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* noetherscher 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 $V(\mathfrak{b} \cap A)$.*

Es sei G eine Gruppe, die auf einem Ring B operiert und es sei $A = B^G \subseteq B$ der Unterring der $x \in B$ mit $x^g = x$ für alle $g \in G$
Ist G eine endliche Gruppe, so ist jedes $x \in B$ Nullstelle von $f(X) = \prod_{g \in G}(X - x^g)$, einem monischen Polynom in $A[X]$. Also ist B/B^G ganz.
Es gilt dann für $S \subseteq A$ auch $(S^{-1}B)^G = S^{-1}(B^G) = S^{-1}A$. Man erkennt dies aus der Sequenz von A-Algebren und A-linearen Abbildungen

$$0 \longrightarrow A \longrightarrow B \underset{\psi}{\overset{\phi}{\rightrightarrows}} \prod_{g \in G} B$$

mit $x \mapsto \phi(x) = (x^{g_1}, \ldots, x^{g_n})$ und $x \mapsto \psi(x) = (x, \ldots, x)$ und der exakten Lokalisierung $- \otimes_A S^{-1}A$.

Proposition 0.10. *Es seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \subseteq B$, prim, die Überideale von $\mathfrak{p} \subseteq A = B^G$. Dann operiert G mit $\mathfrak{q} \mapsto \mathfrak{q}^g$ transitiv auf den $\mathfrak{q}_\nu$.*

Beweis. Durch Übergang zu $A_{\mathfrak{p}}$ kann man $\mathfrak{p}$, und damit auch $\mathfrak{q}_\nu$, maximal annehmen. Es seien $\mathscr{B}_i$ die Bahnen der Operation von G auf den $\mathfrak{q}_\nu$. Wenn es mehr als eine Bahn gibt, so wähle $x \in B$ nach dem chinesischen Restsatz so, daß $x \equiv 0 \pmod{\mathfrak{q}_\nu}$ für die $\mathfrak{q}_\nu$ der Bahn $\mathscr{B}_1$ und $x \equiv 1 \pmod{\mathfrak{q}_\nu}$ für die $\mathfrak{q}_\nu$ der übrigen Bahnen.
Es ist dann $x \in \mathfrak{q}_1^{g^{-1}}$ für jedes g und für ein $\mathfrak{q}_1$ der ersten Bahn, also $x^g \in \mathfrak{q}_1$.
Also ist $z = \prod_{g \in G} x^g \in \mathfrak{q}_1 \cap A = \mathfrak{p}$. Damit ist $z \in \mathfrak{q}_\nu$ für jedes $\mathfrak{q}_\nu$, insbesondere auch für die Ideale der zweiten Bahn $\mathscr{B}_2$. Also ist auch $x^g \in \mathfrak{q}_2$ für ein Element $\mathfrak{q}_2$ der zweiten Bahn $\mathscr{B}_2$ und ein $g \in G$, also $x \in \mathfrak{q}_2^{g^{-1}} = \mathfrak{q}_2'$ mit $\mathfrak{q}_2'$ aus $\mathscr{B}_2$ im Widerspruch zu $x \equiv 1 \pmod{\mathfrak{q}_2'}$.

Proposition 0.11. *Es sei B/A ganz, A, B Integritätsringe und A normal sowie L/K algebraisch mit $L = Q(B)/K = Q(A)$.*
Weiter seien $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq A$, prim, und $\mathfrak{q}_2 \subseteq B$, prim, mit $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Dann existiert ein $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, prim, mit $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

