Höhere Algebra (Säule II)

LVA 405.450

C. Fuchs
Inhaltsübersicht **31.01.2014**

Inhaltsübersicht

Diese Lehrveranstaltung ist eine der vier Säulenvorlesungen im neuen Masterstudium Mathematik (gemäß Curriculum 2013). Der Inhalt der Vorlesung ist rund um Ringe im weiteren Sinne angesiedelt. Wir beginnen mit einer Einführung in die allgemeine Ringtheorie und wiederholen dabei auch ein paar Grundbegriffe, die aus dem Bachelorstudium bekannt sind (wie Ideale und Faktorringe). Wir gehen dann aber insbesondere auf Ideale in kommutativen Ringen ein, behandeln die Lokalisierung von Ringen sowie die Hirarchie der faktoriellen Ringe, Hauptidealringe und euklidischen Ringe. Im nächsten Kapitel gehen wir dann genauer auf Polynomringe ein; insbesondere wird der Hauptsatz über symmetrische Polynome gezeigt sowie Irreduzibilität von Polynomen behandelt. Im Anschluss wenden wir uns der Theorie der Körper inklusive der Galoistheorie zu; Körper sind ja bekanntlich Ringe in denen jedes von Null verschiedene Element invertierbar ist. Im letzten Teil der Vorlesung kommen wir zu weiterführenden Begriffen über Ringe. Wir definieren den Begriff der Ganzheit und kommen dann zu noetherschen und dedekindschen Ringen. Hier erklären sich einige interessante Phänomene, die wir am Anfang der Vorlesung behandelt haben. All dies sind wichtige Grundlagen für eine weitere Vertiefung in der algebraischen Zahlentheorie sowie der algebraischen Geometrie in Säule II des Masterstudiums.

Die Vorlesung behandelt (voraussichtlich) die folgenden Themen:

Bei Fragen oder Bemerkungen (speziell Hinweise auf Fehler aller Art sind willkommen) schicken Sie ein Email an clemens.fuchs@sbg.ac.at.

§1. Allgemeine Ringtheorie

1.1 Grundlagen

1.2 Homomorphismen und Unterringe

1.2.1 Unterring

1.2.2 Ringhomomorphismus

1.2.3 Primring

1.2.4 Charakteristik

1.2.5 Frobenius in Ringen mit Primzahlcharakteristik

1.3 Produkte von Ringen

1.3.1 Produkte von Ringen

1.3.2 Zentrale Idempotente

1.3.3 **Satz** Sei R ein unitärer Ring. R ist genau dann isomorph zum direkten Produkt unitärer Ringe, falls das Einselement eine Zerlegung in eine Summe von paarweise orthogonalen zentralen Idempotenten besitzt.
Beispiel

1.4 Ideale und Faktorringe

1.4.1 Ideale

1.4.2 Faktorring

1.4.3 **Satz** (Homomorphiesatz für Ringe)
Beispiel: Ideale von $\mathbb{Z}$, Restklassenringe

1.4.4 Summe und Produkt von Idealen

Stand: 04.10.2013

1.5 Ideale in kommutativen Ringen

1.5.1 Primideale, Teilbarkeit von Idealen
Beispiele: Primideale in $\mathbb{Z}$

1.5.2 Nullteiler, nilpotent, Integritätsbereich
Beispiele

1.5.4 **Satz** R/I ist ein Integritätsbereich $\Leftrightarrow$ I ist Primideal.

1.5.5 Maximale Ideale, Primärideale
Beispiele

1.5.6 **Satz** 1. Ein Ring R ist ein Körper $\Leftrightarrow$ R besitzt nur die trivialen Ideale $\{0\}$ und R. 2. R/I ist ein Körper $\Leftrightarrow$ I ist maximal.

1.5.7 Mit dem Lemma von Zorn folgt: Jedes Ideal ist in einem maximalen Ideal enthalten.

Stand: 08.10.2013

1.6 Der Chinesische Restsatz

1.6.1 $\equiv \pmod{I}$

1.6.2 **Chinesischer** Restsatz

1.6.3 **Satz** Mit den VS aus 1.6.3: $R/(I_1 \cap \cdots \cap I_k) \cong (R/I_1) \times \cdots \times (R/I_k)$.
Beispiele

1.7 Lokalisierung

1.7.1 Multiplikative Mengen

1.7.2 $\sim$

1.7.3 **Satz** $S^{-1}R$ ist ein kommutativer Ring mit Nullelement $0/1$ und Einselement $1/1$ (genannt die Lokalisierung von R nach S). Die Abbildung $\iota_S : R \to S^{-1}R, r \mapsto r/1$ ist ein Homomorphismus mit $\varphi(S) \subseteq (S^{-1}R)^\times$ und $\ker\iota_S = \{r \in R; \exists s \in S\colon rs = 0\}$.

