Zahlentheorie
Sommersemester 2004

Prof. Dr. Annette Huber-Klawitter

Fassung vom 14. Juli 2004

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Augustusplatz 10/11
04109 Leipzig

0341-97 32 185
huber@mathematik.uni-leipzig.de

Kapitel 0

Einleitung

Zahlentheorie beschäftigt sich mit Eigenschaften von Zahlen, d.h. Elementen von $\mathbb{Z}$. Damit ist sie eine der ältesten Wissenschaften überhaupt - die Königin der Mathematik. Wir wissen sehr viel, sehr vieles aber auch nicht. Unter

`http://www.ams.org/mathscinet`

finden Sie die "Mathematical Reviews", in denen alle wissenschaftlichen Arbeiten der Mathematik besprochen werden. Unter "MSC Primary" 11 sind die Arbeiten zur Zahlentheorie zu finden. Eine genauere Untergliederung können Sie nachlesen, wenn Sie den Link "Browse by MSC" und dann "2000 Mathematical Subject Classification" folgen.
Heute sollen einige Teilgebiete der Zahlentheorie vorgestellt werden.

Elementare Zahlentheorie

Es werden nur die Mittel der Mittelstufe verwendet, d.h. Mathematik bis zum 17. Jahrhundert. Zum Beispiel:

Satz 0.1. *Eine ganze Zahl ist durch* 3 *teilbar genau dann, wenn ihre Quersumme durch* 3 *teilbar ist.*

Beweis: Sei $n = \sum_{n=0}^{m} a_i 10^i$ mit $0 \leq a_i \leq 10$. Wegen $10 \equiv 1 \mod 10$ folgt $n \equiv \sum_{n=0}^{m} a_i \mod 3$. □

Aber Vorsicht: elementar heißt nicht unbedingt einfach!

Übungsaufgabe (Fermat). *Jede natürliche Zahl ist Summe von vier Quadraten. (*0 *ist als Summand zugelassen).*

Literatur: W. Scharlau, H. Opolka, Von Fermat bis Minkowski, Springer Verlag.

Analytische Zahlentheorie

Zahlentheoretische Information wird in Reihen kodiert und analytisch weiterverarbeitet.

Satz 0.2. *Es gibt unendlich viele Primzahlen.*

Beweis: Sei $\zeta(s) = \sum_{n\geq 1} 1/n^s$ die Riemannsche ζ-Funktion.

Behauptung. *$\zeta(s)$ konvergiert absolut und gleichmäßig in* $\mathrm{Re}\, s \geq \sigma > 1$.

$s = u + iv$ mit $u, v \in \mathbb{R}$.

$$|n^{-s}| = |n^{-u}||n^{-iv}| = n^{-u}|\mathrm{e}^{-iv\log n}| = n^{-u}$$

Für $u \geq \sigma$ folgt

$$\sum |n^{-s}| = \sum n^{-u} \leq \sum n^{\sigma} < \infty$$

Behauptung.

$$\zeta(s) = \prod_{p\ prim} \frac{1}{1-p^{-s}}$$

Summenformel für die geometrische Reihe:

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \ldots$$

Beim Ausmultiplizieren kommt jeder Term

$$n^{-s} = (p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k})^{-s}$$

genau einmal vor. Sorgfältigeres Hinsehen zeigt auch die Grenzwertaussage, siehe: Hardy, Wright: An introduction to the Theory of Numbers, Theorem 280. Damit können wir nun den Satz beweisen. Gäbe es nur endliche viele Primzahlen, so wäre

$$\lim_{s\to 1} \prod_p \frac{1}{1-p^{-s}} = \prod_p \frac{1}{1-p^{-1}} \leq \infty$$

Der Grenzwert $\lim_{s\to 1} \zeta(s)$ existiert jedoch nicht (harmonische Reihe). □

Durch genaueres Studium der ζ-Funktion wurde das große Ergebnis der analytischen Zahlentheorie bewiesen.

Theorem 0.3 (Primzahlsatz). *Sei $\pi(x)$ die Anzahl der Primzahlen kleiner gleich x. Dann gilt*

$$\pi(x) \sim \frac{x}{\log x}$$

(d.h. der Quotient geht gegen 1).

Diese Aussage wurde von Gauß ca 1792 vermutet. Der erste Beweis stammt von Hadamard und de la Vallée Poussin (unabhängig) 1896. Ein sehr einfacher Beweis stammt von Newman, vergleiche
D. Zagier, Newman's short proof of the prime number theorem, American Math. Monthly 104 (97) 705-708.
Wir werden hoffentlich später Zeit für diesen Beweis haben.

Vermutung 0.4 (Riemannsche Vermutung). *Die Nullstellen von $\zeta(s)$ in $\mathbb{C}$ sind $-2n$ für $n \in \mathbb{N}$ oder haben* $\mathrm{Re}\, s = 1/2$.

Dies hat Folgen für den Fehlerterm im Primzahlsatz.

