Algebraische und analytische Theorie der Zetafunktion

Vorlesung SS 2002. Vers.2.1.2003

Inhaltsverzeichnis

Die Riemannsche Zetafunktion: Motivation

Aus der Kenntnis des analytischen Verhaltens der Riemannschen Zetafunktion

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) := \sum_{n\in\mathbb{N}} \frac{1}{n^s},\ \operatorname{Re} s > 1,$$

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

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

$$\pi(N) = \int_2^N \frac{dt}{\log t} + O\Big(Ne^{-\beta(\log N)^\alpha}\Big).$$

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

Einige, relativ einfache, analytische Eigenschaften von $\zeta_{\mathbb{R}}$ aus denen man mit Hilfe Tauberscher Sätze solche Aussagen erhalten kann sind:

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

$$\zeta_{\mathbb{Q}}(s) = \prod_{p\ \mathrm{PZ}} \frac{1}{1-\frac{1}{p^s}}.$$

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

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

$$\pi^{-\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)\zeta_{\mathbb{Q}}(s) = \pi^{-\frac{1-s}{2}}\Gamma\Big(\frac{1-s}{2}\Big)\zeta_{\mathbb{Q}}(1-s).$$

Weiters benötigt man für diese genaue Abschätzung des Restgliedes Kenntnis über nullstellenfreie Bereiche der ζ-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

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

wobei φ die Eulersche φ-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 ζ-Funktion, sondern allgemeiner jene sogenannter Dirichletscher L-Reihen: Sei $k \in \mathbb{N}$ und χ 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

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

Für den trivialen Charakter $\chi = \chi_0$ erhält man genau $L_{\mathbb{Q}}(s,\chi_0) = \zeta_{\mathbb{Q}}(s) \cdot \Pi_{p|k}(1 - \frac{1}{p^s})$.

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

Tatsächlich ist $L_{\mathbb{Q}}(s,\chi)$ für $\chi \neq \chi_0$ ganz und genügt ebenfalls einer Funktionalgleichung.

Aussagen über Anzahl bzw. Verteilung o.ä. von "Primzahlen" sind auch in allgemeineren Fällen als $\mathbb{Z}$ von Interesse. Z.B. hat Kummer quadratische Erweiterungen $\mathbb{Z}[\sqrt{3}]$ o.ä. betrachtet in der Hoffnung beim Satz von Fermat weiterzukommen. Allgemein spricht man von algebraischen Zahlkörpern: Eine endliche Erweiterung K von $\mathbb{Q}$ heißt algebraischer Zahlkörper. Dann betrachtet man sogenannte ganze algebraische Zahlen A in K. Man hat also die Situation

$$\begin{array}{ccc} \mathbb{Q} & \to & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \to & A \end{array}$$

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

$$A = \mathbb{Z} + \mathbb{Z} \begin{cases} \sqrt{m} & , \ m \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{m}}{2} & , \ m \equiv 1 \mod 4 \end{cases}$$

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

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}(w) \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Z}[w] \end{array}$$

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. $k = \mathcal{GF}(q)$. Dann ist die Zetafunktion vom Funktionenkörper $k(x)/k$ gegeben als

$$Z\Big(z\Big) = \frac{1}{1-t} \prod_{p} \frac{1}{1-t^{\deg p}}$$

wobei p alle irreduziblen (normierten) Polynome durchläuft.

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

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

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. $K = \mathcal{GF}(q)$, $charK \neq 2, 3$, 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 $n \in \mathbb{N}$. Man spricht von

$$\mathcal{C}_n = \big\{(\alpha, \beta) \in \mathcal{GF}(q^n)^2 : \beta^2 = \alpha^3 + a\alpha + b\big\}$$

als einer elliptischen Kurve über $\mathcal{GF}(q^n)$. Sei

$$N_n := 1 + |\mathcal{C}_n|$$

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

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

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

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

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

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

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

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

Kennt man nullstellenfreie Bereiche der Riemannsche Zetafunktion, kann man daraus α, β konstuieren. 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 $X \leq M$ heißt Basis wenn sie linear unabhängig ist und M (als R-Modul) erzeugt.

DEAI.1

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

Ist zum Beispiel I irgend eine Menge, so ist

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

frei mit der Basis

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

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

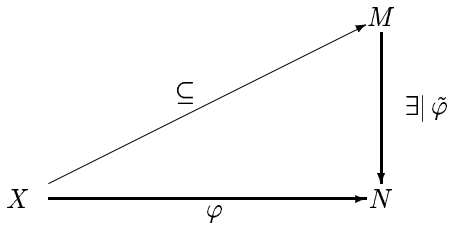
$$M \cong \bigoplus_{i \in I} R.$$

Denn ist $x \in M$, so existieren a_i, $i \in I$, fast alle gleich Null, sodaß $x = \sum a_i x_i$. 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 Moduloperationen.

1.1.2 Satz. *Sei M ein R-Modul. Ist $X \leq M$ eine Basis von M so hat man die folgende Eigenschaft (N ist irgendein R-Modul)*



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

$$F = \bigoplus_{i \in M} R.$$

COAI.3

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.

□

LEAI.4

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

$$M = \bigoplus_{i \in I} Rx_i, \quad M/\mathfrak{a}M \cong \bigoplus_{i \in I} Rx_i/\mathfrak{a}x_i.$$

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

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

$$\varphi : M \to \bigoplus_{i \in I} Rx_i/\mathfrak{a}x_i$$

hat Kern $\mathfrak{a}M$ denn: Sei $x = \sum a_i x_i$. Dann ist

$$0 = \varphi(x) = (a_i x_i + \mathfrak{a}x_i)_{i \in I}$$

genau dann, wenn $a_i \in \mathfrak{a}$ für alle $i \in I$. Weiters ist $Rx_i/\mathfrak{a}x_i \cong R/\mathfrak{a}$ vermöge

$$ax_i + \mathfrak{a}x_i \mapsto a.$$

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

□

COAI.5

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 $|X| = |Y|$.

□

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

$$M \cong R/\operatorname{Ann}_R\{x\}$$

wobei $\operatorname{Ann}_R\{x\} := \{r \in R : rx = 0\}$.

LEAI.6

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*) $\exists\varphi : M'' \to M : g \circ \varphi = \mathrm{id}\, M''$.

(*ii*) $\exists\psi : M \to M' : \psi \circ f = \mathrm{id}\, M'$.

In diesem Fall ist

$$M = \operatorname{Im} f \oplus \ker\psi = \ker g \oplus \operatorname{Im}\varphi,$$

$$M \cong M' \oplus M'',$$

und man sagt die exakte Sequenz ist split exakt.

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

$$x - \varphi\Big(g(x)\Big) \in \ker g.$$

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

$$g(x) = g(y + z) = g\big(\varphi(w)\big) = w.$$

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

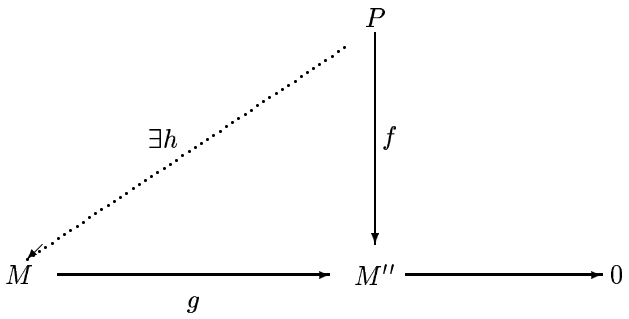
Wir haben also $M = \ker g \oplus \operatorname{Im}\varphi$. Wegen der Exaktheit ist $\ker g = \operatorname{Im} f$. Definiere ψ wie folgt: Ist $x = y + z \in M$, $y = f(u)$, so sei $\psi(x) := u$. ψ ist wohldefiniert denn f ist injektiv und erfüllt offenbar $\psi \circ f = \mathrm{id}_{M'}$. Weiters ist $\ker\psi = \operatorname{Im}\varphi$, also $M = \operatorname{Im} f \oplus \ker\psi$. Weiters ist $\operatorname{Im} f \cong M'$ und $g|\operatorname{Im}\varphi$ ein Isomorphismus von $\operatorname{Im}\varphi$ auf M''.

Gilt (*ii*), so schließt man analog.

□

DEAI.7

1.1.7 Definition. Ein R-Modul P heißt projektiv, wenn gilt (M,M'' irgendwelche R-Moduln)



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

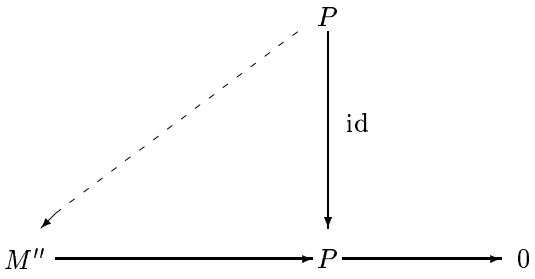
1.1.8 Satz. *Es sind äquivalent:*

(*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



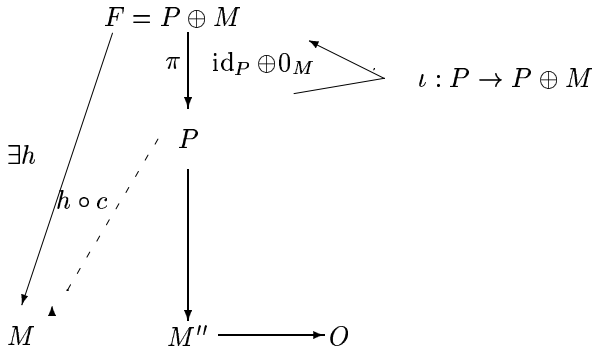
liefert das splitting der Sequenz.

(*ii*) $\Rightarrow$ (*iii*): Sei F frei sodaß 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 $\mathrm{Ann}_R\{x\} = \{0\}$: Denn sei $(v_i)_{i\in I}$ Basis von F, $x = \sum a_i v_i$ und $a_{i_0} \neq= 0$. Sei φ der Homomorphismus $\varphi : F \to R$ mit $v_{i_0} \mapsto 1$, $v_i \mapsto 0$, $i \neq i_0$. Ist $r \in \mathrm{Ann}_R\{x\}$, so folgt

$$0 = \varphi(rx) = r a_{i_0}.$$

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

$$\{a \in R : a v_1 \in M_1\}$$

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

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

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

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

Sei S die Menge aller Paare $(M_J,\ w)$ sodaß $w : J' \subseteq J \to M_J$ 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. $\exists J' \leq J$ und $w : J' \to M_J$ Basis, d.h. $(M_J,\ w) \in S$.

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

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

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 $k \in I\ J$, $K = J \cup \{k\}$.

Gilt $M_K = M_J$ so ist $(M_K, w) \gneq (M_J, w)$, ein WS!. Andernfalls ist

$$\{0\} \neq \{c \in R : \exists c v_k + y \in M, y \in M_J\} \lhd R,$$

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

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

eine Basis von M_K und es gilt

$$\big(M_K, \tilde{w}\big) \gneq \big(M_J, w\big),$$

ein WS!

□

COAI.10

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

(i) Sei 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 $\varphi : F \to E$. 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 sodaß $P \oplus M = F$ frei. Es ist also $P \leq F$ ebenfalls frei.

□

Sei E ein R-Modul, $x \in E$ heißt Torsionselement, wenn gilt $\mathrm{Ann}_R\{x\} \neq \{0\}$ $E_{tor} := \{x \in E : x \text{ Torsionselement}\}$. Ist $E_{tor} = E$, so heißt E Torsionsmodul, ist $E_{tor} = \{0\}$, so heißt E torsionsfrei.

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.

LEAI.12

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

$$0 \to \ker f \xrightarrow{\iota} E \xrightarrow{f} E' \to 0$$

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

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

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

□

Beweis. (Satz 1.2.3):
·) 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 $x \in E_{tor}$.

·) Wir zeigen: Jeder endlich erzeugte torsionsfreie Modul M ist frei: Sei $\{y_1, \ldots, y_m\}$ ein Erzeugendensystem von M und wähle eine maximale linear 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

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

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

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

□

1.3 Nöthersche 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 $M_1 \subsetneq M_2 \subsetneq \ldots$ von Untermoduln von M ist endlich.*

(*iii*) *Jede nichtleere Menge von Untermoduln von M hat ein maximales 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

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \ldots$$

ein WS!.

$(iii) \Rightarrow (i)$: Sei $N \leq M$ gegeben, $a_0 \in N$. Ist $N \neq \langle a_0 \rangle$ wähle $a_i \in N \setminus \langle a_0 \rangle$. 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

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

und diese Menge hat kein maximales Element.

□

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 $\pi : M \to N$ surjektiv, so ist mit einer echt aufsteigenden Kette

$$N_1 \subsetneq N_2 \subsetneq \ldots \leq N$$

auch

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

□

LEAI.15

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

Beweis. Mit $L \leq M$ assoziiere das Paar

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

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

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

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

□

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 $\pi_1 : N_1 \oplus N_2 \to N_1$, hat Kern N_2. Ist $M = N_1 + N_2$, so hat man $N_1 \oplus N_2 \to M$. Rest induktiv.

□

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

LEAI.17

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 $\mathfrak{b}_1 \subsetneq \ldots \subsetneq \mathfrak{b}_n \subsetneq \ldots \lhd B$, dann ist $\varphi^{-1}(\mathfrak{b}_1) \subsetneq \ldots \subsetneq \varphi^{-1}(\mathfrak{b}_n) \subsetneq \ldots \lhd A$.

ad(iii): Ist $\mathfrak{b}_1 \subsetneq \ldots \subsetneq \mathfrak{b}_n \subsetneq \ldots \lhd S^{-1}A$ und schreibt man $\mathfrak{b}_i = S^{-1}\mathfrak{a}_i$ so ist $\mathfrak{a}_1 \subsetneq \ldots \subsetneq \mathfrak{a}_n \subsetneq \ldots \lhd A$ eine echte Kette.

□

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

$$(a_1, s_1) \sim (a_2, s_2) \;:\Longleftrightarrow\; \exists t \in S : \, ta_2s_1 = ta_1s_2$$

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

$$(a_1, s_1) + (a_2, s_2) := (a_1s_2 + a_2s_1, s_1s_2),$$

$$(a_1, s_1) \cdot (a_2, s_2) := (a_1a_2, s_1s_2)$$

ein Ring, der sogenannte Quotientenring *von A nach S. Das Element (a, s) wird oft mit $\frac{a}{s}$ bezeichnet.*

Beweis. Klar durch nachrechnen.

□

Ein echtes Ideal $\mathfrak{p} \lhd A$ eines Ringes A heißt *Primideal*, wenn gilt:

$$x \cdot y \in \mathfrak{p} \;\Rightarrow\; \big(x \in \mathfrak{p} \vee y \in \mathfrak{p}\big),$$

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

REI.2

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

$$\iota_{A,S} : \left\{ \begin{array}{ccc} A & \to & S^{-1}A \\ a & \mapsto & (a, 1) \end{array} \right.$$

ist 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.

