Algebraische und analytische Theorie der Zetafunktion

Inhaltsverzeichnis

Die Riemannsche Zetafunktion: Motivation

1 Algebraische Grundlagen
   1.1 Freie Moduln .......................................................... 1
   1.2 Moduln über Hauptidealringen ...................................... 5
   1.3 Nöthersche Moduln ..................................................... 7
   1.4 Lokalisierung ............................................................ 9
   1.5 Der Chinesische Restsatz ............................................. 15
   1.6 Der ganze Abschluss .................................................. 16
   1.7 Primideale ............................................................... 19
   1.8 Fortsetzung von Homomorphismen .................................. 21

2 Dedekind Ringe
   2.1 Dedekind Ringe ......................................................... 27
   2.2 Diskrete Bewertungsringe .......................................... 31
   2.3 Galois Erweiterungen ............................................... 33
   2.4 Verzweigung von Primidealen ...................................... 37
   2.5 Explizite Faktorisierung einer Primstelle ....................... 41
   2.6 Die Diskriminante ..................................................... 44
   2.7 Quadratische Zahlkörper, Kreisteilungskörper ................. 49

3 Die Riemannsche Zetafunktion: Definition
   3.1 Die Riemannsche Zetafunktion .................................... 61
   3.2 Definition von $\zeta_k$ ............................................... 64

Literaturverzeichnis ............................................................... 67
iv

INHALTSVERZEICHNIS
Die Riemannsche Zetafunktion: Motivation

Aus der Kenntnis des analytischen Verhaltens der Riemannschen Zetafunktion

\[ \zeta_Q(s) = \zeta(s) := \sum_{n \in \mathbb{N}} \frac{1}{n^s}, \text{ Re } s > 1, \]

gewinnt man Aussagen zahlentheoretischer Natur, z.B. über die Verteilung der Primzahlen:

Satz (Primzahlsatz). Sei \( \pi(N) \) die Anzahl der Primzahlen \( p \leq N \). Dann gilt für gewisse Konstanten \( \alpha, \beta > 0 \) (z.B. \( \alpha = 0.1, \beta = 0.01 \))

\[ \pi(N) = \int_2^N \frac{dt}{\log t} + O\left(N e^{-\beta \log N} \right). \]

Insbesondere ist \( \pi(N) \sim \frac{N}{\log N} \).

Einige, relativ einfache, analytische Eigenschaften von \( \zeta_Q \) aus denen man mit Hilfe Tauberscher Sätze solche Aussagen erhalten kann sind:

Satz. (i) Eulersche Produktdarstellung: Für \( \text{Re } s > 1 \) gilt

\[ \zeta_Q(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}. \]

(ii) \( \zeta_Q \) besitzt eine analytische Fortsetzung auf die gesamte rechte Halbebene \( \{ z \in \mathbb{C} : \text{Re } z > 0 \} \) mit Ausnahme des Punktes \( s = 1 \). An der Stelle 1 hat \( \zeta_Q \) einen Pol erster Ordnung mit Residuum 1.

(iii) \( \zeta_Q \) besitzt eine analytische Fortsetzung auf \( \mathbb{C} \setminus \{1\} \), nämlich vermöge der Funktionalgleichung

\[ \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta_Q(s) = \pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \zeta_Q(1-s). \]

Weiters benötigt man für diese genaue Abschätzung des Restgliedes Kenntnis über nullstellenfreie Bereiche der \( \zeta \)-Funktion. Kennt man große nullstellenfreie Bereiche, so kann man die Abschätzung besser machen.

Weiters studiert man auch die Häufigkeit von Primzahlen in arithmetischen Progressionen:
Satz (Page-Siegel-Walfisz). Sei $k \in \mathbb{N}$, $(a, h) = 1$, und bezeichne $\pi(N; k, a) = \# \{ p \text{ prim} : p \leq N, p \equiv a \mod k \}$. Dann gilt

$$
\pi(N; k, a) = \frac{1}{\varphi(k)} \int_2^N \frac{dt}{\log t} + O\left( Ne^{-\beta(\log N)^{\alpha}} \right)
$$

wobei $\varphi$ die Eulersche $\varphi$-Funktion bezeichnet.

Insbesondere erhält man so den

Satz (Dirichlet). Sei $m \in \mathbb{N}$, $M := m\mathbb{Z}$. Dann gilt

$$
\lim_{N \to \infty} \frac{\# \{ p \text{ prim} : p \in M, p \leq N \}}{\# \{ p \text{ prim} : p \leq N \}} = \frac{1}{\varphi(m)}.
$$

Insbesondere gibt es in jeder arithmetischen Folge unendlich viele Primzahlen.

Zum Beweis solcher Aussagen verwendet man nicht nur analytische Eigenschaften der $\zeta$-Funktion, sondern allgemeiner jene sogenannter Dirichletscher $L$-Reihen: Sei $k \in \mathbb{N}$ und $\chi$ ein Charakter $\mod k$, d.h. ein Charakter der Gruppe $(\mathbb{Z}/k\mathbb{Z})^*$ in natürlicher Weise definiert auf $\mathbb{Z}$ ($(a, k) \neq 1 \Rightarrow \chi(a) = 0$). Dann ist die $L$-Reihe definiert als

$$
L_Q(s, \chi) = \sum_{n \in \mathbb{N}} \frac{\chi(n)}{n^s}.
$$

Für den trivialen Charakter $\chi = \chi_0$ erhält man genau $L_Q(s, \chi_0) = \zeta_Q(s) \cdot \Pi_{p \mid k} (1 - \frac{1}{p^s})$.

Satz. Für $\chi \neq \chi_0$ ist $L_Q(s, \chi)$ analytisch für $\Re s > 0$. Für $\chi = \chi_0$ ist $L_Q(s, \chi_0)$ analytisch für $\Re s > 0$ mit Ausnahme eines einfachen Pols bei $s = 1$ mit Residuum $\frac{\chi_0}{\phi(k)}$.

Tatsächlich ist $L_Q(s, \chi)$ für $\chi \neq \chi_0$ ganz und genügt ebenfalls einer Funktionalgleichung.


$$
\mathbb{Q} \rightarrow K \\
\uparrow \quad \uparrow \\
\mathbb{Z} \rightarrow A
$$

Zum Beispiel für $K = \mathbb{Q} (\sqrt{m})$ für $m \in \mathbb{N}$ quadratfrei wäre

$$
A = \mathbb{Z} + \mathbb{Z} \left\{ \sqrt{m} \right\} , \quad m \equiv 2, 3 \mod 4 \\
A = \mathbb{Z} + \mathbb{Z} \frac{\sqrt{m}}{2} , \quad m \equiv 1 \mod 4
$$

Neben den quadratischen Zahlkörpern sind auch die Kreisteilungskörper $\mathbb{Q}(w)$ wobei $W$ eine primitive $m$-te ($m \in \mathbb{N}$) Einheitswurzel ist, fundamentale Beispiele algebraischer Zahlkörper. In dieser Situation wäre

$$
\mathbb{Q} \leftrightarrow \mathbb{Q}(w) \\
\uparrow \quad \uparrow \\
\mathbb{Z} \leftrightarrow \mathbb{Z}[w]
$$
Um Aussagen über die Primelemente von $A$ zu bekommen benützt man wieder die Zetafunktion des Zahlkörpers $K, \zeta_K(s)$, und ihre analytischen Eigenschaften.

Wir werden im wesentlichen immer nur algebraische Zahlkörper betrachten. Zetafunktionen spielen aber auch in anderen Kontexten eine wichtige Rolle.

Sei z.B. $k = GF(q)$. Dann ist die Zetafunktion vom Funktionenkörper $k(x)/k$ gegeben als

$$Z(z) = \frac{1}{1-t} \prod_p \frac{1}{1 - z^{d(p)}}$$

wobei $p$ alle irreduziblen (normierten) Polynome durchläuft.

Satz. Sei $\pi_q(n)$ die Anzahl der irreduziblen (normierten) Polynome vom Grad $\leq N$. Dann gilt

$$\pi_q(N) \sim \frac{q}{q-1} \frac{q^N}{N}.$$  

Eine weitere interessante Situation ist die der algebraischen Funktionenkörper. Sei $K$ ein Körper, $x$ transzendent über $K$. Ein algebraischer Funktionenkörper ist eine endliche Erweiterung $F$ von $K(x)$.

Betrachte z.B. $K = GF(q)$, $char K \neq 2, 3, x$ transzendent über $K$, und ein Element $y$ das über $K(x)$ der Gleichung

$$y^2 = x^3 + ax + b$$

genügt wobei $a, b \in K, 4a^3 + 27b^2 \neq 0$. Dann ist $k(x, y)$ ein algebraischer Funktionenkörper über $K$.

Sei $n \in N$. Man spricht von

$$C_n = \{ (\alpha, \beta) \in GF(q^n)^2 : \beta^2 = \alpha^3 + a\alpha + b \}$$
als einer elliptischen Kurve über $GF(q^n)$. Sei

$$N_n := 1 + \vert C_n \vert$$

Dann ist die Zetafunktion von $K(x, y)/K$ gegeben als jene Potenzreihe $Z(t)$ sodass

$$\frac{Z'}{Z} = \sum_{n=1}^{\infty} N_n t^{n-1}$$

Mit Hilfe des Satzes von Hasse-Weil der besagt daß

$$Z(t) = \frac{(1 - \alpha t)(1 - \beta t)}{(1 - t)(1 - qt)}$$

wobei $|\alpha| = \sqrt{q}$ gilt, und der das genaue Analogon zur Riemannschen Vermutung darstellt, erhält man zum Beispiel

Satz (Hasse-Weil bound). Sei $N(r)$ die Anzahl der Primstellen von $GF(q^r)(x, y)/GF(q^r)$ mit Grad 1. Dann gilt

$$|N(r) - (q^r + 1)| \leq 2q^{r/2},$$

insbesondere also $N(r) \sim q^r$. 

Man sieht daß die Approximationsgüte in $N(r) \sim q^r$ wie $\sqrt{q}$ ist. Analogon beim Primzahlsatz (mit Restglied)

$$\pi(N) = \int_2^N \frac{dt}{\log t} + O\left(N e^{-\beta (\log N)^\alpha} \right)$$

wobei $\beta, \alpha > 0$ klein sind, wäre ”$\alpha$ beliebig klein”.

Kennt man nullstellenfreie Bereiche der Riemannsche Zetafunktion, kann man daraus $\alpha, \beta$ konstieren. Umgekehrt würde eine Nullstelle die nicht auf der kritischen Geraden liegt solcherart Abschätzung zumindest sehr unwahrscheinlich machen.
Kapitel 1

Algebraische Grundlagen

1.1 Freie Moduln

Im folgenden sei $R$ immer ein kommutativer Ring mit Einselement.

Ist $M$ ein $R$-Modul, so heißen $x_1, \ldots, x_n \in M$ linear unabhängig, wenn gilt ($r_1, \ldots, r_n \in R$)

$$\sum_{i=1}^{n} r_i x_i = 0 \Rightarrow r_1 = \ldots = r_n = 0.$$ 

Eine Teilmenge $X \subseteq M$ heißt linear unabhängig wenn jede endliche Teilmenge von $X$ linear unabhängig ist. Eine Teilmenge $X \subseteq M$ heißt Basis wenn sie linear unabhängig ist und $M$ (als $R$-Modul) erzeugt.

1.1.1 Definition. Ein $R$-Modul $M$ heißt frei, wenn er eine Basis besitzt (und $
eq \{0\}$ ist).

Ist zum Beispiel $I$ irgendeine Menge, so ist

$$M = \bigoplus_{i \in I} R$$

frei mit der Basis

$$\{(0, \ldots, 0, 1_{i-te Stelle}, 0, \ldots, 0) : i \in I\}$$

Umgekehrt: Ist $M$ frei mit Basis $\{x_i : i \in I\}$, so gilt

$$M \cong \bigoplus_{i \in I} R.$$

Denn ist $x \in M$, so existieren $a_i, i \in I$, fast alle gleich Null, so daß $x = \sum a_i x_i$. Wegen der linearen Unabhängigkeit sind die $a_i$ eindeutig bestimmt und offenbar gibt es zu jeder Wahl von $a_i$, fast alle $= 0$, ein $x$. Also ist

$$x \mapsto (a_i)_{i \in I}$$

eine Bijektion. Klarerweise respektiert sie die Modulooperationen.
1.1.2 Satz. Sei $M$ ein $R$-Modul. Ist $X \subseteq M$ eine Basis von $M$ so hat man die folgende Eigenschaft ($N$ ist irgendein $R$-Modul)

\[
\begin{array}{c}
\subseteq \\
\varphi \\
\exists \tilde{\varphi} \\
\end{array}
\]

Beweis. Sei $x \in M$. Da $X$ Basis ist existieren eindeutige $a_i$ sodaß

\[ x = \sum a_i x_i. \]

Definiere $\tilde{\varphi}(x) := \sum a_i \varphi(x_i)$.

Jeder Modul $M$ ist Faktor eines freien Moduls. Z.B. von

\[ F = \bigoplus_{x \in M} R. \]

1.1.3 Korollar. (i) Sei $M$ frei mit Basis $X = (x_i)_{i \in I}$. Ist (mit der Notation wie im Satz) $(\varphi(x_i))_{i \in I}$ eine Basis von $N$, so ist $\tilde{\varphi}$ ein Isomorphismus.

(ii) Sind $M_1, M_2$ frei mit Basis $X_1, X_2$ und gilt $|X_1| = |X_2|$ so folgt $M_1 \cong M_2$.

Beweis. 

ad(i): $\tilde{\varphi}$ ist surjektiv da $(\varphi(x_i))_{i \in I}$ ein Erzeugendensystem von $N$ ist. $\tilde{\varphi}$ ist injektiv da $(\varphi(x_i))_{i \in I}$ linear unabhängig ist.

ad(ii): Eine Bijektion $\varphi : X_1 \to X_2$ induziert einen Isomorphismus.

1.1.4 Lemma. Sei $M$ ein freier $R$-Modul mit Basis $(x_i)_{i \in I}$ und sei $a \in R$. Dann gilt

\[ M = \bigoplus_{i \in I} Rx_i, \quad M/aM \cong \bigoplus_{i \in I} Rx_i/ax_i. \]

Es ist $Rx_i/ax_i \cong R/a$, der Modul $M/aM$ ist freier $R/a$-Modul mit Basis $(x_i + aM)_{i \in I}$.

Beweis. Klar ist $M = \bigoplus_{i \in I} Rx_i$. Die kanonische Abbildung

\[ \varphi : M \to \bigoplus_{i \in I} Rx_i/ax_i \]

hat Kern $aM$ denn: Sei $x = \sum a_i x_i$. Dann ist

\[ 0 = \varphi(x) = (a_i x_i + ax_i)_{i \in I}. \]
1.1. FREIE MODULN

genau dann, wenn \( a_i \in a \) für alle \( i \in I \). Weiters ist \( R x_i / a x_i \cong R / a \) vermöge

\[
x x_i + a x_i \mapsto a.
\]

Also ist \( M / a M \) frei mit Basis \((x_i + a M)_{i \in I}\).

\[\square\]

1.1.5 Korollar. Sei \( M \) frei und seien \( X, Y \) Basen von \( M \). Dann gilt \( |X| = |Y| \).

Diese Kardinalität heißt die Dimension von \( M \).

Beweis. Sei \( \mathfrak{m} \) ein maximales Ideal von \( R \) (existiert wegen \( R \) hat Einselement und ist kommutativ). Dann ist

\[
M / \mathfrak{m} M
\]
ein \( R / \mathfrak{m} - \) Vektorraum mit Basen \( \{x + \mathfrak{m} M : x \in X\} \) und \( \{y + \mathfrak{m} M : y \in Y\} \)
also ist \( |X| = |Y| \).

\[\square\]

Ein \( R \)-Modul \( M \) heißt Hauptmodul, wenn er von einem Element erzeugt wird, d.h. \( \exists x \in M : M = Rx \). In diesem Fall ist

\[
M \cong R / \text{Ann}_R \{x\}
\]
wobei \( \text{Ann}_R \{x\} := \{r \in R : rx = 0\} \).

1.1.6 Lemma. Sei \( 0 \to M' \xrightarrow{f} M' \xrightarrow{g} M'' \to 0 \) eine exakte Sequenz von \( R \)-Moduln. Dann sind äquivalent:

(i) \( \exists \varphi : M'' \to M : g \circ \varphi = \text{id} M'' \).

(ii) \( \exists \psi : M \to M' : \psi \circ f = \text{id} M' \).

In diesem Fall ist

\[
M = \text{Im} f \oplus \text{ker} \psi = \ker g \oplus \text{Im} \varphi,
\]

\[
M \cong M' \oplus M''
\]
und man sagt die exakte Sequenz ist split exakt.

Beweis. Es gelte (i): \( M'' \xrightarrow{\varphi} M \xrightarrow{f} M' \to 0 \). Sei \( x \in M \), dann ist

\[
x - \varphi \left( g(x) \right) \in \ker g.
\]

Also folgt \( M = \ker g + \text{Im} \varphi \). Diese Summe ist direkt, denn ist \( x = y + z \) mit \( y \in \ker g \) und \( z \in \text{Im} \varphi \), so folgt

\[
g(x) = g(y + z) = g(\varphi(w)) = w.
\]

Also ist \( w \) und damit \( z \) und damit \( y \) eindeutig bestimmt durch \( x \).

Wir haben also \( M = \ker g \oplus \text{Im} \varphi \). Wegen der Exaktheit ist \( \ker g = \text{Im} f \).

Definieren \( \psi \) wie folgt: Ist \( x = y + z \in M \), \( y = f(u) \), so sei \( \psi(x) := u \). \( \psi \) ist wohldefiniert denn \( f \) ist injektiv und erfüllt offenbar \( \psi \circ f = \text{id} M' \). Weiters ist \( \ker \psi = \text{Im} \varphi \), also \( M = \text{Im} f \oplus \ker \psi \). Weiters ist \( \text{Im} f \cong M' \) und \( g|\text{Im} \varphi \) ein Isomorphismus von \( \text{Im} \varphi \) auf \( M'' \).

Gilt (ii), so schließt man analog.

\[\square\]
1.17 Definition. Ein $R$-Modul $P$ heißt projektiv, wenn gilt ($M,M''$ irgendeine $R$-Module)

\[ \exists h \quad \forall f \quad g \]

Zum Beispiel ist jeder freie Modul projektiv. Denn ist $P$ frei mit Basis $X$ so definiere $h$ auf $X$ so daß $(g \circ h)(x) = f(x)$ (das ist möglich da $g$ surjektiv) und setze $h|X$ zu einem Homomorphismus fort.

1.18 Satz. Es sind äquivalent:

(i) $P$ ist projektiv.

(ii) Jede exakte Sequenz $0 \to M' \to M'' \to P \to 0$ splits.

(iii) $P$ ist direkter Summand eines freien Moduls, d.h. $\exists M : F = P \oplus M$ frei.

Beweis.

(i) $\Rightarrow$ (ii): Die Abbildung aus

\[ \exists h \quad \forall f \quad g \]

liefert das splitting der Sequenz.

(ii) $\Rightarrow$ (iii): Sei $F$ frei so daß $P$ ein Faktor von $F$ ist:

\[ 0 \to M \to F \to P \to 0. \]

Diese Sequenz ist split, also $F \cong P \oplus M$.

(iii) $\Rightarrow$ (i): Sei $F = P \oplus M$ frei (und daher projektiv)
1.2 Moduln über Hauptidealringen

1.2.1 Satz. Sei $F$ freier Modul über dem Hauptidealring $R$ (nullteilerfrei) und $M$ ein Untermodul von $F$. Dann ist $M$ frei und die Dimension von $M$ höchstens so groß wie die von $F$.

**Beweis.**

Ist $x \in F$, $x \neq 0$, so folgt $\text{Ann}_R \{x\} = \{0\}$. Denn sei $(v_i)_{i \in I}$ Basis von $F$, $x = \sum a_i v_i$ und $a_i \neq 0$. Sei $\varphi$ der Homomorphismus $\varphi : F \to R$ mit $v_0 \mapsto 1$, $v_i \mapsto 0$, $i \neq 0$. Ist $r \in \text{Ann}_R \{x\}$, so folgt

$$0 = \varphi(rx) = ra_0.$$ 

Da $R$ nullteilerfrei ist folgt $r = 0$.

Wir betrachten zuerst den Fall das $I$ endlich ist, $I = \{1, \ldots, n\}$. Sei $M_r := M \cap \langle v_1, \ldots, v_r \rangle$. Es ist $M_1 = M \cap \langle v_1 \rangle \subseteq \langle v_i \rangle$ und daher von der Gestalt $M_1 = \langle a_1 v_1 \rangle$ für ein $a_1 \in R$, denn

$$\{a \in R : av_1 \in M_1\}$$

ist ein Ideal von $R$ und daher gleich $(a_1)$. Also ist $M_1$ entweder $= \{0\}$ oder frei mit Dimension $1$.

Sei nun induktiv angenommen, daß $M_r$ frei von Dimension $\leq r$ ist. Sei

$$a := \{a \in R : \exists b_1 v_1 + \ldots + b_r v_r + av_{r+1} \in M\} \triangleleft R,$$

und sei $a = (a_{r+1})$. Ist $a_{r+1} = 0$, so folgt $M_{r+1} = M_r$. Andernfalls sei $w \in M_{r+1}$ so daß $w = b_1 v_1 + \ldots + b_r v_r + a_{r+1} v_{r+1}$. Für jedes $x \in M$ gibt es dann $c \in R$ so daß $x - cw \in M_r$, also folgt

$$M_{r+1} = M_r + \langle w \rangle.$$

Wegen $M_r \cap \langle w \rangle = \{0\}$ ist diese Summe direkt und da $\langle w \rangle$ frei ist folgt daß $M_{r+1}$ frei ist und

$$\dim M_{r+1} = \dim M_r + 1 \leq r + 1.$$
§) Wir kommen zum Fall $|I| = \infty$. Für $J \subseteq I$ bezeichne

\[ F_J := \langle v_i : i \in J \rangle, \ M_J := F_J \cap M. \]

Sei $S$ die Menge aller Paare $(M_J, w)$ so daß $w : J' \subseteq J \rightarrow M_J$ eine Basis von $M_J$ ist. Die Menge $S$ ist nicht leer. Denn sei $J$ endlich so daß $M_J \neq \{0\}$. Dann ist $M_J$ frei mit Dimension $\leq |J|$, d.h. $\exists J' \subseteq J$ und $w : J' \rightarrow M_J$ Basis, d.h. $(M_J, w) \in S$.

Wir definieren für $(M_J, w), \ (M_K, u) \in S$

\[ (M_J, w) \leq (M_K, u) : \iff J \subseteq K, \ J' \subseteq K', \ u|_{J'} = w. \]

Offenbar ist $\leq$ eine Ordnung und jede Kette hat ein Supremum $(\bigcup J)$.

Sei $(M_J, w)$ ein maximales Element von $S$. Wir zeigen $J = I$, denn dann sind wir fertig. Angenommen $J \neq I$. Sei $k \in I \sm J, \ K = J \cup \{k\}$.

Gilt $M_K = M_J$ so ist $(M_K, w) \geq (M_J, w)$, ein WSI. Andernfalls ist

\[ \{0\} \neq \{ c \in R : \exists c_{V_k} + y \in M, y \in M_J \} < R, \]

also gleich (a). Sei $w_k := av_k + y \in M$ (mit einem $y \in M_J$). Genau wie im "endlichen Fall" ist nun

\[ \tilde{w} : \begin{cases} 
K & \to M_K \\
I & \to \begin{cases} 
w(l), & l \in J \\
w_k, & l = k \end{cases} 
\end{cases} \]

eine Basis von $M_K$ und es gilt

\[ (M_K, \tilde{w}) \geq (M_J, w), \]

ein WSI.

\[ \square \]

COAl.10

1.2.2 Korollar. Sei $R$ Hauptidealring. Dann gilt:

(i) $E$ endlich erzeugt und $E' \leq E$. Dann ist $E'$ endlich erzeugt.

(ii) Jeder projektive Modul ist frei.

Beweis.

ad(i): Sei $F$ freier Modul mit endlicher Basis und $\varphi : F \rightarrow E$. Dann ist $\varphi^{-1}(E')$ freier Modul mit endlicher Basis und daher $E' = \varphi(\varphi^{-1}(E'))$ endlich erzeugt.

ad(ii): Ist $P$ projektiv so existiert $M$ so daß $P \oplus M = F$ frei. Es ist also $P \leq F$ ebenfalls frei.

\[ \square \]

Sei $E$ ein $R$-Modul, $x \in E$ heißt Torsionselement, wenn gilt $	ext{Ann}_R\{x\} \neq \{0\}$

$E_{\text{tor}} := \{ x \in E : x \text{ Torsionselement} \}$. Ist $E_{\text{tor}} = E$, so heißt $E$ Torsionsmodul, ist $E_{\text{tor}} = \{0\}$, so heißt $E$ torsionsfrei.
1.3 Nötherische Moduln

1.2.3 Satz. Sei $R$ Hauptidealring, $E$ endlich erzeugter $R$-Modul. Dann ist $E/E_{tor}$ frei. Es existiert $F \leq E$ frei, sodass

$E = E_{tor} \oplus F$.

Die Dimension von $F$ ist eindeutig.

1.2.4 Lemma. Seien $E, E'$ Moduln, $E'$ frei, $f : E \to E'$ surjektiv. Dann existiert $F \leq E$ frei sodass $f|F$ ein Isomorphismus von $F$ auf $E'$ ist und es gilt $E = F \oplus \ker f$.

