*Induktionsschluss:* Sei $l = l(\delta_s) = l(d_t) \geq 2$. Sei $p$ ein irreduzibler Faktor von $\delta_s$ und $d_t$:

$$l(p^{-1}\delta_s) = l(p^{-1}d_t) = l - 1 \qquad (*)$$

Betrachte den Modul $M_p = \{m \in M, pm = 0\}$, ein Untermodul von $M_{tor}$. $(*)$ $\Rightarrow$ seien $s_0$, $t_0$ die Indizes so, dass $p \mid \delta_i$ falls $i > s_0$ bzw. $p \mid d_j$ falls $j > t_0$.

$$\begin{aligned} \Rightarrow M_p &\cong (p^{-1}\delta_{s_0+1})/(\delta_{s_0}) \oplus \cdots \oplus (p^{-1}\delta_s)/(\delta_s) \\ &\cong (p^{-1}d_{t_0+1})/(d_{t_0}) \oplus \cdots \oplus (p^{-1}d_t)/(d_t) \end{aligned}$$

$M_p$ ist $R/(p)$-Vektorraum

$$\Rightarrow s - s_0 = t - t_0 \qquad (**)$$

Andererseits betrachte den Faktormodul

$$\begin{aligned} M/M_p &\cong R/(\delta_1) \oplus \cdots \oplus R/(\delta_{s_0}) \oplus R/(p^{-1}\delta_{s_0+1}) \oplus \cdots \oplus R/(p^{-1}\delta_s) \\ &\cong R/(d_1) \oplus \cdots \oplus R/(d_{t_0}) \oplus R/(p^{-1}d_{t_0+1}) \oplus \cdots \oplus R/(p^{-1}d_t) \end{aligned}$$

$l(p^{-1}\delta_s) = l(p^{-1}d_t) = l - 1$. Also können wir auf $(1)$ die Induktionvoraussetzung anwenden.

$$\Rightarrow \delta_1, \ldots, p^{-1}\delta_s \sim d_1, \ldots, p^{-1}d_t \Rightarrow s = t$$

$$\begin{aligned} (**) &\Rightarrow s_0 = t_0 \\ &\Rightarrow \delta_1 \sim d_1, \ldots, \delta_{s_0} \sim d_{t_0}, p^{-1}\delta_{s_0+1} \sim p^{-1}d_{t_0+1}, \ldots, p^{-1}\delta_s \sim p^{-1}d_t \end{aligned}$$

□

**1.7.17 Weiterverarbeitung des Hauptsatzes.** Bisher: $M \cong R^r \oplus R/(\delta_1) \oplus \cdots \oplus R/(\delta_s)$. Sei $R/(\delta)$ ein Summand aus dem Torsionanteil. $R$ faktoriell $\Rightarrow$ $\delta \sim p_1^{l_1} \cdots p_t^{l_t}$ Produkt verschiedener Primelementpotenzen. Chinesicher Restsatz:

$$\Rightarrow R/(\delta) \cong R/(p_1^{l_1}) \oplus \cdots \oplus R/(p_t^{l_t})$$

Wir können die Zerlegung des Torsionsanteils $M_{tor}$ noch weiter fortsetzten bis in den „Nennern“ nur noch Potenzen von Primelementen von $R$ vorkommen.

**Beispiel.** $R = \mathbb{Z}$

$$M \cong \mathbb{Z}/(2) \oplus \underbrace{\mathbb{Z}/(6)}_{Z/(2)\oplus\mathbb{Z}/(3)} \oplus \underbrace{\mathbb{Z}/(12)}_{\mathbb{Z}/(3)\oplus\mathbb{Z}/(4)}$$

## 1.8 Normalformen quadratischer Matrizen

$K$ ein Körper, $A, B \in K^{n\times n}$ heißen ähnlich, falls $P \in \mathrm{GL}_n(K)$ existiert mit:

$$B = P^{-1}AP \qquad \text{(Äqivalenzrelation } B \sim A\text{)}$$

Wir wollen in jeder Äquivalenzklasse eine Normalform finden. In LAAG II hatten wir die Fälle $A$ diagonalisierbar bzw. $A$ triagonalisierbar, d.h. bei geeigneter Wahl von $P$ wird $B$ Diagonal- bzw. Dreiecksmatrix.

**1.8.1 Hilfssatz** (A). *Für eine Menge $V$ ist folgendes äquivalent:*

*(i) $V$ ist ein $K[X]$-Modul*

*(ii) $V$ ist ein $K$-Vektorraum, $X$ operiert auf $V$ linear, und die Potenzen von $X$ operieren durch wiederholte Anwendung auf $X$.*

*Beweis.* (i) $\Rightarrow$ (ii): $V = K[X]$-Modul $\Rightarrow$ erst recht ein $K$-Modul $= K$-Vektorraum. $K[X]$ ist kommutativer Ring.

$$\begin{aligned} \Rightarrow \lambda X &= X\lambda \qquad \lambda \in K \\ \lambda X\nu &= X\lambda\nu \end{aligned}$$

und für die Operatoren von $R = K[X]$ gilt das Assoziativgesetz

$$\begin{aligned} \Rightarrow \lambda(X\nu) &= X(\lambda\nu) \qquad \text{d.h. } X \text{ operiert } K\text{-linear} \\ X^2\nu &= X(X\nu) \qquad \text{u.s.w.} \end{aligned}$$

□

**1.8.2 Hilfssatz** (B). *Seien $V, W$ zwei $K[X]$-Moduln, welche als $K$-Vektorräume endlich dimensional sind. Dann ist folgendes äquivalent:*

*(i) $V$ und $W$ sind isomorphe $K[X]$-Moduln*

*(ii) Es existiert ein $K$-Isomorphismus $\phi\colon V \to W$, so dass zusätzlich:*

$$\phi(X \cdot_V \nu) = X \cdot_W \phi(\nu) \quad \forall \nu \in V$$

*(iii) Es gilt: $\dim_K V = \dim_K W = n$ und für beliebige Basen $B$ von $V$, $C$ von $W$, (genügt für ausgewählte Basen) sind die Matrizen*

$$\begin{aligned} [X]_B &= \textit{Koordinatenmatrix des linearen Op. } X \textit{ auf } V \\ &\quad \textit{bzgl. der Basis } B \textit{ (d.h. } B, B\textit{)} \\ [X]_C &= \textit{entsprechend: } X \textit{ auf } W \textit{ bzgl. } C \end{aligned}$$

*ähnliche Matrizen in $K^{n\times n}$.*

*Beweis (teilweise).* (i) $\Rightarrow$ (ii) $R = K[X], V, W$ sind isomorphe $R$-Moduln

$$\Rightarrow \text{ ex. } \quad \phi\colon V \xrightarrow{\sim} W \qquad\qquad \phi(r\nu) = r\phi(\nu) \quad \forall r \in R$$

$$\begin{aligned} r = \lambda \in K \quad &\Rightarrow \quad \phi \text{ ist } K\text{-linear} \\ r = X \quad &\Rightarrow \quad \text{Zusatzeigenschaft} \end{aligned}$$

(ii) $\Rightarrow$ (iii) Sei $\phi\colon V \xrightarrow{\sim} W$ ein $K$-Isomorphismus

$$\Rightarrow \dim_K(V) = \dim_K(W) = n$$

Zusatzeigenschaft bedeutet:

$\circlearrowleft$ kommutativ
Diagramm bilinearer Abb.

$$\begin{array}{ccc} V & \xrightarrow{\phi} & W \\ \downarrow{\scriptstyle X} & & \downarrow{\scriptstyle X} \\ V & \xrightarrow{\phi} & W \end{array}$$

Wähle Basen $B$ von $V$, $C$ von $W$. Als Matrizengleichung:

$$X \cdot \phi = \phi \cdot X$$
$$[X \cdot \phi]_{C,B} = [\phi \cdot X]_{C,B}$$
$$[X]_B \cdot [\phi]_{C,B} = [\phi]_{C,B} \cdot [X]_C$$

Setze $P = [\phi]_{C,B}$, weil $\phi$ $K$-Isom. ist $\Rightarrow \exists\ P^{-1} = [\phi^{-1}]_{B,C}$

$$\Rightarrow P^{-1}[X]_B P = [X]_C$$

d.h. $[X]_B, [X]_C$ sind ähnliche Matrizen. □

**Strategie.** $A \in K^{n\times n}$ dazu bilden wir einen $K[X]$-Modul $V_A$ wie folgt:

| | |
|---|---|
| $V_A = K^{n\times 1}$ | als $K$-VR |
| $X\colon \nu \to A\nu$ | sei der fixierte lineare Operator, d.h. $X(\nu) = A\nu$ |

**Grundidee.** Für jeden zu $V_A$ isomorphen $K[X]$-Modul $W$, und für jede Basis $C$ von $W$ ist die Matrix $[X]_C$ auf $W$ ähnlich zu $A = [X]_S$, $S$ Standardbasis auf $K^{n\times 1}$. Dies ist eine direkte Folgerung aus den vorangegangenen Hilfssätzen:

*13. Vorlesung vom 26.01.2004*

**1.8.3 Satz.** *Sei $A \in K^{n\times n}$. Sei $V_A$ der $K[X]$-Modul mit*

$$V_A = K^{n\times 1} \quad \textit{und} \quad (\sum a_i X^i) \circ \nu := \sum a_i A^i \nu$$

*d.h. $X$ operiert via $A$.*

*Sei $W$ ein beliebiger $K[X]$-Modul, welcher zu $V_A$ isomorph ist, und sei $B$ eine beliebige Basis von $W$ (als $K$-Vektorraum). Dann ist die Koordinatenmatrix $[X]_B$ stets ähnlich zu $A$.*

**1.8.4 Hauptsatz.** *Seien $A, V_A$ wie bisher. Betrachte zu $A$ die so genannte* charakteristische Matrix

$$\mathcal{A} = XI_n - A \in (K[X])^{n\times n}$$

*Behauptung: Der $K[X]$-Modul $V_A$ besitzt eine Präsentation mit $\mathcal{A}$ als Relationenmatrix.*

*Beweis.* Setze $R = K[X]$. Das ist unser Hauptidealring. Wir suchen eine Präsentation

$$R^{n\times 1} \xrightarrow{\mathcal{A}} R^{n\times 1} \xrightarrow{f} V_A \to 0$$

mit der chrakteristischen Matrix $\mathcal{A}$ als Relationenmatrix. $V_A = K^{n\times 1}$ hat als $K$-Vektorraum die Standardbasis $e_1, \ldots, e_n$. Diese Basis ist dann auch ein Erzeugendensytem von $V_A$ als $R$-Modul. $R^{n\times 1}$ sind Spaltenvektoren, welche aus Polynomen bestehen. $R^{n\times 1} \ni (a^{(1)}, \ldots, a^{(n)})^t$, alle $a^{(r)}$ sind Polynome $a^{(r)} = \sum_j a_j^{(r)} X^j \in K[X] = R$.

$$R^{n\times 1} \ni \begin{pmatrix} a^{(1)} \\ \vdots \\ a^{(n)} \end{pmatrix} \to \sum_{r=1}^{n} a^{(r)} \circ_{V_A} e_r$$

Um diese Abbildung genauer auszurechnen, machen wir folgende Identifizierung:

$$\underbrace{R^{n\times 1}}_{\substack{\text{Spaltenvektor}\\ \text{aus Polynomen}}} = (K[X])^{n\times 1} = \underbrace{K^{n\times 1}[X]}_{\substack{\text{Polynome mit Spalten-}\\ \text{vektoren als Koeffizienten}}}$$

**Beispiel.**

$$R^{3\times 1} \ni \begin{pmatrix} X+1 \\ 2X-3 \\ X^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} X^2 + \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} X + \begin{pmatrix} 1 \\ -3 \\ 0 \end{pmatrix} \in K^{3\times 1}[X]$$

Polynom-Spaltenvektor, $S_i$ eine Spalte:

$$\mathcal{S} = \sum_{i\geq 0} S_i X^i \tag{1}$$

**Hilfssatz** (Lemma A)**.** *Mit der Identifizierung (1) gilt:*

$$f(\mathcal{S}) = S_0 + AS_1 + A^2S_2 + \cdots \qquad \forall \mathcal{S} \in R^{n\times 1}$$

*Beweis.* $\mathcal{S} = \begin{pmatrix} a^{(1)} \\ \vdots \\ a^{(n)} \end{pmatrix}$. Nach Defintion gilt:

$$\begin{aligned} f(\mathcal{S}) &= a^{(1)} \circ e_1 + \cdots + a^{(n)} \circ e_n = (\sum_j a_j^{(1)} X^1) \circ e_1 + \cdots + (\sum_j a_j^{(n)} X^n) \circ e_n \\ &= \sum_{j\geq 0} (a_j^{(1)} X^1 \circ e_1 + \cdots + a_j^{(n)} X^n \circ e_n) = \sum_{j\geq 0} X^j \circ \underbrace{(\sum_{\nu=1}^{n} a_j^{(\nu)} e_\nu)}_{j\text{-te Spaltenvektor}} \\ &= \sum_{j\geq 0} X^j S_j = \sum_{j\geq 0} A^j S_j \end{aligned}$$

□

Betrachte $\mathcal{A} = XI_n - A \in R^{n\times n} = (K[X])^{n\times n}$.

