Jürgen Böhm

Algebraische Zahlentheorie

3. Oktober 2018

Für V N und R G

Vorwort

Dieses Buch ist eine Einführung in die algebraische Zahlentheorie.

Einige Grundbegriffe aus der kommutativen Algebra und allgemeinen Körpertheorie werden in einleitenden Kapiteln bereitgestellt.

Das Buch orientiert sich an Langs „Algebraic Number Theory“ [2] und an dem Sammelband von Cassels/Fröhlich [1].

Der Autor freut sich über Rückmeldungen an

mathematik@aviduratas.de

mit allgemeinen Kommentaren zu dem Buch, besonders aber mit Meldungen über gefundene Fehler und problematische Stellen.

Wilhermsdorf, 2015 - *Jürgen Böhm*

Inhaltsverzeichnis

1

Grundlagen

1.1 Ganze Ringerweiterungen

Proposition 1.1.1. *Es sei B eine A–Algebra und $x \in B$. Dann ist für x äquivalent*

a) die Gleichung

$$x^n + a_1\, x^{n-1} + \cdots + a_{n-1}\, x + a_n = 0 \tag{1.1}$$

gilt für irgendwelche $a_1, \ldots, a_n \in A$.

b) die Unteralgebra $A[x] \subseteq B$ ist ein endlich erzeugter A–Modul.

c) es gibt eine Unteralgebra $C \subseteq B$ mit $x \in C$ und $1 \in C$ und C ist endlich erzeugter A–Modul.

d) es gibt einen endlich erzeugten A–Modul M sowie einen A–linearen Homomorphismus

$$\phi : A[x] \to \mathrm{End}_A(M)$$

und $\phi(A[x])$ operiert treu auf M.

Beweis. Die Implikationen a) ⇒ b) ⇒ c) ⇒ d) sind direkt einzusehen. Bleibt d) ⇒ a). Es sei also $M = A\, m_1 + \cdots + A\, m_n$ und

$$\phi(x)\ m_i = \sum a_{ij}\, m_j$$

Also gilt für die Matrix

$$A^x = (a_{ij} - \delta_{ij}\, \phi(x))$$

mit Einträgen in $\mathrm{End}_A(M)$, daß

$$A^x\, (m_1, \ldots, m_r)^t = (0, \ldots, 0)^t.$$

Multipliziert man von links mit $(A^x)_{\mathrm{ad}}$ und nennt

$$\chi(T) = T^n + c_1 T^{n-1} + \cdots + c_{n-1} T + c_n$$

das charakterische Polynom von A^x, das die Beziehung

$$A^x{}_{\mathrm{ad}}\, A^x = \chi(\phi(x))E$$

erfüllt, so folgt $\chi(\phi(x))\, m_i = 0$ für alle i, also $\chi(\phi(x))M = 0$. Weiter ist aber $\chi(\phi(x)) = \phi(\chi(x))$ und da $\phi(A[x])$ treu auf M operiert, ist $\chi(x) = 0$. Damit ist aber a) gezeigt.

Definition 1.1.1. *Es sei B eine A–Algebra und $x \in B$ erfülle eine der Bedingungen der vorangehenden Proposition. Dann heißt x* ganz über A.

Sind alle $x \in B$ ganz über A so heißt B ganz über A.

Proposition 1.1.2. *Es sei B eine A–Algebra und $x, y \in B$ ganz über A. Dann ist auch $x + y$, $x - y$, $x\, y \in B$ ganz über A.*

Beweis. Es ist $A[y]$ ein endlich erzeugter A–Modul mit $1 \in A[y]$. Also ist $A[x, y]$ ein endlich erzeugter $A[x]$–Modul mit $1 \in A[x, y]$. Da $A[x]$ ein endlich erzeugter A–Modul ist, ist $A[x, y]$ sogar ein endlich erzeugter A–Modul. Da $(x + y)\, A[x, y] \subseteq A[x, y]$ ist $x + y$ ganz über A (nach Proposition 1.1.1 c)). Ebenso $x - y$ und xy.

Proposition 1.1.3. *Es sei C eine B–Algebra und B eine A–Algebra sowie C ganz über B und B ganz über A. Dann ist auch C ganz über A.*

Beweis. Es sei $x \in C$. Dann ist $x^n + b_1 x^{n-1} + \cdots + b_n = 0$ mit irgendwelchen $b_i \in B$. Der Ring $C' = A[b_1, \ldots, b_n, x]$ ist ein endlich erzeugter A–Modul mit $1 \in C'$ und $x\, C' \subseteq C'$. Also ist x ganz über A.

Definition 1.1.2. *Es sei B eine A–Algebra. Dann heiße die Gesamtheit der $x \in B$, die ganz über A sind, der* ganze Abschluß von A in B. *Wir schreiben auch $\bar{A}$ für diesen Ring.*

Anmerkung 1.1.1. Nach voriger Proposition ist $\bar{A}$ eine Ringerweiterung von A, es ist $A \subseteq \bar{A} \subseteq B$.

Proposition 1.1.4. *Es sei B eine A–Algebra, $x \in B$ und $\mathfrak{a}$ ein Ideal von A. Gegeben seien die Behauptungen*

a) die Gleichung

$$x^n + a_1\, x^{n-1} + \cdots + a_{n-1}\, x + a_n = 0 \tag{1.2}$$

gilt für irgendwelche $a_1, \ldots, a_n \in \mathfrak{a}$.

b) Es gibt einen endlich erzeugten A–Modul M, einen Homomorphismus

$$\phi : A[x^m] \to \mathrm{End}_A(M),$$

es operiere $\phi(A[x^m])$ treu auf auf M und es gelte

$$x^m\, M \subseteq \mathfrak{a}M$$

c) Es ist

$$x \in \sqrt{\mathfrak{a}B}.$$

Dann gilt b) $\Leftrightarrow$ a) und a) $\Rightarrow$ c). Ist überdies B ganz über A, so gilt auch c) $\Rightarrow$ a).

Beweis. Um a) $\Rightarrow$ b) einzusehen, setze $M = A[x]$. Es ist dann $x^n \cdot M \subseteq (a_1, \ldots, a_n)\, M$. Da $1 \in M$ operiert $A[x^n]$ treu auf M. Für b) $\Rightarrow$ a) erkennt man aus den Überlegungen von Proposition 1.1.1, daß x^m eine Ganzheitsgleichung mit Koeffizienten aus $\mathfrak{a}$ erfüllt. Also gilt dies auch für x.

Im Fall c) $\Rightarrow$ a) betrachte man $x^n = a_1\, b_1 + \cdots + a_r\, b_r$ und setze $M = A[b_1, \ldots, b_r]$. Es ist dann $x^n\, M \subseteq (a_1, \ldots, a_r)M$ und x^n operiert wegen $1 \in M$ treu auf M. Also ist wegen b) auch a) erfüllt.

Definition 1.1.3. *Erfüllt in den Bezeichnungen der vorangehenden Proposition x die Bedingung a), so heißt x* ganz über $\mathfrak{a}$.

Proposition 1.1.5. *Es sei B eine A–Algebra und $x, y \in B$ ganz über $\mathfrak{a}$. Dann ist auch $x + y$, $x - y$, $x\, y \in B$ ganz über $\mathfrak{a}$.*

Beweis. Der Ring $B' = A[x, y]$ ist ganz über A und es ist $x^m \in \mathfrak{a}B'$ sowie $y^n \in \mathfrak{a}B'$. Also ist $(x + y)^{(m+n)} \in \mathfrak{a}B'$ bzw. $(x\, y)^{\max(m,n)} \in \mathfrak{a}B'$. Also ist $x + y$ bzw. $x\, y$ nach Proposition 1.1.4 c) ganz über $\mathfrak{a}$.

Proposition 1.1.6. *Es sei $A \subseteq B$ eine ganze Ringerweiterung von Integritätsringen. Dann ist äquivalent*

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

Beweis. Es sei A ein Körper und $b \in B$ mit minimaler Ganzheitsgleichung

$$b^m + a_1\, b^{m-1} + \cdots + a_{m-1}\, b + a_m = 0$$

wobei $a_m \neq 0$ ist. Damit ist dann aber auch

$$-a_m^{-1} \left(b^{m-1} + a_1\, b^{m-2} + \cdots + a_{m-1}\right) b = 1$$

und also b in B invertierbar.

Umgekehrt sei B ein Körper, $a \in A$ und $a\, b = 1$. Wieder erfülle b die obige Ganzheitsgleichung. Multiplizieren wir diese mit a^{m-1} durch, so folgt direkt $b \in A$ und A ist als Körper nachgewiesen.

Proposition 1.1.7. *Es sei $\phi : A \to B$ eine ganze Ringerweiterung. Weiter sei $S \subseteq A$ multiplikativ abgeschlossen. Dann ist auch $S^{-1}(\phi) : S^{-1}A \to S^{-1}B$ eine ganze Ringerweiterung.*

Insbesondere ist $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ eine ganze Ringerweiterung für alle $\mathfrak{p} \subseteq A$ prim.

Proposition 1.1.8. *Es sei B eine A–Algebra und $\bar{A}$ der ganze Abschluß von A in B. Weiter sei $S \subseteq A$ multiplikativ abgeschlossen. Dann ist*

$$(S^{-1}A)^- = S^{-1}\bar{A} \subseteq S^{-1}B.$$

wobei links der ganze Abschluß von $S^{-1}A$ in $S^{-1}B$ steht.

Proposition 1.1.9. *Es sei $\phi : A \to B$ eine ganze Ringerweiterung und $\mathfrak{a} \subseteq A$ ein Ideal von A sowie $\mathfrak{b} \subseteq B$ ein Ideal von B. Dann ist auch*

1. *$A/\mathfrak{a} \to B/\mathfrak{a}B$ eine ganze Ringerweiterung.*
2. *$A/\phi^{-1}(\mathfrak{b}) \to B/\mathfrak{b}$ eine ganze Ringerweiterung.*

Proposition 1.1.10. *Es sei $i : A \subseteq B$ eine ganze Ringerweiterung. Dann gilt*

1. *(Lying Over) Für jedes Primideal $\mathfrak{p} \subseteq A$ existiert ein Primideal $\mathfrak{q} \subseteq B$ mit $\mathfrak{q} \cap A = \mathfrak{p}$. Man sagt* $\mathfrak{q}$ liegt über $\mathfrak{p}$.
2. *(Unvergleichbarkeit) Sind $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq B$ prim mit $\mathfrak{q}_i \cap A = \mathfrak{p}$, so ist $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Beweis. Lying Over: Da $B_\mathfrak{p} \supseteq A_\mathfrak{p}$ ganz, kann man $\mathfrak{p}$ maximal annehmen. Es genügt zu zeigen, daß $1 \notin \mathfrak{p}B$. Andernfalls wäre 1 ganz über $\mathfrak{p}$, also $1^r + a_1 1^{r-1} + \cdots + a_r = 0$ mit $a_i \in \mathfrak{p}$, also $1 \in \mathfrak{p}$ Widerspruch.

Unvergleichbarkeit: Wieder ist $B_\mathfrak{p} \supseteq A_\mathfrak{p}$ ganz. Man kann also $\mathfrak{p}$ maximal annehmen. Betrachte dann $B/\mathfrak{q}_1 \supseteq A/\mathfrak{p}$, ganz. Rechts steht ein Körper, also auch links. Also ist $\mathfrak{q}_2/\mathfrak{q}_1 = 0$, also $\mathfrak{q}_2 = \mathfrak{q}_1$.

Mit anderen Worten: Im vorliegenden Fall ist $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ surjektiv.

Korollar 1.1.1. *Es sei $A \subseteq B$ eine ganze Ringerweiterung. Weiter sei $\mathfrak{p}_2 \supseteq \mathfrak{p}_1$, mit $\mathfrak{p}_i \in \operatorname{Spec}(A)$, und $\mathfrak{q}_1 \in \operatorname{Spec}(B)$, so daß $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$ ist.*

Dann existiert ein Primideal $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$ von B mit $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

Korollar 1.1.2 (Going-Up). *Es sei $A \subseteq B$ eine ganze Ringerweiterung und es sei $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ eine echt aufsteigende Primidealkette in A. Weiter sei $\mathfrak{q}_1 \in \operatorname{Spec}(B)$ mit $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.*

Dann existiert eine echt aufsteigende Primidealkette $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ in B für die $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ ist.

Definition 1.1.4. *Es sei A ein kommutativer Ring. Dann heißt A* normal, *falls für alle $\mathfrak{p} \subseteq A$, prim, der Ring $A_\mathfrak{p}$ integer und ganzabgeschlossen in $Q(A_\mathfrak{p})$ ist.*

Lemma 1.1.1. *Es sei A ein Integritätsring. Dann ist A genau dann normal, wenn A in $Q(A)$ ganzabgeschlossen ist.*

Lemma 1.1.2. *Es sei A ein normaler, noetherscher Ring. Dann ist $A = A_1 \times \cdots \times A_r$ mit normalen Integritätsringen A_i.*

Beweis. Es seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die minimalen Primideale von A. Dann ist $\mathfrak{p}_i + \mathfrak{p}_j = 1$, denn für ein maximales Ideal $\mathfrak{m} \supseteq \mathfrak{p}_i, \mathfrak{p}_j$ wäre $A_\mathfrak{m}$ nicht integer.

Außerdem ist $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = (0)$. Sei nämlich $x \in \mathfrak{p}_i$ für alle i und es sei $Ax \subseteq A$ ein von Null verschiedener A–Modul. Dann muß $A_\mathfrak{q} \supseteq (Ax)_\mathfrak{q} \neq 0$ für ein Primideal $x \in \mathfrak{p}_i \subseteq \mathfrak{q} \subseteq A$ sein. Da $(\mathfrak{p}_i)_\mathfrak{q} = 0$ folgt $x/1 = 0$ in $A_\mathfrak{q}$ im Widerspruch zu $(Ax)_\mathfrak{q} \neq 0$. Also $x = 0$.

Aus dem Chinesischen Restsatz folgt nun $A = A/\mathfrak{p}_1 \times \cdots \times A/\mathfrak{p}_r$.

Proposition 1.1.11. *Es sei A ein noetherscher Integritätsring, A ganz abgeschlossen in $K = Q(A)$, seinem Quotientenkörper. Dann ist*

$$A = \bigcap_{\substack{\mathfrak{p} \subseteq A \\ \operatorname{ht} \mathfrak{p} = 1}} A_{\mathfrak{p}}.$$

Beweis. Es sei f in allen $A_{\mathfrak{p}}$ mit $\operatorname{ht} \mathfrak{p} = 1$ enthalten. Betrachte den A–Modul $M = (A + A\,f)/A$. Ist f nicht von vornherein in A, so gibt es ein $h \in A$ mit $\operatorname{Ann}_M(h\,f) = \mathfrak{q}$ für ein Primideal $\mathfrak{q} \subsetneq A$. Dies folgt aus der Theorie der assoziierten Primideale zum Modul M. Das Ideal $\mathfrak{q}$ ist ungleich (0), enthält also ein Primideal $\mathfrak{p}' \subseteq \mathfrak{q}$ der Höhe 1. Es gilt also

$$\mathfrak{p}'\,h\,f \subseteq A$$

Nun ist aber für $x \in \mathfrak{p}'$ wegen $v_{\mathfrak{p}'}(f) \geqslant 0$ auch $v_{\mathfrak{p}'}(x\,h\,f) > 0$, also $x\,h\,f \in \mathfrak{p}'$. Damit hat man

$$\mathfrak{p}'\,h\,f \subseteq \mathfrak{p}'$$

und also $h\,f \in A$, weil A normal. Daraus folgte aber $\operatorname{Ann}_M(h\,f) = A \neq \mathfrak{q}$, so daß doch f von vornherein in A gelegen haben muß.

Proposition 1.1.12. *Es sei $A \subseteq B$ ganz abgeschlossen und A noethersch. Dann ist auch $A[x] \subseteq B[x]$ ganz abgeschlossen.*

Beweis. Es sei $f = b_s\,x^s + \cdots + b_0$ ganz über $A[x]$. Es gibt also eine Gleichung

$$f^m + a_1(x)\,f^{m-1} + \cdots + a_m(x) = 0$$

Also ist jeder Koeffizient $b_{j,r}$ von x^j eines beliebigen f^r als Linearkombination über A von den endlich vielen $b_{j,r'}$ mit $1 \leqslant r' \leqslant m-1$ darstellbar. Insbesondere ist $A[b_s]$ ein endlich erzeugter A–Modul. Damit ist dann b_s ganz über A, also in A. Nun betrachte man $f - b_s\,x^s$, das ebenfalls ganz über $A[x]$ ist. Induktiv folgt, daß alle $b_i \in A$ sind.

Lemma 1.1.3. *Es sei $A \subseteq K = Q(A)$ normal und B/A eine Ringerweiterung mit B integer und $L = Q(B)$. Es sei $b \in B$ ganz über einem Ideal $\mathfrak{a} \subseteq A$, also $f(b) = 0$ mit*

$$f(b) = b^m + a_1\,b^{m-1} + \cdots + a_m = 0$$

wobei alle $a_i \in \mathfrak{a}$ sind. Es sei nun

$$g(b) = b^r + w_1\,b^{r-1} + \cdots + w_r = 0$$

das Minimalpolynom von b über K. Dann sind alle $w_i \in \sqrt{\mathfrak{a}}$.

Beweis. Wir führen den algebraischen Abschluß $\bar{L} \supseteq L \supseteq B$ von L über K ein. Dann zerfällt $f(T) = (T - \lambda_1) \cdot \cdots \cdot (T - \lambda_m)$ in Linearfaktoren über $\bar{L}$. Alle λ_i sind ganz über $\mathfrak{a}$. Nun gilt $g(T) \mid f(T)$ in $K[T]$ weil $g(T)$ ein Minimalpolynom für b ist. Also sind die w_i Polynome in einer Teilmenge der λ_i mit ganzzahligen Koeffizienten. Also sind die w_i ganz über $\mathfrak{a}$. Da A normal, ist dann auch $w_i \in A$ und jedes w_i erfüllt eine Gleichung $w_i^{n_i} + a_{i,1}\,w_i^{n_i-1} + \cdots + a_{i,n_i} = 0$ mit $a_{i,j} \in \mathfrak{a}$. Also auch $w_i \in \sqrt{\mathfrak{a}}$.

Proposition 1.1.13 (Going-Down-Theorem). *Es sei A ein normaler Ring, B ein Integritätsring und $B \supseteq A$ ganz. Weiter seien $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ zwei Primideale von A und $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ ein Primideal von B über $\mathfrak{p}_2$.*

Dann existiert ein Primideal $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ mit $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

Beweis. Wir können annehmen, daß zwischen $\mathfrak{p}_1$ und $\mathfrak{p}_2$ keine weiteren Primideale liegen. Es sei $B' = B_{\mathfrak{q}_2}$. Wir zeigen $\mathfrak{p}_1 B' \cap A = \mathfrak{p}_1$. Es ist dann für ein $f \in \mathfrak{p}_2 \notin \mathfrak{p}_1$ das Ideal $(\mathfrak{p}_1 B')_f$ ungleich dem Einsideal B'_f. Ein Primideal von $(B'/\mathfrak{p}_1 B')_f$ liefert das gesuchte $\mathfrak{q}_1$.

Es sei nun $x \in \mathfrak{p}_1 B' \cap A$. Also $x = b/s$ mit $b \in \mathfrak{p}_1 B$ und $s \notin \mathfrak{q}_2$.

Das Minimalpolynom von b über K ist nach vorigem Lemma

$$b^r + a_1\, b^{r-1} + \cdots + a_r = 0$$

mit Koeffizienten $a_i \in \mathfrak{p}_1$, denn b ist als Element von $\mathfrak{p}_1 B$ ganz über $\mathfrak{p}_1$.

Nun ist $s = b/x$. Sein Minimalpolynom entsteht durch Multiplikation des Polynoms für b mit x^{-r}:

$$(b/x)^r + (a_1/x)\,(b/x)^{r-1} + \cdots + a_r/x^r = 0, \quad b/x = s$$

Da s ganz über A ist, kann man sein Minimalpolynom auch als

$$s^r + a'_1\, s^{r-1} + \cdots + a'_r = 0$$

mit $a'_i \in A$ schreiben. Es ist damit $a'_i = a_i/x^i$, also $a'_i\, x^i = a_i \in \mathfrak{p}_1$. Wäre jetzt $x \notin \mathfrak{p}_1$, so wäre $a'_i \in \mathfrak{p}_1$ für alle i. Damit wäre s ganz über $\mathfrak{p}_1$, also $s \in \sqrt{\mathfrak{p}_1 B} \subseteq \sqrt{\mathfrak{p}_2 B} \subseteq \mathfrak{q}_2$ im Widerspruch zur Voraussetzung.

Wir geben im Folgenden noch einen zweiten Beweis für das Going-Down-Theorem, der einem anderen Gedankengang folgt.

Lemma 1.1.4. *Es sei $B \supseteq A$ eine ganze Ringerweiterung. Die Ringe A, B seien integer mit $Q(A) = K$ und $Q(B) = L$. Weiter sei A normal und L/K galoissch mit Galoisgruppe $G = \mathrm{Gal}(L : K)$.*

Es sei $\mathfrak{b} \subseteq B$ ein Ideal mit $\mathfrak{b}^\sigma \subseteq \mathfrak{b}$ für alle $\sigma \in G$.

Dann ist

$$\mathfrak{b} \subseteq \sqrt{(\mathfrak{b} \cap A)B}$$

Beweis. Es sei $x \in \mathfrak{b}$ und $G = \{\sigma_1, \ldots, \sigma_r\}$. Dann ist $f(x) = (x - x^{\sigma_1}) \cdot \cdots \cdot (x - x^{\sigma_r})$ ein monisches Polynom dessen Koeffizienten a_i in $\cdots + a_i x^i + \cdots$ unter G invariant sind. Also sind sie aus $K \cap \mathfrak{b}$, also, weil A normal, aus $A \cap \mathfrak{b}$. Damit ist die Aussage gezeigt.

Proposition 1.1.14. *Es sei $B \supseteq A$, $L \supseteq K$ und $G = \mathrm{Gal}(L : K)$ wie im vorigen Lemma. Insbesondere A normal.*

Es sei $\mathfrak{p} \subseteq A$ prim und $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ die Primideale von B über $\mathfrak{p}$, also mit $\mathfrak{q}_i \cap A = \mathfrak{p}$.

Dann operiert G transitiv auf den $\mathfrak{q}_i$.

Beweis. Daß $B^G \subseteq B$ und daß $\mathfrak{q}^\sigma$ prim in B für $\mathfrak{q} \subseteq B$ prim und $\sigma \in G$ ist klar.

Betrachte $\mathfrak{b} = \mathfrak{q}_1^{\sigma_1} \cdots \mathfrak{q}_1^{\sigma_r}$ mit den σ_i wie im vorigen Beweis. Dann ist nach vorigem Lemma $\mathfrak{b} \subseteq \sqrt{(\mathfrak{b} \cap A)B} \subseteq \sqrt{\mathfrak{p}B} \subseteq \mathfrak{q}_j$ für jedes $j \geqslant 2$. Also ist mindestens ein $\mathfrak{q}_1^{\sigma_i} \subseteq \mathfrak{q}_j$, also wegen Unvergleichbarkeit diesem gleich. Damit ist alles gezeigt.

Proposition 1.1.15. *Es sei $B \supseteq A$ eine ganze Erweiterung von Integritätsringen, $B = A[\alpha]$ mit $\alpha \in B$ und A normal.*

Weiter seien $L \supseteq K$ die Quotientenkörper und L/K galoissch mit Galoisgruppe $G = \{\sigma_1, \ldots, \sigma_n\}$.

Es seien $\mathfrak{p} \subseteq A$ und $\mathfrak{q} \subseteq B$ zwei maximale Ideale mit $\mathfrak{q} \cap A = \mathfrak{p}$. Es gelte $\mathfrak{q}^{\sigma_i} = \mathfrak{q}$.

Dann induziert jedes $\sigma_i : B \to B$ eine Abbildung $\bar{\sigma}_i : B/\mathfrak{q} \to B/\mathfrak{q}$. Diese Zuordnung $\sigma_i \mapsto \bar{\sigma}_i$ ist eine Surjektion $G \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$.

Beweis. Es sei $F(X) \in A[X]$ das Minimalpolynom von α über K. Dann ist $B = A[X]/(F(X))$.

Es sei nämlich $0 \to I \to A[X] \to A[\alpha] \to 0$ exakt und definiere ein Ideal I von $A[X]$. Ist dann $P(X) \in I$, so ist $P(X) = F(X)Q(X)$ in $K[X]$. Da aber $F(X)$ monisch und $P(X) \in A[X]$, so ist auch $Q(X) \in A[X]$, also $I = F(X)A[X]$.

Es sei $G(X) \in (A/\mathfrak{p})[X]$ das Minimalpolynom von $\alpha + \mathfrak{q}$ über $A/\mathfrak{p}$. Da über $\mathfrak{p}$ nur das Ideal $\mathfrak{q}$ liegt, ist $\bar{F}(X) = G(X)^e$, wobei $\bar{F}(X)$ das Bild von $F(X)$ unter $A[X] \to (A/\mathfrak{p})[X]$ ist.

Man bette $\bar{F}(X)$ mit der Injektion $(A/\mathfrak{p})[X] \hookrightarrow (B/\mathfrak{q})[X]$ ein. Dann entsteht aus der Gleichung

$$F(X) = \prod_i (X - \alpha^{\sigma_i})$$

in $B[X]$ die Beziehung

$$\bar{F}(X) = \prod_i (X - (\alpha^{\sigma_i} + \mathfrak{q})) = \prod_i \left(X - (\alpha + \mathfrak{q})^{\bar{\sigma}_i}\right)$$

in $(B/\mathfrak{q})[X]$.

Also ist wegen $\bar{F}(X) = G(X)^e$ jede Nullstelle von $G(X)$ in $Q(A/\mathfrak{p})^-$ schon in $B/\mathfrak{q}$ und gleich einem $(\alpha + \mathfrak{q})^{\bar{\sigma}_i} = \alpha^{\sigma_i} + \mathfrak{q}$. Ein Automorphismus $\tau : B/\mathfrak{q} \to B/\mathfrak{q}$ über $A/\mathfrak{p}$ ist aber durch seinen Wert $\tau(\alpha + \mathfrak{q})$, der eine Nullstelle von $G(X)$ sein muß festgelegt. Damit ist aber $\tau(\alpha + \mathfrak{q}) = \bar{\sigma}_i(\alpha + \mathfrak{q})$, also $\tau = \bar{\sigma}_i$.

Proposition 1.1.16 (Going-Down-Galois). *Es sei $B \supseteq A$, $L \supseteq K$ und $G = \mathrm{Gal}(L : K)$ wie im vorigen Lemma. Insbesondere A normal.*

Es seien $\mathfrak{p}' \subseteq \mathfrak{p}$ zwei Primideale von A und $\mathfrak{q} \subseteq B$ ein Primideal mit $\mathfrak{q} \cap A = \mathfrak{p}$.

Dann existiert ein Primideal $\mathfrak{q}' \subseteq \mathfrak{q}$ von B mit $\mathfrak{q}' \cap A = \mathfrak{p}'$.

Beweis. Mit Übergang zu $B_\mathfrak{p}$ und $A_\mathfrak{p}$ kann man, wie üblich, $\mathfrak{p}$ maximal annehmen. Es seien $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_s$ die Primideale von B über $\mathfrak{p}'$. Dann sei $\mathfrak{b} = \prod_{\sigma \in G} (\mathfrak{q}'_1)^\sigma = (\mathfrak{q}'_1 \cdots \mathfrak{q}'_s)^k$ mit $k = r/s$. Weiter ist $\mathfrak{b} \subseteq \sqrt{(\mathfrak{b} \cap A)B} \subseteq \sqrt{\mathfrak{p}'B} \subseteq \sqrt{\mathfrak{p}B} \subseteq \mathfrak{q}$. Also muß wenigstens ein $\mathfrak{q}_1'^\sigma \subseteq \mathfrak{q}$ sein. Damit ist alles gezeigt.

Proposition 1.1.17 (Going-Down-Inseparabel). *Es sei $B \supseteq A$ eine ganze Erweiterung von Integritätsringen. Die Erweiterung der Quotientenkörper L/K sei rein inseparabel,* $\operatorname{char} K = p$ *und A normal in K.*

Dann gilt

1. *Über jedem Primideal $\mathfrak{p} \subseteq A$ existiert genau ein Primideal $\mathfrak{q} \subseteq B$ mit $\mathfrak{q} \cap A = \mathfrak{p}$.*
2. *Es seien $\mathfrak{p}' \subseteq \mathfrak{p}$ zwei Primideale von A und $\mathfrak{q}'$, $\mathfrak{q}$ die darüber liegenden Primideale von B. Dann gilt $\mathfrak{q}' \subseteq \mathfrak{q}$.*

Beweis. Es sei $x \in L$. Dann ist $x^{p^m} - z = 0$ für ein $z \in K$. Ist $x \in B$, so ist $z \in B \cap K = A$. Ist $x \in \mathfrak{b}$, dann ist $z \in \mathfrak{b} \cap A \cap K = \mathfrak{b} \cap A$.

Es seien nun $\mathfrak{q}_1$, $\mathfrak{q}_2$ zwei verschiedene Primideale mit $A \cap \mathfrak{q}_i = \mathfrak{p}$. Da sie nicht vergleichbar sind, gibt es $x \in \mathfrak{q}_1 - \mathfrak{q}_2$ und $y \in \mathfrak{q}_2 - \mathfrak{q}_1$.

Nun ist für m geeignet $x^{p^m} \in \mathfrak{q}_1 \cap A = \mathfrak{p}$ und ebenso $y^{p^m} \in \mathfrak{q}_2 \cap A = \mathfrak{p}$. Also $x^{p^m} + y^{p^m} = (x+y)^{p^m} \in \mathfrak{p} \subseteq \mathfrak{q}_i$. Damit ist dann $x + y \in \mathfrak{q}_i$ für $i = 1, 2$, also zum Beispiel auch $x \in \mathfrak{q}_2$ im Widerspruch zur Voraussetzung.

Damit ist 1. gezeigt.

Um 2. einzusehen, wählen wir ein $x \in \mathfrak{q}'$ mit $x^{p^m} \in \mathfrak{q}' \cap A = \mathfrak{p}' \subseteq \mathfrak{p} \subseteq \mathfrak{q}$. Also auch $x \in \mathfrak{q}$, was zu beweisen war.