Beweis. $E'$ ist frei, also auch projektiv. Die exakte Sequenz

$0 \to \ker f \hookrightarrow E \xrightarrow{j} E' \to 0$

ist daher split exakt und es existiert $\varphi : E' \to E$ sodass $f \circ \varphi = \text{id}_{E'}$ und es gilt

$E = \ker f \oplus \text{Im} \varphi$.

Wie in Lemma 1.1.6 gezeigt wurde, ist $f|\text{Im} \varphi$ ein Isomorphismus von $\text{Im} \varphi$ auf $E'$.

Beweis. (Satz 1.2.3):

\(\text{a) } E/E_{tor}\) ist torsionsfrei: Sei $x \in E$, $b \in R \setminus \{0\}$, $b(x + E_{tor}) = 0$. Dann ist $bx \in E_{tor}$, also $\exists c \in R \setminus \{0\} : c(bx) = 0$. Wegen $cb \neq 0$ folgt $x \in E_{tor}$.

\(\text{b) }$ Wir zeigen: Jeder endlich erzeugte torsionsfreie Modul $M$ ist frei: Sei $\{y_1, \ldots, y_m\}$ ein Erzeugendensystem von $M$ und wähle eine maximale lineare unabhängige Teilmenge $\{v_1, \ldots, v_n\}$ von $\{y_1, \ldots, y_m\}$. Hier ist $n \geq 1$, denn $M$ ist torsionsfrei. Für jedes $j = 1, \ldots, m$ gibt es $a_j \in R \setminus \{0\}$, sodass

$\langle a_j y_j \rangle \subseteq \langle v_1, \ldots, v_n \rangle$.

Setze $a := a_1 \cdot \ldots \cdot a_m$, dann gilt also $aM \subseteq \langle v_1, \ldots, v_m \rangle$ und daher $aM$ frei. Nun ist $aM$ torsionsfrei ist, $x \mapsto ax$ ein Isomorphismus von $M$ auf $aM$.

\(\text{c) }$ Wir haben gezeigt $E/E_{tor}$ ist frei. Die Zerlegung $E = E_{tor} \oplus F$ folgt wegen Lemma 1.2.4.

\(\text{\square}\)

1.3 Nötherische Moduln

1.3.1 Satz. Sei $M$ ein $A$-Modul. Dann sind äquivalent.

(i) Jeder Untermodul von $M$ ist endlich erzeugt.

(ii) Jede aufsteigende Folge $M_1 \subseteq M_2 \subseteq \ldots$ von Untermoduln von $M$ ist endlich.

(iii) Jede nichtleere Menge von Untermoduln von $M$ hat ein maximaes Element.
In diesem Fall nennt man $M$ nötherschen $A$-Modul.

**Beweis.**
(i) $\Rightarrow$ (ii): Sei $N = \bigcup_i M_i \leq M$ und daher endlich erzeugt, $N = \langle x_1, \ldots, x_n \rangle$. Also existiert $i$ mit $x_1, \ldots, x_n \in M_i$ und daher $N = M_i$.
(ii) $\Rightarrow$ (iii): Angenommen es gibt eine Menge von Untermoduln ohne maximales Element. Dann erhält man induktiv

$$N_1 \subset N_2 \subset N_3 \subset \ldots$$

ein WS!
(iii) $\Rightarrow$ (i): Sei $N \leq M$ gegeben, $a_0 \in N$. Ist $N \neq \langle a_0 \rangle$ wähle $a_1 \in N \setminus \langle a_0 \rangle$. Ist $N \neq \langle a_0, a_1 \rangle$ wähle $a_2 \in N \setminus \langle a_0, a_1 \rangle$, u.s.w. Wir erhalten

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \ldots$$

und diese Menge hat kein maximales Element.

\[ \Box \]

**LEAI.14**

**1.3.2 Lemma.** Sei $M$ nötherscher $A$-Modul. Dann ist jeder Untermodul und jeder Faktormodul von $M$ auch nöthersch.

**Beweis.** Für Untermoduln klar wegen (i). Für Faktormoduln wegen (ii), denn ist $\pi : M \rightarrow N$ surjektiv, so ist mit einer echt aufsteigenden Kette

$$N_1 \subset N_2 \subset \ldots \subset N$$

auch

$$\pi^{-1}(N_1) \subset \pi^{-1}(N_2) \subset \ldots \subset M.$$ 

\[ \Box \]

**LEAI.15**

**1.3.3 Lemma.** Sei $N \leq M$. Sind $N$ und $M/N$ nöthersch, so auch $M$.

**Beweis.** Mit $L \leq M$ assoziere das Paar

$$L \mapsto (L \cap N, (L + N)/N).$$

Diese Zuordnung bildet echte Ketten auf echte Ketten ab: Sei $E \subset F$ und seien die assoziierten Paare gleich. Sei $x \in F$, dann existieren wegen $(E + N)/N = (F + N)/N$ Elemente $u, v \in N$, $y \in E$, so daß

$$x + u = y + v.$$ 

Es folgt $x - y = u - v \in F \cap N = E \cap N$, also $x \in E$. 

\[ \Box \]

**COAI.16**

**1.3.4 Korollar.** Endliche Summen nötherscher Moduln sind nöthersch.

**Beweis.** Mit $N_1, N_2$ ist auch $N_1 \oplus N_2$ nöthersch, denn $\pi_1 : N_1 \oplus N_2 \rightarrow N_1$, hat Kern $N_2$. Ist $M = N_1 + N_2$, so hat man $N_1 \oplus N_2 \rightarrow M$. Rest induktiv.

\[ \Box \]

Ein Ring $A$ heißt nöthersch, wenn er ein nötherscher Modul über sich selbst ist. D.h. jedes Ideal ist endlich erzeugt.
1.4. LOKALISIERUNG

1.3.5 Lemma. Sei $A$ nöthersch. Es gilt:

(i) Ist $M$ endlich erzeugter $A$-Modul, so ist auch $M$ nöthersch.

(ii) Ist $\varphi : A \to B$ surjektiver Ring ($!)$ Homomorphismus, so ist $B$ nöthersch.

(iii) Sei $S \subseteq A$ multiplikativ. Dann ist $S^{-1}A$ nöthersch.

Beweis.

ad(i): Es gibt einen surjektiven Homomorphismus $A^n \to M$.

ad(ii): Sei $b_1 \subseteq \ldots \subseteq b_n \subseteq \ldots \subseteq B$, dann ist $\varphi^{-1}(b_1) \subseteq \ldots \subseteq \varphi^{-1}(b_n) \subseteq \ldots \subseteq A$.

ad(iii): Ist $b_1 \subseteq \ldots \subseteq b_n \subseteq \ldots \subseteq S^{-1}A$ und schreibt man $b_i = S^{-1}a_i$ so ist $a_1 \subseteq \ldots \subseteq a_n \subseteq \ldots \subseteq A$ eine echte Kette.

\[\square\]

1.4 Lokalisierung

Sei $A$ ein Ring, $S \subseteq A$ eine multiplikative Teilmenge, d.h.

\[s_1, s_2 \in S \Rightarrow s_1 \cdot s_2 \in S\]

Wir definieren eine Relation $\sim$ auf $A \times S$ durch

\[(a_1, s_1) \sim (a_2, s_2) \ : \iff \exists t \in S : ta_2 s_1 = ta_1 s_2\]

1.4.1 Satz. Die Relation $\sim$ ist eine Äquivalenzrelation. Die Menge $S^{-1}A := (A \times S)/\sim$ ist mit den Operationen

\[(a_1, s_1) + (a_2, s_2) := (a_1 s_2 + a_2 s_1, s_1 s_2),\]

\[(a_1, s_1) \cdot (a_2, s_2) := (a_1 a_2, s_1 s_2)\]

ein Ring, der sogenannte Quotientenring von $A$ nach $S$. Das Element $(a, s)$ wird oft mit $a_s$ bezeichnet.

Beweis. Klar durch nachrechnen.

\[\square\]

Ein echtes Ideal $p \triangleleft A$ eines Ringes $A$ heißt Primideal, wenn gilt:

\[x \cdot y \in p \Rightarrow (x \in p \lor y \in p),\]

oder, äquivalent, wenn $A \setminus p$ multiplikativ ist oder, ebenfalls äquivalent, wenn $A/p$ multteilerfrei ist. Die Menge aller Primideale von $A$ heißt das Spektrum von $A$ und wird bezeichnet mit $\text{Spec}A$.

Der Ring $A$ habe ein Einselement, dann heißt ein Element $x \in A$ Einheit, wenn es ein $y \in A$ gibt mit $xy = yx = 1$. Die Menge $A^*$ der Einheiten bildet eine Gruppe, die sogenannte Einheitengruppe des Ringes $A$. 

1.4.2 Bemerkung. (i) Enthält \( S \) keine Nullteiler, so gilt
\[
(a_1, s_1) \sim (a_2, s_2) \iff a_1 s_2 = a_2 s_1
\]
(ii) Habe \( A \) ein Einselement. Die Abbildung
\[
\iota_{A,S} : \begin{cases}
A & \to S^{-1}A \\
\quad a & \mapsto (a, 1)
\end{cases}
\]
is ein Ringhomomorphismus. Sie ist genau dann injektiv wenn \( S \) keine Nullteiler enthält. Ist insbesondere \( A \) nullteilerfrei, so ist \( S^{-1}A \) ein Unterring des Quotientenkörpers \( Q(A) \) von \( A \) (vgl. Korollar 1.4.4).

(iii) Beispiele:
(a) \( A \) nullteilerfrei, \( S = A \setminus \{0\} \). Dann ist \( S^{-1}A = Q(A) \).
(b) Ist \( S \subseteq A^* \), dann ist \( \iota_{A,S} \) ein Isomorphismus.
(c) \( 0 \in S \). Dann ist \( S^{-1}A \cong \{0\} \).
(d) Sei \( p \in \text{Spec}A \) und setze \( S := A \setminus p \). Dann heißt
\[
A_p := S^{-1}A = (A \setminus p)^{-1}A
\]
die Lokalisierung von \( A \) in \( p \) (oder an der Stelle \( p \)).

1.4.3 Satz. Sei \( S \subseteq A \) multiplikativ, \( \phi : A \to B \) ein Ringhomomorphismus mit \( \phi(S) \subseteq B^* \). Dann gibt es einen eindeutigen Ringhomomorphismus \( \psi : S^{-1}A \to B \) mit
\[
\begin{array}{ccc}
A & \xrightarrow{\iota_{A,S}} & S^{-1}A \\
\quad \phi & \downarrow & \\
\quad \psi & \downarrow & B
\end{array}
\]
d.h. mit \( \phi = \psi \circ \iota_{A,S} \).

Beweis. Definiere
\[
\psi\left(\frac{a}{s}\right) := \phi(a)\phi(s)^{-1}
\]
Rest klar durch nachrechnen.

1.4.4 Korollar. Seien \( S \subseteq T \) zwei multiplikative Teilmengen von \( A \). Dann gibt es einen kanonischen Homomorphismus \( \iota_{S,T} : S^{-1}A \to T^{-1}A \) so daß
Im folgenden sei immer $A$ kommutativer Ring mit Einselement.
Allgemein gilt bezüglich der Idealstruktur von $S^{-1}A$ der folgende Satz:

1.4.5 Satz. Bezeichne für ein Ideal $a$ mit $S^{-1}a$ die Menge
$$S^{-1}a := \{\frac{a}{s} : a \in a, s \in S\}$$
Dann gilt

(i) $S^{-1}a$ ist ein Ideal von $S^{-1}A$. Ist $a \cap S \neq \emptyset$, so gilt $S^{-1}a = S^{-1}A$.
(ii) Ist $b$ Ideal von $S^{-1}A$ und $a := \iota_{A,S}(b)$, so gilt
$$b = S^{-1}a.$$ 

Die in obigem Sinne definierte Abbildung $\Psi$ die dem Ideal $a$ von $A$ das Ideal $S^{-1}a$ von $S^{-1}A$ zuordnet induziert eine ordnungserhaltende Bijektion von $\{p \in \operatorname{Spec} A : p \cap S = \emptyset\}$ auf $\operatorname{Spec} S^{-1}A$. Es gilt für $p \in \operatorname{Spec} A, p \cap S = \emptyset$ stets
$$\iota_{A,S}(S^{-1}p) = p.$$ 

Beweis.

ad (i): klar.

ad (ii): Ist $a \in a$, so folgt $\frac{a}{1} \in b$ und damit $\frac{a}{s} \in b$ für jedes $s \in S$. Sei $\frac{b}{1} \in b$, dann folgt auch $\frac{b}{s} \in b$ für jedes $s \in S$. Es gilt $\frac{b}{s} \in b$, daher $b \in a$.

Klarerweise ist $\Psi$ ordnungserhaltend.

Sei $p \in \operatorname{Spec} A, p \cap S = \emptyset$ und sei
$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a}{s} \in S^{-1}p,$$
d.h. $\frac{a_1}{s_1}, \frac{a_2}{s_2} \in S^{-1}p$. Dann existiert $t \in S$ mit $ta_1a_2s = tsp_1s_2 \in p$. Es folgt das eines von $a_1, a_2$ in $p$ sein muss.

Sei $q \in \operatorname{Spec} S^{-1}A$. Dann ist $\iota_{A,S}^{-1}(q) \in \operatorname{Spec} A$ da $\iota_{A,S}$ ein Ringhomomorphismus ist.

Sei $p \in \operatorname{Spec} A$. Klar ist $p \subseteq \iota_{A,S}^{-1}(S^{-1}p)$. Sei $x \in A$ mit $\frac{x}{s} \in S^{-1}p$, d.h. $\frac{x}{s} \in S^{-1}p$. Dann folgt für ein gewisses $t \in S$ daß $txs = tsp \in p$, also folgt $x \in p$.  

\[\square\]
1.4.6 Korollar. Es gilt: Ist $A$ Hauptidealing, so auch $S^{-1}A$.

Beweis. Sei $b$ ein Ideal von $S^{-1}A$. Dann gilt $b = S^{-1}a$ mit $a = \iota_{A,S}^{-1}b$. Sei $a = (a)$, dann gilt $b = S^{-1}(a) = S^{-1}A : \frac{1}{a}$.

\hfill$\square$

1.4.7 Definition. Ein Ring heißt lokal, wenn er genau ein maximales Ideal besitzt.

1.4.8 Korollar. (i) Sei $p \in \text{Spec} A$. Dann ist $A_p$ lokal mit maximalem Ideal

$$pA_p := \{\frac{p}{s} : p \in p, s \in A \setminus p\} = \iota_{A,A_p}(p)A_p.$$

(ii) Sei $A$ Hauptidealing und $p \in A$ ein Primelement. Dann ist $A_{(p)}$ ein Hauptidealing mit im wesentlichen (d.h. bis auf Einheiten) genau einem Primelement.

1.4.9 Satz. Sei $S \subseteq A$ multiplikativ, $a$ ein Ideal von $A$ und $\pi : A \rightarrow A/a$ die kanonische Projektion. Der kanonische Homomorphismus (vgl. Satz 1.4.3) $\psi : S^{-1}A \rightarrow \pi(S)^{-1}(A/a)$ ist surjektiv und hat Kern $S^{-1}a$. Insbesondere ist also

$$(S^{-1}A)/(S^{-1}a) \cong \pi(S)^{-1}(A/a).$$

Beweis. Betrachte die Homomorphismen.

\begin{center}
\begin{tikzcd}
A \ar{r}{\pi} & A/a \ar{r}{\iota_{A,a,\pi(S)}} & \pi(S)^{-1}(A/a) \\
& S^{-1}A \ar{u}{\iota_{A,S}} \ar{ur}{\psi}
\end{tikzcd}
\end{center}

Jedes Element von $\pi(S)^{-1}(A/a)$ ist von der Gestalt $\frac{\pi(a)}{\pi(s)}$ für gewisse $a \in A$, $s \in S$. Es ist unter $\psi$ also Bild von $\frac{a}{s}$. Ist $\frac{\pi(a)}{\pi(s)} = 0$, so existiert $t \in S$ mit $\pi(t) \cdot \pi(a) = 0$, also $ta \in a$. Damit ist $\frac{a}{s} = \frac{ta}{ts} \in S^{-1}a$.

\hfill$\square$

1.4.10 Korollar. Ist $p \in \text{Spec} A$, so ist $A_p/pA_p \cong Q(A/p)$.

Beweis. Klar.

\hfill$\square$

Sei nun $M$ ein $A$-Modul und $S \subseteq A$ multiplikativ. Definiere die Relation $\sim$ auf $S \times M$ durch

$$(s_1,m_1) \sim (s_2,m_2) :\Leftrightarrow \exists t \in S : ts_1m_2 = ts_2m_1.$$

Dann ist $S^{-1}M := (S \times M)/\sim$ mit den kanonischen Operationen ein $S^{-1}A$-Modul.
1.4. LOKALISIERUNG

Ref. 11

1.4.11 Bemerkung. (i) Vermöge $\iota_{A,S} : A \to S^{-1}A$ ist $S^{-1}M$ auch ein $A$-Modul.

(ii)

$$
\iota_{M,S} : \begin{cases} 
M & \to S^{-1}M \\
n & \mapsto \frac{n}{m} 
\end{cases}
$$

ist ein $A$-Modul Homomorphismus.

(iii) $\iota_{A,S}$ ist genau dann injektiv, wenn $S$ aus Nichtnullteilkern für $M$ besteht (d.h. $sm \neq 0$ für alle $s \in S$, $m \in M \setminus \{0\}$).


(v) Es gilt (Satz vom Hauptnemer)

$$
S^{-1}\left( \sum_{i \in I} M_i \right) \cong \sum_{i \in I} S^{-1}M_i.
$$

(vi) Ist $p \in \text{Spec} A$, so bezeichne $M_p$ den $A_p$-Modul $(A \setminus \{0\})^{-1}M$.

(vii) Ist $a$ ein Ideal von $A$, so erhalten wir die bekannte Definition von $S^{-1}a$.

1.4.12 Satz. Seien $M, N$ $A$-Module, $S \subseteq A$ multiplikativ, $\phi : M \to N$ $A$-linear. Dann gibt es genau eine $S^{-1}A$-lineare Abbildung $(S^{-1}\phi) : S^{-1}M \to S^{-1}N$ sodass

\[
\begin{array}{ccc}
M & \xrightarrow{\phi} & N \\
\downarrow & & \downarrow \\
S^{-1}M & \xrightarrow{\iota_{M,S}} & S^{-1}M \\
\downarrow & & \downarrow \\
S^{-1}\phi & \xrightarrow{\iota_{N,S}} & S^{-1}N
\end{array}
\]

Es gilt $S^{-1}\text{id}_M = \text{id}_{S^{-1}M}$ und

$$
S^{-1}(\phi \circ \psi) = (S^{-1}\phi) \circ (S^{-1}\psi).
$$

Beweis. Definiere $(S^{-1}\phi)((\frac{m}{a})) := \frac{\phi(m)}{a}$. Rest durch nachrechnen.

1.4.13 Satz. Sei $S \subseteq A$ multiplikativ. Ist

$$
M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3
$$

Dann ist $M_2 \xrightarrow{\beta \circ \alpha^{-1}} M_3$

$\square$
Kapitel 1. Algebraische Grundlagen

Eine exakte Folge von $A$-Modul Homomorphismen, so ist auch

$$S^{-1}M_1 \xrightarrow{S^{-1}\alpha} S^{-1}M_2 \xrightarrow{S^{-1}\beta} S^{-1}M_3$$

exakt.

Beweis. $(S^{-1}\beta) \circ (S^{-1}\alpha) = S^{-1}(\beta \circ \alpha) = S^{-1}(0) = 0$. Sei $\alpha \in \text{Kern } S^{-1}\beta$. Dann existiert also $t \in S$ mit $t\beta(m) = 0$, d.h. $\beta(tm) = 0$. Sei $n \in M_1$ mit $\alpha(n) = tm$, dann ist

$$(S^{-1}\alpha)\left(\frac{n}{ts}\right) = \frac{\alpha(n)}{st} = \frac{tm}{ts} = \frac{m}{s}.$$

\[\square\]

1.4.14 Korollar. Ist $U$ ein Untermodul von $M$, so gilt

$$(S^{-1}M)/(S^{-1}U) \cong S^{-1}(M/U).$$

1.4.15 Satz (Lokal-Global-Prinzip). Es gilt:

(i) $M = 0 \iff M_m = 0$ für alle maximalen Ideale $m$ von $A$

(ii) Die $A$-lineare Abbildung $\phi : M \to N$ ist genau dann injektiv (surjektiv, Null), wenn für jedes maximale Ideale $m$ von $A$ die $A_m$-lineare Abbildung $\phi_m : M_m \to N_m$ diese Eigenschaft hat.

(iii) Sei $U$ ein Untermodul von $M$, $x \in M$. Dann ist $x \in U$ genau dann wenn $\iota_{M,A\setminus m}(x) \in U_m$ für alle maximalen Ideale $m$.

(iv) Ist $A$ nullteilerfrei und faßt man $A_m$ auf als Unterring von $Q(A)$, so gilt

$$A = \bigcap_mA_m.$$

Beweis.

ad(i): \iff klar. Angenommen $M \neq 0, m \in M \setminus \{0\}$. Setze $N := A_m \subseteq M$, dann ist $N_m \subseteq M_m$ für jedes $m$. Sei $a$ jedes Ideal von $A$ mit $N \cong A/a$ und wähle ein maximales Ideal $m \supseteq a$. $P := A/\alpha_.$ Der kanonische Homomorphismus $N \to P$ ist surjektiv, also ist auch $N_m \to P_m$ surjektiv. Es genügt zu zeigen $P_m \neq 0$.

Alle Elemente von $A \setminus m$ sind Nichtnullteiler für $P$ denn $A/m$ ist ein Körper. Also ist $\iota_{P,A\setminus m} : P \to P_m$ injektiv. Da $P \neq 0$ folgt $P_m \neq 0$.

ad(ii): \implies wegen Satz 1.4.13, denn $\phi$ injektiv \iff $0 \to M \xrightarrow{\phi} N$, $\phi$ surjektiv \iff $M \xrightarrow{\phi} N \to 0$, $\phi = 0$ \iff $M \xrightarrow{\phi} N \cong N$.

\iff: Injektiv: Setze $K = \ker \phi$, dann hat man $0 \to K \to M \xrightarrow{\phi} N$. Also auch $0 \to K_m \to M_m \cong N_m$. Wegen $\phi_m$ injektiv folgt $K_m = 0$, also wegen (i) $K = 0$.

Surjektiv: Setze $K = \ker \phi$ und verwende genauso $M \xrightarrow{\phi} N \to K \to 0$.

Null: Sei wieder $K = \ker \phi$. Wegen $0 \to K \to M \cong N$ folgt $0 \to K_m \to M_m \cong N_m$ d.h. $K_m = M_m$. Wegen $(M/K)_m \cong M_m/K_m$ also $(M/K)_m = 0$, also $M/K = 0$. 

1.5. DER CHINESISCHE RESTSATZ

ad(iii): Sei
\[ \phi : \begin{cases} A & \to M/U \\ 1 & \mapsto x + U. \end{cases} \]
Dann ist \( \phi = 0 \iff x \in U. \)

Nach (ii) genau dann wenn \( \phi_m : A_m \to (M/U)_m \cong M_m/U_m \) gleich 0 für alle \( m. \)
Wegen \( \phi_m(1) = \frac{1}{m} + U_m \) ist das das Gewünschte.

ad(iv): Faßt man \( A_m \subseteq Q(A) \) auf, so ist \( \frac{1}{m} \) gleich \( x. \)

1.5 Der Chinesische Restsatz

Sind \( a_i \in I, \) Ideale von \( A, \) so ist das kleinste Ideal das alle \( a_i \) umfaßt
\[ \sum_{i \in I} a_i = \left\{ \sum_{i \in I} x_i : x_i \in a_i, x_i = 0 \text{ für f.a. } i \right\} \]
Sind \( a, b \) Ideale, so ist \( a \cdot b \) das Ideal das von den Produkten \( x \cdot y, x \in a, y \in b, \)
erzeugt wird. Es gilt \( ab \subseteq a \cap b \) aber i.a. nicht =. Gilt \( a + b = A, \) so heißen \( a, b \)
coprime.

1.5.1 Lemma. Es gilt

(i) Sind \( a, b \) coprim so ist \( ab = a \cap b. \)
(ii) Sind \( a, b \) und \( a, c \) coprim, so auch \( a, bc. \)

(ii) Gilt \( a_1 + \cdots + a_n = A, \) und sind \( \nu_1, \ldots, \nu_n \in \mathbb{N}, \) so ist auch \( a_1^{\nu_1} + \cdots + a_n^{\nu_n} = A. \)

(iv) Sind \( a_1, \ldots, a_n \) paarweise coprim so gilt \( a_1 \cdot \cdots \cdot a_n = \bigcap_{i=1}^{n} a_i \)

Beweis.

ad(i): \( a \cap b = (a + b)(a \cap b) = a(a \cap b) + b(a \cap b) \subseteq ab. \)

ad(ii): Sei \( a \in a, b \in b \) sodaß \( a + b = 1 \) und \( a' \in a, c \in c \) sodaß \( a' + c = 1. \)
Dann folgt \( bc \in bc = (1-a)(1-a') = 1+[-a-a'+aa'] \in 1 + a. \)

ad(iii): Gilt \( a_1^{\nu_1} + (a_2^{\nu_2} + \cdots + a_n^{\nu_n}) = A, \) so erst recht \( a_1 + (a_2^{\nu_2} + \cdots + a_n^{\nu_n}) = A. \)
Wegen (ii) folgt \( a_1^{\nu_1+1} + a_2^{\nu_2} + \cdots + a_n^{\nu_n} = A. \)

Die Behauptung folgt also mittels Induktion.

ad(iv): Induktion unter Verwendung von (i), (ii).

