Algebra SS16

Prof Wedhorn, Mitschrift von Daniel Kallendorf

25. Januar 2017

Inhaltsverzeichnis

1 Erinnerung: Ringe und Ideale

1A Ideale, Primideal, maximale Ideale und Ring-Homomorphismen

Definition 1.-9. Man nennt $(A, +, \cdot)$ einen **Ring**(in dieser VL=kommutativer Ring), wenn

1. $(A, +)$ abelsch
2. Es gibt ein neutrales Element der Multiplikation $1 \in A : 1a = a \forall a \in A$
3. Die Multiplikation ist $\cdot$ assoziativ und kommutativ
4. Distributivität

Definition 1.-8. Seien A, B Ringe. Eine Abbildung $\varphi : A \to B$ heißt **Ringhomomorphismus**, falls

1. $\varphi(a + a') = \varphi(a) + \varphi(a')$ für alle $a, a' \in A$
2. $\varphi(aa') = \varphi(a)\varphi(a')$ für alle $a, a' \in A$
3. $\varphi(1) = 1$

Definition 1.-7. Ein A-Modul mit A-bilinearer, kommutativer und assoziativer Multiplikation und neutralem Element heißt **A-Algebra**

Korollar 1.-6. *B ist $A-$Algebra genau dann wenn $\varphi : A \to B$ ein Ringhomomporhismus ist.*

Definition 1.-5. Man nennt $\mathfrak{a} \subseteq A$ **Ideal**, falls

1. $\mathfrak{a} \subseteq (A, +)$ Untergruppe
2. $a \in A, b \in \mathfrak{a} \Rightarrow ab \in \mathfrak{a}$.

Sei $S \subseteq A$, dann ist

$$AS = SA = (S) := \left\{ \sum_{i=1}^{n} a_i S_i \mid n \in \mathbb{N}_0, a_i \in A, s \in S \right\}$$

das **Kleinste Ideal** von A das S enthält.

Korollar 1.-4. *Sei $\mathfrak{a} \subseteq A$. Es gilt $1 \in \mathfrak{a}$ genau dann wenn $\mathfrak{A}$.*

Definition 1.-3. Sei A Ring. A heißt **nullteilerfrei**, falls $A \neq \{0\}$ und für $a, b \in A$ mit $a, b \neq 0$ auch $ab \neq 0$ gilt.

Beispiel 1.-2.

- Körper sind Nullteilerfrei
- $\mathbb{Z}$ ist Nullteilerfrei
- $\mathbb{Z}$ ist HIR

Definition 1.-1. Sei A Ring. A heißt **Hauptidealring**(HIR), falls A nullteilrefrei ist und jeds Ideal $\mathfrak{a} \subset A$ von einem Element erzeugt wird.
(d.h. $\mathfrak{a} = As = \{as \mid a \in A\}$ für ein $s \in A$)

Beispiel 1.0.

Körper sind Hauptidealringe (Ideale in einem Körper K sind nur $(0) = \{0\}$ und $(1) = K$)

$\mathbb{Z}, K[X]$ sind HIR

$Z[X]$ ist nicht HIR (p, X) ist für $p \in$ Prim nicht von einem Ideal erzeugt.

Erinnerung 1.1. Sei $\varphi : A \to B$ ein Homomorphismus von Ringen

1. $\varphi(A) \subset B$ ist Unterring.
   $(0, 1 \in \varphi(A),\ a, a' \in \varphi(A) \Rightarrow a + a', aa' \in \varphi(A))$
   $\mathrm{Ker}(\varphi) = \{a \in A \mid \varphi(A) = 0\} \subseteq A$ ist Ideal
   $A/\mathrm{Ker}(\varphi) \xrightarrow{\sim} \varphi(A), \overline{a} \mapsto \varphi(a)$ ist ein Ring Homomorphismus.
2. Sei $\mathfrak{b} \in B$ Ideal, dann $\varphi^{-1}(\mathfrak{b}) = \{y \in A \mid \varphi(a) \in b\} \subseteq A$ Ideal und φ induziert einene injektiven Ring-Homomorphismus:

   $$\overline{\varphi} : A/\varphi^{-1}(\mathfrak{b}) \leftrightarrow B/\mathfrak{b}, \quad \overline{a} \mapsto \varphi(a)$$

   (wende 1) an auf $A \to B \to B/\mathfrak{b}$)
   Falls φ surjektiv ist, ist φ ein Ring-Homomorphismus.

3. Sei φ surjektiv. Dann sind die Abbildungen

$$\{\mathfrak{a} \subseteq A \text{ Ideal mit } \mathrm{Ker}(\varphi) \subseteq \mathfrak{a}\} \leftrightarrow \{\mathfrak{b} \in B \text{ Ideal}\}$$
$$\varphi^{-1(a)} \leftrightarrow \mathfrak{b}$$
$$\mathfrak{a} \leftrightarrow \varphi(a)$$

zueinander Inverse Bijketionen.

Definition 1.2. Sei A Ring

1. Das Ideal $\mathfrak{p} \subseteq A$ heißt **Primideal** falls A/g Nullteilerfrei ist. (Äquivalent: $\mathfrak{p} \subsetneq A$ und für alle $a, b \notin \mathfrak{p}$ gilt $ab \notin \mathfrak{p}$)

2. Das Ideal $m \subseteq A$ heißt **maximales Ideal**, falls A/m ein Körper ist. (Äquivalent: Es gibt kein Ideal $\mathfrak{a}$, sodass $m \subsetneqq \mathfrak{m} \subsetneqq A$).

Jedes Maximale Ideal ist Primideal.

Satz 1.3. *Sei A Ring, $\mathfrak{a} \subsetneqq A$ Ideal.*
Dann existiert ein maximales Ideal $m \subset A$ mit $\mathfrak{a} \subseteq m$.

Beweis. Sei $(I, \leq) = (\{\mathfrak{b} \subsetneqq A \text{ Ideal} \mid \mathfrak{a} \subseteq b\}, \leq)$
Zu zeigen: $(I, \leq)$ besitzt maximale Elemente:

- $\mathfrak{a} \in I \Rightarrow I \neq \emptyset$ erfüllt.

- Sei $S \subseteq I$ total geordnet und sei $\mathfrak{a}_0 = \bigcup_{\mathfrak{b} \in S} \mathfrak{b} \subseteq A$.
Seien $x, y \in \mathfrak{a}_0$, also existieren $\mathfrak{b}, \mathfrak{b}' \in S$, sodass $x \in \mathfrak{b}, y \in \mathfrak{b}'$.
Sei O.E. $\mathfrak{b} \subseteq \mathfrak{b}'$, dann gilt, da S total geordnet ist, dass $x + y\mathfrak{b} \leq \mathfrak{a}_0$.
Es gilt $\mathfrak{a}_0 \neq A$: Angenommen $\mathfrak{a}_0 = A$, dann $1 \in \mathfrak{a}_0$, dann gibt es $b \in S$ mit $1 \in \mathfrak{b}$. dann folgt $b = A$.
Dann folgt mit 1.4, dass es ein maximales Elemente gibt, also maximale Ideal die $\mathfrak{a}_0$ enthalten.

□

Lemma 1.4 (Lemma von Zorn)**.** *Sei $(I, \leq)$ eine partielle geordnete Menge.*
Für jede total geordnete Teilmenge $S \subseteq I$ eine obere Schranke (d.h. $\exists i \in I$ mit $s \leq i \forall s \in S$).
Dann beseitzt $(I, \leq)$ maximale Elemente (d.h. Elemente, sodass für Elemente $i \in I$ gilt, dass $i_0 \leq i, i \neq i_0$).

Beispiel 1.5. Sei A ein Hauptidealring, sei $\mathfrak{a} \subseteq A$ Ideal mit $\mathfrak{a} = (a)$f+r $a \in A$.

1. $\mathfrak{a}$ ist genau dann Primideal, wenn a irrduzibel (d.h. $a \neq 0, a \notin A^\times$ und $a = bc$ für $b, c \in A$, dann muss $b \in A^\times$ oder $c \in A^\times$) oder $a = 0$.

2. Sei $\mathfrak{a}$, dann ist a irreduzibel oder A ist Körper und $a = 0$.

Beispiel 1.6. Sei A ein Ring. Dann ist A genau dann ein Körper, wenn $\{0\} \subseteq A$ maximal ist.

Bemerkung 1.7. Sei $\varphi : A \to B$ ein Ring-Homomorphimsmus

1. Sei $q \subseteq B$ Primideal, dann ist $\varphi^{-1}(q) \subset A$ ein Primideal.

Beweis 1. Wir wissen, dass φ einen injektiven Ring-Homomorphimsmus $A/\varphi^{-1} \to B/q$ induziert.
Da B/q nullteilerfrei ist, folgt, dass $A/\varphi^{-1}(q)$ nullteilerfrei ist. Dann folgt, dass $\varphi^{-1}(q)$ Primideal ist. □

Beweis 2. InhaltEs gilt $1 \notin \varphi^{-1}(q)$. Sei nun $x, y \in A$ mit $x, y \in \varphi^{-1}(q)$, also $\varphi(x), \varphi(y) \notin q$.
Dann folgt, da q Primideal ist, dass $\varphi(xy) = \varphi(x)\varphi(y) \notin q$, also auch $xy \notin \varphi^{-1}(q)$. □

2. Sei φ surjektiv, dann ist $A/\varphi^{-1}(q)\tilde{=}B/q$. Also ist
   (a) q genau dann Primideal, wenn $\varphi^{-1}(q)$ Primideal ist.
   (b) q genau dann maximales Ideal, wenn $\varphi^{-1}(q)$ maximales Ideal ist.
   (c) Es gibt zueinander Inverse Bijektionen:

$$\left\{\begin{matrix}\mathfrak{a}\subseteq A \text{ Primideal/maximales Ideal} \\ \text{mit } \operatorname{Ker}(\varphi) = \mathfrak{a}\end{matrix}\right\} \overset{1:1}{\leftrightarrow} \left\{\begin{matrix}\text{Primideal/maximales Ideal} \\ q\subset B\end{matrix}\right\}$$

$$\mathfrak{p} \mapsto \varphi(\mathfrak{p})$$

$$q \leftarrow\!\shortmid \varphi^{-1}(q)$$

1B Operationen mit Idealen

Sei im folgende A ein Ring.

Definition 1.8. 1. Seien $\mathfrak{a}, \mathfrak{b} \subseteq A$ Ideale.
Dann ist die **Summe von Idealen**

$$\mathfrak{a} + \mathfrak{b} := (\mathfrak{a} \cup \mathfrak{b})\{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

Allgemein für eine Familie von Idealen $(\mathfrak{a}_i)_{i\in I}$

$$\sum_{i\in I} := \left(\bigcup_{i\in I} \mathfrak{a}_i\right)$$

Bzw. das Kleinste Ideal $\mathfrak{b}$ mit $\mathfrak{a}_i \subseteq \mathfrak{b}$ für alle $i \in I$.

2. Sei $(\mathfrak{a}_i)_{i\in I}$ eine Familie von Idealen. Dann ist der **Schnitt von Idealen**

$$\bigcap_{i\in I} \mathfrak{a}_i \subseteq A$$

auch ein Ideal.

3. Sei $\mathfrak{a}, \mathfrak{b} \subseteq A$ Ideale.
Dann ist das **Produkt von Idealen**

$$\mathfrak{a} \cdot \mathfrak{b} := (\{a \cdot b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}) = \left\{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}$$

Es folgt, dass

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$$

Beispiel 1.9. Sei A ein Hauptidealring, $a, b \in A$ und $a, b \neq 0$.
Dann ist $a = up_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ und $b = vp_1^{l_1} p_2^{l_2} ... p_r^{l_r}$ für $u, v \in A^\times$, $p_i \in A$ irreduzibel, $(p_i) \neq p_l$ für $i \neq l$ und $k_i, l_i \in \mathbb{N}_0$.

1. $(b) + (b) = \left(p_1^{\min(k_1,l_1)} ... p_r^{\min(k_r,l_r)}\right)$
   (Ähnlich dem ggT)

2. $(a) \cap (b) = p_i^{\max k_1, l_1} ... p_r^{\max(k_r l_r)}$
   (Ähnlich dem kgV)

3. $(b)(b) = (ab)$ in jedem Ring.

Theorem 1.10 (Chinesischer Restsatz)**.** *Seien* $\mathfrak{a}_1, ... \mathfrak{a}_n \subseteq A$ *Ideale, sodass* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *für* $i \neq j$*. Dann gilt*

1.

$$\bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i$$

2.

$$A/\bigcap_{i=1}^n \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^n A/\mathfrak{a}_i$$
$$\overline{a} \mapsto (a \mod \mathfrak{a}_1, ..., a \mod \mathfrak{a}_n)$$

Proposition 1.11. Sei $\mathfrak{p} \subset A$ Primideal mit $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$ für Ideale $\mathfrak{a}_i, ..., \mathfrak{a}_n \subseteq A$.
Dann ist $\mathfrak{a}_j \subseteq p$ für ein j.

Beweis. Angenommen für alle $j = 1, ..., n$ exitsiert $x_j \in \mathfrak{a}$, sodass $x_j \notin y$. Dann ist $x_1 x_2 ... x_n \in \mathfrak{a}_1 \cap ... \cap \mathfrak{a}_n$.
Da aber $a_1 x_2 ... x_n \notin \mathfrak{p}$ da $\mathfrak{p}$ Primideal. Widerspruch! □

Proposition 1.11. Sei $\mathfrak{a}$ ein Ideal, $\mathfrak{p}_1, ..., \mathfrak{p}_n$ Primideale.
Es gelte $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ für alle i.
Dann gilt

$$\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$$

(= kein Ideal)

Beweis. Induktion nach n:

- $n = 1$ erfüllt.
- Sei $n > 0$.
  Induktionsvoraussetzung für $n-1$: Für alle $i \in \{1, ..., n\}$ existiere $x_i \in \mathfrak{a}_i$, sodass $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$

- Entweder es existiert ein i, sodass $x_i\mathfrak{p}_i$,
  oder für i gilt $x_i \notin \mathfrak{p}_i$.
  Definiere $y \in \mathfrak{a}$ mit

  $$y := \sum_{i=1}^{n} x_1 x_2 ... x_{i-1} x_{i+1} ... x_n$$

  dann $x \notin \mathfrak{p}_i$ für alle $i = 1, ..., n$.

□

1C Radikal und Jakobson-Radikal

Sei A weiterhin ein Ring

Definition 1.12.
1. $x \in A$ heißt **nilpotent**, falls es ein $n \in \mathbb{N}$ gibt, sodass $x^n = 0$
2. A heißt **reduziert**, wenn er keine nilpotenten Elemente außer 0 enthält.

Beispiel.
1. $\overline{2} \in \mathbb{Z}/8\mathbb{Z}$ ist nilpotent.
2. nullteilerfreie Ringe sind reduziert.
   Aber: $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist reduziert aber nicht nullteilerfrei

Definition 1.13. Sei $\mathfrak{a} \subseteq A$ Ideal. Dann heißt das Ideal

$$\mathrm{rad}(\mathfrak{a}) := \sqrt{\mathfrak{a}} := \{x \in A | \exists n \in \mathbb{N}_0 : x^n \in \mathfrak{a}\}$$

das **Radikal** von $\mathfrak{a}$.

Bemerkung 1.14. Sei $\mathfrak{a} \subseteq A$ ein Ideal

1. $\mathfrak{a} \subseteq \mathrm{rad}(\mathfrak{a})$
2. $\mathfrak{a} = \mathrm{rad}(\mathfrak{a})$ genau dann wenn $A/\mathfrak{a}$ reduziert ist

Beweis. Es gilt $\mathfrak{a} = \mathrm{rad}\,\mathfrak{a}$
genau dann wenn für alle $a \in A$ gilt $0^n \in \mathfrak{a}$ für ein $n \in \mathbb{N}$. Es folgt $a \in \mathfrak{a}$.
Genau dann wenn für alle $a \in A$ gilt $\overline{a}^n := (a \mod \mathfrak{a})^n = 0$ für ein n. Es folgt $\overline{a} = 0$.
Ist also äquivalent dazu, dass $A/\mathfrak{a}$ reduziert ist. □

Satz 1.15. *Sei $\mathfrak{a} \subseteq A$ Ideal. Dann gilt*

$$\mathrm{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{g} \subset A Primideal \\ \mathfrak{a} \subseteq \mathfrak{g}}} \mathfrak{g}$$

Beweis. Wir zeigen durch beidseitige Inklusion

- $\subseteq$ Sei $x \in A$ nilpotent. Dann gibt es ein $n \in \mathbb{N}$, sodass $x^n = 0 \in g$ für alle Primideale g
  Dann liegt auch $x \in g$ für alle Primideale g.
- $\supseteq$ Sei $x \in A$ nicht nilpotent

1. Zz: Es gibt ein Primideal $\mathfrak{g} \subset A$, sodass $x \notin \mathfrak{g}$.
   ???...

$\square$

Definition 1.16. $\mathrm{Nil}(A) := \mathrm{rad}(\{0\}) = \{x \in A | x \text{ ist nilpotent}\}$ heißt das **Nilradikal** von A.
Mit 1.15 folgt die äquivalente Definition

$$\mathrm{Nil}(A) = \bigcap_{\substack{\mathfrak{g} \subset A \\ \mathfrak{g} \text{ Primideal}}} \mathfrak{g}$$

Definition 1.17. Das **Jacobson-Radikal** von A ist definiert als

$$\mathrm{Jac}(A) := \bigcap_{\substack{m \in A \\ m \text{ maximales Ideal}}}$$

Beispiel. 1. $\mathrm{Jac}(\mathbb{Z}) = \{0\} = \mathrm{Nil}(\mathbb{Z})$

2. $\mathrm{Jac}(\mathbb{Z}/8\mathbb{Z}) = 2\mathbb{Z}/8\mathbb{Z}$

Proposition 1.18. $\mathrm{Jac}(A) = \{x \in A \mid 1 - xy \in A^\times \forall y \in A\}$

Beweis. Sei $x \in A$, sodass $y \in A$ existiert mit $1 - xy \notin A^\times$ und sei $m \subset A$ maximal, sodass $1 - xy \in m$.
Wäre nun $x \in \mathrm{Jac}(a) \subseteq m$, dann $1 = 1 - xy + xy \in m$. Widerspruch!
Sei also $x \notin \mathrm{Jac}(a)$, d.h. es existiert $m \subset A$ mit $x \notin m$.
Dann ist $m + (x) = A$, d.h. es gibt eine Zerlegung der Eins $1 = z + yx$.
Es folgt, dass es ein $y \in A$ gibt, sodass $1 - xy \in m$ und damit $1 - xy \notin A^\times$. $\square$

2 Polynomringe

Definition 2.1. Sei $A^{(\mathbb{N}_0)} := \{(a_n)_{n \in \mathbb{N}_0} \mid a_n \in A, \text{ fast alle } a_n = 0\}$.
Addition und Multiplikation:

$$(a_n) + (b_n) := (a_n + b_n)$$
$$(a_n) \cdot (b_n) := \sum_{k=0}^{n} a_k b_{n-k}$$

Sei nun $X = (0, 1, 0, ...)$. Dann is nur der n-te Eintrag von $X^n = 1$.
Dann gilt

$$(a_n)_n = \sum_{n=0}^{\infty} a_n X^n$$

Wir erhalten einen Kommutativen Ring und bezeichnen $A[X]$ als den **Polynomring** über A in der Unbestimmten X.
Mit der Abbildung $A \to A[X], a \mapsto a + 0X + 0X^2 + ...$ erhält man eine A-Algebra.

Definition 2.2. Sei $f = a_n X^n + ... + a_1 X + a_0 \in A[X]$

1. $\deg(f) := \sup\{d \in \mathbb{N} | a_d \neq 0\}$ heißt der **Grad** von f (Es folgt $\deg(0) = -\infty$)

2. f heißt **normiert**, falls $f = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$.

3. a_0 heißt **absoluter Koeffizient** von f.

Bemerkung 2.3. Seien $f, g \in A[X]$

1. $\deg(f + g) \leq \max(\deg(f), \deg(g))$

2. $\deg(fg) \leq \deg(f) + \deg(g)$
(Da Ringe Nullteiler haben können. Gleichheit bei nullteilerfreien Ringen)

3. A ist genau dann nullteilerfrei wenn $A[X]$ nullteilerfrei ist.

Satz 2.4 (Division mit Rest)**.** *Sei* $g = a_d X^d + ... + a_0 \in A[X]$ *mit* $a_d \in A^\times$. *Dann existieren für alle Polynome* $f \in A[X]$ *eindeutige* $q, r \in A[X]$*, sodass* $f = qg + r$ *mit* $\deg(r) < \deg(g) = d$

Beweis.

1. Da $a_d \in A^\times$ ist gilt $\deg(gs) = \deg(g) + \deg(s)$

2. Eindeutigkeit: Sei $f = qg + r = q'g + r'$ mit $\deg(r), \deg(r') < d$.
Dann folgt, dass $0 = (q - q')g + (r - r')$. Und da $\deg(r - r') < d$ muss $q = q'$ und $r = r'$.

3. Existenz: Induktion nach $\deg(f)$.

   IA Sei $\deg(f) < d$, dann $f = 0g + r$ und $r = f$.

   IV Für Polynome $f \in A[X]$ mit $\deg(f) \leq n$ sind r, q eindeutig bestimmt.

   IS Sei $\deg(f) \geq d$ ...

$\square$

Definition 2.5. Definiere rekursiv $A[X_1, ..., X_N] := (A[X_1, ..., x_{n-1}])[X_n]$. Also

$$A[X_1, ..., X_n] := \left\{ \sum_{k_1, ..., k_n} a_{k_1, ..., k_n} X_1^{k_1} \cdot ... \cdot X_n^{k_n} | a \in A \right\}$$

Elemente der Form $X_1^{k_1} \cdot ... \cdot X_n^{k_n}$ heißen **Monome**.

Bemerkung 2.6. $A[X_1, ..., X_n]$ ist ein freier Modul. Die Monome bilden eine Basis.

Satz 2.7 (Universaleigenschaft des Polynomrings)**.** *Sei* $\phi : A \to B$ *eine* A*-Algebra und seine* $b_1, ..., b_n \in B$ *Elemente. Dann existiert genau ein* A*-Algebra-Homomorphismus* $\psi : A[X_1, ..., X_n] \to B$*, so dass* $\psi(x_i) = b_i$ *für alle* $i = 1, .., n$*, nämlich*

$$\underbrace{\psi \left(\sum_{i_1, ..., i_n \geq 0} a_{i_1, ..., i_n} X_1^{i_1} \cdot ... \cdot X_n^{i_1} \right)}_{=:f} = \underbrace{\sum_{i_1, ..., i_n \geq 0} \phi(a_{i_1, ..., i_n}) b_1^{i_1} \cdot ... \cdot b_n^{i_n}}_{=f(b_1, ..., b_n)}$$

Bemerkung 2.8.

$$\begin{aligned}\mathrm{Im}(\psi) &= \text{kleinste } A\text{-Unteralgebra die } b_1, ..., b_n \text{ enthält} \\ &= A[b_1, ..., b_n] \subset B\end{aligned}$$

Beispiel 2.9. Sei $\phi : A \to B$ eien A-Algebra, $b \in B$. Es existiere ein $g \in A[X]$ mit $g(b) = 0$. Sei g nomriert. Dann gilt

$$A[b] = \{f(b)|f \in A[x], \deg(f) < \deg(g)\}$$

Beispiel 2.10. Sei $A = \mathbb{Q} \hookrightarrow \mathbb{C}$,$i \in \mathbb{C}$.
Dann gilt $g(i) = 0$ wobei $g = X^3 + X = X(X^2 + 1)$. Es folgt:

$$\mathbb{Q}[i] = \{a_0 + q_1 i + a_2 i^2 | a_0, a_1, a_2 \in \mathbb{Q}\}$$
$$\mathbb{Q}[i] = \mathrm{Im}(\mathbb{Q}[X] \xrightarrow[X \mapsto i, f \mapsto f(i)]{\psi} \mathbb{C})$$

Dann $\tilde{g} \in \mathbb{Q}[X] : \psi(\tilde{g}) = 0 \Leftrightarrow \tilde{g}(i) = 0$.
Also $g \in \mathrm{Ker}(\psi) \Rightarrow (g) \subseteq \mathrm{Ker}(\psi)$.
In diesem Fall $\mathrm{Ker}\,\psi = (X^2 + 1)$.

Begründung von 2.8:

$$(g) \subseteq \mathrm{Ker}\left(A[X] \xrightarrow[f \mapsto f(b)]{\psi} B\right)$$

Also ψ faktorisiert:

$$A[X]/(g) \xrightarrow{\overline{\psi}} A[b] \subseteq B$$

mit $\overline{\psi}$ surjektiv.

Proposition 2.11. Sei $g \in A[X]$ normiert. Dann ist

$$\{f \in A[X], \deg(f) < \deg(g)\} \hookrightarrow A[X] \to A[X]/(g)$$

bijektiv.

Beweis. Gilt, da für alle $f \in A[X]$ genau ein $r \in A[X]$ exitiert mit $\deg(r) < \deg(g)$ mit $f \in r + (g)$ $\square$

3 Tensorprodukte

(A) Tensorprodukte von Moduln
(B) Tensorprodukte von Algebren und Basiswechsel
(C) Exaktheitseigenschaften des Tensorprodukts

3A Erinnerung

Definition 3.1. Ein A-Modul ist ein Tripel $(M, +, \cdot)$ wobei $(M, +)$ abelsche Gruppe und $\cdot : A \times X \to M$ eine Skalare Multiplikation ist.

Bemerkung. Ein $\mathbb{Z}$-Modul entspricht einer ableschen Gruppe.

Beispiel. Sei I eine Menge

$$A^{(I)} = \{(a_i)_{i \in I} | a_i \in A, a_i = 0 \text{für fast alle } i \in I\}$$

A-Modul mit Addition und Skalarprodukt.
Für $i \in I : e_i \in A^{(I)}$ mit

$$e_i = \begin{cases} 1 \text{ an der i-ten Stelle} \\ 0 \text{ sonst} \end{cases}$$

Definition 3.2. Ein A-Modul heißt **frei**, falls $M \approxeq A^{(I)}$ für eine Menge I

Definition 3.3. Sei M, N A-Modul. Dann heißt $u : M \to N$ A-**linear** oder **Homomorphismus von A-Moduln**, falls

$$u(am + m') = au(m) + u(m') \forall a \in A, m, m' \in M$$

Bemerkung. Sei I eine Menge, M ein A-Modul $\underline{m} = (m_i)_{i \in I}$ ein Tupel von Elementen $m_i \in M$. Dann Existiert genau eine Abbildung:

$$A^{(I)} \xrightarrow{u_{\underline{m}}} M$$

mit $u_{\underline{m}}(e_i) = m_i$.
$(m_i)_i = \underline{m}$ heißt linear Unabhängig/ Erzeugende-System/ Basis,
falls $u_{\underline{m}}$ injektiv/ surjektiv / bijektiv ist.