Algebraische Zahltheorie

Satz 0.5 (Euler). *Die Gleichung $x^3+y^3 = z^3$ hat keine Lösung in natürlichen Zahlen.*

Ansatz:

$$x^3 = z^3 - y^3 = (z-y)(z-\varrho y)(z-\varrho^2 y)$$

wobei $\varrho = \mathrm{e}^{2\pi i/3}$ eine dritte Einheitswurzel ist. Allgemeiner:

$$Z^3 - y^3 = (Z-y)(Z-\varrho y)(Z-\varrho^2 y) \in \mathbb{C}[Z]$$

da die Nullstellen übereinstimmen. Sei nun $K = \mathbb{Q}(\varrho)$, $R = \mathbb{Z}[\varrho]$. Die Körpererweiterung $K/\mathbb{Q}$ ist quadratisch, denn das Minimalpolynom von ϱ ist Z^2+Z+1. Es gilt

$$R = \{a + b\varrho \mid a, b \in \mathbb{Z}\}\ .$$

Übungsaufgabe. *R ist ein Hauptidealring.*

Tipp: $N : K \to \mathbb{Q}$ mit

$$a + b\varrho \mapsto (a+b\varrho)(a+b\varrho^2) = |a+b\varrho|^2 = a^2 - ab - b^2$$

kann anstelle des Absolutbetrages benutzt werden, um einen euklidischen Algorithmus in R zu etablieren. Es gilt:

(i) $N(\alpha\beta) = N(\alpha)N(\beta)$

(ii) $\alpha = a + b\varrho \in R$ ist eine Einheit genau dann, wenn $N(\alpha) = 1$,

(iii) $\alpha \in R$ mit $N(\alpha)$ eine Primzahl in $\mathbb{Z} \Rightarrow \alpha$ Primzahl in R.

$\lambda = 1 - \varrho$ hat die Norm $1+1+1 = 3$, also ist dies eine Primzahl.
Man beweist allgemeiner:

Satz 0.6. *Die Gleichung $x^3 + y1^3 + \lambda^{3n} z^3 = 0$ hat in R keine Lösungen mit $xyz \neq 0$.*

Beweis: Geschickte Teilbarkeitsargumente in R modulo λ, vergl. Hardy-Wright, Kapitel 13.4. □

Leider funktioniert diesselbe Idee nicht für

$$x^p + y^p = z^p$$

(p Primzahl), da $\mathbb{Z}[\zeta_p]$ mit $\zeta_p = \mathrm{e}^{2\pi i/p}$ im Allgemeinen kein Hauptidealring ist. Dennoch: Um Eigenschaften von $\mathbb{Z}$ zu studieren, lohnt es sich, endliche Erweiterungen von $\mathbb{Q}$ zu studieren. Diese *Zahlkörper* sind der Hauptgegenstand dieser Vorlesung.
Literatur:

(i) P. Samuel, Algebraic Theory of Numbers

(ii) S. Lang, Algebraic Number Theory

(iii) J. Neukirch, Algebraic Number Theory

(iv) A. Leutbecher, Zahlentheorie - eine Einführung in die Algebra

Arithmetische Geometrie

In diesem Gebiet findet ein großer Teil der aktuellen Forschung der Zahlentheorie statt.
Gleichungen wie $x^p + y^p = z^p$ definieren eine Punktmenge in $\mathbb{R}^3$ oder $\mathbb{C}^3$. Dies ist ein Beispiel für eine algebraische Varietät. Sie können nun mit geometrischen Methoden studiert werden.

Theorem 0.7 (Mordell Vermutung, Faltings 1983). *Sei C eine algebraische Kurve vom Geschlecht größer gleich 2 über $\mathbb{Q}$. Dann hat C nur endliche viele Punkte über jedem Zahlkörper.*

Beispiel. Für $n > 4$ definiert die Gleichung $X^n + Y^n = 1$ eine Kurve vom Geschlecht größer gleich 1. Also hat die Gleichung nur endlich viele rationale Lösungen, d.h. die Fermatgleichung hat nur endlich viele ganzzahlige Lösungen.

Theorem 0.8 (Wiles 1994). *$x^n + y^n = z^n$ hat nur die trivialen Lösungen.*

Wiles benutzt die Methoden der arithmetischen Geometrie, insbesondere Geometrie von Modulformen. Der Beweis ist anspruchsvoll. Unsere algebrasiche Zahlentheorie ist hierfür das Einmaleins.

Kapitel 1

Zahlkörper und Zahlringe

Definition 1.1. *Ein Körper K der Charakteristik Null mit $[K:\mathbb{Q}] < \infty$ heißt* Zahlkörper. *Der* Ganzheitsring *von K ist*

$$\mathcal{O} = \{\alpha \in K \mid es\ gibt n \in \mathbb{N}, a_1, \ldots, a_n \in \mathbb{Z}, \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0\}$$

Ringe von dieser Form heißen Zahlringe

Entscheidend ist hierbei der Koeffizient 1 vor α^n!

Bemerkung. Fast alles, was wir in diesem Semester entwickeln, funktioniert genauso auch für endliche Erweiterungen von $\mathbb{F}_p(X)$, die sogenannten *Funktionenkörper*. Beide Klassen fasst man als *globale Körper* zusammen. Der Ring $\mathbb{F}_p[X]$ übernimmt die Rolle von $\mathbb{Z}$ in der Definition des Ganzheitsrings. Entscheidend ist, dass beides Hauptidealringe sind.

Beispiel. Sei $K/\mathbb{Q}$ quadratisch, d.h. $[K:\mathbb{Q}] = 2 \Rightarrow K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ keine Quadratzahl.

Satz 1.2. *Sei $K = \mathbb{Q}(\sqrt{d})$, d quadratfrei (d.h. kein doppelter Faktor in der Primfaktorzerlegung). Dann gilt:*

(i) Für $d \equiv 2, 3 \mod 4$ ist $\mathcal{O} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$,

(ii) Für $d \equiv 1 \mod 4$ ist $\mathcal{O} = \{1/2(u + v\sqrt{d}) \mid u, v \in \mathbb{Z}, u \equiv v \mod 2\}$.