Für Ideale \( a_1, \ldots, a_n \) sei \( \phi \) der kanonische Homomorphismus
\[ \phi : \begin{cases} A & \to \prod_{i=1}^{n} (A/a_i) \\ a & \mapsto (a + a_1, \ldots, a + a_n) \end{cases} \]
Offenbar gilt \( \ker \phi = \bigcap_{i=1}^{n} a_i. \)
1.5.2 Satz (Chinesischer Restsatz). \( \phi \) ist surjektiv genau dann, wenn die \( a_1, \ldots, a_n \) paarweise coprim sind.

Beweis. \( \Rightarrow \): Sei \( a \in A \) so daß \( \phi(a) = (1, 0, \ldots, 0) \). Dann gilt \( 1 = (1 - a) + a \in a_1 + a_k \) für \( k = 2, \ldots, n \).

\( \Leftarrow \): Seien \( a_i \in a_1, b_i \in a_i, i = 2, \ldots, n \), so daß \( a_i + b_i = 1 \). Setze \( a = \prod_{i=2}^{n} b_i \in a_2 \cap \ldots \cap a_n \). Es gilt

\[
a = \prod_{i=2}^{n} (1 - a_i) = 1 + a'
\]

für ein gewisses \( a' \in a_1 \), also folgt \( \phi(a) = (1, 0, \ldots, 0) \).

Anders formuliert erhält man: Seien \( a_1, \ldots, a_n \) paarweise coprim, und sind \( b_1, \ldots, b_n \in A \), so existiert ein \( x \in A \) mit

\[
x \equiv b_i \text{ mod } a_i, \ i = 1, \ldots, n.
\]

1.6 Der ganze Abschluss

Ab jetzt: Ring = Integritätsbereich.

1.6.1 Definition. Sei \( A \) ein Ring, \( L \) ein Körper mit \( L \supseteq A \), und \( x \in L \). Dann heißt \( x \) ganz über \( A \) wenn \( x \) einer Gleichung der Gestalt

\[
x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, a_i \in A,
\]

genügt. Eine Ringerweiterung \( A \subseteq B \) heißt ganz, wenn jedes Element von \( B \) ganz über \( A \) ist.

1.6.2 Satz. Es gilt:

(i) Sei \( A \subseteq L, x \in L \). Dann ist \( x \) ganz über \( A \) genau dann, wenn es einen endlich erzeugten \( A \)-Modul \( M \subseteq L, M \neq \{0\} \), gibt, so daß \( xM \subseteq M \).

(ii) Sei \( K = Q(A), x \) algebraisch über \( K \). Dann gibt es \( c \in A, c \neq 0 \), so daß \( cx \) ganz über \( A \) ist.

(iii) Sei \( B \supseteq A \) ganz. Ist \( B \) endlich erzeugt als \( A \)-Algebra, so ist \( B \) endlich erzeugt als \( A \)-Modul.

(iv) Sei \( A \subseteq B \subseteq C \). Ist \( B \) ganz über \( A \) und \( C \) ganz über \( B \), so ist \( C \) ganz über \( A \).

(v) Sei \( A \subseteq B \) ganz, \( \sigma \) ein Homomorphismus von \( B \). Dann ist \( \sigma(B) \) ganz über \( \sigma(A) \).

(vi) Sei \( A \subseteq B \) ganz, \( S \subseteq A \) multiplikativ. Dann ist \( S^{-1}A \subseteq S^{-1}B \) ganz.

Beweis.\( \Rightarrow \): Der von \( \{1, \ldots, x^n-1\} \) erzeugte \( A \)-Modul hat die gewünschten Eigenschaften.
1.6. DER GANZE ABSCHLUSS

\[ \iff: \text{Sei } M = v_1 A + \ldots + v_n A \text{ mit } M \neq 0, xM \subseteq M. \text{ dann gibt es } a_{ij} \in A \text{ mit } \]
\[ x v_1 = a_1 v_1 + \cdots + a_1 v_n \]
\[ \vdots \]
\[ x v_n = a_n v_1 + \cdots + a_n v_n \]

Es folgt
\[ \det \begin{pmatrix} x - a_1 & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_m & \cdots & x - a_{nm} \end{pmatrix} = 0 \]

und wir haben eine Ganzheitsgleichung.

\[ \ad(ii): \text{ Sei } a_n x^n + \cdots + a_0 = 0 \text{ mit } a_i \in A, a_n \neq 0. \text{ Dann folgt } \]
\[ (a_n x)^n + \cdots + a_n a_1 (a_n x) + a_n a_0 = 0, \]

also ist \( a_n x \) ganz über \( A \).

\[ \ad(iii): \text{ Induktion nach der Anzahl der Erzeugenden: Sei } B = A[x]. \text{ Ist } x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \text{ eine Ganzheitsgleichung, so ist } \{1, \ldots, x^{n-1}\} \text{ ein } A-\]

Modul-Erzeugendensystem von \( B \).

Sei \( B = A[x_1, \ldots, x_{k+1}] \). Nach Induktionsvoraussetzung ist \( A[x_1, \ldots, x_k] \) endlich erzeugter \( A \)-Modul. Klarerweise ist \( B \) ganz über \( A[x_1, \ldots, x_k] \), also nach Induktionsannahme endlich erzeugter \( A[x_1, \ldots, x_k] \)-Modul.

\[ \ad(iv): \text{ Sei } x \in C, x^n + b_{n-1} x^{n-1} + \cdots + b_0 = 0 \text{ eine Ganzheitsgleichung über } B. \]

Sei \( B_1 = A[b_0, \ldots, b_{n-1}] \), dann ist \( B_1 \) ein endlich erzeugter \( A \)-Modul wegen \( (iii) \). \( B_1[x] \) ist ein endlich erzeugter \( B_1 \)-Modul also auch endlich erzeugter \( A \)-Modul und \( x B_1[x] \subseteq B_1[x] \).

\[ \ad(v): \text{ Eine Ganzheitsgleichung geht bei Anwendung von } \sigma \text{ wegen } \sigma(1) = 1 \text{ in eine } \]

Ganzheitsgleichung über.

\[ \ad(vi): \text{ Sei } x \in B, s \in S. \text{ Sei } M \text{ ein endlich erzeugter } A \text{-Modul mit } x M \subseteq M. \]

Dann ist \( S^{-1} M \) endlich erzeugter \( S^{-1} A \)-Modul und \( x S^{-1} M \subseteq S^{-1} M \).

\[ \square \]

\textit{Definition.} Sei \( A \subseteq L \). Die Menge \( B = \{ x \in L : x \text{ ganz über } A \} \) heißt

der ganze Abschluß von \( A \) in \( L \).

\( A \) heißt ganz abgeschlossen in \( L \) falls \( B = A \). \( A \) heißt ganz abgeschlossen, wenn \( A \) ganz abgeschlossen in \( Q(A) \).

\textit{Satz.} Sei \( A \subseteq L, B \) der ganze Abschluß von \( A \) in \( L \). Dann ist \( B \) ein \( A \text{-Ring. } B \text{ ist ganz abgeschlossen in } L \).

\textit{Beweis.} Seien \( x, y \in B, M, N \subseteq L \) zwei endlich erzeugte \( A \)-Moduln mit \( x M \subseteq M, y N \subseteq N \). Dann ist \( NM \) endlich erzeugter \( A \)-Modul und \( (x \pm y) NM \subseteq NM, (xy) NM \subseteq NM \). \( x \) ist ganz über \( B \) \( \Rightarrow \) ganz über \( A \) \( \Rightarrow \) \( x \in B \).

\[ \square \]
1.6.5 Korollar. Sei $A$ ein Ring, $K = Q(A)$ und $L$ eine endliche separable Erweiterung von $K$. Ist $x \in L$ ganz über $A$, so ist $L/K$-Norm und $L/K$-Spur von $x$ (sowie auch alle anderen Koeffizienten des Minimalpolynoms von $x$ über $K$) ganz über $A$.

Beweis. Sei $\sigma$ ein Homomorphismus von $L$ über $K$. Dann ist $\sigma(x)$ ganz über $\sigma(A) = A$. Damit sind auch alle Polynome in den $\sigma(x)$, insbesondere also die elementarsymmetrischen Funktionen ganz über $A$. \hfill $\square$


(ii) Sei $A$ ZPE, dann ist $A$ ganz abgeschlossen.


(iv) Ist $A$ ganz abgeschlossen in $L$, so auch $S^{-1}A$.

(v) Ist $B$ der ganze Abschluss von $A$ in $L$, dann ist $S^{-1}B$ der ganze Abschluss von $S^{-1}A$ in $L$.

Beweis.

$\text{ad}(i)$: Da $A$ nöthersch ist genügt es zu zeigen, daß $B$ in einem endlich erzeugten $A$-Modul enthalten ist.

Sei $w_1, \ldots, w_n$ eine VR-Basis von $L$ über $K$. Nach Multiplikation mit geeigneten Elementen aus $A$ sei $\operatorname{obd} A w_i \in B$. Die $L/K$-Spur $\text{Tr} : L \to K$ ist $K$-linear und $\neq 0$. Ist $\alpha \in L$, $\alpha \neq 0$, so ist $\text{Tr}(\alpha x) \in L^d$ und $\alpha \mapsto \text{Tr}(\alpha x)$ ist ein $K$-Homomorphismus von $L$ nach $L^d$. Sein Kern ist 0, also ist $L \cong L^d$ unter $\alpha \mapsto \text{Tr}(\alpha x)$. Sei $w'_1, \ldots, w'_n$ die duale Basis bezgl $\text{Tr}(xy)$, d.h.

$$\text{Tr}(w_j w'_j) = \delta_{ij},$$

und sei $c \in A$ so daß $w'_j c \in B$.

Sei $z \in B$, dann ist $zw'_j c \in B$ und damit $\text{Tr}(zw'_j c) \in A$ da $A$ ganz abgeschlossen ist. Sei

$$z = b_1 w_1 + \cdots + b_n w_n, b_j \in K,$$

dann ist also $\text{Tr}(zw'_j c) = cb_j \in A$. Also gilt

$$z \in Ac^{-1} w_1 + \cdots + Ac^{-1} w_n.$$

$\text{ad}(ii)$: Sei $\frac{a}{b} \in Q(A)$ ganz und sei $p$ ein Primelement, $p|b$. Es gilt für gewisse $a_j \in A$

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

also

$$a^n + a_{n-1} b a^{n-1} + \cdots + a_0 b^n = 0,$$

und es folgt $p|a$, d.h. $\frac{a}{b} \in A$.
1.7. PRIMIDEALE

ad(iii): Der $A$-Modul $B$ ist torsionsfrei ($x \in B \setminus \{0\}$, $a \in R$, $ax = 0 \Rightarrow a = 0$), also (Satz 1.2.3) frei. Sei $B = Aw_1 + \ldots + Aw_n$, dann ist $L = Kw_1 + \ldots + K w_n$, und die $w_j$ sind linear unabhängig auch über $K$. Eine solche Basis $\{w_1, \ldots, w_n\}$ nennt man auch Ganzheitsbasis.

ad(iv): Sei $x \in L$ ganz über $S^{-1}A$, sei also

$$x^n + x^{n-1} \frac{b_{n-1}}{s_{n-1}} + \cdots + \frac{b_0}{s_0} = 0, s_j \in S, b_j \in A.$$ 

Dann existiert $s \in S$, sodaß $sx$ ganz über $A$ und daher $sx \in A$. Damit ist $x \in S^{-1}A$.

ad(v): $B \supseteq A$ ist ganz, also auch $S^{-1}B \supseteq S^{-1}A$. Ist $x \in L$ ganz über $S^{-1}A$ so erst recht über $S^{-1}B$ und daher $x \in S^{-1}B$, da mit $B$ auch $S^{-1}B$ ganz abgeschlossen in $L$.

DE1.25

1.6.7 Definition, Sei $K$ eine endliche Erweiterung von $\mathbb{Q}$ und $O_K$ der ganze Abschluß von $\mathbb{Z}$ in $K$. Dann heißt $K$ algebraischer Zahlkörper und $O_K$ Ring der ganzen Zahlen in $K$.

Bemerke, daß $Z$ ganz abgeschlossen ist und $O_K$ ein freier $Z$-Modul vom Rang $[L : \mathbb{Q}]$.

1.7 Primideale

Sei $A \subseteq B$ eine Ringerweiterung

1.7.1 Definition, Sei $p \in \text{Spec } A$, $\mathfrak{p} \in \text{Spec } B$. Wir sagen $\mathfrak{p}$ liegt über $p$, $\mathfrak{p}|p$ wenn gilt $\mathfrak{p} \cap A = p$.

Sei $\mathfrak{p}|p$, dann induziert die Einbettung $A \subseteq B$ eine Einbettung $A/p \subseteq B/\mathfrak{p}$, man hat das Diagramm

$$
\begin{array}{c}
B \rightarrow B/\mathfrak{p} \\
\uparrow \uparrow \\
A \rightarrow A/p
\end{array}
$$

Ist $A \subseteq B$ ganz, so erhält man mit der kanonischen Projektion $\pi : B \rightarrow B/\mathfrak{p}$, daß $B/\mathfrak{p}$ ganz über $A/p$ ist.

1.7.2 Lemma (Nakayama Lemma). Sei $A$ ein Ring, a Ideal von $A$ das in allen maximalen Idealen enthalten ist, $M$ ein endlich erzeugter $A$-Modul. Gilt $aM = M$, so folgt $M = 0$.

Beweis. Sei $M$ erzeugt von $w_1, \ldots, w_m$ wobei $m$ minimal. Dann gibt es $a_i \in a$ so daß

$$w_1 = a_1 w_1 + \cdots + a_m w_m,$$

also

$$(1 - a_1)w_1 = a_2 w_2 + \cdots + a_m w_m.$$ 

Da $a_1$ in allen maximalen Idealen liegt, ist $1 - a_1 \in A^*$, also wird $M$ von $w_2, \ldots, w_m$ erzeugt.

DE1.26
1.7.3 **Satz.** Sei $A \subseteq B$ ganz, $p \in \text{Spec } A$. Dann gilt $pB \neq B$ und es existiert $\mathfrak{P} \in \text{Spec } B$ mit $\mathfrak{P}|p$.

**Beweis.**

:: Sei $S = A \setminus p$. Dann ist $S^{-1}B \subseteq S^{-1}A$ ganz, und es gilt

$$pB_p = pA_pB = pA_pB_p = m_pB_p$$

wobei $m_p$ das maximale Ideal von $A_p$ ist. Es genügt also die erste Behauptung für den Fall $A$ lokal zu zeigen.

:: Angenommen $pB = B$, dann ist

$$1 = a_1b_1 + \cdots + a_nb_n,$$

mit gewissen $a_i \in p$, $b_i \in B$. Sei $B_0 = A[b_1, \ldots, b_n]$, dann ist $pB_0 = B_0$ und da alle $b_i$ ganz sind, ist $B_0$ endlich erzeugter $A$-Modul. Wegen dem Nakayama Lemma folgt $B_0 = 0$, WSI.

:: Zur zweiten Aussage: Wir haben das Diagramm der Inklusionen

$$
\begin{array}{ccc}
B & \longrightarrow & B_p \subseteq (A \setminus p)^{-1}B \\
\uparrow & & \uparrow \\
A & \longrightarrow & A_p
\end{array}
$$

Wir haben schon gezeigt $m_pB_p \neq B_p$, also ist $m_pB_p$ enthalten in einem maximalen Ideal $\mathfrak{M}$ von $B_p$. Dann ist $\mathfrak{M} \cap A_p \supseteq m_p$ und da $m_p$ maximal ist $\mathfrak{M} \cap A_p = m_p$ ($1 \notin \mathfrak{M} \cap A_p$). Setze

$$\mathfrak{P} = \mathfrak{M} \cap B.$$ 

Dann ist $\mathfrak{P} \in \text{Spec } B$ und nach obigem Diagramm ist $\mathfrak{M} \cap A = p$ also $\mathfrak{P} \cap A = p$.

\[ \square \]

1.7.4 **Korollar.** Sei $A \subseteq B$ ganz und sei $\mathfrak{P}|p$. Dann ist $\mathfrak{P}$ maximal genau dann, wenn $p$ maximal.

**Beweis.**

:: Sei $p$ maximal, dann ist $A/p$ ein Körper. Sei $x \in B/\mathfrak{P}$, $x \neq 0$, dann ist $x$ ganz über $A/p$, also algebraisch. Damit ist

$$(A/p)[x] \subseteq B/\mathfrak{P}$$

ein Körper, also $x \in (B/\mathfrak{P})^*$. 

:: Ist $p$ nicht maximal, so ist $\text{Spec}(A/p) \neq \emptyset$, also auch $\text{Spec}(B/\mathfrak{P}) \neq \emptyset$.

\[ \square \]
1.8 Fortsetzung von Homomorphismen

Sei $A$ Ring (kommutativ mit 1) und $p \in \operatorname{Spec} A$. Wir haben gezeigt (Satz 1.4.3) dass sich ein Homomorphismus $\varphi : A \to L$ in einen Körper $L$ mit $\ker \varphi = p$ fortsetzen lässt zu $\psi : A_p \to L$. Und zwar durch

$$\psi\left(\frac{x}{y}\right) := \frac{\varphi(x)}{\varphi(y)}$$

Sei nun $R$ ein lokaler Ring mit maximalem Ideal $m$, $B$ ganz über $R$ und $\varphi : R \to L$ ein Homomorphismus in einen algebraisch abgeschlossenen Körper $L$ mit $\ker \varphi = m$. Wegen Satz 1.7.3 existiert ein maximales Ideal $\mathfrak{m}$ von $B$ das über $m$ liegt. Dann ist $B/\mathfrak{m}$ eine algebraische Erweiterung von $R/m$. $\varphi$ induziert einen Isomorphismus von $R/m$ und $\varphi(R) \subseteq L$. Diesen kann man auf die Erweiterung $B/\mathfrak{m}$ fortsetzen. Man hat also

$$\varphi$$

Insgesamt hat man $\varphi$ auf $B$ fortgesetzt.

1.8.1 Lemma. Sei $A \subseteq B$ ganz, $L$ algebraisch abgeschlossen, $\varphi : A \to L$. Dann hat $\varphi$ eine Fortsetzung auf $B$.

 Beweis. Sei $p = \ker \varphi \in \operatorname{Spec} A$ (da $L$ Körper), $S = A \setminus p$. Dann hat man das $S^{-1}B \supseteq A_p$ ganz ist.
1.8.2 Satz. Sei $A$ Ring, $K$ Körper, $A \subseteq K$, $x \in K \setminus \{0\}$. Weiter sei $\varphi : A \rightarrow L$ in einen algebraisch abgeschlossenen Körper $L$. Dann hat $\varphi$ entweder eine Fortsetzung auf $A[x]$ oder eine auf $A[x^{-1}]$.

Beweis.

:) Sei $p = \ker \varphi$, dann hat $\varphi$ Fortsetzung auf $A_p$. Sei also oBdA $A$ lokal mit maximalen Ideal $m$ und $\ker \varphi = m$.

:) Fall $mA[x^{-1}] = A[x^{-1}]$: Dann ist

$$1 = a_0 + a_1 x^{-1} + \ldots + a_n x^{-n}$$

mit $a_j \in m$. Es folgt

$$(1 - a_0) x^n - a_1 x^{n-1} - \ldots - a_n = 0.$$ 

Wegen $a_0 \in m$ und $A$ lokal, ist $1 - a_0 \in A^*$, also $x$ ganz über $A$. Also hat wegen Lemma 1.8.1 $\varphi$ eine Fortsetzung auf $A[x]$.

:) Fall $mA[x^{-1}] \neq A[x^{-1}]$: Sei $\mathfrak{P}$ maximales Ideal von $A[x^{-1}]$ mit $mA[x^{-1}] \subseteq \mathfrak{P}$. Dann ist $A \cap \mathfrak{P} \supseteq m$ und wegen $m$ maximal sogar $A \cap \mathfrak{P} = m$.

Sei $\psi$ so daß
Nun ist $A/m \rightarrow A[x^{-1}]/\mathfrak{P}$ und $\psi$ hat eine Fortsetzung auf $A[x^{-1}]/\mathfrak{P} = (A/m)(x^{-1} + \mathfrak{P})$. Egal ob $x^{-1} + \mathfrak{P}$ algebraisch ($L$ algebraisch abgeschlossen) oder transzendent (trivial) ist. Zusammensetzen mit der kanonischen Projektion

$$A[x^{-1}] \rightarrow A[x^{-1}]/\mathfrak{P}$$

liefer eine Fortsetzung auf $A[x^{-1}]$.

1.8.3 Korollar. Sei $A \subseteq K$, $L$ algebraisch abgeschlossen, $\varphi : A \rightarrow L$. Sei $B$ ein Unterring von $K$, maximal, so daß $\varphi$ eine Fortsetzung auf $B$ hat. Dann ist $B$ lokal und für jedes $x \in K$ gilt $x \in B$ oder $x^{-1} \in B$. 

$\Box$
Beweis. Wegen dem Zornschen Lemma existieren solche maximale Unterringe und wegen dem letzten Satz haben sie die verlangte Eigenschaft.

Ein Unterring $B$ von $K$ mit $\forall x \in K : (x \in B$ oder $x^{-1} \in B)$ heißt Bewertungsring. Jeder Bewertungsring ist lokal (vgl. Beweis von Satz 2.2.4). Sind $R$, $Q$ lokale Ringe mit maximalen Idealen $m$, $M$ so sagen wir $Q$ liegt über $R$ wenn $Q \supseteq R$, $M \cap R = m$.

1.8.4 Satz. Sei $R$ lokal, $R \subseteq L$ Körper, $x \in L$. Dann ist $x$ ganz über $R$ genau dann wenn $x$ in jedem Bewertungsring $Q \subseteq L$ ist der über $R$ liegt.

Beweis.

: Sei $x$ nicht ganz über $R$ ($\ldots$ maximale Ideal von $R$). Wir zeigen daß das Ideal $(m, x^{-1})$ von $R[\mathbb{Q}]$ nicht ganz $R[\mathbb{Q}]$ ist. Andernfalls hätte man

$$-1 = a_n \left(\frac{1}{x}\right)^n + \ldots + a_1 \left(\frac{1}{x}\right) + y$$

für gewisse $a_j \in R$, $y \in m$. Es folgt

$$\left(1 + y\right)x^n + \ldots + a_n = 0.$$  

Wegen $y \in m$ und $\mathbb{Q}$ lokal ist $1 + y \in \mathbb{Q}$, also $x$ ganz über $R$, ein WS!

Sei $\mathfrak{P}$ maximales Ideal von $\mathbb{A}[\mathbb{Q}]$ mit $\mathfrak{P} \supseteq (m, x^{-1})$. Wegen $\mathfrak{P} \cap R \supseteq m$ folgt $\mathfrak{P} \cap R = m$. Der kanonische Homomorphismus

$$R[\mathbb{Q}] \rightarrow R[\mathbb{Q}] / \mathfrak{P} \subseteq \left(R[\mathbb{Q}] / \mathfrak{P}\right)^n$$

läßt sich fortsetzen auf einen Bewertungsring $Q$ von $L$. Wegen $x^{-1} \mapsto 0$ ist $x \notin Q$. Es ist insbesondere $Q$ kein Körper und das maximale Ideal $M$ von $Q$ umfaßt $\mathfrak{P}$, denn $\mathfrak{P} \mapsto 0$. Also folgt $\mathfrak{P} \cap R = m$.

: Sei $x$ ganz über $R$, $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ eine Ganzheitsgleichung, $a_j \in R$. Sei $Q$ ein Bewertungsring von $L$ der über $R$ liegt. Angenommen $x \notin Q$, dann folgt $x^{-1} \in M$ (maximales Ideal von $Q$). Aus der Ganzheitsgleichung erhält man

$$1 = -a_{n-1}x^{-1} - \ldots - a_0x^{-n} \in M,$$

ein WS!

1.8.5 Satz. Sei $\mathbb{A}$ Ring, $\mathbb{A} \subseteq L$ Körper. Dann ist $x \in L$ ganz über $\mathbb{A}$, genau dann wenn $x$ in jedem Bewertungsring $Q$ mit $\mathbb{A} \subseteq Q \subseteq L$ liegt.

Beweis.

: Sei $x$ in jedem Bewertungsring. oBdA sei $x \neq 0$. Ist $x^{-1} \in \mathbb{A}[\mathbb{Q}]$, so hat man

$$x = c_0 + c_1 \frac{1}{x} + \ldots + c_n \left(\frac{1}{x}\right)^n$$

mit $c_j \in \mathbb{A}$. Es folgt $x$ ganz über $\mathbb{A}$. Ist $x^{-1}$ keine Einheit, so ist also $(x^{-1}) \mathbb{A}[\mathbb{Q}]$ ein echtes Ideal von $\mathbb{A}[\mathbb{Q}]$. Set $M$ maximales Ideal von $\mathbb{A}[\mathbb{Q}]$ mit $(\frac{1}{x}) \subseteq M$

Der Homomorphismus

$$\mathbb{A}[\mathbb{Q}] \rightarrow \mathbb{A}[\mathbb{Q}] / M \subseteq \left(\mathbb{A}[\mathbb{Q}] / M\right)^n$$
setzt sich auf einen Bewertungsring $Q$ von $L$ fort. Es gilt $x^{-1} \to 0$, also $x \notin Q$

WS!