**Hilfssatz** (Lemma B)**.** *Für einen Polynomvektor $\mathcal{T} = \sum_{i\geq 0} T_i X^i \in K^{n\times 1}[X]$ gilt:*

$$f(\mathcal{T}) = 0 \quad \Leftrightarrow \quad \exists \mathcal{S} = \sum S_i X^i : \mathcal{T} = \mathcal{A}\mathcal{S}$$

*Beweis.* Sei $\mathcal{T} = \mathcal{A}\mathcal{S}$, d.h.

$$\begin{aligned} (XI_n - A)(\sum_{j=0}^{m} S_i X^i) &= \sum_{j=0}^{m} S_i X^i - \sum_{i=0}^{m} (AS_i) X^i \\ &= -AS_0 + (S_0 - AS_1)X + (S_1 - AS_1)X^2 + \cdots + S_m X^{m+1} \\ &=: T_0 + T_1 X + T_2 X^2 + \cdots + T_m X^{m+1} \end{aligned}$$

$$\text{Nun:} \qquad f(\mathcal{T}) = \sum_{i\geq 0} A^i T_i = -AS_0 + A(S_0 - AS_1)X + \cdots + S_m X^{m+1} = 0$$

ist eine Teleskopsumme, $\to 0$. Wenn $f(\mathcal{T}) = 0$, dann finde $\mathcal{S}$, so dass $\mathcal{T} = \mathcal{AS}$ gilt. Anfang:

$$\begin{aligned} f(\mathcal{T}) &= T_0 + AT_1 + \cdots + A^m T^m = 0 \\ \Rightarrow T_0 &= -A(T_1 + AT_2 + \cdots + A^{m-1}T_m) \\ \text{nimm } S_0 &= T_1 + AT_2 + \cdots + A^{m-1}T_m \end{aligned}$$

etc. Die Berechnung der weiteren $S_I$ ergibt sich aus dem Ansatz:

$$\sum_{i\geq 0} T_i X^i = (XI_n - A)(\sum_{j\geq 0} S_j X^j)$$

□

$\Rightarrow$ Hauptsatz □

**1.8.5 Folgerung.** *Sei $A \in K^{n\times n} \mapsto \mathcal{A} = XI_n - A \in R^{n\times n} = (K[X])^{n\times 1}$. Finde zu $\mathcal{A}$ die Smithsche Normalform $\mathcal{D}$:*

$$\mathcal{D} = \begin{pmatrix} d_1(X) & & 0 \\ & \ddots & \\ 0 & & d_n(X) \end{pmatrix} \quad \textit{mit: } d_1(X) \mid d_2(X) \mid \cdots \mid d_n(X)$$

*Wir lassen die Polynome $d_i(X), \ldots, d_{i_0}(X)$ welche Konstanten sind ($\in R^\times$) unberücksichtigt. Dann schreibe $\delta_r(X) = d_{i_0+r}(X)$.*

*(i) Dann gilt:*

$$V_A \cong R/(\delta_1(X)) \oplus \cdots \oplus R/(\delta_s(X))$$

*$V_A$ als $K[X]$-Modul, wobei $i_0 + s = n$,*

*(ii) das Hauptideal $(\delta_s(X)) = (d_n(X))$ ist der Annulator von $V_A$.*

*(iii) Genauer heisst das: Sei $a(X) = \sum a_i X^i \in K[X]$ ein beliebiges Polynom. Bilde dazu die Matrix $a(A) = a_0 I_n + a_1 A + a_2 A^2 + \cdots \in K^{n\times n}$. Dann gilt:*

$$a(A) = \textit{Nullmatrix} \quad \Leftrightarrow \quad a(X) \textit{ ist teilbar durch } d_n(X)$$

*Deswegen heißt $d_n(X)$ auch* Minimalpolynom *für $A$.*

*Beweis.* (i), (ii) klar aus der allgemeinen Theorie der $R$-Moduln, weil $\mathcal{A}$ die Relationenmatrix ist.

(iii): Was bedeutet es, dass ein Polynom $a(X) = \sum a_i X^i$ im Annulator von $V_A$ liegt? D.h. $\forall v \in V_A$:

$$\begin{aligned} 0 = a(X) \circ v &= a_0 v + a_1 Av + \cdots + a_m A^m v \\ &= (\underbrace{a_0 I_n + a_1 A + \cdots + a_m A^m}_{=:\, a(A) \in K^{n\times n}})v = 0 \qquad \forall v \in K^{n\times 1} \end{aligned}$$

$\Rightarrow a(A) = 0 \Rightarrow$ (iii) □

**1.8.6 Folgerung.** *(i) Satz von Cayley-Hamilton: Das Minimalpolynom von $A \in K^{n\times n}$ ist Teiler des charakteristischen Polynoms $\chi_A(X)$. D.h.*

$$\chi_A(A) = 0 \quad \textit{(Nullmatrix)}$$

*(ii) Zwei Matrizen $A, B \in K^{n\times n}$ sind ähnlich $\Leftrightarrow$ die charakteristischen Matrizen $\mathcal{A}, \mathcal{B} \in R^{n\times n}$ sind äquivalent im Sinne von 1.7.2.*

*Beweis.* (i):

$$A \mapsto \mathcal{A} \mapsto \mathcal{D} = \begin{pmatrix} d_1(X) & & 0 \\ & \ddots & \\ 0 & & d_n(X) \end{pmatrix}$$

$$R^{n\times n} \ni \mathcal{D} = \mathcal{P}\mathcal{A}\mathcal{Q}$$

$\det \mathcal{P}, \det \mathcal{Q}$ sind Einheiten in $R \Rightarrow \det(\mathcal{P}\mathcal{Q}) = c \neq 0$, Konstante
$\Rightarrow d_1(X) \cdot \cdots \cdot d_n(X) = \det \mathcal{D} = \det(\mathcal{P}) \det(\mathcal{A}) \det(\mathcal{Q}) = c \cdot \chi_A(X)$
$\Rightarrow d_n(X) \mid \chi_A(X) \Rightarrow$ Satz von Cayley-Hamilton.
(ii): $B = P^{-1}AP$, $P \in GL_n(K)$

$$\mathcal{B} = XI_n - B = XI_n - P^{-1}AP = P^{-1}(XI_n - A)P = P^{-1}\mathcal{A}P$$

$\Rightarrow \mathcal{A}, \mathcal{B}$ sind ähnlich, insbesondere äquivalent im Sinne von 1.7.2.
Umkehrung: $\mathcal{B}$ äquivalent zu $\mathcal{A}$ (in $R^{n\times n}$), $\mathcal{B} = \mathcal{P}\mathcal{A}\mathcal{Q} \Rightarrow \mathcal{A}, \mathcal{B}$ haben dieselbe Smithsche Normalform $\mathcal{D}$.

$$\overset{\text{Hauptsatz}}{\Rightarrow} V_A \underset{K[X]}{\cong} V_B \text{ ist durch } \mathcal{D} \text{ bestimmt}$$

Und $A = [X]_S$ in $V_A$, $B = [X]_S$ in $V_B$ ($S$ Standardbasis in $V_A$ oder $V_B$)

$$V_A \underset{K[X]}{\cong} V_B \quad \overset{1.8.2(iii)}{\Rightarrow} \quad A, B \text{ sind ähnlich}$$

□

**1.8.7 Satz** (Jordansche Normalform). *Betrachte $A \in K^{n\times n}$, $\chi_A(X) = \det(\mathcal{A}) \in K[X]$ zerfalle in Linearfaktoren (z.B. wenn $K = \mathbb{C}$). Seien $\lambda_1, \ldots, \lambda_r$ die verschiedenen Eigenwerte von $A$, $m_i$ die Vielfachheit von $\lambda_i$ ($\Rightarrow \chi_A(X) = \prod_i (X - \lambda_i)^{m_i}$). Sei $\mathcal{D} = \mathrm{Diag}(1, \ldots, 1, \delta_1(X), \ldots, \delta_s(X))$ die Smithsche NF von $\mathcal{A} \Rightarrow \delta_1(X) \cdots \delta_s(X) = \chi_A(X)$. Deswegen gehört zu jeder Vielfachheit $m_i$ eine Partition*

$$m_i = m_{i,s} + m_{i,s-1} + \cdots + m_{i,1}$$

*mit $m_{i,r}$ = Vielfachheit von $X - \lambda_i$ im Polynom $\delta_r$.*

$$\Rightarrow m_{i,s} \geq m_{i,s-1} \geq \cdots \geq m_{i,1}$$

*weil $d_1(X) \mid \cdots \mid d_s(X)$. Zu $m_{i,r}$ bilden wir den sogenannten* Jordan-Block:

$$J_{i,r} = \begin{pmatrix} \lambda_i & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda_i \end{pmatrix} \in K^{m_{i,r}\times m_{i,r}}$$

*Dann ist* $J_A = \mathrm{Diag}(J_{i,r}) \quad \forall (i,r)$

$$J_A = \begin{pmatrix} \square & & & 0 \\ & \square & & \\ & & \square & \\ 0 & & & \square \end{pmatrix} \qquad \square : \textit{ Jordanblocks}$$

*die* Jordansche Normalform *von A eindeutig bis auf Vertauschung der Jordanblocks.* $J_A$ *ist ähnlich zu A.*

**Hilfssatz.** *Sei* $V = U \oplus W$ *ein K-Vektorraum,* $\phi \in \mathrm{End}_K(V)$ *linearer Operator auf* $V$, $\phi(U) \subseteq U$, $\phi(W) \subseteq W$. *Wähle Basis* $\mathcal{B} = \mathcal{C} \cup \mathcal{D}$ *von* $V$, *welche sich zusammemsetzt aus Basen der Unterräume* $U$ *und* $W$. *Behauptung: Dann gilt:*

$$[\phi]_{\mathcal{B}} = \left(\begin{array}{c|c} [\phi|_U]_{\mathcal{C}} & 0 \\ \hline 0 & [\phi|_W]_{\mathcal{D}} \end{array}\right)$$

*ist eine Diagonalblockmatrix.*

*Beweis.* Nach Def. ist $j$-te Spalte von $[\phi]_B = [\phi(b_j)]_B$ mit $b_j$ $j$-ter Basisvektor. Wir unterscheiden zwei Fälle. Fall A: $b_j \in \mathcal{C}$ aus Basis von $U \Rightarrow \phi(b_j) \in U$ $\Rightarrow$ im Koordinatenvektor $[\phi(b_j)]_B$ kommen nur Koordinaten vor, welche zu $\mathcal{C}$ gehören. D.h.:

$$[\phi(b_j)]_B = \begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\b\\c\\d\end{matrix}}\right\} \mathcal{C} \\ \left.\vphantom{\begin{matrix}a\\b\\c\\d\end{matrix}}\right\} \mathcal{D} \end{matrix} \qquad \text{nur } \mathcal{C}\text{-Anteil}$$

Fall B: $b_j \in \mathcal{D}$ entsprechend

$$[\phi(b_j)]_B = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ * \\ \vdots \\ * \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\b\\c\\d\end{matrix}}\right\} \mathcal{C} \\ \left.\vphantom{\begin{matrix}a\\b\\c\\d\end{matrix}}\right\} \mathcal{D} \end{matrix} \qquad \text{nur } \mathcal{D}\text{-Anteil}$$

$\Rightarrow$ Behauptung $\square$

Entsprechend: $V = V_1 \oplus \cdots \oplus V_m$, $\phi(V_i) \subseteq V_i \quad \forall i$, $\mathcal{B} = B_1 \cup \cdots \cup B_m$.

$$\begin{aligned} [\phi]_B &= \text{Diagonalblockmatrix} \\ &= \mathrm{Diag}([\phi|_{V_1}]_{B_1}, \ldots, [\phi|_{V_m}]_{B_m}) \end{aligned}$$

Nun zur JNF:

*Beweis von Satz 1.8.7.*

$$A \in K^{n\times n} \mapsto \mathcal{A} \in R^{n\times n} \mapsto \mathrm{SNF}\ \mathcal{D} = \mathrm{Diag}(1, \ldots, 1, \delta_1(X), \ldots, \delta_s(X))$$

Weil $\mathcal{A}$ eine Relationenmatrix für $V_A$ ist.

$$\Rightarrow V_A \cong K[X]/(\delta_1(X)) \oplus \cdots \oplus K[X]/(\delta_s(X)) \qquad (*)$$

sind isomorphe $K[X]$-Moduln. $\chi_A(X)$ zerfällt in Linearfaktoren (nach Voraussetzung)

$$\Rightarrow \delta_r(X) = \prod_i (X - \lambda_i)^{m_{i,r}}$$

Zerlegung von $\delta_r(X)$ in Potenzen irreduzibler Polynome

$$K[X]/(\delta_r(X)) \cong \bigoplus_i K[X]/(X - \lambda_i)^{m_{i,r}} \qquad (**)$$

mit dem Chinesichen Restsatz. Also: $(*)$ kann man verbessern mit $(**)$:

$$V_A \cong \bigoplus_i \bigoplus_r K[X]/(X - \lambda_i)^{m_{i,r}}$$

ist Isomorphie von $K[X]$-Moduln. Wir dürfen auf der rechten Seite eine beliebige Basis wählen und den linearen Operator $X$ bezüglich dieser Basis ausdrücken. Dann erhalten wir immer eine Matrix, die zu $A$ ähnlich ist.

