Algebra II

SS 2018

23. Mai 2018

Inhaltsverzeichnis

VL1 16.04.2018

0 Kursüberblick

(i) Kommutative Algebra

- Moduln $\leftrightsquigarrow$ VRs über Ringe, Lösungen von LGS über $\mathbb{Z}$, $\mathbb{C}[X]$
- Dedekindringe: Algebraische Zahlentheorie, algebraische Kurven

(ii) Algebraische Zahlentheorie

- Eindeutige Primfaktorzerlegung $\leftrightsquigarrow$ Zerlegung in Primideale

$\rightsquigarrow$ Anwendung: suche $x, y, z \in \mathbb{Z}_{\geq 0}$ s.d.

$$x^n + y^n = z^n, \text{ für ein } n \in \mathbb{N}$$

Fermatsche Vermutung: Für $n \geq 3$ gibt es keine Lösung $p > 2$ Primzahl:

$$z^p = x^p + y^p = \prod_{j=0}^{p-1} (x + \zeta^j y), \text{ wobei } \zeta \text{ } p\text{-te primitive Wurzel ist}$$

Frage: Wann (und ob) ist $(x + \zeta^j y)$ die p-te Potenz?

(iii) Reelle Algebra $\rightsquigarrow$ falls die Zeit reicht

Sei $\mathcal{A}$ stets ein kommutativer Ring mit Eins.

1 Moduln

Definition 1.1. *Ein $\mathcal{A}$-Moduln ist eine abelsche Gruppe $(M, +)$ mit einer* Skalarmultiplikation

$$\mathcal{A} \times M \to M, \qquad (a, m) \mapsto a \cdot m,$$

sodass für alle $a, b \in \mathcal{A}$ und alle $m, n \in M$ folgende Eigenschaften gelten:

- $a \cdot (b \cdot m) = (a \cdot b) \cdot m$ (assoziativ)
- $a \cdot (m + n) = a \cdot m + a \cdot n$ (distributiv)
  $(a + b) \cdot m = a \cdot m + b \cdot m$
- $1 \cdot m = m$

Beispiel 1.2. *(a)* Ist $\mathcal{A} = \mathbb{K}$ ein Körper, so sind die $\mathcal{A}$-Moduln genau die $\mathbb{K}$-VRs

(b) Jede abelsche Gruppe G ist ein $\mathbb{Z}$-Modul via

- $n \cdot x = \underbrace{(1 + \cdots + 1)}_{n-\text{mal}} x = \underbrace{x + \cdots x}_{n-\text{mal}}, \qquad n \in \mathbb{Z}_{\geq 0}$
- $n \cdot x = -((-n)x), \qquad n \in \mathbb{Z}_{\leq 0}$

(c) Jedes Ideal $I \subset \mathcal{A}$ ist ein $\mathcal{A}$-Modul bzgl. der Ringmuliplikation in $\mathcal{A}$

(d) Ist $\mathcal{A} \subset \mathcal{B}$ eine Ringerweiterung, so kann man $\mathcal{B}$ als $\mathcal{A}$-Modul (mit der Ringmultiplikation) auffassen

(e) Ist $f : \mathcal{A} \to \mathcal{B}$ ein Ringhomomorphismus, so ist $\mathcal{B}$ ein $\mathcal{A}$-Modul via:

$$\mathcal{A} \times \mathcal{B} \to \mathcal{B} \qquad (a, b) \mapsto f(a) \cdot b$$

Bemerkung 1.3. $0 \cdot x = 0$ für alle $x \in M$

Definition 1.4. *(i) Ein* Modulhomomorphismus *f ist eine Abbildung zwischen zwei $\mathcal{A}$-Moduln M, N*

$$f : M \to N,$$

sodass folgende Eigenschaften gelten:

- $f(x+y) = f(x) + f(y)$ *für alle* $x, y \in M$
- $f(a \cdot x) = a \cdot f(x)$ *für alle* $a \in \mathcal{A}$ *und* $x \in M$

Andere Bezeichnung: $\mathcal{A}$-lineare Abbildung

(ii) *f heißt* (Moduln-)Isomorphismus*, falls f ein bijektiver Modulhomomorphismus ist.*

(iii) *M, N heißen* isomorph*, falls es ein Isomorphismus $f : M \to N$ gibt. Schreibweise: $M \cong N$*

Definition 1.5. *Sei M ein $\mathcal{A}$-Modul. Eine Teilmenge $N \subset M$ ist ein $\mathcal{A}$-Untermodul (UM), falls N eine Untergruppe (UG) von $(M, +)$ ist mit $a \cdot x \in N$ für alle $x \in N$ und $a \in \mathcal{A}$.*

Bemerkung 1.6. *(a)* Jeder UM eines $\mathcal{A}$-Moduls ist ein $\mathcal{A}$-Modul

(b) Der Schnitt beliebig vieler $\mathcal{A}$-Moduln ist ebenfalls ein $\mathcal{A}$-Modul

Beispiel 1.7. *(a)* Ist M ein Modul, so sind $0, M \subset M$ UMs. Außerdem ist für alle $x \in M$ die Menge

$$Ax := \{a \cdot x : a \in \mathcal{A}\}$$

ein UM

(b) $\mathcal{A}$ selbst ist ein $\mathcal{A}$-Modul. Seine UM sind genau die Ideale von $\mathcal{A}$

(c) Ist $\mathcal{A} = \mathbb{Z}$ und M ein $\mathbb{Z}$-Modul und die UM von M sind genau die UG von $(M, +)$

(d) Sei $f : M \to N$ ein Homomorphismus von $\mathcal{A}$-Moduln. Ist $M' \subset M$ ein UM von M, so auch $f(M') \subset N$ ein UM von N. Umgekehrt: Ist $N' \subset N$ ein UM von N, so auch $f^{-1}(N')$ ein UM von M.

Insbesondere.
- $\ker f = f^{-1}(\{0\}) = \{x \in M : f(x) = 0\}$ der Kern von f ist ein UM von M, sowie
- $\operatorname{im} f = f(M)$ das Bild von f ist ein UM von N

Sei M ein $\mathcal{A}$-Modul, $N \subset M$ UM. Dann:
Die Relation $x \equiv y \mod N :\iff x - y \in N$ ist eine Äquivalenzrelation. Schreibe $\bar{x}$ für die Äquivalenzklasse, die x enthält. Die Menge aller Äquivalenzklassen

$$M/N := \{\bar{x} : x \in M\}$$

ist ein $\mathcal{A}$-Modul via:

- $\bar{x} + \bar{y} = x \bar{+} y, \qquad x, y \in M$
- $a \cdot \bar{x} = a \bar{\cdot} x$

M/N heißt *Quotientenmodul*. Die kanonische Abbildung $\pi : M \to M/N$, $x \mapsto \bar{x}$ ist ein surjektiver Modulnhomomorphismus.

Satz 1.8. *Sei $N \subset M$ ein UM und $f : M \to M'$ ein Modulnhomomorphismus mit $N \subset \ker f$. Dann existiert ein eindeutiger Homomorphismus von $\mathcal{A}$-Moduln $\bar{f} : M/N \to M'$, sodass $f = \bar{f} \circ \pi$. Weiterhin gilt:*

- *f surjektiv $\implies$ $\bar{f}$ surjektiv*
- *$N = \ker f \implies \bar{f}$ injektiv*
- *Falls f surjektiv und $N = \ker f$, gilt: $M/N \cong M'$.*

  Insbesondere. $M/N \cong \operatorname{im} f$

Definition 1.9. *(a) Ist M ein $\mathcal{A}$-Modul und $(N_i)_{i \in I}$ eine Familie von UMs, so ist*

$$\sum_{i \in I} N_i = \Big\{ \sum_{i \in I} x_i : x_i \in N_i, \quad \underbrace{x_i = 0 \textit{ für fast alle } i \in I}_{\textit{oder auch: } x \neq 0 \textit{ für endlich viele } i \in I} \Big\}$$

ein UM.

(b) Ist $X \subset M$ eine TM, so sei

$$\operatorname{span}_{\mathcal{A}}(X) := \bigcap \{ N \subset M : N \textit{ ein UM}, X \subseteq N \}$$

der Span *von* X.

Bemerkung 1.10. *(a)* Es gilt:

$$\operatorname{span}_{\mathcal{A}}(X) = \{ \sum_{x \in X} a_x x : a_x \in \mathcal{A}, a_x = 0 \text{ für fast alle } x \in X \} = \sum_{x \in X} \mathcal{A}\, x$$

(b) $(N_i)_{i \in I}$ Familie von UMs, so ist

$$\sum_{i \in I} N_i = \operatorname{span}_{\mathcal{A}} \Big(\bigcup_{i \in I} N_i \Big)$$

Definition 1.11. *Sei $(M_i)_{i \in I}$ eine Familie von $\mathcal{A}$-Moduln.* Das direkte Produkt $\prod_{i \in I} M_i$ *ist ein $\mathcal{A}$-Modul via:*

- $(x+y)_i := x_i + y_i$
- $(ax)_i := ax_i$

Die Teilmenge

$$\bigoplus_{i\in I} M_i := \left\{ x \in \prod_{i\in I} M_i : x_i = 0 \textit{ für fast alle } i \in I \right\}$$

des direkten Produkts ist ein UM. Wir bezeichnen $\bigoplus_{i\in I} M_i$ *als* die direkte Summe.

Bemerkung 1.12. Ist $|I| < \infty$, so ist $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$

VL2, 17.04.2018

Wiederholung: $(M_i)_{i\in I}$ eine Familie von $\mathcal{A}$-Moduln. Dann ist $\prod_{i\in I} M_i$ ebenfalls ein $\mathcal{A}$-Modul mit der komponentenweisen Addition. Die Teilmenge $\bigoplus_{i\in I} M_i$ besteht aus allen Tupeln mit nur endlich vielen Komponenten ungleich 0 und ist ein Untermodul .

Sind die $(M_i)_{i\in I}$ Untermoduln von M, so bekommen wir natürliche Abbildung

$$\bigoplus_{\mathrm{i\in I}} M_i \to M, \qquad (m_i)_{i\in I} \mapsto \sum_{i\in I} m_i.$$

Diese Abbildung ist $\mathcal{A}$-linear mit Bild $\sum_{i\in I} M_i \subseteq M$.

Definition 1.13. *Sei M ein $\mathcal{A}$-Modul. Eine Familie von Elementen $(x_i)_{i\in I}$, $x_i \in M$ heißt*

- erzeugend, *falls $M = \mathrm{span}_{\mathcal{A}} \{x_i : i \in I\}$, d.h. jedes Element $x \in M$ lässt sich als $x = \sum_{i\in I} a_i x_i$ schreiben mit $a_i = 0$ für fast alle* $\mathrm{i} \in \mathrm{I}$.
- linear abhängig, *falls es $a_i \in \mathcal{A}$,* $\mathrm{i} \in \mathrm{I}$ *gibt mit $a_i = 0$ für fast alle* $\mathrm{i} \in \mathrm{I}$, *aber nicht alle a_i sind gleich 0. Anderenfalls heißen x_i* linear abhängig.
- eine Basis von M, *falls x_i linear unabhängig und erzeugend sind.*
- *M heißt* frei, *falls M eine Basis hat.*

Bemerkung 1.14.
- Jeder Modul M hat ein Erzeugendensystem, nämlich M selbst.

- Nicht jeder Modul hat eine Basis (also frei), etwa $\mathcal{A} = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}_{\geq 0}$, dann ist jedes Element $x \in M$ linear abhängig.
  In der Tat: $n \cdot x = 0$, wobei $n \neq 0$.

- Ist M frei mit Basis $(x_i)_{\mathrm{i}\in\mathrm{I}}$, so ist die Abbildung

$$\phi : \bigoplus_{\mathrm{i}\in\mathrm{I}} \mathcal{A} \to M, \qquad (a_i)_{\mathrm{i}\in\mathrm{I}} \mapsto \sum_{\mathrm{i}\in\mathrm{I}} a_i x_i$$

  ein Isomorphismus.