· Ist $x$ ganz, so erhält man genauso wie vorher einen WS!.

☐
Kapitel 2

Dedekind Ringe

2.1 Dedekind Ringe

2.1.1 Definition. Ein nötherscher Ring der ganz abgeschlossen ist und in dem jedes Primideal maximal ist heißt Dedekind Ring.

2.1.2 Definition. Sei $R$ ein Ring, $K = Q(R)$. Eine Menge $a \subseteq K$ heißt gebrochenes Ideal von $R$ in $K$, falls $a$ ein $R$-Modul ist und es ein $c \in R \setminus \{0\}$ gibt, sodass $ca \subseteq R$ (c... „Hauptnenner“)

Ist $R$ nöthersch, so ist $ca$ und damit auch $a$ endlich erzeugt. Zwei gebrochene Ideale $a, b$ können genauso wie Ideale multipliziert werden $a \cdot b = \{x \cdot y : x \in a, y \in b\}_{R-MODULE}.


Beweis. Wir zeigen zuerst die zweite Behauptung.

$\cdot$ Sei $a$ ein Ideal von $R$. Dann existiert ein Produkt von Primidealen $p_1 \cdot \ldots \cdot p_r \subseteq a$: Angenommen es existiert ein Ideal das diese Eigenschaft nicht hat. Da $R$ nöthersch ist, gibt es ein maximales solches $a$. Dieses kann nicht prim sein, also existiert $b_1, b_2 \in R$ mit $b_1, b_2 \notin a, b_1 b_2 \in a$. Sei $a_1 = (a, b_1), a_2 = (a, b_2)$, dann gilt $a_1 a_2 \subseteq a$ aber $a_1 \not\supseteq a, a_2 \not\supseteq a$. Also enthält $a_1, a_2$ ein Produkt von Primidealen. Damit aber auch $a$, WSI.

$\cdot$ Jedes maximale Ideal $p$ ist invertierbar: Sei $p^{-1}$ die Menge aller $x \in K$ sodass $xp \subseteq R$. Dann ist $p^{-1} \supseteq R$. Wir zeigen daß $p^{-1} \not\subseteq R$: Sei $a \in p, a \neq 0$. Wähle $r$ minimal sodass

$p_1 \cdot \ldots \cdot p_r \subseteq (a) \subseteq p.$

Dann ist eines der $p_j$ enthalten in $p$ und da jedes Primideal maximal ist folgt

$p_i = p_i$. ObdA sei $i = 1$. Es gilt $p_2 \cdot \ldots \cdot p_r \not\subseteq (a)$, wähle $b \in p_2 \cdot \ldots \cdot p_r \setminus (a)$. Dann ist $bp \subseteq (a)$ und daher $ba^{-1}p \subseteq R$, also ist $ba^{-1} \in p^{-1}$. Wegen $b \notin (a)$ ist

$ba^{-1} \not\subseteq R.$

Es folgt $p \subseteq pp^{-1} \subseteq R$, also da $p$ maximal ist $p = pp^{-1}$ oder $R = pp^{-1}$. Wäre $pp^{-1} = p$, so würde $p^{-1}$ den endlich erzeugten $R$-Modul $p$ invariant lassen und wäre daher ganz über $R$: Ein WSI da $R$ ganz abgeschlossen ist. Also ist $pp^{-1} = R.$

27
Jedes Ideal \( \neq \{0\} \) ist invertierbar: Angenommen nicht. Dann existiert ein Ideal \( a \) das nicht invertierbar ist und maximal mit dieser Eigenschaft. \( a \) kann nicht maximal sein. Sei \( p \) maximal mit \( a \subseteq p \). Dann ist
\[
a \subseteq ap^{-1} \subseteq aa^{-1} \subseteq R
\]
wo \( a^{-1} := \{ x \in K : xa \subseteq R \} \). Da \( a \) endlich erzeugter \( R \)-Modul ist, ist \( ap^{-1} \nsubseteq a \), da \( p^{-1} \) nicht ganz sein kann. Also hat \( ap^{-1} \) ein Inverses \( b \) und \( bp \) ist ein Inverses für \( ap \). 

\( \cdot \) Sei \( a \) ein Ideal \( \neq \{0\} \) und \( \mathfrak{c} \) ein gebrochenes Ideal sodaß \( ac = R \). Dann gilt \( c = a^{-1} := \{ x \in K : xa \subseteq R \}\): Offenbar ist \( \mathfrak{c} \subseteq a^{-1} \). Ist \( xa \subseteq R \), so ist \( xa \mathfrak{c} \subseteq \mathfrak{c} \) und wegen \( \mathfrak{ac} = R \) also \( x \in \mathfrak{c} \).

\( \cdot \) Jedes gebrochene Ideal \( \neq \{0\} \) ist invertierbar: Sei \( a \) gebrochenes Ideal. Wähle \( c \in R \) sodaß \( ca \subseteq R \), und sei \( b \) Inverses für \( ca \), d.h. \( ca b = R \). Dann ist \( cb \) Inverses für \( a \).

Wir kommen zur ersten Behauptung:

\( \cdot \) Angenommen es gibt ein Ideal \( \neq \{0\} \) daß nicht gleich einem Produkt von Primidealen ist. Sei \( a \) maximal mit dieser Eigenschaft und sei \( p \) maximales Ideal mit \( a \subseteq p \). Dann ist \( ap^{-1} \subseteq R \) und \( ap^{-1} \nsubseteq a \). Also ist \( ap^{-1} \) Produkt von Primidealen. Damit auch \( a \). WS!

\( \cdot \) Sind \( a, b \) gebrochene Ideale, so sagen wir \( a \mid b \) wenn gilt \( b \subseteq a \) oder äquivalent wenn es ein Ideal \( \mathfrak{c} \) gibt mit \( b = \mathfrak{ac} \). Sind \( p_1, q_i \) prim und
\[
p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s,
\]
so gilt also \( p_1 \subseteq q_1 \cdot \ldots \cdot q_s \) und daher \( p_i \subseteq q_i \) für ein \( i \), also \( p_1 = q_i \). Induktiv weiter erhält man \( r = s \) und \( p_i = q_i \) bis auf eine Permutation.

\( \cdot \) Ist \( a \) gebrochenes Ideal wähle \( c \in R \) mit \( ca \subseteq R \). Sei \( (c) = p_1 \cdot \ldots \cdot p_r \), \( ca = q_1 \cdot \ldots \cdot q_s \). Dann ist also
\[
a = \frac{q_1 \cdot \ldots \cdot q_s}{p_1 \cdot \ldots \cdot p_r}
\]
Kürzt man alle oben und unten vorkommenden Ideale so ist die Darstellung eindeutig.

\( \Box \)

**2.1.4 Korollar.** Sei \( R \) Dedekind, \( a \in R \). Dann existieren nur endlich viele Ideale \( b \triangleleft R \) mit \( a \triangleleft b \).

*Beispiel.* Sei
\[
(a) = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}.
\]

Dann gilt
\[
b \triangleleft (a) \iff b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r} \text{ mit } \beta_i \leq \alpha_i.
\]

\( \Box \)
2.1. DEDEKIND RINGE

2.1.5 Lemma. Sei $A$ Dedekind, $B$ der ganze Abschluß von $A$ in einer endlichen separablen Erweiterung von $K = Q(A)$. Dann ist $B$ Dedekind.

Beweis. $B$ ist nöthersch wegen Satz 1.6.6, (i), ganz abgeschlossen wegen Satz 1.6.4, jedes Primideal ist maximal wegen Korollar 1.7.4. □

Z ist Dedekind, also folgt

2.1.6 Lemma. Sei $K$ ein algebraischer Zahlkörper, $O_K$ der Ring der ganzen Zahlen in $K$. Dann ist $O_K$ Dedekind Ring. Die multiplikative Gruppe der gebrochenen Ideale $\neq \{0\}$ bezeichnet man mit $I_K$.

Ein gebrochenes Hauptideal, ist ein gebrochener Ideal der Gestalt $\alpha R$ mit $\alpha \in K$. Die Menge $P_K$ der gebrochenen Hauptideale ist eine Untergruppe von $I_K$.

2.1.7 Definition. $C_K := I_K/P_K$ heißt Idealklassengruppe von $K$.

$C_K$ mißt "wie weit $O_K$ von der ZPE-Situation weg ist ".

Sei $R$ ein Dedekind Ring. Dann ist $I_K \cong \sum_{p \in \text{Spec } K} R$, die Divisorengruppe.

Ist $a = \prod_{p \in \text{Spec } K} p^{r_p}$, so sagen wir $r_p = \text{ord}_p a$. Ist $\text{ord}_p a > 0 (= 0, < 0)$, so hat $a$ eine Nullstelle bei $p$ (ist eine Einheit bei $p$, hat einen Pol bei $p$).

Offenbar gilt $a|b \iff \forall p : \text{ord}_p a \leq \text{ord}_p b$. Es ist $\text{ord}_p (\alpha) = 0$ genau dann wenn $\alpha$ eine Einheit in $R_p$ ist.

2.1.8 Lemma. Sei $R$ ein Dedekind Ring mit nur endlich vielen Primidealen. Dann ist $R$ ein Hauptidealring.

Beweis. Seien $p_1, \ldots, p_s$ die Primideale von $R$. Sei $a$ ein Ideal,

$$a = p_1^{r_1} \ldots p_s^{r_s}.$$

Wähle $\pi_i \in p_i \setminus p_i^2$ und $a \in R$ mit $\alpha \equiv p_i^{r_i} \mod p_i^{r_i+1}$. Sei

$$\alpha = p_1^{r_1} \ldots p_s^{r_s},$$

dann folgt unmittelbar $e_i = r_i$ und daher $\alpha = a$. □

2.1.9 Lemma. Sei $A$ Dedekind Ring, $S \subseteq A$ multiplikativ. Dann ist $S^{-1}A$ ein Dedekind Ring. Die Abbildung

$$a \mapsto S^{-1}a = \{\frac{a}{s} : a \in a, s \in S\}$$

induziert einen Homomorphismus der Gruppe der gebrochenen Ideale von $A$ auf die von $S^{-1}A$. Ein Ideal ist ein Kern $\iff a_0S \neq \emptyset$.

Beweis.

·) Wegen Lemma 1.3.5, (iii), ist $S^{-1}A$ nöthersch, wegen Satz 1.6.6, (iv), ganz abgeschlossen, und wegen Satz 1.4.5 ist jedes Primideal von $S^{-1}A$ maximal.

·) Wegen $S^{-1}(a-b) = (S^{-1}a) - (S^{-1}b)$ gibt die Abbildung einen Homomorphismus von der Gruppe der gebrochenen Ideale von $A$ in die von $S^{-1}A$. Wegen Satz 1.4.5, (ii), ist dieser surjektiv.
.. Ist \( a \cap S \neq \emptyset \), so ist \( S^{-1}a = S^{-1}A \). Ist umgekehrt \( S^{-1}a = S^{-1}A \), so ist \( 1 = \frac{a}{s} \) für gewisse \( a \in a, s \in S \), also \( a \cap S \neq \emptyset \).

\[ 1 \]

**2.1.10 Lemma.** Sei \( A \) einen Dedekind Ring und sei die Idealklassengruppe endlich. Sei \( a_1, \ldots, a_r \) ein vollständiges Repräsentantensystem der Idealklassen. Ist \( b \in \bigcap a_i, b \neq 0, b \in A \), und ist \( S = \{1, b, b^2, b^3, \ldots\} \), dann ist \( S^{-1}A \) Hauptidealring.

**Beweis.** Bei Anwendung von \( S^{-1}A \) werden die \( a_i \) auf \( S^{-1}A \) abgebildet. Da Hauptideale auf Hauptideale gehen, folgt die Behauptung, dass \( S^{-1}A \) surjektiv ist.

\[ 2 \]

Für den Ring der ganzen Zahlen in einem algebraischen Zahlkörper ist tatsächlich \( C_K \) endlich.

**2.1.11 Lemma.** Sei \( K \) ein algebraischer Zahlkörper. Dann existiert \( M \in \mathbb{N} \) mit der folgenden Eigenschaft: Sind \( a, b \in O_K, \beta \neq 0 \), dann existiert \( t \in \mathbb{N}, 1 \leq t \leq M \), und \( w \in O_K \), so dass

\[ |N_K^K(ta - w)\beta| < |N_K^K(\beta)|. \]

**Beweis.**

\( 1 \) Es genügt zu zeigen: \( \exists M \in \mathbb{N} : \forall \gamma \in K \exists 1 \leq t \leq M, w \in O_K : |N(t\gamma - w)| < 1. \)

\( 2 \) Betrachte \( K \subseteq \mathbb{C} \). Sei \( w_1, \ldots, w_n \) eine Ganzheitsbasis von \( O_K \). Für \( \gamma \in K, \gamma = \sum \gamma_i w_i \), gilt \( n = [K : \mathbb{R}] \)

\[ |N_K^K(\gamma)| = \prod_{\sigma \text{ Erweiterung}} |\sum \gamma_i \sigma(w_i)| \leq (\max |\gamma_i|)^n \left( \prod_{\sigma} |\sigma(w_i)| \right) \]

Wähle \( m > \sqrt{C} \) und setze \( M := m^n. \)

\( 3 \) Ist \( \gamma \in K, \gamma = \sum \gamma_i w_i \) \( (\gamma_i \in \mathbb{Q}) \) schreibe

\[ \gamma_i = a_i + b_i \text{ mit } a_i \in \mathbb{Z}, 0 \leq b_i < 1. \]

Setze \( [\gamma] := \sum a_i w_i, \{\gamma\} := \sigma b_i w_i \). Dann ist \( \gamma = [\gamma] + \{\gamma\}, [\gamma] \in O_K \), und \( \{\gamma\} \) hat Koordinaten zwischen 0 und 1.

\( 4 \) Betrachte die Abbildung \( \phi : K \rightarrow \mathbb{R}^M \) mit

\[ \phi(\sum \gamma_i w_i) := (\gamma_1, \ldots, \gamma_n). \]

Stets liegt \( \{\gamma\} \) im Einheitswürfel. Zerlege diesen in \( m^n \) Würfeln mit Seitenlänge \( \frac{1}{m} \) und betrachte die Punkte \( \phi([k\gamma]), 1 \leq k \leq m^n + 1. \) Mindestens zwei müssen im gleichen Teilwürfel liegen, z.B. \( \phi([h\gamma]) \) und \( \phi([l\gamma]), h > l. \) Es ist \( t = h - l \leq m^n, \)

\[ t\gamma = h\gamma - l\gamma = [h\gamma] - [l\gamma] + ([h\gamma] - [l\gamma]) \]

Dann ist \( w \in O_K \) und die Beträge der Koordinaten von \( \delta \) höchstens \( \frac{1}{m} \). Es folgt

\[ |N_K^K(\delta)| \leq \left( \frac{1}{m} \right)^n C < 1. \]
2.2. DISKRETE BEWERTUNGSRINGE


Beweis. Sei $a \not\in O_K$. Für jedes $\alpha \in a$, $\alpha \neq 0$, ist $|N^K_0(\alpha)| \in \mathbb{N}$. Wähle $\beta \in a, \beta \neq 0$, so daß $|N^K_0(\beta)|$ minimal ist. Für jedes $\alpha \in O_K$ existiert $t, 1 \leq t \leq M$, so daß $(w \in O_K$ geeignet$)$

$$|N^K_0(t\alpha - w\beta)| < |N^K_0(\beta)|.$$  

Es folgt

$$t\alpha - w\beta = 0,$$

und damit also

$$M!a \subseteq (\beta)_{O_K}.$$  

Setze $b := \frac{1}{M!}M!a$. Dann ist $b \in O_K$, und es gilt $M!a = (\beta)b$. Da $\beta \in a$ folgt $M!\beta \in (\beta)b$, also $M! \in b$. Damit gibt es für $b$ nur endlich viele Möglichkeiten und wir haben $a \equiv b$ in $I_K$ modulo $P_K$.  

2.1.13 Korollar. Sei $a$ gebrochenes Ideal. Dann ist $a^{h_K}$ ein gebrochenes Hauptideal.

Beweis. $a^{h_K} = 1$ in $C_K$.


Beweis. Sei $a \in M$. Zu jedem $p$ existiert $x_p \in N, s_p \in S_p$, so daß $s_p a = x_p$. Sei $b$ das von den $s_p$ erzeugte Ideal, dann gilt $b = A$, also

$$1 = \sum y_p s_p$$

für gewisse $y_p \in A$ die fast alle $= 0$ sind. Es folgt

$$a = \sum y_p s_p a = \sum y_p x_p \in N.$$  

2.2 Diskrete Bewertungsringe

2.2.1 Definition. Ein lokaler Dedekind Ring heißt diskreter Bewertungsring.

$R$ ist ein diskreter Bewertungsring genau dann wenn er ein Hauptidealring mit genau einem Primideal ist. Ist $A$ Dedekind und $p$ ein Primideal, so ist also $A_p$ ein diskreter Bewertungsring. Sei $R$ diskreter Bewertungsring und $\pi$ das Prinziplement. Dann läßt sich also jedes $x \in R$ schreiben als $x = cn^{\nu}$ mit $c \in R^*$ und $\nu \in \mathbb{N} \cup \{0\}$.
2.2.2 Definition. Sei $K$ ein Körper, $\Gamma$ eine geordnete Gruppe ($0 \notin \Gamma$). Eine Abbildung
\begin{align*}
v : \begin{cases} 
K & \to \Gamma \cup \{0\} \\
x & \mapsto |x|
\end{cases}
\end{align*}
heißt Bewertung von $K$ (mit Wertegruppe $v(K \setminus \{0\}) \subseteq \Gamma$) falls gilt
(i) $v(x) = 0 \iff x = 0$
(ii) $v(xy) = v(x) \cdot v(y)$
(iii) $v(x + y) \leq \max\{v(x), v(y)\}$.
Die Bewertung heißt diskret, wenn die Wertegruppe zyklisch ist.

2.2.3 Definition. Sei $K$ ein Körper, $R$ ein Unterring von $K$. $R$ heißt Bewertungerring, falls gilt
\[ \forall x \in K : (x \in R \lor x^{-1} \in R). \]
Ist $R$ diskreter Bewertungerring, so ist $R$ Bewertungerring in $K = Q(R)$.

2.2.4 Satz. Sei $K$ ein Körper, $v$ eine Bewertung von $K$. Dann ist
\[ R_v := \{ x \in K : v(x) \leq 1 \Gamma \}. \]
ein Bewertungerring. Ist umgekehrt $R \subseteq K (= Q(R))$ ein Bewertungerring so existiert eine Bewertung $v$ von $K$ mit $R = R_v$. Es ist $R_v$ lokal mit maximalen Ideal $m = \{ x \in K : v(x) < 1 \}$ und $R_v^* = \{ x \in K : v(x) = 1 \}$.
$R$ ist ein diskreter Bewertungerring genau dann wenn er ein Bewertungerring ist der von einer diskreten Bewertung kommt.

Beweis.
\begin{itemize}
\item[·] Ist $v$ eine Bewertung, so ist $v(1) = v(x)v(x^{-1})$, also entweder $v(x) \leq v(1)$ oder $v(x^{-1}) \leq v(1)$, da $v(1) = v(1)v(1)$ ist, ist $v(1) = 1 \Gamma$ das Einselement von $\Gamma$.
\item[·] Sei $R$ ein Bewertungerring. Wir zeigen, daß $R$ lokal ist: Sei $U = R^*$ die Einheitsgruppe. Es genügt zu zeigen, daß $R \setminus U$ ein Ideal von $R$ ist. Seien $x, y \in R \setminus U$ und sei z.B. $\frac{x}{y} \in R$. Dann gilt
\[ 1 + \frac{x}{y} = (x + y) \frac{1}{y} \in R. \]
Wäre $x + y \in U$, so wäre auch $y \in U$ WSI. Sei $x \in R \setminus U$, $z \in R$. Wäre $zx \in U$, ($zx)b = 1$, für ein $b \in R$, so wäre auch $x \in U$, denn $(zb)x = 1$ WSI.
\item[·] Sei $m$ das maximale Ideal von $R$, dann ist $R = U \cup m$ und daher $(m^* = m \setminus \{0\})$
\[ K^* = m^* \cup U \cup (m^*)^{-1}, \]
as disjunkte Vereinigung. Da $m^*$ multiplikativ ist, ist
\[ \Gamma = K^*/U \]
eine geordnete Gruppe ($xU < U \iff x \in m^*$). Für $x \in K^*$ setze $v(x) := xU \in \Gamma$, für $x = 0$ setze $v(x) = 0$. 

2.3 GALOIS ERWEITERUNGEN

γ) Seien \( x, y \in K^* \), z.B. \( \frac{1}{x}, \frac{1}{y} \in R \) also \( v(x)v(y)^{-1} \leq U \). Dann ist \( 1 + \frac{1}{y} \in R \), also \( v(1 + \frac{1}{y}) \leq U \). Es folgt wegen \( 1 + \frac{z}{y} = (x + y)^{-1} \) daß \( v(x + y)v(y)^{-1} \leq U \) und daher \( v(x + y) \leq v(y) \).

Also ist \( v \) Bewertung von \( K \) und klarerweise ist \( R = R_v \).

γ) Sei \( v \) eine diskrete Bewertung, \( R = R_v \) der Bewertungsring zu \( v \). Wähle einen Erzeuger \( \gamma \) von \( \Gamma \) und schreibe \( \gamma = v(\pi) \). Da mit \( \gamma \) auch \( \gamma^{-1} \) die Gruppe \( \Gamma \) erzeugt sei oBdA \( \pi \in R \). Da \( \gamma \neq 1 \) folgt \( \pi \in \mathfrak{m} \). Jedes Element \( x \in K^* \) läßt sich schreiben (eindeutig) als

\[
x = u\pi^r
\]

mit \( r \in \mathbb{Z} \) und \( u \in U \), denn \( v(x) = \gamma^r \) für ein \( r \). Es folgt daß \( \mathfrak{m} = (\pi) \). Allgemein sind alle Ideale vom \( R \) gegeben durch

\[
(\pi) \supseteq (\pi^2) \supseteq (\pi^3) \supseteq \ldots ,
\]

denn ist \( a \) Ideal von \( R \), so folgt \( a = (\pi^s) \) für \( s = \min\{r : x = u\pi^r \in a\} \). Klarerweise ist \( (\pi^s) \) für \( s > 1 \) nicht prim, also ist \( R \) ein Hauptidealring mit genau einem Primideal. So ein Element \( \pi \) heißt auch oft ein lokaler Parameter.

γ) Sei \( R_v \) ein diskreter Bewertungsring, \( \mathfrak{m} = (\pi) \) dann hat die Primfaktorzerlegung von \( x \in R \) die Gestalt \( x = r\pi^r, r \in \mathbb{Z}, u \in R^* \) weil es nur ein Primitivgitter gibt (bis auf Konjugierte). Damit hat jedes Element \( x \) von \( K^* \) die Gestalt \( x = u\pi^r, r \in \mathbb{Z}, u \in R^* \) und es folgt \( \langle v(\pi) \rangle = \Gamma \).

\[ \square \]

2.3 Galois Erweiterungen

Ist \( A \) ganz abgeschlossen in \( K = Q(A), L \) wie endliche Galois-Erweiterung von \( K \) mit Gruppe \( G \), und \( B \) der ganze Abschluß von \( A \) in \( L \), dann gilt \( \sigma B = B, \sigma \in G \) (vgl. Satz 16.2, (v)).

2.3.1 Satz. Sei \( A \) ganz abgeschlossen, \( L \) eine endliche Galoisische Erweiterung von \( K = Q(A) \) mit Gruppe \( G \), \( B \) der ganze Abschluß von \( A \) in \( L \). Sei \( \mathfrak{p} \in \text{Spec} A, \mathfrak{p}, Q \in \text{Spec} B \) die über \( p \) liegen. Dann existiert \( \sigma \in G \) so daß \( \sigma\mathfrak{p} = \mathfrak{Q} \).

Beweis.

γ) Betrachte zuerst den Fall daß \( p \) maximal ist. Angenommen \( \mathfrak{p} \neq \sigma\Omega \) für alle \( \sigma \in G \). Dann existiert \( x \in B \) mit (Chinesischer Restsatz).

\[
x \equiv 0 \mod \mathfrak{p}, x \equiv 1 \mod \sigma Q, \sigma \in G.
\]

Die Norm \( N^L_K(x) = \prod_{\sigma \in G} \sigma x \) liegt in \( B \cap K = A \) denn \( A \) ist ganz abgeschlossen und sogar in \( \mathfrak{p} \cap K = p \). Jedoch ist stets \( \sigma x \notin \Omega \), also \( N^L_K(x) \notin \Omega \cap K = p \), WS!

γ) Sei nun allgemein \( p \in \text{Spec} A \). Wir lokalisieren: Sei \( S = A \setminus p \). Dann ist \( S^{-1}B \) der ganze Abschluß von \( S^{-1}A \) in \( L \), \( S^{-1}p \) maximales Ideal von \( S^{-1}A \), \( S^{-1}\mathfrak{p}, S^{-1}Q \in \text{Spec} S^{-1}B \) und liegen über \( S^{-1}p \). Es folgt daß \( \sigma \in G \) gibt

mit \( \sigma(S^{-1}\mathfrak{p}) = S^{-1}\mathfrak{Q} \). Da \( S \subseteq K \) und daher bei \( \sigma \) fix bleibt folgt \( \sigma\mathfrak{p} = \mathfrak{Q} \).
2.3.2 Korollar. Sei $A$ ganz abgeschlossen, $E$ endliche separable Erweiterung von $K = Q(A)$, $B$ der ganze Abschluß von $A$ in $E$. Sei $p \in \text{Spec } A$. Dann gibt es nur endliche Primideale von $B$ die über $A$ liegen.