Proposition 1.1.18 (Going-Down). *Es sei $B \supseteq A$ ganz, B, A integer und A normal. Außerdem sei $[Q(B) : Q(A)] = n$ endlich.*

Es seien $\mathfrak{p}' \subseteq \mathfrak{p} \subseteq A$ zwei Primideale und $\mathfrak{q} \subseteq B$ ein Primideal mit $\mathfrak{q} \cap A = \mathfrak{p}$. Dann existiert ein Primideal $\mathfrak{q}' \subseteq \mathfrak{q}$ von B mit $\mathfrak{q}' \cap A = \mathfrak{p}'$. Also

$$\begin{array}{ccc} \mathfrak{q}' & \hookrightarrow & \mathfrak{q} \\ | & & | \\ \mathfrak{p}' & \hookrightarrow & \mathfrak{p} \end{array}$$

Beweis. Es sei $L = Q(B)$ und $K = Q(A)$. Weiter sei $L_1/L/K$ der kleinste Körper der normal über K ist. Ist $G = \operatorname{Aut}_K(L_1)$, so gilt mit $L_i = L_1^G$:

i) L_1/L_i ist galoissch.
ii) L_i/K ist rein inseparabel.

Weiter sei B_i der ganze Abschluß von A in L_i und B_1 der ganze Abschluß von A in L_1. Es ist dann

$$\begin{array}{ccc} & B_1 & \\ & | \; gal & \\ B & B_i & \\ & | \; insep & \\ & A & \end{array}$$

wobei die Striche für Ganzheitserweiterungen von Ringen stehen.

Es sei nun $\mathfrak{q}_1 \subseteq B_1$ prim mit $\mathfrak{q}_1 \cap B = \mathfrak{q}$. Weiter sei $\mathfrak{q}_i \subseteq B_i$ prim mit $\mathfrak{q}_1 \cap B_i = \mathfrak{q}_i$.

Es ist dann $\mathfrak{q}_i \cap A = \mathfrak{q}_1 \cap B_i \cap A = \mathfrak{q}_1 \cap A = \mathfrak{q}_1 \cap B \cap A = \mathfrak{q} \cap A = \mathfrak{p}$. Also existiert nach Proposition 1.1.17 ein $\mathfrak{q}_i' \subseteq \mathfrak{q}_i \subseteq B_i$ mit $\mathfrak{q}_i' \cap A = \mathfrak{p}'$.

Weiter existiert nach Proposition 1.1.16 ein $\mathfrak{q}_1' \subseteq \mathfrak{q}_1 \subseteq B_1$ mit $\mathfrak{q}_1' \cap B_i = \mathfrak{q}_i'$. Für dieses ist $\mathfrak{q}_1' \cap A = \mathfrak{p}'$ und $\mathfrak{q}' = \mathfrak{q}_1' \cap B \subseteq \mathfrak{q}_1 \cap B = \mathfrak{q}$.

Also ist wegen $\mathfrak{q}' \cap A = \mathfrak{q}_1' \cap B \cap A = \mathfrak{q}_1' \cap A = \mathfrak{p}'$ das gesuchte $\mathfrak{q}' \subseteq \mathfrak{q} \subseteq B$ über $\mathfrak{p}'$ gefunden.

1.2 Algebraische Körpererweiterungen

1.2.1 Allgemeines

Definition 1.2.1. *Es sei L/K eine Körpererweiterung und L sei als Ring über K endlich.*

Wir nennen L eine endliche Körpererweiterung von K.

Es ist dann auch die Vektorraumdimension $\dim_K L = n$ endlich und wir schreiben $[L : K] = n$.

Anmerkung 1.2.1. Es sei A ein Ring und R, S zwei A–Algebren vermöge $\psi : A \to R$, $\phi : A \to S$.

Wir führen dann die explizite Bezeichnung $\mathrm{Hom}_\phi(R, S)$ für $\mathrm{Hom}_A(R, S)$ ein.

1.2.2 Normen und Spuren

Es sei L/K eine endliche algebraische Körpererweiterung und ω also $\omega^1, \ldots, \omega^n$ eine K–Basis des Vektorraums L.

Dann gibt es einen Ringhomomorphimus

$$L \to \mathrm{GL}(n, K), \quad \alpha \mapsto A(\alpha, \omega) = (a_j^i)_{ji}, \quad \alpha\,\omega^i = \omega^j a_j^i \tag{1.3}$$

Es ist mit der Kurzform $\alpha\,\omega = \omega\,A(\alpha)$ leicht zu erkennen, daß wirklich

$$A(\alpha\,\beta, \omega) = A(\alpha, \omega)\,A(\beta, \omega) \tag{1.4}$$

$$A(\alpha + \beta, \omega) = A(\alpha, \omega) + A(\beta, \omega) \tag{1.5}$$

für $\alpha, \beta \in L$ ist.

Ersetzt man ω also $\omega^1, \ldots, \omega^n$ durch ω' also ${\omega^1}', \ldots, {\omega^n}'$ mit $\omega = P\,\omega'$ für ein $P \in \mathrm{GL}(n, K)$. Insgesamt ist dann

$$A(\alpha, \omega) = P^{-1} A(\alpha, \omega') P \tag{1.6}$$

Damit ist $\chi(\alpha)$ in folgender Definition ein wohldefiniertes, nur von α abhängendes Polynom vom Grad n aus $K[\lambda]$:

Definition 1.2.2. *Mit den oben eingeführten Bezeichnungen sei*

$$\chi(\alpha)(\lambda) = \det(\lambda\, E - A(\alpha, \omega))$$

das charakteristische Polynom.

Speziell ist

Definition 1.2.3.

$$\mathrm{Norm}_{L|K}(\alpha) = \det A(\alpha, \omega) \tag{1.7}$$
$$\mathrm{Tr}_{L|K}(\alpha) = \mathrm{Tr}\, A(\alpha, \omega) \tag{1.8}$$

die Normabbildung von L nach K *und die* Spurabbildung von L nach K.

Es ist $\mathrm{Norm}_{L|K}(\beta) \in K$ und $\mathrm{Tr}_{L|K}(\beta) \in K$ und natürlich

$$\mathrm{Norm}_{L|K}(\alpha\,\beta) = \mathrm{Norm}_{L|K}(\alpha)\ \mathrm{Norm}_{L|K}(\beta) \tag{1.9}$$
$$\mathrm{Tr}_{L|K}(\alpha + \beta) = \mathrm{Tr}_{L|K}(\alpha) + \mathrm{Tr}_{L|K}(\beta) \tag{1.10}$$

Proposition 1.2.1. *Es sei L/K eine endliche Körpererweiterung und $\gamma \in L$. Dann ist*

$$\mathrm{Norm}_{L|K}(\gamma) = \big(\mathrm{Norm}_{K(\gamma)|K}(\gamma)\big)^{[L:K(\gamma)]} \tag{1.11}$$
$$\mathrm{Tr}_{L|K}(\gamma) = [L : K(\gamma)]\ \mathrm{Tr}_{K(\gamma)|K}(\gamma) \tag{1.12}$$

Für Körpertürme gilt:

Proposition 1.2.2. *Es sei $M/L/K$ ein Turm von endlichen Körpererweiterungen mit $[M : L] = m$ und $[L : K] = n$. Dann gilt*

$$\mathrm{Norm}_{L|K}\ \mathrm{Norm}_{M|L}(\gamma) = \mathrm{Norm}_{M|K}(\gamma) \tag{1.13}$$
$$\mathrm{Tr}_{L|K}\ \mathrm{Tr}_{M|L}(\gamma) = \mathrm{Tr}_{M|K}(\gamma) \tag{1.14}$$

für alle $\gamma \in M$.

Beweis. Es genügt, dies für $M = L(\gamma)$ zu zeigen. Bezüglich der L–Basis $1, \gamma, \ldots, \gamma^{m-1}$ von M ist γ dargestellt durch

$$A(\gamma) = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_m \\ 1 & 0 & \ldots & 0 & -a_{m-1} \\ \vdots & \ddots & & \vdots & \\ 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix} \tag{1.15}$$

wobei $\gamma^m + a_1\,\gamma^{m-1} + \cdots + a_m$ das Minimalpolynom von γ über L ist. Es ist

$$\mathrm{Tr}_{L(\gamma)|L}(\gamma) = \mathrm{Tr}\, A(\gamma) = -a_1$$

und

$$\mathrm{Norm}_{L(\gamma)|L}(\gamma) = \det A(\gamma) = (-1)^m\, a_m.$$

Ist nun $\omega_1, \ldots, \omega_n$ eine K–Basis von L und führt man die K–Basis $\gamma^i\,\omega_j$ von M ein, so treten an die Stelle der Einsen in der Matrix $A(\gamma)$ $n \times n$–Einheitsmatrizen und an die Stelle der $a_i \in L$ die sie repräsentierenden Matrizen aus $\mathrm{Mat}(n \times n, K)$.

Nennt man die so erzeugte Matrix $B(\gamma)$, so ist $\mathrm{Tr}\, B(\gamma) = \mathrm{Tr}_{L(\gamma)|K}(\gamma)$ und $\det B(\gamma) = \mathrm{Norm}_{L(\gamma)|K}(\gamma)$.

Andererseits ist aufgrund der Struktur von $B(\gamma)$ auch $\mathrm{Tr}\, B(\gamma) = \mathrm{Tr}(-a_1)$ und $\det B(\gamma) = (-1)^{n\,(m-1)} \det(-a_m)$, wobei für a_1, a_m die entsprechenden Matrizen stehen sollen. Nun ist aber

$$\mathrm{Tr}(-a_1) = \mathrm{Tr}_{L|K}(-a_1) = \mathrm{Tr}_{L|K}\,\mathrm{Tr}_{L(\gamma)|L}(\gamma)$$

und entsprechend auch

$$(-1)^{n(m-1)} \det(-a_m) = \mathrm{Norm}_{L|K}((-1)^{m-1}\,(-a_m)) = \mathrm{Norm}_{L|K}\,\mathrm{Norm}_{L(\gamma)|L}(\gamma)$$

Fasst man alle genannten Gleichheiten zusammen, ergibt sich die Behauptung.

1.2.3 Klassen von Körpererweiterungen

Es seien K, L, M drei Körper.

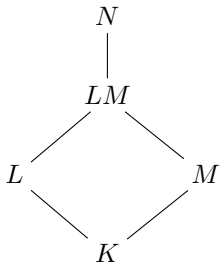
Es sei $M/L/K$ ein Turm von Körpererweiterungen. Das entsprechende Diagramm sei

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array} \tag{1.16}$$

Definition 1.2.4. *Eine Klasse* $\mathbf{K}$ *von Körpererweiterungen*

1. *habe die Eigenschaft* $\mathcal{P}_1$ *wenn aus „*L/K *ist in* $\mathbf{K}$*“ und „*M/L *ist in* $\mathbf{K}$*“ auch* M/K *ist in* $\mathbf{K}$ *folgt.*
2. *habe die Eigenschaft* $\mathcal{P}_2$*, wenn aus „*M/K *ist in* $\mathbf{K}$*“ auch „*L/K *ist in* $\mathbf{K}$*“ und „*M/L *ist in* $\mathbf{K}$*“ folgt.*

Sei jetzt ein Erweiterungsdiagramm



(1.17)

von Körpern N, M, L, K gegeben.

Definition 1.2.5. *Eine Klasse* $\mathbf{K}$ *von Körpererweiterungen habe die Eigenschaft* $\mathcal{P}_3$*, wenn aus „*L/K *ist in* $\mathbf{K}$*“ auch „*LM/M *ist in* $\mathbf{K}$*“ folgt.*

Definition 1.2.6. *Eine Klasse* $\mathbf{K}$ *von Körpererweiterungen habe die Eigenschaft* $\mathcal{P}$*, wenn sie* $\mathcal{P}_1$*,* $\mathcal{P}_2$ *und* $\mathcal{P}_3$ *hat. Die Klasse* $\mathbf{K}$ *ist dann eine* ausgezeichnete Klasse*.*

1.2.4 Algebraischer Abschluß

Anmerkung 1.2.2. Es sei $\phi : K \to L$ ein Körperhomomorphismus und $f(X) = \sum a_i X^i \in K[X]$. Dann schreiben wir $f^\phi(X) = \sum a_i^\phi X^i$.

Proposition 1.2.3. *Es sei* $g(X) \in K[X]$ *irreduzibel und*

$$\begin{array}{ccc} K[X]/(g(X)) & \xrightarrow{\psi} & E \\ \Big| & & \Big| \\ K & \xrightarrow{\phi} & L \end{array} \tag{1.18}$$

ein Diagramm von Körpern. Dann entsprechen sich

$$\psi \in \mathrm{Hom}_K(K[X]/(g(X)), E) \quad \leftrightarrow \quad \{\beta \in E \mid g^\phi(\beta) = 0\} \tag{1.19}$$

Proposition 1.2.4. *Es sei* K *ein gegebener Körper und* $g(X) \in K[X]$ *ein irreduzibles Polynom. Dann gibt es eine Körpererweiterung* L/K *und* $\alpha \in L$ *mit* $g(\alpha) = 0$*.*

Beweis. Man setze nämlich $L = K[X]/(g(X))$ und $\alpha = \bar{X}$ das Bild von X in L.

Proposition 1.2.5. *Es sei nun eine endliche Familie* $(g_i(X))$ *von Polynomen aus* $K[X]$ *gegeben. Dann existiert ein* Zerfällungskörper L/K*, so daß jedes* $g_i(X)$ *eingebettet in* $L[X]$ *in Linearfaktoren zerfällt.*

Beweis. Man zerlege zunächst alle $g_i(X)$ in Faktoren über $K[X]$ und scheide Linearfaktoren aus. Ohne Einschränkung bestehe also $g_i(X)$ nur aus in $K[X]$ irreduziblen Polynomen mit $\deg_X g_i(X) > 1$ Es sei $\Delta = \sum_i \deg_X g_i(X)$.

Man wähle nun eines der $h(X) = g_i(X)$ und konstruiere wie oben $L_1 = K(\alpha) = K[X]/((h(X))$, so daß $h(\alpha) = 0$ wird. Anschließend bette man alle $g_i(X)$ in $K(\alpha)[X]$ ein, faktorisiere in $K(\alpha)[X]$ und scheide Linearfaktoren aus. Es entstehe so eine neue Familie in $L_1[X]$ irreduzibler Polynome $g_j^1(X) \in L_1[X]$.

Dabei wird insbesondere $X - \alpha$ aus $h(X) = g_i(X)$ ausgeschieden und für die verbleibenden $h_p(X)|h(X)$ mit $h_p(X) \in L_1[X]$ und $\deg_X h_p(X) > 1$ ist $\sum_p \deg_X h_p(X) < \deg_X h(X)$. Eine analoge Überlegung für die übrigen $g_i(X)$ zeigt, daß die Größe Δ beim Übergang zu $(g_j^1(X))$ echt abnimmt.

Man gelangt also nach endlich vielen Schritten zu einem Körper L'/K, in dem jedes $g_i(X)$ in Linearfaktoren zerfallen ist.

Proposition 1.2.6. *Es sei K ein gegebener Körper. Dann existiert ein Körper $\bar{K}/K$, so daß jedes Polynom $f(X) \in \bar{K}[X]$ eine Nullstelle in $\bar{K}$ hat.*

Wir nennen $\bar{K}$ einen algebraischen Abschluß *von K.*

Beweis. Führe für jedes irreduzible $f(X) \in K[X]$ eine Variable X_f ein und nenne Θ die Menge dieser Polynome.

Es sei $A = K[X_f]_{f\in\Theta}$ und $\mathfrak{m} = (f(X_f))_{f\in\Theta}$. Dann ist $\mathfrak{m} \neq (1)$. Andernfalls wäre für eine endliche Menge $(X_\alpha) \subseteq (X_f)$

$$1 = \sum a_i(X_\alpha)\, f_i(X_{f_i}) \tag{1.20}$$

in $K[X_\alpha]$. Es sei nun $f_i(\alpha_i) = 0$ mit $\alpha_i \in L'/K$, wobei L'/K der Zerfällungskörper von $(f_i(X))$ ist. Bettet man nun (1.20) in $L'[X_\alpha]$ ein und setzt $X_{f_i} = \alpha_i$, so entsteht der Widerspruch $1 = 0$.

Da $\mathfrak{m} \neq (1)$, gibt es ein maximales Ideal $\mathfrak{n} \supseteq \mathfrak{m}$ und es ist $K_1 = A/\mathfrak{n}$ ein Körper K_1/K.

In K_1 hat jedes irreduzible, also auch jedes, Polynom $f(X) \in K[X]$ wenigstens eine Nullstelle.

Konstruiere nun analog zur Konstruktion von K_1/K auch K_2/K_1 und dann eine unendliche Kette $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$ von Körperweiterungen.

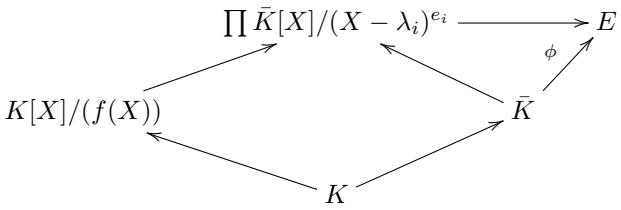
Die Menge $\bar{K} = \bigcup_{i\geqslant 0} K_i$ ist offensichtlich ein Körper mit $K \subseteq \bar{K}$.

Ist irgendein Polynom $f(X) \in \bar{K}[X]$ vorgelegt, so ist dieses schon in einem $K_p[X]$. Also hat es eine Nullstelle in K_p, also auch in $\bar{K}$. Damit hat jedes Polynom in $\bar{K}[X]$ eine Nullstelle in $\bar{K}$ und zerfällt mithin in $\bar{K}[X]$ in Linearfaktoren.

Proposition 1.2.7. *Es sei $\bar{K}/K$ der eben konstruierte algebraische Abschluß von K. Weiter sei E/K ein algebraisch abgeschlossener Körper. Dann gibt es wenigstens eine Körpereinbettung $\phi : \bar{K} \to E$ mit $\phi \in \mathrm{Hom}_K(\bar{K}, E)$.*

Es sei nun K ein Körper und $f(X) \in K[X]$. Weiter sei E/K ein algebraisch abgeschlossener Körper.

Das Polynom $f(X)$ faktorisiere in $\bar{K}[X]$ als $f(X) = \prod_{i=1}^{r}(X-\lambda_i)^{e_i}$. Es ist dann $K[X]/(f(X)) \otimes_K \bar{K} = \prod \bar{K}[X]/(X-\lambda_i)^{e_i}$ und man hat das Diagramm



(1.21)

Aus ihm liest man ab

$$\mathrm{Hom}_K(\prod \bar{K}[X]/(X-\lambda_i)^{e_i}, E) = \\ = \mathrm{Hom}_K(K[X]/(f(X)), E) \times \mathrm{Hom}_K(\bar{K}, E) \tag{1.22}$$

Wählt man ein $\phi \in \mathrm{Hom}_K(\bar{K}, E)$ fest, so ergibt sich eine $1-1$–Beziehung:

$$\begin{aligned}\mathrm{Hom}_K(K[X]/(f(X)),E) \quad &\leftrightarrow \\ \mathrm{Hom}_\phi(\prod \bar{K}[X]/(X-\lambda_i)^{e_i},E) \quad &\leftrightarrow \quad \{\lambda_1^\phi,\ldots,\lambda_r^\phi\} \end{aligned} \tag{1.23}$$

Man erkennt daraus, daß unabhängig von ϕ und E immer

$$\#\,\mathrm{Hom}_K(K[X]/(f(X)),E) = r \tag{1.24}$$

ist.

1.2.5 Separabilität

Definition 1.2.7. *Ein irreduzibles Polynom $f(X) \in K[X]$ heißt* separabel, *falls*

a) Das Ideal $(f(X), f'(X)) = K[X]$ ist.
b) $f(X)$ über $\bar{K}[X]$ keine mehrfachen Nullstellen hat, also in lauter verschiedene Linearfaktoren zerfällt.

ist.

Definition 1.2.8. *Es sei L/K eine Körpererweiterung, $\alpha \in L$ und $f(X) = f_\alpha(x) \in K[X]$ sein Minimalpolynom.*
Dann heißt α separabel über K, *falls $f(X)$ separabel über K ist.*

Lemma 1.2.1. *Es sei K ein Körper und $f(X) \in K[X]$ ein irreduzibles Polynom. Dann gibt es zwei Möglichkeiten:*

1. $\mathrm{char}\, K = 0$ *und $f(X)$ ist separabel.*
2. $\mathrm{char}\, K = p$ *und $f(X) = g(X^{p^m})$ mit $g(X) \in K[X]$ separabel.*

Im zweiten Fall ist $f(X)$ genau dann separabel, falls $m = 0$ ist.

Proposition 1.2.8. *Es sei L/K mit $[L:K] = n$ eine endliche algebraische Körperweiterung. Weiter sei $\phi : K \to E$ eine Einbettung in einen algebraisch abgeschlossenen Körper.*
Dann ist $n_s = \#\,\mathrm{Hom}_\phi(L,E)$ unabhängig von E und es gilt $n_s \mid n$. Die Größe $n_s = [L:K]_s$ heißt Separabilitätsgrad von L über K.

Lemma 1.2.2. *Es seien die Bezeichnungen wie in voriger Proposition und $L = K(\alpha)$. Dann gilt wie in der Proposition $n_s | n$ mit $\mathrm{Hom}_\phi(K(\alpha),E) = n_s$ und mit $n = [K(\alpha):K]$.*

Lemma 1.2.3. *Es sei $M/L/K$ ein Turm aus endlichen algebraischen Körpererweiterungen. Dann gibt es eine Abbildung*

$$\phi \in \mathrm{Hom}_K(L,E) \mapsto (\mathrm{Hom}_\phi(M,E) \mapsto \mathrm{Hom}_K(M,E)) \tag{1.25}$$

Umgekehrt entsteht ein Isomorphismus von Mengen

$$\phi \in \mathrm{Hom}_K(M,E) \mapsto (\psi = \phi|_L \in \mathrm{Hom}_K(L,E), \chi \in \mathrm{Hom}_\psi(M,E)) \tag{1.26}$$

Daraus folgt

Proposition 1.2.9. *Es sei $M/L/K$ eine Folge von Körpererweiterungen mit $[M : L] = m$ und $[L : K] = n$.*

Dann ist

$$[M : L]_s \, [L : K]_s = [M : K]_s \tag{1.27}$$

Der Separabilitätsgrad ist also multiplikativ in einem Erweiterungsturm.

Definition 1.2.9. *Es sei L/K eine Körperweiterung. Dann heißt L* separabel über K*, falls äquivalent*

a) Alle $\alpha \in L$ separabel über K sind.
b) $[K(\alpha) : K]_s = [K(\alpha) : K]$ für alle $\alpha \in L$ ist.
c) $[L' : K]_s = [L' : K]$ für alle endlichen Erweiterungen L'/K mit $L' \subseteq L$ ist.

Lemma 1.2.4. *Es sei $K(\alpha)/K$ eine separable Körpererweiterung und M/K eine beliebige Körpererweiterung. Dann ist auch $M(\alpha)/M$ eine separable Körpererweiterung.*

Beweis. Es sei $f(X) \in K[X]$ das Minimalpolynom von α. Dann ist das Minimalpolynom $g(X) \in M[X]$ von α über M ein Teiler von $f(X)$. Da $f(X)$ keine doppelten Nullstellen hat, gilt dies auch für $g(X)$ und $M(\alpha)$ ist separabel über M.

Lemma 1.2.5. *Es sei L/K eine Körpererweiterung und $\alpha, \beta \in L$, separabel, algebraisch über K. Dann ist auch $K(\alpha, \beta)/K$ separabel.*

Beweis. Es ist $K(\alpha, \beta)/K(\alpha)/K$ ein Turm von separablen Körpererweiterungen.

Proposition 1.2.10. *Die Klasse der separablen, algebraischen Körpererweiterungen L/K ist eine ausgezeichnete Klasse.*

Beweis. Die Eigenschaften $\mathcal{P}_1$ und $\mathcal{P}_2$ folgen aus Proposition 1.2.9. Es sei nun L/K eine separable, algebraische Erweiterung und M/K eine beliebige Körpererweiterung. $LM = \bigcup_{\alpha \in L} M(\alpha)$ also auch separabel über M.

Proposition 1.2.11. *Es sei L/K eine endliche, separable Körpererweiterung. Dann existiert stets ein $\alpha \in L$ mit $K(\alpha) = L$.*

Proposition 1.2.12. *Es sei F/K eine endliche separable Körpererweiterung und E/K eine beliebige Körpererweiterung. Weiter sei $F = K(\alpha)$ mit irreduziblem Polynom $f \in K[X]$ und $f(\alpha) = 0$.*

In $E[X]$ gilt dann $f(X) = g_1(X) \cdot \cdots \cdot g_r(X)$ mit irreduziblen Polynomen $g_i(X) \in E[X]$. Es sei $L_j = E[X]/(g_j(X)) = E(\alpha_j)$. Dann existiert ein Isomorphismus (von E- oder K-Algebren):

$$F \otimes_K E = L_1 \oplus \cdots \oplus L_r \tag{1.28}$$

und man hat kanonische Injektionen $E \to L_j$ und $F \to L_j$, wobei letztere durch $\alpha \mapsto \alpha_j$ gegeben ist.

Beweis. Da wegen Separabilität von F das Polynom $f(X)$ keine mehrfachen Nullstellen hat, ist die allgemeine Form der Zerlegung $f(X) = g_1(X) \cdot \cdots \cdot g_r(X)$ ohne doppelte irreduzible Faktoren klar.

Nun ist $F \otimes_K E = K[X]/(f(X)) \otimes_K E = E[X]/(f(X))$. Damit folgt die obige Gleichung (1.28) nach dem chinesischen Restsatz.

Die Injektionen $E \to E[X]/(g_j(X))$ sind selbstverständlich. Man betrachte nun die exakte Sequenz $0 \to I \to K[X] \to E[X]/(g_j(X)) \to 0$. Da $E[X]/(g_j(X))$ ein Körper, also Integritätsring ist, muß I ein Primideal sein. Das Ideal I enthält auf jeden Fall $f(X)$, ein Primelement von $K[X]$, und ist offensichtlich nicht gleich $K[X]$. Also ist $I = (f(X))$ und man hat die Injektion $F = K[X]/(f(X)) \to E[X]/(g_j(X)) = L_j$.

Proposition 1.2.13. *Es sei die Situation der vorigen Proposition für F/K, E/K und den Isomorphismus*

$$F \otimes_K E = L_1 \oplus \cdots \oplus L_r$$

sowie den Abbildungen $u_j : F \to L_j$ mit $u_j(\alpha) = \alpha_j$ gegeben.

Es sei nun $\beta \in F$ ein beliebiges Element und $u_j(\beta) = \beta_j$. Weiter sei $f(X) \in K[X]$ das charakteristische Polynom von β für die Erweiterung F/K. Für ein β_j sei $g_j(X) \in E[X]$ das charakteristische Polynom von β_j für L_j/E.

Dann ist $f(X) = g_1(X) \cdot \cdots \cdot g_r(X)$.

Beweis. Es sei $\omega_1, \ldots, \omega_n$ eine K–Basis von F und es sei $\beta \cdot \omega_i = \sum_j a_i^j \omega_j$. Dann ist $f(X) = \det((X\delta_i^j - a_i^j))$ das charakteristische Polynom des E–linearen Operators $z \mapsto \beta\, z$ auf dem n–dimensionalen E–Vektorraum $F \otimes_E K$.

Dieser E–Vektorraum ist gleich $L_1 \oplus \cdots \oplus L_r$ auf der rechten Seite von (1.28). Wählt man eine E–Basis η_{ij} mit $(\eta_{ij})_j$ einer E–Basis von L_i, so ist $\beta\, \eta_{ij} = \beta_i \eta_{ij} = \sum_k a_{ij}^k \eta_{ik}$. Es ist dann $g_i(X) = \det((X\delta_j^k - a_{ij}^k))$ das charakteristische Polynom von β_i in L_i/E. In der Basis (η_{ij}) zerfällt die Matrixdarstellung des Operators $z \mapsto \beta z$ also in die direkte Summe von Matrizen (a_{ij}^k) und damit ist das charakteristische Polynom, auf diese Weise berechnet, gleich $g_1(X) \cdot \cdots \cdot g_r(X)$. Also, im Vergleich mit der linken Seite, $f(X) = g_1(X) \cdot \cdots \cdot g_r(X)$.

Es folgt also auch

Korollar 1.2.1. *Für F/K und E/K wie oben mit $F \otimes_K E = L_1 \oplus \cdots \oplus L_r$ und $\beta \in F$ gilt sowie $u_j : F \to L_j$ und $u_j(\beta) = \beta_j$*

$$\mathrm{Norm}_{F|K}(\beta) = \prod_j \mathrm{Norm}_{L_j|E}(\beta_j) \tag{1.29}$$

$$\mathrm{Tr}_{F|K}(\beta) = \sum_j \mathrm{Tr}_{L_j|E}(\beta_j) \tag{1.30}$$

Ist F/K endlich und separabel, mit Einbettungen $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$ so gilt

Proposition 1.2.14. *Für F/K separabel und $\alpha \in F$ ist:*

$$\mathrm{Norm}_{L|K}(\alpha) = \prod_i \sigma_i(\alpha) \tag{1.31}$$

$$\mathrm{Tr}_{L|K}(\alpha) = \sum_i \sigma_i(\alpha) \tag{1.32}$$

Beweis. Man betrachte die Zerlegung $F \otimes_K \bar{K} = \bar{K} \oplus \cdots \oplus \bar{K}$. mit n Summanden rechts.

1.2.6 Normale Erweiterungen

Definition 1.2.10. *Es sei L/K eine algebraische Körpererweiterung und $L \subseteq \bar{K}$ fest eingebettet. Dann ist äquivalent:*

a) Für jede Einbettung $\sigma : L \to \bar{K}$ über K ist $\sigma(L) \subseteq L$.
b) Für jedes $\alpha \in L$ mit Minimalpolynom $f(X) \in K[X]$ zerfällt $f(X)$ in $L[X]$ in Linearfaktoren.
c) Jedes irreduzible Polynom $f(X) \in K[X]$ mit einer Nullstelle $\alpha \in L$ zerfällt in $L[X]$ in Linearfaktoren.

Erfüllt L/K diese Bedingungen, so heißt die Erweiterung normal.

Proposition 1.2.15. *Es gilt:*

1. *Es seien M/L und L/K normale Körpererweiterungen. Dann ist auch M/K normal.*
2. *Es sei $M/L/K$ ein Turm von algebraischen Körpererweiterungen und M/K normal. Dann ist auch M/L normal.*
3. *Es sei L/K eine normale, algebraische Körperweiterung und M/K eine beliebige Körpererweiterung. Dann ist auch LM/M eine normale Körpererweiterung.*

Anmerkung 1.2.3. Die normalen Körpererweiterungen sind *keine* ausgezeichnete Klasse. Insbesondere ist für $M/L/K$ mit M/K normal die Erweiterung L/K offensichtlich nicht notwendig normal.

1.2.7 Duale Basen

Es sei L/K eine endliche separable Körpererweiterung und $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$ die verschiedenen Einbettungen. Wir können nach obigem annehmen, daß $L = K(\alpha)$ mit einem $\alpha \in L$ dessen Minimalpolynom $f(X) \in K[X]$ sei.