Beweis: Es ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Sei $\alpha = a + b\sqrt{d} \in \mathcal{O}$, d.h. Nullstelle von

$$P(X) = X^n + a_1X^{n-1} + \cdots + a_n = 0,\ a_i \in \mathbb{Z}\ .$$

Dann ist auch $\sigma(\alpha)$ eine Nullstelle von $P(X)$. Das Polynom

$$\begin{aligned} Q(\alpha) = (X - \alpha)(X - \sigma(\alpha)) &= X^2 - (\alpha + \sigma\alpha)X + \alpha\sigma\alpha \\ &= X^2 - (a + b\sqrt{d} + a - b\sqrt{d})X + (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= X^2 - 2aX + (a^2 - b^2d \in \mathbb{Q}[X] \end{aligned}$$

muss also $P(X)$ teilen. Nach dem Gauß-Lemma hat Q also ganze Koeffizienten (z.B. Bosch, 2.7 Kor.6). Es gilt also

$$2a, a^2 - b^2 d \in \mathbb{Z} \Rightarrow (2a)^2 - (2b)^2 d \in \mathbb{Z} \Rightarrow (2b^2)d \in \mathbb{Z} \ .$$

Wäre $2b \notin \mathbb{Z}$, so müssten sich die Primfaktoren des Nenners gegen Faktoren von d wegheben. Wegen $(2b)^2$ müsste der Faktor sogar doppelt in d vorkommen. Dies ist ein Widerspruch zur Wahl von d. Also:

$$\begin{gathered} a = \frac{u}{2}, b = \frac{v}{2} \text{ mit } u, v \in \mathbb{Z} \\ \Rightarrow \left(\frac{u}{2}\right)^2 - \left(\frac{v}{2}\right)^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z} \\ \Leftrightarrow 4 \mid u^2 - v^2 d \end{gathered}$$

Die Quadrate u^2 und v^2 können nur 0 oder 1 modulo 4 sein. Für $u^2 - v^2 d$ ergeben sich daher unterschiedliche Möglichkeiten je nach Restklasse von d. Man überprüft tabellarisch, dass für $d \equiv 2, 3$ nur $u^2 \equiv v^{\equiv} 0 \mod 4$ in Frage kommt, also beide gerade. Für $d \equiv 1$ ist $u^2 \equiv v^2 = 1 \mod 4$ ebenfalls möglich, also beide ungerade. □

Übungsaufgabe. *Sei ζ_N eine primitive N-te Einheitswurzel. Der Ganzheitsring von $\mathbb{Q}(\zeta_N)$ ist $\mathbb{Z}[\zeta_N]$.*

In diesem Beispiel sieht man, dass $\mathcal{O}$ ein Ring ist. Für den allgemeinen Fall holen wir weiter aus.

Satz 1.3. *Seien $A \subset R$ Ringe, $x \in R$. Dann sind äquivalent:*

(i) Es gibt $a_1, \ldots, a_n \in A$ mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.

(ii) $A[x] = \{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0, a_i \in A\}$ ist ein endlich erzeugter A-Modul.

(iii) Es gibt einen Teilring $B \subset R$, der A und x enthält und der endlich erzeugter A-Modul ist.

Beispiel. Seien speziell $A \subset R$ Körper. Dann bedeuten die Bedingungen:

(i) x ist algebraisch über A.

(ii) $A[x]$ ist ein endlich dimensionaler A-Vektorraum.

(iii) $A, \{x\} \subset B$ und B ist ein endlich dimensionaler A-Vektorraum.

In dieser Form ist der Satz aus der Algebra bekannt. Der Beweis bleibt derselbe.

Beweis: $(i) \Rightarrow (ii)$: Sei $M \subset R$ der A-Modul, der von $1, x, \ldots, x^{n-1}$ erzeugt wird. Nach Vorraussetzung gilt

$$x^n = -a_1 x^{n-1} - \cdots - a_n \in M$$

Rekursiv erhält man also $x^{n+j} \in M$ für alle j. Es folgt $A[x] \subset M$. Die umgekehrte Inklusion ist klar. Insbesondere ist $A[x]$ endlich erzeugt.
$(ii) \Rightarrow (iii)$: Wähle $B = A[x]$.
$(iii) \Rightarrow (i)$: B werde von $y_1, \ldots, y_n$ also A-Modul erzeugt. Wegen $x \in B$ gilt $xy_i \in B$. Es gibt also Koeffizienten $a_{ij} \in A$ mit

$$xy_i = \sum_j a_{ij} y_j$$

Dies kann als ein lineares Gleichungssystem für die y_j gelesen werden. Sei d die Determinante der Koeffizientenmatrix, also das charakteristische Polynom von $(a_i j)$. Die Spalten der Koeffizientenmatrix sind linear abhängig. Nach Lemma 1.4 folgt $y_i d = 0$ für $i = 1, \ldots, n$. Da B von den y_i erzeugt wird, folgt $bd = 0$ für alle $b \in B$, insbesondere auch $1d = 0$. Das charakteristische Polynom ist die gesuchte Polynomialgleichung für x. □

Lemma 1.4. *Sei R ein Ring, B eine quadratische Matrix mit Koeffiziente in B. Wenn das Gleichungssystem $By = 0$ eine nichttriviale Lösung $(\lambda_1, \ldots, \lambda_n)$ hat, so folgt $\lambda_i \det B = 0$ für alle i.*

