ALGEBRAISCHE ZAHLENTHEORIE

Algebraische Grundlagen

Proposition 0.1. *In einem Ring A gilt:*

1. *Es sei $\mathfrak{p} \subseteq A$, prim und $\mathfrak{p} \supseteq \mathfrak{a}_1 \cdot \cdots \cdot \mathfrak{a}_r$. Dann ist $\mathfrak{p} \supseteq \mathfrak{a}_i$ für ein i.*
2. *Es sei $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$ und $\mathfrak{p}_i$ prim. Dann ist $\mathfrak{a} \subseteq \mathfrak{p}_i$ für ein i.*
3. *Es sei $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ für $1 \leqslant i \neq j \leqslant n$. Dann ist*

$$0 \to \mathfrak{a}_1 \cdot \cdots \cdot \mathfrak{a}_n \to A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n \to 0$$

exakt und deshalb auch $\mathfrak{a}_1 \cdot \cdots \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$.

Proposition 0.2. *Es sei A ein Ring und M ein A-Modul. Dann ist äquivalent*

a) Jede aufsteigende Untermodulkette $M_1 \subseteq M_2 \subseteq \cdots M$ wird stationär.
b) Jeder Untermodul $N \subseteq M$ ist endlich erzeugter A-Modul.
c) Jede nichtleere Menge $\mathscr{M}$ von Untermoduln $M \supseteq N \in \mathscr{M}$ enthält ein maximales Element.

Definition 0.1. *Erfüllt ein A-Modul M die vorigen äquivalenten Bedingungen, so heißt er* noethersch. *Ist A als A-Modul noethersch, so heißt A* noethersch Ring.

Proposition 0.3. *In einer Sequenz von A-Moduln $0 \to N' \to N \to N'' \to 0$ ist äquivalent*

a) N ist noethersch.
b) N', N'' sind noethersch.

Beweis. Es ist für eine Kette (N_i) immer exakt

$$0 \to (N_{i+1} \cap N')/(N_i \cap N') \to N_{i+1}/N_i \to (N_{i+1} + N')/(N_i + N') \to 0$$

□

Theorem 0.1. *Es ist äquivalent*

a) A ist noethersch.
b) $A[x]$ ist noethersch.

Beweis. a) nach b): Für ein Ideal $I \subseteq A[x]$ nehme das A-Ideal $\mathfrak{a}$, das von allen a_f in A gebildet wird, für die es ein $f = a_f x^m + \sum_{j=0}^{m-1} a_j x^j \in I$ gibt. Das Ideal $\mathfrak{a}$ hat endlich viele Erzeuger $a_{f_1}, \ldots, a_{f_p}$. Die f_ν erzeugen I bis auf Polynome g mit $\deg g < n_0$ für ein $n_0 > 0$. Diese werden aufgrund einer analogen Überlegung auch von endlich vielen $g_1, \ldots, g_r$ erzeugt. Also $I = (f_\nu, g_\mu)$.

Lemma 0.1. *Es sei A ein noetherscher Ring. Dann liegen über jedem Ideal $\mathfrak{a} \subseteq A$ nur endlich viele minimale Primideale.*

Beweis. Es sei $\mathfrak{a}$ das maximale Ideal, das die Bedingung nicht erfüllt. Dann kann $\mathfrak{a}$ nicht selbst prim sein. Es gibt also $fg \in \mathfrak{a}$ mit $f, g \notin \mathfrak{a}$. Über $(\mathfrak{a}, f) = \mathfrak{a}_1$ und $(\mathfrak{a}, g) = \mathfrak{a}_2$ liegen jeweils endlich viele minimale Primideale.
Umgekehrt ist $\mathfrak{q} \supseteq \mathfrak{a} \supseteq \mathfrak{a}_1\mathfrak{a}_2$, so ist $\mathfrak{q} \supseteq \mathfrak{a}_1$ oder $\mathfrak{q} \supseteq \mathfrak{a}_2$. Ist $\mathfrak{q}$ minimal über $\mathfrak{a}$, so ist es umsomehr minimal über dem $\mathfrak{a}_i$, das es enthält. Also sind endlich vielen minimalen Primideale über den $\mathfrak{a}_i$ eine Obermenge der minimalen Primideale über $\mathfrak{a}$.

Ganze Ringerweiterungen

Definition 0.2. *Es sei B/A eine Ringerweiterung. Ein Element $x \in B$ heißt* ganz über *A, wenn es eine Gleichung*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

mit $a_i \in A$ erfüllt.
Ein Ring B/A heißt ganz über *A, wenn alle $x \in B$ ganz über A sind.*

Lemma 0.2. *Es sei $M = Am_1 + \cdots + Am_n$ ein endlich erzeugter A-Modul und*

$$x \cdot M \subseteq \mathfrak{a}M$$

dann existiert ein $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ mit $a_i \in \mathfrak{a}$, so daß $f(x) \cdot M = 0$ ist, also $f(x) \in \mathrm{Ann}(M)$.

Beweis. Ist $x m_i = \sum_j a_{ij} m_j$, also $P = (\delta_{ij} x - a_{ij})$ eine Matrix mit $P(m_1, \ldots, m_n)^t = 0$, also nach Multiplikation von links mit P_{ad} auch $\det(P) m_i = 0$, also $\det(P) = f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ ist Annulator von M und $a_i \in \mathfrak{a}$. □

Proposition 0.4. *Es ist für ein $x \in B/A$ äquivalent*

a) $A[x]$ ist endlich erzeugter A-Modul.
b) x ist ganz über A.