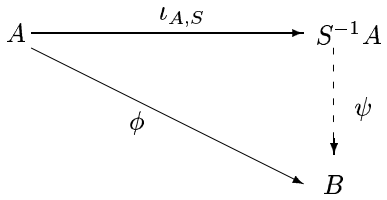
(c) $0 \in S$. Dann ist $S^{-1}A \cong \{0\}$.

(d) Sei $\mathfrak{p} \in$ *SpecA* und setze $S := A \setminus \mathfrak{p}$. Dann heißt

$$A_{\mathfrak{p}} := S^{-1}A = (A \setminus \mathfrak{p})^{-1}A$$

die *Lokalisierung* von A in $\mathfrak{p}$ (oder an der Stelle $\mathfrak{p}$).

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*



d.h. mit $\phi = \psi \circ \iota_{A,S}$.

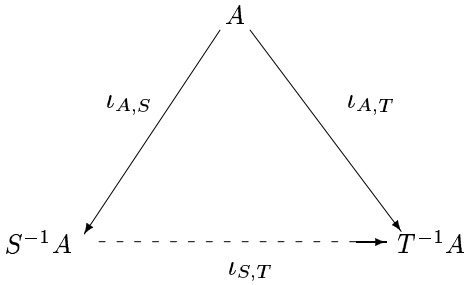
Beweis. Definiere

$$\psi(\frac{a}{s}) := \phi(a)\phi(s)^{-1}$$

Rest klar durch nachrechnen. □

COI.4

1.4.4 Korollar. *Seien $S \subseteq T$ zwei multiplikative Teilmengen von A. Dann gibt es einen kanonischen Homomorphismus $\iota_{S,T} : S^{-1}A \to T^{-1}A$ sodaß*



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 $\mathfrak{a}$ mit $S^{-1}\mathfrak{a}$ die Menge*

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

Dann gilt

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

(ii) Ist $\mathfrak{b}$ Ideal von $S^{-1}A$ und $\mathfrak{a} := \iota_{A,S}^{-1}(\mathfrak{b})$, so gilt

$$\mathfrak{b} = S^{-1}\mathfrak{a}.$$

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

$$\iota_{A,S}^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}.$$

Beweis.
ad (i): klar.

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

Klarerweise ist Ψ ordnungserhaltend.

Sei $\mathfrak{p} \in \operatorname{Spec} A$, $\mathfrak{p} \cap S = \emptyset$ und sei

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in S^{-1}\mathfrak{p},$$

d.h. $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{p}{s}$. Dann existiert $t \in S$ mit $ta_1a_2s = tps_1s_2 \in \mathfrak{p}$. Es folgt das eines von a_1, a_2 in $\mathfrak{p}$ sein muss.

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

Sei $\mathfrak{p} \in \operatorname{Spec} A$. Klar ist $\mathfrak{p} \subseteq \iota_{A,S}^{-1}(S^{-1}\mathfrak{p})$. Sei $x \in A$ mit $\frac{x}{1} \in S^{-1}\mathfrak{p}$, d.h. $\frac{x}{1} = \frac{p}{s}$. Dann folgt für ein gewisses $t \in S$ daß $txs = tp1 \in \mathfrak{p}$, also folgt $x \in \mathfrak{p}$.

□

COI.6

1.4.6 Korollar. *Es gilt: Ist A Hauptidealring, so auch $S^{-1}A$.*

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

DEI.7

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

COI.8

1.4.8 Korollar. *(i) Sei $\mathfrak{p} \in \operatorname{Spec} A$. Dann ist $A_\mathfrak{p}$ lokal mit maximalem Ideal*

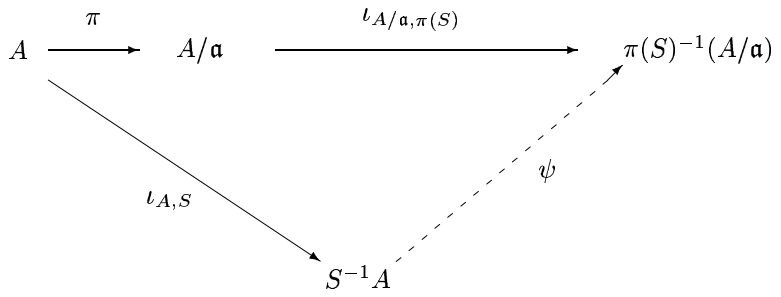
$$\mathfrak{p}A_\mathfrak{p} := \{\frac{p}{s} : p \in \mathfrak{p}, s \in A \setminus \mathfrak{p}\} = \iota_{A,A\setminus\mathfrak{p}}(\mathfrak{p})A_\mathfrak{p}.$$

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

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

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

Beweis. Betrachte die Homomorphismen.



Jedes Element von $\pi(S)^{-1}(A/\mathfrak{a})$ ist von der Gestalt $\frac{\pi(a)}{\pi(s)}$ für gewisse $a \in A$, $s \in S$. Es ist unter ψ 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 $ta \in \mathfrak{a}$. Damit ist $\frac{a}{s} = \frac{ta}{ts} \in S^{-1}\mathfrak{a}$. □

COI.10

1.4.10 Korollar. *Ist $\mathfrak{p} \in \operatorname{Spec} A$, so ist $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong Q(A/\mathfrak{p})$.*

Beweis. Klar. □

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.

REI.11

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

(ii)
$$\iota_{M,S} : \left\{ \begin{array}{ccc} M & \to & S^{-1}M \\ m & \mapsto & \frac{m}{1} \end{array} \right.$$
ist ein A-Modul Homomorphismus.

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

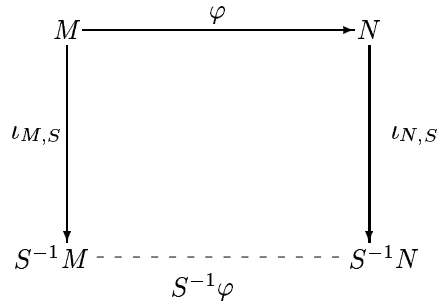
(iv) Ist U ein Untermodul von M, so ist $S^{-1}U$ ein Untermodul von $S^{-1}M$. Jeder $S^{-1}A$-Untermodul N von M ist von der Gestalt $N = S^{-1}U$ mit dem A-Untermodul $U := \iota_{M,S}^{-1}(N)$.

(v) Es gilt (*Satz vom Hauptnenner*)
$$S^{-1}\big(\sum_{i\in I} M_i\big) \cong \sum_{i\in I} S^{-1}M_i.$$

(vi) Ist $\mathfrak{p} \in \operatorname{Spec} A$, so bezeichne $M_{\mathfrak{p}}$ den $A_{\mathfrak{p}}$-Modul $(A \setminus \mathfrak{p})^{-1}M$.

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

1.4.12 Satz. *Seien M, N A-Moduln, $S \subseteq A$ 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*



Es gilt $S^{-1}\operatorname{id}_M = \operatorname{id}_{S^{-1}M}$ und
$$S^{-1}(\phi \circ \psi) = (S^{-1}\phi) \circ (S^{-1}\psi).$$

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

1.4.13 Satz. *Sei $S \subseteq A$ multiplikativ. Ist*
$$M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$$

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 $\frac{m}{s} \in \text{Kern } S^{-1}\beta$. 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

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

□

COl.14

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) $M = 0 \iff M_{\mathfrak{m}} = 0$ *für alle maximalen Ideale* $\mathfrak{m}$ *von* A

(ii) Die A-lineare Abbildung $\phi : M \to N$ ist genau dann injektiv (surjektiv, bijektiv, Null), wenn für jedes maximale Ideale $\mathfrak{m}$ von A die $A_{\mathfrak{m}}$-lineare Abbildung $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ diese Eigenschaft hat.

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

(iv) Ist A nullteilerfrei und faßt man $A_{\mathfrak{m}}$ auf als Unterring von $Q(A)$, so gilt

$$A = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}.$$

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

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

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

$\Leftarrow$: Injektiv: Setze $K = \ker\phi$, dann hat man $0 \to K \to M \xrightarrow{\phi} N$. Also auch $0 \to K_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{\phi_{\mathfrak{m}}} N_{\mathfrak{m}}$. Wegen $\phi_{\mathfrak{m}}$ injektiv folgt $K_{\mathfrak{m}} = 0$, also wegen (i) $K = 0$.

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

Null: Sei wieder $K = \ker\phi$. Wegen $0 \to K \to M \xrightarrow{\phi} N$ folgt $0 \to K_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{\phi_{\mathfrak{m}}} N_{\mathfrak{m}}$ d.h. $K_{\mathfrak{m}} = M_{\mathfrak{m}}$. Wegen $(M/K)_{\mathfrak{m}} \cong M_{\mathfrak{m}}/K_{\mathfrak{m}}$ also $(M/K)_{\mathfrak{m}} = 0$, also $M/K = 0$.

ad (iii): Sei

$$\phi : \left\{ \begin{array}{ccc} A & \to & M/U \\ 1 & \mapsto & x+U. \end{array} \right.$$

Dann ist $\phi = 0 \iff x \in U$.

Nach (ii) genau dann wenn $\phi_{\mathfrak{m}} : A_{\mathfrak{m}} \to (M/U)_{\mathfrak{m}} \cong M_{\mathfrak{m}}/U_{\mathfrak{m}}$ gleich 0 für alle $\mathfrak{m}$. Wegen $\phi_{\mathfrak{m}}(1) = \frac{x}{1} + U_{\mathfrak{m}}$ ist das das Gewünschte.

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

□

1.5 Der Chinesische Restsatz

Sind $\mathfrak{a}_i \in I$, Ideale von A, so ist das kleinste Ideal das alle $\mathfrak{a}_i$ umfaßt

$$\sum_{i \in I} \mathfrak{a}_i = \left\{ \sum_{i \in I} x_i : x_i \in \mathfrak{a}_i, x_i = 0 \text{ für f.a. } i \right\}$$

Sind $\mathfrak{a}, \mathfrak{b}$ Ideale, so ist $\mathfrak{a} \cdot \mathfrak{b}$ das Ideal das von den Produkten $x \cdot y$, $x \in \mathfrak{a}$, $y \in \mathfrak{b}$, erzeugt wird. Es gilt $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ aber i.a. nicht $=$. Gilt $\mathfrak{a} + \mathfrak{b} = A$, so heißen $\mathfrak{a}, \mathfrak{b}$ *coprim.*

LEI.16

1.5.1 Lemma. *Es gilt*

(i) Sind $\mathfrak{a}, \mathfrak{b}$ coprim so ist $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

(ii) Sind $\mathfrak{a}, \mathfrak{b}$ und $\mathfrak{a}, \mathfrak{c}$ coprim, so auch $\mathfrak{a}, \mathfrak{bc}$.

(iii) Gilt $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = A$, und sind $\nu_1, \ldots, \nu_n \in \mathbb{N}$, so ist auch $\mathfrak{a}_1^{\nu_1} + \cdots + \mathfrak{a}_n^{\nu_n} = A$.

(iv) Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise coprim so gilt $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n = \bigcap_{i=1}^n \mathfrak{a}_i$

Beweis.
ad (i): $\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$.

ad (ii): Sei $a \in \mathfrak{a}, b \in \mathfrak{b}$ sodaß $a + b = 1$ und $a' \in \mathfrak{a}$, $c \in \mathfrak{c}$ sodaß $a' + c = 1$. Dann folgt

$$\mathfrak{bc} \ni bc = (1-a)(1-a') = 1 + [-a - a' + aa'] \in 1 + \mathfrak{a}.$$

ad (iii): Gilt $\mathfrak{a}_1^{\nu_1} + (\mathfrak{a}_2^{\nu_2} + \cdots + \mathfrak{a}_n^{\nu_n}) = A$, so erst recht $\mathfrak{a}_1 + (\mathfrak{a}_2^{\nu_2} + \cdots + \mathfrak{a}_n^{\nu_n}) = A$. Wegen (ii) folgt

$$\mathfrak{a}_1^{\nu_1 + 1} + \mathfrak{a}_2^{\nu_2} + \cdots + \mathfrak{a}_n^{\nu_n} = A.$$

Die Behauptung folgt also mittels Induktion.

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

□

Für Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ sei ϕ der kanonische Homomorphismus

$$\phi : \left\{ \begin{array}{ccc} A & \to & \prod_{i=1}^n (A/\mathfrak{a}_i) \\ a & \mapsto & (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n) \end{array} \right.$$

Offenbar gilt $\ker \phi = \bigcap_{i=1}^n \mathfrak{a}_i$.

1.5.2 Satz (Chinesischer Restsatz). *ϕ ist surjektiv genau dann, wenn die $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise coprim sind.*

Beweis. $\Rightarrow$: Sei $a \in A$ sodaß $\phi(a) = (1, 0, \ldots, 0)$. Dann gilt $1 = (1 - a) + a \in \mathfrak{a}_1 + \mathfrak{a}_k$ $(k = 2, \ldots, n)$.
$\Leftarrow$: Seien $a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_i, i = 2, \ldots, n$, sodaß $a_i + b_i = 1$. Setze $a = \prod_{i=2}^{n} b_i \in \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n$. Es gilt

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

für ein gewisses $a' \in \mathfrak{a}_1$, also folgt $\phi(a) = (1, 0, \ldots, 0)$. □

Anders formuliert erhält man: Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise coprim, und sind $b_1, \ldots, b_n \in A$, so existiert ein $x \in A$ mit

$$x \equiv b_i \mod \mathfrak{a}_i,\ i = 1, \ldots, n.$$

1.6 Der ganze Abschluss

Ab jetzt : Ring = Integritätsbereich.

DEI.18

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

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, a_i \in A,$$

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, sodaß $xM \subseteq M$.

(ii) Sei $K = Q(A), x$ algebraisch über K. Dann gibt es $c \in A$, $c \neq 0$, sodaß 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, σ 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.
ad(i): $\Rightarrow$: Der von $\{1, \ldots, x^{n-1}\}$ erzeugte A-Modul hat die gewünschten Eigenschaften.

$\Leftarrow$: Sei $M = v_1A + \cdot + v_nA$ mit $M \neq 0$, $xM \subseteq M$. dann gibt es $a_{ij} \in A$ mit

$$\begin{aligned} xv_1 &= a_1, v_1 + \cdots + a_{1n}v_n \\ &\vdots \\ xv_n &= a_n, v_1 + \cdots + a_{nn}v_n \end{aligned}$$

Es folgt

$$\det \begin{pmatrix} x - a_n & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_m & \cdots & x - a_{nm} \end{pmatrix} = 0$$

und wir haben eine Ganzheitsgleichung.

ad (ii): Sei $a_nx^n + \cdots + a_0 = 0$ mit $a_i \in A, a_n \neq 0$. Dann folgt

$$(a_nx)^n + \cdots + a_n^{n-2}a_1(a_nx) + a_n^{n-1}a_0 = 0,$$

also ist a_nx ganz über A.

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

Sei $\mathfrak{B} = A[x_1, \ldots, x_{k+1}]$. 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 Induktionsanfang endlich erzeugter $A[x_1, \ldots, x_k]$-Modul.

ad (iv): Sei $x \in C, x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ 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 $xB_1[x] \subseteq B_1[x]$.

ad (v): Eine Ganzheitsgleichung geht bei Anwendung von σ wegen $\sigma(1) = 1$ in eine Ganzheitsgleichung über.

ad (vi): Sei $x \in B, s \in S$. Sei M ein endlich erzeugter A-Modul mit $xM \subseteq M$. Dann ist $S^{-1}M$ ein endlich erzeugter $S^{-1}A$-Modul und $\frac{x}{s}S^{-1}M \subseteq S^{-1}M$.