Definieren wir $\langle \alpha, \beta \rangle = \mathrm{Tr}_{L|K}(\alpha\,\beta)$ für $\alpha, \beta \in L$, so haben wir eine K–Bilinearform $\langle , \rangle : L \to K$ definiert.

Proposition 1.2.16. *Die Bilinearform $\langle , \rangle$ von oben ist nicht ausgeartet*

Beweis. Für eine K–Basis $\omega^1, \dots, \omega^n$ von L können wir ausrechnen:

$$(\mathrm{Tr}_{L|K}(\omega^i\,\omega^j)) = (\sigma_k\omega^i)_{ik}\cdot(\sigma_k\omega^j)_{kj} \tag{1.33}$$

Da aus $\sigma_p(\sum a_q\omega^q) = 0$ für $a_q \in K$ immer $a_q = 0$ für alle q folgt, ist $\det(\sigma_p\omega^q)_{pq} \neq 0$ und damit auch $\det(\mathrm{Tr}_{L|K}(\omega^i\,\omega^j))_{ij} = \det(\sigma_p\omega^q)^2_{pq} \neq 0$.

Es gibt deshalb zu jeder K–Basis $\omega^1, \dots, \omega^n$ von L eine *duale Basis* $\omega^{1*}, \dots, \omega^{n*} \in L$ mit $\langle\omega^i, \omega^{j*}\rangle = \delta_{ij}$.

Wie sieht nun die duale Basis von $1, \alpha, \dots, \alpha^{n-1}$ aus?

Proposition 1.2.17. *Mit den obigen Bezeichnungen sei*

$$\frac{f(X)}{X-\alpha} = \beta_0 + \beta_1\,X + \cdots + \beta_{n-1}\,X^{n-1} \tag{1.34}$$

Dann ist

$$\mathrm{Tr}_{L|K}\left(\alpha^i\,\frac{\beta_j}{f'(\alpha)}\right) = \delta_{ij} \tag{1.35}$$

Beweis. Man betrachte das folgende Polynom aus $k(X)(z)$:

$$g(z) = \frac{f(X)}{X-z}\,\frac{z^i}{f(z)} \tag{1.36}$$

Seine möglichen Pole in der Variablen z liegen an den Stellen X und $a_1, \dots, a_n \in k$, wobei wir $f(X) = (X-a_1)\cdot\dots\cdot(X-a_n)$ setzen. Wir rechnen aus

$$\begin{aligned} g(z) &= \frac{f(X)}{X-a_p+a_p-z}\,\frac{(z-a_p+a_p)^i}{\prod_j(z-a_p+a_p-a_j)} = \\ &= \frac{f(X)}{(X-a_p)\left(1+\frac{a_p-z}{X-a_p}\right)}\,\frac{a_p^i+(z-a_p)h(z-a_p)}{(z-a_p)\prod_{j\neq p}(a_p-a_j)\prod_{j\neq p}\left(\frac{z-a_p}{a_p-a_j}+1\right)} \end{aligned} \tag{1.37}$$

Damit ist also

$$\mathrm{res}_{z=a_p}\,g(z)\,dz = \frac{f(X)}{X-a_p}\,\frac{a_p^i}{f'(a_p)} \tag{1.38}$$

Für $z = X$ formen wir um

$$g(z) = -\frac{f(X)}{z-X}\,\frac{(z-X+X)^i}{f(z-X+X)} = -\frac{f(X)}{z-X}\,\frac{X^i+(z-X)\,h(z-X)}{f(X)\left(1+\frac{(z-X)q(z-X)}{f(X)}\right)} \tag{1.39}$$

und lesen unmittelbar

$$\mathrm{res}_{z=X}\,g(z)\,dz = -X^i \tag{1.40}$$

ab. Mit der Transformation $w = 1/z$ ist

$$g(1/w)d(\frac{1}{w}) = -\frac{1}{w^2}\,\frac{f(X)}{X-\frac{1}{w}}\,\frac{(1/w)^i}{f(1/w)}dw = \frac{f(X)}{w\,X-1}\,\frac{w^{n-1-i}}{w^n\,f(1/w)}dw \tag{1.41}$$

Da $w^n\,f(1/w) = 1 + c_1\,w + \cdots + c_nw^n$ ist $g(1/w)\,dw$ bei $w = 0$ holomorph, also $\mathrm{res}_{z=\infty}\,g(z)\,dz = 0$.

Aus $\mathrm{res}_{z=X}\,g(z)\,dz + \sum_p \mathrm{res}_{z=a_p}\,g(z)\,dz = 0$ folgt also

$$X^i = \sum_{p=1}^{n}\frac{f(X)}{X-a_p}\,\frac{a_p^i}{f'(a_p)} = \mathrm{Tr}_{L|K}\left(\frac{f(X)}{(X-\alpha)\,f'(\alpha)}\alpha^i\right) \tag{1.42}$$

Damit ist die $\langle\alpha^i, \beta_j\rangle = \delta_{ij}$ nachgewiesen.

1.3 Transzendente Körpererweiterungen

Im folgenden spezialisieren wir den Begriff der Ringerweiterung auf den Fall, daß die beteiligten Ringe Körper sind.

Definition 1.3.1. *Es sei K/k eine Ringerweiterung und K, k zwei Körper. Dann heißt k* Unterkörper *und K* Oberkörper *der Erweiterung und die Erweiterung selbst eine* Körpererweiterung.

Ist K ganz über k, so heißt K algebraisch *über k.*

Der im folgenden eingeführte Begriff der algebraischen Unabhängigkeit ist in manchen seiner Eigenschaft analog zum Begriff der linearen Unabhängigkeit von Elementen eines Vektorraums.

Definition 1.3.2. *Es sei K/k eine Körpererweiterung und $(b_i)_i$ eine Familie von Elementen von K. Dann heißen die $(b_i)_i$* algebraisch unabhängig *über k, wenn für alle $\psi(b_{i_1}, \ldots, b_{i_s}) = 0$ mit $\psi \in k[T_1, \ldots, T_s]$ gilt, daß $\psi = 0$.*

Die folgenden Lemmata sind Analoga zum *Basisaustauschsatz* der linearen Algebra:

Lemma 1.3.1. *Es sei K/k eine Körpererweiterung und $b_1, \ldots, b_n \in K$ algebraisch unabhängig über k. Weiter erfülle $y \in K$ eine Polynomgleichung $f(y, b_1, \ldots, b_n) = 0$ mit $f \in k[S, T_1, \ldots, T_n]$ in der b_1 wirklich vorkommt.*

Dann ist b_1 algebraisch über $k(y, b_2, \ldots, b_n)$ und $y, b_2, \ldots, b_n$ sind algebraisch unabhängig über k. Es ist sogar

$$k(b_1, \ldots, b_n)^- = k(y, b_2, \ldots, b_n)^-$$

Lemma 1.3.2. *Es sei K/k eine Köpererweiterung, $b_1, \ldots, b_n \in K$ algebraisch unabhängig über k. Weiter seien $y_1, \ldots, y_m \in K$ algebraisch unabhängig über k und algebraisch über $k((b_i)_i)$ und es sei $m \leqslant n$. Dann lassen sich die b_i so numerieren, daß*

$$y_1, \ldots, y_m, b_{m+1}, \ldots, b_n$$

über k algebraisch unabhängig ist und

$$k(b_1, \ldots, b_n)^- = k(y_1, \ldots, y_m, b_{m+1}, \ldots, b_n)^-$$

gilt.

Eine Transzendenzbasis ist in diesem Sinne eine Analogie zur Basis eines Vektorraums.

Definition 1.3.3. *Es sei K/k eine Körpererweiterung und $(b_i)_i$ eine Familie von Elementen aus K, algebraisch unabhängig über k, für die K algebraisch über $k((b_i))$ ist.*

Dann heißt $(b_i)_i$ Transzendenzbasis *von K über k.*

Proposition 1.3.1. *Es sei K/k eine Körpererweiterung und $K/k((b_i)_i)$ algebraisch für eine endliche Transzendenzbasis $(b_i)_i$ mit n Elementen.*

Dann hat jede Transzendenzbasis $(a_j)_j$ mit $K/k((a_j)_j)$ algebraisch auch genau n Elemente.

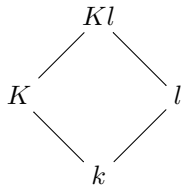
Man sagt $\mathrm{tr.deg}_k K = n$, *der* Transzendenzgrad *von K über k ist n.*

Eine separierende Transzendenzbasis erlaubt eine Darstellung einer Körpererweiterung ohne Inkaufnahme eines inseparablen algebraischen Anteils:

Definition 1.3.4. *Es sei K/k eine Körpererweiterung. Weiter existiere eine Transzendenzbasis $B = (b_i)_i$ mit $b_i \in K$ über k.*

Ist dann $K/k((b_i)))$ eine separable und algebraische *Körpererweiterung, so heißt B eine* separierende Transzendenzbasis *für K über k. Der Körper K heißt dann* separabel erzeugt *über k.*

Vor dem Beweis der beiden folgenden Theoreme brauchen wir einige Hilfsbegriffe. Wir betrachten das Diagramm



(1.43)

von Körpererweiterungen. In diesem soll l/k algebraisch sein und deshalb Kl wohldefiniert als Teil von K^-, dem algebraischen Abschluß von K.

Definition 1.3.5. *In der Situation des vorigen Diagramms heißen K und l* linear disjunkt, *wenn $K \cap l = k$ und die kanonische Abbildung*

$$K \otimes_k l \to Kl \tag{1.44}$$

ein Isomorphismus ist.

Anmerkung 1.3.1. Ist $[l : k] = n < \infty$, so sind K und l genau dann linear disjunkt, wenn $[Kl : K] = n$ ist.

Definition 1.3.6. *Für einen Körper k mit* $\mathrm{char}\, k = p$ *bezeichnen wir mit $k^{1/p^\infty} \subseteq \bar{k}$ den von den Lösungen aller Gleichungen $X^{p^r} - z = 0$ mit $r > 0$, ganz, und $z \in k$ erzeugten Unterkörper von $\bar{k}$*

Lemma 1.3.3. *In den Bezeichnungen der Definition ist l/k rein inseparabel algebraisch für alle $l \subseteq k^{1/p^\infty}$.*

Lemma 1.3.4. *Es sei $K = k((a_i))/k$ mit einer Transzendenzbasis (a_i) von K über k. Weiter sei $k \subseteq l \subseteq k^{1/p^\infty}$.*

Dann sind K und l linear disjunkt über k.

Der Beweis ist eine einfache algebraische Überlegung, die nachweist, daß für

$$\sum g_\alpha((a_i))w_\alpha = 0$$

in $k((a_i))l$ mit $g_\alpha \in k((a_i))$ und $w_\alpha \in l$ auch schon

$$\sum g_\alpha \otimes_k w_\alpha = 0$$

in $k((a_i)) \otimes_k l$ ist.

Definition *Es sei K/k eine endlich erzeugte Körpererweiterung. Enthält jedes Erzeugendensystem (b_i) mit $k((b_i)) = K$ eine separierende Transzendenzbasis, so sagen wir, K/k hat* die Eigenschaft G.

Anmerkung 1.3.2. Ist für K/k die Charakteristik $\operatorname{char} k = p$, so kann das folgende Theorem auf die Erweiterung $Kk^{1/p^\infty}/k^{1/p^\infty}$ des perfekten Körpers k^{1/p^∞} angewandt werden:

Theorem 1.3.1. *Es sei K/k eine endlich erzeugte Körpererweiterung und k ein perfekter Körper. Dann enthält jedes Erzeugendensystem $B = (b_i)_i$ eine separierende Transzendenzbasis für K/k.*

Die Erweiterung K/k hat also die Eigenschaft G.

Beweis. Es sei $B = (b_i)$ ein endliches Erzeugendensystem von K/k. Dann ist $K/k(B')$ endlich algebraisch für jede aus B ausgewählte Transzendenzbasis $B' \subseteq B$.

Wähle B' so, daß $k(B')^{\text{sep}}$ maximal unter den möglichen B' wird. Dann ist K separabel algebraisch über $k(B')$. Sei nämlich ein $z = b_i \in B \setminus B'$ nicht separabel über $k(B')$ und $\phi(z, b_{i_1}, \ldots, b_{i_s}) = 0$ das irreduzible Minimalpolynom von z über $k(B')$.

Alle Potenzen von z in ϕ sind Potenzen von z^p. Würde dies auch für alle b_{i_ν} gelten, so wäre $\phi = \psi^p$, weil k perfekt, und damit ϕ nicht mehr irreduzibel.

Sei also b_{i_1} nicht nur als Potenz von $b_{i_1}^p$ in ϕ enthalten. Es ist dann notwendigerweise:

$$\frac{\partial \phi}{\partial b_{i_1}} = \psi(z, b_{i_1}, \ldots, b_{i_s}) \neq 0 \tag{1.45}$$

Dies gilt aufgrund der folgenden Überlegung: Ist

$$p_0(b_{i_\nu})z^m + p_1(b_{i_\nu})z^{m-1} + \cdots + p_m(b_{i_\nu}) = 0$$

das irreduzible Minimalpolynom von z über $k(b_{i_\nu})$ und außerdem

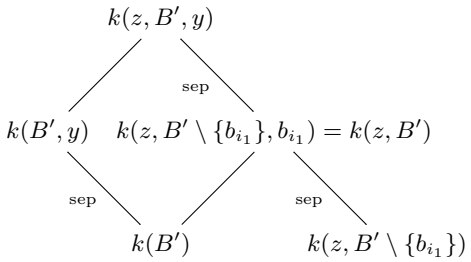
$$q_0(b_{i_\nu})z^{m'} + q_1(b_{i_\nu})z^{m'-1} + \cdots + q_{m'}(b_{i_\nu}) = 0$$

ein weiteres Polynom, das auf z, b_{i_ν} verschwindet mit $m' \leqslant m$, so muß $m = m'$ und $q_i = p_i g$, mit einem Quotient von Polynomen $g(b_{i_\nu}) = R/S$, sein. Da R,S teilerfremd sind, teilt S jedes p_i, ist also gleich 1. Damit kann $g(b_{i_\nu})$ immer als Polynom gewählt werden. Insbesondere kann der Grad in b_{i_1} in den q_i nicht abnehmen.

Schreibt man $\phi(T; z, b_{i_2}, \ldots, b_{i_s}) = f(T) \in k(z, b_{i_2}, \ldots, b_{i_s})[T]$, so ist also $f(b_{i_1}) = 0$ und $\partial f/\partial T(b_{i_1}) \neq 0$.

Also ist b_{i_1} keine mehrfache Nullstelle von $f(T)$ und umsomehr keine mehrfache Nullstelle seines Minimalpolynoms $g_{b_{i_1}}(T)$ über $k(z, b_{i_2}, \ldots, b_{i_s})$.

Mit anderen Worten: b_{i_1} ist separabel algebraisch über der Transzendenzbasis $z, B' \setminus \{b_{i_1}\}$. Damit ist ein Element $y \in K$ das separabel über $k(B')$ ist, auch separabel über $k(z, B' \setminus \{b_{i_1}\})$. Betrachte dazu die Kette von Körpererweiterungen:



Jeder einzelne markierte Erweiterungsschritt ist rein separabel algebraisch, also auch die ganze Erweiterung.

Damit ist $B'' = z, B' \setminus \{b_{i_1}\}$ aber eine Transzendenzbasis deren separabler Abschluß echt größer als der von B' ist, da er zusätzlich z enthält. Also ist schon $k(B')^{\text{sep}} = K$.

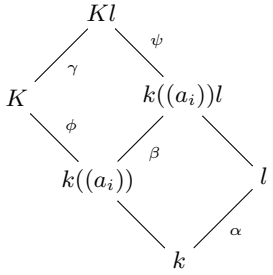
Proposition 1.3.2. *Es sei K/k eine über k endlich erzeugte Körpererweiterung.*

Dann ist äquivalent:

a) Es gibt eine separierende Transzendenzbasis (a_i) für K über k.
b) Für jede endliche Erweiterung l/k mit $l \subseteq k^{1/p^\infty}$ sind die Körper K und l linear disjunkt über k.

Beweis. Es sei (a_i) die separierende Transzendenzbasis: Man betrachte das untenstehende Diagramm. Es ist $[l : k] = [l : k]_i = d$ und $[k((a_i))l : k((a_i))] = [k((a_i))l : k((a_i))]_i = d$ wegen vorigem Lemma.

Da $[K : k((a_i))]_i = 1$ sowie $[Kl : k((a_i))l]_i = 1$ und wegen der Multiplikativität des Inseparabilitätsgrads in Erweiterungstürmen folgt, daß $[Kl : K] = [Kl : K]_i = d$ und mithin nach obiger Bemerkung K und l linear disjunkt sind.



(1.46)

Die umgekehrte Implikation wird mit dem Beweis der nachfolgenden Proposition mitbewiesen.

Proposition 1.3.3. *Es sei K/k eine endlich erzeugte und separabel erzeugte Körpererweiterung. Dann enthält jedes Erzeugendensystem (b_i) mit $K = k((b_i))$ eine separierende Transzendenzbasis für K/k.*

Beweis. Über dem Grundkörper k^{1/p^∞} der alle p^r–ten Wurzeln aus k enthält, lässt sich nach dem vorangehenden Theorem eine Auswahl $B \subseteq (b_i)$ finden, die für Kk^{1/p^∞} eine separierende Transzendenzbasis über k^{1/p^∞} darstellt:

$$\begin{array}{ccc} Kk^{1/p^\infty} & & \\ & \searrow^{\beta} & \\ & k(B)k^{1/p^\infty} & \\ & & \searrow^{\alpha} \\ & & k^{1/p^\infty} \end{array} \tag{1.47}$$

Die Körpererweiterung β ist separabel, so daß jedes b_i separabel über $k(B)k^{1/p^\infty}$ ist. Da in den Abhängigkeitsgleichungen der b_i nur endlich viele Koeffizienten aus k^{1/p^∞} auftauchen, kann man eine Untererweiterung $k \subseteq l \subseteq k^{1/p^\infty}$ mit $[l : k] < \infty$ finden, in der alle diese Koeffizienten vorkommen.

Die b_i sind dann also separabel über $k(B)l$ und es ist $Kl = k((b_i))l$ separabel über $k(B)l$ für diesen über k endlichen Körper l.

$$\begin{array}{ccccc} & & Kl & & \\ & \swarrow^{\gamma} & & \searrow^{\psi} & \\ K & & & & k(B)l \\ & \searrow_{\phi} & & \swarrow_{\beta} & \\ & & k(B) & & \\ & & & \searrow & \\ & & & & l \\ & & & \swarrow & \\ & & k & & \end{array} \tag{1.48}$$

Hier ist die Erweiterung α rein inseparabel vom endlichen Grad d. Ebenso ist γ rein inseparabel vom Grad d nach voriger Proposition. Die Erweiterung ψ ist rein separabel, die Erweiterung β rein inseparabel vom Grad $\leqslant d$. Also ist ϕ rein separabel vom selben Separabilitätsgrad wie ψ.

1.4 Gebrochene Ideale

Es sei A ein Integritätsring, $K = Q(A)$ sein Quotientenkörper. Wir wollen im folgenden A–Untermodule $I \subseteq K$ betrachten. Es seien zwei solche $I, J \subseteq K$ gegegeben.

Dann sind auch $I \cap J$ sowie

$$I + J = \{x + y \mid x \in I, y \in J\} \tag{1.49}$$

$$I\,J = \{\sum a_i\, x_i\, y_i \mid a_i \in A, x_i \in I, y_i \in J\} \tag{1.50}$$

$$(I : J) = \{x \in K \mid x\,J \subseteq I\} \tag{1.51}$$

wohldefinierte A–Untermoduln von K. Für diese gilt neben $I+J = J+I$ und $IJ = JI$ auch

$$I\,(J_1 + J_2) = I\,J_1 + I\,J_2 \tag{1.52}$$

Außerdem besteht Verträglichkeit mit der Lokalisierung:

Proposition 1.4.1. *Es sei A, I, J wie oben und $S \subseteq A$ eine multiplikativ abgeschlossene Teilmenge von A. Dann ist:*

$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J \tag{1.53}$$
$$S^{-1}(I + J) = S^{-1}I + S^{-1}J \tag{1.54}$$
$$S^{-1}(I\,J) = (S^{-1}I)\,(S^{-1}J) \tag{1.55}$$
$$S^{-1}(I : J) \subseteq (S^{-1}I : S^{-1}J) \tag{1.56}$$

Die untenstehende Inklusion ist eine Gleichheit, falls J endlich erzeugter A–Modul ist.

Insbesondere ist

$$(I + J)_{\mathfrak{p}} = I_{\mathfrak{p}} + J_{\mathfrak{p}}, \qquad (I\,J)_{\mathfrak{p}} = I_{\mathfrak{p}}\,J_{\mathfrak{p}}, \qquad (I : J)_{\mathfrak{p}} \subseteq (I_{\mathfrak{p}} : J_{\mathfrak{p}}) \tag{1.57}$$

Als Spezialisierung der oben allgemein eingeführten A–Untermoduln von K definieren wir:

Definition 1.4.1. *Ein A-Modul $I \subseteq K$ heißt* gebrochenes Ideal*, wenn ein $x \in K$ existiert, so daß $x\,I \subseteq A$ gilt.*

Offensichtlich kann man $x \in A$ annehmen. Es gilt dann

Proposition 1.4.2. *Es seien I und J gebrochene Ideale. Dann sind auch*

$$I \cap J, \qquad I + J, \qquad I\,J, \qquad (I : J) \tag{1.58}$$

selbst wieder gebrochene Ideale. Insbesondere ist $(A : I)$ ein gebrochenes Ideal.

Noch spezieller sind die sogenannten *invertierbaren Ideale*:

Definition 1.4.2. *Es sei für einen A–Untermodul I die Beziehung*

$$(A : I)\,I = A$$

erfüllt. Dann heißt I invertierbares Ideal

Offensichtlich sind invertierbare Ideale auch gebrochene Ideale.

Proposition 1.4.3. *Es sei A nothersch. Dann ist für einen A–Untermodul I von K äquivalent:*

a) der Untermodul I ist endlich erzeugt.
b) der Untermodul I ist ein gebrochenes Ideal.

Proposition 1.4.4. *Es sei A ein noetherscher Integritätsring und I ein A–Untermodul von K. Dann ist äquivalent:*

a) I ist ein invertierbares Ideal.
b) I ist ein lokal freier, also projektiver A–Modul vom Rang 1.

Beweis. Es sei I ein invertierbares Ideal. Aufgrund der Lokalisierbarkeit kann man A als lokalen Ring mit $k = A/\mathfrak{m}_A$ annehmen. Es besteht dann eine Surjektion

$$(A : I) \otimes_A I \to A \to 0$$

Tensorieren mit $k \otimes_k k = k$ liefert

$$((A : I) \otimes_A k) \otimes_k (k \otimes_A I) \to k \to 0$$

und damit einen Isomorphismus $I \otimes_A k = k$. Aus diesem entspringt eine Surjektion $A \to I \to 0$, die wegen $I \subseteq K$ und A integer eine Bijektion ist.

1.5 Bewertungsringe

1.5.1 Bewertungen und Normen

Definition 1.5.1. *Es sei K ein Körper. Eine Abbildung $|\cdot|\colon K \to \mathbb{R}_{\geqslant 0}$ mit*

i) Es gibt eine Konstante C mit $|1 + x| \leqslant C$ für alle x aus K mit $|x| \leqslant 1$.
ii) $|x\,y| = |x|\,|y|$ für alle x, y aus K.
iii) $|x| = 0$ genau dann, wenn $x = 0$.

heißt (Absolut–)Bewertung auf K. *Ist $|x| = 1$ für alle $x \neq 0$, so heißt $|\cdot|$ trivial.*

Proposition 1.5.1. *Ist in der Definition von $|\cdot|$ die Konstante C gleich 2, so gilt die* Dreiecksungleichung

$$|x + y| \leqslant |x| + |y| \tag{1.59}$$

für $x, y \in K$.

Ist C gleich 1, so gilt sogar die ultrametrische Ungleichung

$$|x + y| \leqslant \max(|x|, |y|) \tag{1.60}$$

Beweis. Es sei $C = 2$. Dann gelten für $x, y \in K$ die Beziehungen

$$|x + y| \leqslant 2\max(|x|, |y|) \tag{1.61}$$
$$|x + y| \leqslant 2(|x| + |y|) \tag{1.62}$$

Aus der ersten Beziehung leitet man $|n| \leqslant 4n$ für alle $n \in \mathbb{Z}$ ab. Man betrachte dazu für ein $n > 0$ die Summenzerlegung $n = n_1 + n_2$ mit $n_1 = n_2$ oder $n_2 = n_1 + 1$. Dann ist $|n| \leqslant 2\max(|n_1|, |n_2|)$ Dieselbe Zerlegung wende man rekursiv auf n_1 und n_2 an und gelange somit nach maximal $m = \lceil \log(n)/\log(2) \rceil + 1$ Unterteilungen zu

$n_i \leqslant 1$. Die Beziehung für m erkennt man aus der Folge $r_0 = n$ und $r_{i+1} = \frac{1}{2}(r_i + 1)$, wobei $r_i \geqslant n'$ für jeden Teil n' nach der i–ten Unterteilung von n gilt.

Also ist $|n| \leqslant 2^m \leqslant c_1 n$ für ein geeignetes $c_1 < 2^2$, also $|n| < 4n$.

Es ist nun für $N = 2^m$

$$A(x,y,N) = |x+y|^N = |\sum_{i=0}^{N} \binom{N}{i} x^i y^{N-i}| \leqslant 2^m \sum_{i=0}^{N} |\binom{N}{i}||x|^i |y|^{N-i}$$

Die Ungleichung folgt, indem man rekursiv $2^{m-1}, 2^{m-2}, \ldots, 2$–lange Teilsummen mit der Beziehung (1.62) auswertet.

Weiter ist

$$B(x,y,N) = (|x|+|y|)^N = \sum_{i=0}^{N} \binom{N}{i} |x|^i |y|^{N-i}$$

Es ist wegen $|\binom{N}{i}| \leqslant 4\binom{N}{i}$ dann

$$\frac{A(x,y,N)}{B(x,y,N)} \leqslant 2^{m+2}$$

Also folgt durch Anwendung von $z \mapsto z^{1/N}$.

$$\frac{|x+y|}{|x|+|y|} \leqslant 2^{(m+2)/N}$$

Geht m, also $N = 2^m$, gegen unendlich, so folgt

$$\frac{|x+y|}{|x|+|y|} \leqslant 1$$

also die Behauptung.

Definition 1.5.2. *Es sei K ein Körper mit Bewertung $|\cdot|$. Dann heißt $|\cdot|$* nicht–archimedisch *wenn $|x+y| \leqslant \max(|x|,|y|)$ für alle $x, y \in K$ ist.*

Ist diese Bedingung nicht erfüllt, so heißt $|\cdot|$ archimedisch.

Anmerkung 1.5.1. Es sei K ein Körper mit nicht–archimedischer Bewertung $|\cdot|$. Dann ist $R = \{x \mid x \in K,\ |x| \leqslant 1\}$ ein lokaler Integritätsring mit maximalem Ideal $\mathfrak{m} = \{x \mid x \in K,\ |x| < 1\}$.

Proposition 1.5.2. *Es sei K ein Körper mit zwei Bewertungen $|\cdot|_1$ und $|\cdot|_2$. Dann ist äquivalent*

a) Die Bewertungen $|\cdot|_1$ und $|\cdot|_2$ erzeugen dieselbe Topologie auf K.
b) Es gibt ein $\lambda > 0$ mit $|x|_1 = |x|_2^\lambda$ für alle $x \in K$.

Beweis. Es mögen beide Bewertungen dieselbe Topologie erzeugen. Da x^n in beiden Topologien entweder gegen 0 konvergiert oder nicht und wegen $|x|_i^n = |x^n|_i$ ist äquivalent $|x|_1 < 1$ und $|x|_2 < 1$. Also auch $|x|_1 > 1$ und $|x|_2 > 1$ und damit $|x|_1 = 1$ und $|x|_2 = 1$.

Es sei nun für ein a mit $|a| < 1$ ein $\lambda > 0$ mit $|a|_1 = |a|_2^\lambda$ gewählt. Für ein beliebiges $x \in K$ mit $|x|_i < 1$ gibt es dann eine Ungleichung

$$|a|_1^{n+1} < |x^m|_1 \leqslant |a|_1^n$$

Damit gilt auch $|a|_2^{n+1} < |x^m|_2 \leqslant |a|_2^n$, also:

$$|a|_2^{\lambda(n+1)} < |x^m|_2^{\lambda} < |a|_2^{\lambda n}$$

Ganz links und ganz rechts stehen dieselben Ausdrücke, mithin ist

$$|a|_1 = \frac{|a|_1^{n+1}}{|a|_1^n} < \frac{|x^m|_1}{|x^m|_2^{\lambda}} < \frac{|a|_1^n}{|a|_1^{n+1}} = |a|_1^{-1}$$

Es ist also $c < (|x|_1/|x|_2^{\lambda})^m < 1/c$. Wendet man $z \mapsto z^{1/m}$ an und läßt m gegen Unendlich gehen, so folgt $|x|_1 = |x|_2^{\lambda}$.

Wegen $|x^{-1}| = |x|_i^{-1}$ gilt der Beweis dann auch für alle x.

Definition 1.5.3. *Es sei K ein Körper. Dann heißen zwei Bewertungen $|\cdot|_1$ und $|\cdot|_2$, die die Bedingungen der vorigen Proposition erfüllen,* äquivalent.

Korollar 1.5.1. *Jede Bewertung $|\cdot|$ von K ist äquivalent zu einer Bewertung $|\cdot|_1$ für die C gleich 2 in der Definition der Bewertung ist. Also gilt für $|\cdot|_1$ die Dreiecksungleichung.*

Definition 1.5.4. *Eine Klasse äquivalenter Bewertungen auf K heißt auch* Stelle von K. *Die Menge der Stellen von K werde mit Σ_K abgekürzt.*

Der folgende Satz ist von großer Bedeutung

Theorem 1.5.1 (Approximationssatz). *Es sei K ein Körper und $|\cdot|_1, \ldots, |\cdot|_n$ paarweise nichtäquivalente Bewertungen von K. Weiter sei $x_1, \ldots, x_n \in K$ und $\varepsilon > 0$ vorgegeben. Dann gibt es ein $x \in K$ mit*

$$|x - x_i|_j < \varepsilon$$

für alle $j = 1, \ldots, n$.