Bemerkung. Der A-Modul M ist endlich erzeugt, genau dann wenn ein $n \in \mathbb{N}$und eine A-lineare Surjektion $A^n \to M$ existieren.

Definition 3.4. Sei $r \in \mathbb{N}_0$, $M_1, ..., M_r, P$ A-Moduln.
Eine Abbildung $\alpha : M_1 \times ... \times M_r \to P$ heißt r-**multilinear**, falls sie in jeder Komponente linear ist, d.h. Für alle $i = 1, ..., r$ gilt:

$$\alpha(m_1, ..., am_i + m'_i, m_{i+1}, ..., m_r) = a\alpha(m_1, ..., m_i, ..., m_r) + \alpha(m_1, ..., m'_i, ..., m_r)$$

Für alle $m_j \in M_j, m_i \in M_i, a \in A$.
(Insbesondere heißen $r = 1$: linear, $r = 2$: bilinear)

Wir definieren

$$L_a(M_1, ..., M_r, P) := \{\alpha : M_1 \times ... \times M_r \to P \mid \alpha \text{ ist } r\text{-multlinear}\}$$

Satz 3.3. *Sei $r \geq 2$, $M_1, .., M_r$ A-Moduln.*
Dann existiert ein A-Modul $M_1 \otimes_A M_2 \otimes_A ... \otimes_A M_r$ und eine r-multilineare Abbildung $\tau : M_1 \times ... \times M_r \to M_1 \otimes_A M_2 \otimes_A ... \otimes_A M_r$, sodass für jede r-multilineaer Abbildung:

$$\alpha M_1 \times ... \times M_r \to P$$

wobei P ein A-Modul, genau ein A-lineare Abbildung

$$\overline{\alpha} : M_1 \otimes_A ... \otimes_A M_r \to P$$

existiert.

$$\begin{tikzcd} M_1 \times ... \times M_r \arrow[r, "\forall\alpha: r\text{-}multilinear"] \arrow[d, "\tau"] & P \\ M_1 \otimes_A M_2 \otimes_A ... \otimes_A M_r \arrow[ur, dashed, "\exists!\overline{\alpha}"] & \end{tikzcd}$$

Definition 3.3. Der A-Modul $M_1 \otimes_A M_2 \otimes_A ... \otimes_A M_r$ heißt das **Tensorprodukt** von $M_1, ..., M_r$.

Beweis. • Eindeutigkeit des Tensorprodukts

Seien $(T, \tau : M_1 \times ... \times M_r \to T)$ und (T', τ') Tensorprodukte:

$$\begin{tikzcd} & M_1 \times ... \times M_r \arrow[dl, "\tau"'] \arrow[dr, "\tau'"] & \\ T \arrow[rr, dashed, "\exists! u"'] & & T' \arrow[ll, dashed, "\exists! v"'] \end{tikzcd}$$

u existiert aufgrund der universellen Eigenschaft von (T, τ).
v existiert aufgrund der universellen Eigenschaft von (T', τ').

Die Universelle Eigschaft von (T, τ) zeigt, dass $v \circ u = \mathrm{id}_T$, genauso $u \circ v = \mathrm{id}_T$.

- Existenz des Tensorprodukts

1. Suche einen A-Modul N und eine Abbildung $c : M_1 \times ... \times M_r \to R$, sodass
$$\mathrm{Hom}_A(N, P) \xrightarrow[u \mapsto u \circ \tau]{} \mathrm{Abb}(M_1 \times ... \times M_r, P)$$
Für alle A-Moduln P. Wähle also $N := A^{(M_1 \times ... \times M_r)}$ und $l : M_1 \times ... \times M_r \to N, i \mapsto e_i$.
2. Wir wollen, dass $(am_1 + m_1', m_2, ..., m_r)$ und $a(m_1, ..., m_r) + (m_1', ..., m_r)$ auf das gleiche Element abgebildet werden.
Sei $Q \subseteq N$ der von
$$e_{(m_1,...,m_{i-1},am_i+m_i',m_{i+1},...,m_r)} - \left(ae_{(m_1,...,m_i,..,m_r)} + e_{(m_1,...,m_i',...,m_r)}\right)$$
für alle $i = 1, ..., r$ und $m_i, m_i' \in M_i$ und $a \in A$ erzeugt Untermodul.
Dann setze $T := N/Q$. Dann gilt
$$\begin{aligned} \mathrm{Hom}_A(T, P) &= \{u \in \mathrm{Hom}(N, P) | u(Q) = 0\} \\ &= L_A(M_1, ..., M_r, P) \end{aligned}$$
mit $\tau : M_1 \times ... \times M_r \to N \to N/Q$.

□

Bemerkung 3.4. $e_{(m_1,...,m_r)} \in A^{(M_1 \times ... \times M_r)}$ bilden ein Erzeugndensystem.
Also bilden auch die $\tau(m_1, ..., m_r) =: m_1 \otimes ... \otimes m_r$ eine Erzeugenden-System des $A-$Moduls $M_1 \otimes ... \otimes M_r$.
Aber: Nicht jedes Element von $M_1 \otimes ... \otimes M_r$ ist in dieser Form.

Also genügt es eine lineare Abbildung $u : M_1 \otimes ... \otimes M_r \to P$ auf den erzeugenden $m_1 \otimes ... \otimes m_r$ mit $(m_i \in M_i)$ anzugeben.
Umgekehrt sei P ein A-Modul und es seien Elemente $u(m_1 \otimes ... \otimes m_r) \in P$ gegeben für alle $m_i \in M_i$.
Genau dann existiert eine A-lineare Abbildung $u : M_1 \otimes ... \otimes M_r \to P$ mit

$m_1 \otimes ... \otimes m_r \mapsto u(m_1 \otimes ... \otimes m_r)$, wenn für alle $i = 1, ..., r$, $a \in A$, $m_j \in M_j$ und $m_i' \in M_i$ gilt:

$u(m_1 \otimes .. \otimes am_i + m_i' \otimes .. \otimes m_r) = au(m_1 \otimes .. \otimes m_i \otimes .. \otimes m_r) + u(m_1 \otimes .. \otimes am_i' \otimes .. \otimes m_r)$

Satz 3.5 (Tensorprodukt linearer Abbildungen)**.** *Seien M, M', N, n' A-Moduln, $u : M \to M', v : N \to N'$ A-lineare Abbildungen.*
Dann definiert

$$\begin{aligned} M \otimes_A N &\to M' \otimes AN' \\ m \otimes n &\mapsto u(m) \otimes u(n) \end{aligned}$$

eine A-lineare Abbildung bezüglich $u \otimes v : M \otimes N \to M' \otimes N$.

Beweis. Zu zeigen: $u(am + m') \otimes v(n) = a(u(m) \otimes v(n)) + u(m') \otimes v(n)$
Es gilt da das Tensorprodukt r-linear ist.

$$\begin{aligned} u(am + m') \otimes v(n) &= (au(m) + u(n)) \otimes v(n) \\ &= (au(m) \otimes v(n)) + u(m') \otimes v(n) \end{aligned}$$

Außerdem zu zeigen: $u(m) \otimes v(an + n') = a(u(m) \otimes v(n)) + u(m) \otimes v(n)$
($\to$ Genauso.) □

Bemerkung 3.6. 1. $A \otimes_A M \tilde{=} M$

2. $M \otimes_A N \xrightarrow{\sim} N \otimes_A M, m \otimes n \mapsto n \otimes m$ ist ... von A-Moduln.

3.

$$\begin{aligned} M \otimes_A N \otimes_A P &\xrightarrow{\sim} (M \otimes_A N) \otimes_A P && \xrightarrow{\sim} M \otimes_A (N \otimes_A P) \\ m \otimes n \otimes p &\mapsto (m \otimes n) \otimes p && (m \otimes (n \otimes P)) \end{aligned}$$

Beweis. 1. Sei $u : a \otimes m \mapsto am$,$v : 1 \otimes m \leftarrow\!\shortmid m$

- Z.z. u wohldefiniert, d.h. $(a, m) \to am$ ist bilinear:
  Dann $(ba + a') = bam + a'm$ für alle $a, a', b \in A$ und $m \in M$.
  Analog gilt Linearität in m.
  Daraus folgt, dass u A-linear ist.
- Z.z. v ist wohldefiniert:
  analog zu u.
- Z.z.: $v \circ u = \mathrm{id}_{A \otimes_A M}$:

  $$(v \circ u)(a \times m) = v(am) = 1 \otimes am = a(1 \otimes m) = a \otimes m$$

- Z.z.: $u \circ v = \mathrm{id}_M$:

2. Es gilt zu zeigen

- Z.z. Wohldefiniertheit, also $(m, n) \mapsto n \otimes m$ ist bilinear
- Existenz der Umkehrabbildung $n \otimes m \mapsto m \otimes n$

□

Proposition 3.7. 3.7 Sei $(M_i)_{i\in I}$ eine Familie von A-Moduln, N ein A-Modul:

$$\left(\bigotimes_{i\in I} M_i\right) \otimes_A N \xrightarrow{\sim} \bigotimes_{i\in I} (M_1 \otimes_A N)$$
$$(m_i)_{i\in I} \otimes n \mapsto (m_i \otimes n)_{i\in I}$$

Beweis. Umkehrabbildung gegeben durch:

$$Inhalt..m_i \otimes n \mapsto (m_j)_{j\in I} \otimes n$$

mit $m_j := \begin{cases} m_i, & j = i \\ 0 & j \neq i \end{cases}$ □

3B Basiswechsel von Tensorprodukten

Satz 3.8. *1. Sei M ein A-Modul. Dann wird*

$$\varphi^*(M) := B \otimes_A M$$

zu einerm B-Modul mit dem Skalarprodukt

$$B \times (B \otimes_A M) \to B \otimes_A M$$
$$(b, b' \otimes m) \mapsto bb' \otimes m$$

2. Sei $U : M \to M'$ ein Homomorphismus von A-Moduln. Dann ist

$$id_B \otimes u : B \otimes M \to B \otimes_A M'$$
$$b \otimes m \mapsto b \otimes u(m)$$

eine B-lineare Abbildung.S

Proposition 3.9. Sei $\varphi : A \to B$ eine A-Algebra.
Sei M ein freier A-Modul. Dann ist $B \otimes_A M$ ein freier B-Modul und

$$\vartheta_A(M) = \vartheta_B(B \otimes_A M)$$

Beweis. Sei M ein freier A-Modul. Dazu ist äquivalent, dass $M \simeq A^{(I)}$.
Daraus folgt, dass

$$\begin{aligned} B \otimes_A M &\simeq B \otimes_A A^{(I)} \\ &\simeq B \otimes_A \left(\bigoplus_{i\in I} A\right) \\ &\simeq \left(\bigoplus_{i\in I} B \otimes_A A\right) \\ &\simeq \bigoplus_{i\in I} B \\ &= B^{(I)} \end{aligned}$$

Also ist $B \otimes_A M$ frei. □

Proposition 3.10. Sei $\mathfrak{a} \subseteq A$ ein Ideal, M ein A-Modul.Setze

$$\begin{aligned}\mathfrak{a} \cdot M &= \langle\{am|a \in \mathfrak{a}, m \in M\}\\ &= \left\{\sum_{i=1}^{m} a_i m_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{a}, m_i \in M\right\}\\ &\subseteq M \quad \text{Untermodul}\end{aligned}$$

Dann ist

$$\begin{aligned}A/\mathfrak{a} \otimes_A M &\xrightarrow{\sim} M/\mathfrak{a}M\\ \overline{a} \otimes m &\mapsto \overline{am}\end{aligned}$$

ein Homomorphismus von $A/\mathfrak{a}$-Moduln.

Beweis. $\overline{a} \oplus m \mapsto \overline{am}$ ist wohldefiniert: Zu zeigen:

1. Sei $a' \in A$ mit $\overline{a'} = \overline{a} \in A/\mathfrak{a}$.
   Dann ist $\overline{am} = \overline{a'm} \in M/\mathfrak{a}M$. Es gilt $\overline{a}' = \overline{a}$ gena dann wenn es ein $x\imath\mathfrak{a}$ gibt sodass $a' = a + x$.
   Daruas folgt, dass $a'm = am + xm$, und da $xm \in \mathfrak{a}M$ folgt $\overline{a'm} = \overline{am}$.
2. $\overline{am}$ is linear in a, d.h.
   $$\overline{(ba + a')m} = b\overline{am} + a'\overline{m} \quad \text{für } a, a' \in A,\ b \in A$$
3. $\overline{am}$ ist linear in m, d.h.
   $$\overline{a(bm + m')} = b\overline{am} + \overline{am'} \quad \text{für } m, m' \in M,\ b \in A$$

□

Proposition 3.11. Eine Umkehrabbildung ist gegeben durch

$$\begin{aligned}v : M &\to A/\mathfrak{a} \otimes_A M\\ m &\mapsto 1 \otimes m\end{aligned}$$

Beweis. Zu zeigen: $\mathfrak{a}M \subseteq Ker(v)$, also für alle $x \in \mathfrak{a}, m \in M$ gilt $v(xm) = 0$.

$$v(xm) = 1 \otimes xm = \overline{x} \otimes m = 0$$

da $\overline{x} = \overline{0} \in A/\mathfrak{a}$.
Noch zu zeigen:: v ist Umkehrabbildung zu $\overline{a} \otimes m \mapsto \overline{am}$. □

Definition 3.11 (Tensorprodukte von Algebren)**.** Sei $A \to B_1$, $A \to B_2$ A-Algebren.
Dann definieren wir auf dem A-Modul $B_1 \otimes_A B_2$ eine Multiplikation:

$$\begin{aligned}(B_1 \otimes B_2) \times (B_1 \otimes B_2) &\to B_1 \otimes B_1 \otimes B_2\\ (a_1 \otimes b_2, b_1' \otimes b_2') &\mapsto b_1 b_1' \otimes b_2 b_2'\end{aligned}$$

und erhalten die A-Algebra $B_1 \otimes_A B_2$.

Beispiel 3.12. Sei $\varphi : A \to B$ eine A-Algebra und sei $C = A[X_1, ..., X_n]/(f_1, ..., f_r)$ und $f_i \in A[X-1, ..., X_n]$.Dann ist

$$B \otimes_A A[X-1, ..., X_n]/(f_1, ..., f_r) = B[X_1, ..., X_n]/(\tilde{f}_1, ..., \tilde{d}_r)$$

wobei

$$f_i = \sum_{\underline{j} \in \mathbb{N}_0^n} a_{\underline{j}} X^{\underline{j}} \to \tilde{f}_i = \sum_j \varphi(a_j)$$

Beispiel 3.13.

1. Sei $A = \mathbb{Q}$, $C = \mathbb{Q}[i] = \{a + b_i | a, b \in \mathbb{Q}\} = \mathbb{Q}[X]/(X^2 + 1)$
2. $\mathbb{R} \otimes_Q Q[i] = \mathbb{R}[X]/(X^2 + 1) = \mathbb{C}$
3. $C \otimes_Q Q[i] = C[X]/(X^2 + 1) = \mathbb{C}[X]/(X + i) \times \mathbb{C}[X]/(X - i) \simeq \mathbb{C} \times \mathbb{C}$

Beispiel 3.14. $A[X] \otimes_A A[Y] = (A[X])[Y] = A[X, Y]$ mit $f \otimes g \mapsto fg$.
Dann ist die Umkehrabbildung

$$\sum a_{ij} X^i Y^j \mapsto \sum_{i,j} (a_{ij} X^i \otimes Y^j)$$

C) Exaktheitseigenschaften

Definition 3.11 (Homomorphismen-Funktor)**.** Seien M, P A-Moduln.
Wir Definiere auf $\mathrm{Hom}_A(M, P) := \{u : M \to P \text{A-linear}\}$ die Struktur eines A-Moduls.

$$\begin{aligned} (u + v)(m) &:= u(m) + v(m) && u, v \in \mathrm{Hom}_A(M, P) \\ (au)(m) &:= au(m) && a \in A, m \in M \end{aligned}$$

Sei $u : M \to M'$ eine A-lineare Abbildung. Wir erhalten die A-lineare Abbildung

$$\begin{aligned} \mathrm{Hom}_A(u, P) : \mathrm{Hom}_A(M', P) &\to \mathrm{Hom}_A(M, P) \\ w' &\mapsto w' \cdot u \end{aligned}$$

Sei $v : P \to P'$ eine A-lineare Abbildung. Wir erhalten die A-lineare Abbildung

$$\begin{aligned} \mathrm{Hom}_A(M, v) : \mathrm{Hom}_A(M, P) &\to \mathrm{Hom}_A(M, P') \\ w' &\mapsto v \cdot w \end{aligned}$$

Erinnerung 3.12. Eine Sequnez von A-lineare Abbildungen

$$... \to M_{i-1} \xrightarrow{u_{i-1}} M_i \xrightarrow{u_{u_i}} M_{i+1} \to ...$$

heißt exakt, falls $\mathrm{Ker}(u_i) = \mathrm{Im}(u_{i-1})$

Beispiel. $0 \to M* \xrightarrow{u} M$ ist exakt genau dann wenn u injektiv ist.
$M \xrightarrow{v} M'' \to 0$ ist exakt genau dann wenn v surjektiv ist

Satz 3.12.

1. *Sei* $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''(*)$ *eine Sequenz von* $A-$*Moduln. Dann ist* $(*)$ *genau dann exakt, wenn für jeden A-Modul* P *die Sequenz*

$$\begin{aligned} \mathrm{Hom}_A(P, (*)) : 0 \to \mathrm{Hom}_A(P, M') &\to \mathrm{Hom}_A(P, M) && \to \mathrm{Hom}_A(P, M'') \\ w' &\mapsto u \circ w' && w \mapsto v \circ w \end{aligned}$$

exakt ist.

2. *Sei $M' \to M \to M'' \to 0 (**)$ eine Sequenz von A-Moduln. Dann ist $(**)$ genau dann exakt, wenn für jeden A-Modul P die Sequenz*

$$\begin{array}{cccc} 0 \to \mathrm{Hom}_A(M'', P) \to \mathrm{Hom}_A(M, P) & & \to \mathrm{Hom}_A(M', P) \\ w'' \mapsto w'' \otimes v & & w \mapsto w \otimes u \end{array}$$

Beweis. Wir beweisen Schrittweise:

1. "$(*)$ ist exakt $\Rightarrow \mathrm{Hom}_A(P, (*))$ ist exakt"

   (a) $w' \mapsto u \circ w'$ injektiv:
   Sei $w \in \mathrm{Hom}_A(P, M')$ mit $u \circ w' = 0$.
   Dann ist (da u injektiv) $w' = 0$. Also ist $\mathrm{Ker}(w' \mapsto u \circ w') = 0$.

   (b) $\mathrm{Im}(w' \mapsto u \circ w') \subseteq \mathrm{Ker}(w \mapsto v \circ w)$:
   Kompoosition: $w' \mapsto u \circ w' \mapsto \underbrace{(v \circ u)}_{=0} \circ w'$ ist Null.

   (c) $\mathrm{Im}(w \mapsto v \circ w) \subseteq \mathrm{Ker}(w' \mapsto u \circ w')$:
   Sei $w \in \mathrm{Hom}_A(P, M)$ mit $v \circ w = 0$, sodass $\mathrm{Im}(w) \subseteq \mathrm{Ker}(v) = \mathrm{Im}(u)$.

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "u"] & M \arrow[r, "v"] & M'' \\ & & P \arrow[u, "w"] \arrow[ul, dashed, "w'?"] \arrow[ur, "0"'] & \end{tikzcd}$$

   "$\Leftarrow$"

   (a) u injektiv: Sie $m' \in M$ mit $u(m') = 0$, $P := < m' >= Am' \subseteq M', w' : P \to M'$ Inklusion.
   Dann folgt aus $u \circ w' = 0$, da $w' \mapsto u \circ w'$ injektiv ist, dass $w' = 0$ und damit $P = 0$ sodass $m' = 0$.

   (b) $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$. Z.z. $v \circ u = 0$.
   Wir wissen bereits, dass für alls A-Moduln P die Abbildung $\mathrm{Hom}_A(P, M') \to \mathrm{Hom}_A(P, M''), w' \mapsto v \circ u \circ w$ die Nullabbildung ist.
   Wähle $P = M'$ und $w' = \mathrm{id}_{M'}$, dann ist $v \circ u = 0$.

   (c) $\mathrm{Ker}(v) \subseteq \mathrm{Im}(u)$:
   Sei $m \in \mathrm{Ker}(v)$, $P : Am \subseteq M$ und sei $w : P \to M$ eine Inklusion.
   Dann ist $v \circ u = 0$, d.h. $w \in \mathrm{Ker}(w \mapsto v \circ w) = \mathrm{Im}(w' \mapsto u \circ w')$.
   Also exitsiert $w' : P \to M'$ mit $u \circ w' = w$.
   Da $u(w'(m)) = w(m) = m$ gilt $m \in \mathrm{Im}(u)$.

2. Übung

□

Bemerkung 3.13. Seiene M, N, P A-Moduln. Dann ist

$$\begin{aligned} \mathrm{Hom}_A(M \otimes_A N, P) &= L_A(M, N; P) && (*) \\ &= \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \\ (\alpha : M \times N \to P) &\mapsto (n \mapsto \alpha(m, n)) \end{aligned}$$

$$\begin{aligned}
\text{Sei } T_N : (\text{A-Modul}) &\to (\text{A-Modul})\\
M &\mapsto M \otimes_A N\\
(u : M \to M') &\mapsto u \otimes id_N\\
N_N : (\text{A-Modul}) &\to (\text{A-Modul})\\
P &\mapsto \text{Hom}_A(N, P)
\end{aligned}$$

Dann besagt $(*)$:

$$\text{Hom}(T_M(M), P) = \text{Hom}(M, H_N(P))$$

d.h. T_N ist linksadjungiert zu H_N.
Dann ist T_N rechtsexakt und H_N ist linksexakt.

Proposition 3.14. Sei $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine exakte Sequenz von A-Moduln. Dann ist für jeden A-Modul N die Sequenz

$$M' \otimes N \xrightarrow{u \otimes id_N} M \otimes_A N \xrightarrow{u \otimes id_N} M'' \otimes_A N \to 0$$

exakt.

Beweis. Formal mit 3.13.
Sei $M' \to M \to M'' \to 0$ exakt.
Dann gilt mit **??**, dass für alle A-Mdouln P:

$$0 \to \text{Hom}_A(M'', H_N(P)) \to \text{Hom}_A(M, H_N(P)) \to \text{Hom}_A(M', H_N(P))$$

Ist jeweils gleich (3.13)

$$0 \to \text{Hom}_A(T_N(M''), P) \to \text{Hom}_A(T_N(M), P) \to \text{Hom}_A(T_N(M'), P)$$

exakt, sodass mit **??**

$$T_N(M') \to \underbrace{T_N(M)}_{=M \otimes_A N} \to T_N(M'') \to 0$$

exakt ist. □

Beispiel 3.15. Sei $A = \mathbb{Z}$, $u : \mathbb{Z} \xrightarrow{x \mapsto 2x} \mathbb{Z}$.
Dann ist $0 \to \mathbb{Z} \xrightarrow{u} \mathbb{Z}$ exakte und $A \otimes_A M = M$.
Aber

$$\begin{aligned}
0 \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} &\xrightarrow{u \otimes id_{\mathbb{Z}/2\mathbb{Z}}} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}\\
\mathbb{Z}/2\mathbb{Z} &\xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z}
\end{aligned}$$

ist nicht injektiv.

4 Lokalisierung

4A Lokalisierung von Ringen und Moduln

Definition 4.1. Eine Teilmenge $S \subseteq A$ heißt <u>multiplikativ</u>, falls $1 \in S$ uns $s, t \in S \Rightarrow st \in A$.

Beispiel 4.2. 1. $S = \mathbb{Z} \setminus \{0\} \subseteq A = \mathbb{Z}$

2. Sei $f \in A$, dann ist $S_f = \{1, f, f^2, ..., \}$ eine multiplikative Teilmenge.

3. Sei $y \subset A$ Primideal. Dann ist $A \setminus y \subset A$ eine multiplikative Teilmenge.

Definition 4.3. Sei A ein Ring, $S \subseteq A$ eine multiplikative Teilmenge.
Definiere auf $A \times S$ eine Äquivalenzrelation durch

$$(a, s) \sim (b, t) :\Leftrightarrow at = bs$$

Definiere $S^{-1}A := (A \times S)/\sim$. Die Äquivalenzklasse von (a, s) wird mit $\frac{a}{s}$ bezeichnet.

Beweis. Dies ist eine Äquivalenzrelation:

- Refelxivität
- Symmetrie
- Transitiv: Sei $(a, s) \sim (b, t)$ und $(b, t) \sim (c, u)$

  Dann
  $$\begin{array}{ccc} (tvw)au & \overset{(!)}{=\!=} & (tvw)cs \\ \| & & \| \\ vbswu & =\!=\!= & wbuvs \end{array}$$
  Also $\frac{a}{s} = \frac{b}{t}$ genau dann esnn es $v \in S$ gibt sodass $vat = vbs$.

$\square$

Bemerkung. $S^{-1}A$ ist Ring mit

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} \qquad := \frac{ab}{st}$$

Dies ist Wohldefiniert und macht $A^{-1}A$ zu einem kommutativen Ring mit Eins= $\frac{1}{1}$ und Null= $\frac{0}{1}$.
Die Abbildung $\iota : A \to S^{-1}A, a \mapsto \frac{a}{1}$ ist ein Ringhomomorphismus und heißt **kanonisch**.

Beispiel. Sei $S = \mathbb{Z} \setminus \{\} \subseteq A = \mathbb{Z}$. Dann ist $S^{-1}A = \mathbb{Q}$.