Jeder Summand $K[X]/(X - \lambda_i)^{m_{i,r}}$ ist für sich genommen ein $K[X]$-Modul. D.h. $X$ führt jeden Summanden in sich über. Damit ist das vorhergehende Lemma anwendbar, wenn wir eine $K$-Basis wählen, welche sich aus $K$-Basen der einzelnen Summanden zusammen setzt. Im Weiteren sei oBdA:

$$V_A \cong K[X]/(X - \lambda)^m$$

Wir nehmen die $K$-Basis

$$\mathcal{B}: \quad b_1 = [1], \quad b_2 = [X - \lambda], \quad \ldots \quad b_m = [(X - \lambda)^{m-1}]$$

Wegen Division mit Rest hat $V_A$ die Dimension $m$, also $\mathcal{B}$ als eine mögliche Basis. Wir fassen $X$ als linearen Operator auf $K[X]/(X - \lambda)^m$ auf, und berechnen die Koordinatenmatrix $[X]_B$:

$$\begin{aligned}
(X - \lambda)b_1 = b_2 \quad &\Rightarrow \quad Xb_1 = [X \cdot b_1]_B = \lambda b_1 + b_2 \\
(X - \lambda)b_2 = b_3 \quad &\Rightarrow \quad Xb_2 = \lambda b_2 + b_3 \\
&\cdots \\
(X - \lambda)b_m = 0 \quad &\Rightarrow \quad Xb_m = \lambda b_m
\end{aligned}$$

Durch Auswerten: $j$-te Spalte von $[X]_B = [X \cdot b_j]_B$

$$\Rightarrow [X]_B = \begin{pmatrix} \lambda & & & 0 \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda \end{pmatrix}$$

ein Jordan-Block $\Rightarrow$ Gesamtmatrix ist eine JNF. $\square$

# Kapitel 2

# Körpererweiterungen

*14. Vorlesung vom 02.02.2004*

## 2.1 Grundbegriffe

**2.1.1 Definition** (Körper, Charakteristik)**.** *Der* K ö r p e r *F ist definiert durch:*

*(i) Kommutativer Ring mit* $1 \neq 0$

*(ii)* $F^\times = F \backslash \{0\}$

$\Rightarrow$ *in F gibt es keine echten Ideale.* C h a r a k t e r i s t i k *von F: Betrachte* $\mathbb{Z} \to F$, $1 \mapsto 1_F$. *Induziert einen Ringhomorphismus*

$$\phi \colon \mathbb{Z} \to F$$

*Weil F nullteilerfrei ist, muss* $\ker(\phi)$ *ein Primideal in* $\mathbb{Z}$ *sein. Die Charakteristik von* $F = 0$ *bedeutet* $\ker(\phi) = 0 \Rightarrow$ *F enthält eine isomorphe Kopie von* $\mathbb{Q}$. *Charakteristik von* $F = p$, *Primzahl, bedeutet* $\ker(\phi) = \mathbb{Z}p$. *D.h. Der Körper F enthält ein isomorphe Kopie des Körpers* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *mit p Elementen. Die Körper* $\mathbb{Q}$ *bzw.* $\mathbb{F}_p$ *(p Primzahl) werden als* P r i m k ö r p e r *bezeichnet.*

**2.1.2 Definition** (Körpererweiterung)**.** *Eine* K ö r p e r e r w e i t e r u n g *ist die Inklusion* $K \subset L$ *von zwei Körpern, so dass die Operationen* $(+, \cdot)$ *auf der Teilmenge K dieselben sind wie in L. D.h.:*

$$(K, +) \text{ ist die Untergruppe von } (L, +), 0_K = 0_L$$
$$(K^\times, \cdot) \text{ ist die Untergruppe von } (L^\times, \cdot), 1_K = 1_L$$

*Schreibe L/K, sage „L über K“.*

**2.1.3 Hilfssatz.** *Sei L/K ein Körpererweiterung. Dann ist insbesondere L eine K-Algebra (K-Vektorraum mit Multiplikation und entsprechenden Eigenschaften).*

Sei $\theta \in L$. Universalität $\Rightarrow$ wir haben genau einen Homomorphismus von $K$-Algebren:

$$\mathrm{ev}_\theta \colon K[X] \to L, \quad 1 \mapsto 1, \quad X \mapsto \theta$$

Zwei Fälle: a) $\mathrm{ev}_\theta$ ist injektiv, d.h. alle Potenzen von $\theta$ sind über $K$ linear unabhängig. Dann heißt $\theta$ *t r a n s z e n d e n t* über $K$.

b) $\ker(\mathrm{ev}_\theta) \neq 0$, d.h. $\theta$ ist Nullstelle mindestens eines Polynoms. D.h. Potenzen von $\theta$ sind linear abhängig über $K$. Dann heißt $\theta$ *algebraisch* über $K$.

**Beispiel.** $\mathbb{C}/\mathbb{Q}$: $z \in \mathbb{C}$ heißt *transzendente* bzw. *algebraische Zahl*.

$$\left.\begin{array}{l}\#\text{ alg. Zahlen sind abzählbar}\\ \#\,\mathbb{C}\text{ ist überabzählbar}\end{array}\right\} \Rightarrow \begin{array}{l}\text{überabzählbar viele}\\ \text{transzendente Zahlen}\end{array}$$

Berühmte transzendente Zahlen:

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} \qquad \pi = \frac{\text{Kreisumfang}}{\text{Kreisdurchmesser}} \quad (\textsc{Ludolf})$$

Fall b): $K[X]$ HIR $\Rightarrow$ $\ker(e_{V_\theta}) = (f(x))$ Hauptideal $f(x) \in K[X]$, da $K[X]/\ker \mathrm{ev}_\theta$ nullteilerfrei ist. $\Rightarrow$ $f(x)$ ist prim und damit irreduzibel, d.h. $K[X]/\ker \mathrm{ev}_\theta$ ist ein Körper, welcher unter $\mathrm{ev}_\theta$ isomorph abgebildet wird auf einen Teilkörper von $L$.

$$\begin{aligned}\mathrm{Bild}(\mathrm{ev}_\theta) &= \text{der kleinste Körper in } L\text{, welcher } K \text{ und}\\ &\quad\ \text{das Element } \theta \text{ enthält}\\ &= \text{der von } \theta \text{ über } K \text{ erzeugte Teilkörper}\end{aligned}$$

Das irreduzible Polynom $f(X)$, kann so normiert werden, das der höchste Koeffizient $= 1$ ist (*normiertes Polynom*). Dadurch ist $f(X) \in K[X]$ eindeutig bestimmt und heißt das zu $\theta$ gehörige *Minimalpolynom* ($f(X) = f_\theta(X)$).

**2.1.4 Definition** (Grad)**.** *Die Körpererweiterung $L/K$ heißt* endlich*, falls $L$ aufgefasst als $K$-Vektorraum endliche Dimension hat. Dann schreibt man*

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

*und nennt dies den* Grad *der Erweiterung $L/K$.*

**2.1.5 Hilfssatz.** *Sei $\theta \in L$ algebraisch über $K$ ($L/K$). Sei $K(\theta) \subseteq L$, der von $\theta$ erzeugte Teilkörper. Sei $f_\theta(X)$ das Minimalpolynom von $\theta$ über $K$. Dann gilt:*

$$[K(\theta) : K] = \deg f_\theta(X)$$

*d.h. $K(\theta)/K$ ist eine endlich erzeugte Erweiterung. Man bezeichnet diese Zahl als den* Grad von *$\theta$ über $K$ und schreibt dafür auch* $\deg_K(\theta)$.

*Beweis.* Wir haben bereits gesehen:

$$\mathrm{ev}_\theta \colon K[X]/f_\theta(X) \xrightarrow{\sim} K(\theta)$$

Wegen der Division mit Rest in $K[X]$, haben wir als $K$-Basis der linken Seite die Polynome $1, X, X^2, \ldots, X^{n-1}$, mit $n = \deg f_\theta(X) \Rightarrow \dim_K = n$. □

**Beispiele.** • $\sqrt{-1} \in \mathbb{C}/\mathbb{Q}$ hat den Grad 2, $f_{\sqrt{-1}}(X) = X^2 + 1$

- $p$ Primzahl, $e^{\frac{2\pi i}{p}} = \xi$ eine primitive $p^n$-te Einheitswurzel, hat über $\mathbb{Q}$ das Minimalpolynom

$$\frac{X^{p^n}-1}{X^{p^{n-1}}-1} = \phi(X) \qquad \deg_{\mathbb{Q}}(\xi) = p^{n-1}(p-1)$$

**2.1.6 Definition und Satz.** *Die Körpererweiterung $L/K$ heißt* algebraisch, *falls jedes $\theta \in L$ algebraisch über $K$ ist. Jede endliche Körpererweiterung ist algebraisch.*

*Beweis.* $\theta \in L/K$ endlich, d.h. $L$ ist endlich dimensionaler $K$-Vektorraum $\Rightarrow$ die Potenzen von $\theta$ müssen über $K$ linear abhängig sein $\Rightarrow \ker e_{V_\theta} \neq (0)$ □

**2.1.7 Hilfssatz.** *Sei $L/K/F$ ein so genannter* Körperturm, *d.h. $L \supset K \supset F$. Sind $L/K$ und $K/F$ beide endlich, dann ist auch die Gesamterweiterung $L/F$ endlich, und es gilt:*

$$[L:F] = [L:K][K:F]$$

*Beweisidee.* Sei $\mathcal{B} = \mathcal{B}_{L/K}$ eine Basis von $L/K$, und $\mathcal{C} = \mathcal{C}_{K/F}$ eine Basis von $K/F$. Bilde alle Produkte $b \cdot c$, mit $b \in \mathcal{B}, c \in \mathcal{C} \Rightarrow$ das ist eine Basis von $L/F$. (Übung) □

**2.1.8 Folgerung.** *Sei $[K:F] = n$, sei $\theta \in K$. Dann ist $\deg_F(\theta) = [F(\theta):F]$ ein Teiler von $n$.*

*Beweis.* Wegen $K \supset \mathbb{F}(\theta) \supset F$. □

**2.1.9 Satz.** *Eine Körpererweiterung $K/F$ ist endlich $\Leftrightarrow$ $K/F$ ist algebraisch, und wird durch endlich viele Elemente erzeugt.*

*Beweis.* Folgt aus 2.1.6 - 2.1.8. □

**Beispiel.** Sind $p_1, \ldots, p_n \in \mathbb{Z}$ endlich viele Primzahlen, dann ist $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}$ eine endliche Erweiterung vom Grad $2^n$.