Beweis. Wir führen eine Induktion über n durch. Der Satz sei für $n-1$ schon bewiesen. Es sei $w \in K$ mit $|w|_1 > 1$ und $|w|_j < 1$ für $j = 2, \ldots, n-1$. Weiter sei $z \in K$ mit $|z|_1 > 1$ und $|z|_n < 1$. Nenne dann $b_{1n} = wz^N$ mit einem sehr großen geeigneten N. Dann ist $|b_{1n}|_1 > 1$ sowie $|b_{1n}|_n < 1$, dies gilt für jedes $N > N_0$. Weiterhin ist für $j = 2, \ldots, n-1$ immer entweder $|b_{1n}|_j < 1$ oder $|b_{1n}|_j > 1$. Für $|z|_j > 1$ werde N so groß gewählt, daß $|wz^N|_j > 1$ ist, für $|z|_j < 1$ ist umsomehr $|wz^N|_j < 1$ und für $|z|_j = 1$ ist $|wz^N|_j = |w|_j < 1$. Nenne nun $c_{1n} = b_{1n}^M/(1 + b_{1n}^M)$. Dann ist $|c_{1n} - 1|_1 < \delta$ und $|c_{1n}|_n < \delta$ und $|c_{1n} - \gamma_j|_j < \delta$ mit γ_j entweder gleich 1 oder gleich 0 für $j = 2, \ldots, n-1$. Dabei werde $\delta > 0$ vorgegeben und $M \gg 0$ passend gewählt. Definiere nun analog zu c_{1n} beliebige c_{ij}, die bei $|\cdot|_i$ nahe bei 1 und bei $|\cdot|_j$ nahe bei Null sind und bei $|\cdot|_k$, mit $k \neq i, j$, entweder nahe bei 0 oder nahe bei 1 sind.

Nenne dann $z_i = \prod_{l \neq i} c_{il}$. Dann ist $x = \sum_i x_i z_i$ die gesuchte Approximation.

Für die Bewertungen auf $\mathbb{Q}$ gilt folgender Satz

Proposition 1.5.3. *Es sei $|\cdot|$ eine nichttriviale Bewertung auf $\mathbb{Q}$. Dann ist $|\cdot|$ äquivalent zu*

i) dem gewöhnlichen Betrag $|\cdot|$ auf $\mathbb{Q}$, oder zu
ii) der p–adischen Bewertung $|\cdot|_p$, definiert durch $|p^n\, r/s|_p = 1/p^n$ für p prim und r, s aus $\mathbb{Z}$ teilerfremd untereinander und teilerfremd zu p.

Beweis. Es gebe zunächst ein kleinstes $p \in \mathbb{Z}$ mit $|p| = \alpha < 1$. Dann ist p notwendigerweise prim. Andernfalls wäre $p = m\,n$ mit $m, n < p$, also $|m|$, $|n| \geqslant 1$, also $|p| = |m\,n| = |m|\,|n| \geqslant 1$. Es sei nun $|2|, \ldots, |p-1| \leqslant C$ für eine Konstante C. Dann ist

$$|a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k| \leqslant C(1 + \alpha + \alpha^2 + \cdots + \alpha^k) \leqslant \\ \leqslant C/(1-\alpha) = C'.$$

Daraus folgt aber sogar $|x| \leqslant 1$ für alle $x \in \mathbb{Z}$. Es genügt, sich dies für positive x zu überlegen, für 1 bis $x-1$ sei es bereits gezeigt. Nun ist ja

$$|x|^n = |(x-1)+1|^n = |\sum_{i=0}^{n} \binom{n}{i} (x-1)^i| \leqslant \\ \leqslant \sum_{i=0}^{n} |\binom{n}{i}|\,|x-1|^i \leqslant (n+1)C'.$$

Also ist $|x| \leqslant \sqrt[n]{(n+1)C'}$ für jedes ganze $n > 0$, also $|x| \leqslant 1$.

Es sei nun $x = q\,p + r$ mit $0 < r < p$. Dann ist sogar $|x| = 1$. Für $q = 0$ ist dies ja schon gezeigt. Schreibt man nun $x^n = q'p + r'$ mit $0 < r' < p$, so ist $||x|^n - |r'|| \leqslant |x^n - r'| = |q'\,p| \leqslant \alpha$. Da $|r'| = 1$ heißt dies nichts anderes als $||x|^n - 1| \leqslant \alpha$ für alle ganzen $n > 0$, also $|x| = 1$.

Zusammgefaßt erhalten wir

$$|p^n\, r/s| = |p|^n$$

für r, s ganz und teilerfremd zu p. Damit ist $|\cdot|$ zur oben eingeführten p–adischen Bewertung $|\cdot|_p$ äquivalent.

Es bleibt der Fall $|x| \geqslant 1$ für alle $x \in \mathbb{Z}$. Wir ersetzen $|\cdot|$ durch eine äquivalente Metrik für die $|L| > 2$ für das kleinste ganze $L > 0$ mit $|L| > 1$ ist.

Wir zeigen, daß $x \mapsto |x|$ dann eine streng monoton wachsende Funktion auf den positiven ganzen Zahlen ist:

Es sei dafür $K > 0$ eine Zahl mit $|K| > 1$ und $|\cdot|$ bereits streng monoton wachsend für positive ganze Zahlen bis K einschließlich.

Dann ist $(K+1)^n = l_n K^n + B_n$ mit Zahlen l_n für die $l_n \to \infty$ mit $n \to \infty$ und $B_n < K^n$.

Es folgt also $l_n + B_n/K^n = (K+1)^n/K^n$ und durch Anwendung der Bewertungsungleichung

$$||l_n| - |B_n/K^n|| \leqslant |l_n + B_n/K^n| = |(K+1)^n/K^n| \tag{1.63}$$

Nun ist $B_n = a_{n-1}K^{n-1} + \cdots + a_0$ mit $a_i < K$. Also ist $B_n/K^n = a_{n-1}/K + \cdots + a_0/K^n$ und damit auch $|B_n/K^n| \leqslant C$, wobei $C = \sum_{i=0}^{\infty} |(K-1)/K|^i$.

Könnten wir nun zeigen, daß mit $l_n \to \infty$ auch $|l_n| \to \infty$, so wäre klar, daß $|(K+1)/K| > 1$, also $|K+1| > |K|$ ist.

Wir ziehen für diese Überlegung jetzt das oben eingeführte $L > 0$ heran, für das $|L| > 2$ ist. Damit ist ein beliebiges $N = a_n L^n + a_{n-1} L^{n-1} + \cdots + a_0$, also

$$|N| \geqslant ||a_n L^n| - |a_{n-1} L^{n-1} + \cdots + a_0||.$$

Schreiben wir $\alpha = |L| > 2$, so ist $|a_n L^n| = \alpha^n$ und $|a_{n-1} L^{n-1} + \cdots + a_0| \leqslant \sum_{i=0}^{n-1} \alpha^i = (\alpha^n - 1)/(\alpha - 1)$ Zusammengefaßt und ausgerechnet folgt

$$|N| \geqslant \alpha^n - \frac{\alpha^n - 1}{\alpha - 1} = \frac{\alpha^{n+1} - 2\,\alpha^n + 1}{\alpha - 1}$$

so daß $|N| \to \infty$ mit $N \to \infty$ wegen $n \to \infty$.

Durch Übergang zu einer äquivalenten Bewertung $|\cdot|^\gamma$ können wir also nun $|2| = 2$ und damit $|2^n| = 2^n$ für alle $n \in \mathbb{Z}$ annehmen.

Wir setzen voraus, es sei für alle ganzen x mit $1 \leqslant x \leqslant 2^n$ bereits $|x| = x$ gezeigt. Es sei nun $2^n + 1 \leqslant y \leqslant 2^{n+1} - 1$, also $y = 2^n + r = 2^{n+1} - s$ mit $1 \leqslant r, s < 2^n$.

Dann ist $|y| = |2^{n+1} - s| \geqslant ||2^{n+1}| - |s|| = |2^{n+1} - s| = 2^{n+1} - s = y$.

Umgekehrt ist $|y| = |2^n + r| \leqslant |2^n| + |r| = 2^n + r = y$.

Zusammengenommen ist also $|y| = y$ für alle betrachteten y erfüllt. Schreitet man induktiv entsprechend weiter, so gilt $|x| = x$ für alle ganzen $x > 0$ und damit auch für alle x aus $\mathbb{Z}$ und $\mathbb{Q}$.

Anmerkung 1.5.2. Die Bewertungen $|\cdot|_p$ von $\mathbb{Q}$ sind nicht–archimedisch, die gewöhnliche Betragsbewertung $|\cdot|$ ist archimedisch.

Definition 1.5.5. *Es sei E ein Vektorraum über einem bewerteten Körper k mit Bewertung $|\cdot|$.*

Dann heißt eine Abbildung $\|\cdot\|\colon E \to \mathbb{R}$ mit

i) $\|x\| = 0$ *genau dann, wenn* $x = 0$.
ii) $\|\lambda\, x\| = |\lambda|\, \|x\|$ *für* $x \in E$ *und* $\lambda \in k$.
iii) $\|x + y\| \leqslant \|x\| + \|y\|$ *für* $x, y \in E$

eine Norm auf E.

Definition 1.5.6. *Es sei E ein Vektorraum über K mit den Normen $\|\cdot\|_1$ und $\|\cdot\|_2$. Dann heißen $\|\cdot\|_1$ und $\|\cdot\|_2$* äquivalent*, falls sie dieselbe Topologie auf E induzieren.*

Lemma 1.5.1. *Zwei Normen $\|\cdot\|_1$ und $\|\cdot\|_2$ auf E sind genau dann äquivalent, falls es zwei reelle Konstanten $C_1, C_2 > 0$ gibt, mit*

$$C_1\, \|x\|_1 < \|x\|_2 < C_2\, \|x\|_1 \tag{1.64}$$

für alle $x \in E$.

Anmerkung 1.5.3. Man überlegt sich, daß die so definierte Äquivalenz wirklich eine Äquivalenzrelation unter den Normen auf E definiert.

Theorem 1.5.2. *Es sei E ein endlichdimensionaler Vektorraum über dem bewerteten Körper k. Der Körper k sei bezüglich seiner Bewertung vollständig.*

Dann sind alle Normen auf E äquivalent und E ist bezüglich jeder Norm vollständig.

Beweis Wir zeigen, daß eine beliebige Norm $\|\cdot\|$ auf E zu einer beliebigen Norm $\|x\|_\infty$ äquivalent ist, wobei $\|x\|_\infty$ nach Wahl einer Basis $e_1, \ldots, e_n$ durch

$$\|\alpha_1\, e_1 + \cdots + \alpha_n\, e_n\|_\infty = \max(|\alpha_1|, \ldots, |\alpha_n|)$$

definiert ist.

Zunächst einmal ist

$$\|x\| = \|\alpha_1\, e_1 + \cdots + \alpha_n\, e_n\| \leqslant |\alpha_1|\, \|e_1\| + \cdots + |\alpha_n|\, \|e_n\| \leqslant L \max(|\alpha_1|, \ldots, |\alpha_n|) = L\|x\|_\infty \quad (1.65)$$

Dabei hängt die Konstante L nur von den $e_1, \ldots, e_n$ und von n ab.

Es bleibt zu zeigen, daß auch eine Konstante C existiert, mit $C\|x\|_\infty < \|x\|$. Für eindimensionale Vektorräume ist dies wegen $\|\alpha\, x\| = |\alpha|\|x\|$ klar.

Es sei nun wieder $e_1, \ldots, e_n$ eine Basis von E und für Dimensionen kleiner n die Aussage über die Äquivalenz aller Normen bereits gezeigt.

Betrachte nun alle $x = \alpha_1\, e_1 + \cdots + \alpha_n\, e_n$. Wenn wenigstens ein α_i gleich Null ist, so gehört x den n verschiedenen $(n-1)$–dimensionalen Vektorräumen $\alpha_i = 0$ an, die wir ab jetzt auch mit E_i abkürzen.

In jedem gibt es ein C_i mit $C_i\|x\|_\infty < \|x\|$, also auch ein universales C mit $C\,\|x\|_\infty < \|x\|$ für alle x die der Vereinigung dieser n Teilräume angehören.

Können wir für die verbleibenden x auch ein K mit $K\,\|x\|_\infty < \|x\|$ finden, ist natürlich auch ein C' vorhanden mit $C'\,\|x\|_\infty < \|x\|$ für alle $x \in E$.

Es sei also $x = \alpha_1\, e_1 + \cdots + \alpha_n\, e_n$ und alle $\alpha_i \neq 0$.

Wir rechnen

$$\|\sum \alpha_i\, e_i\| = \|\sum \alpha_i\, e_i + \sum_{i=2}^{n} \alpha_1\beta_i\, e_i - \sum_{i=2}^{n} \alpha_1\beta_i\, e_i\| = \|\alpha_1\, (e_1 + \sum_{i=2}^{n} \beta_i\, e_i) + \sum_{i=2}^{n} (\alpha_i - \alpha_1\beta_i) e_i\| \quad (1.66)$$

Dabei sind die β_i zunächst freie Parameter, die wir jetzt als $\beta_i = \alpha_i/\alpha_1$ wählen. Damit setzt sich die Rechnung fort als

$$\|\alpha_1\, (e_1 + \sum_{i=2}^{n} \beta_i\, e_i) \; + \; \sum_{i=2}^{n} (\alpha_i - \alpha_1\beta_i) e_i\| = \|\alpha_1\, (e_1 + \sum_{i=2}^{n} \beta_i\, e_i)\| = |\alpha_1| \|(e_1 + \sum_{i=2}^{n} \beta_i\, e_i)\| \quad (1.67)$$

Wir müssen jetzt noch zeigen, daß für ein $c_1 > 0$ stets $\|(e_1 + \sum_{i=2}^{n} \beta_i e_i)\| > c_1$ bleibt. Andernfalls gäbe es ja eine Folge z_n im Untervektorraum $\alpha_1 = 0$ mit $\|e_1 + z_n\| \to 0$. Diese z_n wären dann eine Cauchy-Folge in E_1 bezüglich der eingeschränkten $\|\cdot\|$.

Kraft Induktion ist auf E_1 die eingeschränkte Norm $\|\cdot\|$ mit der Norm $\|\cdot\|_\infty$ äquivalent und damit auch, wie man sich leicht überlegt, E_1 ein vollständiger Vektorraum bezüglich beider Normen. Also würde die Folge z_n gegen ein $z \in E_1$ konvergieren und es müßte dann $\|e_1 + z\| = 0$, also $e_1 + z = 0$ sein. Das widerspräche aber der linearen Unabhängigkeit der e_i.

Also existiert das geünschte c_1 und man hat

$$\|\sum \alpha_i\, e_i\| > |\alpha_1|\, c_1 \tag{1.68}$$

Stellt man dieselben Überlegungen mit $\alpha_2, \ldots, \alpha_n$ anstelle von α_1 an und benennt die entstehenden Konstanten $c_2, \ldots, c_n$, so folgt aus der Vereinigung der entsprechenden Ungleichungen (1.68) die gewünschte Aussage

$$\|\sum \alpha_i\, e_i\| > \max(|\alpha_1|, \ldots, |\alpha_n|)K = \|\sum \alpha_i\, e_i\|_\infty\, K$$

Damit ist der Beweis dann erbracht.

1.5.2 Bewertungen

Definition 1.5.7. *Es sei R ein Integritätsring und $v : R \to \Gamma \cup \{\infty\}$ eine Abbildung in eine angeordnete abelsche Gruppe $(\Gamma, <)$ vereinigt mit einem Symbol ∞. Dann heißt v* (Exponential–)Bewertung*, falls*

1. Für $0 \in R$ die Beziehung $v(0) = \infty$ gilt.
2. Für $x, y \in R\backslash\{0\}$ die Beziehungen

$$v(xy) = v(x) + v(y) \tag{1.69}$$
$$v(x + y) \geqslant \min(v(x), v(y)) \tag{1.70}$$

gelten. Wir schreiben auch $\mathrm{ord}_v(x) = v(x)$ für $x \in R$.

Anmerkung 1.5.4. In einem Ring R mit Bewertung $v : R \to \Gamma$ ist die Menge $R' = \{x \in R \mid v(x) \geqslant 0\}$ ein Unterring mit maximalem Ideal $\mathfrak{m}_{R'} = \{x \in R \mid v(x) > 0\}$.

Definition 1.5.8. *Ist in den Bezeichnungen der vorangehenden Bemerkung $R = R'$, so ist R ein* Bewertungsring *mit* Bewertungsgruppe Γ.

Anmerkung 1.5.5. Die Bewertung $v : R \to \Gamma$ dehnt sich vermöge $v(x/y) = v(x) - v(y)$ eindeutig auf $K = Q(R)$ aus.

Proposition 1.5.4. *Ein Integritätsring R ist genau dann Bewertungsring mit Quotientenkörper K, falls für $x \in K^*$ gilt, daß aus $x \notin R$ die Aussage $x^{-1} \in R$ folgt.*

Beweis. Es sei entweder x oder x^{-1} in R. Die Wertegruppe Γ ist dann$\{x\, R \mid x \in K\}$ mit $x\, R + y\, R = xy\, R$ und $x\, R \geqslant y\, R$ für $x\, R \subseteq y\, R$.

Die Umkehrung folgt aus $R = \{x \in K \mid v(x) \geqslant 0\}$ und $v(x) + v(x^{-1}) = v(1) = 0$.

Proposition 1.5.5. *Es sei R ein Bewertungsring und $\mathfrak{a}, \mathfrak{a}' \subseteq R$ zwei Ideale von R. Dann ist stets entweder $\mathfrak{a} \subseteq \mathfrak{a}'$ oder $\mathfrak{a}' \subseteq \mathfrak{a}$.*

Korollar 1.5.2. *Ein Bewertungsring R ist ein lokaler Ring $(R, \mathfrak{m})$.*

Proposition 1.5.6. *Es sei $R \subseteq K$ ein Bewertungsring mit Quotientenkörper K. Dann ist R in K ganz abgeschlossen.*

Definition 1.5.9. *Es sei K ein Körper und $(R, \mathfrak{m}_R)$ und $(S, \mathfrak{m}_S)$ zwei lokale Teilringe, die in K liegen. Dann sei $S \geqslant R$, falls $S \supseteq R$ und $\mathfrak{m}_S \cap R = \mathfrak{m}_R$.*

Wir sagen: S dominiert *R und schreiben $S \geqslant R$*

Lemma 1.5.2. *Es sei K ein Körper und $(A, \mathfrak{m})$ ein lokaler Unterring sowie $x, x^{-1} \in K$. Dann ist niemals gleichzeitig $\mathfrak{m}A[x] = (1)$ und $\mathfrak{m}A[x^{-1}] = (1)$.*

Beweis. Es folgt aus $\mathfrak{m}A[x] = (1)$, daß x^{-1} ganz über $\mathfrak{m}$ ist und aus $\mathfrak{m}A[x^{-1}] = (1)$, daß x ganz über $\mathfrak{m}$ ist. Also wäre bei Nichteintreten der Folgerung x und x^{-1} ganz über $\mathfrak{m}$. Damit auch $1 = x\,x^{-1}$ ganz über $\mathfrak{m}$. Also $1 + m_1 + \cdots + m_r = u = 0$, was unmöglich ist, da $u \in A^*$.

Theorem 1.5.3. *Es sei K ein Körper und $(\mathcal{L}(K), \leqslant)$ die Menge seiner lokalen Unterringe geordnet mit $\leqslant$ bezüglich der Dominierungseigenschaft. Dann sind die maximalen Elemente von $\mathcal{L}(K)$ genau die Bewertungsringe $(R, \mathfrak{m}) \subseteq K$.*

Theorem 1.5.4. *Es sei K ein Körper und $A \subseteq K$ ein Unterring. Dann ist der ganze Abschluß $\bar{A}$ von A in K gleich dem Schnitt aller Bewertungsringe $R \subseteq K$ mit $R \supseteq A$.*

1.5.3 Diskrete Bewertungsringe

Definition 1.5.10. *Es sei $v : K \to \mathbb{Z} \cup \{\infty\}$ eine (Exponential–)Bewertung eines Körpers K mit Werten in der geordneten abelschen Gruppe $(\mathbb{Z}, <)$. Dann heißt v* diskrete Bewertung *auf K.*

Der Unterring $R = \{x \mid x \in K,\, v(x) \geqslant 0\}$ ist ein diskreter Bewertungsring.

Anmerkung 1.5.6. Für einen Körper K mit diskreter Bewertung $v : K \to \mathbb{Z}$ ist $|\cdot|_v \colon K \to \mathbb{R}$ mit $|x|_v = \rho^{v(x)}$ für $x \in K$ und $0 < \rho < 1$ in $\mathbb{R}$ eine (Absolut–)Bewertung von K im anfangs genannten Sinne.

Diese Bewertungen sind für verschieden gewählte ρ alle zueinander äquivalent und definieren also eine Stelle $v \in \Sigma_K$.

Proposition 1.5.7. *Ein diskreter Bewertungsring R ist ein Hauptidealring.*

Ein solcher Ring ist also ein lokaler Integritätsring $(R, \mathfrak{m}_R)$ mit $\mathfrak{m}_R = (x)$.

Für seinen Quotientenkörper $K = Q(R)$ gilt, daß jedes $y \in K$ sich eindeutig als $y = u\,x^e$ mit $u \in R^*$ und $e \in \mathbb{Z}$ schreiben läßt. Die Bewertung

$$v : R \to \mathbb{Z}$$

ist dann $v(u\,x^e) = e$.

Proposition 1.5.8. *Es sei R ein noetherscher, lokaler Integritätsring, eindimensional und ganz abgeschlossen in seinem Quotientenkörper. Dann ist R ein diskreter Bewertungsring.*

Beweis. Es genügt zu zeigen, daß für $x, y \in \mathfrak{m} - (0)$ entweder $(x) \subseteq (y)$ oder $(y) \subseteq (x)$ gilt. Seien also zwei x, y gegeben für die $(x) \nsubseteq (y)$ und $(y) \nsubseteq (x)$ ist.

Wir betrachten $(x, y) \supsetneq (y)$. Da $\operatorname{Ass} R/(y) = \mathfrak{m}$, gibt es ein $a \in R$, so daß $\operatorname{Ann}_{A/(y)}(a\,x) = \mathfrak{m}$. Dieses $a\,x$ ist damit nicht in (y), da sonst $1 \in \mathfrak{m}$ wäre. Weiter ist für alle $m \in \mathfrak{m}$ niemals $m\,a\,x = u\,y$ mit $u \in R^*$, da dies $y = a'x$ nach sich zöge. Also $a\,x\,\mathfrak{m} \subseteq \mathfrak{m}y$, also $(a\,x)/y\,\mathfrak{m} \subseteq \mathfrak{m}$.

Da $\mathfrak{m}$ endlich erzeugter R–Modul, R ganzabgeschlossen in $Q(R)$ und integer ist, folgt $a\,x/y \in R$. Das bedeutet aber $a\,x \in (y)$ im Widerspruch zu der oben festgestellten Unmöglichkeit.

2

Grundbegriffe

2.1 Diskrete Bewertungsringe

Es sei im folgenden stets A ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$, Quotientenkörper $K = Q(A)$ und Restkörper $k = A/\mathfrak{p}$.

Definition 2.1.1. *Es sei A ein diskreter Bewertungsring mit Bewertung $v : A \to \mathbb{Z} \cup \{\infty\}$. Weiter sei I ein gebrochenes Ideal von A. Dann sei*

$$v(I) := \inf_{x \in I} v(x) \tag{2.1}$$

Proposition 2.1.1. *Für einen diskreten Bewertungsring $(A, \mathfrak{p})$ ist*

$$I = \mathfrak{p}^{v(I)} \tag{2.2}$$

für jedes gebrochene Ideal I von A.

Lemma 2.1.1. *Es sei $(A, \mathfrak{p})$ ein diskreter Bewertungsring mit $k = A/\mathfrak{p}$. Dann gilt*

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong k \tag{2.3}$$

Proposition 2.1.2. *Es sei $v : A \to \mathbb{Z}$ die Bewertung eines diskreten Bewertungsrings mit $Q(A) = K$. Dann ist die Sequenz*

$$0 \to U \to K^* \xrightarrow{v} \mathbb{Z} \to 0 \tag{2.4}$$

exakt für $U = A^*$, die Einheiten *von A.*

Definition 2.1.2. *Es sei $(A, \mathfrak{p})$ ein diskreter Bewertungsring. Dann sei für $n \geqslant 1$*

$$U_n = 1 + \mathfrak{p}^n \tag{2.5}$$

Anmerkung 2.1.1. Es ist $U_{n+1} \subseteq U_n$ und $\bigcap_n U_n = 1$. Die U_n bilden eine Basis für die von der Bewertung $v : A \to \mathbb{Z}$ erzeugte Topologie auf A und K.

Proposition 2.1.3. *1. Die Restklassenabbildung $A \to k$ induziert einen Isomorphismus*

$$U/U_1 \cong k^* \tag{2.6}$$

mit der multiplikativen Gruppe k^*.
2. Für $n \geqslant 1$ induziert die Abbildung $u \mapsto u - 1$ einen Isomorphismus

$$U_n/U_{n+1} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}. \tag{2.7}$$

Proposition 2.1.4. *Es sei A ein diskreter Bewertungsring mit Bewertung $v : A \to \mathbb{Z} \cup \{\infty\}$. Weiter sei $\hat{A}$ die Komplettierung von A bezüglich der Bewertung v, beziehungsweise bezüglich der Filtrierung $(\mathfrak{p}^n)_n$.*

Dann kann man v eindeutig zu einer diskreten Bewertung $\bar{v} : \hat{A} \to \mathbb{Z} \cup \{\infty\}$ ausdehnen, so daß insbesondere $\mathfrak{p}\hat{A} = \{x \in \hat{A} \mid \bar{v}(x) > 0\}$ ist.

2.2 Dedekindringe

Im folgenden sei der Quotientenkörper eines Integritätsringes A immer $K = Q(A)$.

Proposition 2.2.1. *Für einen Integritätsring A mit Quotientenkörper K ist äquivalent:*

a) Es ist $\dim A = 1$ *und A ist noethersch und abgeschlossen in K.*
b) A ist noethersch und alle Lokalisierungen $A_\mathfrak{p}$ an maximalen Idealen $\mathfrak{p} \subseteq A$ sind diskrete Bewertungsringe.
c) Alle gebrochenen Ideale $I \subseteq K$ von A sind invertierbar, es ist also $I(A : I) = A$

Definition 2.2.1. *Ein Ring A, der die Bedingungen der vorigen Proposition erfüllt, heißt* Dedekindring.

Anmerkung 2.2.1. Ein diskreter Bewertungsring und ein Hauptidealring ist ein Dedekindring.

Definition 2.2.2. *Es sei A ein Dedekindring. Dann sei I_A die Menge seiner gebrochenen Ideale.*

Die gebrochenen Ideale I_A sind eine abelsche Gruppe unter der (multiplikativen) Verknüpfung $(I, J) \mapsto IJ$ für $I, J \in I_A$.

Man hat eine kanonische exakte Sequenz

$$0 \to U \to K^* \xrightarrow{\alpha} I_A \tag{2.8}$$

mit $\alpha(x) = xA$.

Das Bild von α sind die *Hauptideale von A*, eine Untergruppe von I_A, die wir mit P_A bezeichnen. Der Kern U von α sind die *Einheiten von A*.

Wir haben also auch eine exakte Sequenz

$$0 \to P_A \to I_A \to \mathrm{Cl}_A \to 0 \tag{2.9}$$

die eine Quotientengruppe von I_A definiert, die *Idealklassengruppe von A*. Es wird sich später herausstellen, daß es sich dabei stets um eine endliche Gruppe handelt.

Definition 2.2.3. *Es sei A ein Dedekindring mit $K = Q(A)$ und $\mathfrak{p} \subseteq A$ ein maximales Ideal. Dann heiße*

$$v_{\mathfrak{p}} : K \to \mathbb{Z} \tag{2.10}$$

die von $\mathfrak{p}$ auf K induzierte diskrete Bewertung. Sie entsteht durch die Einbettung $A \to A_{\mathfrak{p}}$ in den diskreten Bewertungsrig $A_{\mathfrak{p}}$.

Proposition 2.2.2. *Es sei A ein Dedekindring und $|\cdot|_v$: $K \to \mathbb{R}$ eine multiplikative diskrete Bewertung von K mit $|A| \leqslant 1$. Dann ist $|x|_v = \rho^{v_{\mathfrak{p}}(x)}$ für ein $0 < \rho < 1$ und ein maximales Ideal $\mathfrak{p} \subseteq A$.*

Beweis. Das Ideal $\mathfrak{p}$ ist $\{x \in K \mid |x| < 1\}$.

Definition 2.2.4. *Es sei A ein Dedekindring, K sein Quotientenkörper und $\mathfrak{p} \subseteq A$ ein maximales Ideal. Es sei weiter $I \subseteq K$ eine nichtleere Teilmenge von K.*

Dann sei

$$v_{\mathfrak{p}}(I) := \inf_{x \in I} v_{\mathfrak{p}}(x) \tag{2.11}$$

Lemma 2.2.1. *Es sei A ein Dedekindring, $\mathfrak{p}$ ein maximales Ideal und $I \subseteq K$ ein gebrochenes Ideal. Dann ist*

$$IA_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{v_{\mathfrak{p}}(I)} \tag{2.12}$$

Theorem 2.2.1. *Es sei A ein Dedekindring. Dann ist jedes $I \in I_A$ als*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \tag{2.13}$$

darstellbar. Die gebrochenen Ideale I_A bilden also eine abelsche Gruppe unter Multiplikation, die von den maximalen $\mathfrak{p} \in \mathrm{Spec}\,(A)$ frei erzeugt wird.