Satz 4.4 (Universelle Eigenschaft)**.** *Sei $S \subseteq A$ eine multiplikative Teilmenge und sei $1 : A \to S^{-1}$ kanonisch. Sei B ein Ring, $\varphi : A \to B$ ein Ring-Homomorphimsmus mit $\varphi(s) \in B^\times = \{b \in B \mid \exists c \in B : bc = 1\}$ für alle $s \in S$. Dann existiert ein eindeutiger RIngHomomorphismus $\tilde{\varphi} S^{-1A \to B}$ mit $\tilde{\varphi} \circ 1 = \varphi$:.*

$$\begin{tikzcd} A \arrow[r, "\forall \varphi : \varphi(s) \subseteq B^\times"] \arrow[d, "1"] & B \\ S^{-1}A \arrow[ur, "\exists! \tilde{\varphi}"] & \end{tikzcd}$$

Beweis. <u>Eindeutigkeit</u> Für $\frac{a}{s} - inS^{-1}A$ muss für $\tilde{\varphi}$ gilt:

$$\begin{aligned} \tilde{\varphi}\left(\frac{a}{a}\right) &= \tilde{\varphi}\left(\frac{a}{1}\left(\frac{s}{1}\right)^{-1}\right) = \tilde{\varphi}\left(\frac{a}{1}\right)\tilde{\varphi}\left(\frac{s}{1}\right)^{-1} \qquad (*) \\ &= \varphi(a)\varphi(s)^{-1} \end{aligned}$$

<u>Eindeutigkeit</u> Definiere $\tilde{\varphi}$ durch $(*)$
Z.z: $\tilde{\varphi}$ ist wohldefiniert. $\square$

Bemerkung 4.5. Sei $S \subseteq A$ eine multilineare Teilmenge.
Dann gilt: $1 : A \to S^{-1}A$ ist injektive $\Leftrightarrow$ S enthält keien Nullteiler.

Beweis.

$$\begin{aligned}&1 \text{ ist injektiv}\\ \Leftrightarrow &\operatorname{Ker}(1) = 0\\ \Leftrightarrow &(\forall a \in A : \frac{a}{1} = 1 \Rightarrow a = 0) \Leftrightarrow \quad (\forall a \in A : \exists s \in S : as = 0 \Rightarrow a = 0) \Leftrightarrow S \text{ enthält eine Nullteiler}\end{aligned}$$

□

Satz 4.6 (Lokalisierung von Moduln). *Sei $S \subseteq A$ ein multiplikative Teilmenge, M ein A-Modul. Definiere auf $M \times S$ eine Äquivalenz Relation:*

$$(m, s) \sim (n, t) \Leftrightarrow \exists v \in S : vtm = vsm$$

Man erhält den $S^{-1}A$-Modul $S^{-1}M = (M \times S)/\sim$:

- *Mit Addition: $\frac{m}{s} + \frac{n}{t} := \frac{tm+sn}{st}$*
- *Mit Skalarmultiplikation: $\frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$*

Satz 4.7 (Lokalisierung als Funktor). *Sei $u : M \to N$ eine A-lineare Abbildung, $S \subseteq A$ ein multiplikative Teilgruppe. Dann ist*

$$\begin{aligned}S^{-1}u : S^{-1}M &\to S^{-1}N\\ \frac{m}{s} &\mapsto \frac{u(m)}{s}\end{aligned}$$

eine $S^{-1}A$ lineare Abbildung.

Satz 4.8 (Lokalisierung ist exakt). *InhaltSei $M' \xrightarrow{u} M \xrightarrow{v} M''$ eine exakte Sequenz von A-Moduln, $S \subseteq$ eine multilineare Teilmenge. Dann ist*

$$S^{-1}M' \xrightarrow{S^{-1}u} S^{-1}M \xrightarrow{S^{-1}v} S^{-1}M''$$

eine exakte Sequnez von $S^{-1}A$ Moduln.

Beweis. $v \circ u = 0$. Also ist $S^{-1}v \circ S^{-1}u = 0$.
Noch zu zeigen: $\operatorname{Ker}(S^{-1}v) \subseteq \operatorname{Im}(S^{-1}u)$.
Sei $\frac{m}{s} \in S^{-1}M$ mit $S^{-1}v\frac{v}{s} = \frac{v(m)}{s} = 0$.
Also gibt es $t \in S : tv(m) = v(tm) = 0$.
Damit liegt $tm \in \operatorname{Ker}(v) = \Im(u)$.
Also existiert $m \in M : u(m' = tm)$. Dann ist $S^{-1}u\left(\frac{m'}{st}\right) = \frac{u(m')}{st} = \frac{m}{s}$ und damit $\frac{m}{s} \in \operatorname{Im}(S^{-1}u)$ □

Proposition 4.9. Sei M ein A-Modul, $S \subseteq A$ eine multiplikative Teilmenge, dann ist

$$\begin{aligned}u : S^{-1}A \otimes_A M &\xrightarrow{\sim} S^{-1M}\\ \frac{a}{s} \otimes m &\mapsto \frac{am}{s}\end{aligned}$$

ist Homomorphismus von $S^{-1}A$-Moduln.

Beweis. 1. 1 ist wohldefiniert:

(a) Z.z. $\frac{a}{s} = \frac{b}{t} \Rightarrow \frac{am}{s} = \frac{bm}{t}$:
Sei $\frac{a}{s} = \frac{b}{t}$. Ist äquivalent dazu, dass es $v \in S$ gibt mit $vat = vbs$. Dann erfüllt v auch $vatm = vbsm$ für alle $m \in M$, also auch $\frac{am}{s} = \frac{bm}{t}$.

(b) Z.z. $\frac{am}{s}$ ist linear in $\frac{a}{s}$ und in m:

2. Existenz einer Umkehrabbildung:
Sei $v : S^{-1}M \to S^{-1}A \otimes_A M, \frac{m}{s} \mapsto \frac{1}{s} \otimes m$.
Aus $\frac{m}{s} = \frac{n}{t}$ folgt, dass auch $\frac{1}{s} \otimes m = \frac{1}{t} \otimes n$. Also ist die Abbildung wohldefiniert.
Zusätzlich gilt $v \circ u = \mathrm{id}_{S^{-1}A \otimes_A M}$ und $u \circ v = \mathrm{id}_{S^{-1}M}$.

□

Satz 4.10 (Ideal in $S^{-1}A$)**.** *Sei $S \subseteq A$ eine multilineare Teilmenge.*

$$\{\textit{Ideale in } A\} \underset{b \mapsto \iota^{-1}(b)}{\overset{\mathfrak{a} \mapsto S^{-1}\mathfrak{a}}{\rightleftarrows}} \{\textit{Ideale in } S^{-1}A\}$$

$$1 : A \to S^{-1}A, a \mapsto \frac{a}{1}$$

Nicht zu einander invers.

1. *Sei $\mathfrak{a} \subseteq A$ ein Ideal. Dann ist $S^{-1}\mathfrak{a} = S^{-1}A$ genau dann wenn $\mathfrak{a} \cap S \neq 0$. Dann folgt auch, dass $\mapsto S^{-1}\mathfrak{a}$ ist nur invertierbar , falls $S \subseteq A^\times$.*

2. *Für $b \subseteq S^{-1}A$ Ideal gilt:*

$$S^{-1}(\iota^{-1}(b)) = b$$

Dann folgt $b \mapsto \iota^{-1}(b)$ ist injektiv und jedes Ideal von $S^{-1}A$ ist von der Form $S^{-1}\mathfrak{a}$ für einIdeal $\mathfrak{a} \subseteq A$.

3. *Sei $\mathfrak{a} \subseteq A$ ein Ideal. Dann gilt: Es gibt ein Ideal $b \subseteq S^{-1}A$ mit $\mathfrak{a} = \iota^{-1(b)}$. Dies ist Äquivalent dazu, dass kein $s \in S$ ins $A/\mathfrak{a}$ Nullteiler ist.*

4. *Man hat zueinander inverse Bijektionen:*

$$\left\{q \subset S^{-1A} \mid \textit{Primideal}\right\} \xrightarrow{q \mapsto \iota^{-1(q)}}$$
$$\xleftarrow[\mathfrak{p} \mapsto S^{-1}\mathfrak{p}]{} \{\textit{Primiedeale } \mathfrak{p} \subset A \textit{ mit } \mathfrak{p} \cap S = \emptyset\}$$

Beweis. 1. $\frac{1}{1} - inS^{/1A}$ ist genau dann wenn es ein $a \in \mathfrak{a}, s \in S$ gibt, sodass $\frac{a}{s} = \frac{1}{1}$.

$$\begin{aligned}&\Leftrightarrow \exists a \in \mathfrak{a}, s, t \in S : ta = ts\\ &\Leftrightarrow \mathfrak{a} \cap S \neq 0\end{aligned}$$

2. Sei $\frac{a}{s} \in S^{-1}(\iota^{-1(b)})$.
   Ist äquivalent zu $\exists t \in S$ und $b \in A$ mit $\frac{b}{1} \in b$, so dass

$$\frac{a}{s} = \frac{b}{t} = \frac{b}{1}\frac{1}{t}$$

   $\Leftrightarrow \frac{a}{s} \in b$

3. Sei $\mathfrak{a} = \iota^{-1}(b)$ für ein Ideal $b \subseteq S^{-1}A$.

$$\Leftrightarrow \mathfrak{a} = \iota^{-1}(S^{-1}\mathfrak{a})$$

$$\Leftrightarrow A/\mathfrak{a} \xrightarrow{\overline{a} \mapsto \overline{\left(\frac{a}{1}\right)}} S^{-1}A/S^{-1}\mathfrak{a} =^{\mathbf{??}} S^{-1}A/\mathfrak{a} \quad \text{injektiv}$$

   (Wende **??** an auf die exakte Sequenz

$$0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$$

   Dann ist auch

$$0 \to S^{-1}\mathfrak{a} \to S^{-1}A \to S^{-1}(A/\mathfrak{a}) \to 0$$

   exakt.) Mit **??** gilt äquivalenz dazu, dass kein $s \in S$ ist Nullteiler in $A/\mathfrak{a}$.

4.

□

Satz 4.11 (Universelle Eigenschaft des Quotientenkörpers)**.** *Sei* $\iota : A \to \mathrm{Quot}(A)$ *kanonisch und sei* $\varphi : A \to K$ *ein injektiver Ring-Homomorphismus wobei* K *ein Körper.*
Dann existiert genau ein Homomorphismus von Körpern $\tilde{\varphi} : \mathrm{Quot}(A) \to K$*.*

4B Lokale Ringe und Restklassenkörper

Definition 4.12. Ein Ring A heißt <u>lokal</u> wenn er genau ein Maximales Ideal besitzt.
Dann bezeichnet $\mathfrak{m}_A$ dieses Maximales Ideal.
Der Körper $\kappa(A) := A/\mathfrak{m}_A$ heißt <u>Restklassenkörper von A</u>.

Beispiel 4.13.

- Jeder Körper ist ein lokaler Ring.
- Ein Hauptidealring A ist genau dann lokal, wenn bis auf Multiplikation mit Einheiten genau ein irreduzibles Element existiert.
  Oder wenn A Körper ist

Definition 4.14. Ein lokaler Hauptideal Ring der kein Körper ist, heißt <u>diskreter Bewertungsring</u>.

Beispiel 4.15. Sei $\mathfrak{p} \subset A$ Primideal, $S := A \backslash \mathfrak{p}$ multiplikative Teilmenge, $A_{\mathfrak{p}} := S^{-1}A$.

$$\{\text{Primideals in } A - \mathfrak{p}\} \leftrightarrow \{\text{Primideals } q \subset A \text{ mit } q \subseteq \mathfrak{p}\}$$

(mit 4).
Also ist $A_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal $S^{-1}\mathfrak{p}$.
Der Körper $\kappa(\mathfrak{p}) := A/S^{-1}\mathfrak{p}$ heißt <u>Restklassenkörper in $\mathfrak{p}$</u>.

Bemerkung 4.16. Seien $q \subseteq \mathfrak{p} \subset A$ Primideale.

1.
$$\begin{aligned}\{\text{Primideale in } A_{\mathfrak{p}}\} &= \{\text{Primideale in } A, \text{ die in } \mathfrak{p} \text{ enthalten sind}\}\\ \{\text{Primideal in } A/q\} &= \{\text{Primideal in } A, \text{ die } q \text{ enthalten.}\}\end{aligned}$$

2. Sei $S := S \backsim \mathfrak{p}$. Dann ist $S^{-1}(A/q) = S^{-1}A/S^{-1}q$ und
$$\{\text{Primideal in } S^{-1}(A/q)\} = \{\text{Primideals in } A \text{ die zwischen } q \text{ und } \mathfrak{p} \text{ liegen}\}$$

3. Speziell für $q = \mathfrak{p}$:
$$\begin{aligned}S^{-1}(A/\mathfrak{p}) &= \kappa(\mathfrak{p})\\ &= \mathrm{Quot}(A/\mathfrak{p})\end{aligned}$$

4C Spektren

Erinnerung 4.17. Ein Topologischer Raum ist ein Paar $(X; \mathfrak{T})$ wobei X eine Menge, $\mathfrak{T} \subseteq \mathscr{P}(X)$, sodass gilt:

1. $\emptyset \in \mathfrak{T}, X \in \mathfrak{T}$
2. Sei $(U_i)_{i \in I}$ eine Familie von Mengen $U_i \in \mathfrak{T}$ dann gilt $\forall i \in I : \bigcup_{i \in I} U_i \in \mathfrak{T}$
3. $U, V \in \mathfrak{T}$, dann $U \cap V \in \mathfrak{T}$

Die Mengen in $\mathfrak{T}$ heißen offen.

Erinnerung 4.18. Seine X, Y topologische Räume. Eine Abbildung $f : X \to Y$ heißt stetig, falls $f^{-1}(V) \subseteq X$ ist offen für alle offenen $V \subseteq Y$.

Erinnerung 4.19. Sei $(X, \mathfrak{T})$ ein topologischer Raum $B \subseteq \mathfrak{T}$ heißt Basis der Topologie, falls jeder offenen Teilmenge Vereinigung von Menge aus B ist.

Beispiel 4.20. Sei (X, d) eien metrischer Raum, dann heißt $U \subseteq X$ offen, falls
$$\forall x \in U \exists \epsilon > 0 : B_\epsilon(x)\{y \in X \mid M(x, y) < \epsilon\} \subseteq U$$
Basis der Topologie: $\{B_\epsilon(x) \mid \epsilon \in \mathbb{R}^{>0}, x \in X\}$

Definition 4.21. Sein topologischer Raum X heißt Hausdorffsch, falls $\forall x, y \in X$ mit $x \neq y$ existieren $x \in U \subseteq X$, $y \in V \subseteq X$ offen, sodass $U \cap V = \emptyset$. Metrische Räume sind Hausdorffsch.

Definition 4.22. Ein topologischer Raum X heißt quasikompakt, falls jede offene Überdeckung $(U_i)_{i \in I}$ von X (d.h. $U_i \subseteq X$ offen für alle $i \in I$ mit $\bigcup_{i \in I} U_i = X$) eine endliche Teilüberdeckung besitzt. (d.h. $\exists J \subseteq I$ endliche Teilmenge, sodass $\bigcup_{i \in I} U_i = X$.)

4.23 Spielzeugmodell (der Funktionalanalysis)

Sei X ein kompakter topologischer Raum,

$$A := A_X := \xi(X, \mathbb{C}) := \{f : X \to \mathbb{C} \text{ stetig}\}$$

Sei $x \in X$, dann betrachte

$$\mathfrak{M}_x := \{f \in A \mid f(x) = 0\} \subseteq A$$

Dies ist ein Minimales Ideal, denn

$$A/\mathfrak{M}_x \xrightarrow{\sim} \mathbb{C}, \overline{f} \mapsto f(x)$$

Satz 4.24. *Die Abbildung*

$$\begin{aligned} &X \to \operatorname{Max}(A) := \{\mathfrak{M} \subset A \mid \textit{maximales Ideal}\} \\ &x \mapsto \mathfrak{M}_x \end{aligned}$$

ist bijektiv.

Korollar 4.25. *Sei $f \in A$ und für $\mathfrak{M}_x \in \operatorname{Max}(A)$ sie $f(x) =$ Bild von f in $A/\mathfrak{M}_x = \mathbb{C}$.*

$$\begin{aligned} D(f) &= \{\mathfrak{M} \in \operatorname{Max}(A) \mid \overline{f} \textit{ in } A/\mathfrak{M} \textit{ ist} \neq 0\} \\ &= \{\mathfrak{M} \in \operatorname{Max}(A) \mid f \notin \mathfrak{M}\} \\ &= \sigma(\{x \in X \mid f(x) \neq 0\}) \end{aligned}$$

Definition 4.26. $U \subseteq \operatorname{Max}(A)$ heißt **offen**, falls $\exists F \subseteq \operatorname{Max}(A)$ mit

$$U = \bigcup_{f \in F} D(f)$$

Dies ist die Topologie uf $\operatorname{Max}(A)$.
(Bemerke: $D(f) \cap D(g) = D(fg)$)

Satz 4.27. *σ ist Homomorphismus*

Seien X, Y kompakte topologische Räume, $F : X \to Y$ stetig.
Mann erhält den $\mathbb{C}-$Algebra-Homomorphismus:

$$\begin{aligned} \varphi : A_Y &\to A_x \\ f &\mapsto f \circ F \end{aligned}$$

Habe Kommutierendes Diagramm

$$\begin{tikzcd} X \arrow[d, "\sigma"', "F\sim"] & Y \arrow[d, "\sigma"', "\sim"] \\ \operatorname{Max}(A_x) \arrow[r, "\mathfrak{M} \mapsto \varphi^{-1}(\mathfrak{M})"] & \operatorname{Max}(A_Y) \end{tikzcd}$$

Es folgt $\forall \mathfrak{M} \subset A_x$ maximal, sodass $\varphi^{-1}(\mathfrak{M}) \subset A$ maximal ist.
Sei A ein Ring. Setze $X = \operatorname{Spec}(A) := \{y \subset A \mid \text{Primideal con } A\}$ als das **Spektrum von** A.
Für $x \in X$ bezeichne $y_x \subset A$ das korrespondierene Primideal. Sei $f \in A$, $x \in X$.
Dann definiere

$$f(x) := \text{Bild von } f \text{ unter} A \to A/y_x \hookrightarrow \operatorname{Quot}(A/y_x) = \kappa(x)$$

Bemerkung 4.28. f ist keine Funktion $X \to ?$.
Seetze

$$\begin{aligned} D(f) :&= \{x \in X \mid f(x) \neq 0\} \\ &= \{x \in X \mid f \notin y_x\} \end{aligned}$$

Definition 4.29. Eine Teilmenge $U \subseteq X = \operatorname{Spec}(A)$ heißt **offen**, falls $F \subseteq A$ Teilmenge existiert, sodass $U = \bigcup_{f \in F} D(f)$.
Wir erhalten die sogenannte **Zanski-Topologie**. Dabie

$$\begin{aligned} D(f) \cap D(g) &= D(fg) \\ \emptyset &= D(0) \\ x &= D(x) \end{aligned}$$

Korollar 4.30 ($D(f)$ als Spektrum)**.** *Sei $f \in A$ und sei $S_f := \{1, f, f^2, ..., \}$. Dann ist*

$$\begin{aligned} \operatorname{Spec}(S_f^{-1}A) = \{y \in \operatorname{Spec}(A) \mid y \cap S_f = \emptyset\} \\ \{y \in \operatorname{Spec}(A) \mid f \notin y\} \\ = D(f) \end{aligned}$$

Satz 4.31 (Abgeschlossenen Teilmengen)**.** *Sei $X = \operatorname{Spec}(A)$, $Y \subseteq X$ Teilmenge. Dann*

$$Y \subseteq X \text{ abgeschlossen} \Leftrightarrow X \setminus Y \subseteq X \text{ offen} \Leftrightarrow \exists F \subseteq A : X \setminus Y = \bigcup_{f \in f} D(f)$$

Genau dann wenn

$$\begin{aligned} \exists F \subseteq A \qquad\qquad & Y = \bigcap_{f \in F} (X \setminus D(f)) \\ &= \bigcap_{f \in F} \{y \in A \mid f \in y\} \\ &= \{y \in A \text{ Primideal} \mid (F) \subseteq y\} \\ \Leftrightarrow \exists \mathfrak{a} \subseteq A \text{ Ideal} \qquad\qquad & Y = \{y \in A \text{ Primiedeal} \mid \mathfrak{a} \subseteq y\} \\ &= \operatorname{Spec}(A/\mathfrak{a}) \end{aligned}$$

Satz 4.32 (Funktorialität)**.** *Sei $\varphi A \to B$ ein Homomorphismus on Ringen. Dann ist $\varphi \operatorname{Spec} B \to \operatorname{Spec}(A), q \mapsto \varphi^{-1}(q)$ stetig.*

Beweis. Für $f \in A$ gilt

$$\begin{aligned} \varphi^{-1}(D(f)) &= \{y \in \operatorname{Spec}(B) \mid \varphi(y) \in D(f)\} \\ &= \{q \subset B \text{ Primideal} \mid \varphi^{-1}(q) \in D(f)\} \\ &= \{q \subset B \text{ Primideal} \mid f \in \varphi^{-1}(q)\} \\ &= \{q \subset B \text{ Primideal} \mid \varphi(f) \notin q\} \\ &= D(\varphi(f)) \subseteq \operatorname{Spec}(B) \text{ offen.} \end{aligned}$$

□

4D Lemma von Nokagama???

Definition 4.33. Sei $u : M \to N$ ein Homomorphismus von A-Moduln und sei $(m_1, ..., m_r)$ ein Erzeugendensystem von M und $(n_1, ..., n_s)$ von N.
Dann exitsiert

$$T = (t_{ij})_{\substack{1 \leq i \leq s \\ 1 \leq j \leq r}} \in M_{s \times r}(A)$$

sodass

$$n(m_j) = \sum_{i=1}^{s} t_{ij} n_i$$

Dann heißt T eine **Matrix von** U **bezüglich** $(m_1, ..., m_r)$ **und** $(n_1, ..., n_s)$.

Bemerkung 4.34.
1. T ist nicht eindeutig duch u bestimmt
   (es sei denn $(n_1, ..., n_s)$ ist Basis)
2. Nicht jede Matrix in $M_{s \times r}(A)$ ist eine Matrix von u bezüglich $(m_1, ..., m_r)$ und $(n_1, ..., n_s)$.
   (Es sei denn $m_1, ..., m_r$ ist Basis von M)

Erinnerung 4.35. Sei $T \in M_n(A) = A^{n \times m}$, $n \in \mathbb{N}$.
Dann existiert $S \in M_n(A)$, sodass $TS = ST = \det T I_m$. Dann ist $S = (s_{ij})$

$$s_{ij} = (-1)^{i+j} \det(T_{ji})$$

(T mit j-ter Spalte und $i-$ter Spalte gestrichen.)
S heißt die Adjunkte von T.

Satz 4.36 (Cayley-Hamilton)**.** *Sei M ein A-Modul, $(m_1, ..., m_n)$ ein Erzeugendensystem und sei $u : m \to M$ eine A-Lineare Abbildung. Sei $T \in M_r(A)$ eine Matrix von u bezüglich $(m_1, ..., m_r)$.*
Setze

$$\chi_T := \det \underbrace{(XI_r - A)}_{\in M_r(A[x])} = X^r + a_1 X^{r-1} + ... + a_{r-1} X + a_r$$

Dann gilt

$$\chi_T(u) = u^r + a_1 u^{r-1} + ... + a_{r-1} + a_r \operatorname{Id}_M = 0 \in \operatorname{End}_A(M)$$

1. *Seo $\mathfrak{a} \subseteq A$ Idela, sod ass $u(M) \subseteq \mathfrak{a}M$. Dann $a_i \in \mathfrak{a}^i \forall i = 1, ..., r$.*

Beweis. $u(M) \subseteq \mathfrak{a}M$. Es folgt, dass die Koeffizienten von T in $\mathfrak{a}$ liegen.
a_i ist Summe von i-fachen Produkten von Koeffizienten von T.
Also $a \in \mathfrak{a}^i \forall i = 1, ..., r$.
Sei nun $T^T = (t_{ji})_{i \leq i,j \leq r}$ aber $u(m_j) = \sum_i t_{ji} m_i$.
Dann gilt

$$\sum_i (u\delta_{ji}) - t_{ji} m_i = 0$$

Sei nun

$$C := (X\delta_{ji} - t_{ji})_{ji} \in M_r(A[X])$$

wobei $\chi_T = \det(C)$.
Sei

$$D := (d_{jk})_{jk}$$

Die Adjungte von C, also

$$CD = \chi_T I_r \in M_r(A[X]) \tag{$\star\star$}$$

Betrachte den Homomorphismus $u \in \mathrm{End}_A(A)$

$$A[X] \xrightarrow[f \mapsto f(u)]{} A[u] = \{f(u) \mid f \in A[x]\}$$

$A[u]$ ist nun eine kommutative A-Algebra. Erhalte

$$C(u) = (u\delta_{ij} - t_{ji})_{i,j} \in M_r(A[u])$$
$$C(u) = (\delta_{kj}(u))_{k,j}$$

Multipliziere $(\star)$ mit $\delta_{kj}(u)$.

$$0 = \sum_{i=1}^{r} \underbrace{\sum_{j=1}^{r} \delta_{kj}(u)(u\delta_{ji} - t_{ji})}_{\substack{\text{k-te Koeffizienten von} \\ DC(u) = \chi_T(u)\delta_{ki}}} m_i$$

Also ... $\square$

Lemma 4.37 (Lemma von Nakogama (1. Version)). *Sei M eine endlich erzeugter $A-$Modul, $\mathfrak{a} \subseteq A$ ein Ideal, sodass $M = \mathfrak{a}M$.*
Dann existerit $f \in 1 + \mathfrak{a} = \{1 + x \mid x \in \mathfrak{a}\}$, sodass $fM = 0$

Beweis. Wende 4.36 auf $u = \mathrm{id}_M$: Mit 4.36.1 Gilt

$$u^r + a_1 u^{r-1} + ... + a_{r-1}u + a_r \,\mathrm{id} = 0$$

mit $a_i \in \mathfrak{a}^i = \mathfrak{a}$.
Also ist $f \,\mathrm{id}_M = 0$, wobei

$$f = 1 + a_1 + a_2 + ... + a_r \in 1 + \mathfrak{a}$$

sodass $fM = 0$ $\square$

Bemerkung 4.38. (Einschränkung von A auf $\mathrm{Spec}(A/\mathfrak{a})$)

$$... = A/\mathfrak{a} \otimes_A M = M/\mathfrak{a}M = 0$$

Da $f \in 1 + \mathfrak{a}$ folgt

$$\mathrm{Spec}(A/\mathfrak{a}) \subseteq^{(\star)} D(f) = \mathrm{Spec}(S_g^{-1}A)$$

wobei $S_f = \{1, f, f^2, ...\}$, sodass

$$(\text{Einschränkung von } M \text{ aus } D_f) = S_f^{-1}A \otimes_A M = S_f^{-1}M \overset{(\star\star)}{=} 0$$

Zu $(\star)$: Sei $x \in \mathrm{Spec}(A)$.

$$x \in \mathrm{Spec}(A/\mathfrak{a}) \Leftrightarrow g(\lambda) = 0 \forall g \in \mathfrak{a}$$

Also gilt für $f = 1 + g, g \in \mathfrak{a}$ und $x \in \operatorname{Spec}(A/\mathfrak{a})$:

$$f(x) = 1 + g(x) = 1 \neq 0$$

$$\Rightarrow \operatorname{Spec}(A/\mathfrak{a}) \subseteq \{x | f(x) \neq 0\} = D(f)$$

Zu $(\star\star)$: Sei M endlich erzeugt.
Dann $S_f^{-1} M = 0$ genau dann wenn $\exists g \in S_f : gM = 0$.
$\Leftrightarrow \exists n \in \mathbb{N} : f^n M = 0 \Leftrightarrow fM = 0$

Lemma 4.39 (Lemma von Nakagana (2.Version))**.** *Sei M ein endlich erzeugter A-Modul, $\mathfrak{a} \subseteq \operatorname{Jac}(A)$ ein Ideal mit $M = \mathfrak{a}M$. Dann $M = 0$.*

Beweis. Sei $\mathfrak{a} \subseteq \operatorname{Jac}(A) \overset{??}{\Rightarrow} 1\mathfrak{a} \subseteq A^\times \overset{4.37}{\Rightarrow}$ ... □

...