  Beweis. *zZ:* "ϕ injektiv": reich *zZ:* $\ker\phi = \{0\}$.
  Sei $(a_i)_{\mathrm{i}\in\mathrm{I}} \in \ker\phi$. Dann ist $\sum_{\mathrm{i}\in\mathrm{I}} a_i x_i = 0 \implies a_i = 0$ für alle i ∈ I.
  "ϕ surjektiv": Sei $x \in M$, *zZ:* $x = \phi(a)$ für $a \in \bigoplus_{\mathrm{i}\in\mathrm{I}} \mathcal{A}$. Da $(x_i)_{\mathrm{i}\in\mathrm{I}}$ erzeugend, gibt es $a = (a_i)_{\mathrm{i}\in\mathrm{I}}$ mit $x = \sum_{\mathrm{i}\in\mathrm{I}} a_i x_i = \phi(a)$. □

Satz 1.15. *Ein endlich erzeugter Modul M ist genau dann frei, wenn er isomorph zu $\mathcal{A}^n$ für ein $n \in N_{>0}$.*

Beweis. Sei M frei, also $M \cong \bigoplus_{\mathrm{i}\in\mathrm{I}} M_i$. Ist I nicht endlich, so ist M nicht endlich erzeugt. Angenommen $x_1, ..., x_n \in M$ ist ein Erzeugendensystem. Dann gibt es eine endliche Teilmenge I_j für $j = 1..n$ von I, sodass die k-te Komponente von $\phi(x_j) = 0$ ist, falls $k \notin I_j$. Also ist die k-te Komponente von jeder Linearkombination der $x_i = 0$, falls $k \notin I_1 \cup ... \cup I_n$. Ist I unendlich, so existiert immer so ein k und ebenfalls ein Element in $\bigoplus_{\mathrm{i}\in\mathrm{I}} \mathcal{A}$ mit der k-ten Komponente ungleich 0. □

Definition und Satz 1.16. *Sei $\mathcal{A} \neq \{0\}$ ein Ring und M ein erzeugter freier Modul. Dann ist die Zahl $n \geq 0$ mit $M \cong \mathcal{A}^n$ eindeutig und heißt* Rang *von M. Schreibe:* $\mathrm{rk}\, M = n$. *Ist M nicht endlich erzeugt und frei, dann ist* $\mathrm{rk}\, M = \infty$.

Beweis. Sei $M \cong \mathcal{A}^n$ und $\mathfrak{m} \subsetneq \mathcal{A}$ ein maximales Ideal. Dann ist $\mathbb{K} = \mathcal{A}/\mathfrak{m}$ ein Körper und $M/\mathfrak{m}M$ ein Vektorraum über $\mathbb{K}$ mit $M/\mathfrak{m}M \cong_{\mathbb{K}} \mathbb{K}^n$. Da die Dimension von einem Vektorraum eindeutig bestimmt ist, folgt die Behauptung. □

2 Noethersche Ringe

Definition 2.1. *Ein $\mathcal{A}$-Modul M heißt* noethersch, *wenn jedes Untermodul von M endlich erzeugt ist. Der Ring $\mathcal{A}$ heißt* noethersch, *falls er als $\mathcal{A}$-Modul noethersch ist.*

Bemerkung 2.2. Ein Ring $\mathcal{A}$ ist genau dann noethersch, wenn alle Ideale endlich erzeugt sind.

Beispiel 2.3. Jeder Hauptidealring ist noethersch, zum Beispiel $\mathbb{Z}, \mathbb{K}[X]$ für $\mathbb{K}$ Körper.

Lemma 2.4. *Für jeden $\mathcal{A}$-Modul M sind äquivalent:*

(i) *M ist noethersch*

(ii) *Jede aufsteigende Kette $U_1 \subseteq U_2 \subseteq ...$ von Untermoduln wird stationär, d.h. es existiert ein $n \in N$, sodass $U_n = U_{n+k}$ für alle $k \in \mathbb{N}_{\geq 0}$*

(iii) *Jede Menge nichtleere $\mathfrak{U}$ von Untermoduln von M enthält ein maximales Element.*

Beweis. $(i) \implies (ii)$: Die Vereinigung $U := \bigcup_{i=1}^{\infty}$ ist ein Untermodul von M. Also ist U endlich erzeugt, etwa von $x_1, ..., x_r$. Dann existiert ein $N \in \mathbb{N}_{>0}$, sodass $x_1, ..., x_r \in U_N$, damit folgt $U = U_N$.

$(ii) \implies (iii)$: Angenommen $N \in \mathfrak{U}$ ist ein maximales Element, so existiert $N' \in \mathfrak{U}$ mit $N \subsetneq N'$. Falls kein maximales Element in $\mathfrak{U}$ existiert, finden wir unendliche echt aufsteigende Kette $N \subsetneq N' \subsetneq N'' \subsetneq ...$ $\rightsquigarrow$ **Widerspruch**

$(iii) \implies (i)$: Sei $N \subseteq M$ ein Untermodul . Dazu betrachten wir $\mathfrak{U}$ eine Menge der endlich erzeugter Untermoduln von N. $\mathfrak{U}$ ist nichtleer, da $\{0\} \in \mathfrak{U}$. Also existiert nach (iii) ein maximales Element $N_{\max}$ von $\mathfrak{U}$. *zZ:* $N_{\max} = N$. Angenommen $N_{\max} \subseteq N$, dann gibt es ein $x \in N \backslash N_{\max}$ und $\tilde{N} = \operatorname{span}_{\mathcal{A}}(x \cup N_{\max}) \in \mathfrak{U}$ und $N_{\max} \subseteq \tilde{N} \rightsquigarrow$ **Widerspruch** □

Lemma 2.5. *Seien $N \subseteq M$ $\mathcal{A}$-Moduln*

(a) *M endlich erzeugt $\implies$ M/N endlich erzeugt*

(b) *N und M/N endlich erzeugt $\implies$ M endlich erzeugt*

(c) *M noethersch $\iff$ N und M/N noethersch*

Beweis. *(a)* klar

(b) Sei $m_1, ..., m_r \in M$ sodass die Restklassen $\bar{m_1}, ..., \bar{m_r} \in M/N$ den Modul M/N erzeugen. Seien $n_1, ..., n_s \in N$ Erzeugendensystem von N.

Behauptung. $m_1, ..., m_r, n_1, ...n_s$ erzeugen M.

Sei $x \in M$. Dann gibt es $a_1, ..., a_r \in \mathcal{A}$, sodass $\bar{x} = a_1 m_1 + ... + a_r m_r$ in M/N. Also $y := x - (a_1 m_1 + ... + a_r m_r) \in N$. Also gibt es $b_1, ...b_s \in \mathcal{A}$ mit $y = b_1 n_1 + ... + b_s n_s$. Insgesamt gilt: $x = a_1 m_1 + ... + a_r m_r + b_1 n_1 + ... + b_s n_s$. Dies bekommt man durch das Umstellen.

VL3, 23.04.2018

(c) " $\Rightarrow$ " N noethersch $\rightsquigarrow$ ✓
Jeder Untermodul von M/N ist von der Form $(U + N)/N$ für ein $U \subseteq M$ Untermodul . Da M noethersch, ist $U + N$ endlich erzeugt. Nach $a)$ ist $(U + N)/N$ endlich erzeugt. " $\Leftarrow$ " Sei $U_1 \subseteq U_2 \subseteq ...$ eine Kette von Untermoduln von M. Dann gibt es ein $n \geq 1$ sodass

$$U_{n+k} \bigcap N = U_n \bigcap N, \text{ sowie}$$
$$(U_{n+k} + N)/N = (U_n + N)/N \quad \text{für alle } k \geq 0,$$

da M/N noethersch ist.

Behauptung. $U_{n+k} = U_n$ für alle $k \geq 0$. Dann folgt, dass jede Kette von Untermoduln statinär wird, was gleichzusetzen mit M noethersch ist.

Wir zeigen hier Mengeninklusionen $U_n = U_{n+k}$. $U_n \subseteq U_{n+k} \rightsquigarrow$ ✓.

Sei $x \in U_{n+k}$. Dann ist $\bar{x} \in (U_n + N)/N$, also existiert ein $y \in N$, sodass $x - y \in U_n$. Es folgt:

$$y = x - (x - y) \in U_{n+k} \cap N, \text{ wobei } x \in U_{n+k},\ x - y \in U_n$$
$$\Longrightarrow\ y \in U_n \cap N, \text{ und damit } x = y + (x - y) \in U_n.$$

□

Korollar 2.6. *Ist $\mathcal{A}$ noethersch, so ist jeder endlich erzeugte $\mathcal{A}$-Modul M noethersch.*

Beweis. Sei M erzeugt von $x_1, ..., x_r \in M$. Betrachte die surjektive $\mathcal{A}$-lineare Abbildung

$$\phi : \mathcal{A}^r \to M, \qquad (a_1, ..., a_r) \mapsto a_1 x_1 + ... + a_r x_r.$$

Nach der Isomorphiesatz gilt: $M \cong \mathcal{A}^r / \ker \phi$. Nach Lemma $5a)$ reicht zZ: $\mathcal{A}^r$ ist noethersch. Wir machen Induktion nach r:

$r = 1 : \rightsquigarrow$ ✓

$r \rightsquigarrow r + 1$: Sei $N = \left\{(a_1, ..., a_r, 0) \in \mathcal{A}^{r+1} : a_i \in \mathcal{A}\right\} \subseteq \mathcal{A}^{r+1}$. Nach Induktionsvoraussetzung ist N noethersch. Betrachte:

$$\psi : \mathcal{A}^{r+1} \to \mathcal{A}, \qquad (a_1, ..., a_{r+1}) \mapsto a_{r+1}.$$

ψ ist surjektiv, $\mathcal{A}$-linear und $\ker \psi = N$. Also $\mathcal{A}^{r+1}/N \cong \mathcal{A}$ noethersch nach Voraussetzung. Nach $5c)$ ist $\mathcal{A}^{r+1}$ noethersch. □

Bemerkung 2.7. Ist $\mathcal{A}$ noethersch, so kann jeder endlich erzeugter Modul M als Kokern einer Matrix dargestellt werden.

In der Tat: ist M erzeugt von $x_1, ..., x_n$, so ist die Abbildung

$$\phi : \mathcal{A}^n \to M, \qquad (a_1, ..., a_n) \mapsto a_1x_1 + ... + a_nx_n$$

surjektiv. Der Kern $N = \ker \phi$ ist endlich erzeugt von $y_1, ..., y_m \in N$. Also ist $N = \operatorname{im} \psi$, wobei $\psi : \mathcal{A}^m \to A^n,\ (b_1, ..., b_m) \mapsto b_1y_1 + ... + b_my_m$. Damit ist $M \cong A^n/\operatorname{im} \psi$. Die darstellende Matrix enthält alle Informationen über M (bis auf Isomorphie).

Satz 2.8 (Hilberts Basissatz)**.** *Ist $\mathcal{A}$ noethersch, so ist auch $\mathcal{A}[X]$ noethersch.*

Beweis. Sei $I \subseteq \mathcal{A}[X]$ ein Ideal. Für alle $i \in Z_{\geq 0}$ sei J_i die Menge aller Leitkoeffizienten (LC) eines Polynoms $f \in I,\ \deg f = i$ vereinigt mit $\{0\}$.

Behauptung. J_i ist ein Ideal von $\mathcal{A}$.

Seien $a, a' \in J_i, b \in \mathcal{A}$. OBdA: $a, a' \neq 0$, also es existieren $f, g \in I$ sodass a bzw. b der LC von f bzw. g und $\deg f = \deg g = i$. Dann ist $a + a'$ bzw. ba der LC von $f + g$ bzw. bf, wobei $\deg(f + g) = \deg(bf) = i$, also $a, a' \in J_i, ba \in J_i$, also ist J_i ein Ideal.

Behauptung. $J_i \subseteq J_{i+1}$.

Sei $a \in J_i \backslash \{0\}$. Dann ist a ein LC eines Polynoms $f \in I$ mit $\deg f = i$. Dann ist a der LC von $x \cdot f, f \in I$, wobei $\deg(x \cdot f) = i + 1$. Deswegen ist $a \in J_{i+1}$. Da $\mathcal{A}$ noethersch ist, gibt es ein $N \geq 0$, sodass $J_N = J_{N+k}$ für alle $k \geq 0$.

Weiter sei $a_{i,1}, ..., a_{i,n_i}$ das Erzeugendensystem von J_i für alle $0 \leq i \leq N$.Außerdem sei $f_{i,j} \in I$ ein Polynom mit LC $a_{i,j}$ von Grad i für alle $i = 0...N$, $j = 1...n_i$.