Lemma 2.2.2. *Es sei A ein Dedekindring, $\mathfrak{a} \in I_A$ und $\mathfrak{p} \in \mathrm{Spec}\,(A)$.*

Dann ist isomorph

$$\mathfrak{a}/\mathfrak{p}\mathfrak{a} = A/\mathfrak{p} \tag{2.14}$$

Proposition 2.2.3. *Es sei A ein Dedekindring und $a \in K^*$. Dann ist $v_{\mathfrak{p}}(a) = 0$ für fast alle maximalen Ideale $\mathfrak{p} \subseteq A$.*

Proposition 2.2.4. *Es seien I, I_1, I_2 gebrochene Ideale eines Dedekindrings A und $\mathfrak{p} \subseteq A$ ein maximales Ideal. Dann gilt:*

$$v_\mathfrak{p}(I_1 I_2) = v_\mathfrak{p}(I_1) + v_\mathfrak{p}(I_2) \tag{2.15}$$

$$v_\mathfrak{p}(I^{-1}) = -v_\mathfrak{p}(I) \tag{2.16}$$

$$v_\mathfrak{p}(I_1 + I_2) = \min v_\mathfrak{p}(I_1), v_\mathfrak{p}(I_2) \tag{2.17}$$

$$v_\mathfrak{p}(I_1 \cap I_2) = \max v_\mathfrak{p}(I_2), v_\mathfrak{p}(I_2) \tag{2.18}$$

Proposition 2.2.5. *Es sei A ein Dedekindring, $\mathfrak{p} \subseteq A$ ein maximales Ideal und I ein gebrochenes Ideal von A.*

Die Abbildung $I \mapsto I_\mathfrak{p} A_\mathfrak{p}$ induziert einen surjektiven Gruppenhomomorphismus

$$I_A \to I_{A_\mathfrak{p}} \cong \mathbb{Z}. \tag{2.19}$$

Proposition 2.2.6. *Es sei A ein Dedekindring. Dann existiert ein Isomorphismus*

$$I_A \cong \coprod_\mathfrak{p} I_{A_\mathfrak{p}} \tag{2.20}$$

Proposition 2.2.7. *Es sei A ein Dedekindring und $\mathfrak{p} \subseteq A$ ein maximales Ideal.*

Dann ist

$$I_{A_\mathfrak{p}} \cong I_{\widehat{A_\mathfrak{p}}} \cong \mathbb{Z} \tag{2.21}$$

Korollar 2.2.1. *Es ist für einen Dedekindring A*

$$I_A \cong \coprod_\mathfrak{p} I_{\widehat{A_\mathfrak{p}}} \tag{2.22}$$

2.3 Moduln und Bilinearformen

Es sei im folgenden A ein Dedekindring mit Quotientenkörper $K = Q(A)$ und $U \cong K^n$ ein n-dimensionaler Vektorraum über K. Es sei $T \subseteq U$ ein beliebiger A–Modul.

Weiter seien $L, M, N \subseteq U$ endlich erzeugte A–Moduln mit

$$L \otimes_A K = M \otimes_A K = N \otimes_A K = U$$

Dies ist äquivalent zu der Tatsache, daß L, M, N jeweils eine K–Basis von U enthalten.

Wir betrachten $T_\mathfrak{p} \subseteq U$ als kanonisch in U eingebettet.

Lemma 2.3.1. *Es ist $T = \bigcap_\mathfrak{p} T_\mathfrak{p}$ wobei $\mathfrak{p} \subseteq A$ durch die maximalen Ideale von A läuft.*

Lemma 2.3.2. *Für M, N wie oben existiert ein $a \in K^*$ mit $aM \subseteq N$.*

Lemma 2.3.3. *Für fast alle $\mathfrak{p} \subseteq A$, maximal, ist $M_\mathfrak{p} = N_\mathfrak{p}$.*

Es seien jetzt M, N freie A–Moduln. Dann existiert eine A–lineare, also K–lineare Abbildung $l : U \to U$ mit $l(M) = N$. Ist $M = Ax_1 + \cdots + Ax_n$ und $N = Ay_1 + \cdots + Ay_n$ mit freien A–Erzeugern x_i, y_j, so sind die x_i und y_j auch K–Basen von U und es kann $l(x_i) = y_i$ gesetzt werden.

Wir definieren jetzt

Definition 2.3.1. *Es seien M, N freie A–Moduln und $l : U \to U$, eine A–lineare Abbildung, mit $l(M) = N$. Dann sei*

$$[M : N]_A := [M : N] := (\det l)A \tag{2.23}$$

Begründung. Wir haben hier die Wohldefiniertheit von $[M : N]$ zu zeigen:

Es seien x_i und x_i' zwei A–Basen von M und y_i sowie y_i' zwei A–Basen von N. Weiter seien $l : U \to U$ durch $l(x_i) = y_i = \sum a_{ij}x_j$ und $l' : U \to U$ durch $l'(x_i') = y_i' = \sum a_{ij}'x_j'$ definiert.

Es ist dann $\det l = \det|a_{ij}|$ und $\det l' = \det|a_{ij}'|$. Weiter ist $(x_i') = P(x_i)$ mit $P \in \mathrm{GL}(n, A)$ und $(y_i') = Q(y_i)$ mit $Q \in \mathrm{GL}(n, A)$.

Setzt man $W = |a_{ij}| \in \mathrm{GL}(n, K)$ und $W' = |a_{ij}'| \in \mathrm{GL}(n, K)$ so ist $QW(x_i) = W'P(x_i)$, also $QW = W'P$.

Wegen $\det P, \det Q \in A^*$ ist $\det W = u \det W'$ mit $u \in A^*$, also $(\det W)A = (\det W')A =: [M : N]\, A$ wohldefiniert.

Es ist nun im allgemeinen Fall für beliebigen Dedekindring A und $\mathfrak{p} \subseteq A$, maximal, immer $M_\mathfrak{p}$ und $N_\mathfrak{p}$ ein freier $A_\mathfrak{p}$–Modul.

Wir können daher definieren

Definition 2.3.2. *Es sei das gebrochene Ideal $[M : N]_A := [M : N]$ definiert durch*

$$[M : N]A_\mathfrak{p} = [M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}} \tag{2.24}$$

Proposition 2.3.1. *Es gilt für M, N, L wie oben*

1. $[M : N][N : L] = [M : L]$
2. $[M : M] = A$
3. *Ist $M \supseteq N$, so ist $[M : N] \subseteq A$ ein gewöhnliches Ideal und aus $[M : N] = A$ folgt $M = N$.*

Proposition 2.3.2. *Es sei $t : U \to U$ ein K–linearer Isomorphismus. Dann ist*

$$[tM : tN] = [M : N] \tag{2.25}$$

Es sei nun $B : U \times U \to K$ eine nichtausgeartete symmetrische Bilinearform auf U. Dann definiert B einen Isomorphismus $U \to U^*$ in den Dualraum von U.

Für eine K–Basis von U aus x_i existiert daher eine duale Basis x_j' von U mit der Eigenschaft

$$B(x_i, x_j') = \delta_{ij} \tag{2.26}$$

mit dem Kroneckerschen δ_{ij}.

Definition 2.3.3. *Es sei B eine Bilinearform auf U und $T \subseteq U$ ein A–Modul wie oben eingeführt. Dann ist*

$$D_A(T) = D(T) := \{x \in U \mid B(x,T) \subseteq A\} \tag{2.27}$$

ein A–Untermodul von U, der duale Modul von T.

Es stehe $D_{\mathfrak{p}}(-)$ für $D_{A_{\mathfrak{p}}}(-)$.

Lemma 2.3.4. *Es sei $M \subseteq U$ ein freier A-Modul mit den freien Erzeugern $x_1, \ldots, x_n \in U$.*

Dann ist die duale Basis $x_1', \ldots, x_n' \in U$ mit $B(x_i, x_j') = \delta_{ij}$ ein System freier Erzeuger von $D(M)$ und es gilt

$$D(D(M)) = M \tag{2.28}$$

Proposition 2.3.3. *Für $M, N \subseteq U$ mit den anfangs genannten Eigenschaften gilt:*

1. $D(M)$ ist ein endlich erzeugter A–Modul mit $D(M) \otimes_A K = U$.
2. $D(M)_{\mathfrak{p}} = D_{\mathfrak{p}}(M_{\mathfrak{p}})$.
3. $D(M) = \bigcap_{\mathfrak{p}} D_{\mathfrak{p}}(M_{\mathfrak{p}})$.
4. $D(D(M)) = M$.
5. $[D(M) : D(N)] = [N : M]$.

Definition 2.3.4. *Für ein M wie oben definieren wir $d(M) = d(M/A) = [D_A(M) : M]_A$, die* Diskriminante von M (bezüglich A).

Proposition 2.3.4. *Es seien M, N wie oben. Dann gilt*

1. $d(N) = d(M)[M : N]^2$.
2. $d(M_{\mathfrak{p}}/A_{\mathfrak{p}}) = d(M/A)A_{\mathfrak{p}}$
3. Ist $M = Ax_1 + \cdots + Ax_n$ von den x_i frei erzeugt, so ist

$$d(M/A) = \det|B(x_i, x_j)|\, A \tag{2.29}$$

als gebrochenes Ideal von A.

Korollar 2.3.1. *Es sei $M \supseteq N$. Dann ist $d(M) \mid d(N)$ und aus $d(M) = d(N)$ folgt $M = N$.*

Es sei jetzt $U = U_1 \oplus U_2$ die direkte Summe zweier K–Vektorräume. Ebenso sei $M = M_1 \oplus M_2$ und $N = N_1 \oplus N_2$ mit $M_i, N_i \subseteq U_i$ und $M_i \otimes_A K = N_i \otimes_A K = U_i$. Für die bilineare Form B gelte $B(U_1, U_2) = 0$.

Dann gilt

Proposition 2.3.5. *1. $[M : N] = [M_1 : N_1][M_2 : N_2]$.*
2. $D(M) = D(M_1) + D(M_2)$.
3. $d(M) = d(M_1)d(M_2)$.

Es sei jetzt $\bar{A}/A$ eine Erweiterung von Dedekindringen und $\bar{K} = Q(\bar{A})$. Wir betrachten $\bar{U} = U \otimes_K \bar{K}$ als $\bar{K}$–Vektorraum und $U \subseteq \bar{U}$ als in $\bar{U}$ eingebettet. Die Bilinearform $B : U \times U \to K$ kann dann zu einer ebenfalls nicht ausgearteten symmetrischen Bilinearform $\bar{B} : \bar{U} \times \bar{U} \to \bar{K}$ fortgesetzt werden.

Weiterhin ist $\bar{M} = M\bar{A}$ ein lokal freier $\bar{A}$–Modul mit $\bar{M} \otimes_{\bar{A}} \bar{K} = \bar{U}$. Entsprechend sei $\bar{N} = N\bar{A}$ definiert.

Es gilt dann

Proposition 2.3.6. *1.* $[M\bar{A} : N\bar{A}]_{\bar{A}} = [M : N]_A \bar{A}$.
2. $D_{\bar{A}}(M\bar{A}) = D_A(M)\bar{A}$.
3. $d(M\bar{A}/\bar{A}) = d(M/A)\bar{A}$.

2.4 Erweiterungen

Theorem 2.4.1. *Es sei A ein Dedekindring mit Quotientenkörper K und L/K eine separable endliche Körpererweiterung. Dann ist der ganze Abschluß B von A in L auch ein Dedekindring.*

Beweis. Es ist $(x, y) \mapsto \mathrm{Tr}_{L|K}(xy)$ eine nichtausgeartete K–Bilinearform über L. Es ist damit $L = U$ im Sinne des vorigen Abschnitts und für geeeignetes $N \subseteq L$ ist $D(N)$ definiert.

Es sei nun $N = Ab_1 + \cdots + Ab_n$ mit $n = [L : K]$ und $b_i \in B$ sowie $N \otimes_A K = L$. Dann ist $N \subseteq B$ und damit $D(B) \subseteq D(N)$. Weiter ist aber auch $B \subseteq D(B)$, da $\mathrm{Tr}_{L|K}(b_1' b_2') \in A$ für $b_i' \in B$. Also $B \subseteq D(N)$ und $D(N)$ ist ein freier A–Modul isomorph zu A^n. Damit ist B ein endlich erzeugter A–Modul, also noethersch. Da B ganz über A ist $\dim A = \dim B = 1$ und wegen $B \subseteq L$ ist B auch ein Integritätsring. Damit ist B als Dedekindring erwiesen.

Proposition 2.4.1. *Es sei A, B, L, K wie im vorigen Theorem. Dann ist $I \mapsto IB$ ein Gruppenhomomorphismus $I_A \to I_B$.*

Proposition 2.4.2. *Es sei A ein diskreter Bewertungsring mit Quotientenkörper K und der Bewertung $|\cdot|_v$ auf K. Weiter sei L/K eine endliche separable Erweiterung. Dann existiert (mindestens) eine Fortsetzung $|\cdot|_w$ von $|\cdot|_v$ auf L und diese ist auch eine diskrete Bewertung.*

Beweis. Es sei B der ganze Abschluß von A in L und $\mathfrak{P} \subseteq B$ ein Primideal mit $\mathfrak{P} \cap A = \mathfrak{m}$ und $\mathfrak{m} \subseteq A$, dem maximalen Ideal. Dann ist $v_{\mathfrak{P}} : L \to \mathbb{Z} \cup \{\infty\}$ eine Fortsetzung der Bewertung $v : K \to \mathbb{Z} \cup \{\infty\}$.

Proposition 2.4.3. *Es sei K ein bezüglich der diskreten Bewertung $|\cdot|_v$ vollständiger Körper und A sein diskreter Bewertungsring. Weiter sei L/K eine endliche separable Erweiterung von K.*

Dann existiert eine eindeutige Fortsetzung $|\cdot|_w \colon L \to \mathbb{R}$ von $|\cdot|_v$. Diese ist eine diskrete Bewertung und ihr Bewertungsring B ist der ganze Abschluß von A in L.

Beweis. Es sei wieder B der ganze Abschluß von $(A, \mathfrak{m})$ in L. Jedem Primideal $\mathfrak{P} \subseteq B$ entspricht eine Fortsetzung von $v_{\mathfrak{m}}$ nach L. Diese Fortsetzung ist aber eindeutig, da K vollständig und $\dim_K L = n < \infty$ ist. Also ist B ein Dedekindring mit nur einem Primideal, also ein diskreter Bewertungsring. Da die fortgesetzte Bewertung eindeutig ist, fällt sie mit $w_{\mathfrak{P}}$ zusammen und B ist daher auch der Bewertungsring von $|\cdot|_w$.

Es sei für die folgende Proposition K ein durch $|\cdot|_v$ diskret bewerteter Körper mit Bewertungsring A und L/K eine separable endliche Erweiterung. Weiter sei B der ganze Abschluß von A in L.

Es sei dann $\bar{K}$ die Vervollständigung von K bezüglich $|\cdot|_v$ und es sei $\bar{A}$ der topologische Abschluß von A in $\bar{K}$. Dann ist $\bar{A}$ auch der diskrete Bewertungsring bezüglich der kanonischen Bewertung $|\cdot|_{v'}$ von $\bar{K}$, die aus $|\cdot|_v$ hervorgeht.

Es seien $|\cdot|_{w_i}$, mit $i = 1, \ldots, r$, die Fortsetzungen von $|\cdot|_v$ auf L und $\bar{L}_i$ die Komplettierungen bezüglich dieser Fortsetzungen. Weiter seien $\bar{B}_i$ die zugehörigen diskreten Bewertungsringe. Diese sind gleich den ganzen Abschlüssen von $\bar{A}$ in $\bar{L}_i$.

Proposition 2.4.4. *Es gilt mit den hier eingeführten Bezeichnungen und dem im Beweis benannten $B\bar{A}$*

$$B\bar{A} = \bar{B}_1 \times \cdots \times \bar{B}_r \tag{2.30}$$

als algebraische und topologische Isomorphie.

Beweis. Es ist $L \otimes_K \bar{K} = \bar{L}_1 \times \cdots \times \bar{L}_r$ mit einer Abbildung u von links nach rechts. Es ist $B = A^n$ mit $n = [L : K]$.

Weiter existiert eine injektive Abbildung $i : B \otimes_A \bar{A} \to L \otimes_K \bar{K}$. Das Bild $i(B \otimes_A \bar{A})$ sei $B\bar{A}$ und dessen Bild unter u ist, das ist zu zeigen, gleich $B' = \bar{B}_1 \times \cdots \times \bar{B}_r$.

Zunächst ist nun B ganz über A, also das Bild

$$u(b \otimes_A \bar{a}) = (\bar{b}_1, \ldots, \bar{b}_r)$$

für ein beliebiges $b \in B$ auch ganz über $\bar{A}$. Damit ist jedes $\bar{b}_i$ ganz über $\bar{A}$, also $\bar{b}_i \in \bar{B}_i$ und $B\bar{A} \subseteq B'$.

Des weiteren ist $\bar{B}_i$ gleich dem *topologischen* Abschluß von $B \subseteq \bar{L}_i$ unter der Topologie, die von $|\cdot|_{w_i}$ ausgeht.

Es seien also jetzt $z_i \in \bar{B}_i$ vorgegeben. Wähle dann $b_i \in B$ mit $|z_i - b_i|_{w_i} < \varepsilon$. Da die $|\cdot|_{w_i}$ unabhängige Bewertungen auf B induzieren, gibt es ein $b \in B$ mit $|b - b_i|_{w_i} < \varepsilon$. Damit ist $|z_i - b|_{w_i} < 2\varepsilon$ und $B\bar{A} \subseteq B'$ ist dicht in B'. Andererseits ist $B\bar{A} = \bar{A}^n$ vollständig, also abgeschlossen in B'. Damit ist $B\bar{A} = B'$, was zu zeigen war.

Theorem 2.4.2 (EFG-Theorem). *Es sei A ein Dedekindring mit Quotientenkörper K und einer separablen algebraischen Erweiterung L/K mit $[L : K] = n$. Es sei B der ganze Abschluß von A in L. Es sei schließlich $\mathfrak{p}$ ein Primideal von A.*

Dann ist

$$\mathfrak{p}\,B = \mathfrak{q}_1^{e_1} \cdot \cdots \cdot \mathfrak{q}_g^{e_g} \tag{2.31}$$

mit Primdealen $\mathfrak{q}_i$ *aus* $\operatorname{Spec}(B)$*. Nennt man* $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$*, so gilt*

$$n = \sum_{i=1}^{g} e_i\, f_i \tag{2.32}$$

Beweis Wir können lokalisieren, also B und A durch $B_\mathfrak{p}$ und $A_\mathfrak{p}$ ersetzen. Dann ist A ein diskreter Bewertungsring und $B \cong A^n$, also $B/\mathfrak{p}B = B \otimes_A k(\mathfrak{p}) = k(\mathfrak{p})^n = k^n$. Es ist also $[B/\mathfrak{p}B : k] = n$. Diese Dimension zählen wir nun durch eine Filtrierung ab

$$B \supseteq \cdots \supsetneq \prod \mathfrak{q}_i^{a_{i,s}} \supsetneq \prod \mathfrak{q}_i^{a_{i,s+1}} \supsetneq \cdots \supsetneq \mathfrak{p}B \tag{2.33}$$

Dabei sei $1 \geqslant a_{i,s+1} - a_{i,s} \geqslant 0$, wobei nur eine von Null verschiedene Differenz auftrete. Wir können die Exponenten also Schritt für Schritt, zum Beispiel lexikographisch, heraufzählen.

Offensichtlich ist $\prod \mathfrak{q}_i^{a_{i,s}} / \prod \mathfrak{q}_i^{a_{i,s+1}} = B/\mathfrak{q}_{js}$. Dabei tritt jedes $\mathfrak{q}_i$ genau e_i–mal als Quotient zweier Schritte in der Filtration auf. Da $[B/\mathfrak{q}_i : k] = f_i$ per Definition ist folgt also $n = \sum e_i\, f_i$. Der im folgenden eingeführte Begriff der *Verzweigung* ist ein Schlüsselkonzept:

Definition 2.4.1. *Für* B/A *und mit den Bezeichnungen des EFG-Theorems heißt* $\mathfrak{p}$ verzweigt in B*, falls wenigstens ein* $e_i > 1$ *ist.*

Das folgende Theorem ist ein wichtiger Schlüssel zur „praktischen“ Analyse des Zerlegungs- und Verzweigungsverhaltens:

Theorem 2.4.3. *Es sei* B/A *eine ganze Ringerweiterung und* $\mathfrak{p} \subseteq A$ *ein maximales Ideal. Weiter sei* $\alpha \in B$ *mit* $f_\alpha(\alpha) = 0$ *für ein monisches* $f_\alpha(X) \in A[X]$ *und es gelte*

$$B/\mathfrak{p}B = (A/\mathfrak{p})[\alpha + \mathfrak{p}B] = (A/\mathfrak{p})[\bar{\alpha}]. \tag{2.34}$$

sowie

$$\dim_{k(\mathfrak{p})} B/\mathfrak{p}B = \deg f_\alpha(X) = n \tag{2.35}$$

mit $k(\mathfrak{p}) = A/\mathfrak{p}$*.*

Weiter seien $g_1(X), \ldots, g_r(X) \in A[X]$ *und es sei*

$$f_\alpha(X) = g_1(X)^{e_1} \cdot \cdots \cdot g_r(X)^{e_r} \mod \mathfrak{p}A[X]$$

eine Primfaktorzerlegung im Hauptidealring $k(\mathfrak{p})[X]$*.*

Dann sind die $\mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha)) \subseteq B$ *maximale Ideale und es gilt*

$$\mathfrak{p}B = (\mathfrak{p}, \mathfrak{P}_1^{e_1}) \cdot \cdots \cdot (\mathfrak{p}, \mathfrak{P}_r^{e_r}) = (\mathfrak{p}, g_1(\alpha)^{e_1}) \cdot \cdots \cdot (\mathfrak{p}, g_r(\alpha)^{e_r}) \tag{2.36}$$

Ist B/A *eine Erweiterung von Dedekindringen, so gilt sogar*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdot \cdots \cdot \mathfrak{P}_r^{e_r} \tag{2.37}$$

Beweis. Man betrachte die Sequenz

$$0 \to I \to (A/\mathfrak{p})[X] \xrightarrow{\psi} B/\mathfrak{p}B \to 0$$

wobei $\psi(X) = \bar{\alpha}$ ist. Es ist $I' = (\bar{f}_\alpha(X)) \subseteq I$. Weil $n = \deg f_\alpha(X) = \dim_{k(\mathfrak{p})} B/\mathfrak{p}B$ ist, gilt sogar $I = I'$ aus Dimensionsgründen. Also ist

$$B/\mathfrak{p}B \cong (A/\mathfrak{p})[X]/(\bar{f}_\alpha(X))$$

woraus die erste Behauptung nach dem chinesischen Restsatz folgt. Die zweite Behauptung über Dedekindringe gilt aufgrund folgender Argumentation: Zunächst ist $\mathfrak{P}_i^l/\mathfrak{P}_i^{l+1} = B/\mathfrak{P}_i$, also auch $\dim_{k(\mathfrak{p})} \mathfrak{P}_i^l/\mathfrak{P}_i^{l+1} = f_i = \deg g_i$.

Mit der Sequenz

$$0 \to J \to B \to \prod_{i=1}^{r} A[x]/(\mathfrak{p}, g_i(x)^{e_i}) \to 0$$

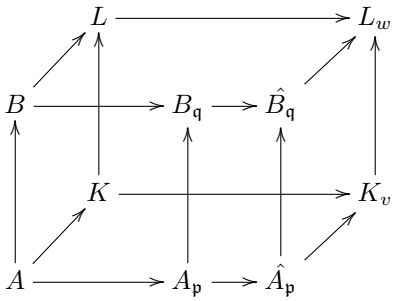
gilt $\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r} \subseteq J = \mathfrak{p}B$. Weiterhin ist

$$\dim_{k(\mathfrak{p})} B/(\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}) = \sum_i e_i f_i = n = \dim_{k(\mathfrak{p})} B/J$$

Also nach Dimensionsgründen $\mathfrak{p}B = J = \mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$.

Es sei A ein Dedekindring mit Quotientenkörper K und L eine endliche, separable Erweiterung von K. Weiter sei B der ganze Abschluß von A in L und es seien $\mathfrak{p} \subseteq A$ und $\mathfrak{q} \subseteq B$ Primideale mit $\mathfrak{q} \cap A = \mathfrak{p}$. Schließlich seien v bzw. w die von $\mathfrak{p}$ bzw. $\mathfrak{q}$ erzeugten Bewertungen von K bzw. L.

Dann hat man das kommutative Diagramm



(2.38)

wobei K_v und L_w die Komplettierungen von K und L bezüglich v und w sind.

2.5 Idealnormen

Es sei im folgenden B/A eine endliche Erweiterung von Dedekindringen und L/K die zugehörige Erweiterung der Quotientenkörper.

Definition 2.5.1. *Es sei J ein gebrochenes Ideal von B. Dann ist*

$$\mathrm{Nm}_{B|A}(J) = [B : J]_A \tag{2.39}$$

die Idealnorm von J, ein gebrochenes Ideal von A.

Proposition 2.5.1. *Es sei L/K wie oben mit $K = \mathbb{Q}$ und $A = \mathbb{Z}$. Weiter sei $\mathfrak{b} \subseteq B$ ein ganzes Ideal von B.*

Dann ist

$$|(B/\mathfrak{b})| \cdot \mathbb{Z} = \mathrm{Nm}_{B|\mathbb{Z}}(\mathfrak{b}) \tag{2.40}$$

Vergleicht man die $\mathrm{Norm}_{L|K}(x)$ und $\mathrm{Nm}_{B|A}(xB)$ so ergibt sich

Proposition 2.5.2. *Für $x \in L$ gilt*

$$\mathrm{Nm}_{B|A}(xB) = \mathrm{Norm}_{L|K}(x)A \tag{2.41}$$

Ist A ein diskreter Bewertungsring, K der Quotientenkörper und $B, L, \bar{A}, \bar{K}, \bar{B}_i$ wie in Proposition (2.4.4) so gilt

Proposition 2.5.3. *Es sei J ein gebrochenes Ideal von B. Dann gilt*

$$\mathrm{Nm}_{B|A}(J)\bar{A} = \prod_{i=1}^{r} \mathrm{Nm}_{\bar{B}_i|\bar{A}}(J\bar{B}_i) \tag{2.42}$$

Beweis. Folgt aus Proposition 2.3.5 und Proposition 2.3.6.

Es sei nun A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung, B der ganze Abschluß von A in L. Über dem Primideal $\mathfrak{p} \subseteq A$ mögen die Ideale $\mathfrak{P}_i \subseteq B$, mit $i = 1, \ldots, r$, liegen. Es seien $A_\mathfrak{p}$ und $B_{\mathfrak{P}_i}$ die Lokalisierungen und $\bar{A}_\mathfrak{p}$ und $\bar{B}_{\mathfrak{P}_i}$ die Komplettierungen.

Dann folgt aus der vorigen Proposition das

Korollar 2.5.1. *Es sei J ein gebrochenes Ideal von B. Dann gilt*

$$\mathrm{Nm}_{B|A}(J)\bar{A}_\mathfrak{p} = \prod_{i=1}^{r} \mathrm{Nm}_{\bar{B}_{\mathfrak{P}_i}|\bar{A}_\mathfrak{p}}(J\bar{B}_{\mathfrak{P}_i}) \tag{2.43}$$

Proposition 2.5.4. *Es sei A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung mit Dedekindring B als ganzem Abschluß von A.*

Dann ist $J \mapsto \mathrm{Nm}_{B|A}(J)$ ein Gruppenhomomorphismus

$$\mathrm{Nm}_{B|A} : I_B \to I_A \tag{2.44}$$

der jeweiligen Gruppen gebrochener Ideale.

Proposition 2.5.5. *Es sei A ein Dedekindring mit Quotientenkörper K und L/K eine separable Erweiterung mit $[L : K] = n$ und mit Dedekindring B als ganzem Abschluß von A.*

Es sei I ein gebrochenes Ideal von A. Dann gilt

$$\mathrm{Nm}_{B|A}(IB) = I^n A \tag{2.45}$$

Proposition 2.5.6. *Es sei A ein Dedekindring mit Quotientenkörper K und separablen Erweiterungen $F/L/K$ die zu Erweiterungen $C/B/A$ von Dedekindringen führen.*

Es sei nun J ein gebrochenes Ideal von C. Dann gilt

$$\mathrm{Nm}_{B|A}\ \mathrm{Nm}_{C|B}(J) = \mathrm{Nm}_{C|A}(J) \tag{2.46}$$

2.6 Differente

Es sei A ein Dedekindring mit Quotientenkörper K und L/K eine separable, endliche Körpererweiterung, sowie B der ganze Abschluß von A in L.

Da $\mathrm{Tr}_{L|K}(b_1 b_2) \in A$ für $b_i \in B$, ist $D(B) \supseteq B$. Damit ist $D(B)^{-1} \subseteq B$ ein ganzes Ideal von B und wir können definieren

Definition 2.6.1. *Es sei B/A und L/K wie oben. Dann ist $\mathfrak{D}_{B|A} = D(B)^{-1} \subseteq B$ ein ganzes Ideal von B, die* Differente von B über A.

Es gilt

Proposition 2.6.1. *Mit B/A und L/K wie oben gilt $\mathrm{Nm}_{B|A}(\mathfrak{D}_{B|A}) = d(B/A)$. Die Diskriminante ist also die Norm der Differente.*

Beweis.

$$\mathrm{Nm}_{B|A}(\mathfrak{D}_{B|A}) = \mathrm{Nm}_{B|A}(D(B)^{-1}) = (\mathrm{Nm}_{B|A}(D(B)))^{-1} =$$

$$= [B : D(B)]^{-1} = [D(B) : B] = d(B/A) \tag{2.47}$$

Die zweite Gleichheit folgt, weil $J \mapsto [B : J]_A$ ein Gruppenhomomorphismus von I_B nach I_A ist.

Es sei nun A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung, B der ganze Abschluß von A in L. Über dem Primideal $\mathfrak{p} \subseteq A$ mögen die Ideale $\mathfrak{P}_i \subseteq B$, mit $i = 1, \ldots, r$, liegen. Es seien $A_\mathfrak{p}$ und $B_{\mathfrak{P}_i}$ die Lokalisierungen und $\bar{A}_\mathfrak{p}$ und $\bar{B}_{\mathfrak{P}_i}$ sowie $K_\mathfrak{p}$ und $L_{\mathfrak{P}_i}$ die Komplettierungen.

Dann gilt

Proposition 2.6.2.

$$\mathfrak{D}_{B|A}\, \bar{B}_{\mathfrak{P}_i} = \mathfrak{D}_{\bar{B}_{\mathfrak{P}_i}|\bar{A}_\mathfrak{p}} \tag{2.48}$$

$$d(B/A)\bar{A}_\mathfrak{p} = \prod_i d(\bar{B}_{\mathfrak{P}_i}/\bar{A}_\mathfrak{p}) \tag{2.49}$$

Beweis. Wir benutzen Proposition 2.3.5. Es ist

$$U = L \otimes_K K_\mathfrak{p} = L_{\mathfrak{P}_1} \oplus \cdots \oplus L_{\mathfrak{P}_r} = U_1 \oplus \cdots \oplus U_r$$

Es ist $B\bar{A}_\mathfrak{p} = \bar{B}_{\mathfrak{P}_1} \oplus \cdots \oplus \bar{B}_{\mathfrak{P}_r}$. Daraus folgt

$$D_A(B)\bar{A}_\mathfrak{p} = D_{\bar{A}_\mathfrak{p}}(B\bar{A}_\mathfrak{p}) = D_{\bar{A}_\mathfrak{p}}(\bar{B}_{\mathfrak{P}_1}) \oplus \cdots \oplus D_{\bar{A}_\mathfrak{p}}(\bar{B}_{\mathfrak{P}_r})$$

Die erste Gleichheit folgt aus Proposition 2.3.6.