Beispiel 4.40. Sei $A = \mathbb{Z}$, $M = \mathbb{Z}$. Dann ist die $\mathbb{Z}$-lineare Abbildung $M \xrightarrow{\cdot 2} \mathbb{Z}$ injektiv aber nicht bijektiv.

Satz 4.41. *Sei M ein endlich erzeugter A-Modul und sein $U : M \to M$ eine surjektive A-lineare Abbildung.*
Dann ist u ein Isomorphismus.

Beweis. Fass (M, u) als $A[X]$ Modul auf durch $X \cdot m := u(m)$ für $m \in M$.
Dann ist u genau dann surjektiv, wenn $X \cdot M = M$ ist.
Es folgt durch 4.37 mit $\mathfrak{a} = (X)$, dass es ein $g \in A[X]$ gibt, sodass $(a+gX)(M) = 0$.
Sei $m \in \operatorname{Ker}(u)$, dann

$$u = (1 + gX)(m) = m + \underbrace{g(u)(m)u(m)}_{=0} = m$$

Also ist u injektiv. □

5 Noethersche und Artinsche Ringe

5A Noethersche und Artinsche Moduln

Lemma 5.1. ...

Beweis. ... □

Definition 5.2. Ein A-Modul heißt **noethersch**, falls die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jede Aufsteigende Kette von Untermoduln von M

   $$N_2 \subseteq N_2 \subseteq ... \subseteq M$$

   wird stationär

2. Jede Nichtleere Menge von Untermoduln von M beseitzt ein Maximales Element

Ein A-Modul heißt **artinsch**, falls die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jede absteigende Kette von Untermoduln von M
$$N_2 \supseteq N_2 \supseteq ...$$
wird stationär.
2. Jede Nichtleere Menge von Untermoduln von M beseitzt ein minimales Element.

Definition 5.2. Der Ring A heißt **noethersch**, wenn er als A-Modul noethersch ist. Äquivalent dazu sind:

1. Jede aufsteigende Kette von Idealen in A wird stationär.
2. Jede nichtleere Menge von Idealen in A besitzt eine maximales Element.

Der Ring A heißt **artinsch**, wenn er als A-Modul artinsch ist. Äquivalent dazu sind:

1. Jede absteigende Kette von Idealen in A wird stationär
2. Jede nichtleere Menge von Idealen in A besitzt eine minimales Element.

Beispiel 5.3. -1. 0 ist noethersch und artinsch.

0. Jeder Körper ist noethersch und artinsch.
1. $\mathbb{Z}$ ist noethersch:
Sei $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ $(\star)$ eine aufsteigende Kette.
Dann $\mathfrak{a}_1 = (x_1)$, $x_1 = p_1^{l_1} \cdot ... \cdot p_r^{l_r}$.
$$\{\text{Idealis die } \mathfrak{a}_1 \text{ enthalten}\} \underset{1:1}{\leftrightarrow} \{\text{Teiler von } x_1\}/\{\text{Einheiten}\}$$
Diese Mengen sind endlich also wird $(\star)$ stationär.
$\mathbb{Z}$ ist nicht artinsch:
Sei $x \in \mathbb{Z}$ $x \neq 0, 1, -1$. Dann
$$(x) \supsetneqq (x^2) \supsetneqq (xs) \supsetneqq ...$$
ist absteigenden Kette die nicht stationär wird.
2. Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist der $\mathbb{Z}$-Modul
$$\{x \in \mathbb{Q}/\mathbb{Z} \mid \exists n \in \mathbb{N} : p^n x = 0\}$$
artinsch aber nicht noethersch. (Wir werden zeigen: A artinscher Ring $\Rightarrow$ noethersch)
3. Sei κ Körper, dann ist $\kappa[T_1, T_2, ...]$ nciht noethersch:
$$(T_1) \subsetneqq (T_1, T_2) \subsetneqq (T_1, T_2, T_3) \subsetneqq ...$$

Satz 5.4. *Sei M ein A-Modul.*
Dann ist M genau dann noethersch, wenn jeder A-Untermodul von M endlich erzeugt ist. (Dann ist auch M endlich erzeugt).
Insbesondere ist M genau dann noethersch, wenn jedes Ideal von A endlich erzeugt ist.

Korollar 5.5. *Jeder Hauptidealring ist noethersch.*

Proposition 5.6. Sei $0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine Exakte Sequenz von A-Moduln.
Dann gilt

1. M ist genau dann noethersch, wenn M', M'' noethersch.
2. M ist genau dann artinsch, wenn M', M'' artinsch.

Beweis. 1. "$\Rightarrow$": Es gilt $M' \tilde{=} u(M') \subseteq M$. Es folgt M' ist noethersch.

Sei $N_1 \subseteq N_2 \subseteq ... \subseteq M''$ eine aufsteigende Kette von Untermoduln von M''. Da M noethersch ist, gibt es ein $r \in \mathbb{N}$, sodass $v^{-1}(N_r) = v^{-1}(N_{r+1}) = ...$
Da v surjektiv ist gilt dann

$$n_r = v(v^{-1}(N_r)) = v(v^{-1}(N_{r+1})) = N_{r+1}$$

Also wird $N_1 \subseteq N_2 \subseteq ...$ stationär.

"$\Leftarrow$": Sei $M_1 \subseteq M_2 \subseteq ... \subseteq M$ eine aufsteigende Kette von Untermoduln in M.
Dann sind auch $u^{-1}(M_1) \subseteq u^{-1}(M_2) \subseteq ... \subseteq M'$ und $v(M_1) \subseteq v(M_2) \subseteq ... \subseteq M''$ aufsteigende Ketten.
Da $M_, M''$ gibt es $r \in \mathbb{N}$, sodass $u^{-1}(M_r) = u^{-1}(M_{r+1}) = ...$ und $v(M_r) = v(M_{r+1}) = ...$
Dies ist äquivalent $(\star)$ dazu, dass $M_r = M_{r+1} = ...$ Also ist M noethersch.

Beweis von $(\star)$:
Seien $P \subseteq Q \subseteq M$ Untermoduln mit $u^{-1}(P) = u^{-1}(Q)$ und $v(P) = v(Q)$, sei $q \in Q$.
Dann existiert ein $p \in P$ mir $v(p) = v(q)$. Dann gilt $v(p - q) = 0$, also $p - q \in \mathrm{Im}(u)$.
Dann existier auch $m' \in u^{-1}(Q) = u^{-1}(P)$ mit $u(m') = p - q$ und es gilt $u(m') \in P$, also $q \in P$, also $q = P - u(m')$.
Es folgt, dass $P = Q$.

2. analoge

$\square$

Korollar 5.7. *Seien $_1, ..., M_r$ A-Moduln und sei $r \in \mathbb{N}$. Dann gilt*

1. *$\bigoplus_{i=1}^r M_r$ ist genau dann noethersch, wenn M_i noethersch für alle $i = 1, ..., r$.*
2. *$\bigoplus_{i=1}^r M_r$ ist genau dann artinsch, wenn M_i artinsch für alle $i = 1, ..., r$.*

Beweis. Induktion nach r:
Der Fall $r = 1$ ist klar. Für $r > 1$ betrachte die Sequenz

$$\begin{array}{rcl} 0 \to M_r & \to & \bigoplus_{i=1}^r M_i \to 0 \\ m_r & \mapsto & (0, ..., 0, m_r) \\ & & (m_1, ..., m_r) \mapsto (m_1, ..., m_{r-1}) \end{array}$$

Mit Proposition 5.6 folgt die Behauptung. □

Korollar 5.8. *Ein Ring A ist genau dann noethersch bzw artinsch, wenn jeder erzeugte A-Modul noethersch bzw. artinsch ist.*

Beweis. Sei A noethersch bzw. artinsch und sei M ein endlich erzeugter A-Modul. Dann gilt $M \tilde{=} A^n/N$ für $n \in \mathbb{N}$ und $N \subseteq A^n$ Untermodul. Dann ist die Sequnez $0 \to N \to A^n \to M \to 0$ exakt.
Mit 5.7 folgt daraus dass A noethersch ist auch dass A^n noethersch ist.
Mit 5.6 folgt dann dass auch M noethersch ist. □

Korollar 5.9. *Sei A noethersch bzw artinsch und $\mathfrak{a} \subseteq A$ ein Ideal, dann ist $A/\mathfrak{a}$ noethersch bzw artinsch.*

Bemerkung 5.10. Sei A noethersch bzw artinsch und S eine A multiplikative Teilmenge.
Dann ist $S^{-1}A$ noethersch bzw artinsch.

Beweis. Beweis in Übung. □

5B Länge von Moduln

Definition 5.11. Sei G eine Gruppe und sei R ein (nicht notwendig kommutativer) Ring, sei M ein $R-$(links-)Modul.

1. Eine **Kompositionsreihe von** G (bzw **von M**) ist eine Folge $G = G_0 \supsetneqq G_1 \supsetneqq ... \supsetneqq G_r = 1$ von Untergruppen, sodass für alle $i = 1, ..., r$ die Gruppe G ein Normalteiler von G_{i-1} ist.
(Analog für die Folge $m = M_0 \supsetneqq M_1 \supsetneqq ... \supsetneqq M_r = 0$ von R-Untermoduln)
Dann heißt $r \in \mathbb{N}_0$ die **Länge der Kompositionsreihe**.

2. G heißt **einfach** falls $G \neq \{0\}$ und falls $\{0\}$ und G die einzigen Normalteiler sind.
M heißt **einfach**, falls $M \neq 0$ und falls 0 und M die einzigen Untermoduln sind.

3. Eine Kompositionsreihe heißt **maximal** oder **Jordan-Hölder Reihe** falls keine echten Normalteiler (bzw. Untermoduln) eingefügt werden können.
(Äquivalent: G_{i+1}/G_1 bzw. m_{i+1}/M_i sind einfach für alle $i = 1, ..., r$)

Bemerkung 5.12. 1. Normalerweise existiert keine Jordan-Hölder-Reihe

2. Sei $R = K$ Körper und sei V ein K-Vektorraum. Dann ist V genau dann einfach, wenn $\dim_K(v) = 0$.
Sei $(v_1, ..., v_r)$ eine Basis von V, dann ist $V = \langle v_1, ..., v_r\rangle \supsetneqq \langle v_1, ..., v_{r-1}\rangle \supsetneqq ... \supsetneqq \langle v_1\rangle \supsetneqq 0$ eine JH-Reihe.

3. Jede Endliche Gruppe besitzt eine JH-Reihe.

Beispiel 5.12. Sei $R = \mathbb{Z} = M$ dann kann man in jede Folge $\mathbb{Z} = n_o\mathbb{Z} \supsetneqq n_1\mathbb{Z} \supsetneqq ... \supsetneqq n_r\mathbb{Z} = 0$ mit $n_0 = 1, n_1 > 1, n_r = 0$ zwischen $n_{r-1}\mathbb{Z}$ und $n_r\mathbb{Z}$ die Untergruppe $2n_{r-1}\mathbb{Z}$ einfügen.

Proposition 5.13. Sei A kein kommutativer Ring, M ein A-Modul, dann gilt M ist genau dann ein einfacher A-Modul wenn $M \tilde{=} A/m$ für maximales Ideal $m \subset A$.

Beweis. "$\Leftarrow$": gilt, da A/m Körper.
"$\Rightarrow$": Sei M einfach ,$x \in M$, $x \neq 0$. Dann ist $Ax = M$ also ist $u : A \to M, x \mapsto ax$ surjektiv. Damit ist für $\mathfrak{a} = \mathrm{Ker}(u)$, dass $M \tilde{=} A/\mathfrak{a}$. Da

$$\{\text{Untermoduln von } A/\mathfrak{a}\} \underset{1:1}{\leftrightarrow} \{\text{Ideale } b \subseteq A \text{ mit } b \supseteq \mathfrak{a}\}$$

muss $\mathfrak{a}$ maximal sein. □

Satz 5.14 (Satz von Jordan-Hölder (simple Variante))**.** *Sei G eine Gruppe (bzw. R ein nicht notwendig kommutativer Ring und M ein R-Modul). Dann besitzen je zwei JH-Reihen von G bzw. M dieselbe Länge.*
In diesem Fall kann jede Kompositionsreihe zu einer JH-reihe ergänzt werden.

Bemerkung (Satz von Hölder (genaue Variante))*.* Seien $G = G_0 \supsetneqq\supsetneqq G_1 \supsetneqq ... \supsetneqq G_r = 1$ und $G = G'_0 =\supsetneqq\supsetneqq G'_1 \supsetneqq ... \supsetneqq G'_s = 1$ JH-Reihen.
Dann ist $r = s$ und es existieren Permutationen $\sigma \in S_r$, sodass $G_{i-1}/G_i \tilde{=} G'_{\sigma(i)-1}/G'_{\sigma(i)}$.

Definition 5.15. Sei G eine Gruppe. Dann heißt

$$l(G) := \begin{cases} \infty & G \text{ beseitzt keine JH-Reihe} \\ r & G \text{ beseitzt eine JH-Reihe der Länge } r \end{cases}$$

die **Länge von** G.

Sei M eine R-Modul. Dann heißt

$$l(M) := \begin{cases} \infty & M \text{ beseitzt keine JH-Reihe} \\ r & M \text{ beseitzt eine JH-Reihe der Länge } r \end{cases}$$

die **Länge von** M.

Bemerkung. Dabei ist $l(M) = 1$ genau dann wenn M einfach und $l(M) = 0$ genau dann wenn $M = 0$.

Beweis. (für Moduln, für Gruppen analog)
Sei M ein R-Modul.
Setze $l(M) := \inf\{\text{Längen von JH-Reihene von } M\} \in \mathbb{N}_0 \cup \{\infty\}$

1. $N \subseteq M$ Untermodul $\Rightarrow l(N) \leq l(M)$.
   Falls $l(M) = \infty$.
   Man kann also annehmen, dass M eine JH-Reihe $M = M_0 \supsetneqq M_1 \supsetneqq ... \supsetneqq M_r = 0$ beitzt mit $r = l(M)$.
   Sei $N_i := N \cap M_i$, $\forall i = 0, ..., r$.
   Die Einbettung $N_{i-1}/N_i \hookrightarrow M_{i-1}/M_i$ ist injektiv, da $M_i \cap N_{i-1} = N_i$.
   Daraus folgt (da M_{i-1}/M_i einfach ist), dass N_{i-1}/N_i entweder einfach

oder $= 0$ ist.
Dann kann die Reihe $N = N_0 \supseteq N_1 \supseteq .. \supseteq N_r = 0$ durch weglassen einger Terme zu einer JH-Reihe werden.
Dann gilt $l(N) \leq l(M)$.

2. Aus $N \subseteq M$ Untermodul mit $l(N) = l(M) < \infty$ folgt $N = M$:
Wie in 1) gilt $M_{i-1}/M_i \tilde{=} N_{i-1}/N_i$, da $l(N) = l(M)$.
Aus $M_r = N_r = 0$ folgt $M_{r-1} = N_{r-1}$ und da $N_{r-2}/N_{r-1} = M_{r-2}/M_{r-1}$ folgt auch $N_{r-2} = M_{r-2}$.
Induktiv gilt damit $N_0 = N = M_0 = M$

3. Jede Kompositions Reihe von M besitzte Länge $\leq l(M)$:
($\Rightarrow$ Alle JH-Riehen haben die selbe Länge)
Sei $M = M_0 \supsetneqq M_1 \supsetneqq ... \supsetneqq M_r = 0$ eine Kompositions-Reihe.
Aus $1), 2)$ folgt $l(M_i) \leq l(M_{i-1})$ für alle $i = 1, ..., r$. Daraus folgt $s \leq l(M)$.

4. Sei $M = M_0 \supsetneqq M_1 \supsetneqq ... \supsetneqq M_s = 0$ eine Kompositions-Reihe, $l(M) < \infty$:
Wenn $s = l(M)$, dann ist (M_i) JH-Reihe. Wenn $s < l(M)$, dann ist (M_i) keine JH-Reihe und die Kompositions-Reihe kann ergänzt werden.

□

Satz 5.16. *Sei $0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine exakte Sequenz von R-Moduln. (Dabei ist R nicht notwendiger weise kommutativ) Dann ist $l(M) = l(M') + l(M'')$.*
(Insbesondere ist $l(M) < \infty$ genau dann wenn $l(M'), l(M'') < \infty$)
Für Gruppen ergibt sich ein anderes Resultat.

Beweis. Sei $M = M_0 \supsetneqq M_1 \supsetneqq ... \supsetneqq M_r = 0$ eine Kompositions-Reihe von M'. Dann ist $M \supsetneqq u(M') = u(M'_0) \supsetneqq ... \supsetneqq u(M'_r) = 0$ eine Kompositions-Reihe und (M''_i) ist eine Kompositionsreihe von M''. Dann folgt duch v^{-1}, dass es auch eine Kompositionsreihe von M.
Insbesondere folgt aus $l(M') = \infty$ oder $l(M'') = 0$, dass $l(M) = \infty$.
Sei $l(M'), l(M'') < \infty$ und sei $M' = M'_0 \supsetneqq M'_1 \supsetneqq ... \supsetneqq M'_r = 0$die JH-Reieh von M' und $M'' = M''_0 \supsetneqq M''_1 \supsetneqq ... \supsetneqq M''_r = 0$ von M''.
Dann ist

$$M = v^{-1}(M''_0) \supsetneqq ... \supsetneqq v^{-1}(M''_s) = \mathrm{Ker}(v) = u(M') \supsetneqq u(M'_1) \supsetneqq ... \supsetneqq u(M'_r) = 0$$

eine Kompositions-Reihe mit einfachen Subquotienten, also eine JH-Reihe.
Diese hat Länge $r + s = l(M') + l(M'')$. □

Satz 5.17. *Sei M ein A-Modul (A ist kommutativer Ring). Dann ist äquivalent:*

1. *$l(M) < \infty$*
2. *M ist artinsch und noethersch.*

Beweis. $1 \Rightarrow 2$:
Aus$l(My\infty)$ folgt , dass jede nicht stationäre Kette endlich ist und damit 2.
$2 \Rightarrow 1$:
Sei o.E. $M \neq 0$, M noethersch.
Dann folgt, dass $\{N \subsetneqq M \text{Untermodul}\}$ besitzt maximale Elemente, etwas M_1.
Induktiv gilt $M = M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq ...$, woebi M_{i-1}/M ist einfach.
Da M artinsch ist folgt, dass es ein $r \in \mathbb{N}_0$ gibt, sodass $M_r = 0$. □

Beispiel 5.18. Sei K Körper, V ein K-Vektorraum. Dann sind äquivalent:

1. $\dim_K(V) y \infty$
2. $l_k(V) y \infty$
3. V ist noethersch
4. V ist artinsch

Es folgt auch, dass $\dim V = l(V)$.

5C Noethersche Ringe

Wenn Anoethersch, so ist auch $A/\mathfrak{a}$ noethersch für alle $\mathfrak{a} \subseteq A$ Ideal und es auch $S^{-1}A$ noethersch für alle $S \subseteq A$ multiplikativ.

Definition 5.19. Sei $\varphi : A \to B$ eine $A-$Algebra.

1. Die A-Algebra B heißt **endlich erzeugt** oder **von endlichem Typ**(v.e.T.), wenn $b_1, ..., b_n \in B$ existierne, die B erzeugen.
   (Äquivalent: $B \tilde{=} A[X-1, ..., X_n]/\mathfrak{a}$ für $\mathfrak{a} \subseteq A[X-1, ...,_n]$ Ideal.)
2. Die $A-$Algebra B heißt **endlich**, falls B als A-Modul endlich erzeugt ist.

Bemerkung 5.20. Sei $\varphi : A \to B$ eine $A-$Algebra

1. B endliche A-Algebra,s o folgt, dass B eine A-Algebra v.e.T.
2. Sei $A = K$ Körper, dann ist $K[X]$ eine K-Algebra v.e.T., aber $K[X]$ ist nicht endliche K-Algebra, da $\dim_K(K[X]) = \infty$.

Satz 5.21 (Hilbertscher Basissatz)**.** *Sei $\varphi : A \to B$ eine A-Algebra v.e.T. und sei A noethersch.*
Dann ist B noethersch.

Beweis.
1. Es gilt B ist genau dann v.e.T. wenn $B \tilde{=} A[X-1, , ..., X_n]/\mathfrak{a}$.
   Also ist o.E. $B = A[X-1, ..., X_n] = (A[X-1, ..., X_{n-1}])[X_n]$.
   Induktiv folgt o.E. $B = A[X]$.
2. Sei $\mathfrak{a} \subseteq A[X]$ Ideal und sei
   $I = \{a \in A \mid \exists f \in \mathfrak{a} \text{ mit } f = aX^d + \text{(Terme niederen Grades)}\}$.
   Da $\mathfrak{a}$ Ideal folgt, dass I Ideal und da A noethersch auch, dass I endlich erzeugt (etwa von $a_1, ..., a_n$).
   Wähle nun $f_1, ..., f_n \in \mathfrak{a}$, sodass $f_i = a_i X^{r_i} +$ (Terme niederer Ordnung).
   Sei nun $\mathfrak{a}' := (f_1, ..., f_n) \subseteq \mathfrak{a}$ und $r := \max\{r_i \mid i = 1, ..., n\}$
3. Für alle $f \in \mathfrak{a}$ existiert $g \in \mathfrak{a}'$, so dass $\deg(f-g) < r$:
   Sei $f = aX^m +$ (Terme niedere Ordnung), $s \in I$.
   Im Fall $m < r$ folgt die Behauptung.
   Falls $m \geq r$ Setze $a = b_1 a_+ ... + b_n a_n$ mit $b_i \in A$. Dann hat

$$f - \underbrace{\sum_{i=1}^{n} b_i f_i X^{m-r_r}}_{\in \mathfrak{a}}$$

Grad $< m$.
Induktiv folgt die Behauptung.

4. Sei $M = A + AX + ... + AX^{n-1}$ eine endlich erzeugter A-Modul.
3 bedeutet, dass $\mathfrak{a} = \mathfrak{a}' + (\mathfrak{a} \cap M)$, sodass (da A noethersch) $\mathfrak{a} \cap M$ als A-Modul endlich erzeugt von $g_1, ..., g_r$.
Dann ist $\mathfrak{a} = (f_1, ..., f_n, g_1, ..., g_r)$.

□

Korollar 5.22. *Sei K Körper. Dann ist $K[X_1, ..., X_n]$ noethersch.*

5D Artin-Ringe

Lemma 5.23. *In einem Artinring A ist jedes Primideal ein maximales Ideal.*

Beweis. Sei $\mathfrak{p} \subset A$ Primiedeal, dann ist $B := A/\mathfrak{p}$ eine nullteilerfreier Artinring.
Behauptung: B ist Körper ($\mathfrak{p}$ ist maximal).
Sei $x \in B, 0 \neq x$. Betraahte die Kette $(x) \supseteq (x^2) \supseteq .....$
Da B Artinring ist gibt es ein $n \in \mathbb{N}$,sodass $(x^n) = x^{n+1}$, also $x^n = yx^{n+1}$ für ein $y \in B$.
Daraus folgt (da x kein Nullteiler) dass $1 = xy$, also $y \in B^\times$. □

Satz 5.24. *Jeder Artinring beseitzt nur endlich viele Primideale.*

Beweis. Sei $\Sigma := \{m_1 \cap ... \cap m_r \mid r \geq 0mm_i \subset A$ maximale Ideale$\}$. Dann folgt aus $A \in \Sigma$, dass $\sigma \neq \emptyset$.
Da A artinsch folgt, dass Σ ein minimales Element beseitzt (etwa $m_1 \cap ... \cap m_n$).
Sei $m \subset A$ ein maximales Ideal. Dann ist $m \cap m_1 \cap ... \cap m_n = m_1 \cap ... \cap m_n$.
Dann ist $m \supset m_1 \cap ... \cap m_n = m_1 \cdot ... \cdot m_n$. Dann gibt es mit **??** ein i, sodass $m \supseteq m_i$. Da m_i minimal folgt, dass es sogar ein i gibt mit $m = m_i$.
Also gilt $\{m \subset A$maximales Ideal$\} = \{m_1, ..., m_n\}$.
Dann folgt, mit 5.23 die Behauptung. □

Lemma 5.25. *Sei A Artinring, dann exitsiert $k \in N$, sodass* $(\mathrm{Nil}(A))^k = 0$.