**2.1.10 Satz** (Stammkörper eines irreduziblen Polynoms)**.** *Sei $K$ ein Körper, und $\varphi(X) \in K[X]$ ein irreduzibles Polynom. Dann existiert eine Körpererweiterung $L/K$ mit folgenden Eigenschaften:*

*(i)* $[L:K] = \deg(\varphi)$

*(ii)* $\varphi(X)$ *hat in $L$ eine Nullstelle $\theta$*

*(iii) Betrachte $\varphi(X)$ als Polynom aus $L[X] \ni \varphi(X)$. Dann gilt: $\varphi(X) = (X-\theta) \cdot \psi(X)$*

*Beweis. (i)* und *(ii)*: Betrachte den Faktorring $K[X]/(\varphi(X))$. $\varphi(X)$ irreduzibel $\Rightarrow L = K[X]/(\varphi(X))$ ist ein Körper mit der $K$-Basis $1, X, X^2, \ldots, X^{n-1}$, $n = \deg(\varphi)$. Nimm in $L$ das Element $\theta = [X]$ (Restklasse von $X$). Offensichtlich gilt $\varphi(\theta) = [0] \in L$. Also hat $\varphi(X)$ in $L$ die Nullstelle $\theta$.
*(iii)* wohl bekannt. □

**2.1.11 Folgerung.** *Sei $f(X) \in K[X]$ ein beliebiges Polynom. Dann existiert eine endliche Erweiterung $L/K$, in welcher $f(X)$ in Linearfaktoren zerfällt.*

*Beweis.* Durch Induktion. Beginne mit einem irreduziblen Faktor von $f(X)$. □

**2.1.12 Satz.** *Sei $K$ ein Körper, $H \subset K^\times$ eine endliche Untergruppe (der multiplikativen Gruppe „$\cdot$"), und $\#H = n$. Dann ist $H$ zyklische Gruppe, welche aus den $n$-ten Einheitswurzeln in $K$ besteht.*

*Beweis.* $\#H = n, \alpha \in H \Rightarrow \alpha^n = 1 \in K \Rightarrow \alpha$ ist Nullstelle von $X^n - 1$ aus $K[X]$. Jedoch hat $X^n - 1$ höchstens $n$ Nullstellen. Also: diese Nullstellen müssen genau die Elemente von $H$ sein. Noch zu zeigen: $H$ ist zyklisch. Aus der Theorie der $\mathbb{Z}$-Moduln:

$$H \cong \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_k) \quad \text{und} \quad d_1 \mid \cdots \mid d_k$$

$\#H = d_1 d_2 \cdots d_k = n$, aber der Annulator von $H$ ist genau $\mathbb{Z} \cdot d_k$. Da wir $H$ als multiplikative Gruppe auffassen, heißt das:

$$\alpha^{d_k} = 1 \qquad \forall \alpha \in H$$

$\Rightarrow \forall \alpha \in H$ sind Nullstellen von $X^{d_k} - 1$ mit $d_k \mid n$. $X^{d_k} - 1$ hat höchstens $d_k$ Nullstellen $\Rightarrow d_k = n$ (weil $\#H = n$) $\Rightarrow$ alle anderen $d_i = 1 \Rightarrow H$ ist zyklisch. □

**Folgerung.** *Die multiplikative Gruppe eines endlichen Körpers ist immer zyklisch.*

*Beweis.* Als Übung □

**2.1.13 Hauptsatz** (Satz vom primitiven Element)**.** *$K/F$ sei Körpererweiterung, $\alpha, \beta \in K$ algebraisch über $F$, und $\alpha, \beta$ sind Nullstellen der Polynome $f(X)$ bzw. $g(X) \in F[X]$. $g(X)$ habe keine mehrfachen Nullstellen. Behauptung: Es existiert $\gamma \in K$, so dass $F(\alpha, \beta) = F(\gamma) \subseteq K$.*

*Beweis.* a) $\#F < \infty \Rightarrow L = F(\alpha, \beta)$ ist ebenfalls endlicher Körper

$$\#L = \#F^{[L:F]}$$

$L$ endlicher Körper $\Rightarrow L^\times$ ist zyklische Gruppe mit erzeugendem Element $\gamma \Rightarrow L = F(\gamma)$.

b) $\#F = \infty$: Betrachte $\Omega/K/F$, so dass die Polynome $f(X), g(X)$ in $\Omega$ in Linearfaktoren zerfallen.

$$\Rightarrow \quad \begin{array}{ll} \alpha_1 = \alpha; & \alpha_2, \ldots, \alpha_s \in \Omega \text{ Nullstelle von } f(X) \\ \beta_1 = \beta; & \beta_2, \ldots, \beta_t \in \Omega \text{ Nullstelle von } g(X), \text{ alle verschieden} \end{array}$$

$\#F = \infty \Rightarrow$ Finde $c \in F^\times$ mit: $c \neq \frac{\alpha_i - \alpha}{\beta - \beta_j} \forall i, j \neq 1$. Dann betrachte $\gamma = \alpha + c\beta \in F(\alpha, \beta)$. Betrachte $h(X) := f(\gamma - cX) \in F(\gamma)[X]$:

$$h(Z) = 0 \Leftrightarrow f(\gamma - cZ) = 0 \Leftrightarrow \gamma - cZ = \alpha_i \Leftrightarrow Z = \frac{\gamma - \alpha_i}{c}$$

$g(X)$ hat die Nullstellen $\beta = \beta_1, \ldots, \beta_t$. Gemeinsame Nullstellen von $h(X)$ und $g(X)$ wäre $\beta_j = Z = \frac{\gamma - \alpha_i}{c}$. Nur möglich: $\alpha_i = \alpha$, $\beta_j = \beta$ ($\gamma = \alpha + c\beta$).

$\Rightarrow Z = \beta$ einzige gemeinsame Nullstelle von $h(X), g(X) \in F(\gamma)[X]$
$\Rightarrow \text{ggT}(f(\gamma - cX), g(X)) = X - \beta$
$\Rightarrow X - \beta$ ist Linearkombination der beiden Polynome in $F(\gamma)[X]$
$\Rightarrow \beta \in F(\gamma) \Rightarrow \alpha = \gamma - c\beta \in F(\gamma)$

□

*15. Vorlesung vom 09.02.2004*

Komplikationen im Charakteristik-$p$-Fall:

**2.1.14 Satz.** *Sei $f(X) \in K[X]$ ein irreduzibles Polynom und sei $L/K$ eine endliche Erweiterung, in der $f(X)$ in Linearfaktoren zerfällt. Dann ist folgendes äquivalent:*

*(i)* *$f(X)$ hat in $L$ mehrfache Nullstellen*

*(ii)* *$\text{char}(K) = p \neq 0$ und $f(X)$ lässt sich schreiben als $f(X) = \varphi(X^p)$, wobei $\varphi \in K[X]$.*

*Beweis.* „⇒“: Wenn $f(X) \in K[X]$ eine mehrfache Nullstelle $\alpha \in L$ hat, dann folgt:

- $(X - \alpha)$ ist gemeinsamer Teiler von $f(X)$ und $f'(X)$
- nach Voraussetzung: $f$ ist irreduzibel

$\Rightarrow$ Wenn $f'(X) \neq 0$, dann folgt $\text{ggT}(f(X), f'(X)) \sim 1$. Wann kann $f'(X) = 0$ sein? Wenn $\text{char}(K) = p$ und $f(X) = \varphi(X^p)$:

$$\overset{\text{Kettenregel}}{\Rightarrow} f'(X) = \varphi'(X^p) \cdot p \cdot X^{p-1} = 0$$

weil $0 = p$ in $K$.

„⇐“: Sei $f(X) = \varphi(X^p)$ und $\alpha \in L/K$ eine Nullstelle von $f$.

$$\begin{aligned}
&\Rightarrow \alpha^p \text{ ist Nullstelle von } \varphi(X) \\
&\Rightarrow \varphi(X) = (X - \alpha^p)\psi(X) \text{ in } L/K \\
&\Rightarrow f(X) = \varphi(X^p) = (X^p - \alpha^p)\psi(X^p) \text{ in } L[X]
\end{aligned}$$

Weil $\text{char}(K) = p$ gilt $p \mid \binom{p}{i} \forall i \neq p, 0$

$$\begin{aligned}
&\Rightarrow \binom{p}{i} = 0 \text{ in } K \\
&\Rightarrow f(X) = (X - \alpha)^p \psi(X^p) \\
&\Rightarrow \alpha \text{ ist } p\text{-fache Nullstelle von } f
\end{aligned}$$

□

Es kann tatsächlich (abhängig von $K$) irreduzible Polynome $f(X)$ von der Form $f(X) = \varphi(X^p)$ geben. Dann ist der Satz vom primitiven Element u.U. nicht anwendbar. Wenn $f(X)$ irreduzibel und $f(X) = \varphi(X^p)$, dann muss $\varphi$ auch irreduzibel sein.

**2.1.15 Definition** (separabel)**.** *Polynome ohne mehrfache Nullstellen heißen* s e p a r a b e l*, anderenfalls inseparabel.*

*Entsprechend heißen $\alpha \in L/K$ s e p a r a b e l ü b e r $K$, falls sein Minimalpolynom (das Polynom kleinsten Grades mit Nullstelle $\alpha$) separabel ist.*

*Die a l g e b r a i s c h e E r w e i t e r u n g $L/K$ heißt s e p a r a b e l, falls jedes $\alpha \in L$ separabel über $K$ ist.*

**Bemerkung.** Im Charakteristik 0 Fall sind alle algebraischen Erweiterungen separabel.

**2.1.16 Satz.** *(i) Eine algebraische Körpererweiterung $L/K$ ist separabel gdw. sich $L$ über $K$ durch separable Elemente erzeugen lässt. (ohne Beweis)*

*(ii) Jede endliche separable Erweiterung $L/K$ lässt sich durch ein einziges Element erzeugen, d.h. $L = K(\gamma)$. (Iteration des Hauptsatzes 2.1.13).*

Sei $L = K(\gamma)$, und sei $f(X)$ das Minimalpolynom von $\gamma$ über $K$. Dann gilt: $L \cong K[X]/(f(X))$. Im separablen Fall lassen sich alle endlichen Erweiterungen des Körpers $K$ in dieser Form realisieren.

## 2.2 Körperisomorphismen, normale Erweiterungen und der Hauptsatz der Galoistheorie

**2.2.1 Bemerkung.** Sei $f\colon K_1 \to K_2$ eine Abbildung zwischen Körpern mit der Homomorphieeigenschaft:

$$f(a+b) = f(a) + f(b)$$
$$f(a \cdot b) == f(a) \cdot f(b)$$

(i) Dann folgt $f(0_{K_1}) = 0_{K_2}$ und $f(-a) = -f(a)$.

(ii) und $f(1_{K_1}) \in \{0,1\}_{K_2}$.

(iii) Falls $f(1) = 0$ gilt $f \equiv 0$.

(iv) Falls $f(1) = 1$ ist $f$ injektiv, und es gilt $f(a^{-1}) = f(a)^{-1} \forall a \neq 0$.

Dann ist $f$ ein Isomorphismus $f\colon K_1 \to \text{Bild}(f)$. Insbesondere ist $\text{Bild}(f)$ wieder ein Körper.

*Beweis.* (i) klar
(ii): $1 \cdot 1 = 1 \Rightarrow f(1) \cdot f(1) = f(1) \overset{K_2 \text{ nullteilerfrei}}{\Longrightarrow} f(1) \in \{0,1\}$
(iv): $\Rightarrow \ker(f)$ ist echtes Ideal (Körper haben aber nur die trivialen Ideale) $\Rightarrow \ker(f) = 0 \Rightarrow f$ injektiv.
Rest: selber machen. □

**2.2.2 Definition.** *Zwei Erweiterungen $K_1/F$ und $K_2/F$ heißen $F$-isomorph, falls ein Isomorphismus $\sigma\colon K_1 \xrightarrow{\sim} K_2$ existiert, der auf $F$ die Identität ist.*

Dadurch sind die Möglichkeiten für $F$-Isomorphismen stark eingeschränkt, denn:

**2.2.3 Bemerkung.** $\sigma\colon K_1 \xrightarrow{\sim} K_2$ sei ein $F$-Isomorphismus und $\alpha \in K_1$ sei Nullstelle eines Polynoms $f(X) \in F[X]$. Dann muss $\sigma(\alpha)$ Nullstelle desselben Polynoms sein. Insbesondere haben $\alpha$ und $\sigma(\alpha)$ über $F$ dasselbe Minimalpolynom.