Behauptung. $f_{i,j}$ erzeugt I

Dazu sei $f \in I \backslash \{0\}$ vom Grad d. *zZ:* $f \in I' = \operatorname{span}_{\mathcal{A}[X]} \left\{ f_{i,j} : i = 0...N, j = 1...n_i \right\}$.

Induktion nach d:

Fall $d \geq N$: Da $J_d = J_N$, liegt der LC von f in J_N, also ist er eine folgende $\mathcal{A}$-Linearkombination:

$$c_1a_{N,1} + ... + c_{n_N}aN, n_N, \quad \text{für } c_i \in \mathcal{A}\,.$$

Also hat $f - \underbrace{\left(c_1 X^{d-N} f_{N,1} + ... + c_{n_N} X^{d-N} f_{N,n_N}\right)}_{\in I'}$ den Grad kleiner als d, liegt also in I' nach Induktionsvoraussetzung. Deswegen muss auch $f \in I'$.

Fall $d > N$**:** folgt analog zum obigen Fall, aber für J_d anstatt J_N und ohne die Multiplikation mit X^{d-N}.

□

Korollar 2.9. *Sei $\mathcal{A}$ noethersch, $\mathcal{A} \subseteq \mathcal{B}$ eine Ringerweiterung mit $\mathcal{B} = \mathcal{A}[b_1, ..., b_r]$ für geeignete $b_1, ..., b_r \in \mathcal{B}$. Dann ist $\mathcal{B}$ noethersch.*

Beweis. Der Polynomring $\mathcal{A}[X_1, ..., X_r]$ ist nach dem Hilbertschen Basissatz 2.8 und Induktion nach r noethersch. Der Ringhomomorphismus

$$\phi : \mathcal{A}[X_1, ..., X_r] \to \mathcal{B}, \qquad X_i \mapsto b_i$$

ist surjektiv. Also $\mathcal{B} \cong \mathcal{A}[X_1, ...X_r]/\ker\phi \implies \mathcal{B}$ noethersch als $\mathcal{A}[X_1, ..., X_r]$-Modul, also auch als $\mathcal{B}$-Modul (Übung!) □

Beispiel 2.10. *(a)* Die folgenden Ringe sind noethersch: $\mathbb{K}$ Körper, $\mathbb{Z}$, $\mathbb{K}[X_1, ..., X_n]$, $\mathbb{Z}[X_1, ..., X_n]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{K}[X_1, ..., X_n]/I$ mit I Ideal. Die Lokalisierungen dieser Ringe sind ebenfalls noethersch.

(b) Der Ring $\mathbb{K}[X_1, X_2, ...]$ mit unendlich vielen Variablen ist *nicht* noethersch:

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X3) \subsetneq ...$$

(c) $\mathbb{Z}$-Modul $\mathbb{Q}$ *nicht* noethersch, da nicht endlich erzeugt.

(d) Ein *Unterring* von einem noetherschen Ring ist im Allgemeinen *nicht* noethersch:

$\mathbb{K}[X_1, X_2, ...] \subset \mathrm{Quot}(\mathbb{K}[X_1, X_2, ...]) \rightsquigarrow$ noethersch, da Köerper,

aber $\mathbb{K}[X_1, X_2, ...]$ ist nach $c)$ nicht noethersch.

VL4, 24.04.2018

3 Moduln über Hauptidealringen

Motivation: Moduln über einem Körper $\mathbb{K}$ endlich erzeugt $\to$ isomorph zu $\mathbb{K}^n$
Moduln über $\mathbb{Z}$ erzeugt von einem Element $\to$ isomorph zu $\mathbb{Z}/(n)$, $n \in \mathbb{Z}$.

Definition 3.1. *(a) Sei* $\mathrm{Mat_{m\times n}}(\mathcal{A})$ die Menge der $m \times n$ Matrizen mit Einträgen aus $\mathcal{A}$.

(b) Eine Matrix $S \in \mathrm{Mat_n}(\mathcal{A})$ *ist* invertierbar*, falls es eine weitere Matrix* $T \in \mathrm{Mat_n}(\mathcal{A})$ *gibt, sodass gilt:*

$$ST = TS = I_n, \qquad \text{wobei } I_n \text{ die Einheitsmatrix}$$

(c) Die Adjunkte *von* S *ist gegeben durch:*

$$\mathrm{adj}(S) = \begin{bmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{n1} \\ \tilde{a}_{12} & \cdots & \tilde{a}_{n2} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{1n} & \cdots & \tilde{a}_{nn} \end{bmatrix},$$

wobei $\tilde{a}_{ij} = (-1)^{i+j} M_{ij}$ *mit* M_{ij} *die Unterdeterminante von* S*, die durch Streichen von der* i*-ten Zeile und* j*-ten Spalte aus* S *entsteht.*

(d) Sei $S \in \mathrm{Mat_n}(\mathcal{A})$*. Die* Determinante *von* S *ist gegeben durch:*

$$\det S = \sum_{i=1}^{n} \mathrm{sgn}(\sigma) \prod_{\sigma \in S_n} a_{i\sigma(i)}$$

Lemma 3.2. *Für* $S, T \in \mathrm{Mat_n}(\mathcal{A})$ *gilt:*

(a) $\det(ST) = \det(S)\det(T)$

(b) $S\,\mathrm{adj}(S) = \det(S) I_n$

Beweis. *(a)* Sei $\mathcal{A}$ zunächst der Polynomring $\mathbb{Z}[a_{ij}, bij : 1 \leq i, j \leq n]$ in den Unbekannten a_{ij}, b_{ij} und sei $S = (a_{ij})$ und $T = (b_{ij})$. Dann sind $\det(ST), \det(S)$ und $\det(T)$ Polynome über $\mathbb{Z}$, welche für jede Einsetzung von komplexen Zahlen gleich sind. Also gilt $\det(ST) = \det(S)\det(T)$ als Polynome über $\mathbb{Z}$ nach Algebra 1. Fü Matrizen S, T über beliebigen Ringen betrachte den Ringhomomorphismus

$$\phi : \mathbb{Z}[a_{ij}, b_{ij}] \to \mathcal{A},$$

welcher a_{ij} bzw. b_{ij} auf den (i, j)-ten Eintrag von S bzw. T abbildet.

(b) Diese Aussage folgt analog zu (a) mit S und $\mathrm{adj}(S)$.

□

Satz 3.3. $S \in \mathrm{Mat_n}(\mathcal{A})$ *ist genau dann invertierbar, wenn* $\det(S) \in \mathcal{A}^\times$. *Dann gilt:* $S^{-1} = \det(S)^{-1}\operatorname{adj}(S)$. *Die Menge* $Gl_n(\mathcal{A}) = \left\{S \in \mathrm{Mat_n}(\mathcal{A}) : \det(S) \in \mathcal{A}^\times\right\}$ *ist eine multiplikative Gruppe.*

Beweis. " $\Rightarrow$ " Sei S invertierbar $\implies ST = I_n \implies \det(S)\det(T) = 1$
" $\Leftarrow$ " $det(S) \in \mathcal{A}^\times \implies \det(S)^{-1}\operatorname{adj}(S) =: T \in \mathrm{Mat_n}(\mathcal{A})$ ist das Inverse von S nach Lemma 3.2. Rest $\rightsquigarrow$ ✓ □

Für Matrizen $T \in \mathrm{Mat_{m\times n}}(\mathcal{A})$ betrachte die üblichen elementaren Zeilen-/Spaltenoperationen:

- Addition eines Vielfachen einer Zeile/Spalte zu einer anderen $\leftrightsquigarrow$ multipliziere dafür T mit $I + aE_{ij}$ von links oder von rechts.
- Zeilen-/Spaltentausch $\leftrightsquigarrow$ multipliziere dafür T mit einer Permutationsmatrix $\prod_{ij}$ von links oder von rechts.

Erinnerung. Ein Integritätsbereich $\mathcal{A}$ heißt *euklidischer Ring*, falls es eine *euklidische Norm* $N : \mathcal{A} \to \mathbb{Z}_{\geq 0}$ existiert, d.h. für alle $x, y \in \mathcal{A}$ mit $y \neq 0$ existieren $q, r \in \mathcal{A}$, s.d. $x = qy + r$ mit entweder $N(q) > N(r)$ oder $r = 0$. Jeder euklidischer Ring ist ein Hauptidealbereich.

Beispiel 3.4. $\mathbb{Z}$ mit der Betragsfunktion $|\cdot|$ ist ein euklidischer Ring. q, r sind im Allgemeinen nicht eindeutig.

Beispiel 3.5. $\mathbb{Z}[i]$ der Ring der Gaußschen Zahlen ist ebenfalls ein euklidischer Ring mit $N(a+bi) = \sqrt{a^2+b^2}$. Seinen $x, y \in \mathcal{A}, y \neq 0$. Sei $q := m + ni$ die Zahl in $\mathcal{A}$, welche dem Bruch $z := \frac{x}{y}$ am nächsten liegt. Dann gilt:

$$|m - \mathrm{Re}(z)| \leq 1/2 \text{ und } |n - \mathrm{Im}(z)| \leq 1/2$$

$$\implies |q - z| \leq 1/\sqrt{2} \implies |qy - x| \leq 1/\sqrt{2}|y| \leq |y|.$$

Satz 3.6 (Elementarteilersatz)**.** *Sei* $\mathcal{A}$ *ein euklidischer Ring,* $T \in \mathrm{Mat_{m\times n}}(\mathcal{A})$. *Durch endlich viele elementaren Zeilen-/Spaltenoperationen kann man* T *in die folgende Form bringen:*

$$\left[\begin{array}{cccc|c} d_1 & 0 & \cdots & 0 & \\ 0 & d_2 & \cdots & 0 & \\ \vdots & & \ddots & 0 & 0 \\ 0 & 0 & \cdots & d_r & \\ \hline & & 0 & & 0 \end{array}\right],$$

s.d. $0 \leq r \leq \min\{m, n\}, d_i \in \mathcal{A}, d_1|d_2|...|d_r \neq 0$. *Ist* $T = (a_{ij})$, *so schreibe* $\mathrm{ggT}\, T = \mathrm{ggT}\{a_{ij} : \textit{für alle } i, j\}$.

Bemerkung 3.7. Sei $U \in Gl_m(\mathcal{A}), V \in Gl_n(\mathcal{A})$, dann ist $\operatorname{ggT} T \sim \operatorname{ggT} UTV$

Beweis. $\operatorname{ggT} T | \operatorname{ggT} UTV$. Da U, V invertierbar sind, gilt andererseits: $\operatorname{ggT} UTV | \operatorname{ggT} U^{-1}(UTV)V^{-1}$ □

Beweis. Wir werden zeigen, dass T in die Gestalt

$$\left[\begin{array}{c|c} d_1 & 0 \\ \hline 0 & \tilde{T} \end{array}\right]$$

gebracht werden kann, wobei $d_1 \sim \operatorname{ggT} T$ und $\tilde{T} \in \operatorname{Mat}_{m-1,n-1}(\mathcal{A})$. Dann folgt die Behauptung per Induktion. Sei $N : \mathcal{A} \setminus \{0\}$ eine euklidische Norm. Sei $N(T) = \min\{N(a_{ij} : 1 \leq i \leq m, 1 \leq j \leq n), a_{ij} \neq 0\}$. Wir machen Induktion nach $N(T)$

$N(T) = 0$: durch Vertauschen von Zeilen und Spalten erreiche $N(a_{11}) = 0$. Dann teilt a_{11} alle Einträge der Matrix und wir können Nullen in der ersten Zeile und Spalte erzeugen.

$N(T) \geq 0$: OBdA: $N(T) = N(a_{11})$.

Fall 1: ist $a_{11} \nmid a_{i1}$ für ein $2 \leq i \leq m$, so dividiere mit Rest $a_{i1} = qa_{11} + r$ mit $N(r) < N(a_{11})$, dann ziehe von der i-ten Zeile das q-fache der ersten Zeile ab $\rightsquigarrow$ $(i,1)$-ter Eintrag ist r mit $N(r) < N(a_{11})$. Wende die Induktionsvoraussetzung an.