Damit ist $D_A(B)\bar{A}_\mathfrak{p}\bar{B}_{\mathfrak{P}_i} = D_A(B)\bar{B}_{\mathfrak{P}_i} = D_{\bar{A}_\mathfrak{p}}(\bar{B}_{\mathfrak{P}_i})$ indem wir die vorige Gleichung mit $\bar{B}_{\mathfrak{P}_i} \cong 0 \oplus \cdots \oplus \bar{B}_{\mathfrak{P}_i} \oplus \cdots \oplus 0$ multiplizieren. Durch Übergang zu den Inversen folgt die Beziehung für die Differente.

Die Gleichung für die Differenten folgt direkt aus Proposition 2.3.5 3.

Es sei weiter B/A und L/K wie oben und $x \in B$, so daß $A[x] \subseteq B$ mit $A[x] \otimes_A K = L$ ist. Weiter sei $g(x) = 0$ mit $g(T) \in A[T]$, monisch, das irreduzible Polynom von x bezüglich L/K.

Proposition 2.6.3. *Mit den obigen Bezeichnungen ist:*

1. $D(A[x]) = \frac{1}{g'(x)}A[x]$
2. $d(A[x]/A) = \mathrm{Norm}_{L|K}(g'(x))A$
3. Es ist $B = A[x]$ *genau dann, wenn* $\mathcal{D}_{B|A} = g'(x)B$

Beweis. 1. Ist $g(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ und

$$g(T) = (T - x)(b_0 + b_1T + \cdots + b_{n-1}T^{n-1})$$

so ist $(\frac{b_i}{g'(x)})_{i=0..n-1}$ die duale Basis zu $1, x, \ldots, x^{n-1}$, der Basis des freien A–Moduls $A[x]$. Weiterhin ist $b_{n-1} = 1$ und $b_{i-1} - xb_i = a_i$, also, per Induktion, b_i monisch in x vom Grad $n - 1 - i$.

Also ist

$$\sum_{i=0}^{n-1} A\frac{b_i}{g'(x)} = \sum_{i=0}^{n-1} A\frac{x^i}{g'(x)}$$

und damit $D(A[x]) = \frac{1}{g'(x)}A[x]$.

2. Es ist

$$d(A[x]/A) = [D(A[x]) : A[x]] = [A[x] : D(A[x])]^{-1} = [A[x] : \frac{1}{g'(x)}A[x]]^{-1} =$$
$$= \mathrm{Norm}_{L|K}(\frac{1}{g'(x)})^{-1}A = \mathrm{Norm}_{L|K}(g'(x))A \quad (2.50)$$

3. Ist $B = A[x]$, so ist $D(B) = D(A[x]) = \frac{1}{g'(x)}A[x] = \frac{1}{g'(x)}B$ und damit $\mathcal{D}_{B|A} = g'(x)B$. Sei umgekehrt $\mathcal{D}_{B|A} = g'(x)B$, so ist $\mathrm{Nm}_{B|A}(\mathcal{D}_{B|A}) = [B : g'(x)B] = \mathrm{Norm}_{L|K}(g'(x))A = d(A[x]/A)$. Nun ist nach Proposition 2.3.4 $d(A[x]/A) = d(B/A)[B : A[x]]^2$. Da $d(A[x]/A) = d(B/A)$ ist $[B : A[x]] = A$ und damit $B = A[x]$.

Proposition 2.6.4 (Differententürme). *Es sei A ein Dedekindring mit Quotientenkörper K und separablen Erweiterungen $F/L/K$ die zu Erweiterungen $C/B/A$ von Dedekindringen führen.*

Dann gilt

$$\mathcal{D}_{C|A} = \mathcal{D}_{C|B}\,\mathcal{D}_{B|A} \quad (2.51)$$
$$d(C/A) = d(B/A)^m\ \mathrm{Nm}_{B|A}\, d(C/B) \quad (2.52)$$

mit $m = [F : L]$.

Beweis.

2.7 Verzweigung I

Es seien $C \supseteq B \supseteq A$ Dedekindringe mit Quotientenkörpern $F/L/K$ und maximalen Idealen $\mathfrak{p}_3 \subseteq C$, $\mathfrak{p}_2 \subseteq B$ sowie $\mathfrak{p}_1 \subseteq A$.

Weiter sei $\mathfrak{p}_2 \cap A = \mathfrak{p}_1$ und $\mathfrak{p}_3 \cap B = \mathfrak{p}_2$.

Definition 2.7.1. *Mit den oben eingeführten Bezeichungen sei*

$$e(\mathfrak{p}_2/\mathfrak{p}_1) = e \text{ mit } ev_{\mathfrak{p}_1}(z) = v_{\mathfrak{p}_2}(z) \text{ für alle } z \in K^* \tag{2.53}$$

$$f(\mathfrak{p}_2/\mathfrak{p}_1) = [B/\mathfrak{p}_2 : A/\mathfrak{p}_1] \tag{2.54}$$

Anmerkung 2.7.1. Wir können e auch finden als $\mathfrak{p}_1 B = \mathfrak{p}_2^e \mathfrak{b}$, wobei $\mathfrak{b}$ zu $\mathfrak{p}_2$ teilerfremd ist.

Proposition 2.7.1. *Mit den oben eingeführten Bezeichnungen gilt:*

$$e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2)e(\mathfrak{p}_2/\mathfrak{p}_1) \tag{2.55}$$

$$f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2)f(\mathfrak{p}_2/\mathfrak{p}_1) \tag{2.56}$$

Es sei nun $\bar{K} = K_{\mathfrak{p}}$ die Komplettierung von K an einem maximalen Ideal $\mathfrak{p} \subseteq A$. Die Komplettierung von $A \supseteq \mathfrak{p}$ sei $\bar{A} \supseteq \bar{\mathfrak{p}}$. Es gilt $\bar{\mathfrak{p}} \cap A = \mathfrak{p}$.

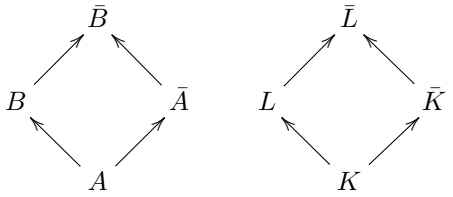
Proposition 2.7.2. *Es gilt mit den eben eingeführten Bezeichnungen*

$$e(\bar{\mathfrak{p}}/\mathfrak{p}) = 1 \tag{2.57}$$

$$f(\bar{\mathfrak{p}}/\mathfrak{p}) = 1 \tag{2.58}$$

Beweis. Es ist $\mathfrak{p}\bar{A} = \bar{\mathfrak{p}}$, also $e = 1$ und $\bar{A}/\bar{\mathfrak{p}} = A/\mathfrak{p}$, also $f = 1$.

Betrachte nun die Diagramme von Erweiterungen und Komplettierungen



(2.59)

Auf dem obigen Vorgehen entsprechende Weise sei $\bar{L} = L_{\mathfrak{p}_2}$, $\bar{B}$, $\bar{\mathfrak{p}}_2 \subseteq \bar{B}$ definiert. Es gilt dann:

Proposition 2.7.3. *Mit den oben eingeführten Bezeichnungen gilt:*

$$e(\bar{\mathfrak{p}}_2/\bar{\mathfrak{p}}_1) = e(\mathfrak{p}_2/\mathfrak{p}_1) \tag{2.60}$$

$$f(\bar{\mathfrak{p}}_2/\bar{\mathfrak{p}}_1) = f(\mathfrak{p}_2/\mathfrak{p}_1) \tag{2.61}$$

Es sei nun L/K separabel und K vollständig bezüglich der diskreten Bewertung $v_K = v_\mathfrak{p}$ für $\mathfrak{p} \subseteq A$, maximales Ideal des DBR A. Dann ist $B \subseteq L$ diskreter Bewertungsring mit Bewertung $v_L = v_\mathfrak{P}$ für $\mathfrak{P} \subseteq B$, maximales Ideal des DBR B.

Damit haben wir die Diagramme (mit $U_K = A^*$ und $U_L = B^*$):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \cdot e} & & \\ 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \end{array} \tag{2.62}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Norm}_{L|K}} & & \downarrow{\scriptstyle \cdot f} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \end{array} \tag{2.63}$$

Das untere Diagramm folgt aus $(\mathrm{Norm}_{L|K} \circ j)(z) = z^{[L:K]}$ für alle $z \in K^*$ und aus $ef = [L : K]$ sowie $\mathrm{Norm}_{L|K}(U_L) \subseteq U_K$.

Es ergibt sich daraus auch die Beziehung

$$\mathrm{Nm}_{B|A}(\mathfrak{P}) = \mathfrak{p}^f \tag{2.64}$$

2.8 Verzweigung II

Definition 2.8.1. *Es sei S eine endlichdimensionale k–Algebra und $z \in S$. Weiter sei e_i eine k–Basis von S und $M_z = |a_{ij}|$ die Darstellungsmatrix von $w \mapsto zw$, also $ze_i = \sum_j a_{ij} e_j$.*

Dann sei

$$\mathrm{Tr}_{S|k}(z) = \mathrm{Tr}\, M_z \tag{2.65}$$

Lemma 2.8.1. *Es sei S eine endlichdimensionale k–Algebra mit Nilradikal $N = N_S \subseteq S$. Weiter sei*

$$S \supsetneq N \supsetneq N^2 \supsetneq \cdots \supsetneq N^{e-1} \supsetneq N^e = (0)$$

und $S/N = R$ sowie $N^i/N^{i+1} \cong S/N = R$.

Es gilt dann

$$\mathrm{Tr}_{S/k}(z) = e\, \mathrm{Tr}_{R/k}(\bar{z}) \tag{2.66}$$

mit $z \mapsto \bar{z}$ aus $S \to S/N = R$.

Es sei im folgenden wieder K vollständig bezüglich v_K und L/K separabel, sowie v_L die eindeutige Bewertung auf L, die von v_K induziert wird. Weiter seien $(A, \mathfrak{p}, k) \subseteq (B, \mathfrak{P}, k_L)$ die Bewertungsringe in $K \subseteq L$, ihre maximalen Ideale und ihre Restkörper.

Lemma 2.8.2. *Für $b \in B$ gilt*

$$\overline{\mathrm{Tr}_{L|K}(b)} = e\ \mathrm{Tr}_{k_L|k}(\bar{b}) \tag{2.67}$$

$$\overline{\mathrm{Norm}_{L|K}(b)} = \mathrm{Norm}_{k_L|k}(\bar{b})^e \tag{2.68}$$

mit $b \mapsto \bar{b}$ gegeben durch $B \mapsto B/\mathfrak{P}$.

Proposition 2.8.1. *Es sei mit den obigen Bezeichnungen $\mathcal{D} = \mathcal{D}_{B|A}$. Dann gilt*

$$v_L(\mathcal{D}) \geqslant e - 1 \tag{2.69}$$

Definition 2.8.2. *Wir nennen, mit den obigen Bezeichnungen, L/K* unverzweigt*, falls*

i) $e(L/K) = e(\mathfrak{P}/\mathfrak{p}) = 1$.
ii) k_L/k *separabel.*

Proposition 2.8.2. *Es ist äquivalent*

a) L/K *ist unverzweigt.*
b) Für die Differente gilt: $\mathcal{D}_{B|A} = B$.
c) Für die Diskriminante gilt: $d(B/A) = A$

Definition 2.8.3. *Wir nennen, mit den obigen Bezeichnungen, L/K* zahm verzweigt*, falls*

i) $\mathrm{char}\, k \nmid e$.
ii) k_L/k *separabel.*

Proposition 2.8.3. *Es ist äquivalent*

a) L/K *ist zahm verzweigt.*
b) $\mathrm{Tr}_{L|K}(B) = A$
c) $v_L(\mathcal{D}_{B|A}) = e - 1$.

2.9 Komplettierungen

Lemma 2.9.1 (Henselsches Lemma). *Es sei K ein mit $|\cdot|$ nichtarchimedisch bewerteter Körper. Dieser sei bezüglich $|\cdot|$ vollständig.*

Es sei

$$A = \{x \in K \mid |x| \leqslant 1\}$$

der zugehörige Bewertungsring. Weiter sei $f(X) \in A[X]$ ein Polynom.

Es sei $\alpha_0 \in A$ und es gelte

$$\left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1 \tag{2.70}$$

Dann existiert ein $\alpha \in A$ mit $|\alpha - \alpha_0| < 1$ und $f(\alpha) = 0$.

Beweis. Es sei $\gamma_0 = \sup_{x\in\mathfrak{m}_A}|x|$.

Man definiert die Folge

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})} \tag{2.71}$$

Induktiv weist man nach

i) Es ist $|\alpha_n| \leqslant 1$.
ii) Es ist $|(\alpha_n - \alpha_{n-1})/f'(\alpha_{n-1})| < 1$

Beide Aussagen sind für $n = 1$ richtig, wie man sich mit Hilfe der Voraussetzungen kurz überlegt. Um ii) induktiv zu zeigen rechnen wir aus

$$\begin{aligned}\frac{\alpha_{n+1}-\alpha_n}{f'(\alpha_n)} &= -\frac{f(\alpha_n)}{f'(\alpha_n)^2} = \\ &= -\frac{f(\alpha_{n-1}) + f'(\alpha_{n-1})(\alpha_n - \alpha_{n-1}) + \eta(\alpha_n - \alpha_{n-1})^2}{(f'(\alpha_{n-1}) + \eta'(\alpha_n - \alpha_{n-1}))^2} = \\ &= -\frac{\eta(\alpha_n - \alpha_{n-1})^2}{f'(\alpha_{n-1})^2(1 + \eta'((\alpha_n - \alpha_{n-1})/f'(\alpha_{n-1})))^2}\end{aligned} \tag{2.72}$$

Da $|(\alpha_n - \alpha_{n-1})/f'(\alpha_{n-1})| < 1$, nach Induktionsannahme, ist damit der Beweis von ii) erbracht. Es gilt sogar

$$\left|\frac{\alpha_{n+1}-\alpha_n}{f'(\alpha_n)}\right| \leqslant \left|\left(\frac{\alpha_n - \alpha_{n-1}}{f'(\alpha_{n-1})}\right)^2\right| \tag{2.73}$$

also

$$\left|\frac{\alpha_{n+1}-\alpha_n}{f'(\alpha_n)}\right| \leqslant c^{2^n} \tag{2.74}$$

mit $c = |(\alpha_1 - \alpha_0)/f'(\alpha_0)| < 1$. Wir rechnen weiter aus

$$\begin{aligned}\alpha_{n+1} - \alpha_n &= -\frac{f(\alpha_n)}{f'(\alpha_n)} = \\ &= -\frac{f(\alpha_{n-1}) + f'(\alpha_{n-1})(\alpha_n - \alpha_{n-1}) + \eta(\alpha_n - \alpha_{n-1})^2}{f'(\alpha_{n-1}) + \eta'(\alpha_n - \alpha_{n-1})} = \\ &= -\frac{\eta(\alpha_n - \alpha_{n-1})^2}{f'(\alpha_{n-1})(1 + \eta'(\alpha_n - \alpha_{n-1})/f'(\alpha_{n-1}))}\end{aligned} \tag{2.75}$$

Also ist offenbar $|\alpha_{n+1} - \alpha_n| \leqslant c^{2^{n-1}}|\alpha_n - \alpha_{n-1}|$ mit dem $c < 1$ von oben. Also ist α_n eine Cauchy–Folge mit Grenzwert α und $|\alpha - \alpha_0| < 1$. Es gilt dann auch $f(\alpha) = 0$. Man beachte die durch den Faktor c^{2^n} erzwungene besonders schnelle Konvergenz der gewählten Iteration.

Proposition 2.9.1 (Krasners Lemma). *Es sei K ein bezüglich $|\cdot|$ vollständiger, nichtarchimedisch bewerteter Körper. Weiter seien α, β zwei Elemente aus dem algebraischen Abschluß $\bar{K}$ und α separabel über $K(\beta)$. Ist dann*

$$|\beta - \alpha| < |\sigma(\alpha) - \alpha| \tag{2.76}$$

für alle Einbettungen $\sigma : K(\alpha) \to \bar{K}$ und $\sigma \neq \mathrm{id}$, so ist $K(\alpha) \subseteq K(\beta)$.

Beweis. Für jeden Automorphismus $\tau \in \mathrm{Aut}_K(\bar{K})$ gilt $|\tau x| = |x|$ für alle $x \in \bar{K}$, denn sowohl $x \mapsto |x|$ als auch $x \mapsto |\tau x|$ sind Fortsetzungen von $|\cdot|_K$ und stimmen daher überein, da $\bar{K}$ ein vollständiger Körper über K ist.

Ist nun $K(\alpha) \not\subseteq K(\beta)$, so gibt es einen Automorphismus τ von $K(\alpha, \beta)$, der β festläßt und für den $\tau(\alpha) \neq \alpha$ ist. Es ist dann $\tau(\beta - \alpha) = \beta - \sigma(\alpha)$ und somit

$$(*) \quad |\beta - \alpha| = |\tau(\beta - \alpha)| = |\beta - \sigma(\alpha)|$$

Andererseits ist

$$|\alpha - \sigma(\alpha)| \leqslant \max(|\beta - \alpha|, |\beta - \sigma(\alpha)|)$$

Wegen $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$ ist dann $|\beta - \alpha| < |\alpha - \sigma(\alpha)| \leqslant |\beta - \sigma(\alpha)|$ im Widerspruch zu $(*)$.

3

Zyklotomische Körpererweiterungen

3.1 Kreisteilungskörper

Die Menge $\{\zeta \in \bar{\mathbb{Q}} \mid \zeta^n = 1\}$ ist mit der Multiplikation als Verknüpfung eine Gruppe und als endliche Untergruppe eines Körpers zyklisch. Einer ihrer Erzeuger sei ausgewählt und mit ζ_n bezeichnet.

Der Körper $\mathbb{Q}(\zeta_n)$ ist dann eine separable und normale Körpererweiterung von $\mathbb{Q}$, also galoissch. Normal ist er nämlich, weil für jede Einbettung $\sigma : \mathbb{Q}(\zeta_n) \to \bar{\mathbb{Q}}$ die Beziehung

$$\zeta_n^\sigma = \zeta_n^a \text{ mit } a = a_\sigma \text{ und } (a, n) = 1 \tag{3.1}$$

gilt. Damit faktorisiert σ also durch $\mathbb{Q}(\zeta_n)$ und $\mathbb{Q}(\zeta_n)$ ist normal über $\mathbb{Q}$.

Weiterhin ist offensichtlich die Zuordnung

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*, \quad \sigma \mapsto a_\sigma$$

ein Monomorphismus. Wir werden zeigen, daß sie auch ein Isomorphismus ist.

3.2 Kummertheorie

Die *Kummertheorie* beschreibt die abelschen Erweiterungen vom Exponent m von Körpern k, die die m–ten Einheitswurzeln enthalten.

Sei k ein Körper, der die m–ten Einheitswurzeln μ_m enthält und B^* eine Untergruppe von k^* mit $(k^*)^m \subset B^*$. Der Körper $k((B^*)^{1/m})$ sei mit l_{B^*} abgekürzt. Es sei $G = \mathrm{Gal}(l_{B^*}/k)$. Dann existiert eine Paarung

$$\psi : G \times B^* \to \mu_m$$

die folgendermassen gegeben ist: Wähle für ein $b \in B^*$ ein $a \in l_{B^*}$ mit $a^m = b$ und setze

$$\psi(\sigma, b) = a^\sigma / a$$

Das ist wohldefiniert, da für ein alternatives a' mit $a'^m = b$ gelten würde, daß $a' = \zeta\, a$ mit $\zeta \in \mu_m$.

Lemma 3.2.1. *Die Abbildung ψ ist links injektiv und hat rechts den Kern $(k^*)^m$.*

Proposition 3.2.1. *Die Abbildung*

$$B^* \to k(B^{*1/m})$$

ist eine Bijektion von den multiplikativen Untergruppen $B^* \subset k^*$ mit $(k^*)^m \subset B^*$ in die abelschen Erweiterungen l/k mit Galoisgruppen $\mathrm{Gal}(l/k)$, die von m annulliert werden.

Die Umkehrabbildung ist

$$l \to (l^*)^m \cap k$$

4

Endlichkeitssätze

4.1 Die Produktformel

Definition 4.1.1. *Es sei K ein Körper und Σ_K die Menge seiner Stellen. Ist dann für jedes $x \in K$ die Anzahl der $v \in \Sigma_K$ mit $\|x\|_v \neq 1$ endlich und außerdem*

$$1 = \prod_{v \in \Sigma_K} \|x\|_v \tag{4.1}$$

so sagen wir, daß in K die Produktformel gilt*.*

Proposition 4.1.1. *In $\mathbb{Q}$ mit den Bewertungen $v_p = |\cdot|_p$ und $v_\infty = |\cdot|$ gilt die Produktformel.*

Proposition 4.1.2. *Es sei $K/\mathbb{Q}$ ein Zahlkörper und $\alpha \in K$. Dann ist $\|\alpha\|_w = 1$ für fast alle $w \in \Sigma_K$.*

Beweis. Es sei $\alpha \in K$ gegeben. Dann ist

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

mit $a_i \in \mathbb{Q}$. Für fast alle $w \in \Sigma_K$ ist $\|a_i\|_w = 1$ für alle i und $\|\cdot\|_w$ nicht–archimedisch.

Wir zeigen, daß dann auch $\|\alpha\| = \|\alpha\|_w \geqslant 1$ sein muß. Wäre nämlich $\|\alpha\| < 1$, so wäre

$$\begin{aligned} 1 = \|a_0\| &= \|\alpha\|\|a_1 + \alpha(a_2 + \alpha(a_3 + \cdots + \alpha(a_{n-1} + \alpha)\cdots))\| = \\ &= \|\alpha\| \max\left(\|a_1\|, \|\alpha\|(\max(\|a_2\|, \cdots, \max(\|a_{n-1}\|, \|\alpha\|)\cdots)\right) \leqslant \|\alpha\| < 1 \end{aligned}$$

Durch Betrachtung von $1/\alpha$ erhält man durch dieselbe Überlegung $\|1/\alpha\|_w \geqslant 1$ für fast alle $w \in \Sigma_K$. Also schließlich $\|\alpha\|_w = 1$ für fast alle $w \in \Sigma_K$.

Lemma 4.1.1. *Es sei $L/K/\mathbb{Q}$ ein Turm von endlichen Erweiterungen von Zahlkörpern. Weiter sei $w \in \Sigma_L$ und $v \in \Sigma_K$ sowie $v_0 \in \Sigma_\mathbb{Q}$ mit $w|v|v_0$.*

Dann ist für $\alpha \in L_w$

$$\|\mathrm{Norm}_{L_w|K_v}(\alpha)\|_v = \|\alpha\|_w \tag{4.2}$$

Beweis. Es gilt

$$\|\mathrm{Norm}_{L_w|K_v}(\alpha)\|_v = |\mathrm{Norm}_{L_w|K_v}(\alpha)|_v^{[K_v:\mathbb{Q}_{v_0}]} = \\ = |\alpha|_w^{[L_w:K_v][K_v:\mathbb{Q}_{v_0}]} = |\alpha|_w^{[L_w:\mathbb{Q}_{v_0}]} = \|\alpha\|_w \quad (4.3)$$

Theorem 4.1.1. *Es sei $L \supseteq K$ ein Zahlkörper mit der Menge seiner Stellen Σ_L. Weiter sei $\alpha \in L$ und K ein Körper in dem die Produktformel gilt. Dann ist*

$$1 = \prod_{w \in \Sigma_L} \|\alpha\|_w \quad (4.4)$$

Beweis. Es ist

$$1 = \prod_{v \in \Sigma_K} \|\mathrm{Norm}_{L|K}(\alpha)\|_v$$

und wegen

$$\mathrm{Norm}_{L|K}(\alpha) = \prod_{w|v} \mathrm{Norm}_{L_w|K_v}(\alpha)$$

sowie $\|\mathrm{Norm}_{L_w|K_v}(\alpha)\|_v = \|\alpha\|_w$ auch

$$1 = \prod_{v \in \Sigma_K} \prod_{w|v} \|\alpha\|_w = \prod_{w \in \Sigma_L} \|\alpha\|_w$$

Korollar 4.1.1. *In jedem Zahlkörper $K/\mathbb{Q}$ gilt die Produktformel.*

4.2 Die Endlichkeit der Klassenzahl

Es sei $K/\mathbb{Q}$ ein algebraischer Zahlkörper und $\mathcal{O}_K = A$ sein Ganzheitsring. Es sei, wie oben eingeführt, I_A die multiplikative Gruppe der gebrochenen Ideale mit der kanonischen Einbettung $K^* \hookrightarrow I_A$, und der exakten Sequenz:

$$1 \to K^* \to I_A \to \mathrm{Cl}_A \to 1$$

Es gilt dann

Theorem 4.2.1 (Dirichlet). *Die Idealklassengruppe Cl_A ist endlich.*

Beweis. Es sei $\mathfrak{a} \subseteq A$ ein ganzes Ideal mit Norm $\mathrm{Nm}(\mathfrak{a}) = N$. Weiter sei $A = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ mit einer $\mathbb{Z}$–Basis (ω_i).

Betrachte die Teilmenge

$$L = a_1\omega_1 + \cdots + a_n\omega_n$$

mit $1 \leqslant a_i \leqslant 2(\mathrm{Nm}(\mathfrak{a}))^{1/n} + 1$ und die Abbildung

$$\phi : L \to A/\mathfrak{a}$$

Die Mächtigkeit links ist größer $2^n \,\mathrm{Nm}(\mathfrak{a})$, die Mächtigkeit rechts ist $\mathrm{Nm}(\mathfrak{a})$. Also gibt es $x, y \in L$ mit $\phi(x) = \phi(y)$ und $x \neq y$, also $0 \neq x - y \in \mathfrak{a}$. Nenne $\xi = x - y$. Da $\xi \in \mathfrak{a}$ folgt $\xi\mathfrak{a}^{-1} = \mathfrak{b} \subseteq A$.

Weiter ist

$$|\mathrm{Norm}_{L|\mathbb{Q}}(\xi)| = \prod_{i=1}^{n} |(b_1\omega_1 + \cdots + b_n\omega_n)^{\sigma_i}| \leqslant$$

$$\leqslant \prod_{i=1}^{n} |b_1||\omega_1^{\sigma_i}| + \cdots + |b_n||\omega_n^{\sigma_i}| \leqslant C\,\mathrm{Nm}(\mathfrak{a}) \quad (4.5)$$

da ja $b_i \leqslant 2(\mathrm{Nm}(\mathfrak{a}))^{1/n} + 1 \leqslant C'(\mathrm{Nm}\,\mathfrak{a})^{1/n}$ ist.

Also ist

$$|\mathrm{Nm}(\xi\mathfrak{a}^{-1})| = |\mathrm{Norm}_{L|\mathbb{Q}}(\xi)||\mathrm{Nm}\,\mathfrak{a}^{-1}| \leqslant C|\mathrm{Nm}\,\mathfrak{a}||\mathrm{Nm}\,\mathfrak{a}^{-1}| \leqslant C \quad (4.6)$$

Jedes Ideal $I = \mathfrak{a}^{-1}$ ist also äquivalent zu einem ganzen Ideal $\mathfrak{b}$ mit $\mathrm{Nm}(\mathfrak{b}) \leqslant C$. Davon gibt es aber nur endlich viele.

Sei nun J ein beliebiges gebrochenes Ideal. Dann ist $dJ = \mathfrak{a}$ mit einem ganzen Ideal $\mathfrak{a}$ und $d \in A$. Also ist $J^{-1} = d\mathfrak{a}^{-1}$. Also ist J^{-1} auch äquivalent zu $\mathfrak{a}^{-1}$ und damit äquivalent zu einem von höchstens endlich vielen ganzen Idealen. Da jedes gebrochene Ideal als J^{-1} geschrieben werden kann, ist der Satz damit gezeigt.

Weiter unten wird ein alternativer Beweis mit Hilfe des folgenden Lemmas gegeben.

Lemma 4.2.1 (Minkowski). *Es sei $\Gamma \subseteq \mathbb{R}^n$ ein Gitter mit Kovolumen d und $X \subseteq \mathbb{R}^n$ konvex und punktsymmetrisch zu $0 \in X$ und $\mathrm{vol}(X) > 2^n\,d$. Dann existiert ein $x \in X \cap \Gamma$ mit $x \neq 0$.*

Es sei $X(\delta)$ die Menge der $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ mit $\|x\| \leqslant \delta$ für eine bestimmte Norm $\|\cdot\|$ auf $\mathbb{R}^n$.

Weiter sei $F_n = \mathrm{vol}(X(1))$ und somit $\mathrm{vol}(X(\delta)) = \delta^n\,F_n$.

Lemma 4.2.2. *Der Ausdruck*

$$|x_1| \cdot \cdots \cdot |x_s|\left(x_{s+1}^2 + x_{s+2}^2\right) \cdot \cdots \cdot \left(x_{s+2\,t-1}^2 + x_{s+2\,t}^2\right)$$

nimmt auf $X(\delta)$ das Maximum $C_n\delta^n$ mit einer geeigneten Konstante C_n an.

Beweis. C_n ist das Maximum des obigen stetigen Ausdrucks auf dem Kompaktum $X(1)$.

Man betrachte nun für K die Einbettung $\Phi : K \to \mathbb{R}^n$ mit

$$\Phi(x) = (\sigma_1(x), \ldots, \sigma_s(x), \Re\tau_1(x), \Im\tau_1(x), \ldots, \Re\tau_t(x), \Im\tau_t(x))$$

wobei die σ_i die rellen Einbettungen und die τ_j die wesentlich verschiedenen komplexen Einbettungen sind. Da

$$|\mathrm{Norm}_{K:\mathbb{Q}}(x)| = |\sigma_1(x)| \cdots |\sigma_s(x)||\tau_1(x)|^2 \cdots |\tau_t(x)|^2,$$

gilt

Korollar 4.2.1. *Es sei $X(\delta)$ wie oben und ein Φ wie oben gegeben. Dann ist $\mathrm{Norm}_{K:\mathbb{Q}}(x) \leqslant C_n\delta^n$ für alle $x \in X(\delta) \cap \Phi(K)$.*

Weiter haben wir

Lemma 4.2.3. *Es sei $\mathfrak{a} \subseteq A$ ein ganzes Ideal und* $\mathrm{Norm}(\mathfrak{a}) = [A : \mathfrak{a}]$ *seine Norm.*

Dann ist

$$\mathrm{vol}(\mathbb{R}^n/\Phi(\mathfrak{a})) = \mathrm{Norm}(\mathfrak{a})\ \mathrm{vol}(\mathbb{R}^n/\Phi(A)) \tag{4.7}$$

Es gilt sogar für jedes gebrochene Ideal $I \subseteq K$:

$$\mathrm{vol}(\mathbb{R}^n/\Phi(I)) = \mathrm{Norm}(I)\ \mathrm{vol}(\mathbb{R}^n/\Phi(A)) \tag{4.8}$$

Beweis. Die erste Gleichung gilt, weil im Fundamentalparellotop von $\mathfrak{a}$ dasjenige von A genau $[A : \mathfrak{a}]$–mal aufgeht. Für I existiert ein $a \in A$ mit $aI = \mathfrak{a}$ mit einem ganzen Ideal $\mathfrak{a}$. Daraus folgt die zweite Gleichung wegen $\mathrm{vol}(\mathbb{R}^n/\Gamma)a^n = \mathrm{vol}(\mathbb{R}^n/(a\,\Gamma))$.