Stand: 15.10.2013

1.7.4 Beispiele

1.7.5 Quotientenring, Quotientenkörper

1.7.6 **Satz** Universelle Eigenschaft der Lokalisierung

1.7.7 Ideale

1.8 Hauptidealringe, faktorielle Ringe und euklidische Ringe

1.8.1 Hauptidealring

1.8.2 Exkurs zu Teilbarkeit in Integritätsbereichen: Teiler, Vielfaches, assoziiert, gemeinsamer Teiler, ggT

1.8.3 Irreduzibel, prim. Es gilt prim $\Rightarrow$ irreduzibel.

Stand: 18.10.2013

1.8.4 Faktorielle Ringe (= ZPE-Ringe, Ringe mit eindeutiger Primelementzerlegung, Gaußsche Ringe); aus der Existenz der Zerlegung in prime Elemente folgt die Eindeutigkeit.

1.8.5 Weitere Begriffe: Zerlegung in irreduzible Elemente, Eindeutigkeit einer solchen Zerlegung

1.8.6 **Satz** Sei R ein Ring in dem jedes Elemente $\neq 0$ und $\notin R^\times$ eine Zerlegung in irreduzible Elemente besitzt. Dann gilt: Die Zerlegung ist stets eindeutig genau dann, wenn (irreduzibel $\Rightarrow$ prim) gilt.

1.8.7 **Satz** Jeder Hauptidealring ist faktoriell.
Beispiele: a) $R = \mathbb{Z}[i]$; b) $R = \mathbb{Z}[\sqrt{-5}]$.

1.8.8 Euklidische Ringe
Beispiele: a) $R = \mathbb{Z}$; b) $R = \mathbb{Z}[i]$.

1.8.9 **Satz** Jeder euklidische Ring ist ein Hauptidealring und somit faktoriell.

Stand: 22.10.2013

§2. Polynomringe

2.1 Grundlagen

2.1.1 Polynome in einer Variablen, $\delta_n = \delta_1^n$, $\delta_1 =: X$

2.1.2 Polynome in mehreren Variablen: Definition $R[X_1, \ldots, X_d] = \Gamma(\mathbb{N}^d, R)$, Addition, Multiplikation, R-Linearität, $\delta_\varepsilon = \delta_1^{\varepsilon(1)} \cdots \delta_d^{\varepsilon(d)}$, Monom, Grad
Beispiel: $f = -X^2 + Y^2 + 2XY \in \mathbb{Z}[X, Y]$

2.1.3 **Satz** (universelle Eigenschaft): φ_ξ heißt der zu (φ, ξ) zugehörige Auswertungshomomorphismus

2.1.4 Auswertung von Polynomen

Stand: 25.10.2013

2.1.5 Polynomfunktionen, Nullstellen eines Polynoms

2.1.6 Jeder Homomorphismus $\varphi : R \to S$ läßt sich zu einem Homomorphismus $\varphi_* : R[X_1, \ldots, X_d] \to S[X_1 \ldots, X_d]$ fortsetzen; insbesondere: $\varphi \in \mathrm{End}(R)$, $\varphi = \pi : R \to R/I$ (Reduktion)

2.1.7 S heißt endlich erzeugt, falls S homomorphes Bild eines Polynomringes $R[X_1, \ldots, X_d]$ ist; Erzeugendensystem, freies Erzeugendensystem

2.2 Symmetrische Polynome

2.2.1 Definition von symmetrischen Polynomen
Beispiele

2.2.2 Elementarsymmetrische Polynome, Gewicht von $\sigma_1^{\varepsilon(1)} \cdots \sigma_d^{\varepsilon(d)}$
Beispiele: $d = 1 \rightsquigarrow \sigma_1 = X, d = 2 \rightsquigarrow \sigma_1 = X_1 + X_2, \sigma_2 = X_1X_2, d = 3 \rightsquigarrow \sigma_1 = X_1 + X_2 + X_3, \sigma_2 = X_1X_2 + X_1X_3 + X_2X_3, \sigma_3 = X_1X_2X_3$

Stand: 29.10.2013

2.2.3 Lexikographische Ordnung auf $\mathbb{N}^d$, Eigenschaft
Beispiel: $(2, 3, 5) < (2, 4, 1)$

2.2.4 Ordnung auf den Monomen, Eigenschaften dieser Ordnung

2.2.5 **Fundamentalsatz** über symmetrische Polynome
Beispiele: $X^2 + Y^2 + XY = \sigma_1^2 - \sigma_2$, etc.