Fall 2: anderenfalls $a_{11} \mid a_{i1}$ für alle $2 \leq i \leq m$ und wir können von der i-ten Zeile das $\frac{a_{i1}}{a_{11}}$-fache der ersten Zeile abziehen

$\rightsquigarrow$ erhalte $\left[\begin{array}{c|c} a_{11} & a'_{12} \cdots a'_{1m} \\ \hline 0 & \tilde{T} \end{array}\right]$

Falls $a_{11} \mid \operatorname{ggT} T$, sind wir fertig. Nehme also an, dass es nicht so ist. Dann existiert es a'_{kl} mit $a_{11} \nmid a'_{kl}$. OBdA existiere ein solches a'_{kl} mit $k = 1$, sonst addiere die k-te Zeile zur ersten. Dann dividiere a'_{1l} mit Rest durch a_{11}. Wir erhalten:

$$a'_{1l} = q'a_{11} + r', \quad \text{mit } N(r') < N(a_{11}).$$

$\rightsquigarrow$ wie oben können wir die Induktionsvoraussetzung nach dem Abziehen anwenden.

□

Beispiel 3.8. $T = \begin{bmatrix} 2 & 3 & 4 \\ 5 & 6 & 7 \end{bmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$, $N(T) = 2$

Division mit Rest liefert: $\rightsquigarrow \left[\begin{smallmatrix} 2 & 3 & 4 \\ 1 & 0 & -1 \end{smallmatrix}\right] \to N(T) = 1$.
Bringe das "kleinste"Element in die erste Position: $\rightsquigarrow \left[\begin{smallmatrix} 1 & 0 & -1 \\ 2 & 3 & 4 \end{smallmatrix}\right]$
Division mit Rest: $\rightsquigarrow \left[\begin{smallmatrix} 1 & 0 & -1 \\ 0 & 3 & 6 \end{smallmatrix}\right]$
Erste Zeile zu Null: $\rightsquigarrow [\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 3 & 6 \end{smallmatrix}]$, wobei $\tilde{T} = \begin{bmatrix} 3 & 6 \end{bmatrix}$ ist
Erhalte schlussendlich die gewünschte Form: $[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{smallmatrix}]$ mit $d_1 = 1$, $d_2 = 3$.

VL5, 30.04.2018

Elementarteilersatz: Sei $\mathcal{A}$ ein euklidischer Ring, $M \in \mathrm{Mat}_{\mathrm{m}\times\mathrm{n}}(\mathcal{A})$, dann kann man M mit elementaren Zeilen-/Spaltenoperationen auf die folgende Gestalt bringen:

$$\left[\begin{array}{cccc|c} d_1 & 0 & \cdots & 0 & \\ 0 & d_2 & \cdots & 0 & \\ \vdots & & \ddots & 0 & 0 \\ 0 & 0 & \cdots & d_r & \\ \hline \multicolumn{4}{c|}{0} & 0 \end{array}\right], \tag{1}$$

s.d. $0 \leq r \leq \min\{m, n\}, d_i \in \mathcal{A}, d_1|d_2|...|d_r \neq 0$

Bemerkung 3.9. Für einen euklidischer Ring $\mathcal{A}$ und $M \in \mathrm{Mat}_{\mathrm{m}\times\mathrm{n}}(\mathcal{A})$ existieren $V \in \mathrm{Mat}_{\mathrm{n}}(\mathcal{A})$ und $U \in \mathrm{Mat}_{\mathrm{n}}(\mathcal{A})$, sodass UMV Gestalt (1) hat. Dies gilt auch über Hauptidelringen. Der Satz 3.6 gilt im Allgemeinen nicht über Hauptidealringen.

Korollar 3.10. *Sei $\mathcal{A}$ ein Hauptidealring und M ein endlich erzeugter Modul über $\mathcal{A}$, dann gilt*

$$M \cong \mathcal{A}^s \oplus \mathcal{A}/(d_1) \oplus \mathcal{A}/(d_2) \oplus ... \oplus \mathcal{A}/(d_r)$$

für gewisse $d_1 \mid d_2 \mid ... \mid d_r \in \mathcal{A}\setminus\{0\}$

Beweis. [Wir führen den Beweis nur für euklidische Ringe]
Sei M endlich erzeugt von $x_1, ..., x_n \in M$. Dann ist die Abbildung

$$\phi : \mathcal{A}^n \to M, \qquad (a_1, ..., a_r) \mapsto a_1x_1 + ... + a_nx_n$$

ein surjektiver Modulnhomomorphismus. Da $\mathcal{A}$ noethersch ist, ist $\ker\phi \subseteq \mathcal{A}^n$ ein endlich erzeugter Modul von etwa $y_1, ..., y_m$. Wir definieren einen

weiteren Modulnhomomorphismus

$$\psi : \mathcal{A}^m \to \mathcal{A}^n, \qquad (a_1, ..., a_m) \mapsto a_1 y_1 + ... + a_m y_m$$

und stellen fest, dass $\operatorname{im}\psi = \ker\phi$. Also ist $M \cong A^n / \operatorname{im}\psi$. Bezüglich einer geeigneter Basis (von jeweils $\mathcal{A}^n$, $\mathcal{A}^m$) hat ψ eine darstellende Matrix der Form (1). Somit ist $\psi : \mathcal{A}^n \to \mathcal{A}^m$, $(a_1, ..., a_m) \mapsto (d_1 a_1, ..., d_r a_r, 0, ..., 0)$. Das Bild von ψ ist dann gerade

$$\mathcal{A}\, d_1 \oplus ... \oplus \mathcal{A}\, d_r \oplus \underbrace{\{0\} \oplus ... \oplus \{0\}}_{s-mal}.$$

Damit bekommen wir:

$$M \cong \mathcal{A} / \operatorname{im}\psi \cong \mathcal{A}^s \oplus \mathcal{A}/(d_1) \oplus ... \oplus \mathcal{A}/(d_r).$$

□

Definition 3.11. *Ein $\mathcal{A}$-Modul heißt* torsiosfrei, *falls für alle $a \in \mathcal{A}, x \in M$ mit $ax = 0$ folgt $x = 0$ oder $a = 0$.*

Korollar 3.12. *Ein endlich erzeugte torsiosfreie Modul M über einem Hauptidealring $\mathcal{A}$ ist automatisch frei.*

Beweis. Nach dem Korollar 3.10 bekommen wir $M \cong \mathcal{A}^s \oplus \mathcal{A}/(d_1) \oplus ... \oplus \mathcal{A}/(d_r)$. Da M torsionsfrei ist und alle $d_1, ..., d_r \in \mathcal{A} \setminus \{0\}$ sind, folgt $r = 0$. Somit gilt $M \cong \mathcal{A}^s$, also ist M frei. □

Korollar 3.13. *Sei $\mathcal{A}$ ein Hauptidealring, M endlich erzeugter freier $\mathcal{A}$-Modul. Dann ist jeder Untermodul von M auch frei.*

Beispiel 3.14.

- $\mathcal{A} = \mathbb{Z}, \mathbb{B} = \mathbb{Z}[\sqrt{-5}]$. $\mathbb{B}$ ist torsionsfrei mit der Basis $(1, \sqrt{-5})$.
- Betrachte das Ideal $I = \left(3, 2 + 4\sqrt{-5}\right) \subseteq \mathbb{B}$. Wir können I als $\mathcal{A}$-Modul auffassen. Nach Korollar 3.13 ist I frei. Welche Basis hat I als $\mathcal{A}$-Modul?

  Sei $x \in I \implies x = 3 \cdot (a + b\sqrt{-5}) + (2 + 4\sqrt{-5}) \cdot (a + b\sqrt{-5}) = (3a + 2c - 20d) + \sqrt{-5}(3b + 2d + 4c)$

  $\rightsquigarrow I$ ist das Bild der Matrix $\left[\begin{smallmatrix} 3 & 0 & 2 & -20 \\ 0 & 3 & 4 & 2 \end{smallmatrix}\right]$. Führe den Algo durch:
  $\left[\begin{smallmatrix} 3 & 0 & 2 & -20 \\ 0 & 3 & 4 & 2 \end{smallmatrix} \middle| \begin{smallmatrix} 1 \\ \sqrt{-5} \end{smallmatrix}\right] \rightsquigarrow \left[\begin{smallmatrix} 1 & 0 & 2 & -20 \\ -4 & 3 & 4 & 2 \end{smallmatrix} \middle| \begin{smallmatrix} 1 \\ \sqrt{-5} \end{smallmatrix}\right] \rightsquigarrow \left[\begin{smallmatrix} 1 & 0 & 2 & -20 \\ 0 & 3 & 12 & 78 \end{smallmatrix} \middle| \begin{smallmatrix} 1-4\sqrt{-5} \\ \sqrt{-5} \end{smallmatrix}\right]$
  $\rightsquigarrow \left[\begin{smallmatrix} 1 & 0 & 2 & -20 \\ 0 & 3 & 0 & 0 \end{smallmatrix} \middle| \begin{smallmatrix} 1-4\sqrt{-5} \\ \sqrt{-5} \end{smallmatrix}\right]$. Wir haben die gewünschte Gestalt (1) und somit ist die $\mathbb{Z}$-Basis von I gegeben durch $\left(1 - 4\sqrt{-5}, 1\right)$.

4 Ganze Ringerweiterungen

Motivaton: Es gilt bekanntlich $\mathbb{Z} \subseteq \mathbb{Q}$ und sei $\mathbb{Q} \subseteq \mathbb{K}$ eine Körpererweiterung. Wir wollen eine Ringerweiterung von $\mathbb{Z} \subseteq \mathcal{A}$ angeben, sodass $\mathcal{A} \subseteq \mathbb{K}$ " analoge Eigenschaften"hat zu $\mathbb{Z} \subseteq \mathbb{Q}$.
Zum Beispiel: $\mathbb{Z} \subseteq \mathbb{Q}$, betrachte die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[i]$ und die Ringerweiterung $\mathbb{Z} \subseteq \mathbb{Z}[i]$. Naiver Gedanke wäre diejenige Ringerweiterung zu wählen, die durch die Adjunktion von den "dazugenommenen Elementen" entstünde. Das Problem dabei ist, dass man eine und dieselbe Körpererweiterung durch Adjunktion von verschiedenen Elementen bekommen kann, zum Beispiel: $\mathbb{Q}(i) = \mathbb{Q}(2i)$. Die darausresultierenden Ringerweiterungen haben aber nicht mehr dieselben Eigenschaften. $\mathbb{Z}[i]$ ist zum Beispiel faktoriell und $\mathbb{Z}[2i]$ ist es nicht.

Definition 4.1. *Sei $\mathcal{A} \subseteq \mathcal{B}$ eine Ringerweiterung.*

- *Ein Element $b \in \mathcal{B}$ heißt* ganz, *falls $n \in \mathbb{N}$ exisitert und $a_1, ..., a_n \in \mathcal{A}$, sodass*

$$1 \cdot b^n + a_1 b^{n-1} + ... + a_n = 0 (\rightsquigarrow \textbf{\textit{" Ganzheitsgleichung"}})$$

- *Eine Ringerweiterung heitßt* ganze Ringerweiterung, *falls jedes $b \in \mathcal{B}$ ganz ist.*

Beispiel 4.2.

- Jedes $a \in \mathcal{A}$ ist ganz über $\mathcal{A}$.
- $\sqrt{2} \in \mathbb{C}$ ist ganz über $\mathbb{Z}$:

$$\left(\sqrt{2}\right)^2 - 2 = 0$$

- $\frac{1}{2} \in \mathbb{Q}$ ist *nicht* ganz über $\mathbb{Z}$: Angenommen $\frac{1}{2}$ wäre ganz über $\mathbb{Z}$, so wäre die Ganzheitsgleichung erfüllt:

$$\begin{aligned} &\frac{1}{2}^n + a_1 \frac{1}{2}^{n-1} + ... + a_n = 0 \text{ für gewisse } a_1, ..., a_n \in \mathbb{Z} \\ &\implies \underbrace{1 + 2a_1 + ... + 2^n a_n}_{\text{ungerade}} = \underset{\text{gerade}}{0} \rightsquigarrow \textbf{Widerspruch} \end{aligned}$$

Definition 4.3. *Ein $\mathcal{A}$-Modul M heißt* treu, *falls für alle $0 \neq a \in \mathcal{A}$ ein $x \in M$ existiert mit $ax \neq 0$*

Beispiel 4.4.
- Freie und torsionsfreie Moduln sind treu (wenn es kein triviales Modul ist).
- $\mathbb{Z} \oplus \mathbb{Z}/(2)$ ist treu, aber nicht torsionsfrei $[n(1,0) \neq 0$ für alle $n \in \mathbb{Z} \setminus \{0\}]$.