□

DEI.20

1.6.3 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 $Q(A)$.

1.6.4 Satz. *Sei $A \subseteq L$, B der ganze Abschluss von A in L. Dann ist B ein Ring. B ist ganz abgeschlossen in L.*

Beweis. Seien $x, y \in B$, $M, N \subseteq L$ zwei endlich erzeugte A-Moduln mit $xM \subseteq M, yN \subseteq N$. 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 $A \Rightarrow x \in B$.

□

CO1.22

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 σ 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 elementarsymetrischen Funktionen ganz über A.

□

1.6.6 Satz. *(i) Sei A nöthersch, ganz abgeschlossen, und sei L eine endliche separable Erweiterung von $K = Q(A)$. Dann ist der ganze Abschluss B von A in L endlich erzeugter A-Modul. Insbesondere ist B nöthersch.*

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

(iii) Sei A Hauptidealring, L endliche separable Erweiterung von $Q(A)$, B der ganze Abschluss von A in L. Dann ist B ein freier A-Modul von Rang $[L : Q(A)]$.

(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.
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 obdA $w_i \in B$. Die L/K-Spur $\mathrm{Tr} : L \to K$ ist K-linear und $\neq 0$. Ist $\alpha \in L$, $\alpha \neq 0$, so ist $\mathrm{Tr}(\alpha x) \in L^d$ und $\alpha \mapsto \mathrm{Tr}(\alpha x)$ ist ein K-Homomorphismus von L nach L^d. Sein Kern ist 0, also ist $L \cong L^d$ unter $\alpha \to \mathrm{Tr}(\alpha x)$. Sei $w_1', \ldots, w_n'$ die duale Basis bzgl $\mathrm{Tr}(xy)$, d.h.

$$\mathrm{Tr}(w_i w_j') = \delta_{ij},$$

und sei $c \in A$ sodaß $w_j' c \in B$.

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

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

dann ist also $\mathrm{Tr}(z w_j' c) = c b_j \in A$. Also gilt

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

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. $\frac{a}{b} \in A$.

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 $B = Aw_1 \dot{+} \ldots \dot{+} Aw_n$, dann ist $L = Kw_1 + \ldots + Kw_n$, 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.

□

DEI.24

1.6.7 Definition. Sei K eine endliche Erweiterung von $\mathfrak{Q}$ 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 $\mathbb{Z}$ ganz abgeschlossen ist und O_K ein freier $\mathbb{Z}$-Modul vom Rang $[L : \mathfrak{Q}]$.

1.7 Primideale

Sei $A \subseteq B$ eine Ringerweiterung.

DEI.25

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

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

$$\begin{array}{ccc} B & \to & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \to & A/\mathfrak{p} \end{array}$$

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

LEI.26

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

Beweis. Sei M erzeugt von $w_1, \ldots, w_m$ wobei m minimal. Dann gibt es $a_i \in \mathfrak{a}$ sodaß

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

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.

□

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

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

$$\mathfrak{p}B_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}B = \mathfrak{p}A_{\mathfrak{p}}B_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}}$$

wobei $\mathfrak{m}_{\mathfrak{p}}$ das maximale Ideal von $A_{\mathfrak{p}}$ ist. Es genügt also die erste Behauptung für den Fall A lokal zu zeigen.

·) Angenommen $\mathfrak{p}B = B$, dann ist

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

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

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

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{p}} \quad = (A \setminus \mathfrak{p})^{-1}B \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array}$$

Wir haben schon gezeigt $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$, also ist $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}}$ enthalten in einem maximalen Ideal $\mathfrak{M}$ von $B_{\mathfrak{p}}$. Dann ist $\mathfrak{M} \cap A_{\mathfrak{p}} \supseteq \mathfrak{m}_{\mathfrak{p}}$ und da $\mathfrak{m}_{\mathfrak{p}}$ maximal ist $\mathfrak{M} \cap A_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$ ($1 \notin \mathfrak{M} \cap A_{\mathfrak{p}}$). Setze

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

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

□

CO1.28

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

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

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

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

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

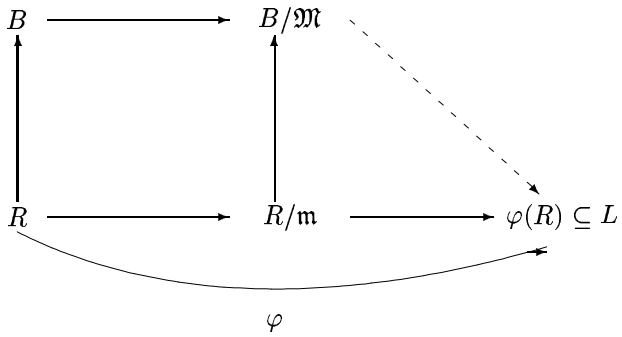
□

1.8 Fortsetzung von Homomorphismen

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

$$\psi\Big(\frac{x}{y}\Big) := \frac{\varphi(x)}{\varphi(y)}.$$

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

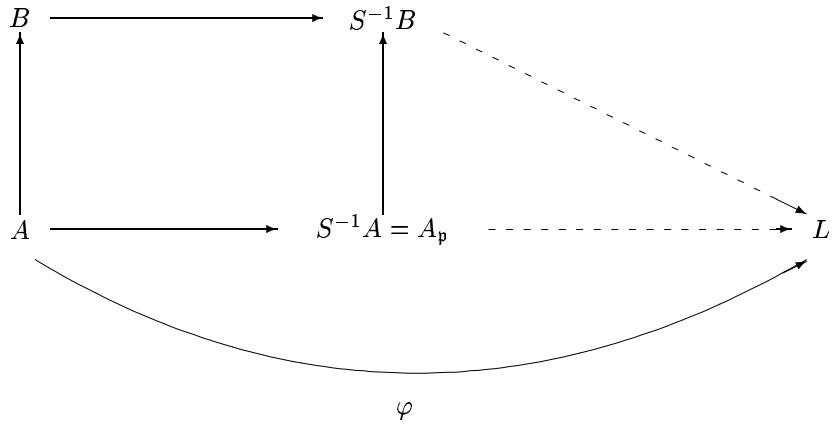


Insgesamt hat man φ auf B fortgesetzt.

LEAI.18

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

Beweis. Sei $\mathfrak{p} = \ker \varphi \in \operatorname{Spec} A$ (da L Körper), $S = A \setminus \mathfrak{p}$. Dann hat man das $S^{-1}B \supseteq A_{\mathfrak{p}}$ ganz ist.



□

1.8.2 Satz. *Sei A Ring, K Körper, $A \subseteq K$, $x \in K \setminus \{0\}$. Weiters sei $\varphi : A \to L$ in einen algebraisch abgeschlossenen Körper L. Dann hat φ entweder eine Fortsetzung auf $A[x]$ oder eine auf $A[x^{-1}]$.*

Beweis.

·) Sei $\mathfrak{p} = \ker\varphi$, dann hat φ Fortsetzung auf $A_{\mathfrak{p}}$. Sei also oBdA A lokal mit maximalen Ideal $\mathfrak{m}$ und $\ker\varphi = \mathfrak{m}$.

·) Fall $\mathfrak{m}A[x^{-1}] = A[x^{-1}]$: Dann ist

$$1 = a_0 + a_1x^{-1} + \ldots + a_nx^{-n}$$

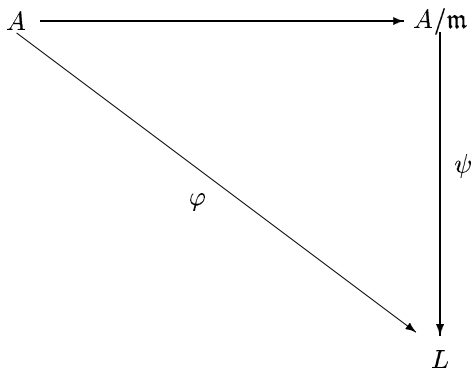
mit $a_j \in \mathfrak{m}$. Es folgt

$$(1 - a_0)x^n - a_1x^{n-1} - \ldots - a_n = 0.$$

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

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

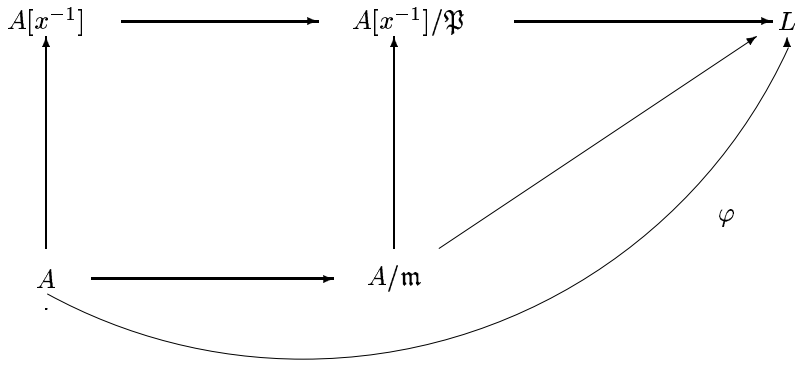
Sei ψ so daß



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

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

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



□

COA1.20

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

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

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

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

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

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

Wegen $y \in \mathfrak{m}$ und R lokal ist $1 + y \in R^*$, also x ganz über R, ein WS!.

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

$$R[x^{-1}] \to R[x^{-1}]/\mathfrak{P} \subseteq \Big(R[x^{-1}]/\mathfrak{P}\Big)^a$$

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 $\mathfrak{M}$ von Q umfaßt $\mathfrak{P}$, denn $\mathfrak{P} \mapsto 0$. Also folgt $\mathfrak{P} \cap R = \mathfrak{m}$.

·) 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 $x^{-1} \in \mathfrak{M}$ (maximales Ideal von Q). Aus der Ganzheitsgleichung erhält man

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

ein WS!.

□

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

Beweis.
·) Sei x in jedem Bewertungsring. oBdA sei $x \neq 0$. Ist $x^{-1} \in A[x^{-1}]^*$, so hat man

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

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

$$A[x^{-1}] \to A[x^{-1}]/\mathfrak{M} \subseteq \big(A[x^{-1}]/\mathfrak{M}\big)^a$$

setzt sich auf einen Bewertungsring Q von L fort. Es gilt $x^{-1} \mapsto 0$, also $x \notin Q$ WS!

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

□

Kapitel 2

Dedekind Ringe

2.1 Dedekind Ringe

DEI.29

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

DEI.30

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

Ist R nöthersch, so ist $c\mathfrak{a}$ und damit auch $\mathfrak{a}$ endlich erzeugt. Zwei gebrochene Ideale $\mathfrak{a}, \mathfrak{b}$ können genauso wie Ideale multipliziert werden $\mathfrak{a} \cdot \mathfrak{b} = \langle x \cdot y : x \in \mathfrak{a}, y \in \mathfrak{b} \rangle_{R\text{-Modul}}$.

2.1.3 Satz. *Sei R ein Dedekind Ring. Dann läßt sich jedes Ideal von R in eindeutiger Weise in ein Produkt von Primidealen zerlegen. Die (von Null verschiedenen) gebrochenen Ideale bilden eine Gruppe (mit der Multiplikation). $I(R)$.*

Beweis. Wir zeigen zuerst die zweite Behauptung.
·) Sei $\mathfrak{a}$ ein Ideal von R. Dann existiert ein Produkt von Primidealen $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{a}$: Angenommen es existiert ein Ideal das diese Eigenschaft nicht hat. Da R nöthersch ist, gibt es ein maximales solches $\mathfrak{a}$. Dieses kann nicht *prim* sein, also existiert $b_1, b_2 \in R$ mit $b_1, b_2 \notin \mathfrak{a}$, $b_i b_2 \in \mathfrak{a}$. Sei $\mathfrak{a}_1 = (\mathfrak{a}, b_1)$, $\mathfrak{a}_2 = (\mathfrak{a}, b_2)$, dann gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ aber $\mathfrak{a}_1 \supsetneq \mathfrak{a}, \mathfrak{a}_2 \supsetneq \mathfrak{a}$. Also enthält $\mathfrak{a}_1$, $\mathfrak{a}_2$ ein Produkt von Primidealen. Damit aber auch $\mathfrak{a}$, WS!.

·) Jedes maximale Ideal $\mathfrak{p}$ ist invertierbar: Sei $\mathfrak{p}^{-1}$ die Menge aller $x \in K$ sodaß $x\mathfrak{p} \subseteq R$. Dann ist $\mathfrak{p}^{-1} \supseteq R$. Wir zeigen daß $\mathfrak{p}^{-1} \neq R$: Sei $a \in \mathfrak{p}$, $a \neq 0$. Wähle r minimal sodaß

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}.$$

Dann ist eines der $\mathfrak{p}_i$ enthalten in $\mathfrak{p}$ und da jedes Primideal maximal ist folgt $\mathfrak{p}_i = \mathfrak{p}$. ObdA sei $i = 1$. Es gilt $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \not\subseteq (a)$, wähle $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_p \setminus (a)$. Dann ist $b\mathfrak{p} \subseteq (a)$ und daher $ba^{-1}\mathfrak{p} \subseteq R$, also ist $ba^{-1} \in \mathfrak{p}^{-1}$. Wegen $b \notin (a)$ ist $ba^{-1} \notin R$.

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

·) Jedes Ideal $\neq \{0\}$ ist invertierbar: Angenommen nicht. Dann existiert ein Ideal $\mathfrak{a}$ das nicht inventierbar ist und maximal mit dieser Eigenschaft. $\mathfrak{a}$ kann nicht maximal sein. Sei $\mathfrak{p}$ maximal mit $\mathfrak{a} \subsetneq \mathfrak{p}$. Dann ist

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq R$$

wo $\mathfrak{a}^{-1} := \{x \in K : x\mathfrak{a} \subseteq R\}$. Da $\mathfrak{a}$ endlich erzeugter R-Modul ist, ist $\mathfrak{a}\mathfrak{p}^{-1} \not\subseteq \mathfrak{a}$, da $\mathfrak{p}^{-1}$ nicht ganz sein kann. Also hat $\mathfrak{a}\mathfrak{p}^{-1}$ ein Inverses $\mathfrak{b}$ und $\mathfrak{b}\mathfrak{p}$ ist ein Inverses für $\mathfrak{a}\mathfrak{p}$ WS!.

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

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

Wir kommen zur ersten Behauptung:

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

·) Sind $\mathfrak{a}, \mathfrak{b}$ gebrochene Ideale, so sagen wir $\mathfrak{a}|\mathfrak{b}$ wenn gilt $\mathfrak{b} \subseteq \mathfrak{a}$ oder äquivalent wenn es ein Ideal $\mathfrak{c}$ gibt mit $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Sind $\mathfrak{p}_i, \mathfrak{q}_i$ prim und

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s\,,$$

so gilt also $\mathfrak{p}_1 \subseteq \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$ und daher $\mathfrak{p}_1 \subseteq \mathfrak{q}_i$ für ein i, also $\mathfrak{p}_1 = \mathfrak{q}_i$. Induktiv weiter erhält man $r = s$ und $\mathfrak{p}_i = \mathfrak{q}_i$ bis auf eine Permutation.