Beweis. Da A artinsch, wird $\mathrm{Nil}(A) \supseteq \mathrm{Nil}(A)^2 \supseteq ...$ stationär.
Also exitsiert ein $k \in \mathbb{N}$, sodass $\mathrm{Nil}(A)^k = \mathrm{Nil}(A)^{k+1} = ... =: \mathfrak{a}$.
Annahme: $\mathfrak{a} \neq 0$.
Sei $\Sigma = \{b \supseteq A \text{ Ideal} \mid b\mathfrak{a} \neq 0\}$. Dann gtil $A \in \Sigma$. Da A artinsch gibt es ein maximales elemetn $b_0 \in \Sigma$.
Sei nun $x \in b_0$ mit $x\mathfrak{a} \neq 0$. Dann ist $(x)\mathfrak{a} \neq 0$ und es folgt (da $(x) \subseteq b_0$), dass $(x) = b_0$.
Da auch $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$ gilt (da $x\mathfrak{a} \subseteq (x)$), dass $x\mathfrak{a} = (x)$.
Also ist $x = xy$ für ein $y \in \mathfrak{a} = \mathrm{Nil}(A)^k \subseteq \mathrm{Nil}(A)$.
Aber mit $x = xy = xy^2 = ...$ da y nilpotent folgt $x = 0$. □

Theorem 5.26. *Sei A ein Ring dann sind äquivalent*

1. *A ist artinsch*
2. *A ist noethersch und jedes Primiedeal ist maximal*
3. *$l_A(A) < \infty$.*

Beweis. 3) $\Rightarrow$ 1): gilt mit 5.17
3) $\Rightarrow$ 2): ???
1) $\Rightarrow$ 3): Aus 5.24 folgt, dass es endlich viele maximale Ideale gibt, etwa $m_1 \cap ... \cap m_n = m_1 \cdot ... m \cdot m_n$.
Mit 5.25 folgt, dass es ein $k \in \mathbb{N}$ gibt, sodass $m_1^k m_2^k \cdot ... \cdot m_n^k = \mathrm{Nil}(A)^k = (0)$.
Schriebe $(0) = M_1 M_2 ... M_s$ mit $M_i \subset A$ maximal.
Behauptung: Für $j = 0, ..., s$ gilt $l_A(M_1 M_1, ..., M_j) < \infty$:
Für $j = s$ gilt die Behauptung.
Für $j \leq s$ ist

$$0 \to \underbrace{M_1 ... M_j M_{j+1}}_{\text{Länge} < \infty} \to M_1 ... M_j \to \underbrace{(M_1 ... M_j / M_1 ... M_{j+1})}_{\substack{A/M_{j+1}-VR \\ \text{ist artinsch} \\ (\textbf{??} \text{ hat endliche Länge}}} \to 0$$

Es folgt, dass $l_A(M_1 ... M_j) < \infty$.
2) $\Rightarrow$ 3): Sei $l_A(A) = \infty$ und Sei $\Sigma := \{\mathfrak{a} \subseteq A \mid l_A(A/\mathfrak{a}) = \infty\}$ mit $(0) \in \Sigma$.
Dann folgt, da A noethersch, dass Σ maximales Element $\mathfrak{a}_0$ besitzt.
Behauptung: $\mathfrak{a}_0$ ist Primideal.
Sei $a, b \in A : ab \in \mathfrak{a}_0, a \notin \mathfrak{a}_0$.
Betrachte nun die exakte Sequenz

$$0 \to A / \underbrace{\{x \in A \mid xa \in \mathfrak{a}_0\}}_{=:\mathfrak{a}'} \xrightarrow{\cdot a} A/\mathfrak{a}_0 \to \underbrace{A/(\mathfrak{a}_0 + (a))}_{l_A(\cdot)<\infty}$$

Dann folgt $l_A(A/\mathfrak{a}') = \infty$.
Wähle $b \neq \mathfrak{a}_0$. $' \geq \mathfrak{a}_0 + (b) \supsetneqq \mathfrak{a}_0$.
Dann folgt $l(A/\mathfrak{a}') < l(A/\mathfrak{a}_0 + (b)) < \infty$, da $\mathfrak{a}_0$ maximal mit $l(A/\mathfrak{a}_0) = \infty$.
Aus dem Wiederspuch folgt,dass $\mathfrak{a}_0$ ein maximales ideal ist,
sodass $l(A/\mathfrak{a}_0) = 1 \neq \infty$. Widerspruch! □

Korollar 5.27. *Sei A ein lokaler Artinring.*
Dann $\mathrm{Spec}(A) = \{m\} m\ m = \mathrm{Nil}(A)$ *und es gibt ein k, sodass $m^k = 0$, $A \backslash m = A^\times$.*

Beispiel. Sei A ein lokaler noetherscher Ring und $m \subset A$ maximal.
Dann gilt für alle $n \geq 1$, dass A/m^n ein lokaler Artinring ist.
Man kann zeigen, dass $\bigcap_{n \geq 1} m^n = \{0\}$.
Definiere eine Metrik auf A: $0 < \rho 1, \rho \in \mathbb{R}$ mit $d(x, y) := \rho^n$, falls $x - y \in m^n \backslash m^{n+1}$.
Approximation von

$$\hat{A} := \text{Vervollstädnigung von } A \text{ bezüglich } d \text{ durch } A/m^n$$

Beispiel. Sei $\mathbb{Z}(p) := \{\frac{a}{b} \in \mathbb{Q} \mid p \text{ teilt nicht } b\}$ für p Primzahl.

Satz 5.28 (Struktursatz für Artinringe)**.** *Jeder Artinring A ist Produkt von endlichen lokalen Artinringen.*

Beweis. Seien $m_1, ..., m_n \subset A$ die maximalen Ideal.
Dann existier ein $k \in \mathbb{N}$, sodass $0{=}m_1^k ... m_n^k = m_1^k \cap ... \cap m_2^k$. Mit derm Chinisischen Restsatz folge, dass

$$A \xrightarrow{\sim} \prod_{i=1}^{n} \underbrace{A/m_i^k}_{\substack{\text{lokale} \\ \text{Artin-Ringe}}}$$

ist ein Isomorphismus. □

6 Ganzheit

6A Ganze Ring-Homomorphismen

Definition 6.1. Sei $\varphi : A \to B$ ein Ring Homomorphismus:

1. Ein Element $b \in B$ heißt **ganz über** A(bezüglich φ) falls ein normiertes Polynom $f \in A[X]$ exitsiert, sodass $f(b) = b^n + \varphi(a_{n-1})b^{n-1} + ... + \varphi(a_0) = 0$.

2. φ heißt **ganz**, falls jedes Elemtn $b \in B$ ganz über A ist.

Bemerkung 6.2.

1. Sei $\varphi : A \to B$ ein surjektiver Ring Homomorphismus.
   Dann ist φ ganz:
   Sei $b \in B$. Wähle $a \in A$ mit $\varphi(a) = b$.
   Dann $f(b) = 0$, wobei $f = X - a$.

2. Sei $\varphi : A \to B$ ein Ring-Homomorphismus, $b \in B$.
   Dann ist b ganz über A genau dann wenn b ganz über $\varphi(A)$.

Beispiel 6.3. Sei A ein faktorieller Ring, $K = \mathrm{Quot}(A)$. Dann ist $x \in K$ ganz über A genau dann wenn $x \in A$.

Beweis. $\Rightarrow$ Sei $x = \frac{1}{b}$ mit $a, b \in A, b \neq 0$, sodass kein Primielement a und b teilt.
Da x ganz ist folgt

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + ... + a_1\frac{a}{b} + a_0 = 0$$

für $a_0, ..., a_{n-1} \in A$: Multiplikaiton mit b^n ergibt:

$$a^n + ba_{n-1}a^{n-1} + ... + b^{n-1}a_1a + b^na_0 = 0$$

Sei p ein Primteiler von b, also p teilt a^n. Dann teilt p auch a. Widerspruch!
Also $b \in A^\times$, also $x \in A$. □

Beispiel. Sei $A = \mathbb{Z}$, $x = \frac{1}{2}$, $f(x) = 0$ mit $f = 2X - 1$

Bemerkung (Anwendung). Sei $f = X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$.
Falls $f(x) = 0$ für $x \in \mathbb{Q}$, dann $x \in \mathbb{Z}$ und x Teiler von a_0.

Satz 6.4. *Sei $\varphi : A \to B$ ei Ring-Homomorphismus und $b \in B$. Dann ist äquivalent:*

1. *b ist ganz über A.*

2. *$A[b] = \{f(b) \mid f \in A[T]\} = \{\sum_{i=1}^n \varphi(a_i)b^i \mid a_i \in A, n \in \mathbb{N}\}$ ist eine endliche A-Algebra (d.h. $A[b]$ ist als A-Modul endlich erzeugt)*

3. *$A[b]$ ist in einem Unterring $C \subseteq B$ enthalten, sodass C eine endliche A-Algebra ist.*

Beweis.

- 1)⇒2): b ist ganz über A, also gibt es $a_i \in A$, sodass $b^n = -(\varphi(a_{n-1})b^{n-1} + ... + \varphi(a_0))$. Dann auch
$$b^{n+r} = -(\varphi(a_{n-1})b^{n-1+r} + ... + \varphi(a_0)b^r)$$
für alle $r \geq 0$. Dann ist $A[b]$ der A-Modul, der von $1, b, ..., b^{r-1}$ erzeugt wird.

- 2) $\Rightarrow$ 3): $C = A[b]$.

- 3) $\Rightarrow$ 1): Sei $U : C \to C, c \mapsto bc$. Mit 4.36 folgt, dass es $a_i \in A$ gibt, sodass $u^n + a_{n-1}u^{n-1} + ... + a_0 = 0 \in \text{End}_A(C)$. Dann ist aber (mit $b = u(1)$)
$$b^n + \varphi(a_{n-1})b^{n-1} + ... + \varphi(a_0) = 0$$

□

Satz 6.5. *Sei $\varphi : A \to B$ ein Ring Homomorphismus. Dann sind äquivalent:*

1. *φ endlich*
2. *φ ist von endlichem Typ und ganz*
3. *Es gibt $b_1, ..., b_n \in B$, sodass b_i ganz über A ist und $B = A[b_1, ..., b_n]$*

Beweis. durch Ringschluss:

- 1) $\Rightarrow$ 2): nach 6.4
- 2) $\Rightarrow$ 3): Betrachte die Abbildung $A[T_1, ..., T_n] \xrightarrow{\sim} B$, wobei $b_i := \psi(T)$.
- 3) $\Rightarrow$ 1): Sei $B = A[b_1, ..., b_n]$ mit b_i ganz über A.
  Wir wissen, dass $A[b_1]$ eine endliche A-Algebra ist.
  Sei nun $A_k := A[b_1, ..., b_k]$ für $k \leq n$.
  Dann ist $A_k = A_{k-1}[b_k]$

□

Satz 6.6. *Seien die Ring-Homomorphismen $\varphi : A \to B$, $\psi : B \to C$ ganz.*
Dann ist auch $\psi \circ \varphi$ ganz.

Beweis. OE (referenz auf bem) $A \subseteq B \subseteq C$. Sei $x \in C$, also existieren $b_0, ..., b_{n-1} \in B$ sodass $x^n + b_{n-1}x^{n-1} + ... + b_0 = 0$.
Betrachte nun $B' = A[b_0, ..., b_{n-1}]$. Dann ist B' ein endlich erzeugter A-Modul und $B'[x]$ ist ein endlich erzeugter B'-Modul.
(d.h. es gibt surjektive Abbildungen $A^r \to B', (B')^k \to B'[x]$, also auch surjektives $B^{rk} \to B'[x]$)
Also ist $B'[x]$ ein endlich erzeugter A-Modul und damit ist nach 6.4 x ganz über A. □

6B Ganzer Abschluss

Korollar 6.7. *Sei $\varphi : A \to B$ ein Ring-Homomorphismus. Dann ist*

$$C := \{b \in B \mid b \text{ ist ganu über } A\} \tag{6.7.1}$$

ein Unterring von B.

Beweis. Sei $x, y \in C$. Betrachte $A[x,y]$ (ist nach 6.5 endliche A-Algebra).
Dann ist mit 6.5 die Abbildung $A \to A[x,y]$ ganz.
Insbesondere sind $x \cdot y, x \pm y \in A[x,y]$ ganz über A. □

Definition 6.8.

1. Sei $\varphi A \to B$ ein Ring-Homomorphismus. Der Unterring C (aus 6.7.1) wird der **ganze Abschluss von A in B** genannt.
2. A heißt **ganz abgeschlossen**, falls $C = \varphi(A)$.

Korollar 6.9. *Sei $\varphi : A \to B$ ein Ring,Homomorphismus und sei C der ganze Abschluss von A in B, dann ist C ganz abgeschlossen.*

Beweis. Sei $b \in B$ und b ganz über C (bezüglich der Inklusion $C \subseteq B$). Da C ganz über Aist, ist auch b ganz über A (vgl 6.6). Also ist $b \in C$. □

Bemerkung 6.10. Sei $\varphi : A \to B$ ein ganzer Ring-Homomorphismus, $\mathfrak{b} \subseteq B$ ein ideal. Dann ist

$$A/\varphi^{-1}(\mathfrak{b}) \to B/\mathfrak{b}$$

auch ganz.

Satz 6.11. *Sei $\varphi : A \to B$ ein Ring-Homomorphismus, $C \subseteq B$ der Ganze Abschluss von A in B und sei $S \subseteq A$ ein multiplikative Teilmenge.*
Dann ist $\varphi(S)^{-1}C$ der ganze Abschluss von $S^{-1}A$ in $\varphi(S)^{-1}B$.
Insbesondere ist $\varphi(S)^{-1}B$ ganz über $S^{-1}A$, falls φ ganz ist.

Beweis. OE $A \subseteq B \subseteq C$. Wir zeigen zuerst, dass $S^{-1}C$ ganz über $S^{-1}A$.
Sei dazu $\frac{c}{s} \in S^{-1C}$. Es existieren a_i, sodass $c^n a_{n-1} c^{n-1} + ... + a_0 = 0$. Dann ist

$$\left(\frac{c}{s}\right)^n + \left(\frac{c}{s}\right)^{n-1} \underbrace{\left(\frac{a_{n-1}}{s}\right)}_{\in S^{-1}A} + ... + \frac{a_0}{s^n}$$

ist Ganzheitsgleichung für $\frac{c}{s}$ über $S^{-1}A$, also ist $\frac{c}{s}$ ganz über $S^{-1}A$.
Sei nun $\frac{b}{s}$ sin $S^{-1}B$ ganz über $S^{-1}A$, d.h. es gibt $a_i \in A, s_i \in S$, sodass

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}} \left(\frac{b}{s}\right)^{n-1} + ... + \frac{a_0}{s_0} = 0 \tag{$\star$}$$

Sei $t = s_0 \cdot ... \cdot s_{n-1}$. Multipliziere $(\star)$ mit $(ts)^n$, dann ist

$$(tb)^n + a_{n-1}x_1(tb)^{n-1} + ... + x_n = 0$$

(wobei $x_1, ..., x_n \in A$)Ganzheitsgleichung von $t \cdot B$ über A. □

Definition 6.12. Ein Nullteiler freie Ring heißt **ganz Abgeschlossen**(ohne Spezifizierung worin) oder **normal**, falls A ganz abegschlossen in Quot(A).

Satz 6.13. *Jeder faktorielle Ring ist normal*

Beweis. in Beispiel 6.3. □

6C Going-Up

Satz 6.14. *Sei B ein nulltieiler freier Ring und $A \subseteq B$ ein Unterring und sei B ganz über A.*
Dann ist A genau dann ein Körper wenn B ein Körper ist.

Beweis.

- Sei A Körper und $y \in B$ mit $y \neq 0$. Nehem Ganzheitsgleichung von y über A mit minimalem Grad:

$$y^n + a_{n-1}y^{n-1} + ... + a_0 = 0$$

Da B nullteilerfrei ist, gilt $a_0 \neq 0$.
(Nehme an , dass $a_0 = 0$, dann $y(y^{n-1+a_{n-1}y^{n-2}+...+a_1}) = 0$ also Grad nciht minimal)
Sei $\delta := -a_0^{-1}(y^{n-1} + a_{n-1}y^{n-2} + ... + a_1) \in B$ mit $\delta y = 1$. Also ist B Körper.

- Sei nun B Körper, $x \in A \backslash \{0\}$. Es gilt $x^{-1} \in B$, also ganz über A.
Also finden wir zur Gleichung $x^{-m} + a_{m-1}x^{-m+1} + ... + a_0 = 0$ durch Multiplikation mit x^{m-1}

$$x^{-1} + \underbrace{a_{m-1} + a_{m-2} + ... + a_0 x^{m-1}}_{\in A} = 0$$

Also liegt $x^{-1} \in A$.

□

Korollar 6.15. *Sei $\varphi : A \to B$ eine ganzer RIng-Homomorphismus. Sei $q \subseteq B$ Primideal, $p := \varphi^{-1}(q)$. Damit ist q maximal gdw p maximal.*

Beweis. Es gilt $A/p \to B/q$ ist ganz. Satz 6.14 gibt uns, dass A/p genau dann Körper ist, wenn B/q Körper ist. Es folgt die Behauptung □

Korollar 6.16. *Sei $\varphi : A \to B$ ein ganzer Ring-Homomorphismus, seien $q \subseteq q' \subset B$ Primideale, so dass $p := \varphi^{-1}(q) = \varphi^{-1}(q')$. Dann gilt $q = q'$*

Beweis. In $A_p = S^{-1}A, S = A \backslash p$ ist pA_p maximal. Betrachte

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "a \mapsto \frac{a}{1}"'] & B \arrow[d, "b \mapsto \frac{b}{1}"] \\
A_p \arrow[r, "\psi = S^{-1}\varphi"'] & B_p
\end{tikzcd}$$

Wobei $pA_p \subset A_p$ und $qB_p \subseteq B_p = \varphi^{-1}SB$ und auch $qB_p \subseteq qB_p$ Primideal.
Mit 6.11 folgt ψ ist ganz.
Also gilt OE $p \subset A$ ist maximal, sodass mit 6.15 folgt, dass q, q' maximal sind und da $q \subseteq q'$ gilt $q = q'$. □

Satz 6.17. *Sei $\varphi : A \to B$ ein injektiver ganzer Ring Homomorphismus. Dann existiert für jedes Primideal $p \subset A$ ein Primideal $q \in B$ mit $\varphi^{-1}(q) = p$.*
(D.h. $\mathrm{Spec}(B) \to \mathrm{Spec}(A), q \mapsto \varphi^{-1}(q)$ *ist surjektiv.)*

Beweis. Ersetze A durch A_p, dann gilt OE, dass $p \subset A$ maximal und A lokal ist.
Da φ injketiv ist folgt $B \neq 0$.
Also existiert ein maximales Ideal $q \subseteq B$ und mit 6.15 ist $\varphi^{-1}(q)$ maximal, also $\varphi^{-1}(q) = p$. $\square$

Theorem 6.18 (Going Up). *Sei $\varphi : A \to B$ ein ganzer injektiver Ring-Homomorphismus und seien $n \geq m \geq 0$ ganze Zahlen. Sei $p_i \subsetneqq ... \subsetneqq p_m \subsetneqq ... \subsetneqq p_n \subset A$ eine Kette von Primidealen und sei $q_1 \subseteq ... \subseteq q_n \subset B$ eine Kette von Primidealen mit $\varphi(q_i) = p_i$ für $i = 1, ..., m$.*
Dann gilt $q_1 \subsetneqq ... \subsetneqq q_m$ und es existiert eine Kette von Primidealen $q_1 \subsetneqq ... \subsetneqq q_m \subsetneqq q_{m+1} \subsetneqq ... \subsetneqq q_n \subset B$ mit $\varphi^{-1}(q) = p_i$ für alle $i = 1, ..., n$.

Beweis. Sei OE $n > m$, $n_1 = 1, m = 0$. Dann folgt mit 6.17, dass $q_1 \subsetneqq ... \subsetneqq q_m$:
Vollständige Induktion: Sei OE $m = 1, n = 2$. Betrachte

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d] & B \arrow[d] \\
A/p_1 \arrow[r, "\overline{\varphi}"] & B/q
\end{tikzcd}$$

Wobei $\overline{\varphi}$ ganz und injektiv ist, da $\varphi^{-1}(q_i) = p_1$ und $p_2/p_1 \subseteq A/p_1$.
Dann folgt mit 6.17, dass es das Primideal $\overline{q_2} \subset B/q_i$ gibt mit $\overline{\varphi}^{-1}(\overline{q_2}) = p_2/p_1$.
Dass ist $\overline{q_2} \hat{=} q_2 \subset B$, wobei q_2 Primideal mir $q_2 \supseteq q_1$ und $\varphi^{-1}(q_2)p_2$. $\square$

7 Irreduziblität

7A Satz von Gauß

Erinnerung 7.1.

1. Sei A ein nullteilerfreier Ring. Ein Element $p \in A$ heißt
   (a) **irrefuzibel**, falls $0 \neq p \notin A^\times$ und falls $p = ab$ mit $a, b \in A$, so gilt $a \in A^\times$ oder $b \in A^\times$.
   (b) **Primelelement**, falls $p \neq 0$ und (p) ist Primideal.

   Es gilt, wenn p Primelement ist, so ist p irreduzibel.
2. A heißt **faktoriell**, falls er die folgenden äquivalenten Bedingung erfüllt:
   (a) Jedes $0 \neq a \notin A^\times$ ist Produkt von irreduziblen Elemente und diese Zerlegung ist eindeutig bis auf Reihenfolge und Multiplikation mit Einheiten.
   (b) Jedes Elemente $o \neq a \notin A^\times$ ist Produkt von Primelemten.
   (c) Jedes Irreduzible Element ist ein Primelement und jede aufsteigende Kette von Hauptidealen wird stationär.

Beweis.

- b)⇒a): Einführung in die Algebra (Beweis HIR sind faktoriell)
- a)⇒c):

1. Sei $p \in A$ irreduzibel. Seien $a, b \in A$ mit $ab \in (p)$.
   Setze $ab = dp$ mit $d \in A$. Seien $a = p_1 ... p_r$, $b = q_1 ... q_s$ und $d = l_1 ... l_t$ irreduzible Zerlegungen. Dann

$$p_1 .. p_r q_1 ... q_s = p l_1 ... l_t$$

   Aus der eindeutigkeit folg, dass es ein i gibt sodass $(p) = (p_i)$ oder ein j, sodass $(p) = (q_j)$.
   Daraus folgt, p teilt a oder b.

2. gibt, dass jdese Elemente $\neq 0$ hat nur endlich viele Teiler. (Bis auf Multiplikation mit Einheiten).

Mit Anderen Worten: Für jedes Hauptideal $\mathfrak{a} \neq 0$ existieren nur endlich viele Hauptideal, die $\mathfrak{a}$ enthalten.
$\Rightarrow$ Jede aufsteigende Kette von Hauptidealen wird stationär.

- c)$\Rightarrow$ b): Sei $\Sigma := \{(a) \mid 0 \neq a \in A^\times und a ist nicht Produkt von irreduziblen Elementen\}$.
  Angenommen $\Sigma \neq 0$:
  Dann folgt mit 5.1

$\square$

Beispiel 7.2. Jeder Hauptidealring ist faktoriell. Insbesondere auch $\mathbb{Z}, K[X]$

Definition 7.3. Sei A ein Ring, $f = a_m X^m + ... + a_1 X + a_0 \in A[X]$ heißt **primitiv**, falls $(a_1, ..., a_n) = A$.

Beispiel. 1. Sei A faktoriell. Dann ist f genau dann Primitiv, wenn kein Primelement alle a_i teilt.

2. Seien $f, g \in A[X]$. Dann sind f, g genau dann primitv, falls fg primitiv.

Definition 7.3. Sei A faktoriell. Ein $c(f) \in A$ heißt **Inhalt von** f, falls $c(f)$ ein größter gemeinsammer Teiler von $a_1, ..., a_0$ ist.

Bemerkung. Also ist g genau dann primitav, falls $c(f) \in A^\times$.
Für $f \in A[X]$ gilt, dass $f = c(f)\tilde{f}$ mit $\tilde{f}$ primitv.

Bemerkung. Sei $f = 3X^{1000} + 30X^7 + 21X + 27$, dann $c(f) = 3$ oder -3.
Dann $f = 3\tilde{f}$, also $\tilde{f} = X^{1000} + 10X^7 + 7X + 9$.

Theorem 7.4 (Satz von Gauß)**.** *Sei A ein faktorieller Ring. Dann ist auch $A[X]$ faktoriell.*
Die irreduziblen Elemente von $A[X]$ sind:

1. *$p \in A$ irreduzibel und*

2. *$f \in A[X]$ primitv, sodass $f \in \mathrm{Quot}(A)[X]$ irreduzibel ist.*

Beispiel. Sei $A = \mathbb{Z}$,

- $2X + 4 \in \mathbb{Z}[X]$ ist reduzibel, da $2X + 4 = 2(X + 2)$
- $X^3 - 5 \in \mathbb{Z}[X]$ ist primitv und irreduzibel in $\mathbb{Q}[X]$

Beweis. 1. Seien $f, g \in K[X] \setminus \{0\}$. Schreibe $f = c(f)\tilde{f}$, $g = c(g)\tilde{g}$ mit $\tilde{f}, \tilde{g}$ primitiv. Dann $fg = c(f)c(g)\tilde{g}\tilde{f}$, sodass $c(fg) = c(f) = c(g)$ gilt.

2. Behauptung:$p \in A$ ist irreduzibel, dann ist $p \in A[X]$ Primelement:

$$A[X]/pA[X] = (A/p)[X]$$

ist nullteilerfrei (da A/p nullteilerfrei ist). Dann ist $p \in A$ prim.

3. Sei $q \in A[X]$ primitiv, $q \in K[X]$ irreduzibel.
Behauptung: $qK[X] \cap A[X] = qA[X]$:

   - "$\supseteq$" ist klar
   - "$\subseteq$": Sei $f \in K[X]$ mit $qf \in A[X]$, sei $f = c(f)\tilde{f}$ mit $\tilde{f}$ primitv. Dann gilt $c(qf) \in A$ und $c(qf) = c(q)c(f)$ wobei $c(q) \in A\times$.
   Dann folgt, dass $c(q)c(f) = c(f)$ und damit $f \in A[X]$.