Satz 4.5. *Sei $\mathcal{A} \subseteq \mathcal{B}$ eine Ringerweiterung, $b \in \mathcal{B}$. Die folgenden Aussagen sind äquivalent:*

(i) *b ganz über $\mathcal{A}$*

(ii) *Der Ring $\mathcal{A}[b]$ ist als $\mathcal{A}$-Modul endlich erzeugt*

(iii) *Es gibt einen treuen $\mathcal{A}[b]$-Modul, welcher als $\mathcal{A}$-Modul endlich erzeugt ist*

Beweis. $(i) \Rightarrow (ii)$: Sei $g(b) = 0$ die Ganzheitsgleichung für $g \in \mathcal{A}[X]$ mit dem Leitkoeffizienten 1. Für alle $f \in \mathcal{A}[X]$ gibt es dann $q, r \in \mathcal{A}[X]$ mit $f = qg + r$ und $\deg(q) > \deg(r)$ oder $r = 0$.

Kleine Anmerkung. Es ist wichtig, dass der Leitkoeffizient von g eine Eins ist (oder besser gesagt, eine Einheit) ist. Nur damit ist es wirklich gewährleistet, dass wir die obige Polynomdivision durchführen dürfen, weil $\mathcal{A}[X]$ im Allgemeinen kein euklidischer Ring ist.

Damit bekommen wir $f(b) = r(b)$ und somit wird $\mathcal{A}[b]$ als $\mathcal{A}$-Modul von $1, ..., b^{\deg(r)-1}$ erzeugt.

$(ii) \Rightarrow (iii)$: $\mathcal{A}[b]$ selbst ist ein gewünschter Modul, da $1 \in \mathcal{A}[b]$.

VL6, 7.05.2018

$(iii) \Rightarrow (i)$: Sei M ein treuer $\mathcal{A}[b]$-Modul, welcher als $\mathcal{A}$-Modul endlich erzeugt ist, etwa von $x_1, ..., x_n \in M$. Da $b \cdot x_i \in M$, folgt:

$$b \cdot x_i = a_{i1}x_1 + ... + a_{in}x_n, \quad a_{ij} \in \mathcal{A}\,.$$

Betrachte die Matrix $C = [a_{ij}]_{1 \leq i,j \leq n} \in \mathrm{Mat_n}(\mathcal{A}) \subseteq \mathrm{Mat_n}(\mathcal{A}[b])$. Nach Definition:

$$C \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = b \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \implies \underbrace{(b \cdot I_n - C)}_{=:D} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0$$

$$\implies \underbrace{\mathrm{adj}(D) \cdot D}_{=\det(D) \cdot I_n} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0 \implies \det(D) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0$$

$$\implies \det(D) \cdot x = 0 \quad \text{für alle } x \in M$$

$$\implies \det(D) = 0 \quad \text{da } M \text{ ein treuer Modul ist.}$$

Also ist $f = \det(T \cdot I_n - C) \in \mathcal{A}[T]$ als das charakteristische Polynom normiert und $f(b) = 0$ ist somit die gesuchte Ganzheitsgleichung. □

Korollar 4.6. *Sei $\mathcal{A} \subseteq \mathcal{B}$ eine Ringerweiterung. Ist $\mathcal{B}$ als $\mathcal{A}$-Modul endlich erzeugt, so ist die Ringerweiterung ganz.*

Beweis. Sei $b \in \mathcal{B}$. Dann ist $\mathcal{B}$ ein treuer $\mathcal{A}[b]$-Modul, da $1 \in \mathcal{B}$. Nach Voraussetzung ist $\mathcal{B}$ als $\mathcal{A}$-Modul endlich erzeugt. Nach dem Satz 4.5 ist b ganz über $\mathcal{A}$, somit ist die Ringerweiterung ganz. □

Definition und Satz 4.7. *Sei $\mathcal{A} \subseteq \mathcal{B}$ eine Ringerweiterung. Die Menge der ganzen Elemente über $\mathcal{A}$ in $\mathcal{B}$ bildet einen Teilring von $\mathcal{B}$. Dieser Teilring wird als* der ganze Abschluss von $\mathcal{A}$ in $\mathcal{B}$ *bezeichnet.*

Beweis. Seien $a, b \in \mathcal{B}$ ganz über $\mathcal{A}$. Betrachte den Teilring $C = \mathcal{A}[a, b] = \left\{ \sum_{i=1}^{r} f_i g_i : r \in \mathbb{N}, f_i \in \mathcal{A}[a], g_i \in \mathcal{A}[b] \right\}$. Da a, b ganz sind, sind die Ringe $\mathcal{A}[a]$ und $\mathcal{A}[b]$ als $\mathcal{A}$-Moduln endlich erzeugt, etwa von $x_1, ..., x_n \in \mathcal{A}[a]$ bzw. $y_1, ..., y_m \in \mathcal{A}[b]$. Dann erzeugen $x_1y_1, ..., x_1y_m, ..., x_ny_m$ den Ring C als $\mathcal{A}$-Modul. Außerdem ist C für alle $c \in C$ ein treuer $\mathcal{A}[a, b]$-Modul, da $1 \in C$. Als ist $\mathcal{A} \subseteq C$ eine ganze Ringerweiterung nach dem Satz 4.5. Da insbesondere $a + b \in C$ liegen, ist $a + b$ ganz über $\mathcal{A}$. Somit bildet der ganze Abschluss einen Teilring von $\mathcal{B}$. □

Definition 4.8. *Ein Ring $\mathcal{A}$ heißt* ganz abgeschlossen, *falls $\mathcal{A}$ nullteilerfrei und gleich seinem ganzen Abschluss in $\mathrm{Quot}(\mathcal{A})$ ist.*

Satz 4.9. *Faktorielle Ringe sind ganz abgeschlossen.*

Beweis. Sei $\mathcal{A}$ faktoriell und $p/q \in \mathrm{Quot}(\mathcal{A})$ ganz über $\mathcal{A}$ mit $p, q \in \mathcal{A} \setminus \{0\}$ teilerfremd. Seien $a_1, ..., a_n \in \mathcal{A}$ mit

$$\begin{aligned} & (p/q)^n + a_1 (p/q)^{n-1} + ... + a_n = 0 \mid \cdot q^n \\ \Longrightarrow\ & p^n + q \cdot (a_1 p^{n-1} + ... + a_n q^{n-1}) = 0 \\ \Longrightarrow\ & qp^n \implies q \in \mathcal{A}^\times, \quad \text{da } p, q \text{ teilerfremd sind} \\ \Longrightarrow\ & p/q \in \mathcal{A}, \quad \text{also ist } \mathcal{A} \text{ ganz abgeschlossen.} \end{aligned}$$

□

Beispiel 4.10. $\mathbb{Z}$, $\mathbb{K}[X_1, ..., X_n]$, $\mathbb{K}$ Körper sind ganz abgeschlossen.

Lemma 4.11. *Sei $\mathcal{A} \subseteq \mathcal{B}$ eine ganze Ringerweiterung mit $\mathcal{B} = \mathcal{A}[b_1, ..., b_n]$. Dann ist $\mathcal{B}$ als $\mathcal{A}$-Modul endlich erzeugt.*

Beweis. Induktion nach n.

$n = 1$: $\rightsquigarrow$ ✓

$n \to n+1$: $\mathcal{A}[b_1, ..., b_n]$ ist endlich erzeugt als $\mathcal{A}$-Modul nach Induktionsvoraussetzung, etwa von $x_1, ..., x_r$. Andererseits wissen wir, dass $\mathcal{A}[b_1, ..., b_{n+1}] = \mathcal{A}[b_1, ..., b_n][b_{b+1}]$ als $\mathcal{A}[b_1, ..., b_n]$-Modul endlich erzeugt ist, etwa von $y_1, ..., y_s$. Damit ist $\mathcal{A}[b_1, ..., b_{n+1}]$ als $\mathcal{A}$-Modul endlich erzeugt von $x_1y_1, ..., x_ry_s$.

□

Lemma 4.12. *Seien $\mathcal{A} \subseteq \mathcal{B}, \mathcal{B} \subseteq \mathcal{C}$ ganze Ringerweiterungen. Dann ist die Ringerweiterung $\mathcal{A} \subseteq \mathcal{C}$ auch ganz.*

Beweis. Sei $c \in \mathcal{C}$. Dann gibt es $b_1, ..., b_n \in \mathcal{B}$ mit

$$c^n + b_1c^{n-1} + ... + b_n = 0.$$

Damit ist c auch ganz über $\mathcal{A}[b_1, ..., b_n] =: \mathcal{B}_1 \subseteq \mathcal{B}$. Da $\mathcal{A} \subseteq \mathcal{B}_1$ ganze Ringerweiterung, ist $\mathcal{B}_1$ als $\mathcal{A}$-Modul endlich erzeugt nach dem vorherigen Lemma, etwa von $y_1, ..., y_s$. Außerdem ist $\mathcal{B}_1[c]$ endlich erzeugt als $\mathcal{B}_1$-Modul, etwa von $x_1, ..., x_r$. Also ist $\mathcal{A}[b_1, ..., b_n, c] = \mathcal{B}_1[c]$ als $\mathcal{A}$-Modul endlich erzeugt von $x_1y_1, ..., x_ry_s$. Nach dem Korollar 4.5 ist $\mathcal{B}_1[c]$ ganz über $\mathcal{A}$. Weil $c \in \mathcal{C}$ beliebig war, folgt die Behauptung. □

Korollar 4.13. *Ist $\mathbb{K}$ ein Körper und $\mathcal{A} \subseteq \mathbb{K}$ ein Teilring, so ist der ganze Abschluss $\mathcal{A}'$ von $\mathcal{A}$ in $\mathbb{K}$ ganz abgeschlossen.*

Beweis. Sei $\mathcal{A}''$ der ganze Abschluss von $\mathcal{A}'$ in $\mathrm{Quot}(\mathcal{A}') \subseteq \mathbb{K}$. Dann sind $\mathcal{A} \subseteq \mathcal{A}'$ und $\mathcal{A}' \subseteq \mathcal{A}''$ jeweils ganze Ringerweiterungen. Nach dem Lemma 4.12 ist $\mathcal{A} \subseteq \mathcal{A}''$ ebenfalls eine ganze Ringerweiterung. Somit gilt $\mathcal{A}'' \subseteq \mathcal{A}'$, da $\mathcal{A}'$ der ganze Abschluss von $\mathcal{A}$ ist. □

Beispiel 4.14. Der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(i)$ ist $\mathbb{Z}[i]$:

- i ist ganz über $\mathbb{Z}$: $i^2 + 1 = 0$
- $\mathrm{Quot}(\mathbb{Z}[i]) = \mathbb{Q}(i)$ und $\mathbb{Z}[i]$ ganz abgeschlossen, da faktoriell.

Satz 4.15. *Sei $\mathcal{A}$ ganz abgeschlossen, $\mathbb{K} = \mathrm{Quot}(\mathcal{A})$ und $\mathbb{K} \subseteq \mathbb{L}$ eine Körpererweiterung. Der ganze Abschluss $\mathcal{B}$ von $\mathcal{A}$ besteht aus $\alpha \in \mathbb{L}$, für die*

$$q_\alpha := \mathrm{MinPol}(\alpha/\mathbb{K}) \in \mathcal{A}[X]$$

liegt.

Beweis. Es ist klar, dass solche $\alpha \in \mathcal{B}$ liegen, dabei ist q_α die Ganzheitsgleichung.