Beweis. Nach Lokalisierung mit $A_{\mathfrak{p}_2}$ kann man annehmen, daß $\mathfrak{p}_2 = \mathfrak{m}$ maximal und $\mathfrak{p} = \mathfrak{p}_1 \subseteq \mathfrak{m}$ ohne Zwischenideale. Es sei $\mathfrak{q} = \mathfrak{q}_2$. Angenommen, es gäbe kein $\mathfrak{r} \subseteq \mathfrak{q}$ mit $\mathfrak{r} \cap A = \mathfrak{p}$. Dann wäre $\mathfrak{q}B_{\mathfrak{q}}$ das einzige Primideal über $\mathfrak{p}B_{\mathfrak{q}}$, also für jedes $b' \in B_{\mathfrak{q}}$ auch $b'^m \in \mathfrak{p}B_{\mathfrak{q}}$. Wähle für $b' = z \in \mathfrak{m} - \mathfrak{p}$. Dann ist $z^m \in \mathfrak{p}B_{\mathfrak{q}}$. Es gibt also ein $s \in B - \mathfrak{q}$ mit $(sz)^m \in \mathfrak{p}B$, also (nach Umbenennung) $sz = b$ mit $b \in \mathfrak{p}B$, also $s = b/z$. Es ist dann b ganz über $\mathfrak{p}$ und damit auch alle Konjugierten $s_1, \ldots, s_k$ von s gleich $s_i = b_i/z$ mit b_i ganz über $\mathfrak{p}$. Es ist also das Minimalpolynom $f(x)$ von s gleich

$$(1) \qquad f(x) = (x - s_1) \cdot \cdots \cdot (x - s_k) = x^k + w_1((b_i/z))x^{k-1} + \cdots + w_k((b_i/z)) = \\ = x^k + c_1 x^{k-1} + \cdots + c_k$$

wobei $w_\nu((b_i/z)) = w_\nu(b_1/z, \ldots, b_k/z)$ die elementarsymmetrischen Funktionen der b_i/z sind.
Es ist also $c_i = d_i/z^i \in A$ mit d_i ganz über $\mathfrak{p}$ und mit $d_i = c_i z^i \in A$, also $d_i \in \mathfrak{p}$ und damit auch $c_i \in \mathfrak{p}$, denn es ist ja $z \notin \mathfrak{p}$. Also ist $s^k \in \mathfrak{p}B \subseteq \mathfrak{m}B \subseteq \mathfrak{q}$ im Widerspruch zu $s \notin \mathfrak{q}$. □

Körpererweiterungen

Es sei L/K eine *Körpererweiterung*, also der Körper L eine K-Algebra über dem Körper K. Dann ist L/K *algebraisch*, wenn L/K ganz. Weiter sei L/K *endlich*, wenn L ein endlicher K-Vektorraum ist, wir schreiben $[L : K] = \dim_K L$, den *Grad von L über K*.
Eine endliche Erweiterung ist auch algebraisch.
Von den relativen Beziehungen mehrerer Körpererweiterungen sind folgende grundlegend:
Der *Körperturm*

(2)
$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

und das *Kompositum LE von L und E*

(3)
$$\begin{array}{ccc} & M & \\ & | & \\ & LE & \\ L & & E \\ & K & \end{array}$$

also der kleinste Körper $M' \subseteq M$, der L und E umfaßt.
Eine Klasse $\mathscr{K}$ von Köpererweiterungen heißt *mit Körpertürmen verträglich*, wenn in einem Körperturm $M/L/K$ die Beziehung $M/K \in \mathscr{K}$ äquivalent zu $M/L, L/K \in \mathscr{K}$ ist.
Sie heißt *verträglich mit Basiserweiterungen*, wenn in einem Diagramm (3) aus $L/K \in \mathscr{K}$ immer $LE/E \in \mathscr{K}$ folgt.