*Beweis.* $f(\alpha) = 0, f(X) := \sum a_k X^k, a_i \in F$

$$\begin{aligned} &\Rightarrow 0 = \sum a_k \alpha^k \\ &\Rightarrow 0 = \sigma(0) = \sigma(\sum a_k \alpha^k) \overset{\text{Iso}}{=} \sum \sigma(a_k)\sigma(\alpha)^k \\ &\qquad = \sum a_k \sigma(\alpha)^k \quad \text{weil } \sigma|_F = \mathrm{id} \end{aligned}$$

□

**Ziel.** Hauptsatz der Galoistheorie: *Sei $K/F$ eine „geeignete" Körpererweiterung. Dann bilden die $F$-Automorphismen (Isomorphismen $K \to K$) eine Gruppe $G = G_{K/F}$ mit folgenden Eigenschaften:*

*(i)* $\#G = [K : F]$

*(ii) Die Untergruppen $U \subset G$ entsprechen eineindeutig den Körpererweiterungen $L/F$ innerhalb von $K$.*

**Weg.** Existenzsätze für Isomorphismen, denn diese sind wegen 2.2.3 großen Einschränkungen unterworfen.

**2.2.4 Satz.** *Sei $\sigma\colon F_1 \xrightarrow{\sim} F_2$ ein Körperisomorphismus, und sei $\varphi(X) = \sum a_k X^k \in F_1[X]$ irreduzibel. Sei $\varphi^\sigma(X) := \sum \sigma(a_k) X^k \in F_2[X]$. Dann gilt:*

*(i) $\varphi^\sigma(X)$ ist wieder irreduzibel.*

*(ii) Seien $K_1/F_1$, $K_2/F_2$ Körpererweiterungen, und $\alpha_1 \in K_1, \alpha_2 \in K_2$ Nullstellen der Polynome $\varphi(X), \varphi^\sigma(X)$.*

*Dann setzt sich $\sigma$ eindeutig fort zu einem Isomorphismus $\tilde{\sigma}\colon F_1(\alpha_1) \xrightarrow{\sim} F_2(\alpha_2)$ mit $\tilde{\sigma}(\alpha_1) = \alpha_2$.*

$$\begin{array}{ccc} \varphi(X) \in F_1 & \xrightarrow[\sigma]{\sim} & F_2 \ni \varphi^\sigma(X) \\ \downarrow & & \downarrow \\ F_1(\alpha_1) & \xrightarrow[\tilde{\sigma}]{\sim} & F_2(\alpha_2) \end{array}$$

*Beweis.* (i) $F_1 \xrightarrow[\sigma]{\sim} F_2$ induziert einen Isomorphismus

$$\hat{\sigma} : F_1[X] \xrightarrow{\sim} F_2[X], \quad f(X) \mapsto f^\sigma(X)$$

(ii) Betrachte:

$$\begin{array}{ccc} F_1[X]/(\varphi(X)) & \xrightarrow[\hat{\sigma}]{\sim} & F_2[X]/(\varphi^\sigma(X)) \\ \text{ist ein Körper, weil } \varphi(X) \text{ irreduzibel} & & \text{Körper, weil } \varphi^\sigma \text{ irreduzibel} \\ e_{V_{\alpha_1}} \downarrow \sim & & e_{V_{\alpha_2}} \downarrow \sim \\ F_1(\alpha_1) & \xrightarrow[\tilde{\sigma}]{\sim} & F_2(\alpha_2) \end{array}$$

Alle Abbildungen sind Isomorphismen, also auch $\tilde{\sigma}$. □

**2.2.5 Folgerung.** *Seien $F(\alpha)/F$ und $F(\beta)/F$ zwei einfache Körpererweiterungen. Dann ist folgendes äquivalent:*

*(i) Es existiert ein $F$-Isomorphismus $\sigma\colon F(\alpha) \to F(\beta)$ mit $\sigma(\alpha) = \beta$.*

*(ii) $\alpha$ und $\beta$ haben das selbe Minimalpolynom.*

*Beweis.* (i) $\Rightarrow$ (ii) ist klar (2.2.3)
(ii) $\Rightarrow$ (i) Spezialfall von 2.2.4: Nimm in 2.2.4 $F_1 = F_2 = F$ und $\sigma = \mathrm{id}_F$ □

**2.2.6 Definition** (Zerfällungskörper). *Sei $f(X) \in F[X]$. Eine Körpererweiterung $K/F$ heißt* Zerfällungskörper *von $f(X)$, falls gilt:*

*(i) $f(X)$ zerfällt in $K[X]$ in Linearfaktoren*

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i) \in K[X]$$

*(ii) $K = F(\alpha_1, \ldots, \alpha_n)$, d.h. $K$ ist minimal.*

**2.2.7 Satz** (Eindeutigkeit des Zerfällungskörpers). *Sei $\sigma\colon F_1 \xrightarrow{\sim} F_2$ ein Isomorphismus mit*

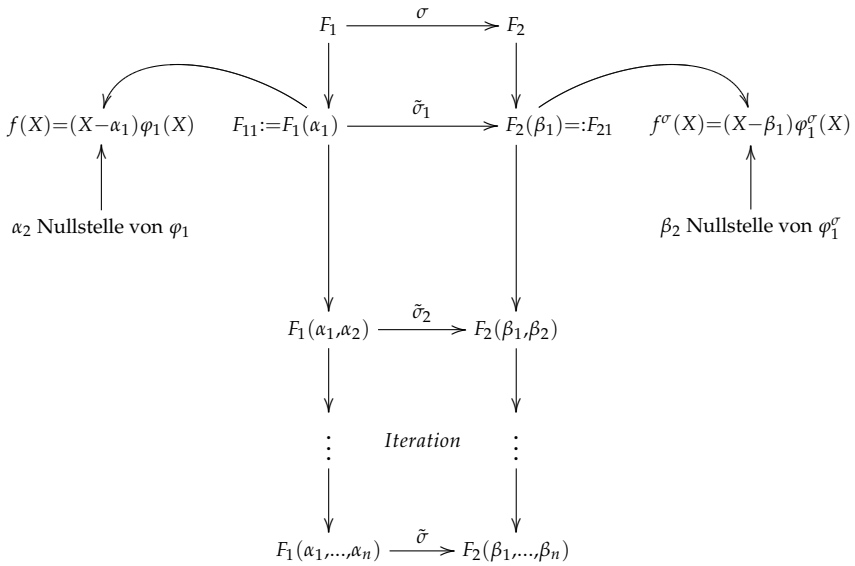
$$F_1[X] \ni f(X) \mapsto f^\sigma \in F_2[X]$$

*Sei $F_1(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von $f(X)$ und $F_2(\beta_1, \ldots, \beta_n)$ einer von $f^\sigma(X)$. Dann lässt sich $\sigma$ fortsetzen zu einem Isomorphismus*

$$\tilde{\sigma}\colon F_1(\alpha_1, \ldots, \alpha_n) \to F_2(\beta_1, \ldots, \beta_n)$$

*wobei $\tilde{\sigma}(\alpha_i) = \beta_{\pi(i)}$ mit einer eventuellen Permutation $\pi$ der Indizes.*

*Beweis.* Durch Iteration von 2.2.4:




□

**2.2.8 Bemerkung.** Sei $F_1 = F_2 = F$ und $\sigma = \mathrm{id}_F$. Dann gilt:

(i) Je zwei Zerfällungskörper eines Polynoms $f(X) \in F[X]$ sind $F$-isomorph.

(ii) Ist $L/F$ ein „große" Erweiterung, dann gibt es innerhalb von $L$ nur einen Zerfällungskörper von $f(X)$.

*Beweis.* (i) Dies ist ein Spezialfall von 2.2.7.
(ii) Seien $F(\alpha_1, \ldots, \alpha_n), F(\beta_1, \ldots, \beta_n) \subseteq L$ zwei Zerfällungskörper.

$$\Rightarrow f(X) = \prod_{i=1}^{n}(X - \alpha_i) = \prod_{i=1}^{n}(X - \beta_i)$$

in $L$. Aber $L[X]$ ist faktoriell, d.h. Primfaktorzerlegung ist eindeutig.

$$\begin{aligned} &\Rightarrow \quad \alpha_i = \beta_i \quad \text{bis auf Vertauschung} \\ &\Rightarrow \quad F(\alpha_1, \ldots, \alpha_n) = F(\beta_1, \ldots, \beta_n) \end{aligned}$$

□

*16. Vorlesung vom 16.02.2004*

**2.2.9 Definition** (normal). *Ein Körpererweiterung $K/F$ heißt* n o r m a l, *falls:*

*(i) $K/F$ ist algebraisch*

*(ii) für alle irreduziblen Polynome $\varphi(X) \in F[X]$ gilt: Wenn $\varphi(X)$ eine Nullstelle in $K$ hat, dann müssen sogar alle Nullstellen in $K$ liegen, d.h. $\varphi(X) \in K[X]$ zerfällt in Linearfaktoren*

**Bemerkung** (zu *(ii)*). Wenn $[K : F] = n < \infty$ und $\varphi(X) \in F[X]$ irreduzibel mit Nullstelle in $K$, dann folgt: $\deg(\varphi) \mid [K : F]$ (vgl. 2.1.5, 2.1.8). In *(ii)* sind also nur irreduzible Polynome mit der Eigenschaft $\deg(\varphi) \mid [K : F]$ zu testen.

**2.2.10 Satz.** *Sei $K/F$ eine endliche Erweiterung. Dann ist $K/F$ normal genau dann, wenn ein (nicht notwendig irredzibles) Polynom $f(X) \in F[X]$ existiert, so dass $K = Z_F(f)$ der Zerfällungskörper von $f(X)$ ist.*

*Beweis.* ($\Rightarrow$) Voraussetzung $K/F$ endlich, also $K = F(\alpha_1, \ldots, \alpha_n)$ (nach 2.1.9). $f_i$ sei Minimalpolynom von $\alpha_i$ über $F$. $f(X) := \prod_{i=1}^{n} f_i(X)$. Da $K/F$ normal, zerfallen alle $f_i(X)$ und damit auch $f(X)$ in $K$ in Linearfaktoren, also $K = Z_F(f)$.
($\Leftarrow$) $\phi(X) \in F[X]$ sei irreduzibel mit einer Nullstelle $\alpha \in K$. Dann gilt:

$$\phi(X) = (X - \alpha)\psi(X) \in K[X]$$

Wir müssen zeigen, dass $\phi(X)$ über $K$ in Linearfaktoren zerfällt.

Sei $\phi_1(X) \in K[X]$ ein irreduzibler Teiler von $\psi(X)$, sei $\Omega/K$ ein Stammkörper von $\phi_1(X)$ (vgl. 2.1.10), und sei $\alpha' \in \Omega$ eine Nullstelle von $\phi_1(X)$.

Da $\alpha'$ auch Nullstelle von $\phi(X) \in F[X]$ ist, und da $\phi(X)$ irreduzibel ist, folgt: $\phi(X)$ ist das Minimalpolynom von $\alpha'$ über $F$. Weil $\alpha$ und $\alpha'$ über $F$ dasselbe Minimalpolynom haben, folgt aus 2.2.5: Es gibt einen $F$-Isomorphismus $\sigma : F(\alpha) \xrightarrow{\sim} F(\alpha')$, mit $\sigma(\alpha) = \alpha'$.

Setze $F_1 = F(\alpha)$, $F_2 = F(\alpha')$. Betrachte die Zerfällungskörper $Z_{F_1}(f)$ und $Z_{F_2}(f)$ des Polynoms $f$ über $F_1$ bzw. $F_2$. Wende 2.2.7 an mit $f^\sigma = f$. Danach setzt sicht $\sigma$ fort in $\tilde{\sigma} : Z_{F_1}(f) \xrightarrow{\sim} Z_{F_2}(f)$.

Doch wir haben $K = Z_F(f) = Z_{F_1}(f) \subset \Omega$ und $F_2 = F(\alpha') \subset \Omega$. Also: Das Polynom $f(X)$ zerfällt über $\Omega$ und der Körper $F_2$ ist in $\Omega$. Daher können wir $Z_F(f) \subset \Omega$ annehmen, denn es gibt einen Zerfällungskörper von $f(X) \in F[X] \subset F_2[X]$, welcher in $\Omega$ liegt.