Umgekehrt sei $\alpha \in \mathcal{B}$, dann existiert ein normiertes Polynom $f \in \mathcal{A}[X]$ mit $f(\alpha) = 0$. Damit muss das Minimalpolynom q_α das Polynom f teilen, also gilt $f = g \cdot q_\alpha$ für ein $g \in \mathbb{K}[X]$. Alle Nullstellen von q_α in $\bar{\mathbb{L}}$ sind auch ganz über $\mathcal{A}$ (wähle f als die Ganzheitsgleichung). Also sind die Koeffizienten von q_α ganz über $\mathcal{A}$. Diese liegen in $\mathbb{K}$, also schon $\mathcal{A}$, da $\mathcal{A}$ ganz abgeschlossen ist. □

VL7, 8.05.18

Satz 4.16. *Für $\pm 1 \neq d \in \mathbb{Z}$ quadratfrei ist der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ gegeben durch:*

- $\mathbb{Z}[\sqrt{d}]$, *falls* $d \not\equiv 1 \mod (4)$
- $\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ *sonst*

Beweis. Sei $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$ und $b \neq 0$. Dann ist $q_\alpha = X^2 - 2aX + (a^2 - b^2 d)$ das Minimalpolynom von α über $\mathbb{Q}$. Falls α ganz über $\mathbb{Q}$ ist, so ist $2a \in \mathbb{Z}$, also $a = k/2$ für $k \in \mathbb{Z}$. Außerdem

$$\frac{k^2}{4} - b^2 d \in \mathbb{Z} \implies \frac{k^2 - 4b^2 d}{4} \in \mathbb{Z}$$

. Da d quadratfrei ist, folgt $b = \frac{m}{2}$ für ein $m \in \mathbb{Z}$. Also

$$\frac{k^2 - m^2 d}{4} \in \mathbb{Z} \implies 4 \mid k^2 - m^2 d \implies k^2 \equiv m^2 d \mod 4$$

.

Fall 1: $d \not\equiv 1 \mod 4$, so ist das nur möglich falls $k, m \in 2\,\mathbb{Z}$

- $d \equiv 2 \mod 4$:
  $2 \mid m^2 d \Rightarrow 2 \mid k^2 \Rightarrow 2 \mid k \Rightarrow 4 \mid k^2 \Rightarrow 4 \mid m^2 d \Rightarrow 2 \mid m$
- $d \equiv 3 \mod 4$:
  Man kann also $k^2 \equiv -m^2 \mod 4$ schreiben.

n	n^2	$-n^2$
1	1	-1
2	0	0
3	1	-1
0	0	0

$\implies k, m \equiv 0, 2 \mod 4$

Also $\alpha = a + b\sqrt{d} = \frac{k}{2} + \frac{m}{2}\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Umgekehrt ist $\mathbb{Z}[\sqrt{d}]$ ganz über $\mathbb{Z}$: $\sqrt{d}^2 - d = 0$.

Fall 2: $d \equiv 1 \mod 4$, dann haben wir $k^2 = m^2 \mod 4 \Rightarrow k \equiv m \mod 4$, also $k = m + 2l$ für ein $l \in \mathbb{Z}$. Es folgt:

$$\alpha = \frac{m}{2} + l + \frac{m}{2}\sqrt{d} = l + m \cdot \frac{1}{2}(1 + \sqrt{d}) \in \mathbb{Z}\left[\frac{1}{2}(1 + \sqrt{d})\right]$$

Umgekehrt:

$$\left(\frac{1}{2}(1 + \sqrt{d})\right)^2 - \frac{1}{2}(1 + \sqrt{d}) + \frac{1 - d}{4} = 0$$

□

Beispiel 4.17. $\mathbb{Z}[\sqrt{3}]$ ist ganz abgeschlossen, $\mathbb{Z}[\sqrt{5}]$ dagegen nicht.

Lemma 4.18. *Sei $\mathcal{A}$ ein Integritätsbereich und $\mathbb{K} = \mathrm{Quot}(\mathcal{A})$. Sei $\mathbb{K} \subseteq \mathbb{L}$ eine Körpererweiterung. Sei $\mathcal{B}$ der ganze Abschluss von $\mathcal{A}$ in $\mathbb{L}$. Sei $S \subseteq \mathcal{A}$ eine multiplikativ abgeschlossenen Teilmenge von $\mathcal{A}$ mit $S \neq 0$. Dann ist der ganze Abschluss von $\mathcal{A}[S^{-1}]$ in $\mathbb{L}$ gleich $\mathcal{B}[S^{-1}]$.*

Beweis. Sei $b/s \in \mathcal{B}[S^{-1}]$ mit $b \in \mathcal{B}$, $s \in S$. Da b ganz über $\mathcal{A}$ ist, existieren $a_1, ..., a_n \in \mathcal{A}$ mit

$$b^n + a_1 b^{n-1} + ... + a_n = 0 \mid \cdot 1/s^n$$
$$(b/s)^n + \underset{\in \mathcal{A}[S^{-1}]}{a/s}\,(b/s)^{n-1} + ... + \underset{\in \mathcal{A}[S^{-1}]}{a_n/s^n} = 0$$

$\Longrightarrow$ b/s ist ganz über $\mathcal{A}[S^{-1}]$.

Umgekehrt sei β ganz über $\mathcal{A}[S^{-1}]$ mit $\beta \in \mathbb{L}$. Dann lautet die Ganzheitsgleichung:

$$\beta^n + a_1/s_1 \beta^{n-1} + ... + a_n/s_n = 0 \quad \text{mit } a_i \in \mathcal{A}, s_i \in S.$$

Sei $s := s_1 \cdot ... \cdot s_n$ der Hauptnenner, dann folgt:

$$(s\beta)^n + s_2 \cdot ... \cdot s_n \cdot a_1 (s\beta)^{n-1} + ... + s_1^n \cdot ... \cdot s_{n-1}^n \cdot s_n^{n-1} \cdot a_n = 0$$

Damit ist $s\beta$ ganz über $\mathcal{A}$, $s\beta \in \mathcal{B}$, also $\beta = \frac{s\beta}{s} \in \mathcal{B}[S^{-1}]$. □

Korollar 4.19. *Ist $\mathcal{A}$ ganz abgeschlossen und $0 \notin S \subseteq \mathcal{A}$ multiplikativ abgeschlossene Teilmenge, so ist auch $\mathcal{A}[S^{-1}]$ ganz abgeschlossen.*

Beweis. Wähle $\mathbb{L} = \mathbb{K}$ und damit $\mathcal{A} = \mathcal{B}$ der ganze Abschluss von $\mathcal{A}$ in $\mathbb{L}$. Nach dem Lemma 4.18 ist der ganze Abschluss von $\mathcal{A}[S^{-1}]$ in $\mathbb{L}$ gerade $\mathcal{A}[S^{-1}]$. □

Korollar 4.20. *Sei $\mathcal{A}$ ein Integritätsbereich, $\mathbb{K} = \mathrm{Quot}(\mathcal{A})$, $\mathbb{K} \subseteq \mathbb{L}$ algebraische Körpererweiterung, $\mathcal{B}$ ganzer Abschluss von $\mathcal{A}$ in $\mathbb{L}$. Dann gibt es für jedes $y \in \mathbb{L}$ ein $0 \neq a \in \mathcal{A}$ mit $a \cdot y \in \mathcal{B}$. Insbesondere gilt $\mathbb{L} = \mathrm{Quot}(\mathcal{B})$.*

Beweis. Wähle $S = \mathcal{A} \setminus \{0\}$. Dann ist $\mathcal{A}[S^{-1}] = \mathbb{K}$ und $\mathcal{B}[S^{-1}]$ ist der ganze Abschluss von $\mathbb{K}$ in $\mathbb{L}$, da $\mathbb{L}$ algebraisch über $\mathbb{K}$ ist. Damit ist $\mathbb{L} = \mathcal{B}[S^{-1}]$. □

Wiederholung: Separable Körpererweiterungen

Sei $\mathbb{K} \subseteq \mathbb{L}$ eine Körpererweiterung. Ein Element $\alpha \in \mathbb{L}$ heißt *separabel über* $\mathbb{K}$, falls sein Minimalpolynom nur einfache Nullstellen im algebraischen Abschluss $\bar{\mathbb{L}}$ besitzt. Die Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ heißt *separabel*, falls jedes $\alpha \in \mathbb{L}$ separabel ist.

Satz 4.21. *Ist $\mathbb{K} \subseteq \mathbb{L}$ eine endliche separable Körpererweiterung, so gibt es ein $\alpha \in \mathbb{L}$, für welches $\mathbb{L} = \mathbb{K}(\alpha)$ gilt.*

Satz 4.22. *Ist $\mathbb{K} \subseteq \mathbb{L}$ eine endliche separable Körpererweiterung mit $[\mathbb{L} : \mathbb{K}] = n$ und $\bar{\mathbb{K}}$ der algebraische Abschluss von $\mathbb{K}$, dann gibt es genau n Körperhomomorphismen $\sigma_1, ..., \sigma_n : \mathbb{L} \to \bar{\mathbb{K}}$ mit $\sigma_i(x) = x$ für alle $x \in \mathbb{K}$. Ist umgekehrt $y \in \mathbb{L}$ mit $\sigma_i(y) = y$ für alle $i = 1...n$, so ist $y \in \mathbb{K}$.*

Bemerkung 4.23. Für jedes $\alpha \in \mathbb{L}$ haben wir eine Äquivalenzklasse auf $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{K}}) = \{\sigma_1, ..., \sigma_n\} : \sigma_i \sim \sigma_j :|\Rightarrow \sigma_i\alpha = \sigma_j\alpha$. Jede Äquivalenzklasse hat genau $[\mathbb{L} : \mathbb{K}(\alpha)]$ Elemente. Sei $\tau_1, ..., \tau_r$ das Repräsentantensystem von $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{K}})$. Dann ist $\prod_{i=1}^{r}(X - \tau_i(\alpha))$ das Minimalpolynom von α über $\mathbb{K}$.

$\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{E}$ endliche separable Körpererweiterung. Sei $\bar{\mathbb{E}}$ der algebraische Abschluss von $\mathbb{E}$ und $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{E}}) = \{\sigma_1, ..., \sigma_n\}$ und $\mathrm{Hom}_{\mathbb{L}}(\mathbb{E}, \bar{\mathbb{E}}) = \{\tau_1, ..., \tau_m\}$ die Homomorphismen von $\mathbb{L}$ bzw. $\mathbb{E}$ nach $\bar{\mathbb{E}}$. Dann ist $\mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \bar{\mathbb{E}}) = \{\sigma_1 \circ \tau_1, ..., \sigma_1 \circ \tau_m, ..., \sigma_n \circ \tau_m\}$

5 Norm, Spur und Diskriminante einer Körpererweiterung

Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche Körpererweiterung. Sei $\alpha \in \mathbb{L}$. Betrachte $\mathbb{K}$-lineare Abbildung $\mu_\alpha : \mathbb{L} \to \mathbb{L}, \quad x \mapsto \alpha \cdot x$ des $\mathbb{K}$-Vektorraum. Sei $p_\alpha \in \mathbb{K}[X]$ dessen charakteristische Polynom. Sei f_α das Minimalpolynom von α über $\mathbb{K}$.

Lemma 5.1. *Für die Abbildung μ_α gilt: $p_\alpha = f_\alpha^m$ mit $m = [\mathbb{L} : \mathbb{K}(\alpha)]$.*

Beweis. Sei $f_\alpha = X^n + c_1 X^{n-1} + ... + c_n$, $c_i \in \mathbb{K}$, wobei $n = [\mathbb{K}(\alpha) : \mathbb{K}]$. Sei $\beta_1, ..., \beta_m$ eine $\mathbb{K}(\alpha)$-Basis von $\mathbb{L}$. Dann ist $\beta_1, \beta_1\alpha, ..., \beta_1\alpha^{n-1}, ..., \beta_m, ..., \beta_m\alpha^{n-1}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$. Die darstellende Matrix von μ_α bezüglich dieser Basis ist:

$$\begin{bmatrix} c & 0 & \cdots & 0 \\ 0 & c & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & c \end{bmatrix}, \quad \text{wobei } c = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_n \\ 1 & 0 & \cdots & 0 & -c_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_1 \end{bmatrix}$$

Man rechnet nach, dass $f_\alpha = \det(XI_n - c)$. □

Definition 5.2. *Für $\alpha \in \mathbb{L}$ heißt*

- $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) := \mathrm{tr}(\mu_\alpha)$ die Spur von α
- $N_{\mathbb{L}/\mathbb{K}}(\alpha) := \det(\mu_\alpha)$ die Norm von α

VL 8, 14.05.18

Wiederholung: $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung, $\alpha \in \mathbb{L}$, $\mu_\alpha : \mathbb{L} \to \mathbb{L}$, $x \mapsto \alpha \cdot x$ $\mathbb{K}$-linear, p_α das charakteristische Polynom der Abbildung, f_α das Minimalpolynom von $\alpha \in \mathbb{L}$ über $\mathbb{K}$

- $p_\alpha = f_\alpha^m$ mit $m = [\mathbb{L} : \mathbb{K}(\alpha)]$
- $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) := \mathrm{tr}(\mu_\alpha)$ die Spur
- $N_{\mathbb{L}/\mathbb{K}}(\alpha) := \det(\mu_\alpha)$ die Norm

Lemma 5.3. *Sei $n = [\mathbb{L} : \mathbb{K}(\alpha)]$ und $\alpha, \beta \in \mathbb{L}$. Dann*

(a) $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) : \mathbb{L} \to \mathbb{L}$ *ist $\mathbb{K}$-linear.*

(b) $N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha) N_{\mathbb{L}/\mathbb{K}}(\beta)$

(c) Ist $\alpha \in \mathbb{K}$, so ist $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha^n$ und $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = n\alpha$

(d) ist $f_\alpha = X^r + a_1 X^{r-1} + ... + a_r$ und $m := [\mathbb{L} : \mathbb{K}(\alpha)]$, so ist $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = -ma_1$ und $N_{\mathbb{L}/\mathbb{K}} = \left((-1)^r a_r\right)^m$

Beweis. *(a)* $\rightsquigarrow$ ✓

(b) $\rightsquigarrow$ ✓

(c) mit $\mu_\alpha = \alpha I_n$ ergibt sich die Aussage

(d) folgt aus Lemma 5.1: $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}$ ist der zweithöchste Koeffizient des charakteristischen Polynoms (-1)-mal, sowie $N_{\mathbb{L}/\mathbb{K}}$ ist $(-1)^n$-mal der konstante Term des charakteristischen Polynoms.