·) Ist $\mathfrak{a}$ gebrochenes Ideal wähle $c \in R$ mit $c\mathfrak{a} \in R$. Sei $(c) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, $c\mathfrak{a} = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$. Dann ist also

$$\mathfrak{a} = \frac{\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s}{\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r}.$$

Kürzt man alle oben und unten vorkommenden Ideale so ist die Darstellung eindeutig.

□

COI.31a

2.1.4 Korollar. *Sei R Dedekind, $a \in R$. Dann existieren nur endlich viele Ideale $\mathfrak{b} \triangleleft R$ mit $a \in \mathfrak{b}$.*

Beweis. Sei

$$(a) = \mathfrak{p}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{p}_r^{\alpha_r}.$$

Dann gilt

$$\mathfrak{b} \supseteq (a) \iff \mathfrak{b} = \mathfrak{p}_1^{\beta_1} \cdot \ldots \cdot \mathfrak{p}_r^{\beta_r} \text{ mit } \beta_i \leq \alpha_i.$$

□

LEI.32a

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. □

$\mathbb{Z}$ ist Dedekind, also folgt

LE32

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 $\alpha\mathfrak{R}$ mit $\alpha \in K$. Die Menge P_K der gebrochenen Hauptideale ist eine Untergruppe von I_K.

DEI.33

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 $I_K \cong \Sigma_{\mathfrak{p}\in \mathrm{Spec}\, R}\mathbb{Z}$, die Divisorengruppe. Ist $\mathfrak{a} = \prod_{\mathfrak{p}\in \mathrm{Spec}\, R} \mathfrak{p}^{r_\mathfrak{p}}$, so sagen wir $r_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}\, \mathfrak{a}$. Ist $\mathrm{ord}_\mathfrak{p}\, \mathfrak{a} > 0$ $(= 0, < 0)$, so hat $\mathfrak{a}$ eine Nullstelle bei $\mathfrak{p}$ (ist eine Einheit bei $\mathfrak{p}$, hat einen Pol bei $\mathfrak{p}$).

Offenbar gilt $\mathfrak{a}|\mathfrak{b} \iff \forall \mathfrak{p} : \mathrm{ord}_\mathfrak{p}\, \mathfrak{a} \leq \mathrm{ord}_\mathfrak{p}\, \mathfrak{b}$. Es ist $\mathrm{ord}_\mathfrak{p}(\alpha) = 0$ genau dann wenn α eine Einheit in $R_\mathfrak{p}$ ist.

LEI.34

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

Beweis. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ die Primideale von R. Sei $\mathfrak{a}$ ein Ideal,

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_s^{rs}.$$

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

$$(\alpha) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s},$$

dann folgt unmittelbar $e_i = r_i$ und daher $(\alpha) = \mathfrak{a}$. □

LEI.35

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

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

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

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 $S^{-1}(\mathfrak{a}\cdot\mathfrak{b}) = (S^{-1}\mathfrak{a})\cdot(S^{-1}\mathfrak{b})$ 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 $\mathfrak{a} \cap S \neq \emptyset$, so ist $S^{-1}\mathfrak{a} = S^{-1}A$. Ist umgekehrt $S^{-1}\mathfrak{a} = S^{-1}A$, so ist $1 = \frac{\alpha}{s}$ für gewisse $\alpha \in \mathfrak{a}, s \in S$, also $\mathfrak{a} \cap S \neq \emptyset$.

□

LEI.36

2.1.10 Lemma. *Sei A Dedekind Ring und sei die Idealklassengruppe endlich. Sei $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ein vollständiges Repräsentantensystem der Idealklassen. Ist $b \in \bigcap \mathfrak{a}_i$, $b \neq 0$, $b \in A$, und ist $S = \{1, b, b^2, b^3, \ldots\}$, dann ist $S^{-1}A$ Hauptidealring.*

Beweis. Bei Anwendung von S^{-1} werden die $\mathfrak{a}_i$ auf $S^{-1}A$ abgebildet. Da Hauptideale auf Hauptideale gehen folgt die Behauptung da S^{-1} surjektiv ist.

□

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

LEI.36A

2.1.11 Lemma. *Sei K ein algebraischer Zahlkörper. Dann existiert $M \in \mathbb{N}$ mit der folgenden Eigenschaft: Sind $\alpha, \beta \in O_K$, $\beta \neq 0$, dann existiert $t \in \mathbb{N}$, $1 \leq t \leq M$, und $w \in O_K$, sodaß*

$$|N_{\mathbb{Q}}^K(t\alpha - w\beta)| < |N_{\mathbb{Q}}^K(\beta)|.$$

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

·) 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 ($n = [K : R]$)

$$|N_{\mathbb{Q}}^K(\gamma)| = |\prod_{\sigma \text{ Einbettung}} \sum \gamma_i \sigma(w_i)| \leq (\max |\gamma_i|)^n \underbrace{(\prod_{\sigma} \sum |\sigma(w_i)|)}_{=:c}$$

Wähle $m > \sqrt[n]{c}$ und setze $M := m^n$.

·) 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.

·) Betrachte die Abbildung $\phi : K \to \mathbb{R}^M$ 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 ($t = h - l \leq m^n$),

$$t\gamma = h\gamma - l\gamma = \underbrace{([h\gamma] - [l\gamma])}_{=:w} + \underbrace{(\{h\gamma\} - \{l\gamma\})}_{\delta}$$

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

$$|N_{\mathbb{Q}}^K(\delta)| \leq (\frac{1}{m})^n C < 1.$$

□

2.1.12 Satz. *Sei K ein algebraischer Zahlkörper. Dann ist $|C_K| =: h_K$ endlich.*

Beweis. Sei $\mathfrak{a} \triangleleft O_K$. Für jedes $\alpha \in \mathfrak{a}, \alpha \neq 0$, ist $|N_{\mathbb{Q}}^K(\alpha)| \in \mathbb{N}$. Wähle $\beta \in \mathfrak{a}, \beta \neq 0$, sodaß $|N_{\mathbb{Q}}^K(\beta)|$ minimal ist. Für jedes $\alpha \in O_K$ existiert $t, 1 \leq t \leq M$, sodaß ($w \in O_K$ geeignet)

$$|N_{\mathbb{Q}}^K(t\alpha - w\beta)| < |N_{\mathbb{Q}}^K(\beta)|.$$

Es folgt

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

und damit also

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

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

□

COI.36c

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

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

□

LEI.36d

2.1.14 Lemma. *Sei A Dedekind, M, N zwei A-Moduln. Sei $\mathfrak{p}$ ein Primideal von A und $S_\mathfrak{p} = A \setminus \mathfrak{p}$. Gilt $S_\mathfrak{p}^{-1}M \subseteq S_\mathfrak{p}^{-1}N$ für alle $\mathfrak{p}$, so folgt $M \subseteq N$.*

Beweis. Sei $a \in M$. Zu jedem $\mathfrak{p}$ existiert $x_\mathfrak{p} \in N, s_\mathfrak{p} \in S_\mathfrak{p}$, sodaß $s_\mathfrak{p} a = x_\mathfrak{p}$. Sei $\mathfrak{b}$ das von den $s_\mathfrak{p}$ erzeugte Ideal, dann gilt $\mathfrak{b} = A$, also

$$1 = \Sigma y_\mathfrak{p} s_\mathfrak{p}$$

für gewisse $y_\mathfrak{p} \in A$ die fast alle $= 0$ sind. Es folgt

$$a = \Sigma y_\mathfrak{p} s_\mathfrak{p} a = \Sigma y_\mathfrak{p} x_\mathfrak{p} \in N.$$

□

2.2 Diskrete Bewertungsringe

DEI.37

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 $\mathfrak{p}$ ein Primideal, so ist also $A_\mathfrak{p}$ ein diskreter Bewertungsring. Sei R diskreter Bewertungsring und π das Primelement. Dann läßt sich also jedes $x \in R$ schreiben als $x = c\pi^\nu$ mit $c \in R^*$ und $\nu \in \mathbb{N} \cup \{0\}$.

DEI.38

2.2.2 Definition. Sei K ein Körper, Γ eine geordnete Gruppe ($0 \notin \Gamma$). Eine Abbildung

$$v : \begin{cases} K & \to & \Gamma \cup \{0\} \\ x & \mapsto & |x| \end{cases}$$

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.

DEI.39

2.2.3 Definition. Sei K ein Körper, R ein Unterring von K. R heißt Bewertungsring, falls gilt

$$\forall x \in K : (x \in R \vee x^{-1} \in R).$$

Ist R diskreter Bewertungsring, so ist R Bewertungsring 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 Bewertungsring. Ist umgekehrt $R \subseteq K$ $(= Q(R))$ ein Bewertungsring so existiert eine Bewertung v von K mit $R = R_v$. Es ist R_v lokal mit maximalen Ideal $\mathfrak{m} = \{x \in K : v(x) < 1\}$ und $R_v^* = \{x \in K : v(x) = 1\}$.

R ist ein diskreter Bewertungsring genau dann wenn er ein Bewertungsring ist der von einer diskreten Bewertung kommt.

Beweis.
·) 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 $v(1) = I_\Gamma$ das Einselement von Γ.

·) Sei R ein Bewertungsring. 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 $y \in U$ WS!. 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 $(zb)x = 1$ WS!.

·) Sei $\mathfrak{m}$ das maximale Ideal von R, dann ist $R = U \cup \mathfrak{m}$ und daher ($\mathfrak{m}^* = \mathfrak{m} \setminus \{0\}$)

$$K^* = \mathfrak{m}^* \cup U \cup (\mathfrak{m}^*)^{-1},$$

als disjunkte Vereinigung. Da $\mathfrak{m}^*$ multiplikativ ist, ist

$$\Gamma = K^*/U$$

eine geordnete Gruppe ($xU < U \iff x \in \mathfrak{m}^*$). Für $x \in K^*$ setze $v(x) := xU \in \Gamma$, für $x = 0$ setze $v(x) = 0$.

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

·) Sei v eine diskrete Bewertung, $R = R_v$ der Bewertungsring zu v. Wähle einen Erzeuger γ von Γ und schreibe $\gamma = v(\pi)$. Da mit γ auch γ^{-1} die Gruppe Γ erzeugt sei oBdA $\pi \in R$. Da $\gamma \neq 1_\Gamma$ 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

$$(\pi) \supsetneq (\pi^2) \supsetneq (\pi^3) \geq \dots,$$

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

·) Sei R_v ein diskreter Bewertungsring. Sei $\mathfrak{m} = (\pi)$ dann hat die Primfaktorzerlegung von $x \in R$ die Gestalt $x = \cap\pi^r$, $r\mathbb{N}_0$, $u \in R^*$ weil es nur ein Primelement 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 $\langle v(\pi)\rangle = \Gamma$.

□

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 1.6.2, (v)).

2.3.1 Satz. *Sei A ganz abgeschlossen, L eine endliche Galoische Erweiterung von $K = Q(A)$ mit Gruppe G, B der ganze Abschluß vor A in L. Sei $\mathfrak{p} \in \operatorname{Spec} A$, $\mathfrak{P}, Q \in \operatorname{Spec} B$ die über $\mathfrak{p}$ liegen. Dann existiert $\sigma \in G$ sodaß $\sigma\mathfrak{P} = \mathfrak{Q}$.*

Beweis.
·) Betrachte zuerst den Fall daß $\mathfrak{p}$ maximal ist. Angenommen $\mathfrak{P} \neq \sigma\mathfrak{Q}$ 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 $N_K^L(x) = \prod_{\sigma \in G} \sigma x$ liegt in $B \cap K = A$ denn A ist ganz abgeschlossen und sogar in $\mathfrak{P} \cap K = \mathfrak{p}$. Jedoch ist stets $\sigma x \notin \mathfrak{Q}$, also $N_K^L(x) \notin \mathfrak{Q} \cap K = \mathfrak{p}$, WS!.

·) Sei nun allgemein $\mathfrak{p} \in \operatorname{Spec} A$. Wir lokalisieren: Sei $S = A \setminus \mathfrak{p}$. Dann ist $S^{-1}B$ der ganze Abschluß von $S^{-1}A$ in L, $S^{-1}\mathfrak{p}$ maximales Ideal von $S^{-1}A$, $S^{-1}\mathfrak{P}, S^{-1}Q \in \operatorname{Spec} S^{-1}B$ und liegen über $S^{-1}\mathfrak{p}$. Es folgt daß es $\sigma \in G$ gibt mit $\sigma(S^{-1}\mathfrak{P}) = S^{-1}\mathfrak{Q}$. Da $S \subseteq K$ und daher bei σ fix bleibt folgt $\sigma\mathfrak{P} = \mathfrak{Q}$.

□

COI.42

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 $\mathfrak{p} \in \operatorname{Spec} A$. 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 $\mathfrak{Q}_1, \mathfrak{Q}_2$ verschiedene Primideale von B über $\mathfrak{p}$, und $\mathfrak{P}_1, \mathfrak{P}_2$ Primideale vom ganzen Abschluß C von A in L die über $\mathfrak{Q}_1$ bzw. $\mathfrak{Q}_2$ liegen, dann ist $\mathfrak{P}_1 \neq \mathfrak{P}_2$ und $\mathfrak{P}_1, \mathfrak{P}_2$ liegen über $\mathfrak{p}$. Wegen dem Satz gibt es nur endlich viele solche $\mathfrak{P}$'s.

□

DEI.43

2.3.3 Definition. Sei $\mathfrak{p}$ 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, $\mathfrak{p} \in \operatorname{Spec} A$ maximal, $\mathfrak{P} \in \operatorname{Spec} B$ über $\mathfrak{p}$. Dann heißt die Körpererweiterung

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

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

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

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

$$G_{\mathfrak{P}} \to \operatorname{Aut}(B/\mathfrak{P} : A/\mathfrak{p}]).$$

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 $\mathfrak{p}$.

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

LEI.44

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.
·) 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 $\mathfrak{P} \cap B^d$.

·) Habe E die obige Eigenschaft und sei H die Gruppe von L über E. Setze $\mathfrak{q} = \mathfrak{P} \cap E$. Wegen Satz 2.3.1 sind die $\sigma\mathfrak{P}, \sigma \in H$, genau die Primideale über $\mathfrak{q}$. Es folgt $\sigma\mathfrak{P} = \mathfrak{P}$, d.h. $H \subseteq G_{\mathfrak{P}}$ und damit $E \supseteq L^d$.

□

2.3.5 Satz. *Sei $\mathfrak{Q} = B^d \cap \mathfrak{P}$. Dann gilt (mittels der kanonischen Einbettung $A/\mathfrak{p} \to B^d/\mathfrak{Q}$) $A/\mathfrak{p} = B^d/\mathfrak{Q}$.*

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 $\mathfrak{Q}_\sigma = \sigma^{-1}\mathfrak{P} \cap B^d$. Dann ist $\mathfrak{Q}_\sigma \neq \mathfrak{Q}$, denn über $\mathfrak{Q}$ liegt ja nur ein Primideal nämlich $\mathfrak{P}$.