Beweis: Falls R nullteilerfrei ist, kann die Rechnung im Quotientenkörper erfolgen. Die Aussagen über die Determinanten folgen dann aus der linearen Algebra. Für den allgmeinen Fall gehen wir die Beweise durch: Die Determinante wird durch die Leibniz-Formel definiert. Sie ist multilinear und alternierend in den Zeilen und Spalten. Insbesondere bleibt sie unverändert, wenn man ein Vielfaches einer Spalte zu einer anderen addiert. Wir multiplizieren also die Spalte i mit λ_i (dies mutlipliziert die Determinante mit λ_i und addieren dann das λ_j-fache der Spalte j für alle $j \neq i$. In der neuen Matrix verschwindet die i-te Spale, also auch die Determinante. □

Definition 1.5. *Ein Element $x \in R$, welches eine der äquivalenten Bedingungen erfüllt, heißt* ganz über A. *R heißt* ganze Erweiterung von A, *wenn alle Elemente von R ganz sind. Die Menge*

$$B = \{x \in R \mid x \text{ ist ganz über } A\}$$

heißt ganzer Abschluss *von A in R.*

Beispiel. $\mathcal{O}$ ist der ganze Abschluss von $\mathbb{Z}$ in K.

Korollar 1.6. *Der ganze Abschluss ist ein Ring.*

Beweis: Es gilt $x + y, x - y, xy \in A[x, y]$. Sei x ganz über A. Dann ist $A[x]$ ein A-Modul mit Erzeugern $\{x_1, \ldots, x_n\}$. Sei y ganz über A. Dann ist $A[y]$ ein A-Modul mit Erzeugern $\{y_1, \ldots, y_m\}$. Dann sind die Elemente $x_i y_j$ Erzeuger von $A[x, y]$, denn in $\alpha = \sum a_{kl} x^k y^l$ können x und y durch die x_i und y_j ausgedrückt werden. Durch Ausmultiplizieren erhält man eine Darstellung von α in Termen der $x_i y_j$. Also ist $A[x, y]$ endlich erzeugt. Nach Satz 1.3 sind dann alle Elemente von $A[x, y]$ ganz über A. □

Korollar 1.7 (Transitivität). *Seien $A \subset B$, $B \subset C$ ganze Ringerweiterungen. Dann ist $A \subset C$ ganz.*

Beweis: Sei $x \in C$. Es erfüllt also eine Gleichung

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0 \ , b_i \in B$$

B ist ganz über A, also ist $A[b_i]$ endlich erzeugter A-Modul. Wie beim letzten Beweis folgt $A[b_1, \ldots, b_n]$ endlich erzeugter A-Modul. Wegen $x \in A[b_1, \ldots, b_n]$ ist x ganz über A (Satz 1.3). □

Korollar 1.8. *Sei B ein Integritätsring, $A \subset B$ ein Unterring, so dass B ganz über A ist. Dann gilt:*

$$B \text{ Körper } \Leftrightarrow A \text{ Körper}$$

Beweis: Sei A ein Körper, $0 \neq b \in B$. Nach Satz 1.3 ist $B' = A[b]$ ein endlich dimensionaler A-Vektorraum. Die Multiplikation mit B ist eine A-lineare Abbildung $B' \to B'$. Da B nullteilerfrei ist, ist diese Abbildung injektiv. Da B' endlich dimensional ist, ist sie dann auch surjektiv. Also hat b ein multiplikatives Inverses in $B' \subset B$.
Umgekehrt sei B ein Körper, $0 \neq a \in A$. Sei $b = a^{-1} \in B$. Dieses Element ist ganz über A, erfüllt also eine Gleichung

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \ a_i \in A \ .$$

Diese Gleichung wird mit a^{n-1} multipliziert.

$$b + a_1 + a_2 a + \ldots a_n a^{n-1} = 0 \ .$$

Alle Summanden außer dem ersten liegen in A, also auch b. □

Definition 1.9. *Sei A ein Integritätsring. A heißt* ganz abgeschlossen, *wenn A mit seinem ganzen Abschluss im Quotientenkörper übereinstimmt.*

Beispiel. Hauptidealringe (z.B. $\mathbb{Z}$, diskrete Bewertungsringe) sind ganz abgeschlossen.

Beweis: Sei A ein Hauptidealring, K der Quotientenkörper, $x \in K$ ganz über A. Dann ist

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

Sei $x = a/b$ mit a und b teilerfremd. Die Gleichung wird mit b^n multipliziert:

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0 \ .$$

b teilt jeden Summanden außer dem ersten, also folgt $b \mid a^n$. Dies ist ein Widerspruch zur Teilerfremdheit. Es folgt $b \in A^*$, $x \in A$. □

Beispiel. Zahlringe sind ganz abgeschlossen.

Beweis: Sei $\mathcal{O}$ der ganze Abschluss von $\mathbb{Z}$ in K, $\mathcal{O}'$ der ganze Abschluss von $\mathcal{O}$ in K. Wegen der Transitivität von ganzen Erweiterung ist dann $\mathcal{O}'$ ganz über Z, also $\mathcal{O}' \subset \mathcal{O}$. □

Theorem 1.10. *Sei $K/\mathbb{Q}$ ein Zahlkörper, $\mathcal{O} \subset K$ der Ganzheitsring. Dann ist $\mathcal{O} \cong \mathbb{Z}^d$ mit $d = [K : \mathbb{Q}]$.*

Übungsaufgabe. *Bestimmen Sie den Isomorphismus für quadratische Erweiterungen von Q.*

Korollar 1.11. *$\mathcal{O}$ ist noethersch.*

Erinnerung: Sei R ein Ring. Ein R-Modul M heißt *noethersch*, wenn jede Kette

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

von Untermoduln von M konstant wird. Ein Ring heißt *noethersch*, wenn er als R-Modul noethersch ist.