Damit liegt das Bild $\tilde{\sigma}(K)$ in $\Omega$. Da $\tilde{\sigma}(K)$ ebenso wie $K$ ein Zerfällungskörper von $f(X)$ über $F$ ist, folgt aus 2.2.8(ii) $\tilde{\sigma}(K) = K$, d.h.

$$K = Z_F(f) = Z_{F_1}(f) = Z_{F_2}(f)$$

Demzufolge ist $\alpha' \in K$, und wir sehen sukzessive, dass $\phi(X)$ über $K$ in Linearfaktoren zerfällt. □

**2.2.11 Beispiele für Normalkörper.** a) $K =$ endlicher Körper $\mathbb{F}_q$ der char $= p \Rightarrow q =$ Potenz von $p \Rightarrow K$ ist Zerfällungskörper des Polynoms $X^q - X \in \mathbb{F}_p[X] \Rightarrow K/\mathbb{F}_p$ ist normal.

b) $[K : F] = 2$. Finde $\alpha \in K, \alpha \notin F$. Wegen 2.1.8 muss $\alpha$ Nullstelle eines quadratischen Polynoms sein. $X^2 + pX + q = 0$, Nullstellen $\alpha_1, \alpha_2, \alpha_1 + \alpha_2 = -p, \alpha_1 \in K \Rightarrow \alpha_2 \in K$, also ist $K$ der Zerfällungskörper.

c) Einheitswurzelkörper: $K = F(\xi), \xi^n = 1$ minimal, Nullstelle von $X^n - 1$. Alle anderen Nullstellen sind Potenzen von $\xi$, also $\in K$.

**2.2.12 Definition** (Galoiserweiterung)**.** *Die Körpererweiterung $K/F$ heißt* g a l o i s c h, *falls die Erweiterung normal und separabel ist. (Die Minmalpolynome aller $x \in K$ haben nur einfache Nullstellen.)*

**2.2.13 Satz.** *Sei $K/F$ eine endliche Galoiserweiterung. Dann gilt:*

*(i) Ist $\Omega/K$ irgendeine Erweiterung, und ist $\sigma : K \to \Omega$ irgendein $F$-Isomorphismus mit Werten in $\Omega$. Dann ist $\sigma(K) = K$. (Man spricht in der Körpertheorie immer nur von Isomorphismen, selbst dann wenn die Abbildung nicht surjektiv ist.)*

*(ii) $\sigma(K) = K$, d.h. $\sigma$ ist $F$-Automorphismus von $K$ und diese Automorphismen bilden bezüglich Hintereinanderausführung eine Gruppe ($1 = \mathrm{id}_K$) $G = G_{K/F}$, die* G a l o i s g r u p p e *der Erweiterung. Wenn $K = Z_F(f(X))$ der Zerfällungskörper von $f(X)$, dann haben wir eine natürliche Einbettung: $G_{K/F} \subset$ Gruppe der Permutationen der Nullstellen von $f(X)$.*

*(iii) Die Menge der Fixpunkte $K^G := \{x \in K, \sigma(x) = x \forall \sigma \in G\} = F$.*

*(iv) $\#G = [K : F]$.*

*Beweis.* (i) $K$ ist normal und endlich über $F \Rightarrow K = Z_F(f)$. $G$ ein $F$-Isomorphismus $\Rightarrow \sigma(K) = Z_F(f^\sigma), f^\sigma = f$. Also: $\sigma(K)$ muss Zerfällungskörper für dasselbe Polynom sein. Aber innerhalb eines großen Körpers $\Omega$ ist der Zerfällungskörper eindeutig bestimmt. (vgl. 2.2.8)

(ii) Durch Hintereinanderausführung $\sigma_1 \circ \sigma_2$ bekommen wir offensichtlich eine Gruppe $G$. Anwendung von $\sigma$ muss die Nullstellen von $f(X)$ in sich überführen, $f \in F[X]$. D.h.: $\sigma$ permutiert die Nullstellen und dadurch ist $\sigma$ eindeutig bestimmt, weil $K = Z_F(f)$ durch die Nullstellen von $f(X)$ erzeugt ist.

(iii) als Übung. (gzz. wenn $x \notin F$, dann existiert $\sigma$ mit $\sigma(x) \neq x$).

(iv) Benutze das $K/F$ separabel und endlich ist. Satz vom primitiven Element $\Rightarrow K = F(\gamma)$, erzeugt durch ein einziges Element. Sei $f_\gamma(X) =$ Minimalpolynom von $\gamma$ über $F$. Insbesondere ist dann $K$ der Zerfällungskörper von $f_\gamma(X)$. $\Rightarrow G_{K/F} \subset$ Permutationen von $f_\gamma(X)$. $\sigma \mapsto$ Permutation. Jetzt ist $\sigma$ bereits durch den Wert $\sigma(\gamma)$ voll bestimmt, weil $K = F(\gamma)$. Möglichkeiten für $\sigma(\gamma) =$ # Nullstellen von $f_\gamma(X) = [K : F]$ (da separabel). Jede Möglichkeit ist auch realisierbar. 2.2.5 $\Rightarrow$ *( i v )*.

□

**2.2.14 Hauptsatz** (der Galoistheorie)**.** *$K/F$ sei eine endliche Galoiserweiterung, und $G = G_{K/F}$. Dann hat man eine Bijektion:*

$$\begin{aligned} \{ \textit{ Zwischenkörper in } K/F \} &\longleftrightarrow \textit{ Untergruppen von } G \\ L &\longmapsto G_{K/L} = \textit{ L-Isomorphismen von } K \\ K^H := \{x \in K, \sigma(x) = x \forall \sigma \in H\} &\longleftarrow\!\shortmid H \end{aligned}$$

*Diese Bijektion hat folgende Eigenschaften:*

*(i)* $L_1 \subset L_2 \Rightarrow G_{K/L_1} \supset G_{K/L_2}$

*(ii)* $\sigma \in G \Rightarrow \boxed{G_{K/\sigma(L)} = \sigma \circ G_{K/L} \circ \sigma^{-1}}$

$$\begin{array}{ccccc} K & \supset & L & \supset & F \\ & \circlearrowleft & \downarrow & \circlearrowright & \\ & & \sigma(L) & & \end{array}$$

*(iii) $L/F$ ist ein Normalkörper genau dann, wenn die Untergruppe $G_{K/L}$ ein Normalteiler in $G$ ist. Dann darf man die Faktorgruppe bilden, und es gilt:*

$$G/G_{K/L} = G_{L/F}$$

*Beweisidee.* $K/F$ normal und separabel, $K \supset L \supset F \Rightarrow K/L$ ist ebenfalls normal und separabel. Damit ist die Abbildung $L \to G_{K/L} \subset G$ wohldefiniert. $G \supset H =$ Untergruppe:

$$\sigma \in H: \quad \begin{aligned} \sigma(x \pm y) &= \sigma(x) \pm \sigma(y) \\ \sigma(x \cdot y) &= \sigma(x) \cdot \sigma(y) \\ \sigma(x^{-1}) &= \sigma(x)^{-1} \end{aligned} \qquad (*)$$

$x, y \in K^H$, d.h. $\sigma(x) = x, \sigma(y) = y \forall \sigma \in H$

$$(*) \quad \Rightarrow \quad x \pm y, x \cdot y, x^{-1} \in K^H$$

Also ist $K^H$ ein Körper, und $K \supset K^H \supset F$. Also: Beide Abbildungen sind wohldefiniert. Zu zeigen: $L \to L, H \to H$

Eigenschaften: (i) ist klar!

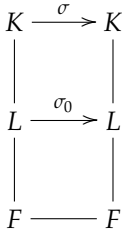
(ii) $G \supset H =$ Untergruppe, $\sigma \in G \Rightarrow \sigma H \sigma^{-1}$ ist wieder Untergruppe:

$$\begin{aligned}(\sigma h_1 \sigma^{-1})(\sigma h_2 \sigma^{-1}) &= (\sigma h_1 h_2 \sigma^{-1}) \\ (\sigma h \sigma^{-1})^{-1} &= \sigma h^{-1} \sigma^{-1} \\ \Rightarrow \quad \#\sigma H \sigma^{-1} &= \#H\end{aligned}$$

$$\#\sigma G_{K/L} \sigma^{-1} = \#G_{K/L} = \frac{[K:F]}{[L:F]} = \frac{[K:F]}{[\sigma(L):F]} = \#G_{K/\sigma(L)}$$

Genügt zu zeigen: $\sigma G_{K/L} \sigma^{-1} \subseteq G_{K/\sigma(L)}, y = \sigma(x) \in \sigma(L)$.

(iii) Aus (ii) folgt: $\sigma(L) = L$ genau dann, wenn $\sigma G_{K/L} \sigma^{-1} = G_{K/L}$. $L/F$ normal gdw. $\sigma(L) = L \forall \sigma \in G$ ($\Rightarrow$ schon klar). Betrachte die Abbildung $\sigma \in G \mapsto \sigma|_L \in G_{L/F}$ (Einschränkung des Argumentenbereichs). Offensichtlich ist $G_{K/L} =$ Kern dieser Abbildung und die Abbildung ist surjektiv, wegen unserer Existenzsätze. Jedes $\sigma_0 \in G_{L/F}$ läßt sich fortsetzen zu einem $\sigma \in G_{K/F}$. Homomorphiesatz $\Rightarrow G/G_{K/L} \cong G_{L/F}$.




□

## 2.3 Anwendungen der Galoistheorie

### 2.3.1 Auflösbarkeit polynomialer Gleichungen $f(X) = 0$ durch Radikale

Nach E. GALOIS und N. H. ABEL.

**2.3.1 Definition** (Radikalerweiterung, R/E)**.** *Eine endliche Erweiterung $L/K$ heisst* R a d i k a l e r w e i t e r u n g, *falls:*

$$\begin{aligned}K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = L \\ \alpha_1^{r_1} \in K, \quad \alpha_2^{r_2} \in K(\alpha_1), \quad \alpha_3^{r_3} \in K(\alpha_1, \alpha_2), \quad \ldots\end{aligned}$$

*$\alpha_1$ Wurzel eines Elementes aus $K$, $\alpha_2$ Wurzel eines Elementes aus $K(\alpha_1)$ etc. Abkürzung: $L/K = R/E$.*

**2.3.2 Definition** (Auflösbare Erweiterung, A/E)**.** *Eine endliche Erweiterung $L/K$ heißt* a u f l ö s b a r, *falls:*

*(i) $L/K$ ist eine Galoiserweiterung*

*(ii) die Galoisgruppe $G_{L/K}$ ist eine auflösbare Gruppe.*

*Kurz: $L/K = A/E$.*

**Definition** (auflösbare Gruppe)**.** *Gruppentheorie: Eine endliche Gruppe $G$ heißt* a u f l ö s b a r, *falls*

$$G = G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$$

*existiert, so dass $G_{i+i}$ Normalteiler in $G_i$ ist, und die Faktorgruppe $G_i/G_{i+1}$ Primzahlordnung (d.h. zyklisch) $\cong \mathbb{Z}/p\mathbb{Z}$ für irgendeine Primzahl $p$ hat.*

**Beispiel.**
- Permutationsgruppe $S_3 \overset{2}{\supset} A_{3\text{ gerade }p} \overset{3}{\supset} \{1\}$ ist auflösbar. $S_4$ ist auch noch auflösbar. $S_n$ für $n \geq 5$ ist nicht auflösbar. In der $S_5$ gibt es einen einzigen Normalteiler, nämlich die $A_5$, $S_5 \underset{2}{\supset} A_5$. $\#A_5 = 60$ und $A_5$ besitzt keinen Normalteiler.
- Körpererweiterung $L/K$, R/E, A/E

Eine RA/E $L/K$ sei eine Körpererweiterung, welche beide Eigenschaften in sich vereint.

$f(X) \in K[X]$ irreduzibel und separabel $\rightsquigarrow$ Zerfallskörper $L = Z_K(f) \Rightarrow L/K$ ist galoisch $\rightsquigarrow G_{L/K}$. Man nennt $G_{L/K} = G(f)$ die Galoisgruppe des Polynoms $f$. Gruppe $G(f)$ ist jedenfalls eindeutig bis auf Isomorphie.

**Definition.** *Wir nennen ein Polynom $f(X) \in K[X]$* d u r c h R a d i k a l e a u f l ö s b a r, *falls sich der Zerfällungskörper $Z_K(f)/K$ in eine Radikalerweiterung $E/K$ einbetten lässt.*

**Bemerkung.** Es wäre unklug zu sagen: falls $Z_K(f)/K$ selbst eine Radikalerweiterung ist, denn wenn $E/K$ Radikalerweiterung und $L$ ein Zwischenkörper, dann muss zwar $E/L$ auch Radikalerweiterung sein, aber nicht unbedingt $L/K$ (vgl. 2.3.1).