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

$$\begin{array}{lll} y \equiv x & \mod & \mathfrak{Q} \\ y \equiv 1 & \mod & \mathfrak{Q}_\sigma, \sigma \in G \setminus G_{\mathfrak{P}}. \end{array}$$

Speziell folgt

$$\begin{array}{lll} y \equiv x & \mod & \mathfrak{P} \\ y \equiv 1 & \mod & \sigma^{-1}\mathfrak{P}, \sigma \in G \setminus G_{\mathfrak{P}}, \end{array}$$

also

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

Die Norm $N_K^{L^d}(y)$ ist das Produkt $\prod \sigma y$ wobei σ ein vollständiges Restsystem modulo $G_{\mathfrak{P}}$ durchläuft. Also folgt

$$N_K^{L^d}(y) \equiv x \mod \mathfrak{P}.$$

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

□

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 $\mathrm{Aut}(B/\mathfrak{P} : A/\mathfrak{p})$ sei bezeichnet mit $\sigma \mapsto \bar{\sigma}$. Dann ist offenbar

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

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

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

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* $\mathrm{Aut}(B/\mathfrak{P} : A/\mathfrak{p})$.

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

$$f(X) = (X - x_1) \cdots (X - x_m).$$

Da $\bar{x}$ eine Wurzel des Polynoms

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

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

·) Wegen obigem folgt daß

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

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 $\mathfrak{p}$ nur ein Primideal: Wegen Satz 2.3.5 ist

$$\mathrm{Aut}(\bar{B} : \bar{A}) = \mathrm{Aut}(\bar{B} : B^d/\mathfrak{Q}),$$

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

·) Sei also $G = G_{\mathfrak{P}}$. 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 $\sigma \in G = G_{\mathfrak{P}}$ sodaß $\sigma x = y$. Zu jedem $\bar{\tau}$ existiert daher ein $\sigma \in G_{\mathfrak{P}}$ sodaß $\bar{\sigma} = \bar{\tau}$.

□

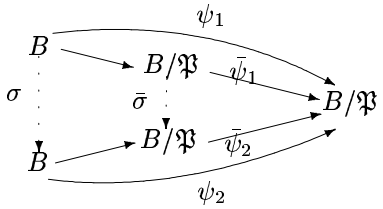
CO1.47

2.3.7 Korollar. *Seien A, K, B, L, G wie im Satz, sei $\mathfrak{p}$ ein maximales Ideal von A, $\varphi : A \to A/\mathfrak{p}$ der kanonische Homomorphismus. Sind ψ_1, ψ_2 Homomorphismen von B in einen algebraischen Abschluß von $A/\mathfrak{p}$ die φ fortsetzen, so existiert $\sigma \in G$ sodaß*

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

Beweis.
·) $\ker \psi_1, \ker \psi_2$ sind Primideale von B die über $\mathfrak{p}$ 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 ψ_1, ψ_2 den gleichen Kern $\mathfrak{P}$.

·) Sei also $\ker \psi_1 = \ker \psi_2 = \mathfrak{P}$. Sei $B/\mathfrak{P} \subseteq (A/\mathfrak{p})^a$. $\psi_1 : B \to (A/\mathfrak{p})^a$ induziert eine Einbettung $\bar{\psi}_1 : B/\mathfrak{P} \to (A/\mathfrak{p})^a$. Da $B/\mathfrak{P}$ normal über $A/\mathfrak{p}$ ist folgt $\bar{\psi}_1 \in \mathrm{Aut}(B/\mathfrak{P} : A/\mathfrak{p})$. Genauso für ψ_2. Also existiert $\sigma \in G_{\mathfrak{P}}$ so daß $\bar{\psi}_2^{-1} \circ \bar{\psi}_1 = \bar{\sigma}$. Man hat das Diagramm



□

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 $\mathfrak{p} \in \operatorname{Spec} A$, so ist $\mathfrak{p}B$ ein Ideal von B. Daher gilt mit gewissen $\mathfrak{P}_i \in \operatorname{Spec} B, e_i \geq 1$,

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

LEI.48

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

Beweis. Da jedes $\mathfrak{P}_E \operatorname{Spec} B$ maximal ist und die Faktoren paarweise coprim, gilt

$$\mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r} = \mathfrak{P}_1^{e_1} \cap \ldots \cap \mathfrak{P}_r^{e_r}.$$

Ist $\mathfrak{P}$ eine Primstelle über $\mathfrak{p}$ die nicht vorkommt, so wäre ($\mathfrak{P} \supseteq \mathfrak{p}B$)

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cap \ldots \cap \mathfrak{P}_r^{e_r} = \mathfrak{P}_1^{e_1} \cap \ldots \cap \mathfrak{P}_r^{e_r} \cap \mathfrak{P},$$

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

DEI.49

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

Für $\mathfrak{P} \in \operatorname{Spec} B$ definiert man

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

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

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

LEI.50

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 Abschlüße von A in an E bzw. L. Sei $\mathfrak{p} \in \operatorname{Spec} A, \mathfrak{q} \in \operatorname{Spec} B, \mathfrak{P} \in \operatorname{Spec} C, \mathfrak{q}/\mathfrak{p}, \mathfrak{P}/\mathfrak{q}$. Dann gilt*

(i)

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

(ii)

$$N_K^E \circ N_E^L = N_K^L.$$

Beweis. Klar nach Definition. □

LEI.51

2.4.4 Lemma. *Sei A lokal, M freier A-Modul vom Rang n, $\mathfrak{p}$ das maximale Ideal von A. Dann ist $M/\mathfrak{p}M$ ein n-dimensionaler Vektorraum über $A/\mathfrak{p}$.*

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

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

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

$$\sum \bar{\lambda}_i \bar{x}_i = 0 \text{ in } M/\mathfrak{p}M,$$

so ist $\sum \lambda_i x_i \in \mathfrak{p}M$. Es gilt $\mathfrak{p}M = \sum \mathfrak{p}x_i$ und wegen der Eindeutigkeit der Darstellung folgt $\bar{\lambda}_i = 0$.

□

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 $\mathfrak{p} \in \operatorname{Spec} A$, so gilt*

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

Beweis.
·) ObdA sei A lokal: Wir lokalisieren bei $\mathfrak{p}$. Ist $S = A \setminus \mathfrak{p}$, 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

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r},$$

so ist wegen Lemma 2.1.9

$$(S^{-1}\mathfrak{p})(S^{-1}B) = S^{-1}(\mathfrak{p}B) = (S^{-1}\mathfrak{P}_1)^{e_1} \cdot \ldots \cdot (S^{-1}\mathfrak{P}_r)^{e_r}$$

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

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

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

·) Sei A ein lokaler Dedekind Ring. Dann ist A, B Hauptidealring, B ein freier A-Modul von Rang $n = [L : K]$ und $B/\mathfrak{p}B$ ein n-dimensionaler $A/\mathfrak{p}$ Vektorraum.
Sei $\mathfrak{p}B = \mathfrak{P}_1^{e_r} \cdots \mathfrak{P}_r^{e_r}$. Der Homomorphismus

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

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

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

ein $A/\mathfrak{p}$-Homomorphismus.

·) Wir bestimmen die Dimension von $B/\mathfrak{P}^e$. Sei π ein Erzeuger von $\mathfrak{P}$ und $j \geq 1$. Wegen $\mathfrak{p}\mathfrak{P}^j \subseteq \mathfrak{P}^{j+1}$ ist $\mathfrak{P}^j/\mathfrak{P}^{j+1}$ ein $A/\mathfrak{p}$-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 $A/\mathfrak{p}$, also gleich $f(\mathfrak{P}/\mathfrak{p})$. 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

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

□

COI.53

2.4.6 Korollar. *Sei $\mathfrak{a} \in I(A)$, dann gilt*

$$N_K^L(\mathfrak{a}B) = \mathfrak{a}^{[L:K]}.$$

Beweis. Ist $\mathfrak{p}$ prim, $\mathfrak{p}B = \mathfrak{P}_i^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, so gilt

$$N_K^L(\mathfrak{p}B) = N_K^L(\mathfrak{P}_1)^{e_1} \cdot \ldots \cdot N_K^L(\mathfrak{P}_r)^{e_r} = \mathfrak{p}^{\sum e_i f_i} = \mathfrak{p}^{[L:K]}.$$

□

COI.54

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

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

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

□

COI.55

2.4.8 Korollar. *Sei L Galois über K mit Gruppe G und sei $\mathfrak{P}/\mathfrak{p}$. Dann gilt ($\mathfrak{p}B = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r)^e$)*

$$N_K^L(\mathfrak{P})B = \prod_{\sigma \in G} \sigma\mathfrak{P} = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r)^{ef}.$$

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

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

□

COI.56

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 $\mathfrak{b} = (\beta)$ ein gebrochenes Hauptideal von B. Dann gilt*

$$N_K^E(\mathfrak{b}) = (N_K^E(\beta))$$

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

$$N_E^L(\mathfrak{b}C) = \mathfrak{b}^{[L:E]},\ N_E^L(\beta) = \beta^{[L:E]}.$$

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

$$N_K^L(\mathfrak{b}C) = (N_K^L(\beta)),$$

und wegen

$$N_K^L = N_K^E \circ N_E^L,$$
$$N_K^E(\mathfrak{b})^{[L:E]} = (N_K^E(\beta))^{[L:E]}.$$

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

$$N_K^E(\mathfrak{b}) = (N_K^E(\beta)).$$

·) Sei also oBdA E Galois über K. Dann gilt $N_K^E(\beta) = \prod_{\sigma\in G}\sigma\beta$, also

$$(N_K^E(\beta))_A \cdot B = \prod_{\sigma\in G}\sigma(\beta)_B = \prod_{\sigma\in G}\sigma\mathfrak{b} = N_K^E\mathfrak{b}\cdot B$$

wegen Korollar 2.4.8. Es folgt

$$(N_K^E(\beta))_A^{[E:K]} = N_K^E[(N_K^E(\beta))_A B] = N_K^E[N_K^E\mathfrak{b}\cdot B] = (N_K^E\mathfrak{b})^{[E:K]}.$$

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

$$(N_K^E(\beta))_A = N_K^E\mathfrak{b}$$

□

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 $\mathfrak{P} \in \operatorname{Spec} B$ 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 π 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

$$\mathfrak{p}B + C = B.$$

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

$$x = \sum c_{ij}\beta^j\pi^i \mod \mathfrak{p}B$$

mit gewissen $c_{ij} \in A$.

□

2.4.11 Satz. *Sei A Dedekind und sei $|A/\mathfrak{p}| < \infty$ für alle $\mathfrak{p} \in \operatorname{Spec} A$. Ist $\mathfrak{a}$ Ideal von A bezeichne mit $N\mathfrak{a} := |A/\mathfrak{a}|$. Dann gilt*

$$N\mathfrak{a} = \prod_{\mathfrak{p}} [N\mathfrak{p}]^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}}.$$

Beweis. Es ist $A/\mathfrak{a} \cong \prod_{\mathfrak{p}} A/\mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}}$, Es genügt also $|A/\mathfrak{p}^n|$ zu bestimmen. Dazu lokalisiere bei $\mathfrak{p}$, dann ist oBdA $\mathfrak{p}$ Hauptideal. Dann ist offenbar $A/\mathfrak{p} \cong \mathfrak{p}/\mathfrak{p}^2 \cong, \ldots$, also $|A/\mathfrak{p}^n| = |A/\mathfrak{p}|^n$. □

REI.58a

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

$$N\mathfrak{p} = p^{f(\mathfrak{p}/(p))}.$$

Ist $\alpha \in O_K$, so gilt $N_{\mathbb{Q}}^K(\alpha) = \pm N(\alpha)$. Es gibt für jedes M nur endlich viele Ideale $\mathfrak{a}$ mit $N\mathfrak{a} \leq M$.

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 $\mathfrak{p} \in \operatorname{Spec} A$.

Sei vorausgesetzt daß $B = A[\alpha]$ für ein geeignetes $\alpha \in B$.

REI.59a

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

$$B_{\mathfrak{p}} = A_{\mathfrak{p}}[\alpha_{\mathfrak{p}}].$$

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

$$\pi : A \to A/\mathfrak{p} =: \bar{A}$$

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

$$\bar{f}(X) = \bar{P}_1(X)^{e_1} \cdot \ldots \cdot \bar{P}_1(X)^{e_r},$$

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

Φ steht in bijektiver Beziehung zu der Nullstellenmenge 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

$$\phi : \begin{cases} B & \to & L \\ g(\alpha) & \mapsto & \bar{g}(\beta) \end{cases} \qquad (g = A[x])$$

wohldefiniert: Ist $g(\alpha) = 0$, so folgt $f|g$ also auch $\bar{f}|\bar{g}$, also $\bar{g}(\beta) = 0$. Offenbar setzt ϕ auch π fort. Wegen $B = A[\alpha]$ ist ϕ 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 $\bar{P}_i$ sind. Es gilt*

$$\{\mathfrak{P} \in \operatorname{Spec} B : \mathfrak{P}/\mathfrak{p}\} = \{\ker\phi : \phi \in \Phi\},$$

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

$$e(\mathfrak{P}/\mathfrak{p}) = e_i,\ f(\mathfrak{P}/\mathfrak{p}) = \deg\bar{P}_i,\ \mathfrak{P} = \mathfrak{p}B + P_i(\alpha)B.$$

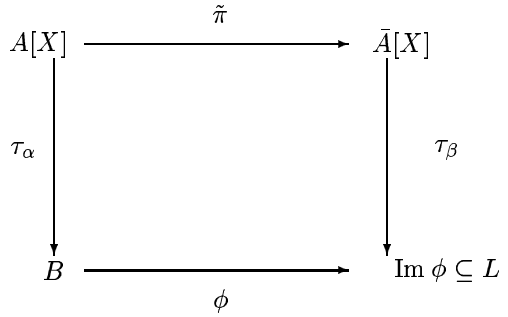
Beweis.

·) Es gilt $\ker\phi \cap A = \mathfrak{p}$: Da ϕ die Projektion π fortsetzt ist $\mathfrak{p} \subseteq \ker\phi$. Sei $\gamma \in A \cap \ker\phi$. Dann ist

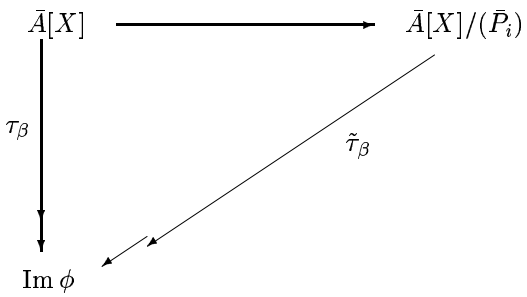
$$0 = \phi(\gamma) = \pi(\gamma),$$

d.h. $\gamma \in \mathfrak{p}$ (...$\mathfrak{p}$ das maximale Ideal von A).