- Quotienten und Untermoduln von noetherschen Moduln sind noethersch.
- R noethersch $\Leftrightarrow$ alle Ideale endlich erzeugt.
- Hauptidealringe sind noethersch.
- R noethersch $\Rightarrow R[X]$ noethersch.
- Falls R noethersch, dann ist M noethersch genau dann, wenn M endlich erzeugt ist.

Beweis: $\mathcal{O}$ ist endlich erzeugter $\mathbb{Z}$-Modul. □

Bemerkung. Auch die Ganzheitsringe von Funktionenkörpern sind noethersch. Sie sind isomorph zu $\mathbb{F}_p[X]^d$.

Übungsaufgabe. *Sei A ein Ring, $A \subset B$ eine ganze Ringerweiterung.*

(i) Sei $S \subset A$ eine multiplikative Teilmenge, $S^{-1}A = \{a/s \mid a \in A, s \in S\}$ die Lokalisierung. Dann ist $S^{-1}A \subset S^{-1}B$ ganz.

(ii) Ist A ganz abgeschlossen, dann auch $S^{-1}A$.

(iii) Sei $I \subset A$ ein echtes Ideal. Dann ist $A/I \to B/BI$ ganz.

Vorüberlegungen

$\mathcal{O} \subset K$ ist eine torsionsfreie abelsche Gruppe. Daher ist ist $\mathcal{O}$ endlich erzeugt genau dann, wenn $\mathcal{O} \cong \mathbb{Z}^N$ für ein N.

Lemma 1.12. *Sei $x \in K$. Dann gibt es $m \in \mathbb{Z}$ mit $mx \in \mathcal{O}$.*

Beweis: x erfüllt $x^n + a_1x^{n-1} + a_2x^{n-1} + \cdots + a_n = 0$ mit $a_i \in \mathbb{Q}$. Sei m der Hauptnenner der a_i. Multiplikation der Gleichung mit m^n ergibt

$$(mx)^n + a_1m(mx)^{n-2} + \ldots m^n a_n = 0 \ .$$

Also gilt $mx \in \mathcal{O}$. □

Korollar 1.13. *$\mathcal{O}$ enthält eine freie Gruppe vom Rang $d = [K : \mathbb{Q}]$.*

Beweis: Sei $x_1, \ldots, x_d$ eine Basis von K über $\mathbb{Q}$. Seien $m_1, \ldots, m_d \in \mathbb{Z}$, so dass $m_i x_i \in \mathcal{O}$.

Behauptung. *$< m_1x_1, \ldots, m_dx_d >$ hat Rang d.*

Wäre der Rang kleiner als d, so hätten wir eine Relation

$$n_1(m_1x_1) + n_2(m_2x_2) + \cdots + n_d(m_dx_d) = 0 \ ,$$

dies ist ein Widerspruch zu linearen Unabhängigkeit von $x_1, \ldots, x_d$. □

Lemma 1.14. *Sei $M \subset K$ eine endlich erzeugte abelsche Gruppe. Dann gilt* $\mathrm{rg}M \leq d$.

Beweis: Sei $M_{\mathbb{Q}} = \{\frac{m}{s} \mid m \in M, s \in \mathbb{Z}\} \subset K$. Dies ist ein $\mathbb{Q}$-Vektorraum der Dimension höchstens d.

Behauptung. $\dim M_{\mathbb{Q}} = \mathrm{rg}M$.

Sei $x_1, \ldots, x_k$ eine Basis von M als $\mathbb{Z}$-Modul. Dies ist eine Basis von $M_{\mathbb{Q}}$ als $\mathbb{Q}$-Vektorraum, da ein linear unabhängiges Erzeugendensystem. □

Insgesamt: Wenn $\mathcal{O}$ endlich erzeugt ist als abelsche Gruppe, dann $\mathcal{O} \cong \mathbb{Z}^d$.

Lemma 1.15. *Für den Beweis von Theorem 1.10 genügt es zu zeigen, dass $\mathcal{O} \subset M \subset K$ wobei M eine endlich erzeugte abelsche Gruppe ist.*

Beweis: M endlich erzeugt $\Rightarrow$ M noetherscher Z-Modul. $\mathcal{O} \subset M \Rightarrow \mathcal{O}$ noethersch. Der Rest des Theorems folgt aus Korollar 1.13 und Lemma 1.14. □

Kapitel 2

Norm, Spur und Diskriminante

Erinnerung an Algebra

Sei L/K algebraisch, $\operatorname{Char} K = 0$, $\alpha \in L$. Das Minimalpolynom $\operatorname{Min}(\alpha)$ von α ist das normierte Polynom minimalen Grades mit Nullstelle α.