Beweis. Sei $L$ die kleinste Galois-Erweiterung von $K$ die $E$ enthält. Sind $\Omega_1, \Omega_2$ verschiedene Primideale von $B$ über $p$, und $\mathfrak{P}_1, \mathfrak{P}_2$ Primideale vom ganzen Abschluß $C$ von $A$ in $L$ die über $\Omega_1$ bzw. $\Omega_2$ liegen, dann ist $\mathfrak{P}_1 \neq \mathfrak{P}_2$ und $\mathfrak{P}_1, \mathfrak{P}_2$ liegen über $p$. Wegen dem Satz gibt es nur endlich viele solche $\mathfrak{P}$'s.

\[\text{DEI.43}\]

2.3.3 Definition. Sei $p$ maximales Ideal von $A, \mathfrak{P}$ maximales Ideal von $B$ das über $A$ liegt. Die Gruppe

$G_\mathfrak{P} := \{\sigma \in G : \sigma \mathfrak{P} = \mathfrak{P}\}$

heißt Zerlegungsgruppe von $\mathfrak{P}$. Ihr Fixpunktkörper $L^d$ heißt Zerlegungskörper von $\mathfrak{P}$.

Sei $A$ nöthersch, ganz abgeschlossen, $L$ separable Erweiterung von $K = Q(A)$, $B$ der ganze Abschluß von $A$ in $L$, $p \in \text{Spec } A$ maximal, $\mathfrak{P} \in \text{Spec } B$ über $p$. Dann heißt die Körpererweiterung

$B/\mathfrak{P} : A/p$

die Restklassenkörpererweiterung von $\mathfrak{P}/p$. Wegen Satz 1.6.6, (i, Beweis), gilt

$[B/\mathfrak{P} : A/p] \leq [L : K].$

Die Gruppe $G_\mathfrak{P}$ operiert in natürlicher Weise auf $B/\mathfrak{P}$ und läßt $A/p$ punktweise fest. Wir haben also einen Homomorphismus

$G_\mathfrak{P} \rightarrow \text{Aut}(B/\mathfrak{P} : A/p)).$

Ist $G = \bigcup \sigma_j G_\mathfrak{P}$ eine Zerlegung von $G$ in Nebenklassen, dann sind die $\sigma_j \mathfrak{P}$ genau die verschiedenen Primideale über $p$.

Die Zerlegungsgruppe von $\sigma \mathfrak{P}$ ist gleich $\sigma G_\mathfrak{P} \sigma^{-1}$.

2.3.4 Lemma. $L^d$ ist der kleinste Zwischenkörper $E, K \subseteq E \subseteq L$, mit der Eigenschaft daß $\mathfrak{P}$ das einzige Primideal von $B$ ist das über dem Primideal $\mathfrak{P} \cap E$ von $B \cap E$ liegt.

Beweis.

1.) Sei $E = L^d$. $B^d = B \cap L^d$ ist der ganze Abschluß von $A$ in $L^d$, ist also ganz abgeschlossen. $L$ ist eine endliche Galoiserweiterung von $L^d$ mit Gruppe $G_\mathfrak{P}$. Wegen Satz 2.3.1 ist $\mathfrak{P}$ das einzige Primideal über $\mathfrak{P} \cap B^d$.

2.) Habe $E$ die obige Eigenschaft und sei $H$ die Gruppe von $L$ über $E$. Setze $q = \mathfrak{P} \cap E$. Wegen Satz 2.3.1 sind die $\sigma \mathfrak{P}, \sigma \in H$, genau die Primideale über $q$. Es folgt $\sigma \mathfrak{P} = \mathfrak{P}$, d.h. $H \subseteq G_\mathfrak{P}$ und damit $E \supseteq L^d$. \[\text{LEI.44}\]
2.3.5 **Satz.** Sei $\Omega = B^d \cap \mathfrak{P}$. Dann gilt (mittels der kanonischen Einbettung $A/\mathfrak{p} \to B^d/\Omega$) $A/\mathfrak{p} = B^d/\Omega$.

**Beweis.** Ist $\sigma \in G \setminus G_\mathfrak{P}$, so ist also $\sigma \mathfrak{P} \neq \mathfrak{P}$ bzw. $\sigma^{-1} \mathfrak{P} \neq \mathfrak{P}$. Setze $\Omega_\sigma = \sigma^{-1} \mathfrak{P} \cap B^d$. Dann ist $\Omega_\sigma \neq \Omega$, denn über $\Omega$ liegt ja nur ein Primideal nämlich $\mathfrak{P}$.

Sei $x \in B^d$, dann existiert $y \in B^d$ mit

$$y \equiv x \mod \Omega$$
$$y \equiv 1 \mod \Omega_\sigma, \sigma \in G \setminus G_\mathfrak{P}.$$  

Speziell folgt

$$y \equiv x \mod \mathfrak{P}$$  
$$y \equiv 1 \mod \sigma^{-1} \mathfrak{P}, \sigma \in G \setminus G_\mathfrak{P},$$

also

$$\sigma y \equiv 1 \mod \mathfrak{P}, \sigma \in G \setminus G_\mathfrak{P}.$$  

Die Norm $N_{K}^{B} (y)$ ist das Produkt $\prod \sigma y$ wobei $\sigma$ ein vollständiges Restsystem modulo $G_\mathfrak{P}$ durchläuft. Also folgt

$$N_{K}^{B} (y) \equiv x \mod \mathfrak{P}.$$  

Die linke Seite liegt in $A$, die rechte in $B^d$. Also gilt die Kongruenz sogar modulo $\Omega$. 

Ist $x \in B$, so bezeichne $\bar{x}$ die Restklasse von $x$ modulo $\mathfrak{P}$, $\bar{x} \in B/\mathfrak{P}$. Der Homomorphismus von $G_\mathfrak{P}$ nach $\operatorname{Aut}(B/\mathfrak{P} : A/\mathfrak{p})$ sei bezeichnet mit $\sigma \mapsto \bar{\sigma}$. Dann ist offenbar

$$\bar{\sigma} \bar{x} = \bar{\sigma x}.$$  

Ist $f(X)$ ein Polynom mit Koeffizienten in $B$, $f(X) = b_nX^n + \cdots + b_0$, so bezeichne $\bar{f}(X)$ das Polynom über $B/\mathfrak{P}$

$$\bar{f}(X) = \bar{b}_nX^n + \cdots + \bar{b}_0.$$  

2.3.6 **Satz.** Sei $A$ ganz abgeschlossen, $L$ eine endliche Galois Erweiterung von $K = Q(A)$ mit Gruppe $G, B$ der ganze Abschluß von $A$ in $L$. Sei $\mathfrak{p}$ maximales Ideal von $A$ und $\mathfrak{P}$ maximales Ideal von $B$ das über $\mathfrak{p}$ liegt. Dann ist $B/\mathfrak{P}$ eine normale Erweiterung von $A/\mathfrak{p}$ und die Abbildung $\sigma \mapsto \bar{\sigma}$ ist ein Homomorphismus von $G_\mathfrak{P}$ auf die Galoisgruppe $\operatorname{Aut}(B/\mathfrak{P} : A/\mathfrak{p})$.

**Beweis.**

1) Setze $\bar{B} = B/\mathfrak{P}, \bar{A} = A/\mathfrak{p}$. Sei $\bar{x} \in \bar{B}$, und sei $f(X)$ das Minimalkopon von $x$ über $K$. Da $x$ ganz über $\bar{A}$ ist sind alle Koeffizienten von $f$ in $\bar{A}$ und damit auch alle anderen Wurzeln in $L$ von $f$ sogar in $B$. Es schreibt sich also $f$ in $B$ in Linearfaktoren und dann $L/K$ ist normal

$$f(X) = (X - x_1) \cdots (X - x_m).$$
Da $\bar{x}$ eine Wurzel des Polynoms

$$f(X) = (X - \bar{x}_1) \cdots (X - \bar{x}_m) \in \bar{B}[X]$$

erfüllt das Minimalpolynom von $\bar{x}$ auch in Linearfaktoren. Also ist $\bar{B}/\bar{A}$ normal.

• Wegen obigem folgt daß

$$[\bar{A}(\bar{x}) : \bar{A}] \leq [K(\bar{x}) : K] \leq [L : K].$$

Da die maximale separable Erweiterung $E$ von $\bar{A}$ in $\bar{B}$ durch ein Element erzeugt wird folgt $[E : \bar{A}] \leq [L : K] < \infty$. Sie ist also eine endliche Galois Erweiterung von $\bar{A}$, denn $\bar{B}/\bar{A}$ ist normal und daher auch $E : \bar{A}$.

• ObdA liegt über $p$ nur ein Primideal: Wegen Satz 2.3.5 ist

$$\text{Aut}(\bar{B} : \bar{A}) = \text{Aut}(\bar{B} : B^d/\Omega),$$

um die Surjektivität von $\sigma \mapsto \bar{\sigma}$ zu zeigen, können wir also die Situation $K = L^d$ annehmen. D.h. $G = G_p$.

• Sei also $G = G_p$. Sei $x \in B$ sodaß $\bar{x}$ die maximale separable Erweiterung von $\bar{A}$ in $\bar{B}$ erzeugt und sei $f$ das Minimalpolynom von $x$ über $K$. Ein Automorphismus $\bar{\tau}$ von $\bar{B} : \bar{A}$ ist durch seine Wirkung auf $\bar{x}$ eindeutig bestimmt. Offenbar ist $\bar{\tau} \bar{x}$ eine Wurzel von $\bar{f}$. Ist $y$ irgend eine Wurzel von $f$ so existiert $\sigma \in G = G_p$ sodaß $\sigma x = y$. Zu jedem $\bar{\sigma}$ existiert daher ein $\sigma \in G_p$ sodaß $\bar{\sigma} = \bar{\tau}$.

\[\square\]

2.3.7 *Korollar*. Seien $A,K,B,L,G$ wie im Satz, sei $p$ ein maximales Ideal von $A$, $\varphi : A \to A/p$ der kanonische Homomorphismus. Sind $\psi_1, \psi_2$ Homomorphismen von $B$ in einen algebraischen Abschluß von $A/p$ die $\varphi$ fortsetzen, so existiert $\sigma \in G$ sodaß

$$\psi_1 = \psi_2 \circ \sigma.$$  

*Beweis.*

• Sei $\psi_1, \psi_2$ Primideale von $B$ die über $p$ liegen, also existiert wegen Satz 2.3.1 ein $\bar{\tau} \in G$ sodaß $\psi_1, \psi_2 \circ \bar{\tau}$ den selben Kern haben. ObdA haben also $\psi_1, \psi_2$ den gleichen Kern $\mathfrak{q}$.

• Sei also $\ker \psi_1 = \ker \psi_2 = \mathfrak{q}$. Sei $B/\mathfrak{q} \subseteq (A/p)^n$. $\psi_1 : B \to (A/p)^n$ induziert eine Einbettung $\psi_1 : B/\mathfrak{q} \to (A/p)^n$. Da $B/\mathfrak{q}$ normal über $A/p$ ist folgt $\bar{\psi}_1 \in \text{Aut}(B/\mathfrak{q} : A/p)$. Genau so für $\psi_2$. Also existiert $\sigma \in G_{\mathfrak{q}}$ so daß $\bar{\psi}_2^{-1} \circ \bar{\psi}_1 = \bar{\sigma}$. Man hat das Diagramm

\[\square\]
2.4 Verzweigung von Primidealen

Sei $A$ ein Dedekind Ring, $L$ eine endliche separable Erweiterung von $K = Q(A)$, $B$ der ganze Abschluß von $A$ in $L$.

Ist $p \in \text{Spec} A$, so ist $pB$ ein Ideal von $B$. Daher gilt mit gewissen $\mathfrak{p}_i \in \text{Spec} B, \epsilon_i \geq 1$,

$$pB = \mathfrak{p}_1^{\epsilon_1} \cdot \ldots \cdot \mathfrak{p}_r^{\epsilon_r}.$$  

2.4.1 Lemma. Eine Primstelle $\mathfrak{p} \in \text{Spec} B$ kommt in obiger Faktorisierung genau dann vor wenn sie über $p$ liegt.

Beweis. Da jedes $\mathfrak{p} \in \text{Spec} B$ maximal ist und die Faktoren paarweise coprim, gilt

$$\mathfrak{p}_1^{\epsilon_1} \cdot \ldots \cdot \mathfrak{p}_r^{\epsilon_r} = \mathfrak{p}_1^{\epsilon_1} \cap \ldots \cap \mathfrak{p}_r^{\epsilon_r}.$$  

Ist $\mathfrak{p}$ eine Primstelle über $p$ die nicht vorkommt, so wäre ($\mathfrak{p} \supset pB$)

$$pB = \mathfrak{p}_1^{\epsilon_1} \cap \ldots \cap \mathfrak{p}_r^{\epsilon_r} = \mathfrak{p}_1^{\epsilon_1} \cap \ldots \cap \mathfrak{p}_r^{\epsilon_r} \cap \mathfrak{p},$$

ein WS! zur Eindeutigkeit der Faktorisierung. Umgekehrt ist klarerweise $\mathfrak{p}_i \supset pB \supset p$ und da $p$ maximal ist und $1 \notin \mathfrak{p}_i$ folgt $\mathfrak{p}_i \cap A = p$. 

2.4.2 Definition. Liegt $\mathfrak{p}$ über $p$, so heißt der Exponent $e(\mathfrak{p}/p)$ von $\mathfrak{p}$ in der Zerlegung von $pB$ der Verzweigungsindex von $\mathfrak{p}/p$, und $f(\mathfrak{p}/p) = [B/\mathfrak{p} : A/p]$ der Restklassengrad von $\mathfrak{p}/p$.

Für $\mathfrak{p} \in \text{Spec} B$ definiert man

$$N_K^L(\mathfrak{p}) := p^{f(\mathfrak{p}/p)}$$

wobei $p := \mathfrak{p} \cap A$. Die Norm $N_K^L$ gibt also einen Homomorphismus

$$N_K^L : I(B) \rightarrow I(A).$$

2.4.3 Lemma. Sei $A$ Dedekind, $K = Q(A), K \subseteq E \subseteq L$ endliche separable Erweiterungen, $A \subseteq B \subseteq C$ die entsprechenden ganzen Abschluß von $A$ in an $E$ bzw. $L$. Sei $p \in \text{Spec} A, q \in \text{Spec} B, \mathfrak{p} \in \text{Spec} C, q/p, \mathfrak{p}/q$. Dann gilt

(i) $$e(\mathfrak{p}/p) = e(\mathfrak{p}/q)e(q/p)$$

(ii) $$f(\mathfrak{p}/p) = f(\mathfrak{p}/q)f(q/p)$$

(iii) $$N_K^E \circ N_E^L = N_K^L.$$  

Beweis. Klar nach Definition. 


LEI.48

LEI.49

LEI.50

LEI.51
Beweis. Ist $x_1, \ldots, x_n$ Basis von $M$ über $A$, d.h.

$$M = \sum_{i=1}^{n} A x_i \text{ (direkte Summe)},$$

so ist $M/pM = \sum_{i=1}^{n} (A/p)x_i \text{ (direkte Summe)}$, wobei $x_i$ die Restklasse von $x_i$ modulo $pM$. Denn ist

$$\sum \lambda_i x_i = 0 \text{ in } M/pM,$$

so ist $\sum \lambda_i x_i \in pM$. Es gilt $pM = \sum p x_i$ und wegen der Eindeutigkeit der Darstellung folgt $\lambda_i = 0$.

\[\square\]

2.4.5 Satz. Sei $A$ Dedekind, $K = Q(A)$, $L$ endlich separable Erweiterung von $K$, $B$ der ganze Abschluß von $A$ in $L$. Ist $p \in \text{Spec } A$, so gilt

$$[L : K] = \sum_{\mathfrak{P}/p} e(\mathfrak{P}/p) f(\mathfrak{P}/p).$$

Beweis.

\(\cdot\) ObdA sei $A$ lokal: Wir lokalisieren bei $p$. Ist $S = A \setminus p$, betrachte also die Situation $S^{-1}A \subseteq K \subseteq L$. Es ist $S^{-1}B$ der ganze Abschluß von $S^{-1}A$ in $L$. Ist

$$pB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

so ist wegen Lemma 2.1.9

$$(S^{-1}p)(S^{-1}B) = S^{-1}(pB) = (S^{-1}\mathfrak{P}_1)^{e_1} \cdots (S^{-1}\mathfrak{P}_r)^{e_r},$$

Daher sind die $S^{-1}\mathfrak{P}_i$ sind alle Primideale über $S^{-1}p$ ($S^{-1}\mathfrak{P}_i \neq S^{-1}B$ da $S \cap \mathfrak{P}_i = \emptyset$) und $e(S^{-1}\mathfrak{P}/S^{-1}p) = e(\mathfrak{P}/p)$. Wegen Satz 1.4.9 ist für jedes $\mathfrak{P}/p$

$$S^{-1}B/S^{-1}\mathfrak{P} \cong B/\mathfrak{P}, \quad S^{-1}A/S^{-1}p \cong A/p,$$

also $f(S^{-1}\mathfrak{P}/S^{-1}p) = f(\mathfrak{P}/p)$.


Sei $pB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Der Homomorphismus

$$B \to \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}$$

ist surjektiv und hat Kern $pB$. Wegen $\mathfrak{P}_i^{e_i} \supseteq p$ ist $B/\mathfrak{P}_i^{e_i}$ ein $A/p$ - Vektorraum, also auch die direkte Summe auf der rechten Seite. Klarerweise ist der Homomorphismus

$$B/pB \to \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}$$

ein $A/p$-Homomorphismus.
2.4. VERZWEIGUNG VON PRIMIDEALEN

Wir bestimmen die Dimension von $B/\mathfrak{P}^e$. Sei $\pi$ ein Erzeuger von $\mathfrak{P}$ und $j \geq 1$. Wegen $p\mathfrak{P}^j \subseteq \mathfrak{P}^{j+1}$ ist $\mathfrak{P}^j/\mathfrak{P}^{j+1}$ ein $A/p$-Vektorraum. Die Abbildung $x \mapsto x\pi^j$ induziert einen Homomorphismus

$$B/\mathfrak{P} \to \mathfrak{P}^j/\mathfrak{P}^{j+1}$$

Die Dimension von $\mathfrak{P}^j/\mathfrak{P}^{j+1}$ ist also stets gleich der von $B/\mathfrak{P}$ über $A/p$, also gleich $f(\mathfrak{P}/p)$. Mit der Kompositionsreihe

$$B > \mathfrak{P} > \mathfrak{P}^2 > \cdots > \mathfrak{P}^e$$

erhält man $\dim B/\mathfrak{P}^e = e \cdot f$. Also ist

$$[L : K] = \dim B/pB = \sum_{\mathfrak{P}/p} e(\mathfrak{P}/p)f(\mathfrak{P}/p).$$


2.4.6 Korollar. Sei $a \in I(A)$, dann gilt

$$N^L_K(aB) = a^{[L:K]}.$$  

Beweis. Ist $p$ prim, $pB = \mathfrak{P}^{e_1} \cdot \cdots \cdot \mathfrak{P}^{e_r}$, so gilt

$$N^L_K(pB) = N^L_K(\mathfrak{P})^{e_1} \cdots N^L_K(\mathfrak{P})^{e_r} = p^{\sum e_iI_i} = p^{[L:K]}.$$  


2.4.7 Korollar. Sei $L$ Galois über $K$ und $p \in \text{Spec} A$. Dann sind alle $e(\mathfrak{P}/p)$ gleich (einer Zahl $e$) und alle $f(\mathfrak{P}/p)$ gleich (einer Zahl $f$). Ist $r = \#\{\mathfrak{P} : \mathfrak{P}/p\}$, so gilt

$$efr = [L : K].$$

Beweis. Man erhält alle $\mathfrak{P}/p$ aus einem durch Anwendung von $\sigma \in G$. Es ist $B/\mathfrak{P} \cong B/\sigma\mathfrak{P}$ und wegen $\sigma(pB) = pB$ sind die Exponenten $e_i$ auch alle gleich.


2.4.8 Korollar. Sei $L$ Galois über $K$ mit Gruppe $G$ und sei $\mathfrak{P}/p$. Dann gilt

$$(pB = (\mathfrak{P}_1 \cdot \cdots \cdot \mathfrak{P}_r)^e)$$

$$N^L_K(\mathfrak{P})B = \prod_{\sigma \in G} \sigma \mathfrak{P} = (\mathfrak{P}_1 \cdot \cdots \cdot \mathfrak{P}_r)^{ef}.$$ 

Es gilt $|G:\mathfrak{P}| = ef$.

Beweis. $G$ operiert transitiv auf $\{\mathfrak{P} : \mathfrak{P}/p\}$ und $G_{\mathfrak{P}}$ ist die Isotropiegruppe.


2.4.9 Korollar. Sei $A$ Dedekind, $K = Q(A)$, $E$ endliche separable Erweiterung von $K$, $B$ der ganze Abschluß von $A$ in $E$. Sei $b = (\beta)$ ein gebrochenes Hauptideal von $B$. Dann gilt

$$N^E_K(b) = (N^E_K(\beta))$$

wobei die Norm rechts die übliche Norm ist.
Beweis.
·) Sei \( L \) die kleinste Galois Erweiterung von \( K \) die \( E \) enthält. \( C \) der ganze Abschluß von \( B \) in \( L \). Es gilt, da \( L : E \) Galois ist

\[
N_{E}^{L}(bC) = b^{[L:E]}, \quad N_{E}^{L}(\beta) = \beta^{[L:E]}. 
\]

Haben wir die Aussage gezeigt für den Fall einer Galois Erweiterung, so haben wir

\[
N_{E}^{L}(bC) = (N_{E}^{L}(\beta)),
\]

und wegen

\[
N_{K}^{E} = N_{K}^{E} \circ N_{E}^{L},
\]

\[
N_{E}^{L}(b)^{[L:E]} = (N_{K}^{E}(\beta))^{[L:E]}.
\]

Wegen der eindeutigen Primzerlegung in \( I(A) \) folgt dann auch

\[
N_{K}^{E}(b) = (N_{K}^{E}(\beta)).
\]

·) Sei also \( \mathfrak{o} \mathfrak{B} \mathfrak{d} \mathfrak{A} \) \( E \) Galois über \( K \). Dann gilt \( N_{K}^{E}(\beta) = \prod_{\sigma \in G} \sigma \beta \), also

\[
(N_{K}^{E}(\beta))A \cdot B = \prod_{\sigma \in G} \sigma(\beta)B = \prod_{\sigma \in G} \sigma b = N_{K}^{E}b \cdot B
\]

wegen Korollar 2.4.8. Es folgt

\[
(N_{K}^{E}(\beta))_{A}^{[E:K]} = N_{K}^{E}[N_{K}^{E}(\beta)]_{A}B = N_{K}^{E}[N_{K}^{E}b \cdot B] = (N_{K}^{E}b)^{[E:K]}
\]

Wegen der eindeutigen Primzerlegung in \( I(A) \) folgt

\[
(N_{K}^{E}(\beta))_{A} = N_{K}^{E}b
\]

\( \square \)

2.4.10 Satz. Sei \( A \) diskreter Bewertungsring, \( K = Q(A) \), \( L \) endliche separable Erweiterung von \( K \), \( B \) ganze Abschluß von \( A \) in \( L \). Weiters liege nur ein \( \mathfrak{P} \in \text{Spec} B \) über dem maximalen Ideal \( \mathfrak{p} \) von \( A \), und sei der Körper \( B/\mathfrak{P} \) über \( A/\mathfrak{p} \) erzeugt von einem \( \beta \) mod \( \mathfrak{P} \), \( \beta \in B \). Sei \( \pi \) ein Element von \( B \) mit Ordnung 1 bei \( \mathfrak{P} \). Dann gilt \( A[\beta, \pi] = B \).

Beweis. Sei \( C = A[\beta, \pi] \). \( C \) ist ein \( A \)-Untermodul von \( B \). Wegen dem Nakayama Lemma angewendet auf \( B/C \) genügt es zu zeigen daß

\[
pB + C = B
\]

Sei \( pB = \mathfrak{P}^{e} \). Dann erzeugen die Elemente \( \beta \pi^{i} \) den Raum \( B/\mathfrak{P}^{e} \) als \( A/p \)-Vektorraum (vgl. Satz 2.4.5). Also kann man jedes \( x \in B \) schreiben als

\[
x = \sum c_{ij} \beta^{i} \pi^{j} \mod pB
\]

mit gewissen \( c_{ij} \in A \).
2.5. EXPLIZITE FAKTORISIERUNG EINER PRIMSTELLE

2.4.11 Satz. Sei A Dedekind und sei \(|A/p| < \infty\) für alle \(p \in \text{Spec } A\). Ist a Ideal von A bezeichne mit \(Na := |A/a|\). Dann gilt

\[ Na = \prod_p |Np|^{\sigma_p a}. \]

Beweis. Es ist \(A/a \cong \prod_p A/p^{\sigma_p a}\), Es genügt also \(|A/p^n|\) zu bestimmen. Dazu lokalisiere bei \(p\), dann ist \(O_D A\) p Hauptideal. Dann ist offenbar \(A/p \cong p/p^2 \cong \ldots\), also \(|A/p^n| = |A/p|^n|\).

\[ \Box \]

2.4.12 Bemerkung. Sei \(K\) ein algebraischer Zahlkörper \(O_K\) der Ring der ganzen Zahlen in \(K\). Sei \(p \in \text{Spec } O_K\), \(p/(p)\). Dann gilt

\[ N_p = p^{f(p/p)}. \]

Ist \(\alpha \in O_K\), so gilt \(N^K_a(\alpha) = \pm N(\alpha)\). Es gibt für jedes \(M\) nur endlich viele Ideale \(a\) mit \(Na \leq M\).