**2.3.3 Satz** (Anwendung der Galoistheorie)**.** *Abgesehen von Ausnahmefällen, welche durch* $\text{char}(K) = p$ *verursacht werden, gilt: Jede A/E lässt sich vergrößern zu einer RA/E. Jede R/E lässt sich vergrößern zu einer RA/E. (ohne Beweis)*

*Beweis.* Wenn es keine Probleme mit der Separabilität gibt, also z.B. im Charakteristik 0 Fall, dann kann man zeigen:

Ist $E/K$ eine Radikalerweiterung, dann ist die galoissche Hülle (= Kompositum aller $\sigma(E)$, wobei $\sigma$ die möglichen $K$-Isomorphismen durchläuft) ebenfalls eine Radikalerweiterung, und darüber hinaus ist diese Erweiterung auflösbar.

Umgekehrt ist $E/K$ eine auflösbare Erweiterung, und adjungiert man alle Einheitswurzeln der Ordnung $[E : K]$, dann ist die vergrößerte Erweiterung ebenfalls auflösbar, und darüber hinaus ist es eine Radikalerweiterung. Grund: Es sei $L/F$ eine zyklische Erweiterung vom Primzahlgrad $p$, und die $p$-ten Einheitswurzeln seien im Grundkörper $F$. Dann kann man $L$ durch Ausziehen einer $p$-ten Wurzel konstruieren. (Das geht natürlich immer für $p = 2$.) □

**2.3.4 Anwendung.** Sei $f(X) \in K[X]$ ein irreduzibles separables Polynom. Sei $G(f) = G_{Z_K(f)/K}$ seine Galoisgruppe. Dann ist folgendes äquivalent:

(i) $G(f)$ ist auflösbare Gruppe.

(ii) $f(X)$ ist durch Radikale auflösbar.

(iii) $f(X)$ besitzt einen Stammkörper $S/K$, welcher sich in eine R/E $L/K$ einbettet.

*Beweis.* (i) $\Rightarrow$ (ii): Voraussetzung $Z_K(f)/K$ ist A/E. $\Rightarrow$ Wir können die Erweiterung vergrößern zu einer RA/E $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (iii): klar!

(iii) $\Rightarrow$ (i): Voraussetzung: $S/K \subset L/K$ vom Typ R/E. Wir können $L/K$ weiter vergrößern zu einer Erweiterung $E/K$ vom Typ RA/E. Insbesondere ist $E/K$ normal. Also jedes irreduzible Polynom mit Nullstelle in $E$ muss über $E$ in Linearfaktoren zerfallen. Daher: $S \subset L \subset E$, also $f(X)$ muss in $E$ zerfallen $\Rightarrow K \subset Z_K(f) \subset E$. $Z_K(f)/K$ ist ebenso wie $E/K$ eine Galoiserweiterung $\Rightarrow G_{Z_K(F)/K} = G_{E/K}/G_{E/Z_K(f)} = G(f)$ (Hauptsatz (iii)). Nach Voraussetzung ist $G_{E/K}$ auflösbare Gruppe. Gruppentheorie: Die Faktorgruppe einer auflösbaren Gruppe ist stets wieder auflösbar. $\Rightarrow G(F)$ auflösbar. □

$f(X) = X^2 + pX + q \rightsquigarrow$ Allgemeine Lösungsformel durch Radikale. Entsprechend betrachten wir die allgemeine Gleichung $n$-ten Grades. Die Galoisgruppe einer solchen allgemeinen Gleichung ist genau die Gruppe $S_n$ der Permutationen der $n$ Nullstellen. $\Rightarrow$ Für $n \geq 5$ ist ein allgemeines Polynom $n$-ten Grades nicht durch Radikale auflösbar, weil $S_n$ keine auflösbare Gruppe ist.

### 2.3.2 Konstruktion mit Zirkel und Lineal

#### Allgemeine Theorie

Punktmenge $M \subset E$ in der Ebene ($\#M \geq 2$). Bilde Geraden $g$ auf denen 2 verschiedene Punkte von $M$ liegen. Bilde Kreise $K$ (Mittelpunkt $\in M$, Radius $= d(m_1, m_2), m_1, m_2 \in M$). Aus $M$ enthält man die größere Punktmenge $M'$ durch Hinzunahme der Schnittpunkte.

$$M \subset M' : \quad g_1 \cap g_2, g \cap k, k_1 \cap k_2$$
$$M = M_0 \mapsto M_1 = {M_0}' \mapsto M_2 = {M_1}' \mapsto \cdots$$
$$\hat{M} = \bigcup_{n=0}^{\infty} M_n$$

$\hat{M} =$ alle Punkte, welche sich aus $M$ mit Zirkel und Lineal konstruieren lassen.

**Analytische Geometrie.** $E = \mathbb{C}$, Menge $M$ besteht aus Zahlen, $\#M \geq 2$. Normiere das Koordinatensytem so, dass $0, 1 \in M$. Was ist $\hat{M}$? Bilde zu $M$ die Menge $\bar{M} =$ konjugiert komplex. Bilde den Körper $K = \mathbb{Q}(M \cup \bar{M})$. Dann gilt:

**2.3.5 Satz.** *$z \in \hat{M}$ genau dann, wenn $z$ in einer 2R/E (d.h. $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots$, und $\alpha_1^2 \in K, \alpha_2^2 \in K(\alpha_1)$ usw.) des Körpers $K$.*

*Beweis.* Siehe E. Kunz, Algebra, 1.14 □

Inhaltlich bedeutet dies: Mit Zirkel und Lineal kann man die Grundoperationen $+, -, \cdot, :$ für komplexe Zahlen $z \in \mathbb{C}$ sowie das Ausziehen einer Quadratwurzel $\sqrt[2]{z}$ realisieren

$$\text{Sei } z \in \hat{M} \Rightarrow [K(z):K] = \text{ Potenz von 2 }, \quad \text{weil } \underbrace{K \subset K(z) \subset L}_{\text{2-Potenz}} = K(\alpha_1, \ldots, \alpha_n)$$

$$[L:K] = [L:K(z)][K(z):K] \Rightarrow [K(z):K] = \text{2-Potenz notwendig}$$

Eine hinreichende Bedingung folgt aus der Galoistheorie:

**2.3.6 Satz.** *$z \in \hat{M}$ genau dann, wenn $f$ das Minimalpolynom von $z$ über $K$ folgende Eigenschaft hat: Der Zerfällungskörper $Z_K(f)/K$ ist eine Erweiterung von 2-Potenzgrad.*

**Quadratur des Kreises.** $r$ Radius, Kreis mit Fläche $F = \pi r^2$. Aufgabe: Beginne mit $M = \{0,1\}$. Konstruiere dann $\sqrt{\pi}$. $K = \mathbb{Q}(M \cup \bar{M}) = \mathbb{Q}$.

Wenn das geht, dann muss $\mathbb{Q}(\sqrt{\pi})/\mathbb{Q}$ eine endliche Erweiterung vom Grad $2^r$ sein. Jedoch $\pi$ und damit $\sqrt{\pi}$ genügt über $\mathbb{Q}$ keiner polynomialen Gleichung.

**Konstruktion eines regelmäßiges $n$-Eck.** Gegeben $0, 1 \in \mathbb{C}$. Aufgabe: Konstruiere daraus $\zeta = e^{\frac{2\pi i}{n}}$. Notwendig: $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^r$. In diesem Fall ist die Bedingung auch hinreichend, weil $\mathbb{Q}(\zeta)/\mathbb{Q}$ eine normale Erweiterung ist.

**Satz.** *Das Minimalpolynom von $\zeta = e^{\frac{2\pi i}{n}}$ hat den Grad $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.*

**Satz** (Gauß)**.** *Das regelmäßige n-Eck ist konstruierbar genau dann, wenn $\varphi(n)$ eine Potenz von 2 ist.*

### Beispiele

**Klassifizierung der Erweiterungen $K/\mathbb{Q}$, welche Grad 2 haben.** Aussage: Jedes solche $K$ kann dargestellt werden als $K = \mathbb{Q}(\sqrt{d})$, wobei $d$ eine quadratfreie ganze Zahl ist. $d_1 \neq d_2 \Rightarrow \mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$.

Einheitswurzel in $K$: I.A. nur $\pm 1$. Zwei Sonderfälle: $\mathbb{Q}(\sqrt{-1}) \ni$ vier Einheitswurzeln, $\mathbb{Q}(\sqrt{-3}) \ni$ sechs Einheitswurzeln. Zu zeigen: $\exists d \in \mathbb{Z}, K = \mathbb{Q}(\sqrt{d})$, wenn $[K:\mathbb{Q}] = 2$

*Beweis.* Wähle $\gamma \in K, \gamma \notin \mathbb{Q}$ beliebig. Dann ist $K = \mathbb{Q}(\gamma)$, da die Elemente $(a + b\gamma)$ alle verschieden sind. $\gamma$ genügt einer Gleichung $\gamma^2 + a_1\gamma + a_0 = 0$ mit $a_1, a_0 \in \mathbb{Q}$. Dann ist für $\hat{\gamma} = \gamma + \frac{a_1}{2}, \hat{\gamma}^2 + (a_0 - (\frac{a_1}{2})^2 = 0$ und $\mathbb{Q}(\gamma) = \mathbb{Q}(\hat{\gamma})$.

Also kann man $\gamma = \sqrt{c}$ mit $c \in \mathbb{Q}$ annehmen. Sei $c = \frac{c_1}{c_2}, c_1, c_2 \in \mathbb{Z}, c_2 \neq 0$, dann ersetze $\gamma$ durch $c_2\gamma = c_2\sqrt{\frac{c_1}{c_2}} = \sqrt{c_1c_2} = \sqrt{d}$, mit $d = c_1c_2 \in \mathbb{Z}$. Dabei kann man $d$ quadratfrei annehmen. Ist $p^2 \mid d$, $p$ prim, ersetze $\sqrt{d}$ durch $\frac{1}{p}\sqrt{d} = \sqrt{\frac{d}{p^2}}$. Die Iteration führt zu $d$ quadratfrei.

Nun zu $d_1 \neq d_2 \Rightarrow \mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$. Annahme: $\sqrt{d_1} = a + b\sqrt{d_2}, a, b \in \mathbb{Q} \Rightarrow b \neq 0 \Rightarrow d_1 = a^2 + 2ab\sqrt{d_2} + b^2d_2 \Rightarrow a = 0$, sonst wäre $\sqrt{d_2}$ eine rationale Zahl $\lightning$. $\Rightarrow d_1 = b^2d_2$ mit $b \neq 0, b \in \mathbb{Q} \Rightarrow \operatorname{sgn}(d_1) = \operatorname{sgn}(d_2)$. Da $d_1$ und $d_2$ beide ganz und quadratfrei sind, folgt $b^2 = 1$.

Einheitswurzeln: $d > 0 \Rightarrow K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R} \Rightarrow \pm 1$ sind die einzigen Einheitswurzeln in K.

$d < 0$, $\zeta \in \mathbb{Q}(\sqrt{d})$. Ist $\zeta$ Nullstelle von $X^2 + pX + q$, dann auch $\overline{\zeta}$. Also $X^2 + pX + q = (X - \zeta)(X - \overline{\zeta})$, und daraus folgt $q = 1$. Also

$$\zeta = -(p/2) \pm (1/2)\sqrt{p^2 - 4}$$

Wenn die Einheitswurzel $\neq \pm 1$, dann muss jedenfalls unter der Wurzel eine negative Zahl stehen. Da $p$ ganz ist, gibt es nur die Möglichkeiten $p = 0$ oder $p = \pm 1$. □

Es gibt komplexe Zahlen $z$ mit der Eigenschaft $[\mathbb{Q}(z) : \mathbb{Q}] = 4$, und trotzdem ist $z$ nicht konstruierbar, weil der Zerfällungskörper $Z_{\mathbb{Q}}(f)/\mathbb{Q}$ das Minimalpolynom $f$ von $z$ einen Grad $[Z_{\mathbb{Q}}(f) : \mathbb{Q}] \neq$ Potenz von 2 hat.

**Beispiel.** $f(X) = X^4 - aX - 1 \rightsquigarrow$ Stammkörper $K/\mathbb{Q}$, $[K : \mathbb{Q}] = 4$. Wenn $K/\mathbb{Q}$ keine quadratischen Zwischenkörper $L$ hat, dann kann $K/\mathbb{Q}$ kein Normalkörper sein. Sonst hätten wir eine Gruppe $G$ der Ordnung 4. $G = \mathbb{Z}/4\mathbb{Z}$ oder $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow L$ existiert und wäre Fixkörper einer Untergruppe der #2. $G(f) \subseteq S_4$. Möglichkeiten: $D_4$ (#8), $A_4$ (#12), $S_4$ (#24). $D_4$ scheidet aus, weil hier drin würden wir $L$ wiederfinden. Also $G(f) = A_4, S_4$. $f(z) = 0$, $[\mathbb{Q}(z) : \mathbb{Q}] = 4$. Trotzdem ist $z$ nicht konstruierbar, denn $\#G(f) = 12, 24$ ist keine Potenz von 2.