   Die Behauptung gilt also genau dann wenn $A[X]/qA[X] \to K[X]/qK[X]$ injektiv ist.
   Also ist $q \in A[X]$ Primelemnt.

4. Jedes $f \in A[X]$ mit $0 \neq f \notin A^\times$ ist Produkt der Primelemente von (a) und (b).
Schrieeb $f = c(f)\tilde{f}$, $c(f)$ ist Produkt von Primelementen in (a) und $\tilde{f}$ ist primitv.
Sei $\tilde{f} = g_1, ..., g_r$ mit $g_i \in K[X]$ irreduzibel, $g_i = c_i\tilde{g}_i$, $c_i \in K^\times$, $\tilde{g}_i$ primitiv.
Es folgt, dass $\tilde{f} = c_1...c_r\tilde{g}_1...\tilde{g}_r$.
Da $c(\tilde{f}) \in A^\times$ und $c(\tilde{g}_1...\tilde{g}_r) \in A^\times$ ist auch $c_1...c_r \in A^\times$.
Mit 7.1 folgt die Aussage.

□

Korollar 7.5. *Sei A ein faktorieller Ring. Dann ist $A[X_1, ..., X_n]$ faktoriell. Insbesondere folgt dies wenn A Körper.*

7B Irreduziblitätskriterien

Sei K Körper, $f \in K[X]$, $f \neq 0$.

0. Sei $\deg(f) = 0$, dann f nicht irreduzibel in $K[X]$, da $f \in K[X]^\times = K^\times$.
1. Sei $\deg(f) = 1$, dann ist f immer irreduzibel in $K[X]$.
2. Sei $\deg(f) = 2$ oder $\deg(f) = 3$, dann ist f genau dann reduzibel, wenn f eine Nullstelle hat.
3. Sei $\deg(f) > 1$ und f habe eine Nullstelle, dann ist f reduzibel

Satz 7.6 (Reduziblitätskriterium)**.** *Sei A ein faktorieller Ring, $K = \mathrm{Quot}(A)$, $f = a_nX^n + ... + a_1X + a_0 \in A[X]$, zu $p \in A$ Primelement mit p teilt nicht a_n. Sei $\overline{f} \in A/p[X]$ das Bild von f.
Dann folgt aus $\overline{f}$ irreduzibel in $A/p[X]$, dass f in $K[X]$ irreduzibel ist.*

Beweis. Betrachte zuerst f primitiv:
Sei $f \in K[X]$ reduzibel, dann folgt mit 7.4, dass f in $A[X]$ reduzibel ist.
Also gibt es $g, h \in A[X]$, mit $\deg(g), \deg(g) \geq 1$, sodass $f = gh$.
Da der Führende Koeffizient von f nach Voraussetzung nicht durch p teilbar ist, sind auch die Führenden Koeffizienten von g, h nicht durch p teilbar.
Da $\deg(\overline{g}) = \deg(g) \geq 1$ und $\deg(\overline{h}) = \deg(h) \geq 1$ folgt, dass $\overline{f} = \overline{g}\overline{h}$ reduzibel ist.

Allgemeiner Fall: Schriebe $f = c(f)\tilde{f}$ mit $c(f) \in A \setminus \{0\}$ und $\tilde{f}$ primitiv.
f ist genau dann in $K[X]$ reduzibel, wenn $\tilde{f}$ in $K[X]$ reduzibel ist.
Im gezeigten Spezialfall folgt aus $\tilde{f}$ ist reduzibel in $A/p[X]$, dass $\overline{f} = \overline{c(f)}\overline{\tilde{f}}$ reduzibel ist. □

Beispiel. 1. Sei $f = 3X^4 + 2X^2 + 7X^2 + X - 5 \in \mathbb{Z}[X]$. Dann gilt $\mod 2$:

$$f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$$

Betrachte nun die Reduziblen Polynome mit $\deg = 2$: $\{X^2 + X + 1, X^2 + 1, X^2\}$, wobei deren Quadrate keien Teiler von f sind.
Also ist f irreduzibel.

2. Sei $f = X + Y^2 + YX - 2Y + 3 \in \mathbb{Q}[X, Y]$ ist gleich $XY^2 + (X-2)Y + 3 \in (\mathbb{Q}[X])[X]$ modulo $X - 2$ gilt:
$2Y^2 + 3 \in Q[Y] = \mathbb{Q}[X, Y]/(X - 2)$ ist irreduzibel, also ist f irreduzibel.

Satz 7.7 (Eisensteinkriterium)**.** *Sei A faktoriell, $f = a_nX^n + ... + a_1X + a_0 \in A[X]$ primitiv und es existiert ein Primelement $p \in A$, sodass*

1. *p teilt nicht a_n*
2. *p teil a_i für alle $i = 0, ..., n-1$*
3. *p^2 teilt nicht a_0*

Dann ist f irreduzibel in $\mathrm{Quot}(A)[X]$.

Beweis. Sei f reduzibel in $A[X]$,$f = gh$ für $g, h \in A[X]$ mit $\deg(g), \deg(f) \geq 1$ (und $< n$).
Modulo p gilt: $\overline{a}_nX^n = \overline{f} = \overline{g}\overline{h} \in A/p[X]$ und $a_n \neq 0$.
Da die irreduzible Zerlegung Eindeutig in $\mathrm{Quot}(A/p)[X]$ ist:
$\overline{g} = uX^m$, $\overline{h} = vX^r$, mit $u, v \neq 0$ und $m, r > 0$.
Dann sind die Absoluten Koeffizienten von g, h duch p Teilbar, was einen Widerspruch zu 3) darstellt. □

Beispiel 7.8. Sei A faktorielle $p \in A$ prim, $n \geq 1$.
Dann ist $X^n - p$ irreduzibel.

8 Algebraische Körpererweiterungen

8A Körpererweiterungen

Definition 8.1. Eine K-Algebra $\iota : K \hookleftarrow L$ heißst **Körpererweiterung**, falls L Körper ist. (Also $K \to L$ injektiv).
Eine **Teilerweiterung** ist ein Unterkörper M von L, sodass $\iota(K) \subset M$.

Hier könnte ~~Ihre Werbung~~ die VL vom 12.12.2016 stehen

Definition 8.17. Sei A eine K-Algebra, $a \in A$ algebraisch. Betrachte den K-Algebra Homomorphismus $\varphi : K[X] \to A$, $f \mapsto f(a)$. Dann ist $\mu_{a,K} \in K[X]$ das **Minimalpolynom von a über K**, wenn $\operatorname{Ker}(\varphi) = (\mu_{a,K})$.

Bemerkung. Sei A eine K-Algebra, $a \in A$. Betrachte den K-Algebra Homomorphismus $\varphi : K[X] \to A$, $f \mapsto f(a)$. Dann ist

$$\operatorname{Im}\varphi = \{f(a) \in A \mid f \in K[X]\} = K[a]$$

und es sind äquivalent:

1. a ist algebraisch
2. φ ist nicht injektiv
3. $\operatorname{Ker}(\varphi) = (\mu_{a,K})$ für ein eindeutiges, normiertes Polynom $\mu_{a,K} \in K[X]$.
4. $[K[a] : K] < \infty$.
   In diesem Fall gilt $[K[a] : K] = \deg(\mu_{a,K})$

Beweis.
- 1)$\Leftrightarrow$2)$\Leftrightarrow$3) ist klar.
- 3)$\Rightarrow$4): Es gilt, 3) ist äquivalent dazu, dass $K[a] = K[X]/(\mu_{a,K})$ für normierte Polynome $\mu_{a,K}$.
  Es folgt, dass $K[a]$ eine endliche K-Algebra ist mit $[K[a] : K] = \deg(\mu_{a,K})$.
- 4)$\Rightarrow$2): gilt, da sonst $K[a] \tilde{=} K[X]$.

□

8.18 Bestimmung von $\mu_{a,K}$ I

Sei A eine K-Algebra, $a \in A$ algebraisch. Sei $f \in K[X]$ mit $f(a) = 0$, dann ist $\mu_{a,K}$ ein Teiler von f. Also gilt für $f \in K[X]$:
$\mu_{a,K}$ ist genau dann gleich f, wenn f normiert $f(a) = 0$ und $\deg(f) \leq [K[a] : K]$.

Beispiel. Sei $A = K \times K$, (mit $x \mapsto (x, x)$), sei $a = (1, 0)$. Dann ist $\mu_{a,K} = X^2 - X = X(X - 1)$.

Proposition 8.19. Sei $K \hookrightarrow K$ eine Körpererweiterung, $a \in L$.
Dann ist a genau dann algebraisch über K, wenn $K[a] = K(a)$ ($\Leftrightarrow$ $K[a]$ Körper).

Bestimmung von $\mu_{a,K}$ II

Für $f \in K[X]$:
$f = \mu_{a,K}$ genau dann wenn f normiert, $f(a) = 0$ und f irreduzibel ist.

Beweis. "$\Rightarrow$": Sei a algebraisch, dann ist $K[a] \subseteq L$ nullteilerfrei und ganz über K.
Dann folgt mit **??**, dass $K[a]$ ein Körper ist, sodass $K(a) = K[a]$.
Ferner gilt $K[a] = K[X]/(\mu_{a,K})$ ist genau dann Körper wenn $\mu_{a,K}$ eine maximales Ideal, was äquivalent dazu ist, dass $\mu_{a,K}$ irreduzibel ist. "$\Leftarrow$": Sei a transzendent, dann folgt mit **??**, dass $K[X] \xrightarrow{\sim} K[a]$, dann ist $K[a]$ kein Körper. □

Beispiel 8.20. Sei $K = \mathbb{Q}$.

1. Sei $a = \sqrt{2} \in \mathbb{R}$, dann ist $\mu_{a,\mathbb{Q}} = X^2 - 2$ (da $X^2 - 2$ irreduzibel, normiert und $(\sqrt{2})^2 - 2 = 0$ ist.)
   Allgemein: Sei p Primzahl, $a = \sqrt[n]{p} \in \mathbb{C}$. Dann ist $\mu_{a,\mathbb{Q}} = X^n - p$ (da $X^n - p$ mit 7.7 irreduzibel ist.)

2. Sei $a = \sqrt[4]{2}$, dann ist $\mu_{a,\mathbb{Q}[\sqrt{2}]} = X^2 - \sqrt{2} \in \mathbb{Q}[\sqrt{2}][X]$.

3. Sei p Primzahl, $\zeta \in \mathbb{C}$, $\zeta \neq 1$ mit $\zeta^p = 1$.
   (Dann $\zeta = e^{\frac{2\pi i k}{p}}$ für $k = 1, ..., p-1$) Sei $f = X^p - 1$, dann $f(\zeta) = 0$ und
   $$f = (X-1)(X^{p-1} + ... + X + 1)$$
   ist irreduzible Zerlegung.
   Da $\zeta \neq 1$, gilt $\mu_{a,K} = X^{p-1} + ... + X + 1$.
   Also $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$.

8E Algebraische Erweiterungen

Definition 8.21. Eine K-Algebrau A heißt **algebraisch über** K, falls A eine ganze K-Algebra ist. (d.h. jedes $a \in A$ ist algebraisch über K).

Proposition 8.22. Sei A eine K-Algebra. Dann sind äquivalent:

1. $[A : K] < \inf$ (d.h. A ist endliche K-Algebra)

2. A ist algebraisch und endlich erzeugt K-Algebra.

3. Es gibt algebraische Elemente $a_1, ..., a_n \in A$, sodass $A = K[a_1, ..., a_n]$

Beweis. Siehe 6.4 □

Proposition 8.23. Sei $K \hookrightarrow L$ eine Köerpererweiterung und $L \hookrightarrow A$ ist L-Algebra, dann gilt:
A ist algebraisch über K genau dann, wenn L algebraische Erweiterung von K und A algebraisch über L.

Beweis. Siehe 6.6 □

8F Algebraischer Abschluss

Definition 8.24. Ein Körper K heißt **algebraisch abgeschlossen**, falls die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jedes Polynom $f \in K[X]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in K.

2. Jedes Polynom $f \in K[X]$ mit $\deg(g) \geq 1$ ist Produkt von Polynomen vom Grad 1.

3. Jedes irreduzible Polynom in $K[X]$ hat Grad 1.

4. Jede algebraische Körpererweiterung von K hat Grad 1.

Beweis.
- 1)⇔2)⇔3).

- 3)⇒4): Sei $K \hookrightarrow L$ algebraische Körpererweiterung, $a \in L$.
  Dann folgt aus 3), dass $\mu_{a,K}$ Grad 1 hat, also $\mu_{a,K} = X - a \in K[X]$. Also $a \in K$.

- 4)⇒3): Sei $f \in K[x]$ irreduzibel.
  Dann ist $K[X]/(f)$ eine endliche Körpererweiterung mit $[K[X]/(f) : f] = \deg(f)$.
  Es folgt mit 4), dass $\deg(f) = 1$.

□

Beispiel 8.25. $\mathbb{C}$ ist Algebraisch abgeschlossen.

Definition 8.26. Sei K Körper. Eine Algebraische Erweiterung $K \hookrightarrow \overline{K}$ heißt **algebraischer Abschluss von** K, wenn $\overline{K}$ abgeschlossen ist.

Beispiel. 1. $\mathbb{R} \hookrightarrow \mathbb{C}$ ist algebraischer Abschluss.

2. $\mathbb{Q} \hookrightarrow \mathbb{C}$ ist kein algebraischer Abschluss.

Theorem 8.27. *Sei K Körper.*
Dann existiert ein algebraischer Abschluss von K.

8G Fortsetzung von Körperhomomorphismen

Bemerkung 8.28. Seien $K \hookrightarrow A_1$, $K \hookrightarrow A_2$ K-Algebren und sei

$$\mathrm{Hom}_{K-\mathrm{Alg}}(A_1 A_2) = \{\varphi : A_1 \to A_2 | \varphi \text{ist } K\text{−Algebra-Homomorphismus}\}$$

Jedes $\varphi \in \mathrm{Hom}_{K-\mathrm{Algebra}}$ ist K-linear.
Falls $A - 1 = L$ ein Körper, $A_2 \neq 0$, dann ist φ injektiv und es gilt

1. $[L : K] \leq [A_2 : K]$
2. Falls $[L : K] = [A_2 : K] \leq \infty$, dann ist φ ein Homomorphismus von K-Algebren.

Satz 8.29. *Sei $K \hookrightarrow L$ und $K \hookrightarrow L'$ Körpererweiterungen. Sei $a \in L$ algebraisch über K.*

1. *Sei $\varphi : K[a] \to L'$ ein K−Algebra-Homomorphismus.*
   Dann ist $\varphi(a) \in L'$ algebraisch und $\mu_{\varphi(a),K} = \mu_{a,K}$.
2. *Es gibt die Bijektion*

$$\begin{aligned} Inhalt\, \mathrm{Hom}_{K-Algebra}(K[a], L') &\to \{a' \in L' | \mu_{a,K} = 0\} \\ \varphi &\mapsto \varphi(a) \end{aligned}$$

Insbesondere gilt

$$\deg(\mu_{a,K}) = [K[a] : K] \geq \#\, \mathrm{Hom}_{K-Algebra}(K[a], L')$$

mit Gleichheit genau dann wenn $\mu_{1,K}$ in L' vollständig in Linearfaktoren zerfällt und alle Nullstellen von $\mu_{a,K}$ in L' paarweise verschieden sind.

Beweis. Sei $\varphi : K[a] \to L'$ ein K-Algebra-Homomorphismus.
Dann ist $\mu_{a,K} = 0$, denn:
Sei $\mu_{a,K} = X^+ \lambda_{n-1} X^{n-1} + ... + \lambda_0 \in K[X]$.

$$\begin{aligned}\mu_{a,K}(\varphi(a)) &= \varphi(a)^n + \lambda_{n-1}\varphi(a)^{n-1} + ... + \lambda_0 \\ &= \varphi(a^n) + \varphi\left(\lambda_{n-1}a^{n-1}\right) + ... + \lambda_0 \\ &= \varphi\left(a^n + \lambda_{n-1} + ... + \lambda_0\right) \\ &= \varphi(0) = 0\end{aligned}$$

Also ist $\varphi(a)$ algebraisch und $\mu_{\varphi(a),K}$ teilt $\mu_{a,K}$.
Da $\mu_{a,K}$ irreduzibel ist folgt, dass $\mu_{\varphi(a),K} = \mu_{a,K}$.
Dies zeugt (1) und dass die Abbildung $\varphi \mapsto \varphi(a)$ in (2) wohldefiniert ist.

Sei $a' \in L'$ mit $\mu_{a,K}(a) = 0$, dann teilt $\mu_{a',K}$ das Polynom $\mu_{a,K}$, also $\mu_{a',K}\mu_{a,K}$.

$$K[a] = \mathrm{Ker}[X]/(\mu_{a,K}) = K[X]/(\mu_{a',K}) = K[a'] \subseteq L$$

stellen K-Algebra Homomorphismen $\varphi : K[a] \to L'$ mit $\varphi(a) = a'$ dar.
φ ist eindeutig, da die K-Algebra $K[a]$ durch a erzeugt wird. □

Satz 8.30. *Sei $K \hookrightarrow L$ eine algebraische Erweiterung und sie L' eine algebraische abgeschlossene Erweiterung von K.*

1. *Dass existiert ein $K-$Algebra-Homomorphismus $\varphi : L \hookrightarrow L'$.*
2. *Falls L und L' algebraisch Abschlüssen von K sind, ist φ ein Homomorphismus.*

Korollar 8.31. *Sei $\overline{K}$ und $\overline{K}'$ algebraische Abschlüsse von K. Dann existiert ein K-Algebra-Homomorphismus $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$.*

Beweis. Sei $\mathfrak{F} := \{(Z,\tau) \mid K \hookrightarrow Z \subseteq L$ Teilkörper und $\tau : Z \hookrightarrow L'$ K-Algebra-Homomorphismen$\}$.
Für $(Z,\tau).(Z',\tau')$ schreibe

$$(Z,\tau) \leq (Z',\tau') :\Leftrightarrow Z \subset Z', \tau = \tau'|_Z$$

Also ist $\leq$ eine partielle Ordnungn auf $\mathfrak{F}$.
Und da $(K, K \hookrightarrow L') \in \mathfrak{F}$ gilt $\mathfrak{F} \neq \emptyset$.
Sei nun $\xi \subseteq \mathfrak{F}$ eine total geordnete Teilmenge, dass ist

$$\left(\bigcup_{(Z,\tau_Z)\in\xi} Z, \tau\right)$$

mit $\tau|Z = \tau$ für alle $(Z,\tau_Z) \in \xi$ eine obere Schranke in $\mathfrak{F}$.
Mit 1.4 folgt, dass es ein maximales Element $(Z_0,\tau_0) \in \mathfrak{F}$ gibt.

Behauptung: $Z_0 = L$ (setze dann $\varphi := \tau_0$)
Angenommenes existert ein $a \in L \setminus Z_0$. Dann ist a algebraisch über Z_0 und

$$\mathrm{Hom}_{Z_0}(Z_0[a], L') \overset{\leftrightarrow}{\textbf{??}} \{a' \in L' \mid \mu_{a,Z_0}(a') = 0\} \neq \emptyset$$

Also existiert ... □

9 Normale und separable Körpererweiterungen

9A Zerfällungskörper

Definition 9.1. Sei $\mathfrak{F} \subseteq K[x]$ eine Menge nicht konstanter Polynome. Eine Körpererweiterung $K \hookrightarrow L$ heißt **Zerfällungskörper** von $\mathfrak{F}$, falls gilt

1. Jedes $f \in \mathfrak{F}$ zerfällt über L vollstädnig ein Linearfaktoren
2. Für $f \in \mathfrak{F}$ sei $R_f := \{a \in L | f(a) = 0\}$. Dann ist

$$L = K \left(\bigcup_{f \in \mathfrak{F}} R_f \right)$$

Bemerkung. Dann ist $L = K \left[\bigcup_{f \in \mathfrak{F}} R_f \right]$ eine algebraische Erweiterung von K.

Beispiel 9.2. Sei $f \in K[X], \deg(f) \geq 1$ und Sei $\overline{K}$ ein algebraischer Abschluss von K.
Seien $a_1, ..., a_{\in}\overline{K}$ die Nullstellen von F.
Dann ist $K[a_1, ..., a_n] \subseteq \overline{K}$ ein Zerfällungskörper von f.

Proposition 9.3. Sei $\mathfrak{F} \subseteq K[X]$ eine Menge nicht konstanter Polynome.

1. Dann existiert ein Zerfällungskörper von $\mathfrak{F}$.
2. Seien L_1 und L_2 Zerfällungskörper von $\mathfrak{F}$, seien $\overline{L}_1$ und $\overline{L}_2$ algebraische Abschlüsse von L_1 bzw L_2 und sei $\varphi : olL_1 \to \overline{L}_2$ ein K-Algebra-Homomorphismus. Dann ist $\varphi(L_1) = L_2$

Beweis.
1. Sei $\overline{K}$ ein algebraischer Abschluss und sei $S := \{a \in \overline{K} \mid \exists f \in \mathfrak{F} : f(a) = 0\}$.
   Dann ist $K(S)$ Zerfällungskörper von $\mathfrak{F}$.
2. Seien $\overline{L}_1$ und $\overline{L}_2$ bereits algebraische Abgeschlüsse von K.
   Dann folgt 8.30, dass φ Homomorphismus ist.
   Sei $S_1 := \{a \in L_1 \mid \exists f \in \mathfrak{F} : f(a) = 0\}$.
   Es folgt, dass $L_1 = K(S_1)$.
   Zeige: $\varphi(S_1) \subseteq L_2$. Sei: $f \in \mathfrak{F}$, $a \in L_1$ Nullstelle von f.
   Dann ist $f(\varphi(a)) = \varphi(f(a)) = 0$. Also $\varphi(a) \in \overline{L}_2$, also Nullstelle von f ist.
   Es folgt $\varphi(a) \in L_2$.
   Also folgt $\varphi(S_1) \subseteq L_2$, dann ist $\varphi(L_1) \subseteq L_2$.
   Analog für $\varphi^{-1} : \varphi^{-1}(L_2) \subseteq L_1$.
   Zusammen folgt, dass $\varphi(L_1) = L_2$.

□

Korollar 9.4. *Sei $\mathfrak{F} \subseteq K[X]$ eine Menge nicht konstatnert Polyome, sei Ω Körpererweiterung von K und seien $L_1, L_2 \subseteq \Omega$ Zerfällngskörper von $\mathfrak{F}$. Dann ist $L_1 = L_2$.*

Beweis. Übergang zu einem algebraischen Abschluss von Ω:
Sei OE Ω ein algebraischer Abgeschlossen.
Dann folgt aus L_1, L_2 ist algebraisch über K, dass $L_1, L_2 \subseteq \{q \in R \mid a \text{ algebraisch über } K\}$.
Also ist OE Ω algebraischer Abschluss von K.
Dann ist Ω ein algerischer Abschluss von L_1 und von L_2.
Wende nun **??** an auf $\overline{L}_1 = \overline{L}_2\Omega$ und $\varphi = \mathrm{id}_\Omega$ □

Beispiel 9.5. Sei $p \in \mathbb{N}$ Primzahl, sei $f = X^3 - p$. (Es folgt f ist irreduzibel über $K = \mathbb{Q}$) und sei $\alpha = \sqrt[3]{p} \in \mathbb{R}_{>0}$.
Sei $\zeta := e^{\frac{2\pi i}{3}}$. Dann sind $\alpha, \zeta\alpha, \zeta^2\alpha \in \mathbb{C}$ die Nullstellen von f.
Der Zerfällungskörper von f ist

$$\mathbb{Q}[\alpha, \zeta\alpha\zeta^2\alpha] = \mathbb{Q}[\alpha, \zeta]$$

$$\begin{tikzcd}
 & \mathbb{Q}[\alpha, \xi] & \\
\mathbb{R} \supseteq \mathbb{Q}[\alpha] \arrow[ur, hook, "2"] & & \mathbb{Q}[\xi] \arrow[ul, hook', "3"'] \\
 & \mathbb{Q} \arrow[ul, hook', "3"] \arrow[uu, hook, "6"] \arrow[ur, hook, "2"'] &
\end{tikzcd}$$

9B Normale Erweiterungen

Definition 9.6. Eine algebraische Körpererweiterung $K \hookrightarrow L$ heißt **normal**, falls eine der folgenden äquivalenten Bedingungen erfüllt ist

1. Es existiert eine Menge $\mathfrak{F} \subseteq K[X]$ mit konstanten Polynomen, sodass L der Zerfällungskörper von $\mathfrak{F}$ in A ist.
2. Sei $f \in K[X]$ irreduzibel mit Nullstelle in L, dann zerfällt f in $L[X]$ vollständig in Linearfaktoren.
3. Für jede Körpererweiterung L' von L und für jeden K-Algebra-Homomorphismus $\varphi : L \hookrightarrow L'$ gilt $\varphi(L) = L$.
4. Für jeden algebraischen Abschluss Ω von L und für jeden K-Algebra-Automorphismus $\varphi : \Omega \to \Omega$ gilt $\varphi(L) = L$.

Beweis.

- 1)$\Rightarrow$2): Sei L Zerfällungskörper von $\mathfrak{F}$, dann folgt $\varphi(L)$ ist zerfällungskörper von $\mathfrak{F}$. Dann folgt mit **??**, dass $\varphi(L) = L$.
- 3)$\Rightarrow$4): Sei $\varphi : \Omega \xrightarrow{\sim} \Omega$ ein K-Algebra-Automorphismus.
  Wende 3) auf $\varphi|_L : L \to \Omega$ an.
- Sei OE L' algebraisch abgeschlossen. Ersetze L' durch

  $$L'_{\text{alg}} := \{a \in L' | a \text{ ist algebraisch über } K\}$$

  Da $K \subseteq L$ algebraisch ist, folgt, dass $\varphi(L) \subseteq L'_{\text{alg}}$. Also ist OE L' algebraischer Abschluss von L.
  Aus 8.30 folgt die Exitsnez einer Fortsetzung $\varphi' : L' \to L'$ zu φ und φ' ist Automorphismus.
  Also $\varphi(L) = \varphi'(L) = L$.

- 3)$\Rightarrow$2): Sei $f \in K[X]$ irreduzible, $a \in L$ mit $f(a) = 0$.
  Sei L' ein algebraischer Abschluss von L, $b \in L'$ mit $f(b) = 0$.
  Zu Zeigen: auch $b \in L$.