2.5 Explizite Faktorisierung einer Primstelle

Wir betrachten die folgende Situation: A Dedekind, \(K = Q(A)\), \(E\) endliche separable Erweiterung von \(K\), \(B\) ganze Abschluß von \(A\) in \(E\). Sei \(p \in \text{Spec } A\).

Sei vorausgesetzt \(B = A[\alpha]\) für ein geeignetes \(\alpha \in B\).

2.5.1 Bemerkung. Es gilt nicht immer \(B = A[\alpha]\). Jedoch ist für alle bis auf endlich viele \(p \in \text{Spec } A\)

\[ B_p = A_p[\alpha_p]. \]

Sei \(f\) das Minimalpolynom von \(\alpha\) (über \(K\)). Beachte daß \(f \in A[X]\). Die kanonische Projektion

\[ \pi : A \to A/p =: \bar{A} \]

sei (koeffizientenweise) fortgesetzt zu \(\bar{\pi} : A[X] \to \bar{A}[X]\). Sei \(\bar{f} := \bar{\pi}f\) und sei

\[ \bar{f}(X) = \bar{P}_1(X)^{e_1} \cdots \bar{P}_r(X)^{e_r}, \]

\(\bar{P}_i = \bar{A}[X]\), \(\bar{P}_i = \bar{\pi}P_i\), \(P_i\) normiert, die Zerlegung von \(\bar{f}\) in irreduzible (normierte) Faktoren. Sei \(L\) ein algebraischer Abschluß von \(\bar{A}\). Sei \(\Phi\) die Menge aller Fortsetzungen \(\phi\) von \(\pi\) zu einem Homomorphismus \(\phi : B \to L\).

\(\Phi\) steht in bijektiver Beziehung zu der Nullstellennmenge von \(\bar{f}\) vermöge \(\phi \mapsto \phi(\alpha)\). Denn wegen \(f(\alpha) = 0\) muß für \(\phi \in \Phi\) gelten

\[ 0 = \phi(f(\alpha)) = \bar{f}(\phi(\alpha)). \]

Ist umgekehrt \(\bar{f}(\beta) = 0\), so ist die Abbildung

\[ \phi : \begin{array}{c} B \\ g(\alpha) \end{array} \to \begin{array}{c} L \\ \bar{g}(\beta) \end{array} \quad (g = A[X]) \]

wohldefiniert: Ist \(g(\alpha) = 0\), so folgt \(f|g\) also auch \(\bar{f}|\bar{g}\), also \(\bar{g}(\beta) = 0\). Offenbar setzt \(\phi\) auch \(\pi\) fort. Wegen \(B = A[\alpha]\) ist \(\phi\) überall definiert. Weiters wegen \(B = A[\alpha]\) ist ein \(\phi \in \Phi\) durch \(\phi(\alpha)\) eindeutig bestimmt.
2.5.2 **Satz.** Seien \( \phi, \psi \in \Phi \), dann ist \( \ker \phi = \ker \psi \) genau dann, wenn \( \phi(\alpha) \) und \( \psi(\alpha) \) Nullstellen des gleichen irreduziblen Faktors \( \overline{P}_i \) sind. Es gilt

\[
\{ \mathfrak{p} \in \text{Spec} \ B : \mathfrak{p}/p \} = \{ \ker \phi : \phi \in \Phi \},
\]

d.h. die über \( p \) liegenden Primideale stehen in bijektiver Beziehung zu den irreduziblen Faktoren von \( f \). Gehört \( \mathfrak{p} \) zu \( \overline{P}_i \), so gilt

\[
e(\mathfrak{p}/p) = e_i, \ f(\mathfrak{p}/p) = \deg \overline{P}_i, \ \mathfrak{p} = pB + \overline{P}_i(\alpha)B.
\]

**Beweis.**

\( \cdot \) Es gilt \( \ker \phi \cap A = p \): Da \( \phi \) die Projektion \( \pi \) fortsetzt ist \( p \subseteq \ker \phi \). Sei \( \gamma \in A \cap \ker \phi \). Dann ist

\[
0 = \phi(\gamma) = \pi(\gamma),
\]

d.h. \( \gamma \in p \) (\( p \) das maximale Ideal von \( A \)).

\( \cdot \) Betrachte das Diagramm

\[
\begin{array}{ccc}
A[X] & \xrightarrow{\pi} & \overline{A}[X] \\
\downarrow{\tau_\alpha} & & \downarrow{\tau_\beta} \\
B & \xrightarrow{\phi} & \text{Im } \phi \subseteq L \\
\end{array}
\]

wobei \( \tau_\alpha \) bzw. \( \tau_\beta \) die Punktauswertung an \( \alpha \) bzw. \( \beta \) ist und \( \beta = \phi(\alpha) \). Sei \( \beta \) Nullstelle von \( \overline{P}_i \), dann faktorisiert sich \( \tau_\beta \) als

\[
\begin{array}{ccc}
\overline{A}[X] & \xrightarrow{\tau_\beta} & \overline{A}[X]/(\overline{P}_i) \\
\downarrow{\tau_\beta} & & \downarrow{\tau_\beta} \\
\text{Im } \phi & & \\
\end{array}
\]

und \( \phi \) als
2.5. EXPLIZITE FAKTORISIERUNG EINER PRIMSTELLE

\[
\begin{array}{c}
B \\
\phi \\
\downarrow \\
\text{Im } \phi \\
\downarrow \\
\tilde{\phi} \\
\downarrow \\
B/\ker \phi \\
\end{array}
\]

Es folgt \( B/\ker \phi \cong \tilde{A}[X]/(\tilde{P}_i) \). Da \( \tilde{P}_i \) irreduzibel ist, folgt \( \ker \phi \in \text{Spec } B \). Weiter ist

\[ \ker \tau_\beta \circ \tilde{\pi} = \ker \phi \circ \tau_\alpha. \]

Die linke Seite ist gleich \( \tilde{\pi}^{-1}((\tilde{P}_i)) \), die rechte gleich \( \tau_\alpha^{-1}(\ker \phi) \). Da \( \tau_\alpha \) surjektiv ist, folgt

\[ \ker \phi = \tau_\alpha(\tau_{\alpha}^{-1}(\ker \phi)) = \tau_\alpha(\tilde{\pi}^{-1}((\tilde{P}_i))), \]

gehören also \( \phi, \psi \) zu \( \tilde{P}_i \) so ist \( \ker \phi = \ker \psi \).

\( \cdot \) Ist umgekehrt \( \ker \phi = \ker \psi \), und gehört \( \phi \) zu \( \tilde{P}_i \) und \( \psi \) zu \( \tilde{P}_j \), so folgt

\[ (\tilde{P}_i) = \tilde{\pi}(\tilde{\pi}^{-1}((\tilde{P}_i))) = \tilde{\pi}(\tau_\alpha^{-1}(\ker \phi)) = \tilde{\pi}(\tau_\alpha^{-1}(\ker \psi)) = (\tilde{P}_j), \]

also \( \tilde{P}_i = \tilde{P}_j \).

\( \cdot \) Sei \( \mathfrak{P} \in \text{Spec } B, \mathfrak{P}/p \), und sei \( L' \) ein algebraischer Abschluß von \( A/p \) mit \( L' \supseteq B/\mathfrak{P} \). \( L' \cong L \) über \( \tilde{A} \) vermöge \( \iota, \sigma : B \rightarrow B/\mathfrak{P} \) die kanonische Projektion. Dann ist

\[ \phi := \iota \circ \sigma : B \rightarrow L \]

eine Fortsetzung von \( \pi \) und \( \ker \phi = \mathfrak{P} \).

\( \cdot \) Wie schon festgestellt, ist (wenn \( \mathfrak{P}/p \) zu \( \tilde{P}_i \) gehört)

\[ B/\mathfrak{P} \cong \tilde{A}[X]/(\tilde{P}_i) \]

und dieser Isomorphismus ist ein \( \tilde{A} \)-Vektorraum Isomorphismus denn eingeschränkt auf \( \tilde{A} \) ist er id. Also folgt

\[ f(\mathfrak{P}/p) = [B/\mathfrak{P} : \tilde{A}] = \deg \tilde{P}_i (= \deg P_i) \]

Es gilt \( pB = \tau_\alpha(p[X]) \). Denn ist \( \gamma \in B \), so schreibt sich \( \gamma = g(\alpha) \) und daher \( p\gamma = (pg)(\alpha) \) und für \( p \in \mathfrak{P} \) ist \( pg \in p[X] \). Umgekehrt ist

\[ \tau_\alpha(pX^k) = p\alpha^k \in pB. \]

Offenbar ist \( p[X] = \ker \tilde{\pi} \). Gehört nun \( \mathfrak{P} \) zu \( \tilde{P}_i \) so ist

\[ \mathfrak{P} = \ker \phi = \tau_\alpha(\tilde{\pi}^{-1}((\tilde{P}_i))) = \tau_\alpha((P_i)_{\tilde{A}[X]} + p[X]) = P_i(\alpha)B + pB. \]
Es gilt $f - P_1^{e_1} \cdots P_r^{e_r} \in \ker \pi = p[X]$, also wegen $f(\alpha) = 0$

$$-P_1(\alpha)^{e_1} \cdots P_r(\alpha)^{e_r} = \pi(f - P_1^{e_1} \cdots P_r^{e_r}) \in pB.$$  

Nun gilt, wenn $\Psi_i / p$ zu $\tilde{\Psi}_i$ gehört,

$$\Psi_i^{e_i} \subseteq pB + P_i^{e_i}(\alpha)B,$$

also folgt

$$\Psi_1^{e_1} \cdots \Psi_r^{e_r} \subseteq pB + P_1^{e_1}(\alpha) \cdots P_r^{e_r}(\alpha)B \subseteq pB.$$  

Damit ist

$$e_i \geq e(\Psi_i / p), \ i = 1, \ldots, r.$$  

Wegen

$$\sum e_i \deg P_i = \deg f = \left[ E : K \right] = \sum e(\Psi_i / p) f(\Psi_i / p) =: \sum e(\Psi_i / p) \deg P_i$$

folgt $e_i = e(\Psi_i / p)$.  

\[
\square
\]

## 2.6 Die Diskriminante

Sei im folgenden $L / K$ endliche Erweiterung, $[L : K] = n$.

### 2.6.1 Definition. Seien $\alpha_1, \ldots, \alpha_n \in K$. Dann heißt

$$\Delta(\alpha_1, \ldots, \alpha_n) := \det(\text{tr}(\alpha_i \alpha_j))_{i,j=1}^n$$

die Diskriminante von $\alpha_1, \ldots, \alpha_n$.

### 2.6.2 Satz. Ist $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, dann ist $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von $L/K$. Ist $L/K$ separabel auch umgekehrt.

**Beweis.**

1. Seien $\alpha_1, \ldots, \alpha_n$ linear abhängig. Dann existieren $a_1, \ldots, a_n \in K$, nicht alle gleich 0, so dass $\sum a_i \alpha_i = 0$. Es folgt

$$\sum a_i \text{tr}(\alpha_i \alpha_j) = 0, \ j = 1, \ldots, n,$$

also muß $\det(\text{tr}(\alpha_i \alpha_j))_{i,j=1}^n = 0$ gelten.

2. Seien $\alpha_1, \ldots, \alpha_n$ linear unabhängig und sei $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Dann gibt es eine nichttriviale Lösung $x_1, \ldots, x_n$ von

$$\sum x_i \text{tr}(\alpha_i \alpha_j) = 0, \ j = 1, \ldots, n.$$  

Setze $\alpha := \sum x_i \alpha_i$. Dann ist $\alpha \neq 0$. Es gilt $\text{tr}(\alpha \alpha_j) = 0$ für alle $j = 1, \ldots, n$. Da $\alpha_1, \ldots, \alpha_n$ Basis folgt $\text{tr}(\alpha \beta) = 0$, $\beta \in L$, also $\text{tr} \gamma = 0$, $\gamma \in L$. WS! zu $L/K$ separabel.

\[
\square
\]
2.6. DIE DISKRIMINANTE

2.6.3 Lemma. Seien \( \{\alpha_1, \ldots, \alpha_n\} \), \( \{\beta_1, \ldots, \beta_n\} \) Basen von \( L/K \). Seien \( a_{ij} \in K \) sodass \( \alpha_i = \sum a_{ij} \beta_j \). Dann gilt

\[
\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 \Delta(\beta_1, \ldots, \beta_n).
\]

Beweis. Es gilt

\[
\alpha_i \alpha_k = \sum_{j=1}^{n} a_{ij} a_{kj} \beta_j \beta_k.
\]

Setze \( A = (\text{tr}(\alpha_i \alpha_k)), B = (\text{tr}(\beta_j \beta_k)), C = (a_{ij}) \), dann ist \( A = C^T B C \).

2.6.4 Lemma. Sei \( L/K \) separabel, \( \{\sigma_j : j = 1, \ldots, n\} \) die Einbettungen von \( L/K \). Dann gilt

\[
\Delta(\alpha_1, \ldots, \alpha_n) = \left( \det(\sigma_j(\alpha_i))_{i,j=1}^{n} \right)^2.
\]

Beweis. Es gilt

\[
\text{tr}(\alpha_i \alpha_j) = \sum_i \sigma_i(\alpha_i \alpha_j).
\]

Setze \( A = (\text{tr}(\alpha_i \alpha_j)), B = (\sigma_i(\alpha_i)) \), dann gilt \( A = BB^T \).

2.6.5 Satz. Sei \( L/K \) separabel und sei \( \beta \in L \) sodass \( \{1, \beta, \ldots, \beta^{n-1}\} \) linear unabhängig ist. Sei \( f \in K[X] \) das Minimalpolynom von \( \beta \) über \( K \). Dann gilt

\[
\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N(f'()\beta)).
\]

Beweis. Die Determinante der Vandermonde Matrix \( (\sigma_j(\beta^i)) \) ist gleich

\[
\prod_{i<j}(\sigma_j(\beta) - \sigma_i(\beta)),
\]

und es folgt

\[
\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\sigma_j(\beta) - \sigma_i(\beta)).
\]

Es gilt \( f(X) = \prod_i (X - \sigma_i(\beta)) \) und daher

\[
f'(\sigma_j(\beta)) = \prod_{i \neq j}(\sigma_j(\beta) - \sigma_i(\beta), \ j = 1, \ldots, n.
\]

Nun ist \( f'(\sigma_j(\beta)) = \sigma_j(f'(\beta)) \) und

\[
N(f'(\beta)) = \prod_j \sigma_j(f'(\beta)).
\]
2.6.6 Satz. Sei $K$ ein algebraischer Zahlkörper, $n = [K : \mathbb{Q}]$, $a \in O_K$. Sei $\alpha_1, \ldots, \alpha_n \in a$ eine Basis von $K/\mathbb{Q}$, sodass $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimal ist (solche $\alpha_1, \ldots, \alpha_n$ existieren stets). Dann gilt

$$a = Z\alpha_1 + \cdots + Z\alpha_n.$$  

Und umgekehrt.

Beweis.

.: Es gibt stets eine Basis in $\alpha$, denn es gibt eine in $O_K$ und multipliziert man diese mit einem $a \in \alpha \setminus \{0\}$, so hat man das Gewünschte. Es gilt $\Delta(\alpha_1, \ldots, \alpha_n) \in Z \setminus \{0\}$ also $|\Delta(\alpha_1, \ldots, \alpha_n)| \in \mathbb{N}$, daher existiert eine Basis mit der geforderten Minimalitätseigenschaft.

.: Trivial ist $Z\alpha_1 + \cdots + Z\alpha_n \subseteq \alpha$. Sei also $\alpha \in \alpha$ und schreibe

$$\alpha = \gamma_1 \alpha_1 + \cdots + \gamma_n \alpha_n, \quad \gamma_i \in \mathbb{Q}.$$  

Sind alle $\gamma_i \in Z$ sind wir fertig. Sei angenommen ein $\gamma_i \not\in Z$, o.B.d.A $\gamma_1 \not\in Z$. Schreibe $\gamma_1 = \theta m + \vartheta, m \in Z, 0 < \vartheta < 1$, und setze

$$\beta_1 := \alpha - m \alpha_1, \quad \beta_2 := \alpha_2, \ldots, \beta_n := \alpha_n.$$  

Dann ist $\{\beta_1, \ldots, \beta_n\}$ eine Basis und $\subseteq \alpha$. Die Transformationsmatrix zwischen diesen Basen ist wegen $\beta_1 = \vartheta \alpha_1 + \gamma_2 \alpha_2 + \cdots + \gamma_n \alpha_n$ gleich

$$\begin{pmatrix} \vartheta & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$  

Wir erhalten $|\Delta(\beta_1, \ldots, \beta_n)| = |\vartheta^2 \Delta(\alpha_1, \ldots, \alpha_n)| < |\Delta(\alpha_1, \ldots, \alpha_n)|$ ein WSI zur Minimalitätseigenschaft.

.: Sind $\{\alpha_1, \ldots, \alpha_n\}$ und $\{\beta_1, \ldots, \beta_n\}$ Basen mit $a = Z\alpha_1 + \cdots + Z\alpha_n = Z\beta_1 + \cdots + Z\beta_n$, so ist die Transformationsmatrix ganzzahlig und invertierbar. Ihre Determinante also $= \pm 1$.

$\square$

DEI.67

2.6.7 Definition. Der Wert $\Delta(a) = \min |\Delta(\alpha_1, \ldots, \alpha_n)|$ heißt die Diskriminante von $a$, $\delta_K := \Delta(O_K)$ kurz Diskriminante von $K$.

LEI.67a

2.6.8 Lemma. Sei $F/\mathbb{Q}$ ein algebraischer Zahlkörper, $[F : \mathbb{Q}] = n$. Sei $\alpha_1, \ldots, \alpha_n \in O_F$ eine Basis von $F/\mathbb{Q}$. Dann gilt

$$\Delta(\alpha_1, \ldots, \alpha_n) O_F \subseteq Z\alpha_1 + \cdots + Z\alpha_n.$$  

Beweis. Sei $w \in O_F$, $w = \sum a_i \alpha_i$, $a_i \in \mathbb{Q}$ Alle Elemente $\text{tr}(w \alpha_j)$ und $\text{tr}(\alpha_i \alpha_j)$ sind in $Z$ und es gilt

$$\text{tr}(w \alpha_j) = \sum a_i \text{tr}(\alpha_i \alpha_j), \quad j = 1, \ldots, n.$$
Wegen der Cramerschen Regel schreibt sich $a_i$ als ganze Zahl dividiert durch $\Delta(a_1, \ldots, a_n)$.

Sei $K$ ein algebraischer Zahlkörper, $[K : \mathbb{Q}] = n$. Wir konstruieren eine Ganzheitsbasis.

**2.6.9 Satz.** Seien $a_1, \ldots, a_n \in O_K$ linear unabhängig (über $\mathbb{Q}$). Dann existiert eine Ganzheitsbasis $w_1, \ldots, w_n$ so daß

$$a_j = c_{ji} w_1 + \cdots + c_{jj} w_j, \quad j = 1, \ldots, n,$$

mit gewissen $c_{ji} \in \mathbb{Z}$.

*Beweis.*

(1) Sei $d_{ii}$ die kleinste natürliche Zahl so daß für gewisse $d_{i1}, \ldots, d_{i,i-1} \in \mathbb{Z}$

$$w_i = \frac{1}{\Delta(a_1, \ldots, a_n)} \sum_{j=1}^{i} d_{ij} a_j \in O_K.$$

Die $w_i$ sind linear unabhängig über $\mathbb{Q}$, denn sie entstehen aus $(a_1, \ldots, a_n)$ durch Multiplikation mit einer Dreiecksmatrix und $d_{ii} \neq 0$.

(2) Sei $c \in O_K$ von der Form

$$c = \frac{1}{\Delta(a_1, \ldots, a_n)} (c_1 a_1 + \cdots + c_j a_j)$$

für gewisse $c_i \in \mathbb{Z}$ und ein gewisses $j \in \{1, \ldots, n\}$. Dann gilt $d_{jj} | c_j$: Schreibe $c_j = s d_{jj} + r$ mit $s, r \in \mathbb{Z}$, $0 \leq r < d_{jj}$. Es ist

$$c - s w_j \in O_K$$

und es ist

$$c - s w_j = \frac{1}{\Delta(a_1, \ldots, a_n)} \left( (c_1 - s d_{jj}) a_1 + (c_2 - s d_{jj}) a_2 + \cdots + r a_j \right),$$

ein WS! zur Minimalität von $d_{jj}$ falls nicht $r = 0$.

(3) Sei $M_0$ der von $w_1, \ldots, w_n$ erzeugte $\mathbb{Z}$-Modul. Wir zeigen mit Induktion nach $j$, daß jedes Element von $O_K$ der Gestalt

$$x = \frac{1}{\Delta(a_1, \ldots, a_n)} (x_1 a_1 + \cdots + x_j a_j), \quad x_i \in \mathbb{Z},$$

in $M_0$ liegt. Für $j = n$ heißt dies wegen Lemma 2.6.8 daß $M_0 = O_K$.

$j = 1$ wegen dem letzten Punkt ist $d_{11} | x_1$ und daher $x = \frac{x_1}{d_{11}} w_1 \in M_0$.

$j - 1 \rightarrow j$ Es gilt $d_{jj} | x_j$. Es ist

$$x - \frac{x_j}{d_{jj}} w_j \in O_K$$

und nach Induktionsvoraussetzung in $M_0$: $\frac{x_j}{d_{jj}} w_j \in M_0$, also folgt $x \in M_0$. 


2.6.10 Satz. Seien \( a_1, \ldots, a_n \in O_K \) linear unabhängig über \( \mathbb{Q} \) und sei \( m \) der Index von \( M = \mathbb{Z} a_1 + \cdots + \mathbb{Z} a_n \) in \( O_K \). Dann gilt

\[
\Delta(a_1, \ldots, a_n) = \pm m^2 \delta_K.
\]

Beweis. Sei \( w_1, \ldots, w_n \) eine Ganzheitsbasis von \( O_K \). Sei \( b_1, \ldots, b_n \in M \) so daß

\[
b_i = \sum_{k=1}^{n} c_{ik} w_k, \quad c_{ik} \in \mathbb{Z},
\]

wobei \( c_{ii} \in \mathbb{N} \) kleinstmöglich ist. Genau wie in Satz 2.6.9 sieht man daß \( b_1, \ldots, b_n \) ein freies Erzeugendensystem von \( M \) ist und das \( t_1 w_1 + \cdots + t_i w_i \) \( (t_j \in \mathbb{Z}) \) nur in \( M \) liegen kann, wenn \( c_{ii} \) ist. Also sind die Zahlen

\[
\alpha_1 w_1 + \cdots + \alpha_n w_n, \quad 0 \leq \alpha_j < c_{jj},
\]

paarweise inkongruent modulo \( M \). Offenbar sind es genau \( c_1 \cdot \ldots \cdot c_n \) viele.

Wir zeigen, daß sie ein vollständiges Repräsentantensystem modulo \( M \) bilden. Sei

\[
\xi = \sum_{k=1}^{n} \lambda_k w_k, \quad \lambda_k \in \mathbb{Z},
\]

ein Element von \( O_K \). Sei \( 0 \leq \mu_n < c_{nn} \) so daß \( \lambda_n \equiv \mu_n \) mod \( c_{nn} \) und setze

\[
A_n = \frac{\lambda_n - \mu_n}{c_{nn}},
\]

Dann gilt

\[
\xi = A_n b_n + \mu_n w_n + \sum_{k=1}^{n-1} (\lambda_k - A_n c_{nk}) w_k.
\]

Sei \( 0 \leq \mu_{n-1} < c_{n-1,n-1} \), so daß \( \lambda_{n-1} = A_n c_{n,n-1} \equiv \mu_{n-1} \) mod \( c_{n-1,n-1} \). Setze

\[
A_{n-1} = \frac{\lambda_{n-1} - \mu_{n-1} - A_n c_{n,n-1}}{c_{n-1,n-1}}.
\]

Dann gilt

\[
\xi = A_n b_n + \mu_n w_n + A_{n-1} b_{n-1} + \mu_{n-1} w_{n-1} + \sum_{k=1}^{n-2} (\lambda_k - A_n c_{nk} - A_{n-1} c_{n-1,k}) w_k.
\]

Verfährt man weiter, so erhält man schließlich

\[
\xi = \sum_{k=1}^{n} \alpha_k b_n + \sum_{k=1}^{n} \mu_k w_k
\]

wobei \( \alpha_k, \mu_k \in \mathbb{Z}, \quad 0 \leq \mu_k < c_{kk} \). Also ist der Index

\[
m = [O_K : M] = c_1 \cdot \ldots \cdot c_{nn}.
\]
2.7. QUADRATISCHE ZAHLKÖRPER, KREISTEILUNGSKÖRPER

und

\[ \Delta(b_1, \ldots, b_n) = (\det(c_{ij}))^2 \Delta(w_1, \ldots, w_n) = (c_1 \cdot \ldots \cdot c_{nn})^2 \delta_K. \]

Da sowohl \( \{a_1, \ldots, a_n\} \) als auch \( \{b_1, \ldots, b_n\} \) den Modul \( M \) erzeugen ist

\[ (a_1, \ldots, a_n) = (b_1, \ldots, b_n)(\gamma_{ij}) \]

mit \( (\gamma_{ij}) \in \mathbb{Z}^{n \times n} \) invertierbar, also

\[ \Delta(a_1, \ldots, a_n) = \pm \Delta(b_1, \ldots, b_n). \]

\[
\Box
\]

2.6.11 Lemma. Ist \( n \in \mathbb{Z}, a \in K, b = a + n, \) so gilt \( \Delta(1, a, \ldots, a^{n-1}) = \Delta(1, b, \ldots, b^{n-1}). \)

Beweis. Wie in Satz 2.6.5 gilt

\[ \Delta(1, a, \ldots, a^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_j(a) - \sigma_i(a)). \]

Es ist

\[ \sigma_j(b) - \sigma_i(b) = (\sigma_j(a) + n) - (\sigma_i(a) + n) = \sigma_j(a) - \sigma_i(a). \]

\[
\Box
\]

2.7 Quadratische Zahlkörper, Kreisteilungskörper

Ein algebraischer Zahlkörper \( F \) heißt quadratischer Zahlkörper, wenn \( |F : \mathbb{Q}| = 2. \)

2.7.1 Satz. Sei \( F \) ein quadratischer Zahlkörper. Dann ist \( F = \mathbb{Q}(\sqrt{d}) \) für eine gewisse quadratfreie ganze Zahl \( d. \) \( F/\mathbb{Q} \) ist Galois mit Gruppe

\[ G = \{ \text{id}_F, \sqrt{d} \mapsto -\sqrt{d} \}. \]

Es gilt

\[ \mathcal{O}_F = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d}, & d \equiv 2, 3 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{-1+\sqrt{d}}{2}, & d \equiv 1 \mod 4 \end{cases} \]

Beweis.