□

Korollar 5.4. *Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung mit $[Lk : \mathbb{K}] = n$ und $\sigma_1, ..., \sigma_n : \mathbb{L} \to \bar{\mathbb{K}}$ die verschiedenen $\mathbb{K}$-Einbettungen von $\mathbb{L}$ in den algebraischen Abschluss von $\mathbb{K}$. Für $\alpha \in \mathbb{L}$ gilt:*

$$\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \textit{und} \quad N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

Beweis. Sei $\tau_1, ..., \tau_r$ ein Repräsentantensystem von $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{K}})$ bezüglich der Äquivalezrelation $\sigma \sim \sigma' :\iff \sigma(\alpha) = \sigma'(\alpha)$. Dann ist $p_\alpha = f_\alpha^m = \left(\prod_{i=1}^{r}(X - \tau_i(\alpha))\right)^m = \prod_{i=1}^{n}\left(X - \sigma_i(\alpha)\right)$

Kleine Anmerkung. Weil jede Äquivalenzklasse von $\tau_i(\alpha)$ aus dem Repräsentantensystem genau m Stück Abbildungen hat. Diese Tatsache folgt aus der Galois-Theorie.

□

Satz 5.5. *Seien $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{E}$ endliche separable Körpererweiterungen. Für jedes $\alpha \in \mathbb{E}$ gilt:*

$$\mathrm{tr}_{\mathbb{E}/\mathbb{K}}(\alpha) = \mathrm{tr}_{\mathbb{E}/\mathbb{L}}\left(\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha)\right) \quad \textit{sowie} \quad N_{\mathbb{E}/\mathbb{K}}(\alpha) = N_{\mathbb{E}/\mathbb{L}}\big(N_{\mathbb{L}/\mathbb{K}}(\alpha)\big)$$

Beweis. Sei $\bar{\mathbb{E}}$ ein algebraischer Abschluss von $\mathbb{E}$. Sei $\sigma_1, ..., \sigma_r$ ein Repräsentantensystem von $\mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \bar{\mathbb{E}})$ bezüglich der Äquivalezrelation: $\sigma \sim \sigma' :\iff \sigma\mid_{\mathbb{L}} = \sigma'\mid_{\mathbb{L}}$. Dann ist $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{E}}) = \left\{\sigma_i\mid_{\mathbb{L}} : i = 1...r\right\}$ und somit

$$\mathrm{tr}_{\mathbb{E}/\mathbb{K}}(\alpha) = \sum_{i=1}^{r} \sum_{\sigma \sim \sigma_i} \sigma(\alpha) = \sum_{i=1}^{r} \sigma_i(\mathrm{tr}_{\mathbb{E}/\mathbb{L}}(\alpha)) = \mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\mathrm{tr}_{\mathbb{E}/\mathbb{L}}(\alpha))$$

Die Aussage für die Norm folgt analog. □

Erinnerung: Ist V ein $\mathbb{K}$-Vektorraum mit $\dim V = n < \infty$, so heißt eine symmetrische Bilinearform $b : V \times V \to \mathbb{K}$ *nicht ausgeartet*, falls für jedes $0 \neq v \in V$ existiert ein $w \in V$ sodass $b(v, w) \neq 0$. Man kann b als eine Abblidung von V in seinen Dualraum auffassen: $b : V \to V^V, \quad v \mapsto [w \mapsto b(v, w)]$. Falls b nicht ausgeartet ist, ist b als Abbildung ins Duale ein Isomorphismus. Dazu äquivalent ist die Bedingung, dass $\det[b(v_i, v_j)] \neq 0$ für eine Basis $v_1, ..., v_n$ von V. In dem Fall existiert eine Basis $w_1, ..., w_n \in V$ mit $b(v_i, w_j) = \delta_{i,j}$.

Definition 5.6. *Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung.*

(a) Die symmetrische Bilinearform b

$$b : \mathbb{L} \times \mathbb{L} \to \mathbb{K}, \quad b(\alpha, \beta) = \mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha \cdot \beta)$$

heißt die Spurform von $\mathbb{K} \subseteq \mathbb{L}$.

(b) Sei $n = [\mathbb{L} : \mathbb{K}]$ und $\mathcal{B} = (\alpha_1, ..., \alpha_n) \in \mathbb{L}^n$ eine Basis von $\mathbb{L}$. Dann ist

$$d(\mathcal{B}) = d_{\mathbb{L}/\mathbb{K}}(\mathcal{B}) := \det(\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j))_{i,j}$$

die Diskriminante von $\mathbb{K} \subseteq \mathbb{L}$.

Lemma 5.7. *Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung mit $[\mathbb{L} : \mathbb{K}] = n$. Für $\alpha_1, ..., \alpha_n \in \mathbb{L}$ ist $d_{\mathbb{L}/\mathbb{K}}(\alpha_1, ..., \alpha_n) = (\det V)^2$ mit $V = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}$, wobei $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{K}}) = \{\sigma_1, ..., \sigma_n\}$.*

Beweis. Betrachte

$$V^T V = \left(\sum_{i=1}^{n} \sigma_i(\alpha_k)\sigma_i(\alpha_l) \right)_{k,l} = \left(\sum_{i=1}^{n} \sigma_i(\alpha_k \alpha_l) \right)_{k,l} = \left(\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha_k \alpha_l) \right)_{k,l}$$

Damit bekommen wir $d(\alpha_1, ..., \alpha_n) = \det V^T V = (\det V)^2$ □

Satz 5.8. *Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung. Dann ist die Spurform nicht ausgeartet.*

Beweis. Sei $\mathbb{L} = \mathbb{K}(\alpha)$ für ein geeignetes $\alpha \in \mathbb{L}$ (die Existenz von α folgt aus dem Satz vom primitiven Element). Dann ist $1, \alpha, ..., \alpha^{n-1}$ mit $n = [\mathbb{L} : \mathbb{K}]$ eine $\mathbb{K}$-Basis von $\mathbb{L}$. Es ist:

$$d(1, \alpha, ..., \alpha^{n-1}) = (\det V)^2, \quad \text{mit } V = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \end{bmatrix}$$

, wobei $\alpha_j = \sigma_j(\alpha), \sigma_j \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \bar{\mathbb{K}}) \rightsquigarrow \alpha_1, ..., \alpha_n$ sind die verschiedenen Nullstellen des Minimalpolynoms f_α. Da die Körpererweiterung separabel ist, ist $\det V = \prod_{1 \geq i < j \leq n} (\alpha_j - \alpha_i) \neq 0$.

□

Lemma 5.9. *Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung mit $[\mathbb{L} : \mathbb{K}] = n$, $\alpha_1, ..., \alpha_n \in \mathbb{L}$.*

(a) $d(\alpha_1, ..., \alpha_n) = 0 \iff \alpha_1, ..., \alpha_n$ *linear abhängig*

(b) Für jede $\mathbb{K}$-lineare Abbildung $s : \mathbb{L} \to \mathbb{L}$ gilt

$$d(s(\alpha_1), ..., s(\alpha_n)) = \det(s)^2 d(\alpha_1, ..., \alpha_n)$$

Beweis. *(a)* " $\Rightarrow$ " folgt daraus, dass die Spurform nicht ausgeartet ist
" $\Leftarrow$ " Ist $\lambda_1\alpha_1 + ... + \lambda_n\alpha_n = 0$ für $\lambda_i \in \mathbb{K}$, so ist

$$\big(\mathrm{tr}(\alpha_i\alpha_j)\big)_{i,j}[\lambda_1, ..., \lambda_n]^T = 0$$

(b) OBdA $\alpha_1, ..., \alpha_n$ eine Basis, M sei die darstellende Matrix von s. Dann ist

$$\big(\mathrm{tr}(s(\alpha_i)s(\alpha_j))\big)_{i,j} = M^T \big(\mathrm{tr}(\alpha_i\alpha_j)\big)_{i,j} M$$

Die Behauptung folgt aufgrund des Determinantenproduktsatzes.

□

Satz 5.10. *Sei $\mathcal{A}$ ganz abgeschlossen und noethersch, $\mathbb{K} = \mathrm{Quot}(\mathcal{A})$. Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche separable Körpererweiterung. Dann ist der ganze Abschluss $\mathcal{B}$ von $\mathcal{A}$ in $\mathbb{L}$ ebenfalls noethersch und endlich erzeugt als $\mathcal{A}$-Modul.*

Beweis. Sei $a_1, ..., a_n \in \mathbb{L}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$. Nach Korollar 4.20 existiert zu jedem a_i ein $s_i \in \mathcal{A} \setminus \{0\}$, sodass $s_i a_i \in \mathcal{B}$. Wir können also oBdA annehmen, dass $a_1, ..., a_n \in \mathcal{B}$. Sei $b_1, ..., b_n \in \mathbb{L}$ die zu $a_1, ..., a_n$ duale Basis. Sei $b \in \mathcal{B}$, dann gibt es $\lambda_1, ...\lambda_n \in \mathbb{K}$ mit $b = \lambda_1 b_1 + \lambda_n b_n$. Dann ist $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(a_i b) = \lambda_i$ *weil die Basis dual ist*.

Behauptung. $\lambda_i \in \mathcal{A}$

In der Tat: nach Lemma 5.3 ist $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(a_i b) = -mc$ mit $m \in \mathbb{Z}_{\geq 0}$ und c ein Koeffizient des Minimalpolynoms von $a_i b$. Damit liegt $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(a_i b) \in \mathcal{A}$, da $a_i b \in \mathcal{B}$ ganz über $\mathcal{A}$ ist. $\implies$ $\mathcal{B}$ enthalten im $\mathcal{A}$-Modul, welchen von $b_1, ..., b_n$ erzeugt wird. Da $\mathcal{A}$ noethersch ist, ist dieser erzeugter Modul ebenfalls noethersch, wodurch $\mathcal{B}$ als $\mathcal{A}$-Modul endlich erzeugt ist. □

Bemerkung 5.11. In der Situation vom Satz 5.10 haben wir gesehen, dass $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(b) \in \mathcal{A}$ für alle $b \in \mathcal{B}$. Analog kann man zeigen, dass auch $N_{\mathbb{L}/\mathbb{K}}(b) \in \mathcal{A}$ für alle $b \in \mathcal{B}$ gilt.

VL9, 16.05.18

6 Dedekindringe

Definition 6.1. *Ein* Dedekindring *ist ein Integritätsbereich, der noethersch, ganz abgeschlossen und jedes seiner Primideale $\neq (0)$ ist maximal.*

Beispiel 6.2. *(a)* Jeder Hauptidealbereich $\mathcal{A}$ ist ein Dedekindring .

- noethersch $\rightsquigarrow$ ✓
- ganzabgeschlossen, da faktoriell
- Seien $(0) \subsetneq \mathfrak{P} \subseteq I \subsetneq \mathcal{A}$ ein Primideal $\mathfrak{P}$ und I ein Ideal. Da $\mathcal{A}$ Hauptidealring ist, gibt es ein p und ein a, sodass $\mathfrak{P} = (p)$ und $I = (a)$, wobei p irreduzibel und $a \notin \mathcal{A}^\times$. Da $\mathfrak{P} \subseteq I$, folgt $a \mid p$, also $a \sim p$, weil p irreduzibel ist. Damit folgt $\mathfrak{P} = I$.