Beweis. Folgt aus dem vorigen Lemma, da $1 \in A[x]$. □

Lemma 0.3. *Ist $x, y \in B$ ganz über A, so ist $A[x, y]$ ein endlich erzeugter A-Modul.*

Beweis. $A[x]$ ist ein endlich erzeugter A-Modul und weil y auch ganz über $A[x]$ ist, auch $A[x, y]$ ein endlich erzeugter $A[x]$-Modul. Insgesamt also $A[x, y]$ ein endlich erzeugter A-Modul. □
Damit sind für $x, y \in B$, ganz über A auch $x + y, x - y, xy \in B$ alle ganz über A und $\bar{A} \subseteq B$, die Menge der $x \in B$, ganz über A ist ein Unterring von B, der *algebraische Abschluß von A in B*.

Proposition 0.5. *Ist B/A ganz, so ist für ein C/A auch $B \otimes_A C/C$ ganz, insbesondere für $C = S^{-1}A$ auch $S^{-1}B/S^{-1}A$ ganz und noch spezieller $B_\mathfrak{p}/A_\mathfrak{p}$ ganz für ein $\mathfrak{p} \subseteq A$, prim.*
Weiterhin ist für $\mathfrak{b} \subseteq B$ und $\mathfrak{a} = \mathfrak{b} \cap A$ auch $(B/\mathfrak{b})/(A/\mathfrak{a})$ ganz.

Proposition 0.6. *Ist $C/B/A$ ein Turm von Ringerweiterungen so ist äquivalent:*

a) C/A ganz.
b) C/B ganz und B/A ganz.

Proposition 0.7. *Es ist $\overline{S^{-1}A}$, der ganze Abschluß von $S^{-1}A$ in $S^{-1}B$ gleich $S^{-1}(\bar{A})$.*

Beweis. Ist b ganz über A, so ist jedes b/s ganz über $S^{-1}A$. Umgekehrt, sei $(a/s_0)^n + a_1/s_1(a/s_0)^{n-1} + \cdots + a_n/s_n = 0$. Man kann dann durch Erweitern der Brüche ein s finden, so daß $(a/s)^n + a_1'/s(a/s)^{n-1} + \cdots + a_n'/s^n = 0$ gilt. Also $s^n(a^n + a_1' a^{n-1} + \cdots + a_n') = 0$ mit einem geeigneten s, also $(sa)^n + sa_1'(sa)^{n-1} + \cdots + s^n a_n' = 0$ und damit sa ganz über A.

Lemma 0.4. *Ist B/A ganz und $\mathfrak{a} \subseteq A$ ein Ideal sowie $x = \mathfrak{a}B$, so ist $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ mit $a_i \in \mathfrak{a}$.*

Beweis. Ist $x = \sum_{j=1}^r a_j b_j$, so ist mit $B' = A[b_1, \ldots, b_r]$ auch $xB' \subseteq \mathfrak{a}B'$ und B' endlich erzeugter A-Modul. □

Korollar 0.1. *Ist $\mathfrak{a} \subsetneq A$ ein echtes Ideal, so ist $1 \notin \mathfrak{a}B$.*

Proposition 0.8. *Ist B/A eine ganze Erweiterung von Integritätsringen, so ist äquivalent*

a) B ist ein Körper.
b) A ist ein Körper.

Beweis. Betrachte $f = b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0$. Ist A Körper, so ist $a' a_n = 1$ und damit $b^{-1} \in A[b, a']$. Umgekehrt ist B Körper und $ba = 1$, so ist wegen $a^{n-1} f = 0$ auch $b \in A$.

Definition 0.3. *Ist A ein Integritätsring und A gleich seinem ganzen Abschluß in $K = K(A)$, so heißt A auch* normal.

Proposition 0.9. *Ein Ring A mit eindeutiger Primfaktorzerlegung (UFD) ist normal.*

Beweis. Es sei $x = a/b$ und $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, also $a^n + a_1 a^{n-1} b + \cdots + a_{n-1} a b^{n-1} + a_n b^n = 0$. Ist p ein Primteiler von b, so auch einer von a. Widerspruch zur angenommenen Teilerfremdheit von a, b. □

Theorem 0.2. *Ist B/A ganz, so gilt*

(1) Über jedem $\mathfrak{p} \subseteq A$, prim, liegt ein $\mathfrak{q} \subseteq B$, prim mit $\mathfrak{q} \cap A = \mathfrak{p}$. („Lying-over").
(2) Ist $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq B$, beide prim mit $\mathfrak{q}_i \cap A = \mathfrak{p}$, so ist $\mathfrak{q}_1 = \mathfrak{q}_2$. („Incomparability").
(3) Ist $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq A$, beide prim und $\mathfrak{q}_1 \subseteq B$, prim, mit $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$, so gibt es ein $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$ mit $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. („Going-Up").

Korollar 0.2. *Ist $B \supseteq A$ ganz, so ist $\dim B = \dim A$ und die induzierte Abbildung $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ ist surjektiv und abgeschlossen, das Bild von $V(\mathfrak{b})$ ist $V(\mathfrak{b} \cap A)$.*

Dedekindringe

Normen

Komplettierungen

Differenten und Diskrimianten

Klassengruppe

Einheitengruppe

Adele und Idele

Jürgen Böhm, Wertheim, 22. Mai 2026