\( \cdot \) Sei \( \alpha \in F \setminus \mathbb{Q}. \) Dann gilt \( F = \mathbb{Q}(\alpha) \) und \( \alpha \) muß einer Gleichung der Gestalt

\[ aX^2 + bX + c = 0 \]

mit gewissen \( a, b, c \in \mathbb{Z} \) genügen. Es folgt

\[ \alpha = \frac{1}{2a} \left( -b \pm \sqrt{b^2 - 4ac} \right). \]
Schreibe $b^2 - 4ac$ in der Form $A^2d$ mit $A, d \in \mathbb{Z}, d$ quadratfrei. Dann gilt offenbar

$$\alpha = \frac{1}{2a}( - b \pm A\sqrt{d} ),$$

also ist $F = \mathbb{Q}(\sqrt{d})$.

1. Die Abbildung

$$\sigma : \begin{cases} F & \rightarrow F \\ a + b \sqrt{d} & \mapsto a - b \sqrt{d}. \end{cases}$$

ist offenbar ein Automorphismus von $F/\mathbb{Q}$, denn $\sqrt{d}, -\sqrt{d}$ sind Nullstellen des irreduziblen Polynoms $X^2 - d$. Der Fixpunktkörper von $G = \{\text{id}_F, \sigma\}$ ist gleich $\mathbb{Q}$, also ist $F/\mathbb{Q}$ Galois mit Gruppe $G$. $F$ ist der Zerfallungskörper des separablen Polynoms $X^2 - d$.

1. Ist $\gamma \in \mathcal{O}_F$, so ist $\text{tr}_F^\mathbb{Q}(\gamma), N_F^\mathbb{Q}(\gamma) \in \mathbb{Z}$. Da das Minimalpolynom von $\gamma$ die Gestalt $X^2 - \text{tr}_F^\mathbb{Q}(\gamma)X + N_F^\mathbb{Q}(\gamma)$ hat gilt auch die Umkehrung. Man berechnet für $\gamma = r + s\sqrt{d}, r, s \in \mathbb{Q}$

$$\text{tr}_F^\mathbb{Q}(\gamma) = 2r, \ N_F^\mathbb{Q}(\gamma) = r^2 - s^2d.$$  

Es folgt

$$\gamma \in \mathcal{O}_F \Leftrightarrow 2r \in \mathbb{Z} \wedge r^2 - s^2d \in \mathbb{Z}.$$  

Sei nun $\gamma \in \mathcal{O}_F$. Dann folgt $4s^2d \in \mathbb{Z}$ und da $d$ quadratfrei ist $2s \in \mathbb{Z}$. Bezeichne $m := 2r, n = 2s$. Dann gilt $m^2 - n^2d = 4(r^2 - s^2d) \equiv 0 \mod 4$.

Sei $d \equiv 1, 3 \mod 4$. Dann gilt

$$0 \equiv m^2 - dn^2 \equiv \begin{cases} m^2 + 2n^2 & , d \equiv 2 \\ m^2 + n^2 & , d \equiv 3 \quad (\mod 4) \end{cases}$$

Da

$$x^2 \equiv \begin{cases} 0 & , x \text{ gerade} \\ 1 & , x \text{ ungerade} \quad (\mod 4) \end{cases}$$

ist dies nur möglich für $m, n$ gerade. Es folgt $r, s \in \mathbb{Z}$. Umgekehrt ist trivialerweise $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathcal{O}_K$, denn $\sqrt{d} \in \mathcal{O}_K$.

Sei $d \equiv 1 \mod 4$. Dann ist $m^2 - dn^2 \equiv m^2 - n^2 \mod 4$, also sind $m$ und $n$ entweder beide gerade oder beide ungerade. Es ist

$$\gamma = \frac{m}{2} + \frac{n}{2}\sqrt{d} = \frac{m + n}{2} - \frac{1 + \sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\sqrt{d} = \frac{1 + \sqrt{d}}{2}.$$

Umgekehrt ist $\text{tr}_F^\mathbb{Q}(\frac{1 + \sqrt{d}}{2}) = -1, N_F^\mathbb{Q}(\frac{1 + \sqrt{d}}{2}) = \frac{1 - d}{4} \in \mathbb{Z}$.

\[\square\]
2.7. QUADRATISCHE ZAHLKÖRPER, KREISTEILUNGSKÖRPER

2.7.2 Lemma. Es gilt

\[ \delta_F = \begin{cases} 4d & , d \equiv 2, 3 \mod 4 \\ d & , d \equiv 1 \mod 4 \end{cases} \]

Beweis.

\( \triangleright \) Sei \( d \equiv 2, 3 \mod 4, \alpha_1 = 1, \alpha_2 = \sqrt{d} \). Dann ist

\[ \delta_F = \det(\text{tr}(\alpha_i \alpha_j)) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d. \]

\( \triangleright \) Sei \( d \equiv 1 \mod 4, \alpha_1 = 1, \alpha_2 = \frac{1 + \sqrt{d}}{2} \). Dann ist

\[ (\text{tr}(\alpha_i \alpha_j)) = \begin{pmatrix} 2 & -1 \\ -1 & \frac{1 - \sqrt{d}}{2} \end{pmatrix}, \]

also \( \delta_F = d \).

\[ \blacklozenge \]

Den durch \( \sqrt{d} \rightarrow -\sqrt{d} \) gegebenen Anhomorphismus von \( F/\mathbb{Q} \) bezeichne mit \( x \mapsto x' \). Ist \( p \) eine Primzahl, und ist \( p \in \text{Spec } O_F, p/(p), \) so sind alle über \( (p) \) liegenden Primideale gegeben durch \( \{p, p'\} \) (es kann \( p = p' \) sein).

2.7.3 Satz. Sei \( p \) Primzahl. Dann gilt:

Fall \( p \) ungerade:

(i) \( p \nmid \delta_F, d \text{ quadratischer Rest } \mod p \Rightarrow (p) = pp', p \neq p' \).

(ii) \( p \nmid \delta_F, d \text{ quadratischer Nichtrest } \mod p \Rightarrow (p) = p. \)

(iii) \( p^2 \delta_F \Rightarrow (p) = p^2. \)

Fall \( p = 2; \)

(i) \( 2 \nmid \delta_F, d \equiv 1 \mod 8 \Rightarrow (2) = pp', p \neq p' \)

(ii) \( 2 \nmid \delta_F, d \equiv 5 \mod 8 \Rightarrow (2) = p \)

(iii) \( 2^2 \delta_F \Rightarrow (2) = p^2 \)

Bemerkungen: Ist \( d \equiv 2, 3 \mod 8, \) so ist \( \delta_F \equiv 4d \) also \( 2 \mid \delta_F. \) Ist \( d \equiv 0, 4 \mod 8 \) so ist \( d \) nicht quadratfrei.

Beweis. Sei \( r = \#\{p \in \text{Spec } O_F : p/(p)\} \), \( e \) der (gemeinsame) Verzweigungindex und \( f \) der (gemeinsame) Restklassengrad. Wegen \( efr = [F : \mathbb{Q}] = 2 \) können nur drei Fälle eintreten:

(I) \( r = 2, e = 1, f = 1 \)

(II) \( r = 1, e = 1, f = 2 \)

(III) \( r = 1, e = 2, f = 1 \)

Sei \( p \neq 2. \)
(i): Sei \( a^2 \equiv d \mod p \). Wir zeigen
\[
(p) = (p)\left(p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2 - d}{p}\right) = (p, a + \sqrt{d}, a - \sqrt{d}).
\]

Zum ersten "\(": Der zweite Faktor rechts enthält \( p \) und \( 2a \). Da \( p, 2a \) relativ prim sind, ist er gleich \( O_F \). Zum zweiten "\(": Es gilt:
\[
p \cdot p = p \cdot (a + \sqrt{d}) \cdot p, p(a - \sqrt{d}) = p \cdot (a - \sqrt{d}),
\]
\[
p \cdot \frac{a^2 - d}{p} = (a + \sqrt{d})(a - \sqrt{d}).
\]

Es kann nicht gelten \((p, a + \sqrt{d}), (p, a - \sqrt{d}) \subseteq p\), denn dann würde \( p \) sowohl \( p \) als auch \( 2a \) enthalten. Also gibt es mehr als ein Primideal über \( (p) \).

(ii): Sei \( p/(p) \). Wir zeigen \( f(p/(p)) = 2 \). Wäre \( f(p/(p)) = 1 \), so ist also \( O_F/p = \mathbb{Z}/p\mathbb{Z} \). Sei \( a \in \mathbb{Z} \), so dass \( a \equiv \sqrt{d} \mod p \), dann gilt \( a^2 \equiv d \mod p \) und wegen \( p/(p) \) auch \( a^2 \equiv d \mod p \). WS!

(iii): Wir zeigen
\[
(p) = (p)(p, \sqrt{d}/p) = (p, \sqrt{d}).
\]

Zum ersten "\(": Der zweite Faktor ist gleich \( O_F \) denn er enthält \( p \) und \( \sqrt{d} \) und die beiden sind relativ prim denn \( d \) ist quadratfrei. Zum zweiten "\(": Es gilt
\[
p \cdot p = p \cdot p, p\sqrt{d} = p\sqrt{d}, p \cdot \frac{d}{p} = \sqrt{d} \cdot \sqrt{d}.
\]

Es folgt dass jedes \( \mathfrak{p} \) in der Darstellung von \( (p) \) mindestens quadratisch auftreten muss.

Sei \( p = 2 \):

(i): Sei \( d \equiv 1 \mod 8 \) (dann ist \( \delta_F = d \) also \( 2 \nmid \delta_F \)). Es gilt
\[
(2) = (2, 1 + \sqrt{d}/2, 1 - \sqrt{d}/2) = (2, 1 + \sqrt{d}/2, 1 - \sqrt{d}/2).
\]
Zum ersten "\(": Der zweite Faktor ist gleich \( O_F \). Zum zweiten "\(":
\[
2 \cdot 2 = 2 \cdot 2, 2 \cdot \frac{1 + \sqrt{d}}{2} = \frac{1 + \sqrt{d}}{2}, 2 \cdot \frac{1 - \sqrt{d}}{2} = \frac{1 - \sqrt{d}}{2},
\]
\[
\frac{2 - 1 - d}{8} = \frac{1 + \sqrt{d}}{2}, \frac{1 - \sqrt{d}}{2}.
\]

Weiter kann nicht \((2, \frac{1 + \sqrt{d}}{2}), (2, \frac{1 - \sqrt{d}}{2}) \subseteq p \), denn sonst \( 1 \in \mathfrak{p} \).

(ii): Sei \( d \equiv 5 \mod 8 \) (wieder ist \( \delta_F = d \) also \( 2 \nmid \delta_F \)). Sei \( p|(2) \), und angenommen \( f(p/(2)) = 1 \). Dann existiert \( a \in \mathbb{Z} \) mit \( a \equiv \frac{1 + \sqrt{d}}{2} \mod p \). Da \( \frac{1 + \sqrt{d}}{2} \) der Gleichung \( X^2 - X + \frac{1 - d}{4} = 0 \) genügt folgt \( a^2 - a + \frac{1 - d}{4} = 0 \mod p \) also auch
\[
a^2 - a + \frac{1 - d}{4} \equiv 0 \mod (2).
\]
Da stets \( a^2 - a \equiv 0 \mod 2 \) folgt \( 2|\frac{1 - d}{4} \) d.h. \( d \equiv 1 \mod 8 \). WS!
2.7. **QUADRATISCHE ZAHLKÖRPER, KREISTEILUNGSKÖRPER**

(iii): Sei $2|\delta_F$. Dann muß $d \equiv 2,3 \mod 4$ sein. Für $d \equiv 2 \mod 4$ gilt

$$(2) = \left(2, \sqrt{d}\right)^2,$$

für $d \equiv 3 \mod 4$ gilt

$$(2) = \left(2, 1 + \sqrt{d}\right)^2.$$

\[\square\]

**2.7.4 Satz.** Sei $d < 0$. Dann gilt

(i) $d = -1 \Rightarrow O_F^* = \{1, i, -1, -i\}$

(ii) $d = -3 \Rightarrow O_F^* = \{\pm 1, \pm w, \pm w^2\}$ mit $w = \frac{-1 + \sqrt{-3}}{2}$

(iii) $d < -3, d = -2 \Rightarrow O_F^* = \{\pm 1\}$

Sei $d > 0$. Dann gibt es eine Einheit $u > 0, u \in O_F \subseteq \mathbb{R}$, sodaß

$O_F^* = \{\pm u^m : m \in \mathbb{Z}\}$.

**Beweis.** Sei $d < 0$.

• $d \equiv 2,3 \mod 4$. Ist $u \in O_F^*$, schreibe $u = x + y \sqrt{d}, x, y \in \mathbb{Z}$. Dann ist

$$\pm 1 = N(u) = x^2 + |d|y^2.$$

Ist $d = -1$, folgt (i). Ist $|d| > 1$ folgt $u = \pm 1$.

• $d \equiv 1 \mod 4$. Schreibe $u \in O_F^*$ als $u = \frac{x + y \sqrt{d}}{2}$ mit $x, y \in \mathbb{Z}, x \equiv y \mod 2$. Dann ist

$$\pm 1 = N(u) = \frac{x^2 + |d|y^2}{4},$$

also $x^2 + |d|y^2 = 4$. Im Fall $d = -3$ erhält man aus $x^2 + 3y^2 = 4$ die Möglichkeiten

(ii). Ist $|d| > 3$, folgt $u = \pm 1$.

Sei $d > 0$:

• Wähle $x, y \in \mathbb{N}$ eine Lösung der Pellschen Gleichung $x^2 - dy^2 = 1$. Dann ist

$$1 = N(u) = u \cdot u',$$

und $u > 1$. Wähle $M > u$.

• Es gibt nur endlich viele $\alpha \in O_F$ mit $\max\{|\alpha|, |\alpha'|\} \leq M$: In jedem Fall läßt sich $\alpha \in O_F$ schreiben als $\alpha = \frac{x + y \sqrt{d}}{2}$ mit gewissen $x, y \in \mathbb{Z}$. Wegen $\alpha' = \frac{x - y \sqrt{d}}{2}$ folgt

$$\max\{|\alpha|, |\alpha'|\} = \frac{|x| + |y| \sqrt{d}}{2},$$

• Ist $v \in O_F^*$, $1 < v < M$, so ist $v' = \pm \frac{1}{v}$, also $1 < v' < 1$. Es kann daher nur endlich viele solche $v$ geben.

• Sei $\epsilon$ die kleinste Einheit $1 < \epsilon < M$. Ist $\tau \in O_F^*, \tau > 0$, sei $s \in \mathbb{Z}$ sodaß $\epsilon^s \leq \tau < \epsilon^{s+1}$. Dann ist also $1 \leq \tau \epsilon^{-s} < \epsilon$ und da $\tau \epsilon^{-s} \in O_F^*$ folgt $\tau \epsilon^{-s} = 1$.

Ist $\tau < 0, \tau \in O_F^*$, so folgt $-\tau = \epsilon^s$, also $\tau = -\epsilon^s$. 
2.7.5 Definition. Sei \( m \in \mathbb{N}, \zeta_m := e^{\frac{2\pi i}{m}} \). Der algebraische Zahlkörper \( F = \mathbb{Q}(\zeta_m) \) heißt Kreisteilungskörper der Ordnung \( m \).

Es ist \( \zeta_m \) Nullstelle von \( X^m - 1 \) und es gilt

\[
X^m - 1 = (X - 1)(X - \zeta_m) \cdots (X - \zeta_m^{m-1}),
\]
also ist \( F \) der Zerfallungskörper des (separablen) Polynoms \( X^m - 1 \) und daher ist \( F/\mathbb{Q} \) Galois.

2.7.6 Lemma. Sei \( G = \text{Gal}(F/\mathbb{Q}) \) für \( F = \mathbb{Q}(\zeta_m) \). Dann ist \( G \cong (\mathbb{Z}/m\mathbb{Z})^* \) via \( \vartheta : G \rightarrow (\mathbb{Z}/m\mathbb{Z})^* \) wobei für \( \sigma \in G \) gilt \( \sigma \zeta_m = \zeta_m^{\vartheta(\sigma)} \). Also ist \( [F : \mathbb{Q}] = \varphi(m) \), wobei \( \varphi \) die Eulersche \( \varphi \)-Funktion bezeichnet.

Beweis. Ist \( \sigma \in G \) so folgt aus \( \zeta_m^m = 1 \) auch \( (\sigma(\zeta_m))^m = 1 \), also

\[
\sigma \zeta_m = \zeta_m^{\vartheta(\sigma)}
\]

für ein geeignetes \( \vartheta(\sigma) \in \mathbb{Z}/m\mathbb{Z} \). Da \( \sigma^{-1} \) existiert und \( \zeta_m = \zeta_m^1 \) folgt \( \vartheta(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^* \). Wegen \( F = \mathbb{Q}(\zeta_m) \) ist \( \vartheta \) injektiv.

Sei \( f \) das Minimalpolynom von \( \zeta_m \), dann gilt \( f \in \mathbb{Z}[X] \) und \( X^m - 1 = f(X) \cdot h(X) \) für ein gewisses \( h \in \mathbb{Z}[X] \). Sei \( p \) prim, \( p \nmid m \). Angenommen \( f(\zeta_m^p) \neq 0 \). Dann folgt \( h(\zeta_m^p) = 0 \). Betrachte modulo \( p \) Dann ist \( h(X^p) \equiv h(X)^p \), also \( h(\zeta_m^p) \equiv 0 \) und damit haben \( f \) und \( h \) modulo \( p \) einen gemeinsamen Faktor. Also hat \( X^m - 1 \) modulo \( p \) mehrfache Nullstellen, ein Widerspruch, denn \( (X^m - 1)^m = mX^{m-1} \) hat nur die Nullstelle 0. Es folgt dass für jedes \( a \) mit \( (a, m) = 1 \) gilt \( f(\zeta_m^a) = 0 \). Damit ist \( \vartheta \) surjektiv.

\[
\phi_m(X) := \prod_{(a, m) = 1} (X - \zeta_m^a). \phi_m \text{ heißt } m \text{-tes Kreisteilungspolynom. Offenbar gilt } \prod_{d|\text{max}} \phi_d(X) = X^m - 1.
\]

2.7.7 Lemma. Es gilt \( \phi_m(X) \in \mathbb{Z}[X] \), \( \phi_m \) ist irreduzibel.

Beweis. Es gilt \( \phi_m(X) = \prod_{\sigma \in G} (X - \sigma \zeta_m) \), also ist \( \phi_m \) das Minimalpolynom von \( \zeta_m \) über \( \mathbb{Q} \). Wegen \( \zeta_m \) ganz und \( \mathbb{Z} \) ganz abgeschlossen gilt \( \phi_m \in \mathbb{Z}[X] \).

2.7.8 Lemma. Sei \( p \) Primzahl, \( p \nmid \mathfrak{p} \), \( \mathfrak{p} \in \text{Spec} \mathbb{O}_F, \mathfrak{p}/(p), \zeta := \zeta_m \). Dann sind \( 1, \zeta, \ldots, \zeta^{m-1} \) verschiedene Elemente in \( O_F/\mathfrak{p} \). Es gilt:

\[
p^{f(\mathfrak{p}/(p))} \equiv 1 \mod m.
\]

Beweis. Es gilt \( 1 + X + \ldots + X^{m-1} = \prod_{i=1}^{m-1} (X - \zeta^i) \), also folgt \( (X = 1) \)

\[
m = \prod_{i=1}^{m-1} (1 - \zeta^i).
\]

Da \( p \nmid m \) ist \( m \not\equiv 0 \mod \mathfrak{p} \). Also folgt \( \zeta^i \not\equiv 1 \mod \mathfrak{p} \) für alle \( i = 1, \ldots, m-1 \). Damit ist \( i \neq j \mod \mathfrak{p} \) für alle \( 0 \leq i, j \leq m-1, i \neq j \).

Die Elemente \( \{1, \zeta, \ldots, \zeta^{m-1}\} \) sind also eine Untergruppe von \( (O_F/\mathfrak{p})^* \) mit Ordnung \( m \). Es folgt \( m|(p^f(\mathfrak{p}/(p)) - 1) \).
2.7. QUADRATISCHE ZAHLKÖRPER, KREISTEILUNGSKÖRPER

2.7.9 Lemma. Es gilt $\Delta(1, \zeta, \ldots, \zeta^{(m)-1}) \mid m^{\phi(m)}$.

Beweis. Es gilt $X^m - 1 = \phi_m(X)g(X)$ für ein gewisses $g \in \mathbb{Z}[X]$. Es folgt $mX^{m-1} = \phi'_m(X)g(X) + \phi_m(X)g'(X)$ und damit

$$m\zeta^{m-1} = \phi'_m(\zeta)g(\zeta).$$

Wegen $N(\zeta) = \pm 1$ folgt

$$\pm m^{\phi(m)} = N\left(\phi'_m(\zeta)\right)N\left(g(\zeta)\right) = \pm \Delta(1, \zeta, \ldots, \zeta^{(m)-1})N\left(g(\zeta)\right).$$

\[\square\]

2.7.10 Lemma. Sei $p$ Primzahl, $p \nmid m$. Dann gilt

(i) $O_F \equiv \mathbb{Z}[\zeta] \mod (p)_{O_F}$.

(ii) Ist $n \in \mathbb{N}$ mit $p^n \equiv 1 \mod m$, so gilt $w^{p^n} \equiv w \mod (p)_{O_F}$, $w \in O_F$.

(iii) $\sigma_w w \equiv w^p \mod (p)_{O_F}$, $w \in O_F$ ($\sigma_w(\zeta) = \zeta^p$).

Beweis.

\[\square\]

2.7.11 Satz. Sei $p$ Primzahl, $\mathfrak{P} \in \text{Spec} O_F$, $\mathfrak{P} / (p)$. Dann gilt: Ist $p$ ungerade so ist $\mathfrak{P}$ verzweigt ($e(\mathfrak{P} / (p)) > 1$) $\iff p \mid m$. Ist $p = 2$ so ist $\mathfrak{P}$ verzweigt $\iff 4 \mid m$. Genauer gilt

(i) Sei $p \nmid m$ und sei $f \in \mathbb{N}$ die kleinste Zahl mit $p^f \equiv 1 \mod m$. Dann ist

$$p_{O_F} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r$$

mit paarweise verschiedenen $\mathfrak{P}_i$. Es ist $f(\mathfrak{P} / (p)) = f$ und $r = \left(\frac{m}{f}\right)$. 

\[\square\]
(ii) Angenommen $m$ ist prim. Sei $p = m$, dann ist $(p)$ vollständig verzweigt, es gilt für $\mathfrak{P} := (1 - \zeta_p)_{O_F} \in \text{Spec } O_F$ daß $f(\mathfrak{P}/(p)) = 1$ und

$$(p)_{O_F} = \mathfrak{P}^{p^{-1}}$$

Beweis.

1) Sei $p \nmid m$, dann ist $\mathfrak{P}$ unverzweigt: Angenommen $pO_F \subseteq \mathfrak{P}^2$. Wähle $w \in \mathfrak{P} \setminus \mathfrak{P}^2$. Es gilt (für ein $n$ mit $p^n \equiv 1 \mod m$)

$$w^{p^n} \equiv w \mod pO_F$$

und daher $w^{p^n} \equiv w \mod \mathfrak{P}^2$. Wegen $p^n \geq 2$ ist $w^{p^n} \in \mathfrak{P}^2$ und damit auch $w \in \mathfrak{P}^2$. Wegen Lemma 2.7.8 gilt $p^{f_1} \equiv 1 \mod m$ und daher $f|f_1$.