Wähle nun ein beliebiges ganzes Ideal $\mathfrak{a} \subseteq A$ und betrachte $\mathfrak{a}^{-1}$. Dann ist das Kovolumen

$$\mathrm{vol}(\mathbb{R}^n/\Phi(\mathfrak{a}^{-1})) = \mathrm{Norm}(\mathfrak{a}^{-1})\, 2^{-t} \sqrt{|d_{K:\mathbb{Q}}|} = \beta \tag{4.9}$$

Um dies einzusehen beachte man, daß

$$\begin{aligned}\sqrt{|d_{K:\mathbb{Q}}|} &= \begin{vmatrix} \sigma_1(a_1) & \dots & \sigma_s(a_1) & \tau_1(a_1) & \bar\tau_1(a_1) & \dots & \tau_t(a_1) & \bar\tau_t(a_1) \\ \dots & & & & & & & \dots \\ \sigma_1(a_n) & \dots & \sigma_s(a_n) & \tau_1(a_n) & \bar\tau_1(a_n) & \dots & \tau_t(a_n) & \bar\tau_t(a_n) \end{vmatrix} \\ &= \det\left(\begin{pmatrix} \sigma_1(a_1) & \dots & \sigma_s(a_1) & \Re\tau_1(a_1) & \Im\tau_1(a_1) & \dots & \Re\tau_t(a_1) & \Im\tau_t(a_1) \\ \dots & & & & & & & \dots \\ \sigma_1(a_n) & \dots & \sigma_s(a_n) & \Re\tau_1(a_n) & \Im\tau_1(a_n) & \dots & \Re\tau_t(a_n) & \Im\tau_t(a_n) \end{pmatrix} \cdot M \right)\end{aligned}$$

wobei $A = \mathbb{Z}\,a_1 + \dots + \mathbb{Z}\,a_n$ mit $a_i \in A$. Die Matrix M ist eine $n \times n$–Matrix die aus s Einsen auf der Hauptdiagonalen und t Blöcken der Form $\left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right)$ entlang der Hauptdiagonalen besteht. Es ist also $|\det M| = 2^t$ und damit jedenfalls

$$\mathrm{vol}(\mathbb{R}^n/\Phi(A)) = 2^{-t} \sqrt{|d_{K:\mathbb{Q}}|}.$$

Damit und wegen vorigem Lemma ist die Behauptung nachgewiesen.

Man wählt nun δ so, daß $\mathrm{vol}(X(\delta)) = F_n\,\delta^n = 2^n\,\beta$. Damit enthält $X(\delta)$ in seinem Inneren einen Punkt $x \in \mathfrak{a}^{-1}$ und $x \neq 0$.

Für diesen ist dann auch

$$\begin{aligned}|\mathrm{Norm}(x)| \leqslant C_n\delta^n = C_n\, 2^n\, \frac{\beta}{F_n} = \\ = \frac{C_n}{F_n}\, 2^n\, 2^{-t}\, \mathrm{Norm}(\mathfrak{a}^{-1}) \sqrt{|d_{K:\mathbb{Q}}|}\end{aligned}$$

Da $A\,x \subseteq \mathfrak{a}^{-1}$ ist $x\,\mathfrak{a} \subseteq A$ ein ganzes Ideal mit

$$|\mathrm{Norm}(x)|\mathrm{Norm}(\mathfrak{a}) \leqslant \frac{C_n}{F_n}\, 2^n\, 2^{-t} \sqrt{|d_{K:\mathbb{Q}}|}.$$

Es gibt also eine absolute Konstante C_K, so daß jedes ganze Ideal $\mathfrak{a}$ zu einem ganzen Ideal $\mathfrak{a}' = x\,\mathfrak{a}$ in Cl_A äquivalent ist, für das $\mathrm{Norm}(\mathfrak{a}') < C_K$ gilt. Von diesen $\mathfrak{a}'$ kann es aber nur endlich viele geben.

Wir wählen nun eine konkrete Norm $\|\cdot\|_1$ auf $\mathbb{R}^n$, nämlich

$$\|(x_1,\ldots,x_n)\|_1 = |x_1|+\cdots+|x_s|+2\sqrt{x_{s+1}^2+x_{s+2}^2}+\cdots+2\sqrt{x_{s+2t-1}^2+x_{s+2t}^2}. \quad (4.10)$$

Unter der obigen Abbildung $\Phi : K \to \mathbb{R}^n$ ist dann

$$\|\Phi(\alpha)\|_1 = |\sigma_1(\alpha)|+\cdots+|\sigma_s(\alpha)|+|\tau_1(\alpha)|+|\bar{\tau}_1(\alpha)|+\cdots+|\tau_t(\alpha)|+|\bar{\tau}_t(\alpha)| \quad (4.11)$$

Der oben beschriebene Wert C_n ist dann das Maximum von

$$|\mathrm{Norm}_{K:\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)|\cdot\cdots\cdot|\sigma_s(\alpha)||\tau_1(\alpha)|^2\cdot\cdots\cdot|\tau_t(\alpha)|^2$$

auf $\|\Phi(\alpha)\|_1 \leqslant 1$.

Wir suchen also das Maximum von $w_1\cdot\cdots\cdot w_n$ auf $w_1+\cdots+w_n \leqslant 1$ für $w_i \geqslant 0$. Dabei ist

$$w_1 = |\sigma_1(\alpha)|,\ldots,w_s = |\sigma_s(\alpha)|, \quad w_{s+1} = |\tau_1(\alpha)|, w_{s+2} = |\bar{\tau}_1(\alpha)|,\ldots \quad \ldots, w_{s+2t-1} = |\tau_t(\alpha)|, w_{s+2t} = |\bar{\tau}_t(\alpha)| \quad (4.12)$$

Dieses Maximum ist

$$C_n = \frac{1}{n^n} \quad (4.13)$$

Dies folgt aus dem Lemma

Lemma 4.2.4. *Es ist der arithmetische Mittelwert niemals kleiner als der geometrische Mittelwert für $w_i \geqslant 0$:*

$$(w_1\cdot\cdots\cdot w_n)^{1/n} \leqslant \frac{w_1+\cdots+w_n}{n} \quad (4.14)$$

Es bleibt, noch F_n, also das Volumen von $\|x\|_1 \leqslant 1$ mit $x \in \mathbb{R}^n$, zu bestimmen.

Wir nennen

$$F_{n-i} = \mathrm{vol}_{\mathbb{R}^{n-i}}(\{x \in 0^i \times \mathbb{R}^{n-i} \mid \|x\|_1 \leqslant 1\}) \quad (4.15)$$

Es ist dann für $i > s$ immer

$$F_j = 2\int_0^1 (1-u)^{j-1}du\,F_{j-1} = 2/j\,F_{j-1} \quad (4.16)$$

Also ist schon einmal

$$F_n = \frac{2^s}{n(n-1)\cdot\dots\cdot(n-s+1)} F_{n-s} = \frac{2^s}{n(n-1)\cdot\dots\cdot(2t+1)} F_{n-s} \quad (4.17)$$

Wir nennen nun

$$G_{2t-2j} = \mathrm{vol}_{\mathbb{R}^{2t-2j}}(\{x \in 0^s \times 0^{2j} \times \mathbb{R}^{2t-2j} \mid 1/2\|x\|_1 \leqslant 1\}) \quad (4.18)$$

Es ist dann

$$G_k = 2\,\pi \int_0^1 (1-u)^{k-2}\, u\, du\, G_{k-2} = \frac{2\,\pi}{k(k-1)} G_{k-2} \quad (4.19)$$

Damit ist $G_{2t} = 2^t \pi^t / ((2t)!)$

Nun ist aber

$$F_{n-s} = \frac{G_{2t}}{2^{2t}} = \frac{\pi^t}{2^t (2t)!}.$$

Also ist

$$F_n = \frac{2^s \pi^t}{2^t n!} = \frac{2^{s-t}\pi^t}{n!} \quad (4.20)$$

Wir erinnern uns an die Ungleichung

$$\mathrm{Norm}(\mathfrak{a}') \leqslant \frac{C_n}{F_n}\, 2^n\, 2^{-t} \sqrt{|d_{K:\mathbb{Q}}|}.$$

Setzt man ein, so folgt

$$\mathrm{Norm}(\mathfrak{a}') \leqslant \frac{n!\, 2^{s+t}}{n^n\, 2^{s-t}\, \pi^t} \sqrt{|d_{K:\mathbb{Q}}|} = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^t \sqrt{|d_{K:\mathbb{Q}}|} \quad (4.21)$$

Der Ausdruck

$$C_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^t, \quad (4.22)$$

der die vorige Ungleichung regiert, ist die berühmte *Minkowskische Konstante*.

4.3 Divisoren und Parallelotope

4.3.1 Definition

Es sei $K/\mathbb{Q}$ ein algebraischer Zahlkörper und Σ_K die Menge seiner Stellen.

Wir definieren

Definition 4.3.1. *Es sei $c : \Sigma_K \to \mathbb{R}$ eine Abbildung mit*

i) $c_v = c(v) > 0$ *für alle* $v \in \Sigma_K$.
ii) $c_v = 1$ *für fast alle* $v \in \Sigma_K$.
iii) $c_v = |a_v|_v$ *für alle nicht–archimedischen v mit einem geeigneten* $a_v \in K_v$.

Dann nennen wir c einen Divisor oder Σ_K–Divisor von K.

Wir schreiben auch c_v für $c(v)$ und definieren

$$\|c\|_v = c_v^{n_v} \tag{4.23}$$

$$\|c\| = \prod_{v\in\Sigma_K} \|c\|_v \tag{4.24}$$

Dabei stehe n_v für $[K_v : \mathbb{Q}_w]$ wobei $w \in \Sigma_{\mathbb{Q}}$ die durch v auf $\mathbb{Q}$ induzierte Bewertung ist.

Für ein $\alpha \in K^*$ sei αc durch $(\alpha c)(v) = |\alpha|_v c_v$ definiert. Es ist dann $\|\alpha c\| = \|c\|$ wegen $\prod_v \|\alpha\| = \prod_v |\alpha|_v^{n_v} = 1$.

Definition 4.3.2. *Es sei c ein Σ_K–Divisor. Dann heiße die Menge*

$$L(c) = \{x \in K \mid |x|_v \leqslant c_v\} \tag{4.25}$$

*ein c–*Parallelotop oder einfach Parallelotop*.*

Es ist dann auch $\|x\|_v \leqslant \|c\|_v$ für alle $x \in L(c)$.

Lemma 4.3.1. *Für ein $\alpha \in K^*$ definiert $x \mapsto \alpha x$ eine Bijektion von $L(c) \to L(\alpha c)$.*

Lemma 4.3.2. *Es sei $x \in L(c)$. Dann ist $|x|_v > C(c)$ mit einer Konstanten $C(c)$ die nur von c abhängt.*

Beweis. Es ist

$$\|x\|_v = \frac{1}{\prod_{v'\neq v}\|x\|_{v'}} \geqslant \frac{1}{\prod_{v'\neq v}\|c\|_{v'}} = \frac{\|c\|_v}{\|c\|} \tag{4.26}$$

und $|x|_v = (\|x\|_v)^{1/n_v}$.

Proposition 4.3.1. *Die Kardinalität $|L(c)|$ ist endlich.*

Beweis. Es seien $v_1, \ldots, v_r \nmid \infty$ die nicht–archimedischen Stellen mit $c_{v_i} > 1$. Wähle dann ein $\alpha \in \mathfrak{O}_K$ mit $\alpha \equiv 0 \mod \mathfrak{p}_{v_i}^{m_i}$ mit geeigneten $m_i \gg 0$, so daß $|\alpha|_{v_i} c_{v_i} \leqslant 1$ ist. Ersetze dann c durch αc, was wegen $L(c) \cong L(\alpha c)$ erlaubt ist.

Wir nehmen also an, daß $c_v \leqslant 1$ für alle $v \nmid \infty$. Damit ist jedes $x \in L(c)$ auch in $\mathfrak{O}_K$. Weiter ist $|x|_v < c_v$ für alle $v \mid \infty$. Da die $x \in \mathfrak{O}_K$ ein Gitter in $\prod_{v|\infty} K_v$ bilden, ist die Endlichkeit von $L(c)$ klar.

Anmerkung 4.3.1. Wir schreiben auch $\lambda(c)$ für die Kardinalität $|L(c)|$.

4.3.2 Parallelotopungleichungen

Es sei im folgenden $K/\mathbb{Q}$ ein Zahlkörper mit $[K : \mathbb{Q}] = n$ mit Ganzheitsring $A = \mathfrak{O}_K$.

Definition 4.3.3. *Es sei c ein Σ_K–Divisor und $L(c)$ ein Parallelotop. Dann gilt*

$$C_1\|c\| \leqslant \lambda(c) \leqslant C_2 \max(1, \|c\|) \tag{4.27}$$

mit Konstanten $C_1, C_2 > 0$, die nur von K abhängen.

Beweis. Wir beginnen mit der linken Ungleichung.

Wir wählen ein $\lambda \in K$, so daß für $c' = \lambda c$ die Beziehungen

$$2nc_0 \leqslant c'_v \leqslant 4nc_0 \tag{4.28}$$

für alle $v \mid \infty$ gilt, mit einem unten festgestzten $c_0 > 0$, das nur von K abhängt. Dies ist aufgrund des Approximationssatzes für die Bewertungen $v \mid \infty$ immer möglich.

Ebenso ist es aufgrund des Approximationssatzes bzw. schon des chinesischen Restsatzes möglich, ein $a \in \mathbb{Z}$ zu wählen, so daß $(ac')_v \leqslant 1$ für alle $v \nmid \infty$ wird. Wir nennen $c'' = ac'$ und bemerken

$$2nc_0|a|_v \leqslant c''_v \leqslant 4nc_0|a|_v \tag{4.29}$$

für alle $v \mid \infty$.

Es sei nun $\mathfrak{a} = \prod_{v \nmid \infty} \mathfrak{p}_v^{\operatorname{ord}_v(c'')}$, wobei $\operatorname{ord}_v(c'') = \operatorname{ord}_v(\alpha)$ mit einem $\alpha \in K_v$ mit $|\alpha|_v = c''_v$ ist. Es ist dann

$$\frac{1}{\operatorname{Nm}(\mathfrak{a})} = \|c''\|_{\text{endl.}} = \prod_{v \nmid \infty} \|c''\|_v \tag{4.30}$$

Wähle nun eine $\mathbb{Q}$–Basis $\omega_1, \ldots, \omega_n$ von K aus $\mathcal{O}_K$ und betrachte

$$W(C) = \{x \in \mathcal{O}_K \mid x = w_1\omega_1 + \cdots + w_n\omega_n, 0 \leqslant w_i \leqslant C, w_i \in \mathbb{Z}\}$$

mit einer Konstanten $C > 0$, die noch festzulegen ist. Setze

$$c_0 = \max_{\substack{v \mid \infty \\ i}} |\omega_i|_v.$$

Betrachte die Abbildung

$$\Phi : W(C) \to \mathcal{O}_K/\mathfrak{a}, \quad w \mapsto w + \mathfrak{a}$$

Es gibt dann immer ein $\theta \in \mathcal{O}_K/\mathfrak{a}$ mit

$$|\Phi^{-1}(\theta)| \geqslant \frac{C^n}{|\operatorname{Nm}(\mathfrak{a})|}.$$

Nenne $W_0 = \Phi^{-1}(\theta)$. Dann ist für $x, y \in W_0$ auch $x - y \in \mathfrak{a}$, also $|x - y|_v \leqslant c''_v$ für $v \nmid \infty$.

Für $v \mid \infty$ ist

$$|x - y|_v \leqslant 2nc_0C.$$

Wir beachten $|a|_v = a$ für alle $v \mid \infty$, weil $a \in \mathbb{Z}$, und setzen

$$C = a \tag{4.31}$$

Wegen $2nc_0|a|_v \leqslant c''_v$ ist dann auch $|x - y|_v \leqslant c''_v$ für $v \mid \infty$.

Kurzum haben wir dann für ein festes $y \in W_0$ eine Injektion

$$W_0 \hookrightarrow L(c''), \quad x \mapsto x - y$$

und es ist damit

$$|L(c)| = |L(c'')| \geqslant |W_0| \geqslant C^n/|\operatorname{Nm}\mathfrak{a}|.$$

Nun ist

$$\frac{C^n}{|\mathrm{Nm}\,\mathfrak{a}|} = \left(\prod_{v|\infty} |a|_v^{n_v}\right) \|c''\|_{\text{endl.}} \geqslant \left(\prod_{v|\infty} (c_v''^{n_v}/(4nc_0)^{n_v})\right) \|c''\|_{\text{endl.}} =$$
$$= \frac{\|c''\|_\infty \|c''\|_{\text{endl.}}}{(4nc_0)^n} = \frac{\|c''\|}{(4nc_0)^n} = C_1\|c\| \quad (4.32)$$

Damit ist die linke Seite der Ungleichung mit $C_1 = \frac{1}{(4nc_0)^n}$ gezeigt.

Für die rechte Seite der Ungleichung sei angenommen, daß wenigstens ein komplexes $v_0 \mid \infty$ existiert und daß $\lambda(c) > 1$ sei. Man wähle zunächst ein ganzes $m > 0$ mit

$$m < \lambda(c)^{1/2} \leqslant m + 1$$

In $\mathbb{C} = K_{v_0}$ wähle ein Quadrat um den Nullpunkt mit Kantenlänge $2c_{v_0}$ und teile es in m^2 gleiche, kleine Quadrate auf. Da $m^2 < \lambda(c)$ und alle $x \in L(c)$ bei v_0 in das große Quadrat fallen, gibt es ein kleines Quadrat Q mit Elementen $x, y \in Q$, so daß $x, y \in L(c)$ sind. Wir haben dann für $x - y$ folgende Beziehungen

$$\|x - y\|_w \leqslant \|c\|_w$$

für alle nichtarchimedischen $w \in \Sigma_K$. Weiter ist

$$\|x - y\|_v \leqslant 2\|c\|_v$$

für alle $v \mid \infty$ und $v \neq v_0$. Schließlich ist aufgrund unserer Quadratunterteilung

$$\|x - y\|_{v_0} \leqslant 2\left(\frac{2c_{v_0}}{m}\right)^2 = \frac{8\|c\|_{v_0}}{m^2}$$

Nun ist aber $\prod_{w\in\Sigma_K} \|x - y\|_w = 1$, und andererseits aufgrund unserer obigen drei Ungleichungen

$$1 = \prod_{w\in\Sigma_K} \|x - y\|_w \leqslant C \prod_{w\nmid\infty} \|c\|_w \prod_{w|\infty} \|c\|_w \frac{1}{m^2} =$$
$$= \frac{C}{m^2} \prod_{w\in\Sigma_K} \|c\|_w = \frac{C}{m^2}\|c\| \quad (4.33)$$

mit einer geeigneten Konstante C, die sich aus den angeschriebenen Potenzen von 2 ergibt. Also ist $m^2 \leqslant C\|c\|$ und $\lambda(c) \leqslant (m+1)^2 < 4m^2 \leqslant 4C\|c\|$, was die rechte Seite der Ungleichung ergibt.

Sollte kein komplexes $v_0 \mid \infty$ existieren, so betrachte man analog ein in m Teilintervalle unterteiltes Intervall in $\mathbb{R}$ um die Null herum mit Länge $2c_{v_0}$. Die ausgeschlossenen Fälle $\lambda(c) \leqslant 1$ sind unproblematisch für die Ungleichung.

4.4 Der Satz von Hermite-Minkowski

Es stehe im folgenden stets $K/\mathbb{Q}$ für einen algebraischen Zahlkörper mit $[K : \mathbb{Q}] = n_K = n$.

Definition 4.4.1. *Es sei $K/\mathbb{Q}$ ein algebraischer Zahlkörper mit s reellen Einbettungen $\sigma_1, \dots, \sigma_s : K \to \mathbb{R}$ und t wesentlich verschiedenen komplexen Einbettungen $\tau_1, \dots, \tau_t : K \to \mathbb{C}$.*

Dann sei

$$\phi : K \to \mathbb{R}^n, \quad \phi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \Re\tau_1(\alpha), \Im\tau_1(\alpha), \dots, \Re\tau_t(\alpha), \Im\tau_t(\alpha))$$

$$\psi : K \to \mathbb{C}^n, \quad \psi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \tau_1(\alpha), \bar\tau_1(\alpha), \dots, \tau_t(\alpha), \bar\tau_t(\alpha))$$

Lemma 4.4.1. *Es ist dann $\phi(\mathcal{O}_K) = \Gamma_K = \Gamma$ ein Gitter im $\mathbb{R}^n$.*

Lemma 4.4.2. *Für eine $\mathbb{Z}$–Basis $\beta_1, \dots, \beta_n$ von $\mathcal{O}_K$ gilt*

$$(\phi(\beta_1) \dots \phi(\beta_n))^t M = (\psi(\beta_1) \dots \psi(\beta_n))^t \tag{4.34}$$

wobei

$$M = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & i & -i \end{pmatrix} \tag{4.35}$$

mit t Blöcken $\left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right)$ ist.

Es ist $|\det M| = 2^t$. Insgesamt folgt aus Gleichung (4.34)

Lemma 4.4.3. *Mit den schon eingeführten Bezeichnungen gilt:*

$$|\det(\phi(\beta_1) \dots \phi(\beta_n))| = \operatorname{covol} \Gamma_K \tag{4.36}$$

$$|\det(\psi(\beta_1) \dots \psi(\beta_n))| = \sqrt{d_{K:\mathbb{Q}}} \tag{4.37}$$

$$\operatorname{covol}(\Gamma_K) = 2^{-t} \sqrt{d_{K:\mathbb{Q}}} \tag{4.38}$$

Dabei stehe $\operatorname{covol}(\Gamma_K)$ *natürlich für das Volumen eines Fundamentalparallelogramms aus einer $\mathbb{Z}$–Basis von Γ_K, respektive von $\mathcal{O}_K$.*

Wir wollen nun $\langle \phi(\alpha_1), \phi(\alpha_2) \rangle$ und $\operatorname{Tr}(\alpha_1 \alpha_2)$ für $\alpha_i \in \mathcal{O}_K$ miteinander vergleichen. Dabei sei $\langle \cdot, \cdot \rangle$ das euklidische Skalarprodukt in $\mathbb{R}^n$

Es sei $\sigma_j(\alpha_i) = x_j^i$ und $\Re\tau_k(\alpha_i) = y_k^i$ sowie $\Im\tau_k(\alpha^i) = z_k^i$.

Dann ist

$$\langle \phi(\alpha_1), \phi(\alpha_2) \rangle = \sum_j x_j^1 \, x_j^2 + \sum_k (y_k^1 \, y_k^2 + z_k^1 \, z_k^2) \tag{4.39}$$

und weiter

$$\begin{aligned} \operatorname{Tr}(\alpha_1 \alpha_2) &= \sum_j \sigma_j(\alpha_1 \alpha_2) + \sum_k (\tau_k(\alpha_1 \alpha_2) + \bar\tau_k(\alpha_1 \alpha_2)) = \\ &= \sum_j \sigma_j(\alpha_1) \, \sigma_j(\alpha_2) + \sum_k 2 \, \Re(\tau_k(\alpha_1) \, \tau_k(\alpha_2)) = \\ &= \sum_j x_j^1 \, x_j^2 + \sum_k 2(y_k^1 \, y_k^2 - z_k^1 \, z_k^2) \end{aligned} \tag{4.40}$$

Setzt man $\alpha_1 = \alpha_2 = \alpha$, also $x_j = x_j^1 = x_j^2$ und $y_k = y_k^1 = y_k^2$ sowie $z_k = z_k^1 = z_k^2$ so folgt:

$$\langle \phi(\alpha), \phi(\alpha) \rangle = \sum_j (x_j)^2 + \sum_k ((y_k)^2 + (z_k)^2) \tag{4.41}$$

$$\mathrm{Tr}(\alpha) = \sum_j (x_j)^2 + \sum_k 2\,((y_k)^2 - (z_k)^2) \tag{4.42}$$

Es gilt also

Lemma 4.4.4. *Mit den oben verwendeten Bezeichnungen ist*

$$2\,\|\phi(\alpha)\|_2^2 \geqslant \mathrm{Tr}(\alpha^2) \tag{4.43}$$

Da für $\alpha \in \mathcal{O}_K$ immer $\mathrm{Tr}(\alpha^2) \in \mathbb{Z}$ ist, gilt auf jeden Fall folgendes:

Lemma 4.4.5 (Abstandslemma). *Setzt man $B(\rho) = \{x \in \mathbb{R}^n \mid \|x\|_2 < \rho\}$, so ist*

$$\{0\} = B(\rho) \cap \Gamma_K \tag{4.44}$$

für jedes in Frage kommende K und $\rho > 0$ genügend klein und unabhängig von K (zum Beispiel $\rho = 1/\sqrt{2}$).

Theorem 4.4.1 (Hermite-Minkowski). *Es sei $K/\mathbb{Q}$ eine algebraische Körpererweiterung mit Grad $[K : \mathbb{Q}] = n$. Es sei $K/\mathbb{Q}$, also $\mathcal{O}_K/\mathbb{Z}$ nur in den Primstellen $p_1, \ldots, p_r$ verzweigt.*

Dann gibt es nur endlich viele verschiedene K, die diese beiden Bedingungen erfüllen.

Dieser Satz ergibt sich aus folgendem Lemma und der danachstehenden Proposition:

Lemma 4.4.6. *Es sei $K/\mathbb{Q}$ eine algebraische Körpererweiterung mit $[K : \mathbb{Q}] \leqslant n$. Weiter sei $K/\mathbb{Q}$ nur in den fest gewählten Primstellen $p_1, \ldots, p_r$ verzweigt.*

Dann existiert ein $D > 0$, abhängig von n und den p_i, so daß $d_{K:\mathbb{Q}} < D$ ist.

Proposition 4.4.1. *Es sei $K/\mathbb{Q}$ algebraisch, $[K : \mathbb{Q}] = n$ und Diskriminante $d_{K:\mathbb{Q}}$ fest.*

Dann gibt es nur endlich viele verschiedene K, die diese Bedingungen erfüllen.

Beweis. Es sei $n = s + 2\,t$, es gebe also s reelle Einbettungen $\sigma_1, \ldots, \sigma_s : K \to \mathbb{R}$ von K und t wesentlich verschiedene komplexe $\tau_1, \ldots, \tau_t : K \to \mathbb{C}$.

Es ist dann wie oben bemerkt $\phi(\mathcal{O}_K) = \Gamma_K = \Gamma$ ein Gitter im $\mathbb{R}^n$.

Nenne $e_1 \in \mathbb{R}^n$ nun den Vektor $\phi(1) = (1, \ldots)$ mit $\|e_1\|_2 = \sqrt{s+t}$. Führe dann zu e_1 bezüglich des euklidischen Skalarproduktes $\langle \cdot, \cdot \rangle$ senkrechte Vektoren $e_2, \ldots, e_n$ (der Länge 1 oBdA) ein, so daß insgesamt $e_i \perp e_j$ für $i \neq j$ ist.

Nun kommt die eigentliche Überlegung: Γ_K ist ein Gitter mit

$$\operatorname{covol}(\Gamma_K) = 2^{-t}\sqrt{d_{K:\mathbb{Q}}} \tag{4.45}$$

Wähle nun für jeden der Vektoren $e_2, \ldots, e_n$ einen sehr langgestreckten (notwendig konvexen) extrem schmalen Kreiszylinder E_i mit Achse $\mathbb{R}\, e_i$ dessen Deckelflächen senkrecht auf der Achse stehen. Dieser erstrecke sich in beiden Achsenrichtungen gleichweit von der Null als dem Mittelpunkt seiner Achse und ist so bezüglich 0 auch punktsymmetrisch.

Es ist offensichtlich, daß man diese Zylinder so einrichten kann, daß

i) Für das Volumen $\operatorname{vol}(E_i) > 2^n \operatorname{covol}(\Gamma_K) = 2^n\, 2^{-t}\, \sqrt{d_{K_\mathbb{Q}}}$ gilt.
ii) Es ist für alle i stets $E_i \cap B(\rho) = \{0\}$.

Nach dem Fundamentalsatz von Minkowski über Gitter und konvexe Polyeder gibt es dann $z_2, \ldots, z_n$ mit $z_i \in \Gamma_K \cap E_i$ und $z_i \neq 0$ also $z_i = \phi(\alpha_i)$ und $\alpha_i \in \mathfrak{O}_K$ und $\alpha_i \neq 0$.

Diese $z_2, \ldots, z_n$ sind linear unabhängig über $\mathbb{R}$, ja es ist sogar $\phi(1), z_2, \ldots, z_n$ linear unabhängig über $\mathbb{R}$. Das erscheint anschaulich klar, wenn man die langgestreckte schmale Gestalt der E_i bedenkt, muß aber noch bewiesen werden.

Nennt man ϵ den kleinen Radius der Kreiszylinder E_i und beachtet, daß wegen des oben Abstandslemma genannten Lemmas jedes z_i in e_i Richtung mindestens den Betrag $\rho - \epsilon$ hat, so ist es einfach nötig einzusehen, daß für eine Matrix

$$A = \begin{pmatrix} 1 & a_{12} & \ldots & a_{1n} \\ a_{21} & 1 & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & 1 \end{pmatrix} \tag{4.46}$$

für die $|a_{ij}| < \epsilon_1$ stets $\det A \neq 0$ bei ϵ_1 genügend klein ist. Dies ist aber offenkundig.

Damit ist dann auch $1, \alpha_2, \ldots, \alpha_n$ linear unabhängig über $\mathbb{Q}$, also $\mathbb{Q}(\alpha_2, \ldots, \alpha_n) = K$, denn es folgt ja $[\mathbb{Q}(\alpha_2, \ldots, \alpha_n) : \mathbb{Q}] \geqslant n$ und wegen $\mathbb{Q}(\alpha_2, \ldots, \alpha_n) \subseteq K$ auch $K = \mathbb{Q}(\alpha_2, \ldots, \alpha_n)$.

Es bleibt zu zeigen, daß es nur endlich viele mögliche Tupel $(\alpha_2, \ldots, \alpha_n)$ gibt. Dies ist aber einfach zu sehen: In jedem E_i sind für $\phi(\alpha_i) = z_i = (x_{i1}, \ldots, x_{in})$ die Koordinaten $x_{ip} \leqslant C$ für ein geeignetes $C > 0$ das nur von $d_{K:\mathbb{Q}}$ und n abhängt. Damit sind aber auch alle elementarsymmetrischen Funktionen

$$|S^i_\nu| = |S_\nu(\ldots, \sigma_j(\alpha_i), \ldots, \tau_k(\alpha_i), \bar{\tau}_k(\alpha_i), \ldots)| < C' \tag{4.47}$$

mit einem C', das nur von C und ν abhängt. Da $S^i_\nu \in \mathbb{Z}$ gibt es von diesen also nur endlich viele.