Sei OE f normiert. Dann $f = \mu_{a,K}$. Also exitsiert ein eindeutiger K-Algebra-Homomorphismus $\overline{\varphi} : K[a] \to L'$ mit $\overline{\varphi}(a) = b$.
Setze nun $\overline{\varphi}$ fort mit $\varphi : L \to L'$ (existenz durch 8.30). Dann folgt durch 3), dass $\varphi(L) = L$, also $\varphi(a) = b \in L$.

- Sei $S \subseteq L$ Teilmenge und $L = K(S)$. Sei $\mathfrak{F} := \{\mu_{a,K} \mid a \in S\}$.
  Aus 2) folgt, dass $\mu_{a,K}$ über L für alle $a \in S$ in Linearfaktoren zerfällt.
  Sei $S' := \{b \in L \mid \exists f \in \mathfrak{F} : f(b) = 0\} \supseteq S$.
  Dann ist $K(s) = L$, $K(s) =\subseteq K(s') \subseteq L$.
  Also $L = K(s')$, d.h. L ist Zerfällungskörper von $\overline{f}$.

□

Beispiel. Sei $L = K[a]$ normal, dann ist L Zerfällungskörper von $\mu_{a,K}$.

Proposition 9.7. Sei $K \hookrightarrow L$ eine normale Körpererweiterung. Sei $M \subseteq L$ Teilkörpererweiterung.

1. Jeder K-Algebra-Homomorphismus $\varphi : M \hookrightarrow L$ kann ein einem K-Algebra-Automorphismus $\overline{\varphi} : L \xrightarrow{\sim} L$ fortgesetzt werden.
2. $K \hookrightarrow M$ ist genau dann normal, wen für jeden K-Automorphims $\sigma : L \xrightarrow{\sim} L$ gilt $\sigma(M) = M$.

Beweis. 1. Betrachte $\varphi' : M \hookrightarrow L \hookrightarrow L'$ und L' ist algebraischer Abschluss von L.
Dann gibt 8.30 die Existenz einer Fortsetzung $\overline{\varphi}' : L' \xrightarrow{\sim} L'$, die K-Algebra-Automorphismus ist.
Dann folgt mit 9.6.3, dass $\overline{\varphi}' = L$, sodass $\overline{\varphi} = \overline{\varphi'|_L}$ ein K-Algebra-Automorphismus von L ist.

2. "$\Rightarrow$ ist durch 9.6.3 gegeben. "$\Rightarrow$ Sei L' algebraischer Abgeschluss von L, $\overline{\sigma} : L' \xrightarrow{\sim} L'$ Fortsetzung von σ und jeder Automorphismus von L ist Einschränkung eines Automorphismus von L'.
Also gilt $\overline{\sigma}(M) = M$ für alle $\overline{\sigma}\, \mathrm{Aut}_{K\text{-Algebra}}(L')$.
Dann folgt mit 9.6.3, dass $K \hookrightarrow M$ normal ist.

□

Beispiel 9.8. 1. Sei $\varphi : K \hookrightarrow L$ Körpererweiterung mit $[L : K] = 2$. Dann ist φ normal.

Beweis. Sei $f \in K[X]$ irreduzible, $a \in L$ mit $f(a) = 0$. Dann ist $f = \mu_{a,K}$, also $\deg(\mu_{a,K}) = [K[a] : K] \leq 2$. Wenn $\deg(\mu_{a,K}) = 1$, dann $\mu_{a,K} = X - a$ mit $a \in K$.
Wenn $\deg(\mu_{a,K}) = 2$ genau dann gilt $a \in L \setminus K$. Dann ist $\mu_{a,K} = (X - a)g$ mit $g \in L[X]$ vom Grad 1, also $g = X - b \in L[X]$.
Also sind ie Nullstellen von $\mu_{a,K}$ beide in L.
Dann folgt mit 9.6.3, dass $K \hookrightarrow L$ normal ist. □

2. Sei $K \hookrightarrow \overline{K}$ ein algebraischer Abschluss. Dann ist $K \hookrightarrow \overline{K}$ eine normale Erweiterung.
(z.B. ist $\overline{K}$ Zerfällungskörper von $\{f \in K[x] \mid f \text{ nicht konstant}\}$).

3. $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{7}]$ ist nicht normal.
   Denn $X^3 - 7$ hat Nullstelle in $\mathbb{Q}[\sqrt[3]{7}]$, aber nicht jede Nullstelle von $X^3 - 7$ liegt in $\mathbb{Q}[\sqrt[3]{7}]$:
$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{7}] \subset \mathbb{Q}[\sqrt[3]{7}, \zeta]$$
   für $\zeta = e^{\frac{2\pi i}{3}}$.

Bemerkung 9.9. Seien $K \hookrightarrow L \hookrightarrow M$ Körpererweiterungen.

1. Wenn $K \hookrightarrow M$ normal ist, dann ist $L \hookrightarrow M$ normal.
   (M ist Zerfälllungskörper von $\mathfrak{F} \subseteq K[X] \subseteq L[X]$).
2. Aus $K \hookrightarrow M$ normal folgt i.A. **nicht**, dass $K \hookrightarrow L$ normal ist mit **??**.3.
3. Aus $K \hookrightarrow L$, $L \hookrightarrow M$ normal folgt i.A. **nicht**, dass $K \hookrightarrow M$ normal.

9C Separabilitätsgrad

Proposition 9.10. Sei A ein Ring, sei $E \neq 0$ ein freier A-Modul.
Dann ist die Sequenz $0 \to M' \to M'' \to 0$ von A-Moduln genau dann exakt, wenn
$$0 \to E \otimes_A M' \to E \otimes_A M \to E \otimes_A M'' \to 0$$
exakt ist.
(Insbesondere $E \otimes_A M = 0 \Leftrightarrow M = 0$)

Beweis. E ist genau dann frei, wenn $E \tilde{=} A^{(I)}$ mit $I \neq \emptyset$.
Man erhält insbesondere die Isomorphismen

$$\begin{tikzcd}
0 \arrow[r] & E \otimes_A M' \arrow[r, "\mathrm{id}_E \otimes u"] \arrow[d, leftrightarrow, "\sim"] & E \otimes_A M \arrow[r, "\mathrm{id}_E \otimes v"] \arrow[d, leftrightarrow, "\sim"] & E \otimes_A M'' \arrow[r] \arrow[d, leftrightarrow, "\sim"] & 0 \\
0 \arrow[r] & (M')^{(I)} \arrow[r, "(m'_i)_{i\in I} \mapsto (u(m'_i))_{i\in I}"] & M^{(I)} \arrow[r] & (M'')^{(I)} \arrow[r] & 0
\end{tikzcd}$$

Es folgt die Behauptung. □

Bemerkung 9.11. Sei A eine endliche K-Algebra. Dann folgt mit **??**, dass $A = \prod_{i=1}^r A/m_i e_i$, mit $m_1, ..., m_r \subset A$ maxmimale Ideale.
Sei B eine nullteilerfreie K-Algebra, sie $\varphi : A \to B$ein K-Algebra-Homomorphimsmus.
Dann ist $\varphi(A) \subseteq B$ nullteilerfrei, oder $\mathrm{Ker}(\varphi) = m_i$ für ein $I \in \{1, ..., r\}$.
Also faktorisiert φ in $A \to A/m_i \hookrightarrow B$- Insebsondere:
$$\mathrm{Hom}_{K-\mathrm{Algebra}}(A, B) = \dot{\bigcup_{i=1}^{r}} \mathrm{Hom}_{k-\mathrm{Algebra}}(A/m_i, B)$$

Bemerkung 9.12. Sei $K \hookrightarrow A$ eine K-Algebra, $K \hookrightarrow K$ eine Körpererweiterung, $L \hookrightarrow B$ ein L-Algebra. Dann hat man zueinander inverse Bijektionen:

$$\begin{array}{rcl}
\mathrm{Hom}_{K\text{-Algebra}}(A, B) & \overset{1:1}{\leftrightarrow} & \mathrm{Hom}_{L\text{-Algebra}}(L \otimes_K A, B) \\
\varphi & \mapsto & (l \otimes a \mapsto l\varphi(a)) \\
(a \mapsto \varphi(1 \otimes a)) & \leftarrow\!\shortmid & \varphi
\end{array}$$

Bemerkung 9.15. Sei A algebraische K-Algebra, $K \hookrightarrow L$ Körpererweiterung. Dann
$$[A \otimes_K L : L]_S = [A : K]_S$$

Beweis. Sei Ω eine algebraisch abgeschlossene Erweiterung von L. Dann gibt es die Bijektion

$$\begin{aligned} \mathrm{Hom}_{K-\text{Algebra}} &\overset{\longleftrightarrow}{1:1} \mathrm{Hom}_L(A \otimes_K L, \Omega) \\ \sigma &\mapsto (a \otimes l \mapsto l\sigma(a)) \\ a \mapsto \tau(a \otimes 1) &\leftarrow\!\shortmid \tau \end{aligned}$$

□

Lemma 9.16. *Sei A eine endliche K-Algebra. Dann ist $(A:K)_S$ die Anzahl der maximalen Ideale von $A \otimes_K \Omega$. (Ω als algebraisch abgeschlossene Erweiterung von K)*

Beweis. Mit 9.15 folgt, dass OE $\Omega = K$.
Seien $m_1, ..., m_r \subset A$ die maximalen Ideal. Dann ist A/m_i eine endliche Körpererweiterung von Ω, also $A/m_I = \Omega$.
Dann folgt mit 9.11, dass

$$\#\,\mathrm{Hom}_{\Omega-\text{Algebra}}(A, \Omega) = \#\bigcup_{i=1}^{r} \mathrm{Hom}_{\Omega-\text{Algebra}}(\underbrace{A/m_i}_{=\Omega}, \Omega) = r$$

□

Proposition 9.17. Sei a endliche K-Algebra. Dann gilt

$$[A:K]_S \leq [A:K](= \dim_K(A))$$

Beweis. Sei OE $K = \Omega$ algebraisch abgeschlossen. Sei $A = \prod_{i=1}^r A/m_i e_i$. Also

$$\begin{aligned} [A:K]_S &\overset{9.16}{=} r = \sum_{i=1}^{r} \dim_K(\underbrace{A/m_i}_{=K}) \\ &\leq \sum_{i=1}^{r} \dim_K(A/m_i e_i) = [A:K] \end{aligned}$$

□

Bemerkung 9.18. Der Beweis von 9.17 zeigt $[A:K]_S = [A:K] \Leftrightarrow A \otimes_K \Omega$ ist reduziert $\Leftrightarrow A \otimes_K \Omega \tilde{=} \Omega \times ... \times \Omega$ ($r = [A:K]$ mal).

Proposition 9.19. Sei $K \hookrightarrow L$ algebraische Körpererweiterung, A ganze L-Algebra.
Dann ist

$$[A:K]_S = [A:L]_S \cdot [L:K]_S$$

Beweis. Sie Ω ein algebraischer Abschluss in L. Betrachte

$$\rho : \mathrm{Hom}_{K-\text{Algebra}}(A; \Omega) \to \mathrm{Hom}_{K-\text{Alg}}(L, \omega), \quad \sigma \mapsto \sigma|_L$$

ρ ist surjektiv (8.30). Sei $\varphi : L \hookrightarrow \Omega$ ein K-Algebra-Homomorphismus. Dann ist

$$\begin{aligned} \rho^{-1}(\{\varphi\}) &= \{\sigma \in \mathrm{Hom}_{K-\text{Algebra}}(A, \Omega) \mid \sigma|_L = \varphi\} \\ &= \mathrm{Hom}_{L-\text{Algebra}}(A, \Omega) \end{aligned}$$

wobei Ω von φ als L-Algebra aufgefasst wird.
Also

$$\begin{aligned}[A:K]_S &= \#\operatorname{Hom}_{K-\mathrm{Alg}}(A,\Omega) \\ &= \sum_{\varphi\in\operatorname{Hom}_{K-\mathrm{Alg}}(L,\Omega)} \#\varrho^{-1}(\{\varphi\}) \\ &= \sum_{\varphi}[A:L]_S \\ &= [L_K]_S[A_L]_S\end{aligned}$$

□

9D Separable Polynome

Definition 9.20. Sei $f = a_nX^n + ... + a_1X + a_0 \in A[X]$.
Definiere

$$f' := na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + ... + 2a_2X + a_1$$

f' heißt die (formale) **Ableitung** von f.

Bemerkung. Seien $f, g \in A[X]$ und $a, b \in A$.

- Die Ableitung ist Linear: $(af + bg)' = af' + bg'$
- Es gilt die Leibnitz-Regel $(fg)' = fg' + f'g$

Beweis.

- Linearität. klar.
- Aus der Linearität können wir OE annehmen, dass $f = X^i, g = X^j$.
  Dann

$$(fg)' = (X^{i+j})' = (i+j)X^{i+j-1} = iX^{i-1}X^j + jX^iX^{j-1} = fg' + f'g$$

□

Beispiel. Sei $\dim(K) = p > 0$. Dann folgt aus $f = X^p+1$, dass $f' = pX^{p-1} = 0$.

Definition 9.21. Sei $f \in K[X]$, $a \in K$. Dann ist

$$\operatorname{Ord}_a(f) := \sup\{n \geq 0 \mid (X-a)^n \text{ teilt } f\}$$

die **Ordnung der Nullstelle** a von f.

Bemerkung 9.21.

- $\operatorname{Ord}_a(f) = \infty \Leftrightarrow f = 0$.
- $\operatorname{Ord}_a(f) = 0 \Leftrightarrow f(a) \neq 0$.
- $\operatorname{Ord}_a(f) = 1 \Leftrightarrow f(a) = 0$ und $f'(a) \neq 0$.

  Beweis. $\operatorname{Ord}_a(f) = 1$ genau dann wenn $f = (X-a)g$ mit $g(a) \neq 0$.
  $\Leftrightarrow f(a) = 0$ und $f'(a) = g(a) + g'(a)(a-a) = g(0) \neq 0$. □

Definition 9.22. Ein Polynom $f \in K[X]$, $f \neq 0$ heißt **separabel**, falls alle Nullstellen in einem Zerfällungskörper paarweise verschieden sind.

Proposition 9.23. Sei Ω eine algebraisch abgeschlossen Erweiterung von K, $f \in K[X], f \neq 0$. Dann sind äquivalent:

1. f ist separabel
2. Alle Nullstellen von f in Ω sind verschieden
3. f und f' haben in Ω keine gemeinsame Nullstelle.
4. f und f' sind in $K[X]$ teilerfremd

Beweis. **(1)⇔ (2)** Sei L ein Zerfällungskörper von f. Dann existiert (8.30) eine eindeutiges Körpererweiterung $L \hookrightarrow \Omega$.

(ii)⇔(iii) aus 9.21

(iii)⇔(iv) f und f' zerfallen in $\Omega[X]$ in Linearfaktoren.
Also ist (iii) äquivalent daszu, dass f und f' sind in $\Omega[X]$ teilerfremd sind.
Ist äquivalent $\Omega \otimes_K K[X]/(f, f') \tilde{=} \Omega[X]/(f, f') = 0$.
?? gibt uns dann die Äquivalenz zu $K[X]/(f, f') = 0$, genau dann wenn f, f' auch teilerfremd in $K[X]$ sind.

□

Beispiel. 1. $(X^3 - 2)(X - 1) \in \mathbb{Q}[X]$ ist separabel

2. Sei $K = \mathrm{Quot}(\mathbb{F}_p[T])$ und $f = X^p - T \in K[X]$ ist nach dem Eisensteinkriterium mit $p = T$ irreduzibel.
Aber f ist nicht separabel:
Im Zerfällungskörper $K[\sqrt[p]{T}]$ gilt $f = (X - \sqrt[p]{T})^p$.
Äquivalent: f ist nciht teilerfremd zu $f' = pX^{p-1} = 0$.

Satz 9.24. *Sei $f \in K[X]$ irreduzibel. Dann gilt*

1. *f ist separabel genau dann wenn $f' \neq 0$.*
2. *Sei* $\mathrm{char}(K) = 0$*. Dann ist f separabel.*

Beweis. 1. Sei $f' = 0$, dann sind f' und f zueinander teilerfremd und somit (9.23) f separabel.

2. Sei $\mathrm{char}(K) = 0$, dann $\deg(f') = \deg(f) - 1$, also $\deg(f' \geq 0)$.
Also ist $f \neq 0$, sodass (1) f separabel ist.

□

9E Separable Algebren

Definition 9.25. Eine algebraisch K-Algebra A.
Ein $a \in A$ heißt **separabel**, falls $\mu_{a,K}$ separabel ist.
A heißt **separabel**, falls jedes $a \in A$ separabel ist.

Theorem 9.26. *Sei A eine endliche K-Algebra und sei Ω eine algebraisch abgeschlossen Erweiterung von K.*
Dann sind äquivalent:

1. *A ist separable K-Algebra*

2. $[A : K]_S = [A : K]$

3. $A \otimes_K \Omega$ *ist reduziert.*

4. $A \otimes \Omega \tilde{=} \Omega^r$ *also* Ω*-Algebra.*

5. Es existieren $a_1, ..., a_n \in A$ *separabel, sodass* $A = K[a_1, ..., a_n]$

6. Es exitsiert $a \in A$ *separabel, sodass* $A = K[a]$.

Beweis. Zeige:

$$\begin{tikzcd}
(6) \arrow[r, Rightarrow] & (4) \arrow[r, Leftrightarrow, "9.19"] & (3) \arrow[r, Leftrightarrow, "9.19"] \arrow[dr, Rightarrow] & (2) \\
 & (5) \arrow[u, Rightarrow] & & (1) \arrow[ll, Rightarrow] \arrow[ulll, Rightarrow, dashed, "??9.31"]
\end{tikzcd}$$

(3)⇒(1) Sei $a \in A$. (Zz. a ist separabel)
Dann ist $K[a] = K[X]/\mu_{a,K} \hookrightarrow A$.
Dass ist $\Omega \otimes_K K[a] \hookrightarrow \Omega \otimes_K A$ injektiv.
Dann ist (mit (3)) $\Omega \otimes_K K[a] = \Omega[X]/(\mu_{a,K})$ ist reduziert.
Mit **??** folgt, dass alle Nullstellen von $\mu_{a,K}$ in Ω verschieden sind. Also ist $\mu_{a,K}$ separabel, also auch a.

(1)⇒(5) klar

(6)⇒(4) Es gelte (6), dann ist $A = K[X]/(\mu_{a,K})$.
Dann ist

$$A \otimes_K \Omega = \Omega[X]/(\mu_{a,K}) \tilde{=} \prod \Omega[X]/(X - \alpha_i) = \prod \Omega$$

Da $\mu_{a,K}$ in Ω in Linearfaktoren zerfällt.

(5)⇒(4) Seien $a_1, ..., a_n \in A$. Wir verwenden (6)⇒(4). Also gilt $K[a_i] \otimes_\Omega \tilde{=} \Omega_i^d$ und $\mu_{a,K} = \prod (x - a_i)$.
Dann gilt, dass

$$\begin{aligned}
(K[a_1]) \otimes_K ... \otimes_K K[a_n]) \otimes_\Omega \Omega &= (K[a_i] \otimes_K \Omega) \otimes_K ... \otimes_K (K[a_n] \otimes_K \Omega) \\
&\tilde{=} \omega^{d_1} \otimes_\Omega \Omega^{d_2} \otimes_\Omega ... \otimes_\Omega \\
&= \Omega^{d_1 \cdot ... \cdot d_n}
\end{aligned}$$

Wähle nun

$$\begin{aligned}
\varphi : K[a_1]) \otimes_K ... \otimes_K K[a_n] &\to K[a_1, ..., a_n] \\
x_1 \otimes ... \otimes y_n &\mapsto x_1 \cdot ... \cdot x_n
\end{aligned}$$

Dann ist φ surjektiver K-Algebra-Homomorphimsmus.
Es folgt, dass $A \otimes_K \Omega$ Quotient der Ω-Algebra $\Omega^{d_1 \cdot ... \cdot d_n}$ und damit $A \otimes_K \Omega \tilde{=} \Omega^m$, $m \leq d_1 \cdot ... \cdot d_n$

□

Definition 9.27. Ein Körper K heißt **perfekt** wenn $\mathrm{char}(K) = 0$ ist oder $\mathrm{char}(K) = p > 0$ und $x \mapsto x^p$ surjektiv ist.

Satz 9.27. *Sei K perfekt. Dann ist jede endliche Körpererweiterung separabel*

Beweis. Sei $K \hookrightarrow L$ eine endliche Körpererweiterung, $a \in L$. Z.z. $\mu_{a,K}$ ist separabel.
Wir wissen $\mu_{a,K}$ ist irreduzibel und (9.24) falls $\mathrm{char}(K) = 0$ auch separabel.
Sei nun $\mathrm{char}(K) = p > 0$. Z.z. $\mu_{a,K} \neq 0$.
Sei $\mu_{a,K} = X^n + a_{n-1}X^{n-1} + ... + a_0$.
Angenommen $\mu'_{a,K} = nX^n + (n-1)a_{n-1}X^{n-1} + ... + a_1 = 0$ dann muss $a_i = 0$ falls p nicht i teilt.
Dann ist $\mu_{a,K} = X^{pk} + b_k X^{p(k-1)} + ... + b_0$ mit $b_j = a_{p \cdot j}$.
Wähle nun $\beta_j^p = b_j$.
Dann ist

$$\mu_{a,K} = \sum_j \beta_j^p X^{pj} = \left(\sum_j \beta_j X^j \right)^p$$

Also ist $\mu_{a,K}$ nicht irreduzibel. Widerspruch! □

Beispiel 9.28. Sei $K = \mathrm{Quot}(\mathbb{F}_{|}[T])$.
Dann ist $K(\sqrt[p]{T})$ eine nicht separable Erweiterung von K.

Proposition 9.29. Sei $K \hookleftarrow L$ eine endliche Körpererweiterung, $L \hookleftarrow A$ endliche L-Algebra, $A \neq 0$. Dann gilt:
A ist genau dann separable K-Algebra, wenn A separabel L-Algebra und L separabel K-Algebra.

Beweis. Sei A separabel K-Algebra. Dies ist äquivalent (9.26)dazu , dass

$$[A : L][L : K] = [A : K] = [A : K]_S = [A : L]_S[L_K]_S$$

$\Leftrightarrow$ A ist separable L-Algebra und L ist separable K-Algebra. □

9F Satz vom primitiven Element

Satz 9.30. *Sei $G \subseteq (K^\times, \cdot)$ eine endliche Untergruppe.*
Dann ist G zyklisch ($\Leftrightarrow G \tilde{=} (\mathbb{Z}/n\mathbb{Z}, +)$)

Beweis. Sei G endliche abelsche Gruppe.

Dann $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ mit $1 < n_r$ und $n_r | n_{r-1} \vdots | n_1$.
ALso gilt für jedes $g \in G \subseteq K^\times$, dass g Nullstelle von $X^{n_1} - 1 \in K[X]$, Also $\#G \subset n_1$, Also $G \tilde{=} \mathbb{Z}/n_1\mathbb{Z}$. □

Definition 9.31. Sei A eine endliche separable K-Algebra und sei $a \in A$ mit $A = K[a]$ dann heißt a **primitves** Element.

Theorem 9.31 (Satz vom primitiven Element)**.** *Sei A eine endliche separable K-Algebra. Dann existiert ein primitives Element $a \in A$.*

Beweis. Sei Ω eine algebraisch abegschlossen Erweiterung von K zu $\mathrm{Hom}_{K-\mathrm{Algebra}}(A, \Omega) = \{\varphi_1, ..., \varphi_m\}$, $m = [A : K]_S = [A : K]$.

1. Sei $a \in A$. Z.z. a ist primitives Element ist äquivalent $\varphi_i(a) \neq \varphi_j(a)$ für alle $i \neq j$:

   "$\Rightarrow$" ist klar, da a Erzeuger von A als K-Algebra ist.

   "$\Leftarrow$" Seien $\varphi_i(a) \neq \varphi_j(a)$ für alle $i \neq j$, dann sind auch $\varphi_I|_{K[a]}$ paarweise verschieden.
   Also gilt

   $$m \leq [K[a] : K]_S \leq [A : K]_S = [A : K] = m$$

   Daraus folgt, dass $[K[a] : K] = [A : K]$ und damit $A = K[a]$.

2. Sei A endlich und separabel, $\Leftrightarrow$ (Übung) $A \tilde{=} K_1 \times ... \times K_d$ für endliche separable Erweiterungen K_i von K.
   Falls $_i = K[a_i]$, so gilt $A = K[a, ..., a_d]$.
   Als ist $A = L$ endliche separable Körpererweiterung.

3. Sei K endlich. Dannn ist L endlich, also $L^\times = \{1 = a^0, a, a^2, ...\}$ für $a \in L^\times$ (9.30).
   Dann ist $L = K[a]$.

4. Sei nun K unendlich, $L = [a_1, ..., a_n]$, $a_i \in L$ separabel.
   Wir beweisen durch Induktion nach n.

   $n = 1$ Klar.

   $n > 1$ $L = K[a_1, ..., a_{n-1}][a_n] = K[b, a_n]$. Also gilt OE$L = K[b, c]$

5. Z.z. Sei $N := \{\lambda \in K \mid \lambda b + c \text{ nicht primitiv}\}$, dann ist $\#N \leq \frac{m(m-1)}{2}$.

   $$\begin{aligned} N &\overset{(1)}{=} \{\lambda \in K \mid \exists i < j : \varphi_i(\lambda b + b) = \varphi_j(\lambda b + c)\} \\ &= \bigcup_{1 \leq i < j \leq m} \underbrace{\{\lambda \in K | \lambda(\varphi_i(b) - \varphi_j(b)) + \varphi_i(c) - \varphi_j(c) = 0\}}_{\text{hat } \leq 1 \text{ Elemente, da } b, c\ L \text{ erzeugen}} \end{aligned}$$

   Da K unendlich ist folgt die Behauptung

$\square$

Beispiel 9.31. Sei $L = \mathbb{Q}[\sqrt[3]{7}, \sqrt{5}]$, $\varphi : L \to \mathbb{C}$. (...)

10 Galois-Theorie

10A Galois-Erweiterungen

Definition 10.1. Eine algebraische Körpererweiterung $K \hookrightarrow L$ heißt **Galois-Erweiterung** oder **galoisch**, falls sie normal und separabel ist.