# Literaturverzeichnis


[Art98] ARTIN, MICHAEL: *Algebra*. Birkhäuser Verlag, 1. Auflage, 1998. Kapitel 10-14 überdeckt die Vorlesung.

[Bou98] BOURBAKI, NICOLAS: *Algebra II*. Springer Verlag, 1998. Kapitel 7, Moduln über Hauptidealringen. (französisch, englische und russische Übersetzung existiert.) Bringt die allgemeinsten Resultate die es hier gibt.

[Kun02] KUNZ, ERNST: *Algebra*. Vieweg, 3. Auflage, 2002. §1 bringt schöne Einführung in Konstruktionen mit Zirkel und Lineal. Der Hauptsatz benutzt natürlich Galoistheorie und kommt erst in §12, Satz 12.12, anschliessend die Hauptanwendungen.

[vdW93] WAERDEN, BARTEL L. VAN DER: *Algebra I*. Springer Verlag, 9. Auflage, 1993. Kapitel 6 und Kapitel 8 bringen die Grundlagen der Körpertheorie und Galoistheorie, ähnlich wie in der Vorlesung. Insbesondere kommt hier der §63 über die allgemeine Gleichung n-ten Grades.

# Index

# Anhang A

# Übersicht

**Legende**

D Definition L Lemma/Hilfsatz F Folgerung/Korollar
S Satz K Bemerkung B Beispiel

## 1 Ringe

### 1.1 Definitionen & Grundlagen

1 D Ring – D Ring mit 1, kommutativer R., nullteilerfrei
– B Marizenring über $K$
2 S Rechenregeln im Ring
– D 0-Ring
3 D Teilring – K Teilringe mit/ohne 1
– B TR+1 $\mathbb{Z} \supset 2\mathbb{Z}$ TR-1
4 B Matrizenring über $R$
5 D Zentrum $Z(R)$
6 B $Z(R^{n\times n}) = \{\mathrm{Diag}(z); z \in Z(R)\}$
7 D Einheit – F $1 \in R^\times$ – F $(R^\times, \cdot)$ Gruppe
– B $\mathbb{Z}^\times = \{\pm 1\}$, $K[X]^\times = K - 0$, $(K^{n\times m})^\times = \mathrm{GL}_n(K)$
8 D Potenzen im Ring

– D Schiefkörper – B Quaternionen $\mathbb{H}$
9 D $K$-Algebra, dim – B $K^{n\times n}$, $K[X]$, $\mathbb{H}$
– K Algebra durch Multiplikation auf Basen
– B Basen von $\mathbb{H}$ – K Quaternionengruppe
– K Einbettung von $K$ – B $\lambda I_n$, $K[X]$
10 S Über Divisionalgebren

— D geordneter Ring — F Eigenschaften
— F Existenz der Ordnung
— D Wohlgeordneter Ring
11 S Charakterisierung von $\mathbb{Z}$ 12 F Division mit Rest in $\mathbb{Z}$

### 1.2 Ideale, Faktorringe und Homomorphiesatz

1 D Ring-Homorphismus
– F $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ Hom. $\Leftrightarrow m \mid n$
2 D Ring-Isomorphismus – B Chin. Restsatz
3 S Kern und Bild von Homomorphismen, injektiv

4 D Ideal – B Hauptideale – L $\mathbb{Z}$ HIR
5 S $R/I$ Ring – D Faktorring
6 S Homomorphiesatz
7 K $I \subset J \leftrightarrow J/I \subset R/I$
8 S $R$ kom. mit 1, keine echten Ideale $\Leftrightarrow$ $R$ Körper
9 S $I$ maximal $\Leftrightarrow$ $R/I$ Körper

### 1.3 Teilbarkeit in Ringen

1 D Teiler, Vielfaches – D echter Teiler, assozierte
2 S $a \mid b \Leftrightarrow Ra \supset Rb$
– F $0 \mid a$ und $a|x \forall x \in R$
3 K Ziel: Hauptsatz der Arithmeik

4 D Irreduzible, Primelemente
5 L $0, a$ irreduzibel bzw. prim
– K irreduzibel/prim $\Leftrightarrow$ assozierte irreduzibel/prim
6 S nullteilerfrei / HIR $\Rightarrow$ (prim/irred. $\Rightarrow$ irred./prim)
– K $\mathbb{Z}$ ntf & HIR: irreduzibel $\Leftrightarrow$ prim

7 D Teilerkettensatz
8 S Satz von Euklid – F $\mathbb{Z}$ unendliche viele irred. Zahlen

9 D äquivalente, eindeutige Zerlegung, faktorieller Ring
10 S Hauptsatz $\sim$ faktorielle Ringe & TKS für Elemente
— L assozierte & Vielfache im fakt. Ring
— K Variante der Zerlegung — B $\mathbb{Z}$

11 S TKS für Ideale & Äquivalenzen
12 D Noethersche Ringe

### 1.4 Euklidische Ringe

1 D Integritätsbereich, Euklidischer Ring
2 B $(\mathbb{Z}, |\circ|)$, $(K[X], \deg)$
3 S Eigenschaften euklid. Ringe
4 S Hauptsatz: fakt. Ringe $\supset$ ntf HIR $\supset$ euklid. Ringe
5 K ggT und kgV ex. & eindeutig (bis aus Assozierte)

### 1.5 Quotientenkörper & Satz von Gauß

1 S Konstruktion des Quotientenkörpers
2 S Satz von Gauß: $R$ fakt. $\Rightarrow$ $R[X]$ fakt.
/1 L $R$ IB $\Rightarrow$ $R[X]$ IB

/2 L $R, R[X] \ni p \neq 0$ irred. $\Leftrightarrow p$ prim
/3 L In $R$ ex. ggT und kgV, eindeutig bis auf Assoziierte
/4 L Inhalt, primitives Polynom, Zerlegung
/5 L $c(ab) \sim c(a)c(b)$, $a, b$ primitiv $\Rightarrow ab$ primitiv
/6 L $f \in K[X] \Rightarrow f = c(f) \cdot \varphi$ „eindeutig“
/7 L Irreduzible Elemente in $K[X]$, Typ I & II
/8 L $K[X] \in f$ irreduzibel $\Rightarrow$ prim
/9 L TKS für Elemente gilt in $R[X]$
— B $\mathbb{Z}[X]$ faktoriell, kein HIR

### 1.6 Polynomring in mehreren Variablen & Universalität

1 D Multipotenz, Grad
2 D Polynomring – D $m$-Form – B Quadratische Polynome
3 D Modul, freier, $R$-Aktion, $R$-Algebra – B $R/I$ nicht frei

– D Kategorie, Morphismus
4 S Hauptsatz: $R[X_i]$ universelles Anfangsobjekt, ev
5 L Universelle Anfangsobjekte isomorph
6 F Natürlicher Isomorphismus $R[X_1] \cdots [X_n] \xrightarrow{\sim} R[X_i]$
7 L $R$ ntf bzw. faktoriell $\Rightarrow R[X_i]$ ntf bzw. faktoriell
8 D erzeugt, Relationenideal, Relationen
– F Relationen: $f_i(a) = 0$, $f_i \in \ker(\mathrm{ev})$
– K Jede komm. Grp ist $\mathbb{Z}$-Modul, jeder Ring ist $\mathbb{Z}$-Algebra

### 1.7 Moduln über Hauptidealringen

1 L $A \in \mathrm{GL}_n(R) \Leftrightarrow \det A \in R^\times$
2 D $A \sim B \Leftrightarrow B = PAQ, P, Q \in \mathrm{GL}(R)$
3 S Hauptsatz: Smithsche Normalform – D $k$-Minor
– K $k$-Minor Lin.komb. von $(k-1)$-Minoren, Rang als Max.
4 D Invariante Teiler, Determinantenteiler
5 L Über $k$-Minoren von $AB \in R^{l \times n}$
6 F $A \in R^{m \times n} \Rightarrow AX = 0$ hat nichtriviale Lösungen

7 D Grundbegriffe über $R$-Moduln
– D freie Moduln – K frei: $M \cong R^{n \times 1}$
8 S $R$ HIR, $M$ hat $n$ Erzeugende $\Rightarrow n+1$ Elemente lin.abh.
9 L $\mathrm{Rang}(M)$: Alle Basen haben gleiche Kardinalzahl
– B $\mathbb{Z} \times \mathbb{Z} \supset 5\mathbb{Z} \times 7\mathbb{Z}$, beide Rang $= 2$
10 S Koordinatenmatrix und Basiswechsel
11 F Folgerung für freie Moduln und Untermoduln
12 L $R$ noethersch $\Leftrightarrow$ Untermodul endlich erzeugt
13 S Hauptsatz: Klassifizierung endlich erzeugter Moduln
— D exakte Sequenz
14 D Torsionelemente, Torsionsmodule
15 D Annulator
16 L $M_{tor} \cong \bigoplus_i R/\delta_i$
17 K Weiterverarbeitung des Hauptsatzes

### 1.8 Normalformen quadratischer Matrizen

1 L $V$ $K[X]$-Modul $\Leftrightarrow V$ $K$-VR, $X$ lineare Operator auf $V$
2 L $V \cong W \Leftrightarrow \exists \phi \in \mathrm{Iso}(V, W), \phi X = X\phi \Leftrightarrow [X]_B \sim [X]_C$
3 S $V_A$, $A \sim [X]_B$
4 S Hauptsatz über die charakteristische Matrix
– L $f(\mathcal{S}) = \sum S_i A^i$ – L $f(\mathcal{T}) = 0 \Leftrightarrow \exists \mathcal{S} : \mathcal{T} = \mathcal{A}\mathcal{S}$
5 F Eigenschaften der Smith. NF vom $\mathcal{A}$, Minimalpolynom
6 F Cayley-Hamilton, und: $A \sim B \Leftrightarrow \mathcal{A} \sim \mathcal{B}$
7 S Jordansche Normalform

## 2 Körpererweiterunggen

### 2.1 Grundbegriffe

1 D Körper, Charakteristik, Primkörper
2 D Körpererweiterung $L/K$
3 L $L/K \Rightarrow L$ ist $K$-Algebra
– D algebraische, transzendente Elemente von $L/K$
– B transzendente, algebraische Zahlen 4 D endliche Körpererweiterung, deren Grad
5 L Grad eines Elements
6 D algebraische Körperweiterungen
7 L Körperturm und Gradformel
8 F $\deg_F(a) \mid [K : F]$
9 S Stammkörper über irreduziblen Polynomen
11 F $\exists L/K$: $f(X)$ zerfällt in $L/K$ in Linearfaktoren
12 S Über zyklische Grupper der Einheitswurzeln
13 S Hauptsatz: Satz vom primitiven Element
14 D (in)separable Polynome

### 2.2 Körperisomorphismen & Galoistheorie

1 D Körperisomorphismen
2 D $K_1/F \cong K_2/F$, $F$-isomorph
3 K Nullstellen und Minimalpolynome gleich in $F$-Isomorphismen
4 S Existenzsatz zur Forsetzung eines Isomorphismus
5 F $\exists \phi \in \mathrm{Iso}(F(\alpha), F(\beta)) : \phi(\alpha) = \beta \Leftrightarrow \alpha, \beta$ selbes Min.pol.

6 D Zerfällungskörper $Z_F(f)$
7 S Eindeutigkeit des Zefällungskörpers
8 K Zerfällungkörper in großen Universalkörper eindeutig
9 D normale Körpererweiterung
10 S $K/F$ normal $\Leftrightarrow \exists f \in F[X] : K = Z_F(f)$
11 B endliche Körper und Kreisteilungskörper

12 D Galoiserweiterung
13 S Über Galoisgruppen einer Galoiserweiterung
14 S Hauptsatz der Galoistheorie

### 2.3 Anwendungen der Galoistheorie

1 D Radikalerweiterung
2 D Auflösbare Erweiterung – D Auflösbare Gruppe
3 S $\mathrm{char}(K) \neq p$ : A/E bzw. R/E vergrößerbar zu RA/E
4 S Anwendung der Galoistheorie

– D Punktmenge, mit Zirkel und Lineal konstruierbar
– K Analytische Geometrie
– S Quadratur des Kreises
– S Konstruktion eines regelmäßigen $n$-Ecks
– S Satz von Gauß
– S Klassifizierungen von $K/\mathbb{Q}$ mit Grad 2