Lemma 2.1. $\operatorname{Min}(\alpha)$ *ist das charakteristische Polynom* $\det(X \operatorname{id} - m_\alpha)$ *der* K*-linearen Multiplikationsabbildung* $m_\alpha : K(\alpha) \to K(\alpha)$ *mit* $x \mapsto \alpha x$*.*

Beweis: Sei P das charakteristische Polynom. Es hat den Grad $[K(\alpha) : K] = \deg \operatorname{Min}(\alpha)$. Es ist normiert. Es gilt $P(m_\alpha)$ als Abbildung $K(\alpha) \to K(\alpha)$. Auswerten in 1 ergibt $P(\alpha) = 0$. Also erfüllt P alle Eigenschaften von $\operatorname{Min}(\alpha)$. □

Seien $\alpha_1, \ldots, \alpha_d$ die d verschiedenen ($\operatorname{Char} K = 0$!) Nullstellen von $\operatorname{Min}(\alpha)$ in $\overline{K}$. Jedes α_i definiert einen Körperhomomorphismus $\sigma_i : K(\alpha) \to \overline{K}$ mit $\sigma_i(\alpha)_i$. Dies sind alle Körperhomomorphismen $\sigma : K(\alpha) \to K$ mit $\sigma|_K = \operatorname{id}$.

Lemma 2.2. *Es gilt*

$$\operatorname{Min}(\alpha) = \prod_{i=1}^{d} (X - \alpha_i) = \prod_{i=1}^{d} (X - \sigma_i(\alpha)) \ .$$

Beweis: Klar □

Bemerkung. $K(\alpha)/K$ ist galois genau dann, wenn alle $\alpha_i \in K(\alpha)$. Dann ist $\{\sigma_1, \ldots, \sigma_d\} = \operatorname{Gal}(K(\alpha)/K)$.

Definition 2.3. *Sei* L/K *endliche Körpererweiterung,* $\alpha \in L$*. Das* charakteristische Polynom *von* α *ist* $P_\alpha = \det(X \operatorname{id} - m_\alpha)$*, wobei* m_α *die Multiplikationsabbildung mit* α *ist. Die* Norm *von* α *ist* $N_{L/K}(\alpha) = \det(m_\alpha)$*. Die* Spur *von* α *ist* $\operatorname{Tr}_{L/K}(\alpha) = \operatorname{Tr}(m_\alpha)$*.*

Bemerkung. Es gilt $P_\alpha(X) = X^{[L:K]} - \mathrm{Tr}(\alpha)X^{[L:K]-1} + \cdots + (-1)^{[}L : K]N(\alpha)$.

Lemma 2.4. *Sei* $\mathrm{Char}\, K = 0$, $[L : K] = d$. *Seien* $\alpha_1, \ldots, \alpha_d$ *die Nullstellen von* $\mathrm{Min}(\alpha)$, *jede mit Vielfachheit* $[L : K(\alpha)]$. *Seien* $\sigma_1, \ldots, \sigma_d : L \to \overline{K}$ *die Einbettungen mit* $\sigma_i|_K = \mathrm{id}$. *Dann gilt*

$$P_\alpha(X) = \mathrm{Min}(\alpha)^{[L:K(\alpha)]} = \prod_{i=1}^{e}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha))$$
$$\mathrm{Tr}_{L/K}(\alpha) = \sum \alpha_i = \sum \sigma_i(\alpha)$$
$$N_{L/K}(\alpha) = \prod \alpha_i = \prod \sigma_i(\alpha)\ .$$

Beweis: Es genügt, die Aussge für P_α zu zeigen. Es gilt

$$\{\alpha_1, \ldots, \alpha_d\} = \{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$$

als Mengen mit Vielfachheit, denn jede der $[K(\alpha) : K]$ vielen Einbettungen $K(\alpha) \to \overline{K}$ lässt sich auf $[L : K(\alpha)]$ viele Weisen nach L fortsetzen. Der Fall $L = K(\alpha)$ ist Lemma 2.1. Sei nun $r : [L : K(\alpha)]$.

Behauptung. $P_{L/K} = P^r_{K(\alpha)/K}$.

Sei $y_1, \ldots, y_r$ eine Basis von $L/K(\alpha)$, $z_1, \ldots, z_q$ eine Basis von $K(\alpha)/K$. Dann ist $\{y_i z_j \mid i = 1, \ldots, r, j = 1, \ldots, q\}$ eine Basis von L/K. Sei $M = (m_{jk})$ die Matrix der Multiplikation mit α bezüglich er z_j, d.h. $m_\alpha(z_j) = \sum_k m_{jk} z_k$. Dann gilt $m_\alpha(y_i z_j) = \sum_k m_{jk} y_i z_k$. Die Matrix von m_α bezüglich der Basis $y_i z_j$ ist eine diagonale Blockmatrix aus r Kopien von M. □

Korollar 2.5. *Sei* L/K *Erweiterung von Zahlkörpern,* $\alpha \in \mathcal{O}_L$. *Dann gilt* $P_\alpha \in \mathcal{O}_K[X]$. *Insbesondere ist* $\mathrm{Tr}_{L/K}(\alpha), N_{L/K}(\alpha) \in \mathcal{O}_K$.

Bemerkung. Falls $\mathcal{O}_L \cong \mathcal{O}_K^d$ (im Allgemeinen falsch!), so hat die Matrix von m_α Einträge in $\mathcal{O}_K$ und die Aussage ist klar.