Definition 10.2. Sei $K \hookrightarrow L$ eine Körpererweiterung. Dann ist

$$\mathrm{Aut}_{K-\mathrm{Algebra}}(L) := \{\sigma : L \to L, \text{ bijektiver } K\text{-Algebra-Homomorphismen}\}$$

Bemerkung. Sei $K \hookrightarrow L$ eine Körpererweiterung. Dann ist $\mathrm{Aut}_{K-\mathrm{Algebra}}(L)$ eine Gruppe bezüglich der Komposition.

Beispiel. 1. $\mathrm{Aut}_{\mathbb{Q}-\text{Algebra}}(\mathbb{Q}[\sqrt{7}]) = \{\mathrm{id}_{\mathbb{Q}[\sqrt{7}]}, a + b\sqrt{7} \mapsto a - b\sqrt{7}\}$

2. $\mathrm{Aut}_{\mathbb{Q}-\text{Algebra}}(\mathbb{Q}[\sqrt[3]{2}]) = \{\mathrm{id}\}$

Definition 10.2. Sei $K \hookrightarrow L$ eine Galois-Erweiterung. Dann heißt

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_{K-\text{Algebra}}(L)$$

Galoisgruppe von $K \hookrightarrow L$.

Definition 10.3. Sei $K \hookrightarrow L$ eine Körpererweiterung und sei $H \subseteq \mathrm{Aut}_{K-\text{Algebra}}(L)$ eine Untergruppe. Dann heißt

$$L^H := \{a \in L \mid \sigma(a) = a, \forall \sigma \in H\}$$

der **Fixkörper** von H.

Hier könnte ~~Ihre Werbung~~ die VL vom 16.01.2016 stehen

Satz 10.8. *Sei $K \hookrightarrow L$ eine endliche Galoiserweiterung und $M \subseteq L$ ein Zwischenkörper.*
Dann ist $K \hookrightarrow L$ normal $\Leftrightarrow$ $\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K)$ ist Normalteiler.

In diesem Fall ist die Sequenz

$$\begin{aligned}1 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) &\to \mathrm{Gal}(M/K) \to 1\\ \sigma &\mapsto \sigma|_M\end{aligned}$$

Beweis. Sei $\sigma \in \mathrm{Gal}(L/K)$, $H \subseteq \mathrm{Gal}(L/K)$. Dann ist

$$\begin{aligned}\sigma(L^H) &= \{\sigma(a) \mid a \in L^H\}\\ &= \{\sigma(a) \mid \forall \gamma \in H : \gamma(a) = a\}\\ &\overset{a'=\sigma(a)}{=} \{a' \in L \mid \forall \gamma \in H : \underbrace{\gamma(\sigma^{-1}(a')) = \sigma^{-1}(a')}_{\Leftrightarrow \sigma(\gamma(\sigma^{-1}(a')))=a'}\}\\ &= L^{\sigma H \sigma^{-1}}\end{aligned}$$

Sei $M = L^H$. Dann ist $K \hookrightarrow L$ normal $\overset{??}{\Leftrightarrow}$ für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt $L^{\sigma H \sigma^{-1}} \sigma(M) = M = L^H$.

Da $H \mapsto L^H$ injektiv ist, folgt

$$\begin{aligned}K \hookrightarrow M = L^H &\Leftrightarrow \forall \sigma \in \mathrm{Gal}(L/K) : \sigma H \sigma^{-1} = H\\ &\Leftrightarrow H \subseteq \mathrm{Gal}(L/K) \text{ Normalteiler}\end{aligned}$$

Dann folgt mit **??**, dass $\sigma \mapsto \sigma|_M$ ist surjektiv und $\mathrm{Ker}(\sigma \mapsto \sigma|_M) = \mathrm{Gal}(L/M)$. □

Bemerkung 10.9. Bestimmung von L^H: Sei $K \hookrightarrow L$ eine endliche Galois-Erweiterung, $H \subseteq \mathrm{Gal}(L/K)$.

1. Sei $a \in L$. Setze $Z_a^H := \{\sigma(a) \mid \sigma \in H\} \subseteq L$. Dann ist

$$\mu_{a,L^H} = \prod_{b \in Z_a^H} (X - b)$$

2. Sei $a \in L$ mit $L = K[a]$ und sei $S \subseteq L^H$ die Menge der Koeffizienten von μ_{a,L^H}.
   Dann ist $L^H = K[S]$.

Beweis. 1. Sei $K \hookrightarrow L$ normal Dann zerfällt μ_{a,L^H} über L' vollständig in Linearfaktoren.
   Die Nullstellen von μ_{a,L^H} sind $\{\sigma(a) \mid \sigma \in \mathrm{Gal}(L/L^H) = H\}$. Es folgt die Behauptung

2. Es ist klar, dass $K[S] \subseteq L^H$.
   Zusätzlich ist μ_{a,L^H} irreduzibel in $K[S][X]$, also ist $\mu_{a,L^H} = \mu_{a,K[S]}$. Dann ist

$$\begin{aligned}[L : L^H] &\overset{L=K[a]}{=} [L^H[a] : L^H] = \deg \mu_{a,L^H} = \deg \mu_{a,K[S]} \\ &= [K[S][a] : K[S]] = [L : K[S]]\end{aligned}$$

   Es folgt die Behauptung.

□

Beispiel 10.10. Sei $g = X^3 + a_2X^2 + a_1 + a_0 \in K[X]$ und $\mathrm{char}(K) \neq 3$.
Substituiere $X \mapsto M_{\frac{1}{3}}a_2$:

$$f = X^3 + aX + b \in K[X]$$

Beachte: f ist genau dann irreduzibel wenn g irreduzibel ist. (bzw separabel)
Sei L ein Zerfällungskörper von f (dann ist $K \hookrightarrow L$ normal) .
$f' = 3X^2 + ... \neq 0$, also ist f separabel, also ist $K \hookrightarrow L$ Galois-Erweiterung.
Es gilt $3 \leq [L : K]$ und $[L : K]$ teil $3! = 6$, also

1. Entweder $[L : K] = 3$,

2. oder $[L : K] = 6$

$\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe von S_3. Also im Fall

1. $\mathrm{Gal}(L : K) \tilde{=} A_3 := \{\sigma \in S_3 \mid \mathrm{sgn}(\sigma) = 1\}$

2. $\mathrm{Gal}(L/K) \tilde{=} S_3$

Seien $a_1, a_2, a_3 \in L$ die Nullstellen von f. Schriebe

$$\delta_f = \prod_{i \leq i < j \leq 3} (a_i - a_j) = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$$

$\Delta_f := \delta_f^2$ heißt die **Diskriminante** von f.
Jedes $\sigma \in \mathrm{Gal}(L/K)$ permutiert die Nullstellen und

$$\sigma(\delta_f) = \mathrm{sgn}(\sigma)\delta_f$$

Es folgt $\mathrm{sgn}(\Delta_f) = \Delta_f$.

Also $\Delta_f \in L^{\mathrm{Gal}(L/K)} = K$.
Es ist $\Delta_f = -4a^3 - 27b^2$:
und $\delta_f \in K$ genau dann wenn $\mathrm{Gal}(L/K) \tilde{=} A_3$.

Fazit: $[L : K] = 3 \Leftrightarrow \mathrm{Gal}(L : K) \tilde{=} A_3 \Leftrightarrow \Delta_f$ ist Quadrat.

11 Anwendung der Galois-Theorie

11A Endliche Körper

Bemerkung 11.1. Sei K ein endlicher Körper.

1. $\mathrm{char}(K) = p > 0$ dann ist $\#K = p^m$ mit $m = K : \mathbb{F}_p$
2. K ist perfekt. Insbesondere ist jede algebraische Erweiterung $K \hookrightarrow L$ separabel.

Satz 11.2. *Sei p Primzahl und $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann ist für alle $m \in \mathbb{N}$:*

$$K = \{a \in \overline{\mathbb{F}_p} \mid a^{p^m} = a\}$$

ein Körper mit p^m Elementen.
Jeder Körper mit p^m Elementen ist Zerfällungskörper von $X^p - X \in F_p[X]$.
(Dann ist K, K' Körper mit p^m Elementen, $K \tilde{=} K'$.)
Es gilt: K besteht genau aus den Nullstellen von $X^p - X$.

Beweis. Sei $f = X^{p^m} - X$, dann ist $f' = -1$, also ist f separabel.
Es folgt $\#\{a \in \overline{\mathbb{F}_p} \mid a^{p^m} = a\} = p^m$.
Sei K ein beliebiger Körper mit p^m Elementen.
Wähle einen $\mathbb{F}_p$-Algebra-Homomorphimsmus $K \hookrightarrow \overline{\mathbb{F}_p}$ (betrachte K als Unterkörper von $\overline{\mathbb{F}_p}$)
Also $K^\times = \{a \in \overline{F_p} \mid a^{p^m - 1} = 1\}$. Es folgt $K = \{a \in \overline{\mathbb{F}_p} \mid a^{p^m} = a\}$ □

Satz 11.3. *Sei K ein endlicher Körper, sei $q := \#K$, $K \hookrightarrow L$ eine endliche Erweiterung und $d := [L : K]$.*
Dann ist $K \hookrightarrow L$ Galois-Erweiterung mit $\mathrm{Gal}(L/K) \tilde{=} \mathbb{Z}/d\mathbb{Z}$ erzeugt von $\varphi : X \mapsto x^q$.

Beweis. Aus 11.2 folgt, dass $K \hookrightarrow L$. Dann ist

$$L = \{a \in \overline{L} \mid a^{q^d} = a\}$$
$$K = \{a \in \overline{L} \mid a^q = a\}$$

Also $\varphi \in \mathrm{Gal}(L/K)$ hat Ordnung d, und dann $\mathrm{Gal}(L/K)$ ist zyklisch. □

11B Zyklische Erweiterungen

Definition 11.4. Sei $n \in \mathbb{N}$. Ein $\xi \in K$ heißt n-te **Einheitswurzel**, falls $\xi^n = 1$. Definiere $\mu_n(K) := \{\xi \in K \mid \xi^n = 1\} \subseteq K^\times$ als Menge der n-ten Einheitswurzeln von K.

Bemerkung. $\mu_n(K)$ ist Untergruppe von $(K^\times, \cdot)$.

Bemerkung 11.5. Sei $n \in \mathbb{N}$. Definiere $m := n$, falls $\operatorname{char}(K) = 0$.
Falls $\operatorname{char}(K) = p > 0$ schreibe $n = p^r m$ ($r \in \mathbb{N}_0$) mit m teilerfrems zu p.

1. $\mu_n(K) = \mu_m(K)$
2. $\mu_n(K)$ ist endlich erzeugte zyklische Gruppe und $\#\mu_n(K)$ teilt m.
3. Ist K algebraisch abgeschlossen, dann ist $\#\mu_n(K)$

Beweis. 1. $\mu_n(K) = \{\text{Nullstellen von } X^n - 1 \text{ in } K\}$. Nun gilt

$$X^n - 1 = (X^m)^{p^r} - 1 = (X^m - 1)^{p^r}$$

Also gilt $\mu_n(K) = \{\text{Nullstellen von } X^m - 1 \text{ in } K\} = \mu_m(K)$.

2. $\mu_n(K)$ ist endlich, da $X^n - 1$ nur endlich viele Nullteiler hat.
Dann folgt mit **??**, dass $\mu_n(K)$ zyklisch ist.
Sei $\overline{K}$ algebraischer Abschluss. Dann hat $X^m - 1$ genau m Nullstellen, da $X^m - 1$ separabel ist. (Denn $mX^{m-1} \neq 0$ teilerfremd zu $X^m - 1$).
Also ist $\mu_n(\overline{K}) = \mu_n(\overline{K})$ und hat Ordnung m.
Da $\mu_n(K) \subseteq \mu_n(\overline{K})$ Untergruppe ist, folgt $\#\mu_m(K)$ teilt m.

□

Definition 11.6. Sei $n \in \mathbb{N}$. Eine n-te Einheitswurzel $\xi \in K$ heißt **primitv**, falls $\operatorname{Ord}(\xi) = n$.

Beispiel 11.7. 1. Sei $K = \mathbb{C}$.

$$\mu_n(\mathbb{C}) = \left\{ e^{\frac{2\pi i k}{n}} \mid k \in \mathbb{Z}/n\mathbb{Z} \right\} \tilde{=} Z/n\mathbb{Z}$$

$e^{\frac{2\pi i k}{n}}$ ist genau dann primitiv, wenn k teilerfremd zu m ist. Genau dann wenn $k \in (\mathbb{Z}/n\mathbb{Z})^\times$

2. Sei $K = \mathbb{Q}$

$$\mu_m(\mathbb{Q}) = \mu_m(\mathbb{R}) = \begin{cases} \{+1, -1\} & n \text{ ist gerade} \\ \{1\} & n \text{ ist ungerade} \end{cases}$$

3. Sei q Primzahlpotenz. Dann

$$\mu_{q-1}(\mathbb{F}_q) = \mathbb{F}_q^\times$$

Definition 11.8. Die Abildung

$$\begin{aligned} \varphi &: \mathbb{N}_0 \to \mathbb{N} \\ \varphi(n) &\mapsto \#(\mathbb{Z}/n\mathbb{Z}) = \#\{0 \le k < n-1 \mid k \text{ teilerfrems zu } n\} \end{aligned}$$

heißt **Eulersche φ-Funktion**

Proposition 11.9. 1. Seien $m, n \in \mathbb{N}$ teilerfremd, dann

$$\varphi(mn) = \varphi(m)\varphi(n)$$

2. Sei p Primzahl, $l \in \mathbb{N}$. Dann ist

$$\varphi(p^l) = p^l - p^{l-1} = (p-1)p^{l-1}$$

Beweis. 1. Es gilt:

$$\varphi(mn) = \#(\mathbb{Z}/mn\mathbb{Z})^\times = \#((\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(m)\varphi(n)$$

2. $\varphi(p^l) = \#\{0 \leq < p^l \mid p \text{ teilt nicht } k\} = p^l - ^{l-1}$
und $p^{l-1} = \#\{0 \leq k < p^l \mid p \text{ teilt nicht } k\}$

$\square$

Beispiel.

$$\begin{aligned}
\varphi(1200) &= \varphi(3 \cdot 2^4 \cdot 5^2) \\
&= \varphi(3) \cdot \varphi(2^4) \cdot \varphi(5^2) \\
&= (3-1)(2^4 - 2^3)(5^2 - 5^1) \\
&= 2 \cdot 8 \cdot 20 = 2^6 \cdot 5
\end{aligned}$$

Satz 11.10. *Die Körpererweiterung $K \hookrightarrow K[\zeta]$ ist endlich und galoisch. Die Abbildung*

$$\alpha : \mathrm{Gal}(K[\zeta]/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

,$\sigma \mapsto a_\sigma$, wobei $\sigma(\zeta) = \zeta^{a_0}$ ist wohldefinierter injektiver Gruppen-Homomorphimsmus. Insbesondere $[K[\zeta] : K] : \#\,\mathrm{Gal}(K[\zeta]/K)$ teilt $\varphi(n)$.

Beweis.
- $K \hookrightarrow K[\zeta]$ ist separabel, denn $\mu_{\zeta,K}$ teilt $X^n - 1$ und $X^n - 1$ ist separabel, da $n \in K^\times$.
  $K[\zeta]$ ist Zerfällunskörper von $X^n - 1$, also ist $K \hookrightarrow K[\zeta]$ normal.
- Z.z α ist wohldefiniert (insbesondere $a_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$):
  Da Gruppen-Automorphismen die Ordnung erhalten ist $\sigma(\zeta)$ primitv. Also $\sigma(\zeta = \zeta^{a_0})$ Einheint von $\mathbb{Z}/n\mathbb{Z}$.
- Z.z. α ist Gruppen-Homomorphimsmus:
  Seien $\sigma, \tau \in \mathrm{Gal}(K[\zeta]/K)$. Dann ist

  $$\tau(\sigma(\zeta)) = \tau(\zeta^{a_0}) = \zeta^{a_\tau a_\sigma}$$

  Es folgt, dass

  $$\alpha(\tau\sigma) = a_\tau a_\sigma = \alpha(\tau)\alpha(\sigma)$$
- Z.z. $\mathrm{Ker}(\alpha) = \{\mathrm{id}\}$:
  Sei $\sigma \in \mathrm{Ker}(\alpha)$ ist äquivalent $\sigma(\zeta) = \zeta$.
  Dann ist $\sigma = \mathrm{id}$.

$\square$

Theorem 11.11. *Sei $K = \mathbb{Q}$, $\zeta \in \mathbb{C}$ primitve n-te Einheitswurzel. Dann ist $\mathbb{Q} \hookrightarrow \mathbb{Q}$ eine endliche Galois-Erweiterung und* $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \tilde{=} (\mathbb{Z}/n\mathbb{Z})^\times$
Insbesondere ist $[\mathbb{Q}[\zeta] : Q] = \varphi(n)$.

Beweis. Sei $0 \leq r < n$ mit $(r, n) = 1$

- Z.z. Es existiert $\sigma \in G := \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ mit $\sigma(\zeta) = \zeta^r$.
  Sei $r = p_1 p_2 ... p_s$ Primfaktoerzerlegung, p_i Primzahlen mit $(p_i, n) = 1$.
  Falls ein $\sigma_i \in G$ mit $\sigma_i(\zeta) = \zeta^{p_i}$. Dann schreiben $\sigma = \sigma_1 \sigma_2 ... \sigma_s$.
  Dann genügt es zu zeigen, dass $f := \mu_{\zeta,\mathbb{Q}} = \mu_{\zeta^p,\mathbb{Q}} =: g$ für p Primzahl mit $(p, n) = 1$.

  Sei $f \neq g$, dann $X^n - 1 = fgu$ mit normiertem $u \in \mathbb{Q}[X]$.
  Mit 7.4(?Lemma) $f, g, u \in \mathbb{Z}[X]$.
  Reduktion modulo p ergibt

  $$X^n - 1 = \overline{f}\overline{g}\overline{u} \in \mathbb{F}_p[X]$$

  $\overline{g}(X^p) = \overline{g}(X^p) = \overline{f}$. Sei v ein irreduzibbler Teiler von $\overline{g}$.
  Dann $(\star)$ gilt v^2 teilt $X^n - 1$ in $\mathbb{F}_p[X]$. Dann ist also $X^n - 1$ nicht separabel in $\mathbb{F}_p[X]$. Widerspruch zu $(p, n) = 1$.
  Also ist α separabel und mit 11.10 folgt die Behauptung.

□

Satz 11.12 (Satz von Konecker Weber). *Sei $\mathbb{Q} \hookrightarrow L$ eine endliche Galois-Erweiterung mit abelscher Galoisgruppe.*
Dann existiert $n \in \mathbb{N}$ und primitive n-te Einheitswurzeln $\zeta \in \mathbb{C}$ und eine Einbettung $L \hookrightarrow \mathbb{Q}[\zeta]$

Beweis. Nicht im Zeitrahmen der Vorlesung □

11C Konstruktion mit Zirkel und Lineal

Definition 11.13. Sei $M \subseteq \mathbb{C}$ Teilmenge.
Dann heißst $z \in \mathbb{C}$ **mit Zirkel und Lineal aus** M **konstruierbar**, falls z durch endlich viele Elementarkonstruktionen aus Elementen von M konstruierbar ist.

Als **Elementarfunktionen** aus S bezeichnet man

1. Schnittpunkte von zwei Geraden die jeweils durch Punkte in S gegeben sind.
2. Schnittpunkte von einer Geraden y durch zwei Punkte in S und einem Kreis mit Mittelpunkt in S und einem Radius der der Entfernung von zwei punkten in S entspricht
3. Schnittpunkt von Kreisen wie in (2).

$$K(M) := \{z \in \mathbb{C} \mid z \text{ kann aus } M \text{ mit Zirkel und Lineal konstruiert werden}\}$$

Theorem 11.14. *Seien $0, 1 \in M$. Setze $\overline{M} := \{\overline{z} \mid z \in M\}$.*

1. *$\mathbb{Q}(M \cup \overline{M}) \hookrightarrow K(M)$ ist eine algebraische Körper-Erweiterung.*
2. *Für $z \in \mathbb{C}$ sind äquivalent:*
   (a) $z \in K(M)$

(b) *z ist enthalten in einer Galois-Erweiterung L von $\mathbb{Q}(M \cup \overline{M})$, sodass $[L : \mathbb{Q}(M \cup \overline{M})] = 2^n$ für ein $n \in \mathbb{N}$.*

Beweis. Bosch, Algebra, §6.3 □

Beispiel 11.15.
1. Quadratur des Kreises: Es ist nicht möglich aus einem Kreis mit Radius 1 ein Quadrat mit gleichem Flächeninhalt mit Zirkel und Lineal zu Konstruieren.
   Äquivalent: $\sqrt{\pi} \notin K(\{0,1\})$.

   Beweis. Durch "Satz von Lindemenn": π ist transzendent über $\mathbb{Q}$. □

2. Verdopplung des Würfels: Es ist nicht möglich aus einem Würfel W mit Kantenlänge 1 einen Würfel W' zu konstruieren, sodass $\mathrm{vol}(W') = 2\,\mathrm{vol}(W)$.
   Äquivalent: $\sqrt[3]{2} \notin K(\{0,1\})$.

   Beweis. Angenommen $\sqrt[3]{2} \in K(\{0,1\})$, dann $\sqrt[3]{2} \in L$ mit $[L : \mathbb{Q}] = 2^n$ für ein $n \in \mathbb{N}$.
   Aus $\mathbb{Q}[\sqrt[3]{2}] \subseteq L$ folgt jedoch $[L : Q]$ ist durch 3 teilbar. Widerspruch! □

3. Konstruktion eines regelmäßigen n-Ecks: Das in den Einheitskreis eingeschlossenen regelmäßige n-Eck mit Ecke 1 ist genau dann in $K(\{0,1\})$, wenn $\varphi(n)$ eine 2-er Potenz ist.
   Äquivalent: $e^{\frac{2\pi i}{n}} \in K(\{0,1\}) \Leftrightarrow [Q[e^{2\pi i/n} : \mathbb{Q}]] = 2^k$ für ein $k \in \mathbb{N}$.
   Sei $n = p_q^{l_1} ... p_r^{l_r}$, dann $\varphi(n) = (p_1^{l_1} - p_1^{l_1 - 1}) ... (p_r^{l_r} - p_r^{l_r - 1})$.
   $\varphi(n)$ ist 2-er Potenz $\Leftrightarrow n = 2^k p_1 ... p_s$, wobei p_i verschiedene Primzahlen von der Form $2^{r_i} + 1$ für $r_i \in \mathbb{N}$.

11D Auflösbare Erweiterungen

Definition 11.16. Eine Körpererweiterung $K \hookrightarrow L$ heißt **durch Radikale auflösbar**, falls es eine Kette von Erweiterungen $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_r = L$ gibt, sodass $K_i = K_{i-1}[a_i]$, wobei:

1. Falls $\mathrm{char}(K) = 0$: $a_i = \sqrt[n_i]{\alpha_i}$, $\alpha_i \in K_{i-1}$, $n_i \in \mathbb{N}$.
2. Falls $\mathrm{char}(K) = p > 0$: $a_i = \sqrt[n_i]{\alpha_i}$, $\alpha_i \in K_{i-1}$, $n_i \in \mathbb{N}$ mit $(n_i, p) = 1$
   Oder a_i ist Nullstelle eines Polynoms der Form $X^p - X - \alpha_i$, $\alpha_i \in K_{i-1}$.

Definition 11.17. Eine Gruppe G heißt **auflösbar**, falls es eine Kompositionsreihe (Kette von Untergruppen) $\{e\} = G_0 \subseteq g_1 \subseteq ... \subseteq G_r = G$ gibt, sodass G_i/G_{i-1} abelsch ist für alle $i = 1, ..., r$.

Bemerkung 11.18. Sei G auflösbar und $H \subseteq G$ Untergruppe, dann ist H auflösbar.

Beispiel 11.19. Die Symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$.

Definition 11.20. Eine endliche separable Erweiterung von Körpern $K \hookrightarrow L$ heißt **auflösbar**, wenn Erweiterung $L \hookrightarrow M$ existiert, sodass $K \hookrightarrow L$ galoisch und mit ausflösbarer Galois-Gruppe ist.

Beweis. Man kann M als normale Hülle von $K \hookrightarrow L$ wählen. $\square$

Theorem 11.21. *Sei $K \hookrightarrow L$ endlich separabel.*
Dann ist $K \hookrightarrow K$ genau dann durch Radikale auflösbar, wenn $K \hookrightarrow L$ auflösbar ist.

Beweis. Lang, Algebra, VI, §7 $\square$

Definition 11.22. Sei $f \in K[X]$ normiert und separabel. Dann heißt f **durch Radikale auflösbar**, falls der Zerfällungskörper L von f eine auflösbare Erweiterung von K ist.

Korollar 11.22. *$f \in K[X]$ ist genau dann durch Radikale auflösbar, wenn* $\mathrm{Gal}(L/K)$ *auflösbar ist.*

Beispiel 11.23. Sei $\mathrm{char}(K) = 0$, $f \in K[X]$ irreduzibel und $n := \deg(f)$.
Sei L Zerfällungskörper von f. Dann ist $\mathrm{Gal}(L/K)$ isomorph zu Untergruppen von S_n.
Also folgt aus $n \leq 4$, dass f durch Radikale auflösbar ist.
Falls $n \geq 5$ und $\mathrm{Gal}(L/K) \xrightarrow{\sim} S_n$, dann ist f nicht durch Radikale auflösbar.

Beispiel 11.24. Sei $\mathrm{char}(K) = 0$, $\deg(f) = 3$. Sei OE $f = X^2 + 3pX + 2q$, mit $p, q \in K$.
Berechnung der Nullstellen von f:

$$u := \sqrt[3]{-q + \sqrt{q^2 + p^3}}, \quad v := \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$

So dass $uv = -p$.
Dann sind die Nullstellen von f:

$$x_1 = u + p, \quad x_2 = \zeta u + \zeta^2 v \quad x_3 := \zeta^2 u + \zeta v$$

Wobei ζ primitive 3-te Einheitswurzel. (In einem Zerfällungskörper von f)

Beweis. Van der Waerden: Algebra(?) $\square$

12 Endlich erzeugt Algebren über Körper

(Oder: Lineare Algebra)

12A Hilbertscher Nullstellensatz