Stand: 05.11.2013

2.2.6 Diskriminate

2.2.7 Resultante

2.3 Resultante und Diskriminante

2.3.1 Resultante

2.3.2 **Satz** $\mathrm{Res}(f, g) = \varphi f + \psi g$

2.3.3 **Satz** Resultante und gemeinsame Nullstellen

2.3.4 Diskriminante, Diskriminante und mehrfache Nullstellen

Stand: 08.11.2013

2.3.5 Resultante und Diskriminante revisited

2.4 Primfaktorzerlegung

2.4.1 **Satz** Division mit Rest

2.4.2 Polynomringe über einem Körper sind euklidische Ringe

2.4.3 Teiler vs. Nullstelle

2.4.4 **Satz** (Eisensteinsches Irreduzibilitätskriterium)
Beispiele

Stand: 12.11.2013

2.4.5 **Satz** (Lemma von Gauss)

2.4.6 **Satz** R faktoriell $\Rightarrow R[T]$ faktoriell

2.4.7 Irreduzibel über $\mathbb{Z}$ = irreduzibel über $\mathbb{Q}$
Beispiel: $f = X^7 + 2X^5 + 4X + 2 \in \mathbb{Z}[X]$ ist irreduzibel über $\mathbb{Q}$

§3. Körpertheorie

3.1 Primkörper und Körpererweiterungen

3.1.1 Definition Körper, Eigenschaften

3.1.2 Körperhomomorphismen

3.1.3 Charakteristik, Primkörper

3.1.4 Körpererweiterung, Grad, Turm von Körpererweiterungen

Stand: 15.11.2013

Beispiel: $\mathbb{C} \supseteq \mathbb{R}, \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$, $\mathbb{F} \supseteq \mathbb{F}_p$ = Primkörper von $\mathbb{F}$ mit $p = \text{char}(\mathbb{F}) \Rightarrow |\mathbb{F}| = p^n$ für ein $n \in \mathbb{N}$.

3.1.5 **Gradsatz** $L \supseteq E \supseteq K \Rightarrow [L : K] = [L : E][E : K]$.

3.1.6 $K(S)$ der von S über K erzeugte Körper, $K(S) = \{f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n); n \in \mathbb{N}, f, g \in K[T_1, \ldots, T_n], s_1, \ldots, s_n \in S, g(s_1, \ldots, s_n) \neq 0\}$, endlich erzeugt

Beispiele: $\mathbb{R} \supseteq \mathbb{Q}(\{\sqrt{2}, \sqrt{3}\}) \supseteq \mathbb{Q}, \mathbb{C} \supseteq \mathbb{Q}[n] := \mathbb{Q}(\exp(2\pi i/n)) \supseteq \mathbb{Q}, \mathbb{R} \supseteq \mathbb{Q}(\sqrt[3]{5} + \sqrt{7}) \supseteq \mathbb{Q}$

3.1.7 **Satz** Charakterisierung von endlich erzeugt

3.1.8 $K(S, T)$, $E \cdot F = K(E, F)$ = Kompositum von E, F

3.2 Algebraische Erweiterungen

3.2.1 endliche Erweiterungen

3.2.2 $\alpha \in L$ heißt algebraisch über K, falls...