(b) $\mathbb{Q}[X, Y]$ oder $\mathbb{Z}[X]$ sind keine Dedekindringe:

- $(0) \subsetneq (X) \subsetneq (X, Y) \subsetneq \mathbb{Q}[X, Y]$
- $(0) \subsetneq (X) \subsetneq \mathbb{Z}[X]$

Satz 6.3. *Sei $\mathcal{A}$ ein Dedekindring , $\mathbb{K} = \mathrm{Quot}(\mathcal{A})$ und $\mathbb{K} \subseteq \mathbb{L}$ eine endliche separable Körpererweiterung . Dann ist der ganze Abschluss $\mathcal{B}$ von $\mathcal{A}$ in $\mathbb{L}$ ein Dedekindring .*

Um den obigen Satz zu beweisen, benötigen wir etwas Vorarbeit.

Lemma 6.4. *Sei $\mathcal{A} \subseteq \mathcal{B}$ eine ganze Erweiterung der Integritätsringe. Sei $\mathfrak{Q} \subseteq \mathcal{B}$ ein Primideal, sodass $\mathcal{A} \cap \mathfrak{Q}$ ein maximales Ideal von $\mathcal{A}$ ist. Dann ist $\mathfrak{Q}$ bereits maximal gewesen.*

Beweis. Betrachte ein Homomorphismus

$$\begin{array}{ccc} \mathcal{A} \hookrightarrow \mathcal{B} & \to & \mathcal{B} \,/\, \mathfrak{Q} \\ \downarrow & \nearrow & \\ \mathcal{A} \,/\, \mathfrak{P} & & \end{array}$$

Wir bekommen eine Inklusion von $\mathcal{A} \,/\, \mathfrak{P} \hookrightarrow \mathcal{B} \,/\, \mathfrak{Q}$. Es ist sogar eine ganze Ringerweiterung, da sich die Ganzheitsgleichung aus der ursprünglichen Ringerweiterung auf die Äquivalenzklassen überträgt. Da $\mathcal{A} \,/\, \mathfrak{P}$ ein Körper ist, ist $\mathcal{B} \,/\, \mathfrak{Q}$ ebenfalls ein Körper. Also muss $\mathfrak{Q}$ maximal gewesen sein. □

Nun kommen wir zum Beweis vom Satz 6.3

Beweis. (vom Satz 6.3) Wir weisen jede Eigenschaft eines Dedekindringes für $\mathcal{B}$ nach

- $\mathcal{B}$ noethersch: Siehe den Satz 5.10
- $\mathcal{B}$ ganz abgeschlossen, weil $\mathcal{B}$ der ganze Abschluss ist.
- Idealeigenschaft: Sei $(0) \subsetneq \mathfrak{Q} \subseteq \mathcal{B}$ ein Primideal in $\mathcal{B}$. Dann ist $\mathfrak{Q} \cap \mathcal{A} := \mathfrak{P}$ ein Primideal von $\mathcal{A}$ (falls nicht klar, überlege was die Primidealeigenschaft heißt und dass $\mathcal{A}$ in $\mathcal{B}$ enthalten ist). Es ist auch $(0) \neq \mathfrak{P}$, denn etwa $0 \neq N_{\mathbb{L}\,/\,\mathbb{K}}(\alpha) \in \mathfrak{P}$ für ein $0 \neq \alpha \in \mathfrak{Q}$ (so eins muss es nach Voraussetzung geben): Denn $N_{\mathbb{L}\,/\,\mathbb{K}}(\alpha) \in \mathfrak{Q}$ (warum?) und $N_{\mathbb{L}\,/\,\mathbb{K}}(\alpha) \in \mathcal{A}$, siehe Bemerkung zum Satz 5.10. Nach Lemma 6.4 ist $\mathfrak{Q}$ ein maximales Ideal.

Damit ist $\mathcal{B}$ ein Dedekindring . □

Beispiel 6.5. Sei $\mathbb{Q} \subseteq \mathbb{K}$ eine endliche separable Körpererweiterung . Dann ist der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{K}$ nach Satz 6.3 ein Dedekindring , etwa $\mathbb{Z}[i], \mathbb{Z}[\sqrt{3}], \mathbb{Z}\left[1/2(1+\sqrt{5})\right]$.

Lemma 6.6. *Sei $\mathcal{A}$ ein Integritätsbereich und noethersch, $\mathbb{K} = \mathrm{Quot}(\mathcal{A})$. Für jeden $\mathcal{A}$-Untermodul I von $\mathbb{K}$ sind äquivalent:*

(i) I ist endlich erzeugt als $\mathcal{A}$-Modul

(ii) Es existiert ein $0 \neq a \in \mathbb{K}$ mit $aI = \{ax : x \in I\}$

(iii) Es existiert ein $0 \neq a \in \mathcal{A}$ und ein J Ideal von $\mathcal{A}$ mit $I = a^{-1}J$

Falls $(i) - (iii)$ *erfüllt sind und falls* $(0) \neq I$*, so heißt* I *ein* gebrochenes Ideal *von* $\mathcal{A}$*.*

Beweis. $(i) \Rightarrow (iii)$ Sei I endlich erzeugt von $\frac{a_1}{s_1}, ..., \frac{a_n}{s_n} \in \mathbb{K}$ Wir können $a := s_1 \cdot ... \cdot s_n$ wählen.

$(iii) \Rightarrow (ii) \rightsquigarrow \checkmark$

$(ii) \Rightarrow (i)$ Die Abbildung $I \to aI, \quad x \mapsto ax$ ist ein Isomorphismus von $\mathcal{A}$-Moduln. Da aI ein Ideal von $\mathcal{A}$ ist, ist aI (und damit auch I) endlich erzeugt als $\mathcal{A}$-Modul, da $\mathcal{A}$ noethersch ist.

□

Lemma 6.7. *Sind* I, J *gebrochene Ideale von einem noetherschen Ring* $\mathcal{A}$*. Dann sind auch*

- $I + J = \{x + y : x \in I, y \in J\}$
- $I \cdot J = \{$*der von allen* xy *erzeugte Untermodul von* $\mathbb{K}\}$
- $I : J = \{a \in \mathbb{K} : aJ \subseteq I\}$

gebrochene Ideale von $\mathcal{A}$*. Insbesondere* $I^* := (\mathcal{A} : I)$ *mit* $I^* = \{a \in \mathbb{K} : aI \subseteq \mathcal{A}\}$*.*

Beweis. Sei I von $x_1, ..., x_n$ erzeugt und J von $y_1, ..., y_m$. Dann sind $I + J$ bzw. $I \cdot J$ von $x_1 + y_1, ..., x_1 + y_m, ..., x_n + y_m$ bzw. $x_1y_1, ..., x_1y_m, ..., x_ny_m$ erzeugt.

"$(I : J)$": $aI \subseteq \mathcal{A}, b \in J$ für alle $a, b \in \mathbb{K}^\times$. Dann ist für alle $x \in (I : J)$: $xJ \subseteq I \implies axJ \subseteq aI\,\mathcal{A}$. Dann gilt $abx \in \mathcal{A}$, da $b \in J \implies ab(I : J) \subseteq \mathcal{A}$. □

Bemerkung 6.8. Sein $a, b \in \mathcal{A} \setminus \{0\}$ und $I = (a), J = (b)$. Dann $I \cdot J = (ab), (I : J)$ ist der $\mathcal{A}$-Untermodul von $\mathbb{K}$, welcher von a/b erzeugt wird.

Nun sei $J_\mathcal{A}$ die Menge der gebrochenen Ideale von $\mathcal{A}$. Durch das Idealprodukt $I \cdot J$ wird $J_\mathcal{A}$ zum kommutativen Monoid mit neutralem Element $(1) = \mathcal{A}$.

Satz 6.9. *Sei* $\mathcal{A}$ *ein Dedekindring . Jedes Ideal* $(0) \neq I$ *von* $\mathcal{A}$ *ist ein Produkt von Primidealen:* $I = \mathfrak{P}_1 \cdot ... \cdot \mathfrak{P}_r, \mathfrak{P}_i \subseteq \mathcal{A}$*. Die Darstellung ist eindeutig bis auf die Reihenfolge.*

Lemma 6.10. *Sei* $\mathcal{A}$ *ein Dedekindring ,* $(0) \neq I \subseteq \mathcal{A}$ *ein Ideal. Es gibt Primideale, sodass* $0 \neq \mathfrak{P}_1 \cdot ... \cdot \mathfrak{P}_r \subseteq I$*.*

Beweis. Sei $M := \{$ die Menge aller Ideale von $\mathcal{A}$, wo die Aussage nicht stimmt $\}$

Angenommen $\emptyset \neq M$. Jede aufsteigende Kette in M wird stationär, da $\mathcal{A}$ noethersch ist. Nach dem Lemma von Zorn existiert ein maximales Element von $J \in M$. J ist kein Primideal, da $J \in M$ liegt. Deswegen gibt es $a, b \in \mathcal{A}$, sodass $ab \in J$, aber $a, b \notin J$. Setze

$$J_1 := (a) + J \quad \text{sowie} \quad J_2 := (b) + J$$

Es gilt stets $J \subsetneq J_1, J_2 \implies J_1, J_2 \notin M$, sonst wäre J kein maximales Element. Also existieren $\mathfrak{P}_1, ..., \mathfrak{P}_r$ und $\mathfrak{P}'_1, ..., \mathfrak{P}'_s$, sodass $\mathfrak{P}_1 \cdot ... \cdot \mathfrak{P}_r \subseteq J_1$ und $\mathfrak{P}'_1 \cdot ... \cdot \mathfrak{P}'_s \subseteq J_2$. Daraus folgt, dass $\mathfrak{P}_1 \cdot ... \cdot \mathfrak{P}_r \cdot \mathfrak{P}'_1 \cdot ... \cdot \mathfrak{P}'_s \subseteq J_1 J_2$. Aber es gilt: $J_1 J_2 \subseteq J$, weil jedes Element aus $J_1 J_2$ folgende Gestalt besitzt: $(ax + y)(bx' + y') = abxx' + axy' + bx'y + yy' \in J \rightsquigarrow$ **Widerspruch** $\square$

Lemma 6.11. *Sei $\mathcal{A}$ ein Dedekindring und $0 \neq \mathfrak{P} \subseteq \mathcal{A}$ ein Primideal. Für jedes Ideal $(0) \neq I \subsetneq \mathcal{A}$ ist $\mathfrak{P}^* I \neq I$*

Beweis. Zuerst zeigen wir: $\mathcal{A} \subsetneq \mathfrak{P}^*$. Klar ist, dass $\mathcal{A} \subseteq \mathfrak{P}^*$. Sei also $0 \neq a \in \mathfrak{P}$ und $\mathfrak{P}_1 \cdot ... \cdot \mathfrak{P}_r \subseteq (a)$ mit $0 \neq \mathfrak{P}_1, ..., \mathfrak{P}_r$ Primideale und r minimal. Dann ist $\mathfrak{P}_i \subseteq \mathfrak{P}$ für ein i. **In der Tat:** gäbe es ein $a_i \in \mathfrak{P}_i \setminus \mathfrak{P}$ für alle i, so wäre $a_1 \cdot ... \cdot a_r \in \mathfrak{P} \rightsquigarrow$ **Widerspruch** zu $\mathfrak{P}$ Primideal.

OBdA: $\mathfrak{P}_1 \subseteq \mathfrak{P} \implies \mathfrak{P}_1 = \mathfrak{P}$, da $\mathcal{A}$ ein Dedekindring . Wegen $\mathfrak{P}_2 \cdot ... \cdot \mathfrak{P}_r \subsetneq (a)$ (r minimal) existiert es ein $b \in \mathfrak{P}_2 \cdot ... \cdot \mathfrak{P}_r$ mit $a^{-1}b \notin \mathcal{A}$. Andererseits ist $b\mathfrak{P} \subseteq (a)$, also $a^{-1}b\mathfrak{P} \subseteq \mathcal{A}$. Damit folgt $a^{-1}b \in \mathfrak{P}^* \setminus \mathcal{A}$. $\square$