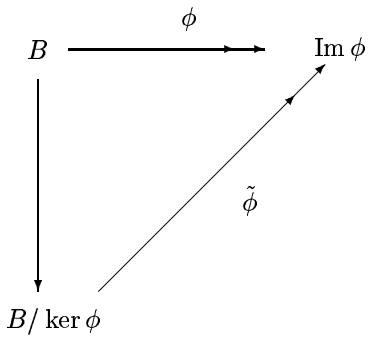
·) Betrachte das Diagramm



wobei τ_α bzw. τ_β die Punktauswertung an α bzw. β ist und $\beta = \phi(\alpha)$. Sei β Nullstelle von $\bar{P}_i$, dann faktorisiert sich τ_β als



und ϕ als



Es folgt $B/\ker\phi \cong \bar{A}[X]/(\bar{P}_i)$. Da $\bar{P}_i$ irreduzibel ist, folgt $\ker\phi \in \operatorname{Spec} B$. Weiters ist

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

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

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

gehören also ϕ, ψ zu $\bar{P}_i$ so ist $\ker\phi = \ker\psi$.

$\cdot$) Ist umgekehrt $\ker\phi = \ker\psi$, und gehört ϕ zu $\bar{P}_i$ und ψ zu $\bar{P}_j$, so folgt

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

also $\bar{P}_i = \bar{P}_j$.

$\cdot$) Sei $\mathfrak{P} \in \operatorname{Spec} B$, $\mathfrak{P}/\mathfrak{p}$, und sei L' ein algebraischer Abschluß von $A/\mathfrak{p}$ mit $L' \supseteq B/\mathfrak{P}$. $L' \cong L$ über $\bar{A}$ vermöge ι, $\sigma : B \to B/\mathfrak{P}$ die kanonische Projektion. Dann ist

$$\phi := \iota \circ \sigma : B \to L$$

eine Fortsetzung von π und $\ker\phi = \mathfrak{P}$.

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

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

und dieser Isomorphismus ist ein $\bar{A}$-Vektorraum Isomorphismus denn eingeschränkt auf $\bar{A}$ ist er id. Also folgt

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

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

$$\tau_\alpha(pX^k) = p\alpha^k \in \mathfrak{p}B.$$

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

$$\mathfrak{P} = \ker\phi = \tau_\alpha(\tilde{\pi}^{-1}((\bar{P}_i))) = \tau_\alpha\big((P_i)_{A[X]} + \mathfrak{p}[X]\big) = P_i(\alpha)B + \mathfrak{p}B.$$

·) Es gilt $f - P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} \in \ker \tilde{\pi} = \mathfrak{p}[X]$, also wegen $f(\alpha) = 0$

$$-P_1(\alpha)^{e_1} \cdot \ldots \cdot P_r(\alpha)^{e_r} = \tau_\alpha(f - P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}) \in \mathfrak{p}B.$$

Nun gilt, wenn $\mathfrak{P}_i/\mathfrak{p}$ zu $\bar{P}_i$ gehört,

$$\mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}B + P_i^{e_i}(\alpha)B,$$

also folgt

$$\mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}B + P_i^{e_i}(\alpha) \cdot \ldots \cdot P_r^{e_r}(\alpha)B \subseteq \mathfrak{p}B.$$

Damit ist

$$e_i \geq e(\mathfrak{P}_i/\mathfrak{p}),\ i = 1, \ldots, r.$$

Wegen

$$\sum e_i \deg P_i = \deg f = [E : K] = \sum e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) := \sum e(\mathfrak{P}_i/\mathfrak{p}) \deg P_i$$

folgt $e_i = e(\mathfrak{P}_i/\mathfrak{p})$.

□

2.6 Die Diskriminante

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

DEI.61

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

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

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

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

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

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

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

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

□

LEI.63

2.6.3 Lemma. *Seien $\{\alpha_1,\dots,\alpha_n\}$, $\{\beta_1,\dots,\beta_n\}$ Basen von L/K. Seien $a_{ij}\in K$ sodaß $\alpha_i=\sum a_{ij}\beta_j$. Dann gilt*

$$\Delta(\alpha_1,\dots,\alpha_n)=\det(a_{ij})^2\Delta(\beta_1,\dots,\beta_n).$$

Beweis. Es gilt

$$\alpha_i\alpha_k=\sum_{j,l}a_{ij}a_{kl}\beta_j\beta_l.$$

Setze $A=(\mathrm{tr}(\alpha_i\alpha_k))$, $B=(\mathrm{tr}(\beta_j\beta_l))$,$C=(a_{ij})$, dann ist $A=C^TBC$.

□

LEI.64

2.6.4 Lemma. *Sei L/K separabel, $\{\sigma_j : j=1,\dots,n\}$ die Einbettungen von L/K. Dann gilt*

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

Beweis. Es gilt

$$\mathrm{tr}(\alpha_i\alpha_j)=\sum_l\sigma_l(\alpha_i\alpha_j).$$

Setze $A=(\mathrm{tr}(\alpha_i\alpha_j))$, $B=(\sigma_l(\alpha_i))$, dann gilt $A=BB^T$.

□

2.6.5 Satz. *Sei L/K separabel und sei $\beta\in L$ sodaß $\{1,\beta,\dots,\beta^{n-1}\}$ linear unabhängig ist. Sei $f\in K[X]$ das Minimalpolynom von β über K. Dann gilt*

$$\Delta(1,\beta,\dots,\beta^{n-1})=(-1)^{\frac{n(n-1)}{2}}N(f'(\beta)).$$

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

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

und es folgt

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

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

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

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, $n = [K : \mathbb{Q}]$, $\mathfrak{a} \triangleleft O_K$. Sei $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$ eine Basis von $K/\mathbb{Q}$ sodass $|\triangle(\alpha_1, \ldots, \alpha_n)|$ minimal ist (solche $\alpha_1, \ldots, \alpha_n$ existieren stets). Dann gilt*

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

Und umgekehrt.

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

·) Trivial ist $\mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n \subseteq \mathfrak{a}$. Sei also $\alpha \in \mathfrak{a}$ und schreibe

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

Sind alle $\gamma_i \in \mathbb{Z}$ sind wir fertig. Sei angenommen ein $\gamma_i \notin \mathbb{Z}$, oBdA $\gamma_1 \notin \mathbb{Z}$. Schreibe $\gamma_1 = m + \vartheta$, $m \in \mathbb{Z}$, $0 < \vartheta < 1$, und setze

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

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

$$\begin{pmatrix} \vartheta & \gamma_2 & \gamma_3 & \cdots & \gamma_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & 1 \end{pmatrix}$$

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

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

□

DEI.67

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

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

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

$$\mathrm{tr}(w\alpha_j) = \sum a_i \,\mathrm{tr}(\alpha_i\alpha_j), \ j = 1, \ldots, n.$$

Wegen der Cramerschen Regel schreibt sich a_i als ganze Zahl dividiert durch $\Delta(\alpha_1, \ldots, \alpha_n)$.

□

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 $w_1, \ldots, w_n$ sodaß*

$$a_j = c_{j1}w_1 + \cdots + c_{jj}w_j, \ j = 1, \ldots, n,$$

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

Beweis.
·) Sei d_{ii} die kleinste natürliche Zahl sodaß 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 $d_{ii} \neq 0$.

·) Sei $c \in O_K$ von der Form

$$c = \frac{1}{\Delta(a_1, \ldots, a_n)}(c_1a_1 + \cdots + c_ja_j)$$

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

$$c - sw_j \in O_K$$

und es ist

$$c - sw_j = \frac{1}{\Delta(a_1, \ldots, a_n)} \Big((c_1 - sd_{j1})a_1 + (c_2 - sd_{j2})a_2 + \cdots + ra_j\Big),$$

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

·) 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

$$x = \frac{1}{\Delta(a_1, \ldots, a_n)}(x_1a_1 + \cdots + x_ja_j), \ x_i \in \mathbb{Z},$$

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 $x = \frac{x_1}{d_11}w_1 \in M_0$.
$j - 1 \mapsto j$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 $\mathbb{M} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$ 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 $b_1, \ldots, b_n \in M$ sodaß

$$b_i = \sum_{k=1}^{i} c_{ik} w_k, \ c_{ik} \in \mathbb{Z},$$

wobei $c_{ii} \in \mathbb{N}$ kleinstmöglich ist. Genauso 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 $c_{ii} | t_i$. Also sind die Zahlen

$$\alpha_1 w_1 + \cdots + \alpha_n w_n, \ 0 \leq a_j < c_{jj},$$

paarweise inkongruent modulo M. Offenbar sind es genau $c_{11} \cdot \ldots \cdot c_{nn}$ viele.

Wir zeigen daß sie ein vollständiges Repräsentantensystem modulo M bilden: Sei

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

ein Element von O_K. Sei $0 \leq \mu_n < c_{nn}$ sodaß $\lambda_n \equiv \mu_n \mod c_{kn}$ 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 $0 \leq \mu_{n-1} < c_{n-1,n-1}$, sodaß $\lambda_{n-1} - A_n c_{n,n-1} \equiv \mu_{n-1} \mod c_{n-1,n-1}$. 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 $\alpha_k, \mu_k \in \mathbb{Z}, 0 \leq \mu_k < c_{kk}$. Also ist der Index

$$m = [O_K : M] = c_{11} \cdot \ldots \cdot c_{nn},$$

und

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

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

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

□

LEI.84

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

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

Es ist

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

□

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*

$$G = \left\{ \mathrm{id}_F,\ \sqrt{d}\mapsto -\sqrt{d}\ \right\}.$$

Es gilt

$$O_F = \begin{cases} \mathbb{Z}+\mathbb{Z}\sqrt{d} & ,\ d\equiv 2,3 \mod 4 \\ \mathbb{Z}+\mathbb{Z}\frac{-1+\sqrt{d}}{2},\ d\equiv 1 \mod 4 \end{cases}$$

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

$$aX^2+bX+c = 0$$

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

$$\alpha = \frac{1}{2a}\Big(-b\pm\sqrt{b^2-4ac}\Big).$$

Schreibe b^2-4ac in der Form A^2d mit $A,d\in\mathbb{Z}, d$ quadratfrei. Dann gilt offenbar

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

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

·) Die Abbildung

$$\sigma:\left\{\begin{array}{ccc} F & \longrightarrow & F \\ a+b\sqrt{d} & \mapsto & a-b\sqrt{d}. \end{array}\right.$$

ist offenbar ein Automorphismus von $F/\mathbb{Q}$, denn $\sqrt{d}$, $-\sqrt{d}$ sind Nullstellen des irreduziblen Polynoms X^2-d. Der Fixpunktkörper von

$$G=\{\mathrm{id}_F,\sigma\}$$

ist gleich $\mathbb{Q}$, also ist $F/\mathbb{Q}$ Galois mit Gruppe G. F ist der Zerfällungskörper des separablen Polynoms X^2-d.

·) Ist $\gamma\in O_F$, so ist $\mathrm{tr}^F_{\mathbb{Q}}\gamma$, $N^F_{\mathbb{Q}}(\gamma)\in\mathbb{Z}$. Da das Minimalpolynom von γ die Gestalt

$$X^2-\mathrm{tr}^F_{\mathbb{Q}}(\gamma)X+N^F_{\mathbb{Q}}(\gamma)$$

hat gilt auch die Umkehrung. Man berechnet für $\gamma=r+s\sqrt{d}$, $r,s\in\mathbb{Q}$,

$$\mathrm{tr}^F_{\mathbb{Q}}(\gamma)=2r,\ N^F_{\mathbb{Q}}(\gamma)=r^2-s^2d.$$

Es folgt

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

Sei nun $\gamma\in O_F$. 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 $d\equiv 2,3 \mod 4$. Dann gilt

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

Da

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

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

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

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

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

□

LEI.68

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

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

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

$$(\mathrm{tr}(\alpha_i\alpha_j)) = \begin{pmatrix} 2 & -1 \\ -1 & \frac{1+d}{2} \end{pmatrix},$$

also $\delta_F = d$.

□

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

2.7.3 Satz. *Sei p Primzahl. Dann gilt:*
Fall p ungerade:

(i) $p \nmid \delta_F$, *d quadratischer Rest* $\mod p \Rightarrow (p) = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$.

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

(iii) $p|\delta_F \Rightarrow (p) = \mathfrak{p}^2$.

Fall $p = 2$:

(i) $2 \nmid \delta_F$, $d \equiv 1 \mod 8 \Rightarrow (2) = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$

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

(iii) $2|\delta_F \Rightarrow (2) = \mathfrak{p}^2$

Bemerke: Ist $d \equiv 2,3 \mod 8$, so ist $\delta_F = 4d$ also $2|\delta_F$. Ist $d \equiv 0,4 \mod 8$ so ist d nicht quadratfrei.

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

$$\begin{array}{lllll} (I) & r = 2 & , & e = 1 & , \ f = 1 \\ (II) & r = 1 & , & e = 1 & , \ f = 2 \\ (III) & r = 1 & , & e = 2 & , \ f = 1 \end{array}$$

Sei $p \neq 2$.

(i): Sei $a^2 \equiv d \mod p$. Wir zeigen

$$(p) = (p)\Big(p, a+\sqrt{d},\ a-\sqrt{d},\ \frac{a^2-d}{p}\Big) = (p, a+\sqrt{d}\,)(p, a-\sqrt{d}).$$

Zum ersten $''=''$: Der zweite Faktor rechts enthält p und $2a$. Da $p, 2a$ relative prim sind ist er gleich O_F. Zum zweiten $''=''$. Es gilt:

$$p \cdot p = p \cdot p, p \cdot (a+\sqrt{d}) = (a+\sqrt{d}) \cdot p, p(a-\sqrt{d}) = p \cdot (a-\sqrt{d}),$$

$$p \cdot \frac{a^2-d}{p} = (a+\sqrt{d})(a-\sqrt{d}).$$

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

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

(iii): Wir zeigen

$$(p) = (p)(p, \sqrt{d}, \frac{d}{p}) = (p, \sqrt{d})^2.$$

Zum ersten $''=''$: Der zweite Faktor ist gleich O_F denn er enthält p und $\frac{d}{p}$ 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

$$(2) = (2)\Big(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8}\Big) = \Big(2, \frac{1+\sqrt{d}}{2}\Big)\Big(2, \frac{1-\sqrt{d}}{2}\Big).$$

Zum ersten $''=''$. Der zweite Faktor ist gleich O_F. Zum zweiten $''=''$:

$$2 \cdot 2 = 2 \cdot 2, 2\frac{1+\sqrt{d}}{2} = \frac{1+\sqrt{d}}{2} \cdot 2, 2 \cdot \frac{1-\sqrt{d}}{2} = 2 \cdot \frac{1-\sqrt{d}}{2},$$

$$2\frac{1-d}{8} = \frac{1+\sqrt{d}}{2} \cdot \frac{1-\sqrt{d}}{2}.$$

Weiters kann nicht $(2, \frac{1+\sqrt{d}}{2}), (2, \frac{1-\sqrt{d}}{2}) \subseteq \mathfrak{p}$, denn sonst $1 \in \mathfrak{P}$.
(ii): Sei $d \equiv 5 \mod 8$ (wieder ist $\delta_F = d$ also $2 \nmid \delta_F$). Sei $\mathfrak{p}|(2)$, und angenommen $f(\mathfrak{p}/(2)) = 1$. Dann existiert $a \in \mathbb{Z}$ mit $a \equiv \frac{1+\sqrt{d}}{2} \mod \mathfrak{p}$. Da $\frac{1+\sqrt{d}}{2}$ der Gleichung $X^2 - X + \frac{1-d}{4} = 0$ genügt folgt $a^2 - a + \frac{1-d}{4} \equiv 0 \mod \mathfrak{p}$ 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!.