Da α_i das Polynom $\alpha_i^n + \sum_{\nu=1}^n S^i_\nu \alpha_i^{n-\nu} = 0$ erfüllt, gibt es also auch nur endlich viele α_i, also auch nur endlich viele Tupel $(\alpha_2, \ldots, \alpha_n)$.

5

Verallgemeinerte Idealklassen

5.1 Zykel und verallgemeinerte Idealklassengruppe

Es sei k ein Zahlkörper und Σ_k die Menge seiner Stellen. Dann sei

$$\mathfrak{c} = \prod_{v \in \Sigma_k} v^{m(v)}$$

ein abstraktes Produkt von Stellen mit Exponenten $m(v) \geqslant 0$ und $m(v) = 0$ für fast alle v.

Definition 5.1.1. *Mit den obigen Bezeichnungen heiße* $\mathfrak{c} = \prod_{v \in \Sigma_k} v^{m(v)}$ *ein* Zykel für k.

Für die unendlichen Stellen treffen wir eine besondere Vereinbarung: Ist $v \in \Sigma_k^\infty$ eine komplexe Stelle, so sei stets $m(v) = 0$. Ist $v \in \Sigma_k^\infty$ eine reelle Stelle, so ist $m(v)$ entweder 1 oder 0. Wir können also die komplexen unendlichen Stellen in $\mathfrak{c}$ ignorieren.

Wir schreiben $v|\mathfrak{c}$ für eine Stelle v, für die $m(v) > 0$ ist. Weiter sei

$$\mathfrak{c}_0 = \prod_{\substack{v|c \\ v \text{ endlich}}} v^{m(v)}$$

der *endliche Teil von* $\mathfrak{c}$.

Es sei nun $x \in k^*$ ein Element des Zahlkörpers. Wir sagen, daß

$$x \equiv 1 \mod {}^*\mathfrak{c}$$

genau dann, wenn

i) $\mathrm{ord}_v(x) \geqslant 0$ und $\mathrm{ord}_v(x-1) \geqslant m(v)$ für alle endlichen Stellen $v|\mathfrak{c}$ ist
ii) $x_v > 0$ für alle reellen Stellen v mit $v|\mathfrak{c}$ gilt. Dabei stehe x_v für das Bild von x unter $k \to k_v = \mathbb{R}$.

Anmerkung 5.1.1. Wir nennen für eine unendliche reelle Stelle v die Gruppe $k_v^+ = \mathbb{R}_{>0}$ und $k_v^* = \mathbb{R}_{\neq 0}$. Es ist dann $k_v^*/k_v^+ = \{-1, 1\}$.

Es sei nun

$$k(\mathfrak{c}) = \{x \in k^* \mid \mathrm{ord}_v(x) = 0 \text{ für alle } v|\mathfrak{c}_0\} \tag{5.1}$$

$$k_{\mathfrak{c}} = \{x \in k^* \mid x \equiv 1 \mod {}^*\mathfrak{c}\} \tag{5.2}$$

Wir nennen die Elemente von $k(\mathfrak{c})$ *zu* $\mathfrak{c}$ *prim*, die von $k_{\mathfrak{c}}$ *kongruent* 1 *modulo* $\mathfrak{c}$. Es ist selbstverständlich $k_{\mathfrak{c}} \subseteq k(\mathfrak{c})$.

Allgemein werden wir im folgenden die Abkürzungen $X(\mathfrak{c})$ und $X_{\mathfrak{c}}$ benutzen um für ein algebraisches Objekt X, für das die Begriffe „prim zu $\mathfrak{c}$“ und „kongruent 1 modulo $\mathfrak{c}$“ sinnvoll definiert sind, die entsprechenden Unterobjekte zu bezeichnen.

Definition 5.1.2. *Es sei k ein Zahlkörper mit Ganzheitsring A und einem Zykel $\mathfrak{c}$. Es sei I_A die Gruppe der gebrochenen Ideale. Dann ist*

$$I_A(\mathfrak{c}) = \{I \in I_A \mid \mathrm{ord}_v(I) = 0 \textit{ für alle } v|\mathfrak{c}_0\} \tag{5.3}$$

Wir schreiben auch einfach I und $I(\mathfrak{c})$, falls k und A feststehen.

Wir nennen, wie schon weiter oben eingeführt, $P = \mathrm{im}(k^* \to I)$ die Gruppe der Hauptideale von k und $P_{\mathfrak{c}} = \mathrm{im}(k_{\mathfrak{c}} \to I) \subseteq P \subseteq I$ die Gruppe der *Hauptideale kongruent* 1 *modulo* $\mathfrak{c}$.

Proposition 5.1.1. *Das folgende Diagramm ist exakt:*

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & I(\mathfrak{c})/P(\mathfrak{c}) & \longrightarrow & I/P & \longrightarrow & 0 & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & I(\mathfrak{c}) & \longrightarrow & I & & & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & P(\mathfrak{c}) & \longrightarrow & P & & & & \\
 & & \uparrow & & \uparrow & & & & \\
 & & 0 & & 0 & & & &
\end{array} \tag{5.4}$$

Dabei sei $P(\mathfrak{c}) = I(\mathfrak{c}) \cap P = \ker(I(\mathfrak{c}) \to I \to I/P)$.

Es gilt also $I(\mathfrak{c})/P(\mathfrak{c}) = I/P = \mathrm{Cl}_A$.

Definition 5.1.3. *Wir nennen $I(\mathfrak{c})/P_{\mathfrak{c}}$ die* verallgemeinerte Idealklassengruppe von k bzw. A *oder auch* $\mathfrak{c}$–Idealklassengruppe *und schreiben auch* $\mathrm{Cl}_k(\mathfrak{c})$ *für diese Gruppe.*

Das folgende Diagramm ist exakt:

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \uparrow & & \uparrow & & \\
 & & 0 & \longrightarrow & k(\mathfrak{c})/(Uk_{\mathfrak{c}}) & \longrightarrow & P(\mathfrak{c})/P_{\mathfrak{c}} & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & U & \longrightarrow & k(\mathfrak{c}) & \longrightarrow & P(\mathfrak{c}) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & U & \longrightarrow & Uk_{\mathfrak{c}} & \longrightarrow & P_{\mathfrak{c}} & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{5.5}$$

Die verallgemeinerte Idealklassengruppe sitzt als mittlerer Term in

$$0 \to P(\mathfrak{c})/P_{\mathfrak{c}} \to I(\mathfrak{c})/P_{\mathfrak{c}} \to I(\mathfrak{c})/P(\mathfrak{c}) \to 0 \tag{5.6}$$

Wir zeigen im folgenden, daß die linke Gruppe ebenfalls endlich, mithin $I(\mathfrak{c})/P_{\mathfrak{c}}$ endlich ist.

Proposition 5.1.2. *Die folgende Sequenz ist exakt:*

$$0 \to k_{\mathfrak{c}} \to k(\mathfrak{c}) \to \prod_{v|\mathfrak{c}_0} (\mathcal{O}_{\mathfrak{p}_v}/\mathfrak{p}_v^{m(v)})^* \times \prod_{\substack{v|\mathfrak{c} \\ v \text{ reell}}} k_v^*/k_v^+ \to 0 \tag{5.7}$$

In der vorigen Sequenz hat die rechts stehende Gruppe die Mächtigkeit

$$\begin{aligned}
\varphi(\mathfrak{c}) = 2^{s(\mathfrak{c})} \prod_{v|\mathfrak{c}_0} \left((\mathrm{Nm}_{k|\mathbb{Q}}\, \mathfrak{p}_v) - 1 \right) \left(\mathrm{Nm}_{k|\mathbb{Q}}\, \mathfrak{p}_v \right)^{m(v)-1} = \\
= 2^{s(\mathfrak{c})} \prod_{v|\mathfrak{c}_0} \left| (\mathcal{O}_{\mathfrak{p}_v}/\mathfrak{p}_v^{m(v)})^* \right| = 2^{s(\mathfrak{c})} \prod_{v|\mathfrak{c}_0} \varphi_v(\mathfrak{c}) = 2^{s(\mathfrak{c})} \varphi(\mathfrak{c}_0)
\end{aligned} \tag{5.8}$$

wobei $s(\mathfrak{c})$ die Anzahl der reellen Stellen $v|\mathfrak{c}$ angibt.

Die folgende Sequenz ist exakt:

$$0 \to Uk_{\mathfrak{c}}/k_{\mathfrak{c}} \to k(\mathfrak{c})/k_{\mathfrak{c}} \to k(\mathfrak{c})/Uk_{\mathfrak{c}} \to 0 \tag{5.9}$$

Es gilt also für die Mächtigkeiten:

$$\frac{\varphi(\mathfrak{c})}{(U : U_{\mathfrak{c}})} = \#(k(\mathfrak{c})/Uk_{\mathfrak{c}}) = \#(P(\mathfrak{c})/P_{\mathfrak{c}}) \tag{5.10}$$

wobei $Uk_{\mathfrak{c}}/k_{\mathfrak{c}} = U/(k_{\mathfrak{c}} \cap U) = U/U_{\mathfrak{c}}$.

Insgesamt haben wir ein Diagramm

$$\begin{array}{ccccc} & & & & I(\mathfrak{c}) & \longrightarrow & I \\ & & & & \big| & & \big| \\ & & k(\mathfrak{c}) & \longrightarrow & P(\mathfrak{c}) & \longrightarrow & P \\ & & \big| & & \big| & & \\ U & \longrightarrow & k_{\mathfrak{c}}U & \longrightarrow & P_{\mathfrak{c}} & & \\ \big| & & \big| & & & & \\ U_{\mathfrak{c}} & \longrightarrow & k_{\mathfrak{c}} & & & & \end{array} \tag{5.11}$$

wobei parallele senkrechte Striche für Isomorphie der entsprechenden Quotientengruppen stehen. Es ergibt sich

Proposition 5.1.3. *Die Mächtigkeit von* $\mathrm{Cl}_k(\mathfrak{c})$ *ist:*

$$|I(\mathfrak{c})/P_{\mathfrak{c}}| = \frac{|\mathrm{Cl}_k|\,\varphi(\mathfrak{c})}{(U : U_{\mathfrak{c}})} = \frac{h\,\varphi(\mathfrak{c}_0)\,2^{s(\mathfrak{c})}}{(U : U_{\mathfrak{c}})} \tag{5.12}$$

6

Anzahl der Ideale in einer gegebenen Klasse

6.1 Ein grundlegendes Lemma

Es sei $D \subseteq \mathbb{R}^n$ eine Teilmenge so daß $\bar{D}$ kompakt und mit Lipschitz–Rand ausgestattet ist. Es existiert dann $d = \mathrm{vol}(\bar{D})$ und es ist $\mathrm{vol}(D) = \mathrm{vol}(\bar{D})$.

Weiter sei λD für $\lambda > 0$ das Bild von D unter der Homothetie $x \mapsto \lambda x$ mit $\mathrm{vol}(\lambda D) = \lambda^n \mathrm{vol}(D)$.

Es sei $\Gamma \subseteq \mathbb{R}^n$ ein volles Gitter mit $\Gamma \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^n$ und $\mathrm{vol}(\mathbb{R}^n/\Gamma) = \gamma$.

Definition 6.1.1. *Mit*

$$j(\Gamma, D) = \#\{x \mid x \in \Gamma \cap D\}$$

sei die Anzahl der Punkte aus $\Gamma \cap D$ bezeichnet.

Lemma 6.1.1. *Mit den obigen Bezeichnungen gilt*

$$j(\Gamma, \lambda D) = \lambda^n \frac{d}{\gamma} + O(\lambda^{n-1})$$

6.2 Gewöhnliche Ideale

Es sei K ein algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$ und $\mathfrak{a} \subseteq \mathcal{O}_K$ ein ganzes Ideal. Mit $\mathfrak{a} \sim \mathfrak{a}'$ sei bezeichnet, daß $\mathfrak{a}$ und $\mathfrak{a}'$ derselben Idealklasse angehören, also $\mathfrak{a}\mathfrak{a}'^{-1} = (x)$ mit $x \in K^*$ ist.

Definition 6.2.1. *Es sei $j(\mathfrak{a}, t)$ gleich der Anzahl der ganzen Ideale $\mathfrak{a}' \subseteq \mathcal{O}_K$ in derselben Idealklasse wie $\mathfrak{a}$ mit $\mathrm{Norm}(\mathfrak{a}') \leqslant t$. Also*

$$j(\mathfrak{a}, t) = \#\{\mathfrak{a}' \subseteq \mathcal{O}_K \mid \mathfrak{a}' \sim \mathfrak{a},\ \mathrm{Norm}(\mathfrak{a}') \leqslant t\} \tag{6.1}$$

Um diese Ideale abzuzählen bedient man sich folgender Überlegung: Es sei $\mathfrak{b} \subseteq \mathcal{O}_K$ ein ganzes Ideal mit $\mathfrak{a}^{-1} \sim \mathfrak{b}$. Weiter sei $\mathfrak{a}' \sim \mathfrak{a}$ mit $\mathrm{Norm}(\mathfrak{a}') \leqslant t$. Dann ist $\mathfrak{a}'\mathfrak{b} = (x)$, denn links steht ein Element aus der Einsklasse von Cl_K. Es gilt $(x) \subseteq \mathfrak{b}$, äquivalent $x \in \mathfrak{b}$, und es ist $\mathrm{Norm}(x) = \mathrm{Norm}(\mathfrak{a}'\mathfrak{b}) \leqslant t\,\mathrm{Norm}(\mathfrak{b})$.

Man hat somit eine $1-1$–Abbildung

$$\{0 \neq \mathfrak{a}' \subseteq \mathcal{O}_K \mid \mathfrak{a}' \sim \mathfrak{a},\ \mathrm{Norm}(\mathfrak{a}') \leqslant t\} \leftrightarrow \{0 \neq (x) \subseteq \mathfrak{b} \mid \mathrm{Norm}(x) \leqslant t\,\mathrm{Norm}(\mathfrak{b})\} \quad (6.2)$$

die durch

$$\mathfrak{a}' \mapsto \mathfrak{a}'\mathfrak{b} = (x) \quad (6.3)$$

$$(x) \mapsto \mathfrak{b}^{-1}(x) = \mathfrak{a}' \quad (6.4)$$

gegeben ist.

Es ist also $j(\mathfrak{a}, t)$ gleich der Anzahl der Elemente x des Ideals $\mathfrak{b}$ mit $\mathrm{Norm}(x) \leqslant t\,\mathrm{Norm}(\mathfrak{b})$ modulo der Äquivalenz $x \sim x'$, wenn $(x) = (x')$, also $x = xu$ mit $u \in \mathcal{O}_K^*$.

Theorem 6.2.1. *Es ist*

$$j(\mathfrak{a}, t) = \frac{2^{r_1+r_2}\pi^{r_2}R}{w\sqrt{|D_k|}}t + O(t^{1-1/n}) \quad (6.5)$$

wobei r_1 und r_2 die Anzahl der reellen und komplexen Stellen von K bezeichne, D_K die Diskriminante von K sei und w für die Anzahl der Einheitswurzeln in $\mathcal{O}_K^*$ steht.

Beweis. Wir schicken dem Beweis einige Definitionen voraus:
Es sei $\Phi : K \to \mathbb{R}^n$ die weiter oben eingeführte Einbettung

$$\Phi : (x) \to (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\tau_1(x), \Im\tau_1(x), \ldots, \Re\tau_{r_2}(x), \Im\tau_{r_2}(x))$$

wobei σ_i die reellen und τ_j die wesentlich verschiedenen komplexen Einbettungen von K in $\mathbb{R}$ bzw. in $\mathbb{C}$ sind.

Weiter sei $\log_K : K^* \to \mathbb{R}^{r_1+r_2}$ die Abbildung

$$\log_K : (x) \to (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, \log|\tau_1(x)|^2, \ldots, \log|\tau_{r_2}(x)|^2)$$

Wir führen die Koordinaten $(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2})$ in $\mathbb{R}^n$ als Bildraum von Φ ein. Im Bildraum von $\log_K$ seien $(l_1, \ldots, l_{r_1}, m_1, \ldots, m_{r_2})$ die Koordinaten.

Die Einheiten $x \in \mathcal{O}_K^*$ sind durch $|\mathrm{Norm}_{L:\mathbb{Q}}(x)| = 1$, also durch

$$|\mathrm{Norm}_{L:\mathbb{Q}}(x)| = \prod_i |\sigma_i(x)| \prod_j |\tau_j(x)|^2 = 1$$

gekennzeichnet. Es ist also

$$\log_K : \mathcal{O}_K^* \to V(l_1 + \cdots + l_{r_1} + m_1 + \cdots + m_{r_2})$$

eine surjektive Abbildung auf ein Gitter in $V(\sum_i l_i + \sum_j m_j)$ deren Kern gleich den Einheitswurzeln μ_K^* in K^*, also in $\mathcal{O}_K^*$, ist. Mit $r = r_1 + r_2 - 1$ und den Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$, also mit

$$\mathcal{O}_K^* = \mu_K^* \times \varepsilon_1^{\mathbb{Z}} \times \cdots \times \varepsilon_r^{\mathbb{Z}} = \mu_K^* \times U^*$$

hat man somit die Sequenz

$$0 \to \mu_K^* \to \mathcal{O}_K^* \xrightarrow{\log_K} \mathbb{Z}\log_K(\varepsilon_1) + \cdots + \mathbb{Z}\log_K(\varepsilon_r) \to 0$$

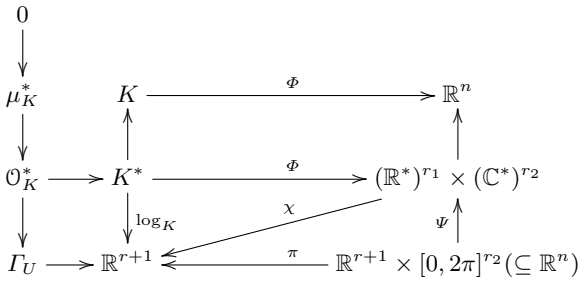
und das obenerwähnte Gitter

$$\Gamma_U = \mathbb{Z}\log_K(\varepsilon_1) + \cdots + \mathbb{Z}\log_K(\varepsilon_r) \subseteq V(\sum_i l_i + \sum_j m_j) \cong \mathbb{R}^r$$

Das Volumen $R = \mathrm{vol}(\mathbb{R}^r/\Gamma_U)$ ist der *Regulator* von K.

Für weitere Betrachtungen schreiben wir $\mathbb{R}\Gamma_U = \mathbb{R} \otimes_{\mathbb{Z}} \Gamma_U = V(z) = \mathbb{R}^r$ mit $z = \sum_i l_i + \sum_j m_j$ und zerlegen den Logarithmenraum als $\mathbb{R}^{r+1} = \mathbb{R}\Gamma_U \oplus \mathbb{R}e$, wobei e ein zu $\mathbb{R}\Gamma_U$ orthogonaler Vektor mit $z(e) = 1$ ist. Schließlich kürzen wir ab: $\log_K \varepsilon_i = \varepsilon_i'$

Insgesamt haben wir folgendes Diagramm



(6.6)

mit den Abbildungen

$$\chi : (x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) \mapsto$$
$$(\log|x_1|, \ldots, \log|x_{r_1}|, \log(y_1^2 + z_1^2), \ldots, \log(y_{r_2}^2 + z_{r_2}^2))$$

und

$$\Psi : (l_1, \ldots, l_{r_1}, m_1, \ldots, m_{r_1}, \alpha_1, \ldots, \alpha_{r_2}) \mapsto$$
$$(e^{l_1}, \ldots, e^{l_{r_1}}, e^{m_1/2}\cos(\alpha_1), e^{m_1/2}\sin(\alpha_1), \ldots, e^{m_{r_2}/2}\cos(\alpha_{r_2}), e^{m_{r_2}/2}\sin(\alpha_{r_2}))$$

sowie der Projektion auf den ersten Faktor $\pi : \mathbb{R}^{r+1} \times \mathbb{R}^{r_2} \to \mathbb{R}^{r+1}$.

Nennt man $\theta_{\nu_1,\ldots,\nu_{r_1}} : \mathbb{R}^n \to \mathbb{R}^n$ mit $\nu_i \in \{-1, +1\}$ die Abbildungen

$$\theta_{\nu_1,\ldots,\nu_{r_1}}(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) =$$
$$= (\nu_1 x_1, \ldots, \nu_{r_1} x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) \quad (6.7)$$

so ist für $P \in \mathbb{R}^{r+1}$, dem Logarithmenraum,

$$\chi^{-1}(P) = \bigcup_{(\nu_1,\ldots,\nu_{r_1})} \theta_{\nu_1,\ldots,\nu_{r_1}} \Psi(\pi^{-1}(P)) \tag{6.8}$$

wobei die Vereinigung rechts eine disjunkte ist. Die gleiche Beziehung gilt daher auch für $P \subseteq \mathbb{R}^{r+1}$.

Es sei nun F'_U ein Fundamentalbereich für $\Gamma_U \subseteq \mathbb{R}^r$, wir nehmen

$$F'_U = \{\sum_{i=1}^{r} t_i \varepsilon'_i \mid 0 \leqslant t_i < 1\}$$

Weiter sei

$$F_U = F'_U \oplus \{z \leqslant 0\} \subseteq \mathbb{R}^{r+1}$$

in der Zerlegung $\mathbb{R}^{r+1} = \mathbb{R}\Gamma_U \oplus \mathbb{R}e$ von oben. Es sei

$$F_{K^*} = \log_K^{-1}(F_U)$$

und

$$F = \chi^{-1}(F_U).$$

Es ist dann auch $\Phi^{-1}(F) = F_{K^*}$.

Für $F_U \subseteq \mathbb{R}^{r+1}$ und mit $G = [0, 2\pi]^{r_2}$, ist $\pi^{-1}(F_U) = F_U \times G$ und wir haben

$$\begin{aligned}\int_{\Psi(F_U\times G)} dx_1 dx_2 \cdots dy_{r_2} dz_{r_2} = \\ = \frac{1}{2^{r_2}} \int_{F_U\times G} e^{\sum_i l_i + \sum_j m_j} dl_i dm_j d\alpha_j = \\ = \pi^{r_2} \int_{F_U} e^z dl_i dm_j = \pi^{r_2} \int_{F'_U\times\{z\leqslant 0\}} e^z dl_i dm_j = \\ = \pi^{r_2} \left(\int_{F'_U} dw_i\right) \left(\int_{z=-\infty}^{z=0} e^z dz\right) = \pi^{r_2} R \end{aligned} \tag{6.9}$$

mit $z = \sum_i l_i + \sum_j m_j$, wie oben und mit Koordinaten $w_1, \ldots, w_r$ in $\mathbb{R}\Gamma_U$. Es ist also wegen (6.8):

$$\begin{aligned}\mathrm{vol}(F) = \mathrm{vol}(\chi^{-1}(F_U)) = 2^{r_1}\,\mathrm{vol}(\Psi(\pi^{-1}(F_U))) = \\ = 2^{r_1}\,\mathrm{vol}(\Psi(F_U \times G)) = 2^{r_1}\pi^{r_2} R \end{aligned} \tag{6.10}$$

nach obiger Ausrechnung des Integrals.

Mit dem eben eingeführten Fundamentalbereich F gilt also die Beziehung für $x \in K^*$: Es ist $\Phi(x) \in F$ äquivalent zu $x \in F_{K^*}$ äquivalent zu $|\mathrm{Norm}(x)| \leqslant 1$ und $\log_K(x) \in F_U$. Weiterhin gilt

$$\begin{aligned}\#\{0 \neq (x) \subseteq \mathfrak{b} \mid |\mathrm{Norm}(x)| \leqslant t\} = \\ = \#\{x\,\mathcal{O}_K^* \mid 0 \neq x \in \mathfrak{b}, |\mathrm{Norm}(x)| \leqslant t\} = \\ = 1/w \#\{x\,U^* \mid 0 \neq x \in \mathfrak{b}, |\mathrm{Norm}(x)| \leqslant t\} \end{aligned} \tag{6.11}$$

wobei $w = \#\mu_K^*$ die Anzahl der Einheitswurzeln in K ist.

Aus der Beziehung $\log_K(U^*) = \Gamma_U$ und der Definition von F_U aus einem Fundamentalbereich F'_U für $\Gamma_U \subseteq \mathbb{R}\Gamma_U$, sowie aus der Beziehung $\log_K = \chi \circ \Phi$, ergeben sich die folgenden Tatsachen:

Gilt für ein $x \in K^*$ mit $|\mathrm{Norm}(x)| \leqslant t$ und $u \in U^*$, daß $\Phi(x), \Phi(ux) \in t^{1/n}F$, so ist $\log_K(x), \log_K(ux) \in \chi(t^{1/n}F) = F_U + \log(t)e$. Nach Konstruktion von F_U aus F'_U ist dann $u = 1$ und $x = ux$.

Umgekehrt gibt es für jedes $x \in K^*$ mit $|\mathrm{Norm}(x)| \leqslant t$ ein $u \in U^*$, so daß $\log_K(ux) = \log_K(u) + \log_K(x) \in F_U + \log(t)e$ ist. Es ist dann auch $\Phi(ux) \in \chi^{-1}(F_U + \log(t)e) = t^{1/n}F$.

Jede Bahn xU^* mit $|\mathrm{Norm}(x)| \leqslant t$ und $x \in K^*$ hat deshalb genau einen Vertreter $x' \neq 0$ mit $\Phi(x') \in t^{1/n}F$. Damit und wegen (6.11) haben wir:

$$j(\mathfrak{a}, t) = \#\{0 \neq (x) \subseteq \mathfrak{b} \mid \mathrm{Norm}(x) \leqslant t'\} = \\ = \frac{1}{w}\#\{\Phi(\mathfrak{b}) \cap t'^{1/n}F\} = \frac{1}{w}j(\Phi(\mathfrak{b}), t'^{1/n}F) \quad (6.12)$$

mit $t' = t\,\mathrm{Norm}(\mathfrak{b})$.

Um nun

$$\#\{0 \neq (x) \subseteq \mathfrak{b} \mid \mathrm{Norm}(x) \leqslant t\,\mathrm{Norm}(\mathfrak{b})\}$$

abzuzählen, also $j(\mathfrak{a}, t)$ zu bestimmen, genügt es, die $(x) \subseteq \mathcal{O}_K$ mit $\mathrm{Norm}(x) \leqslant t$ abzuzählen. Gilt für diese, also für $j((1), t) = Ct + O(t^{1-1/n})$, so ist auch

$$j(\mathfrak{a}, t) = Ct + O(t^{1-1/n})$$

Sei nämlich $F \subseteq \mathbb{R}^n$ der Fundamentalbereich, wie wir ihn oben konstruiert haben. Es gilt dann:

$$j(\mathfrak{a}, t) = \frac{1}{w}j(\Phi(\mathfrak{b}), (t\,\mathrm{Norm}(\mathfrak{b}))^{1/n}F) = \frac{\mathrm{vol}(F)}{w\,\mathrm{vol}(\mathbb{R}^n/\Phi(\mathfrak{b}))}t\,\mathrm{Norm}(\mathfrak{b}) = \\ = \frac{\mathrm{vol}(F)}{w\,\mathrm{vol}(\mathbb{R}^n/\Phi(\mathcal{O}_K))\,\mathrm{Norm}(\mathfrak{b})}t\,\mathrm{Norm}(\mathfrak{b}) = \frac{\mathrm{vol}(F)}{w\,\mathrm{vol}(\mathbb{R}^n/\Phi(\mathcal{O}_K))}t = \\ = \frac{1}{w}j(\Phi(\mathcal{O}_K), t^{1/n}F) = j((1), t) \mod O(t^{1-1/n}) \quad (6.13)$$

Da $\mathrm{vol}(\mathbb{R}^n/\Phi(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|D_K|}$, genügt es also, $\mathrm{vol}(F)$ zu bestimmen. Dies haben wir aber oben schon getan und $\mathrm{vol}(F) = 2^{r_1}\pi^{r_2}R$ erhalten. Zusammengesetzt folgt das Ergebnis.

6.3 Verallgemeinerte Ideale

Es sei $\mathfrak{c}$ ein Zykel für den algebraischen Zahlkörper K. Wir betrachten nur Ideale aus $I(\mathfrak{c})$ und nennen $\mathfrak{a}' \sim \mathfrak{a}$, wenn $\mathfrak{a}'\mathfrak{a}^{-1} \in P_{\mathfrak{c}}$ ist.

Definition 6.3.1. *Es sei $j(\mathfrak{c}, \mathfrak{a}, t)$ gleich der Anzahl der ganzen Ideale $\mathfrak{a}'$ aus $I(\mathfrak{c})$ mit $\mathfrak{a} \sim \mathfrak{a}'$ und $\mathrm{Norm}(\mathfrak{a}') \leqslant t$. Also*

$$j(\mathfrak{c}, \mathfrak{a}, t) = \#\{\mathfrak{a}' \in I(\mathfrak{c}) \mid \mathfrak{a}'\mathfrak{a}^{-1} \in P_{\mathfrak{c}},\ \mathrm{Norm}(\mathfrak{a}') \leqslant t\} \quad (6.14)$$

Theorem 6.3.1. *Es ist*

$$j(\mathfrak{c},\mathfrak{a},t)=\frac{2^{r_1+r_2}\pi^{r_2}(U:U_{\mathfrak{c}})R}{w_{\mathfrak{c}}\sqrt{|D_k|}\,2^{s(\mathfrak{c})}\operatorname{Norm}(\mathfrak{c}_0)}t+O(t^{1-1/n}) \tag{6.15}$$

wobei r_1 und r_2 die Anzahl der reellen und komplexen Stellen von K bezeichne, D_K die Diskriminante von K sei und $w_{\mathfrak{c}}$ für die Anzahl der Einheitswurzeln α mit $\alpha\equiv 1 \mod {}^*\mathfrak{c}$ steht.

Weiter ist R der Regulator und $U=\mathcal{O}_K^*$, die Einheitengruppe, mit $U_{\mathfrak{c}}\subseteq U$ als Einheiten in $k_{\mathfrak{c}}$ sowie $s(\mathfrak{c})$ die Anzahl der unendlichen reellen Stellen in $\mathfrak{c}$.

Literaturverzeichnis

[1] Cassels, J.W.S. (ed.); Fröhlich, A. (ed.): *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. London and New York: Academic Press 1967. xv, 366 pp. 100 s. , 1967

[2] Lang, Serge: *Algebraic number theory. 2nd ed.* Graduate Texts in Mathematics. 110. New York: Springer-Verlag. xiii, 357 p. , 1994

Sachverzeichnis