Lemma 0.5. *Mit Körpertürmen und mit Basiserweiterungen verträglich sind*

1. *Endliche Erweiterungen.*
2. *Algebraische Erweiterungen.*

Ein Element $\alpha \in L$ heiße *algebraisch über* K, wenn es ganz über K ist. Sind $(\alpha_i \in L)$ ein System von Elementen aus L, so sei $K((\alpha)_i) \subseteq L$, der kleinste Unterkörper $E \subseteq L$, der K und die α_i enthält. Sind alle α_i algebraisch über K, so ist auch $K((\alpha_i))/K$ algebraisch.
Ist $\alpha \in L$ algebraisch, so ist die Sequenz

$$0 \to I \to K[x] \to K(\alpha) \to 0$$

exakt und damit $I = (f(x))$ mit einem eindeutigen, irreduziblen monischen Polynom $f(x)$, das *Minimalpolynom von* α *über* K. Wir schreiben auch $f(x) = \mathrm{Irr}(\alpha, K, x)$.
Ist $p(x) \in K[x]$ mit $p(\alpha) = 0$, so ist $f(x)q(x) = p(x)$.
Für ein irreduzibles $f(x) \in K[x]$ ist

$$L = K[x]/(f(x))$$

eine Körpererweiterung L/K, wir nennen sie *elementare Körpererweiterung*.
Ist $f(x) \in K[x]$ ein monisches Polynom, so ist entweder $f'(x) \neq 0$ oder $\mathrm{char}\, K = p$ und $f(x) = x^{pm} + \sum_{j=0}^{m-1} a_j x^{pj}$, also $f(x) = g(x^p)$. Also kann man über Charakteristik p immer $f(x) = g(x^{p^s})$ schreiben, mit einem $g(x)$ für das $g'(x) \neq 0$ ist.
Ein Körper E heiße *algebraisch abgeschlossen*, wenn jedes Polynom $f(x) \in E[x]$ *über* E *in Linearfaktoren zerfällt*, also $f(x) = c\prod_{j=1}^{\deg f}(x - \alpha_j)$ mit $c, \alpha_j \in E$ ist.
Es sei $L = K[x]/(f(x))$ eine elementare Erweiterung und $f(x) = g(x^{p^s})$ wie oben mit $g'(x) \neq 0$ und $n_s = \deg g$ sowie $n_i = p^s$ und $n = \deg f$, also $n = n_i n_s$. Da f irreduzibel, ist auch g irreduzibel.
Ist dann E/K eine Erweiterung mit E algebraisch abgeschlossen, so gibt es

$$\alpha_1, \ldots, \alpha_{n_s} \in E,$$

so daß

$$g(x) = \prod_{i=1}^{n_s}(x - \alpha_i).$$

Wäre ein $\alpha = \alpha_i = \alpha_j$ mit $i \neq j$, so wäre α auch Nullstelle von $g'(x) \neq 0$. Es ist aber $g(\alpha) = 0$, also $g(x) = \mathrm{Irr}(\alpha, K, x)$, also $g'(x) = q(x)g(x)$ im Widerspruch zu $g'(x) \neq 0$.
Zu jedem α_i gehört ein β_i mit $\beta_i^{p^s} - \alpha_i$, so daß gilt $x^{p^s} - \alpha_i = (x - \beta_i)^{p^s}$, also letztlich

$$f(x) = g(x^{p^s}) = \prod_{j=1}^{n_s}(x - \beta_j)^{p^s}$$

Lemma 0.6. *Ist* $\sigma : L = K[x]/(f(x)) \to E$ *eine Einbettung, so ist demzufolge* $\sigma(x) = \beta_i$, *es gibt also genau* n_s *Einbettungen von* L/K *in* E/K.
Dies ist offensichtlich unabhängig von der Wahl des konkreten algebraisch abgeschlossenen Körpers E, entscheidend ist die Zerlegung $f(x) = g(x^{p^s})$, die für Charakteristik 0 immer $f(x) = g(x)$ ist, und für die die Wahl des p^s im Fall von Charakteristik p nur von $f(x) \in K[x]$ abhängt.