Beweis: $P_\alpha(X) = \prod(X - \sigma(\alpha)$ mit σ wie im Lemma. Nach Vorraussetzung erfüllt α eine Gleichung

$$X^n + a_1 X^{n-1} + \cdots + a_0 = 0\ a_i \in \mathcal{O}_K$$

Dann erfüllt $\sigma(\alpha)$ dieselbe Gleichung, ist also ebenfalls ganz über $\mathcal{O}_K$. Da $\mathcal{O}_K$ ein Ring ist, liegen dann alle Koeffizienten von P_α in $\mathcal{O}_K$. □

Beispiel. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{3})$, $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. Wir wählen die Basis $1, \sqrt{3}$. Sei $\alpha = a + b\sqrt{3}$. Die Multiplikation mit α hat die Matrix

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

Also ist die Spur $2a$, die Norm $a^2 - 3b^2$, das charakteristische Polynom

$$P_\alpha(X) = X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = X^2 - 2aX + (a^2 - 3b^2)$$

Für $b \neq 0$ ist dies das Minimalpolynom von α. Für $b = 0$ gilt $X^2 - 2aX + a^2 = (X - a)^2 = \mathrm{Min}(\alpha)^2$.

Definition 2.6. *Sei $A \subset B$ eine Ringerweiterung, B ein freier A-Modul vom Rang d. Die* Spurpaarung *ist die symmetrische A-bilineare Abbildung*

$$(\cdot,\cdot) : B \times B \to A \ , (x,y) = \mathrm{Tr}_{B/A}(xy) \ .$$

Die Diskriminante $\mathcal{D}_{B/A}$ *ist das Ideal, das von*

$$D(x_1, \ldots, x_d) = \det(\mathrm{Tr}(x_i x_j)_{i,j})$$

erzeugt wird, wobei $x_1, \ldots, x_d$ eine Basis von B ist.

Bemerkung. Uns interessiert vor allem L/K endliche Köpererweiterung, aber auch $\mathcal{O}_K/\mathbb{Z}$.

Beispiel. Sei $L = \mathbb{Q}[X]/X^2 + pX + q$ mit $p, q \in \mathbb{Q}$. Dies ist ein 2-dimensionaler $\mathbb{Q}$-Vektorraum, Basis $1, X$. Es gilt $\mathrm{Tr}(1) = 2$. Muliplikation mit X hat die Matrix

$$\begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

also, $\mathrm{Tr}(X) = -q$.
Es gilt

$$D(1,X) \ = \ \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(X) \\ \mathrm{Tr}(X) & \mathrm{Tr}(X^2) \end{pmatrix} \ = \ \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} \ = \ p^2 \ - \ 4q$$

Dies ist genau die Diskriminate der quadratischen Gleichung.

Lemma 2.7. *Sei $y_1, \ldots, y_d \in B$ mit $y_i = \sum a_{ij} x_j$. Dann gilt*

$$D(y_1, \ldots, y_d) = \det(a_{ij})^2 D(x_1, \ldots, x_d)$$

Insbesondere ist $\mathcal{D}_{B/A}$ wohldefiniert.

Beweis: Es gilt

$$\mathrm{Tr}(y_p y_q) = \mathrm{Tr}(\sum_{i,j} a_{pi} a_{qj} x_i x_j) = \sum a_{pi} a_{qj} \mathrm{Tr}(x_i x_j)$$

Es folgt

$$(\mathrm{Tr}(y_p y_q))_{pq} = (a_{pi})_{pi} (\mathrm{Tr}(x_i x_j))_{ij} (a_q j)^t$$

wobei ^{t} die transponierte Matrix ist. Dies impliziert die Gleichheit der Determinanten. □

Exkurs in die bilineare Algebra

Sei $(\cdot,\cdot) : V \times V \to k$ eine symmetrische Bilinearform, (k Körper, V ein Vektorraum). Sei $v_1, \ldots, v_d$ eine Basis von V, $M = (v_i, v_j)_{ij}$ die zugehörige symmetrische Matrix. Dann gilt für $v = \sum a_i v_i, w = \sum_j b_j v_j$

$$(v,w) = (\sum a_i v_i, \sum_j b_j v_j) = \sum_{i,j} a_i (v_i, v_j) b_j = (a_1, \ldots, a_d) M (b_1, \ldots, b_d)^t$$

Definition 2.8. *Die Bilinearform $(\cdot,\cdot)$ heißt nicht-degeneriert, wenn aus $(v,w) = 0$ für alle w die Gleichung $v = 0$ folgt.*

Lemma 2.9. *$(\cdot,\cdot)$ ist nichtdegeneriert genau dann, wenn die zugehörige Matrix M invertierbar ist, also genau dann, wenn* $\det M \neq 0$.

Beweis: Falls M nicht invertierbar ist, so gibt es v mit $v^t M = 0$, also auch $v^t M w = 0$ für alle w. Sei nun M invertierbar, $v = \sum a_i v_i$. Der Fall $d = 1$ ist trivial, also sei $d > 1$. Wähle $(c_1, \ldots, c_d)$ mit

$$a_1 c_1 + \cdots + a_d c_d \neq 0$$

Wir lösen das Gleichungssystem $Mw = (c_1, \ldots, c_d)^t$. Dies ist möglich, da M invertierbar ist. Es folgt $v^t M w \neq 0$. □

Bemerkung. Die Diskriminante entscheidet also, ob die Spurpaarung nichtdegeneriert ist.