Stand: 19.11.2013

Beispiele: $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$, $\sqrt{2}$ über $\mathbb{Q}$

3.2.3 algebraische Erweiterungen

3.2.4 **Satz** endlich = endlich erzeugt und algebraisch.
Beispiel: $\mathbb{Q}(\{\sqrt{p}; p \in \mathbb{P}\})$ algebraisch aber nicht endlich

3.2.5 **Satz** $L \supseteq K$ algebraisch $\Leftrightarrow L \supseteq E$ und $E \supseteq K$ algebraisch

3.2.6 **Satz** von Kronecker $\forall f \in K[X] \backslash K$: $\exists L \supseteq K$ und $\alpha \in L$ mit $f(\alpha) = 0$

3.3 Algebraisch abgeschlossene Erweiterungen

3.3.1 algebraisch abgeschlossen

3.3.2 **Satz** Linearfaktorzerlegung

Stand: 26.11.2013

3.3.3 algebraischer Abschluss
Beispiel: $\mathbb{C}$

3.3.4 **Sätze** von Steinitz

3.3.5 Folgerungen

3.3.6 $\mathrm{Hom}(K, \bar{K})$ lässt sich injektiv in $\mathrm{Aut}(\bar{K})$ abbilden

3.4 Konjugierte Erweiterungen

3.4.1 Konjugierte Elemente, konjugierte Körper
Beispiele

Stand: 03.12.2013

3.4.2 K-Homomorphismen

3.4.3 **Satz**

3.4.4 Konjugiertheit über K

3.4.5 Eigenschaften

3.5 Separabilität

3.5.1 Nullstellenmenge eines Polynoms, Zerfällungskörper

3.5.2 Separabilitätsgrad für Elemente, Separabilität für Elemente und Körpererweiterungen, Separabilitätsgrad
Beispiel

Stand: 06.12.2013

3.5.3 separabler Abschluss

3.5.4 res_E^F

3.5.5 Technisches Lemma

3.5.6 $|\Sigma_f| = |\operatorname{Hom}_K(K(\alpha), \Omega)|$

3.5.7 **Satz** Charakterisierung von Separabilität: Separabilitätsgrad = Grad

Stand: 10.12.2013

3.5.8 Separabilität für Polynome

3.5.9 Separabilität und Körpertürme

3.5.10 **Hauptssatz** über endliche Körper

3.5.11 **Satz** vom primitiven Element

Stand: 13.12.2013

3.6 Normale Erweiterungen

3.6.1 normale Erweiterungen

3.6.2 **Satz** Charakterisierung von Normalität

3.6.3 Folgerungen

§4. Galoistheorie

4.1 Galoissche Erweiterungen

4.1.1 Glaois-Erweiterung, Galois-Gruppe

4.1.2 Galois-Gruppe einer Familie von Polynomen

Stand: 20.12.2013

4.1.3 Die Galois-Gruppe kann stets als Untergruppe von $\mathscr{S}_n$ aufgefasst werden.

4.2 Hauptsatz der Galoistheorie

4.2.1 Galoiskorrespondenz: κ, γ

4.2.2 **Hauptsatz** der Galoistheorie

4.2.3 Beweis I: $\kappa \circ \gamma = \mathrm{id}$

Stand: 07.01.2014

4.2.4 Beweis II

4.2.5 Beweis III (Lemma von Artin). Es folgt $\gamma \circ \kappa = \mathrm{id}$

4.2.6 Beweis IV

4.2.7 Ende des Beweises

4.2.8 Galois-Äquivarianz

Stand: 10.01.2014

4.2.9 Zusatz zum Hauptsatz
Paradebeispiel

Stand: 14.01.2014

4.2.10 zyklische, abelsche, auflösbare (separable) Körpererweiterungen, auflösbar durch Radikale

§5. Weiterführende Themen der Ringtheorie

5.1 Ganzheit

5.1.1 Sei L ein Ring und A ein Unterring von L. $\alpha \in L$ heißt ganz über A falls...
Beispiele

5.1.2 Ganzheit von Ringerweiterungen
Beispiel

5.1.3 **Satz** Charakterisierung von ganzen Elementen eines Ringes in einem Körper

5.1.4 **Satz** Der ganze Abschluss B eines Ringes A in einem Körper L ist ein Ring.

5.1.5 Ganzabgeschlossen
Beispiele

Stand: 17.01.2014

Beispiel: $\mathbb{Z}[(1+\sqrt{5})/2]$ ist nicht ganzabgeschlossen.

5.1.6 **Satz** Faktorielle Integritätsbereiche sind ganzabgeschlossen

5.1.7 **Satz** Sei A ein ganzabgeschlossener Integritätsbereich. α ist ganz über $A \Leftrightarrow$ das Minimalpolynom von α hat Koeffizienten in A
Beispiel: $L = \mathbb{Q}(\sqrt{5}), K = \mathbb{Q}, A = \mathbb{Z}$

5.1.8 **Satz** Türme von Integritätsbereichen und Ganzheit

5.1.9 **Satz** Der ganze Abschluss eines Integriätsbereichs in einer endlichen Erweiterung L des Quotientenkörpers K erfüllt...