Proposition 0.12. *Ist* $f_\nu(x) \in K[x]$ *ein System irreduzibler (monischer) Polynome, so gibt es stets einen Erweiterungskörper* L/K, *so daß in* $L[x]$ *jedes* f_ν *in Linearfaktoren zerfällt.*

Beweis. Wir konstruieren ihn schrittweise, indem wir ein $f = f_{\nu_0}$ auswählen und die elementare Erweiterung $L' = K[x]/(f(x)) = K(\alpha)$ bilden.
In ihr faktorisieren wir alle f_ν und nennen das so entstandene System aller irreduziblen Faktoren f'_μ. Wir nehmen an, daß in den f'_μ alle Linearfaktoren weggeworfen sind, insbesondere $x - \alpha$ von $f(x)$. Also ist $\sum_\mu \deg f'_\mu < \sum_\nu \deg f_\nu$ und induktiv gelangt man nach endlich vielen elementaren Erweiterungen zu einem Zerfällungskörper L/K. □

Theorem 0.3. *Es sei* K *ein Körper. Dann gibt es stets eine algebraische Körpererweiterung* E/K *mit* E *algebraisch abgeschlossen.*

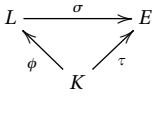
Beweis. Wir konstruieren aus dem Körper K einen algebraischen Erweiterungskörper $K^\sharp/K$. Dazu bilden wir den Polynomring $R = K[(X_f)]$ mit einer Unbestimmten X_f für jedes irreduzible, monische $f \in K[X]$. Es sei das Ideal $I = (f(X_f)) \subseteq R$. Es ist $I \neq (1)$, denn sonst wäre $s = \sum_{j=1}^m g_j((X_f))f_j(X_{f_j}) = 1$. Im Zerfällungskörper L/K haben die $f_j(X)$ die Nullstellen α_j. Die Abbildung $X_{f_j} \mapsto \alpha_j$ und $X_f \mapsto 0$ für $f \neq f_j$ würde also $s = 1$ in L auf Null abbilden. Also gibt es ein maximales Ideal $\mathfrak{m} \supseteq I$ in R und es sei $K^\sharp = R/\mathfrak{m}$. Alle Polynome $g \in K[x]$ zerfallen in $K^\sharp[x]$ in Linearfaktoren.
Man nenne nun $K_0 = K$ und $K_1 = K^\sharp \supseteq K_0$. Iterativ bilde man dann $K_{i+1} = K_i^\sharp$. Die Vereinigung $E = \bigcup_i K_i$ ist algebraisch abgeschlossen und algebraisch über K. □
Der so konstruierte E/K heißt *algebraischer Abschluß von* K. Wir schreiben $E = \bar{K}$.

Separabilität Es sei E ein algebraisch abgeschlossener Körper über K.

Lemma 0.7. *Für ein* $f \in K[x]$ *ist äquivalent*

a) f *hat keine mehrfachen Nullstellen in* E.
b) $f'(\alpha) \neq 0$ *für jede Nullstelle* $f(\alpha) = 0$ *mit* $\alpha \in E$.
c) $(f, f') = (1)$ *in* $K[x]$

Man nennt ein solches f dann *separabel als Polynom in* $K[x]$. Ein $\alpha \in L$ mit L/K heißt *separabel über* K, wenn $f(x) = \mathrm{Irr}(\alpha, K, x) \in K[x]$ separabel in $K[x]$ ist. Dies ist äquivalent zur Existenz eines beliebigen separablen $g(x) \in K[x]$ mit $g(\alpha) = 0$ und zur Existenz eines separablen $h(x) \in E[x]$ mit einer Erweiterung E/K und $h(x) = f(x)q(x)$ in $E[x]$.
Ist ein Dreieck von Körpererweiterungen



gegeben, in dem ϕ und τ fix seien, so sei die Gesamtheit der möglichen σ mit $\mathrm{Hom}_{K,\tau}(L, E)$ bezeichnet. Ist $M/L/K$ ein Körperturm, so hat man für $\tau : K \to E$ eine Bijektion

$$\sigma \in \mathrm{Hom}_{K,\tau}(M, E) \longleftrightarrow (\chi = \sigma|_L \in \mathrm{Hom}_{K,\tau}(L, E), \psi \in \mathrm{Hom}_{L,\chi}(M, E)) \tag{4}$$