Also ist $f = f(\mathfrak{P}/(p))$. Nach obigem ist $e(\mathfrak{P}/(p)) = 1$ und es folgt

$$r = \frac{|F: \mathfrak{P}|}{ef} = \frac{\varphi(m)}{f}.$$
2.7. QUADRATISCHE ZAHLKÖRPER, KREISTEILUNGSKÖRPER

.) Sei \( p = 2, 4|m \). Dann ist \( i \in \Omega(\zeta_m) \) und klarerweise ist \( i \in O_F^\ast \). Wegen 
\[(1 - i)^2 = (-i)^2 \text{ folgt}
\]
\[(2)_{OF} = (1 - i)^2_{OF}\]
und es folgt wie oben das alle \( \mathfrak{p}/(2) \) verzweigt sind.

\(\square\)

2.7.12 Korollar. Sei \( \mathfrak{p}/(p), \ p \mid m \). Dann ist \( G_{\mathfrak{p}} = \langle \sigma_p \rangle \).

Beweis. Sei \( w \in \mathfrak{p} \). Dann gilt \( \sigma_p(w) \equiv w^p \equiv 0 \mod \mathfrak{p} \), also \( \sigma_p \mathfrak{p} \subseteq \mathfrak{p} \). Da \( \sigma_p \mathfrak{p} \) maximal ist folgt \( \sigma_p \mathfrak{p} = \mathfrak{p} \). Es gilt \( r \cdot |G_{\mathfrak{p}}| = \varphi(m) \), also muß \( |G_{\mathfrak{p}}| = f \) sein. Nun ist \( f \) die Ordnung von \( \sigma_p \), also \( f = |\langle \sigma_p \rangle| \).

\(\square\)

2.7.13 Satz. Sei \( m \) prim. Dann gilt \( O_F = \mathbb{Z}[\zeta] \).

Beweis.

.) Die Inklusion \( O_F \supseteq \mathbb{Z}[\zeta] \) ist klar. Sei \( \alpha \in O_F, \alpha = a_0 + a_1 \zeta + \ldots + a_{m-2} \zeta^{m-2} \) mit gewissen \( a_i \in \mathbb{Q} \) (beachte \( [F : \mathbb{Q}] = \varphi(m) = m - 1 \)).

.) Es gilt \( ma_i \in \mathbb{Z} \): Da \( m \) prim ist, ist \( \deg \phi_m = [F : \mathbb{Q}] = \varphi(m) = m - 1 \), also 
\( \phi_m(X) = 1 + X + \ldots + X^{m-1} \). Es folgt

\[ \text{tr} \ z = -1, \ m \mid j. \]

Also ist (\( s = 0, \ldots, m - 2 \))

\[ \text{tr}(\alpha z^{-s}) = \text{tr}(a_0 z^{-s} + a_s + \ldots + a_{m-2} z^{m-2-s}) = \]
\[ = -a_0 - \ldots - a_{s-1} + (m - 1)a_s - a_{s+1} - \ldots - a_{m-2}, \]
und daher

\[ \text{tr}(\alpha z^{-s} - \alpha z) = ma_s. \]

Wegen \( \alpha z^{-s} - \alpha z \in O_F \) folgt \( ma_s \in \mathbb{Z} \).

.) Sei \( \lambda := 1 - \zeta \), dann gilt \( (m)_{OF} = (\lambda)^{m-1}_{OF} \). Schreibe

\[ ma = b_0 + b_1 \lambda + \ldots + b_{m-2} \lambda^{m-2}, b_i \in \mathbb{Z}. \]

Wegen \( ma \in (m)_{OF} \subseteq (\lambda)_{OF} \) folgt \( \lambda b_0 \in O_F \). Wegen \( m = \lambda^{m-1} u \) für ein \( u \in O_F^\ast \) gilt

\[ m^{m-1} = N(m) = \pm N(\lambda^{m-1}) = \pm N(\lambda)^{m-1} \]
und es folgt wegen \( N(\lambda)|N(b_0) \) in \( \mathbb{Z} \) auch \( m^{m-1} | (b_0^{m-1})^{m-1} \) in \( \mathbb{Z} \). Da \( m \) prim folgt \( m|b_0 \). Also folgt \( \lambda^{m-1} | b_0 \) in \( O_F \) und wir erhalten wegen \( ma \in (m)_{OF} \subseteq (\lambda^2)_{OF} \) auch

\[ \lambda^2 | b_1 \lambda \in O_F, \]
also \( \lambda | b_1 \) in \( O_F \). Nimmt man die Norm so folgt wieder \( m|b_1 \). Fährt man so fort erhält man \( m|b_i, i = 0, \ldots, m - 2 \), also

\[ \alpha = \frac{b_0}{m} + \frac{b_1}{m} \lambda + \ldots + \frac{b_{m-2}}{m} \lambda^{m-2} \in \mathbb{Z}[\lambda] = \mathbb{Z}[\zeta]. \]
Wir betrachten als weiteres Beispiel den algebraischen Zahlkörper $K = \mathbb{Q}(\sqrt{2})$. Dieser ist nicht Galois, die Homomorphismen von $K/\mathbb{Q}$ sind gegeben durch

\[
\begin{align*}
\text{id} & : 3\sqrt{2} \mapsto 3\sqrt{2} \\
\sigma_1 & : 3\sqrt{2} \mapsto \zeta_3 3\sqrt{2} \\
\sigma_2 & : 3\sqrt{2} \mapsto \zeta_3^2 3\sqrt{2}
\end{align*}
\]

wobei $\zeta_3 = e^{\frac{2\pi i}{3}}$.

Wir wollen zunächst (für allg. $\mathbb{Q}(\sqrt[m]{m})$ siehe [Narkiewicz] $O_K$ bestimmen. Dazu brauchen wir ein Lemma.

\textbf{2.7.14 Lemma.} Sei $K = \mathbb{Q}(a)$, $a \in O_K$ ein algebraischer Zahlkörper, $f(X)$ das Minimalpolynom von $a$. Sei angenommen daß $f$ Eisenstein ist bezüglich einer Primzahl $p$, d.h. mit $f(X) = X^m + \ldots + a_0$ gilt

\[p|a_i, \ i = 0, \ldots, m-1, \ p^2 \not| a_0.\]

Dann ist der Index $[O_K : \mathbb{Z}[a + \ldots + Za^{n-1}]]$ nicht durch $p$ teilbar.

\textbf{Beweis.} Wegen $a^n = -(a_{n-1}a^{n-1} + \ldots + a_0)$ und $p|a_i$ ist $\frac{a^n}{p} \in O_K$. Weiter ist $N_K^O(a) = a_0$ nicht durch $p^2$ teilbar.

Setze $M = \mathbb{Z} + Za + \ldots + Za^{n-1}$, $m = [O_K : M]$. Angenommen $p|m$.

Dann existiert ein Element $\xi \in O_K$ sodass

\[\xi \not\in M, \ p\xi \in M.\]

Denn $O_{K/M}$ ist eine abelsche Gruppe der Ordnung $m$, und wegen $p|m$ existiert ein Element mit Ordnung $p$. Dann ist also $\xi = (b_0 + b_1a + \ldots + b_{n-1}a^{n-1})\frac{1}{p}$ mit gewissen $b_i \in \mathbb{Z}$ so daß nicht alle $b_i$ durch $p$ teilbar sind. Sei $f$ minimal so daß $p \not| b_j$, und betrachte

\[\eta := (b_ja^j + \ldots + b_{n-1}a^{n-1})\frac{1}{p} = \xi - \left(\frac{b_0}{p} + \frac{b_1}{p} a + \ldots + \frac{b_{j-1}}{p} a^{j-1}\right) \in O_K.
\]

Es folgt

\[\zeta := b_ja^{n-1}\frac{1}{p} = \frac{a^n}{p} - \left(\frac{b_{j+1}}{p} a^{j+1} + \ldots + \frac{b_{n-1}}{p} a^{n-2}\right) \in O_K.
\]

Es folgt

\[N(\zeta) = b_j^nN(a)^{n-1}\frac{1}{p^n} \in \mathbb{Z}.
\]

Da $p^2 \not| N(a)$ folgt $p|b_j^n$ und damit $p|b_j$ WS!.

\textbf{2.7.15 Satz.} Sei $K = \mathbb{Q}(\sqrt{2})$. Dann gilt

\[O_K = \mathbb{Z}[\sqrt{2}].\]
2.7. QUADRATISCHE ZAHLKÖRPER, KREISTEILUNGSKÖRPER

Beweis. Setze $\alpha = \sqrt[3]{2}$. Das Minimalpolynom ist $f(X) = X^3 - 2$. Wegen Satz 2.6.5 gilt

$$\Delta(1, \alpha, \alpha^2) = (-1)^3N(3\sqrt[3]{4}) = 3^3 \cdot 2^2.$$ 

Sei $m = [O_K : \mathbb{Z}[\alpha]]$. Dann gilt wegen Satz 2.6.10

$$\pm 3^3 \cdot 2^2 = m^2 \delta_K \quad (2.1, \ast)$$

$f$ ist Eisenstein bzgl. 2, also gilt $2 \nmid m$. Betrachte das Element $\beta = \alpha - 2$. Sein Minimalpolynom ist

$$g(X) = f(X + 2) = (X + 2)^3 - 2 = X^3 + 3 \cdot 2X^2 + 3 \cdot 4X + 6.$$ 

Es gilt $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, also auch $m = [O_K : \mathbb{Z}[\alpha]] = [O_K : \mathbb{Z}[\beta]]$ und $\Delta(1, \alpha, \alpha^2) = \Delta(1, \beta, \beta^2)$. Da $g$ Eisenstein bzgl. 3 ist folgt $3 \nmid m$.

Wegen (2.1, *) folgt $m = 1$.

Wir betrachten das Primideal (5). Es gilt

$$X^3 - 2 \equiv (X - 3)(X^2 + 3X - 1) \mod 5$$

und $X^2 + 3X - 1$ ist irreduzibel $\mod 5$ denn es hat keine Nullstelle (ausprobieren).

Wegen Satz 2.5.2 erhält man

$$5O_K = \mathfrak{p}_1 \mathfrak{p}_2$$

wobei $f(\mathfrak{p}_1/(5)) = 1$, $f(\mathfrak{p}_2/(5)) = 2$. 
Kapitel 3

Die Riemannsche Zetafunktion: Definition

3.1 Die Riemannsche Zetafunktion

Zuerst einige Resultate über Dirichlet-Reihen.
Seien \((a_n)_{n \in \mathbb{N}}\) und \((b_n)_{n \in \mathbb{N}}\) Folgen komplexer Zahlen. Setze \(A_n := a_1 + \ldots + a_n, B_n := b_1 + \ldots + b_n\). Dann gilt

\[
\sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1})
\]

Eine Dirichlet-Reihe ist eine Reihe der Gestalt

\[
\sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad s \in \mathbb{C},
\]

wobei \((a_n)_{n \in \mathbb{N}}\) eine Folge komplexer Zahlen ist. Schreibe im folgenden \(s = \sigma + it\) mit \(\sigma, t \in \mathbb{R}\).

3.1.1 Lemma. Ist die Dirichlet-Reihe \(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\) konvergent für ein \(s = s_0\), so auch für alle \(s\) mit \(\text{Re}\, s > \text{Re}\, s_0\), und zwar gleichmäßig auf allen kompakten Teilmengen dieser offenen Halbebene.

Beweis. Schreibe \(n^s = n^{s_0} n^{(s-s_0)}\) und wende partielle Summation an auf die Reihe

\[
\sum \frac{a_n}{n^s} = \sum \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^{s-s_0}}.
\]

Ist \(P_n(s_0) = \sum_{m=1}^{n} \frac{a_m}{m^s}\), so erhält man

\[
\sum_{k=m+1}^{n} \frac{a_k}{n^{s_0}} = \frac{P_n(s_0)}{n^{s-s_0}} - \frac{P_m(s_0)}{m^{s-s_0}} + \sum_{k=m+1}^{n} P_k(s_0) \left[ \frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right] = (*)
\]

61
Es gilt

\[
\frac{1}{k^{s-s_0}} - \frac{1}{(k + 1)^{s-s_0}} = (s - s_0) \int_k^{k+1} \frac{1}{x^{s-s_0+1}} \, dx.
\]

Sei \( M \) so daß \( |P_k(s_0)| \leq M, \; k \in \mathbb{N} \). Dann ist

\[
\left| \left( s \right) \right| \leq \frac{M}{n^{s-s_0}} + \frac{M}{m^{s-s_0}} + M(s-s_0) \int_{m+1}^{n+1} \frac{1}{x^{s-s_0+1}} \, dx \leq \frac{M(1}{n^{s-s_0}} + \frac{1}{m^{s-s_0}} + \frac{s-s_0}{(m+1)^{s-s_0}}
\]

und dieser Ausdruck strebt für \( m,n \to \infty \) gegen 0 und zwar gleichmäßig auf jedem Kompaktum in \( \{\sigma \geq \sigma_0\} \). □

Die Zahl

\[
\sigma_0 := \inf \left\{ \sigma \in \mathbb{R} : \sum \frac{a_n}{n^\sigma} \text{ konvergiert} \right\}
\]

heißt Konvergenzabzisse von \( \sum \frac{a_n}{n^\sigma} \).

Ist die Dirichlet-Reihe konvergent für \( s_1 = \sigma_1 + it_1 \), so muß gelten \( a_n = o(n^{\sigma_1}) \). Es folgt daß die Reihe in jeder Halbebene \( \{ \text{Re}(s) \geq \sigma_1 + \delta \} \) absolut und gleichmäßig konvergiert. Denn vergleiche mit \( \sum \frac{1}{n^{\sigma+\delta}} \).

**Lemma.** Sei \( \sigma_1 \geq 0 \) und sei \( A_\infty = a_1 + \ldots + a_n = O(n^{\sigma_1}) \). Dann ist die Konvergenzabzisse von \( \sum \frac{a_n}{n^\sigma} \) stets \( \leq \sigma_1 \).

**Beweis.** Sei \( |A_\infty| \leq C n^{\sigma_1} \), sei \( \delta > 0 \) und \( \sigma \geq \sigma_1 + \delta \), sei \( P_n(s) = \sum_{k=1}^{n} \frac{a_k}{k^s} \). Dann gilt

\[
P_n(s) - P_m(s) = \frac{A_n}{n^s} - \frac{A_m}{m^s} + \sum_{n=m+1}^{n-1} A_k \left( \frac{1}{k^s} - \frac{1}{(k+1)^s} \right) = \frac{A_n}{n^s} - \frac{A_m}{m^s} + \sum_{k=m+1}^{n-1} A_k \frac{k^{1-s}}{k} \int_k^{k+1} \frac{1}{x^{s+1}} \, dx.
\]

Also folgt

\[
\left| P_n(s) - P_m(s) \right| \leq \frac{C}{n^{\sigma-\sigma_1} + \frac{C}{m^{\sigma-\sigma_1}} + C|s| \int_{m+1}^{\infty} \frac{1}{x^{\sigma+1}} \, dx \leq \frac{C}{n^\sigma + \frac{1}{m^\sigma} + |s| \frac{1}{(m+1)^\sigma}} \to 0, \; m,n \to \infty.
\]

□

**Definition.** Die Riemannsche Zetafunktion ist definiert als die Reihe

\[
\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.
\]
3.1. DIE RIEMANNSCHE ZETA-FUNKTION

Die Funktion $\zeta(s)$ ist analytisch auf $\{Re\ s > 1\}$, denn setze in Lemma 3.1.2 $\sigma_1 = 1$. Weiter gilt für $s \in \mathbb{R}$, $s > 1$,

$$\frac{1}{s-1} = \int_1^\infty \frac{1}{x^s} \, dx \leq \zeta(s) \leq 1 + \frac{1}{s-1}.$$

Also folgt

$$1 \leq (s-1)\zeta(s) \leq s, \ s > 1, \quad (3.1, +)$$

3.1.4 Satz. Die Funktion $\zeta(s)$ ist analytisch auf $\{Re\ s > 0\}$ mit Ausnahme des Punktes $s = 1$ wo sie einen Pol erster Ordnung mit Residuum 1 hat.

Beweis.
• betrachte die Dirichlet-Reihe

$$\sum_{n=1}^\infty \frac{(-1)^{n-1}}{n^s} =: \zeta_2(s).$$

Wegen Lemma 3.1.2 ist $\zeta_2$ analytisch auf $\{Re\ s > 0\}$. Nun gilt

$$2 \cdot \frac{\zeta(s)}{2^s} + \zeta_2(s) = \zeta(s),$$

also $\zeta(s)(1 - \frac{1}{2^s}) = \zeta_2(s)$. Daher hat $\zeta$ eine analytische Fortsetzung auf $\{Re\ s > 0\}$ mit möglicher Ausnahme der Punkte $s$ mit $2^s = 1$, das sind

$$s = 1 + \frac{2\pi n}{\log 2}, n \in \mathbb{Z}.$$

Dort liegen höchstens Pole. Bei $s = 1$ ist also ein einfacher Pol mit Residuum 1 wegen (3.1, +).

• betrachte die Reihe

$$\zeta_r(s) := 1 + \frac{1}{2^s} + \ldots + \frac{1}{(r-1)^s} - \frac{r-1}{r^s} + \frac{1}{(r+1)^s} + \ldots .$$

Die Partialsummen der Koeffizienten sind $\leq r$, also ist $\zeta_r$ analytisch für $Re\ s > 0$.

Es gilt

$$\zeta_r(s) = \left(1 - \frac{1}{r^s}\right)\zeta(s),$$

also ist $\zeta$ analytisch auf $\{Re\ s > 0\}$ mit möglicher Ausnahme von

$$s = 1 + \frac{2\pi n}{\log r}, n \in \mathbb{Z}.$$

Es bleibt nur $s = 1$ als Pol möglich, denn wäre z.B.

$$1 + \frac{2\pi m}{\log 3} = 1 + \frac{2\pi n}{\log 2},$$

so wäre $3^m = 2^n$, ein WSI.
3.1.5 Korollar. Sei $(a_n)_{n \in \mathbb{N}}, A_n = a_1 + \ldots + a_n, 0 \leq \sigma_1 < 1, \rho \in \mathbb{C}$. Ist
\[ A_n = n \rho + O(n^{\sigma_1}), \]
dann hat die Dirichlet-Reihe
\[ f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \]
eine analytische Fortsetzung auf $\{\Re s > 0\}$ mit Ausnahme von $s = 1$ wo ein einfacher Pol mit Residuum $\rho$ liegt.

Beweis. Wende Lemma 3.1.2 und Satz 3.1.4 an auf $f(s) - \rho \zeta(s)$.

3.2 Definition von $\zeta_k$
Wir schreiben im folgenden $f \sim g$ wenn sich $f$ und $g$ nur um eine analytische Funktion unterscheiden.

3.2.1 Lemma. Es gilt
(i) (Eulersche Produktdarstellung)
\[ \zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}, \Re s > 1. \]
(ii)
\[ \log \zeta(s) = \sum_{p \in \mathbb{P}, m \geq 1} \frac{1}{mp^m s}. \]
(iii)
\[ \log \zeta(s) \sim \sum_{p \in \mathbb{P}} \frac{1}{p^s} \sim \log \frac{1}{s - 1}. \]

Beweis. Betrachte die Reihe
\[ R = \sum_{p \in \mathbb{P}} \sum_{m \geq 1} \frac{1}{mp^m s}. \]
Es gilt für $\sigma > 1$
\[ \sum_{p \in \mathbb{P}} \sum_{m \geq 1} \left| \frac{1}{mp^m s} \right| = \sum_{p \in \mathbb{P}} \sum_{m \geq 1} \frac{1}{mp^m s} = - \sum_{p \in \mathbb{P}} \log \left( 1 - \frac{1}{p^s} \right) \]
Wegen $\lim_{p \to \infty} \frac{1}{p^s} = 0$ und $\lim_{s \to 0} \frac{\log(1 - x)}{x} = -1$. Ist diese Reihe mit $\sum_{p \in \mathbb{P}} \frac{1}{p^s}$ konvergent ($\sigma > 1$). Man darf in $R$ also die Summationsreihenfolge austauschen sowie beliebig anordnen. Wegen der absoluten Konvergenz von $\sum_{p} \log(1 - \frac{1}{p^s})$
3.2. Definition von $\zeta_K$

folgt das das Eukl-Produkt absolut konvergiert. Damit ist die Anwendung des Distributivgesetzes erlaubt und man erhält wegen ZPE in $\mathbb{Z}$:

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \prod_p \sum_{m \geq 1} \frac{1}{p^{ms}} = \sum_{n \in \mathbb{N}} \frac{1}{n^s} = \zeta(s).$$

Gleichzeitig folgt

$$\log \zeta(s) = -\sum_p \log \left(1 - \frac{1}{p^s}\right) = \sum_{p \in \text{FZ}, m \geq 1} \frac{1}{mp^m}.$$ 

Klarerweise ist $\log \zeta(s) \sim \log \frac{1}{s-1}$. Beachte, daß

$$\sum_{p \in \text{FZ}, m \geq 2} \left|\frac{1}{mp^m}\right| = \sum_{p \in \text{FZ}} \sum_{m \geq 2} \frac{1}{mp^m} = \frac{1}{2} \sum_{p \in \text{FZ}} \left(\log(1 - \frac{1}{p^s}) + \frac{1}{p^s}\right).$$

Wegen

$$\lim_{x \to 0} \frac{\log(1 - x) + x}{x^2} = -\frac{1}{2}$$

ist diese Reihe vergleichbar mit $\sum_{p \in \text{FZ}} \frac{1}{p^s}$ und daher konvergent für $\sigma > \frac{1}{2}$ und dort analytisch. Es ist

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + \sum_{p \in \text{FZ}, m \geq 2} \frac{1}{mp^m}.$$ 

□

Sei nun $k \neq \mathbb{Q}$ ein algebraischer Zahlkörper, $[k : \mathbb{R}] = N$. Es ist für ein $p \in \text{Spec } O_k$, $p/(p)$,

$$N^A_k(p) = (p^{f(p/(p))})_Z = (Np)_Z$$

wo $Np = |O_k/p| = p^{f(p/(p))}$ ist.

3.2.2 Definition. Die Dedekindsche Zetafunktion des algebraischen Zahlkörpers $k$ ist

$$\zeta_k(s) := \prod_{p \in \text{Spec } O_k} \frac{1}{1 - \frac{1}{Np^s}}.$$ 

3.2.3 Lemma. $\zeta_k$ ist analytisch für $\sigma > 1$. Es gilt

(i) $\zeta_k(s) = \sum_{a \in O_k} \frac{1}{N_a^s}$

(ii) $\log \zeta_k(s) = \sum_{p, m \geq 1} \frac{1}{mNp^{ms}}$

(iii) $\log \zeta_k(s) \sim \sum_{p, l_p = 1} \frac{1}{Np^s}$. 

DEll. 7 LEll. 8
KAPITEL 3. DIE RIEMANNSCHE ZETAFUNKTION: DEFINITION

Beweis. Es gilt \( \sum_{p/(p)} f_p \leq N \), also gibt es höchstens \( N \) viele \( p/(p) \) und es folgt

\[
\sum_{p, m \geq 1} \left| \frac{1}{m N p^{\sigma m}} \right| \geq \sum_{p \not\in \mathbb{Z}, m \geq 1} \frac{N}{m N p^{\sigma m}} < \infty, \sigma > 1.
\]

Es ist

\[
\sum_p \log \left( 1 - \frac{1}{N p^s} \right) \approx 1 \sum_{p, m \geq 1} \frac{1}{N m N p^{\sigma m}} \leq \sum_{p \not\in \mathbb{Z}} \frac{N}{p^s}
\]

absolut konvergent, und damit auch das Produkt in der Definition von \( \zeta_k \) und stellt eine in \( \{ \Re s > 1 \} \) analytische Funktion dar. Weiter ist

\[
\log \zeta_k(s) = - \sum_p \log \left( 1 - \frac{1}{N p^s} \right) = \sum_{p, m \geq 1} \frac{1}{m N p^{\sigma m}}.
\]

Die Reihe

\[
\sum_{(p > 1) \vee (m \geq 2)} \frac{1}{m N p^{\sigma m}} = R
\]

vergleicht man mit \( \sum_{p \not\in \mathbb{Z}, m \geq 2} \frac{N}{m p^{\sigma m}} + \sum_{p > 1} \frac{1}{N p^s} \) und die zweite Reihe ist \( \leq \sum_{p \not\in \mathbb{Z}} \frac{N}{p^s} \). Also ist \( R \) konvergent für \( \sigma > \frac{1}{2} \).

\( \square \)
Literaturverzeichnis

[BIV, brueske.et.al] R. BRÜSKE, F. ISCHEBECK, F. VOEGEL: 

[I, ireland.rosen] K. IRELAND, M. ROSEN: 
A Classical Introduction to Modern Number 
Theory, GTM 84, Springer Verlag, 1990.

[L, lang] S. LANG: 
Algebraic Number Theory, 
GTM 110, Springer Verlag, 1986.

[L, lang/algebra] S. LANG: 
Algebra, 
GTM 211, Springer Verlag, ???.

[N, narkiewicz] W. NARKIEWICZ: 
Elementary and Analytic Theory of Algebraic Num-
bers, ???.

[RV, ramakrishnan.valenza] D. RAMAKRISHNAN, R. VALENZA: 
Fourier Analysis on 
Number Fields, 
GTM 186, Springer Verlag, 1999

[S, stichtenoth] H. STICHTENOTHE: Algebraic Function Fields and Codes, 
Springer Verlag, 1993.

[vdW, vdw] B. L. VAN DER WAERDEN: 
Algebra I/II, 

[W, weil] A. WEIL: Basic Number Theory, 
Springer Verlag, 1967.