(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

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

□

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 $u = \frac{x+\sqrt{d}\, y}{2}$ 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 $u = x + \sqrt{d}\, y \in O_F^*$ denn

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

und $u > 1$. Wähle $\mathfrak{M} > u$.

·) 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 ϵ die kleinste Einheit $1 < \epsilon < M$. Ist $\tau \in O_F^*, \tau > 0$, sei $s \in \mathbb{Z}$ sodaß $\epsilon^s \leq \tau \leq \epsilon^{s+1}$. 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 $\tau = -\epsilon^s$.

□

DEI.71

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 ζ_m Nullstelle von $X^m - 1 = 0$ und es gilt

$$X^m - 1 = (X-1)(X-\zeta_m)\cdot\ldots\cdot(X-\zeta_m^{m-1}),$$

also ist F der Zerfällungskörper des (separablen) Polynoms $X^m - 1$ und daher ist $F/\mathbb{Q}$ Galois.

LEI.72

2.7.6 Lemma. *Sei $G = \mathrm{Gal}(F/\mathbb{Q})$ für $F = \mathfrak{Q}(\zeta_m)$. Dann ist $G \cong (\mathbb{Z}/m\mathbb{Z})^*$ via $\vartheta : G \to (\mathbb{Z}/m\mathbb{Z})^*$ wobei für $\sigma \in G$ gilt $\sigma\zeta_m = \zeta_m^{\vartheta(\sigma)}$. Also ist $[F:\mathbb{Q}] = \varphi(m)$, wobei φ die Eulersche φ-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 σ^{-1} existiert und $\mathrm{id} : \zeta_m = \zeta_m^1$ folgt $\vartheta(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^*$. Wegen $F = \mathbb{Q}(\zeta_m)$ ist ϑ injektiv.

Sei f das Minimalpolynom von ζ_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 $h(\zeta_m) \equiv 0$ und damit haben f und h modulo p einen gemeinsamen Faktor. Aslo hat $X^m - 1$ modulo p mehrfache Nullstellen, ein WS!, denn $(X^m-1)' = mX^{m-1}$ hat nur die Nullstelle 0. Es folgt daß für jedes a mit $(a,m) = 1$ gilt $f(\zeta_m^p) = 0$. Damit ist ϑ surjektiv.

□

Sei $\phi_m(X) := \prod_{(a,m)=1}(X - \zeta_m^a)$. ϕ_m heißt m-tes Kreisteilungspolynom. Offenbar gilt $\prod_{d|m}\phi_d(X) = X^m - 1$.

LEI.73

2.7.7 Lemma. *Es gilt $\phi_m(X) \in \mathbb{Z}[X]$. ϕ_m ist irreduzibel.*

Beweis. Es gilt $\phi_m(X) = \prod_{\sigma\in G}(X - \sigma\zeta_m)$, also ist ϕ_m das Minimalpolynom von ζ_m über $\mathbb{Q}$. Wegen ζ_m ganz und $\mathbb{Z}$ ganz abgeschlossen gilt $\phi_m \in \mathbb{Z}[X]$.

□

LEI.74

2.7.8 Lemma. *Sei p Primzahl, $p \nmid m, \mathfrak{P} \in \mathrm{Spec}\, O_F, \mathfrak{P}/(p), \zeta := \zeta_m$. 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 $\zeta^i \not\equiv \zeta^j \mod \mathfrak{P}$ 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 $m | (p^{f(\mathfrak{P}/(p))} - 1)$.

□

LEI.77

2.7.9 Lemma. *Es gilt* $\Delta(1,\zeta,\ldots,\zeta^{\varphi(m)-1})|m^{\varphi(m)}$.

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 $N(\zeta)=\pm1$ folgt

$$\pm m^{\varphi(m)}=N\Big(\phi_m'(\zeta)\Big)N\Big(g(\zeta)\Big)=\pm\Delta\Big(1,\zeta,\ldots,\zeta^{\varphi(m)-1}\Big)N\Big(g(\zeta)\Big).$$

□

LEI.78

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* $p^n\equiv1 \mod m$, *so gilt* $w^{p^n}\equiv w \mod (p)_{O_F}$, $w\in O_F$.

(iii) $\sigma_p w\equiv w^p \mod (p)_{O_F}$, $w\in O_F$ $(\sigma_p(\zeta)=\zeta^p)$.

Beweis.
·) Sei $\Delta=\Delta(1,\zeta,\ldots,\zeta^{\varphi(m)-1})$, dann ist $p\nmid\Delta$. Sei $\Delta'\in\mathbb{Z}$ sodaß $\Delta'\Delta\equiv1 \mod p$, dann folgt für $w\in O_F$

$$w\equiv\Delta'\Delta w \mod (p)_{O_F},$$

und es ist $\Delta w\in\mathbb{Z}[\zeta]$ nach Lemma 2.6.8.

·) Sei $w\in O_F$ und schreibe $w\equiv\sum a_i\zeta^i \mod (p)$ mit gewissen $a_i\in\mathbb{Z}$. Wegen $a_i^p\equiv a_i \mod p$ folgt

$$w^p\equiv\sum a_i\zeta^{ip} \mod (p)_{O_F}$$

und daher auch $w^{p^n}\equiv\sum a_i\zeta^{ip^n}=\sum a_i\zeta^i\equiv w \mod (p)_{O_F}$.

·) Wegen $\sigma((p)_{O_F})=(p)_{O_F}$ für $\sigma\in G$ gilt $(\sigma_p(\zeta)=\zeta^p$

$$\sigma(w)\equiv\sum a_i\zeta^{ip}\equiv w^p \mod (p)_{O_F}.$$

□

2.7.11 Satz. *Sei p Primzahl, $\mathfrak{P}\in\operatorname{Spec}O_F$, $\mathfrak{P}/(p)$. Dann gilt: Ist p ungerade so ist $\mathfrak{P}$ verzweigt $(e(\mathfrak{P}/(p))>1)$ $\iff$ $p|m$. Ist $p=2$ so ist $\mathfrak{P}$ verzweigt $\iff$ $4|m$. Genauer gilt*

(i) Sei $p\nmid m$ und sei $f\in\mathbb{N}$ die kleinste Zahl mit $p^f\equiv1 \mod m$. Dann ist

$$pO_F=\mathfrak{P}_1\cdot\ldots\cdot\mathfrak{P}_r$$

mit paarweise verschiedenen $\mathfrak{P}_i$. Es ist $f(\mathfrak{P}/(p))=f$ und $r=\frac{\varphi(m)}{f}$.

(ii) Angenommen m ist prim. Sei $p = m$, dann ist (p) vollständig verzweigt, es gilt für $\mathfrak{P} := (1-\zeta_p)_{O_F} \in \operatorname{Spec} O_F$ daß $f(\mathfrak{P}/(p)) = 1$ und

$$(p)_{O_F} = \mathfrak{P}^{p-1}$$

Beweis.
·) 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 $p^n \equiv 1 \mod m$)

$$w^{p^n} \equiv w \mod pO_F \text{ und daher } \mod \mathfrak{P}^2.$$

Wegen $p^n \geq 2$ ist $w^{p^n} \in \mathfrak{P}^2$ und damit auch $w \in \mathfrak{P}^2$. WS!

(i): Klarerweise ist f die Ordnung von σ_p in G. Sei nun $f_1 = f(\mathfrak{P}/(p))$, dann gilt $|O_F/\mathfrak{P}| = p^{f_1}$ und daher ist für $w \in O_F$ stets

$$w^{p^{f_1}} \equiv w \mod \mathfrak{P},$$

und es ist f_1 die kleinste Zahl mit dieser Eigenschaft, denn $(O_F/\mathfrak{P})^*$ ist als EInheitengruppe eines endlichen Körpers zyklisch. Es folgt $f_1 | f$. Wegen Lemma 2.7.8 gilt $p^{f_1} \equiv 1 \mod m$ und daher $f | f_1$.

Also ist stets $f = f(\mathfrak{P}/(p))$. Nach obigem ist $e(\mathfrak{P}/(p)) = 1$ und es folgt

$$r = \frac{[F:\mathbb{Q}]}{ef} = \frac{\varphi(m)}{f}.$$

(ii): Es gilt $p = \prod_{i=1}^{p-1}(1-\zeta^i)$. Setze $v_i = \frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \ldots + \zeta^{i-1}$. Dann ist $v_i \in O_F^*$: Wegen $p \nmid i$ wähle $j \in \mathbb{Z}$ sodaß $ij \equiv 1 \mod p$, dann ist

$$v_i^{-1} = \frac{1-\zeta}{1-\zeta^i} = \frac{1-(\zeta^i)^j}{1-\zeta^i} = 1 + \zeta^i + \ldots + (\zeta^i)^{j-1} \in O_F.$$

Es folgt daß $p = (1-\zeta)^{p-1} \cdot \prod_{i=1}^{p-1} v_i$, und damit

$$(p)_{O_F} = (1-\zeta)_{O_F}^{p-1} = \mathfrak{P}^{p-1}.$$

Wegen $efr = \varphi(p) = p-1$ muß $\mathfrak{P}$ schon prim sein und $e(\mathfrak{P}/(p)) = p-1$, $f(\mathfrak{P}/(p)) = 1$ gelten.

·) Sei p ungerade, $p|m$. Dann ist $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_m)$. Seien O_p und O_m die entsprechenden Ringe ganzer Zahlen. Es gilt

$$pO_p = (1-\zeta_p)_{O_p}^{p-1}.$$

Schreibe $(1-\zeta_p)_{O_m} = \mathfrak{P}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{P}_r^{\alpha_r}$ mit $\mathfrak{P}_i \in \operatorname{Spec} O_m, \alpha_i \geq 1$. Dann ist also

$$pO_m = (\mathfrak{P}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{P}_r^{\alpha_r})^{p-1}$$

und also $e(\mathfrak{P}_i/(p)) = \alpha_i(p-1) \geq p-1 > 1$. Da jedes Primideal das über p liegt auftreten muß ist also jedes verzweigt.

·) Sei $p = 2$, $2|m$, $4 \nmid m$. Schreibe $m = 2m_0$ mit m_0 ungerade. Dann ist $-\zeta_{m_0}$ eine primitive m_0-te Einheitswurzel, also

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m_0}).$$

Da $2 \nmid m_0$ ist $\mathfrak{P}/(2)$ in O_{m_0} unverzweigt.

·) Sei $p = 2$, $4|m$. Dann ist $i \in \mathfrak{Q}(\zeta_m)$ und klarerweise ist $i \in O_F^*$. Wegen $(1-i)^2 = (-i)2$ folgt

$$(2)_{O_F} = (1-i)^2_{O_F}$$

und es folgt wie oben das alle $\mathfrak{P}/(2)$ verzweigt sind.

□

COI.80

2.7.12 Korollar. *Sei $\mathfrak{P}/(p)$, $p \nmid m$. 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 σ_p also $f = |\langle \sigma_p \rangle|$.

□

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

$$\operatorname{tr} \zeta^j = -1, \ m \nmid j.$$

Also ist $(s = 0, \ldots, m-2)$

$$\operatorname{tr}(\alpha\zeta^{-s}) = \operatorname{tr}(a_0\zeta^{-s} + \ldots + a_s + \ldots + a_{m-2}\zeta^{m-2-s}) =$$

$$= -a_0 - \ldots - a_{s-1} + (m-1)a_s - a_{s+1} - \ldots - a_{m-2},$$

und daher

$$\operatorname{tr}(\alpha\zeta^{-s} - \alpha\zeta) = ma_s.$$

Wegen $\alpha\zeta^{-s} - \alpha\zeta \in O_F$ folgt $ma_s \in \mathbb{Z}$.

·) Sei $\lambda := 1 - \zeta$, dann gilt $(m)_{O_F} = (\lambda)^{m-1}_{O_F}$. Schreibe

$$m\alpha = b_0 + b_1\lambda + \ldots + b_{m-2}\lambda^{m-2}, b_i \in \mathbb{Z}.$$

Wegen $m\alpha \in (m)_{O_F} \subseteq (\lambda)_{O_F}$ folgt $\lambda | b_0$ in O_F. Wegen $m = \lambda^{m-1}u$ für ein $u \in O_F^*$ 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 $m\alpha \in (m)_{O_F} \subseteq (\lambda^2)_{O_F}$ auch

$$\lambda^2 | b_1\lambda \text{ in } O_F,$$

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 $K = \mathbb{Q}(\sqrt[3]{2})$. Dieser ist nicht Galois, die Homomorphismen von $K/\mathbb{Q}$ sind gegeben durch

$$\begin{array}{rcccc} \mathrm{id} & : & \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ \sigma_1 & : & \sqrt[3]{2} & \mapsto & \zeta_3 \sqrt[3]{2} \\ \sigma_2 & : & \sqrt[3]{2} & \mapsto & \zeta_3^2 \sqrt[3]{2} \end{array}$$

wobei $\zeta_3 = e^{\frac{2\pi i}{3}}$.

Wir wollen zunächst (für allg. $\mathbb{Q}(\sqrt[3]{m})$ siehe [N,narkiewicz]) O_K bestimmen. Dazu brauchen wir ein Lemma.

LEI.85

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 $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ gilt*

$$p|a_i,\ i = 0, \ldots, n-1,\ p^2 \nmid a_0.$$

Dann ist der Index $[O_K : (\mathbb{Z} + \mathbb{Z}a + \ldots + \mathbb{Z}a^{n-1})]$ nicht durch p teilbar.

Beweis. Wegen $a^n = -(a_{n-1}a^{n-1} + \ldots + a_0)$ und $p|a_i$ ist $\frac{a^n}{p} \in O_K$. Weiters ist $N_{\mathbb{Q}}^K(a) = a_0$ nicht durch p^2 teilbar.

Setze $M = \mathbb{Z} + \mathbb{Z}a + \ldots + \mathbb{Z}a^{n-1}$, $m = [O_K : M]$. Angenommen $p|m$. Dann existiert ein Element $\xi \in O_K$ sodaß

$$\xi \notin M,\ p\xi \in M.$$

Denn $O_{K/M}$ ist eine abelsche Gruppe der Ordnung m, und wegen $p|m$ existiert ein Element mit Ordnung p. Dann ist also $\xi = (b_0 + b_1 a + \ldots + b_{n-1}a^{n-1})\frac{1}{p}$ mit gewissen $b_i \in \mathbb{Z}$ sodaß nicht alle b_i durch p teilbar sind. Sei j minimal sodaß $p \nmid b_j$, und betrachte

$$\eta := (b_j a^j + \ldots + b_{n-1}a^{n-1})\frac{1}{p} =$$

$$= \xi - (\frac{b_0}{p} + \frac{b_1}{p}\, a + \ldots + \frac{b_{j-1}}{p}\, a^{j-1}) \in O_K.$$

Es folgt

$$\zeta := b_j a^{n-1}\frac{1}{p} = \eta a^{n-j-1} - \frac{a^n}{p}\Big(b_{j+1} + b_{j+2}a + \ldots + b_{n-1}a^{n-j-2}\Big) \in O_K.$$

Es folgt

$$N(\zeta) = b_j^n N(a)^{n-1}\frac{1}{p^n} \in \mathbb{Z}.$$

Da $p^2 \nmid N(a)$ folgt $p|b_j^n$ und damit $p|b_j$ WS!.