Nennt man $n_s = [L : K]_s = \mathrm{card}\,\mathrm{Hom}_{K,\tau}(L, E)$ für einen algebraisch abgeschlossenen Körper E, so ist für eine elementare Körpererweiterung $n_s = [K(\alpha) : K]_s < \infty$ mit dem schon weiter oben so benannten n_s. Es ist dann auch

$$[K(\alpha) : K] = [K(\alpha) : K]_s [K(\alpha) : K]_i = n_s n_i = n$$

mit $n_i = p^s$, dem sogenannten *Inseparabilitätsgrad*, der nur im Fall von Charakteristik p ungleich 1 sein kann.
Sind im Körperturm von (4) alle Erweiterungen elementar und ist E algebraisch abgeschlossen, so haben alle $\mathrm{Hom}_{L,\chi}(M, E)$ dieselbe Kardinalität (Lemma 0.6) und es ist

$$[M : K]_s = [M : L]_s [L : K]_s \tag{5}$$

$$[M : K]_i = [M : L]_i [L : K]_i \tag{6}$$

$$[M : K] = [M : L][L : K] \tag{7}$$

Ebenso ist dann $[M : K]_s = \mathrm{Hom}_{K,\tau}(M, E)$ unabhängig von der Wahl von E und τ. Dies gilt also für jedes M/K endlich und damit kann die Entsprechung (4) auf *beliebige* Körpertürme $M/L/K$ angewandt werden und die Gleichungen (5), (6) (und (7)) gelten dann ebenso.

Definition 0.4. *Eine Körpererweiterung* L/K *heißt* separabel *wenn sie algebraisch ist und jedes* $\alpha \in L$ *über* K *separabel ist.*

Lemma 0.8. *Ein Element* $\alpha \in L$ *mit* L/K *ist separabel, genau dann, wenn* $[K(\alpha) : K] = [K(\alpha) : K]_s$ *ist. Es ist dann jedes* $\beta \in K(\alpha)$ *über* K *separabel.*

Lemma 0.9. *Ist* L/K *eine endliche Körpererweiterung, so ist* L/K *separabel, wenn* $[L : K] = [L : K]_s$ *ist.*

Benutze $[L : K(\alpha)]_s [K(\alpha) : K]_s = [L : K]_s$ und $[L : K(\alpha)][K(\alpha) : K] = [L : K]$.

Lemma 0.10. *Ist* L/K *eine Körpererweiterung und* $\alpha \in L$ *separabel über* K *und ist* LE/E *eine Basiserweiterung mit* E/K, *so ist* α *auch separabel über* E.

Ist nämlich $f(x) = \mathrm{Irr}(\alpha, K, x) \in K[x]$, so daß $(f, f') = (1)$, so ist $g(x) = \mathrm{Irr}(\alpha, E, x) \in E[x]$ ein Teiler $g \mid f$ in $E[x]$ und daher ohne mehrfache Nullstellen in $\bar{E}$.

Lemma 0.11. *Sind* $\alpha_1, \alpha_2 \in L/K$, *separabel über* K, *so ist* $K(\alpha_1, \alpha_2)/K(\alpha_1)/K$ *ein separabler Körperturm und daher* $\alpha_1 + \alpha_2, \alpha_1 - \alpha_2, \alpha_1\alpha_2 \in L$ *separabel über* K.

Proposition 0.13. *Separable Erweiterungen sind verträglich mit Körpertürmen und Basiserweiterungen.*

Dedekindringe

Normen

Komplettierungen

Differenten und Diskrimianten

Klassengruppe

Einheitengruppe

Adele und Idele

Jürgen Böhm, Wertheim, 1. Juni 2026