Stand: 21.12.2014

5.1.10 A ganzabgeschlossen, $S \subseteq A$ multiplikativ $\Rightarrow S^{-1}A$ ganzabgeschlossen.

5.1.11 B der ganze Abschluss von A in $L \Rightarrow S^{-1}B$ ist der ganze Abschluss von $S^{-1}A$

5.2 Noethersche Ringe und Ringe mit Dimension 1

5.2.1 Definition von noethersch
Beispiele: Körper, $K[X]/(X^2)$, Hauptidealringe und Ringe, die als abelsche Gruppe endlich erzeugt sind, wie z.B. $\mathbb{Z}[X]/(f)$ mit $f \in \mathbb{Z}[X]$ normiert, sind noethersch.

5.2.2 **Satz** Charakterisierung von noetherschen Ringen

5.2.3 Die Lokalisierung eines noetherschen Ringes ist noethersch.

5.2.4 Krull-Dimension eines Ringes
Beispiele: Körper haben Dimension 0, $\dim(K[X]/(X^2)) = 1$, Hauptidealringe haben Dimension 1, $\dim(K[X_1, \ldots, X_n]) \geq n$, Integritätsbereiche haben Dimension 1 $\Leftrightarrow$ es gibt ein Primideal und jedes Primideal ist maximal.

Stand: 24.01.2014

Weiter Beispiele: $\dim(\mathbb{Z}[X]) \geq 2$, $\dim(A_P) = \mathrm{ht}(P)$, $\dim A = \sup\{\dim(A_P); P \text{ Primideal von } A\}$

5.2.5 P_1, P_2 zwei verschiedene, nicht-triviale prime Hauptideale in einem Integritätsbereich, dann gilt nicht $P_1 \subset P_2$. Insbsondere haben Hauptidealringe Dimension $= 1$.

5.2.6 In einem faktoriellen Integritätsbereich gilt für ein Primideal $P \neq 0$: $\mathrm{ht}(P) = 1 \Leftrightarrow P = (p)$.

5.2.7 **Satz** Ein faktorieller noetherscher Integritätsbereich der Dimension 1 ist ein Hauptidealring.

5.2.8 **Satz** Ist B eine ganze Erweiterung eines Ringes A mit Dimension $= 1$, so hat B Dimension $= 1$.

5.2.9 Ist A ein Ring mit Dimension $= 1$, so hat der ganze Abschluss B von A in L ebenfalls Dimension $= 1$.

5.2.9 Die Lokalisierung eines Ringes mit Dimension 1 nach einer multiplikativen Menge S, für die das Komplement ein maximales Ideal enthält, hat Dimension 1. Insbesondere $\dim(A_P) = 1$.

Stand: 28.01.2014

5.3 Dedekindsche Ringe

5.3.1 Definition
Beispiele: Hauptidealringe insbesondere $\mathbb{Z}$ und $K[X]$, $\mathbb{Z}[\sqrt{-5}]$, quadratische Zahlringe

5.3.2 **Satz** Die Lokalisierung eines Dedekindschen Ringes nach einer multiplikativen Menge S, dessen Komplement ein maximales Ideal enthält, ist ein Dedekindscher Ring.

5.3.3 Eindeutige Faktorisierung von Idealen

5.3.4 Ausblick: a) Ein noetherscher Ring mit Dimension 1 ist ein Hauptidealring genau dann, wenn er die Eigenschaft aus 5.3.3 besitzt. b) Der ganze Abschluss eines Dedekindschen-Ringes in einem Körper ist wieder ein Dedeking-Ring. c) algebraische Zahlkörper, Ganzheitsringe und Diophantische Gleichungen...

Stand: 31.01.2014

Literatur

1. G. Wüstholz, Algebra, Springer Spektrum, 2013
2. D. Lorenzini, An Invitation to Arithemtic Geometry, AMS, 1997
3. T.W. Hungerford, Algebra, Springer, 1984
4. S. Lang, Algebra, Reading, 1993
5. B.L. van der Waerden, Algebra I und II, Springer, 1993