□

2.7.15 Satz. *Sei $K = \mathfrak{Q}(\sqrt[3]{2})$. Dann gilt*

$$O_K = \mathbb{Z}[\sqrt[3]{2}]$$

Beweis. Setze $\alpha = \sqrt[3]{2}$. Das Minimalpolynom ist $f(X) = X^3 - 2$. Wegen Satz 2.6.5 gilt

$$\Delta(1, \alpha, \alpha^2) = (-1)^3 N(3\sqrt[3]{4}) = 3^3 \cdot 2^2.$$

Sei $m = \left[O_K : \mathbb{Z}[\alpha]\right]$. Dann gilt wegen Satz 2.6.10

$$\pm 3^3\ 2^2 = m^2 \delta_K \qquad (2.1, *)$$

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 $m = \left[O_K : \mathbb{Z}[\alpha]\right] = \left[O_K : \mathbb{Z}[\beta]\right]$ 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. Sezte $A_n := a_1 + \ldots + a_n$, $B_n := b_1 + \ldots + b_n$. Dann gilt

$$\sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n \Big(b_n - b_{n+1} \Big)$$

Eine Dirichlet-Reihe ist eine Reihe der Gestalt

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},\ s \in \mathbb{C},$$

wobei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen ist. Schreibe im folgenden $s = \sigma + it$ mit $\sigma_1 t \in \mathbb{R}$.

LEII.1

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 $\operatorname{Re} s > \operatorname{Re} s_0$, 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

$$\sum_{k=m+1}^{n} \frac{a_k}{n^{s_0}} = \frac{P_n(s_0)}{n^{s-s_0}} - \frac{P_m(s_0)}{m^{s-s_0}} +$$

$$+ \sum_{k=m+1}^{n} P_k(s_0) \Big[\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \Big] = (*)$$

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 $|P_k(s_0)| \le M$, $k \in \mathbb{N}$. Dann ist

$$\Big|(*)\Big| \le \frac{M}{n^{s-s_0}} + \frac{M}{m^{s-s_0}} + M(s-s_0)\int_{m+1}^{n+1} \frac{1}{x^{s-s_0+1}}\,dx \le$$

$$\le M\Big(\frac{1}{n^{s-s_0}} + \frac{1}{m^{s-s_0}} + \frac{s-s_0}{(m+1)^{s-s_0}}\Big)$$

und dieser Ausdruck strebt für $m,n \to \infty$ gegen 0 und zwar gleichmäßig auf jedem Kompaktum in $\{\sigma > \sigma_0\}$.

□

Die Zahl

$$\sigma_0 := \inf\Big\{\sigma \in \mathbb{R} : \sum \frac{a_n}{n^s} \text{ konvergiert}\Big\}$$

heißt Konvergenzabzisse von $\sum \frac{a_n}{n^s}$.

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 $\{\mathrm{Re}(s) \ge \sigma_1 + 1 + \delta\}$ absolut und gleichmäßig konvergiert. Denn vergleiche mit $\sum \frac{1}{n^{1+\delta}}$.

LEII.2

3.1.2 Lemma. *Sei $\sigma_1 \ge 0$ und sei $A_n = a_1 + \ldots + a_n = O(n^{\sigma_1})$. Dann ist die Konvergenzabszisse von $\sum \frac{a_n}{n^s}$ stets $\le \sigma_1$.*

Beweis. Sei $|A_n| \le Cn^{\sigma_1}$, sei $\delta > 0$ und $\sigma \ge \sigma_1 + \delta$, sei $P_n(s) = \sum_{k=1}^n \frac{a_k}{k^s}$. Dann gilt

$$P_n(s) - P_M(s) = \frac{A_n}{n^s} - \frac{A_m}{m^s} + \sum_{n=m+1}^{n-1} A_k\Big[\frac{1}{k^s} - \frac{1}{(k+1)^s}\Big] =$$

$$= \frac{A_n}{n^s} - \frac{A_m}{m^s} + \sum_{k=m+1}^{n-1} A_k s \int_k^{k+1} \frac{1}{x^{s+1}}\,dx.$$

Also folgt

$$\Big|P_n(s) - P_m(s)\Big| \le \frac{C}{n^{\sigma-\sigma_1}} + \frac{C}{m^{\sigma-\sigma_1}} + C|s|\int_{m+1}^{\infty} \frac{1}{x^{\sigma+1}}\,dx \le$$

$$\le C\Big(\frac{1}{n^\delta} + \frac{1}{m^\delta} + |s|\frac{1}{(m+1)^\delta}\Big) \to 0,\ m,n \to \infty.$$

□

DEII.3

3.1.3 Definition. Die Riemannsche Zetafunktion ist definiert als die Reihe

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Die Funktion $\zeta(s)$ ist analytisch auf $\{\operatorname{Re} s > 1\}$, denn setze in Lemma 3.1.2 $\sigma_1 = 1$. Weiters 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

$$1 \leq (s-1)\zeta(s) \leq s, \ s > 1. \qquad (3.1,+)$$

3.1.4 Satz. *Die Funktion $\zeta(s)$ ist analytisch auf $\{Res > 0\}$ 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 ζ_2 analytisch auf $\{\operatorname{Re} s > 0\}$. Nun gilt

$$2 \cdot \frac{\zeta(s)}{2^s} + \zeta_2(s) = \zeta(s),$$

also $\zeta(s)(1 - \frac{1}{2^{s-1}}) = \zeta_2(s)$. Daher hat ζ eine analytische Fortsetzung auf $\{\operatorname{Re} s > 0\}$ mit möglicher Ausnahme der Punkte s mit $2^{s-1} = 1$, das sind

$$s = 1 + \frac{2\pi n}{\log 2}\, i, n \in \mathbb{Z}.$$

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 ζ_r analytisch für $\operatorname{Re} s > 0$. Es gilt

$$\zeta_r(s) = \Big(1 - \frac{1}{r^{s-1}}\Big)\zeta(s),$$

also ist ζ analytisch auf $\{\operatorname{Re} s > 0\}$ mit möglicher Ausnahme von

$$s = 1 + \frac{2\pi n}{\log r}\, i, n \in \mathbb{Z}.$$

Es bleibt nur $s = 1$ als Pol möglich, denn wäre z.B.

$$1 + \frac{2\pi m}{\log 3} i = 1 + \frac{2\pi n}{\log 2} i,$$

so wäre $3^n = 2^m$, ein WS!.

□

COII.5

3.1.5 Korollar. *Sei* $(a_n)_{n\in\mathbb{N}}$, $A_n = a_1 + \ldots + a_n$, $0 \le \sigma_1 < 1$, $\rho \in \mathbb{C}$. *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 $\{\operatorname{Re} s > 0\}$ *mit Ausnahme von* $s = 1$ *wo ein einfacher Pol mit Residuum* ρ *liegt.*

Beweis. Wende Lemma 3.1.2 und Satz 3.1.4 an auf $f(s) - \rho\zeta(s)$. □

3.2 Definition von ζ_k

Wir schreiben im folgenden $f \sim g$ wenn sich f und g nur um eine analytische Funktion unterscheiden.

LEII.6

3.2.1 Lemma. *Es gilt*

(i) (Eulersche Produktdarstellung)

$$\zeta(s) = \prod_{p \ PZ} \frac{1}{1 - \frac{1}{p^s}}, \ \operatorname{Re} s > 1.$$

(ii)

$$\log \zeta(s) = \sum_{p \ PZ, m\ge 1} \frac{1}{m p^{m s}}.$$

(iii)

$$\log \zeta(s) \sim \sum_{p \ PZ} \frac{1}{p^s} \sim \log \frac{1}{s-1}.$$

Beweis. Betrachte die Reihe

$$R = \sum_{p \ \mathrm{PZ}} \sum_{m\ge 1} \frac{1}{m p^{m s}}.$$

Es gilt für $\sigma > 1$

$$\sum_{p \ \mathrm{PZ}} \sum_{m\ge 1} \left| \frac{1}{m p^{m s}} \right| = \sum_{p \ \mathrm{PZ}} \sum_{m\ge 1} \frac{1}{m p^{m\sigma}} = -\sum_{p \ \mathrm{PZ}} \log\left(1 - \frac{1}{p^\sigma}\right)$$

Wegen $\lim_{p\to\infty} \frac{1}{p^\sigma} = 0$ und $\lim_{x\to 0} \frac{\log(1-x)}{x} = -1$. Ist diese Reihe mit $\sum_{p \ \mathrm{PZ}} \frac{1}{p^\sigma}$ konvergent ($\sigma > 1$). Man darf in R also die Summationsreihenfolge austauschen sowie beliebig anordnen. Wegen der absoluten Konvergenz von $\sum_p \log(1 - \frac{1}{p^s})$

folgt das das Euler-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

$$\log \zeta(s) = -\sum_p \log\Big(1-\frac{1}{p^s}\Big) = \sum_{p \text{ PZ}, m\geq 1} \frac{1}{mp^{ms}}.$$

Klarerweise ist $\log\zeta(s) \sim \log\frac{1}{s-1}$. Beachte, daß

$$\sum_{p \text{ PZ}, m\geq 2} \Big|\frac{1}{mp^{sm}}\Big| = \sum_{p \text{ PZ}} \sum_{m\geq 2} \frac{1}{mp^{\sigma m}} = -\sum_{p \text{ PZ}} \Big(\log(1-\frac{1}{p^\sigma}) + \frac{1}{p^\sigma}\Big).$$

Wegen

$$\lim_{x\to 0} \frac{\log(1-x)+x}{x^2} = -\frac{1}{2}$$

ist diese Reihe vergleichbar mit $\sum_{p \text{ PZ}} \frac{1}{(p^\sigma)^2}$ und daher konvergent für $\sigma > \frac{1}{2}$ und dort analytisch. Es ist

$$\log\zeta(s) = \sum_p \frac{1}{p^s} + \sum_{p,m\geq 2} \frac{1}{mp^{sm}}$$

□

Sei nun $k \neq \mathbb{Q}$ ein algebraischer Zahlkörper, $[k:\mathbb{R}] = N$. Es ist für ein $\mathfrak{p} \in \operatorname{Spec} O_k$, $\mathfrak{p}/(p)$,

$$N_{\mathbb{Q}}^k(\mathfrak{p}) = \big(p^{f(\mathfrak{p}/(p))}\big)_{\mathbb{Z}} = \big(N\mathfrak{p}\big)_{\mathbb{Z}}$$

wo $N\mathfrak{p} = |O_k/\mathfrak{p}| = p^{f(\mathfrak{p}/(p))}$ ist.

DEII.7

3.2.2 Definition. Die Dedekindsche Zetafunktion des algebraischen Zahlkörpers k ist

$$\zeta_k(s) := \prod_{\mathfrak{p}\in\operatorname{Spec} O_k} \frac{1}{1-\frac{1}{N\mathfrak{p}^s}}.$$

LEII.8

3.2.3 Lemma. *ζ_k ist analytisch für $\sigma > 1$. Es gilt*

(i)

$$\zeta_k(s) = \sum_{\mathfrak{a}\triangle O_k} \frac{1}{N\mathfrak{a}^s}$$

(ii)

$$\log\zeta_k(s) = \sum_{\mathfrak{p},m\geq 1} \frac{1}{mN\mathfrak{p}^{ms}}$$

(iii)

$$\log\zeta_k(s) \sim \sum_{\mathfrak{p}:f_{\mathfrak{p}}=1} \frac{1}{N\mathfrak{p}^s}.$$

Beweis. Es gilt $\sum_{\mathfrak{p}/(p)} f_{\mathfrak{p}} \leq N$, also gibt es höchstens N viele $\mathfrak{p}/(p)$ und es folgt

$$\sum_{\mathfrak{p},m\geq 1} \left|\frac{1}{mN\mathfrak{p}^{ms}}\right| \geq \sum_{p \text{ PZ},m\geq 1} \frac{N}{mp^{m\sigma}} < \infty, \sigma > 1.$$

Es ist

$$\sum_{\mathfrak{p}} \log\left(1 - \frac{1}{N\mathfrak{p}^s}\right) \text{ vgl. } \sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^\sigma} \leq \sum_{p \text{ PZ}} \frac{N}{p^\sigma}$$

absolut konvergent, und damit auch das Produkt in der Definition von ζ_k und stellt eine in $\{\operatorname{Re} s > 1\}$ analytische Funktion dar. Weiters ist

$$\log \zeta_k(s) = -\sum_{\mathfrak{p}} \log\left(1 - \frac{1}{N\mathfrak{p}^s}\right) = \sum_{\mathfrak{p},m\geq 1} \frac{1}{mN\mathfrak{p}^{ms}}.$$

Die Reihe

$$\sum_{(f_{\mathfrak{p}}>1)\vee(m\geq 2)} \frac{1}{mN\mathfrak{p}^{m\sigma}} = R$$

vergleicht man mit $\sum_{p \text{ PZ},m\geq 2} \frac{N}{mp^{m\sigma}} + \sum_{f_{\mathfrak{p}}>1} \frac{1}{N\mathfrak{p}^\sigma}$ und die zweite Reihe ist $\leq \sum_{p \text{ PZ}} \frac{N}{p^{2\sigma}}$. Also ist $\mathfrak{R}$ konvergent für $\sigma > \frac{1}{2}$.

□

Literaturverzeichnis

[BIV,brueske.etal] R.Brüske, F.Ischebeck, F.Vogel: *Kommutative Algebra,*
BI, 1989.

[IR,ireland.rosen] K.Ireland, M.Rosen: *A Classical Introduction to Modern Number Theory,*
GTM 84, Springer Verlag, 1990.

[L1,lang] S.Lang: *Algebraic Number Theory,*
GTM 110, Springer Verlag, 1986 .

[L2,lang/algebra] S.Lang: *Algebra,*
GTM 211, Springer Verlag, ???.

[N,narkiewicz] W.Narkiewicz: *Elementary and Analytic Theory of Algebraic Numbers,*
???.

[RV,ramakrishnan.valenza] D.Ramakrishnan, R.Valenza: *Fourier Analysis on Number Fields,*
GTM 186, Springer Verlag, 1999.

[S,stichtenoth] H.Stichtenoth: *Algebraic Function Fields and Codes,*
Springer Verlag, 1993.

[vdW,vdw] B.L.van der Waerden: *Algebra I/II,*
Heidelberger Taschenbücher 12/23, Springer Verlag, 1971/67.

[W,weil] A.Weil: *Basic Number Theory,*
Springer Verlag, 1967.