Beispiel. $K = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$. Es gilt

$$\mathcal{D} = D(1, \sqrt{3}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{3}) \\ \mathrm{Tr}(\sqrt{3}) & \mathrm{Tr}(3) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} = 12$$

Lemma 2.10. *Sei $(\cdot,\cdot)$ nicht-degnererierte symmetrsiche Bilinearform, $v_1, \ldots, v_d$ eine Basis. Dann gibt es eine* duale Basis *$w_1, \ldots, w_d$ mit $(v_i, w_j) = \delta_{ij}$.*

Beweis: Die Bestimmung von w_j bedeutet das Lösen eines linearen Gleichungssystems $Mw_j = (0, \ldots, 1, \ldots, 0)$ (mit 1 an der j-ten Stelle. Dies ist möglich, da M invertierbar ist. □

Satz 2.11. *Sei L/K endliche Körpererweiterung der* Char 0. *Dann ist $\mathcal{D}_{L/K} \neq 0$. Die Spurpaarung ist nicht-degeneriert.*

Beweis: Es gilt $\mathrm{Tr}(\alpha) = \sum \sigma_i(\alpha)$, wobei $\sigma_i : L \to \overline{K}$ die Einbettungen mit $\sigma_i|_K = \mathrm{id}$ durchläuft. Sei $x_1, \ldots, x_d$ eine Basis von L über K. Es gilt

$$\begin{aligned} D(x_1, \ldots, x_d) &= \det(\mathrm{Tr}(x_i y_j)_{ij}) = \det(\sum_k \sigma_k(x_i x_j))_{ij} \\ &= \det(\sum_k \sigma_k(x_i)\sigma_k(x_j))_{ij} = \det((\sigma_k(x_i))_{ik}(\sigma_k(x_j))_{kj}) = \det(\sigma_i(x_j))^2 \end{aligned}$$

Angenommen diese Determinante verschwindet. Dann gibt es $u_1, \ldots, u_d \in \overline{K}$ mit $\sum_i u_i \sigma_i(x_j) = 0$ für alle j. Da die x_j eine Basis sind, folgt $\sum u_i \sigma_i = 0$ als Abbildungen $L^* \to \overline{K}$. Als Gruppenhomomorphismen $L^* \to \overline{K}^*$ sind die σ_i jedoch linear unabhänging (vergleiche Beweis des Hauptsatzes der Galois-Theorie, Bosch §4.6 Satz 2). □

Beispiel. $L = \mathbb{Q}[X]/X^2 + pX + q$ hatte Diskriminante $p^2 - 4q$. Diese Zahl verschwindet genau dann, wenn $X^2 + pX + q$ eine doppelte Nullstelle hat, also wenn L kein Körper ist.

Beweis von Theorem 1.10. Sei $\mathcal{O} \subset K$ der Ganzheitsring. Nach Lemma 1.15 genügt es zu zeigen, dass $\mathcal{O}$ in einem endlich erzeugten $\mathbb{Z}$-Modul $M \subset K$ enthalten ist. Sei $x_1, \ldots, x_d$ eine Basis von $K/\mathbb{Q}$. Ohne Einschränkung gilt $x_i \in \mathcal{O}$. Sei $y_1, \ldots, y_d$ die duale Basis bezüglich der Spurpaarung.

Behauptung. $\mathcal{O} \subset < y_1, \ldots, y_d >_{\mathbb{Z}}$.

Sei $z \in \mathcal{O}$. Wir schreiben $z = \sum b_j y_j$ mit $b_j \in \mathbb{Q}$, da die y_j eine Basis bilden. Es gilt $x_i z \in \mathcal{O}$, da $\mathcal{O}$ ein Ring ist. Nach Korollar 2.5 ist $\mathrm{Tr}(x_i z) \in \mathbb{Z}$. Es folgt weiter

$$\mathrm{Tr}(x_i z) = \sum \mathrm{Tr}(x_i b_j y_j) = \sum b_j \mathrm{Tr}(x_i y_j) = b_i$$

□

Kapitel 3

Ideale

Satz 3.1. *Sei $\mathcal{O}$ ein Zahlring. Dann ist $\mathcal{O}$ ein* Dedekindring*, d.h. noethersch, ganz abgeschlossen und* 1*-dimensional (d.h. jedes Primideal ungleich* 0 *ist maximal).*

Beweis: Wir wissen bereits, dass $\mathcal{O}$ noethersch und ganz abgeschlossen ist. Sei nun $\mathfrak{p} \subset \mathcal{O}$ ein Primideal ungleich 0. Dann ist auch $\mathfrak{p}' = \mathfrak{p} \cap \mathbb{Z}$ ein Primideal.

Behauptung. $\mathfrak{p}' \neq 0$.

Sei $x \in \mathfrak{p}$ mit

$$0 = x^n + a_1 x^{n-1} + \cdots + a_n = x(x^{n-1} + a_1 x^{n-2} + \ldots a_{n-1}) + a_0$$

und $a_i \in \mathbb{Z}$, ohne Einschränkung $a_n \neq 0$. Es folgt $a_0 \in \mathfrak{p} \cap \mathbb{Z}$.
Es folgt $\mathfrak{p}' = (p)$ für eine Primzahl p. Die Abbildung

$$\mathbb{Z}/(p) \to \mathcal{O}/\mathfrak{p}$$

ist ein injektiver Ringhomomorphismus. Also ist der Integritätsring $\mathcal{O}/\mathfrak{p}$ eine ganze Erweiterung des Körpers $\mathbb{Z}/(p)$. Nach Lemma 1.8 ist dann auch $\mathcal{O}/pf$ ein Körper, d.h. $\mathfrak{p}$ ist maximal. □

Übungsaufgabe. *(i) Sei A ein Dedekindring, $S \subset A$ eine multiplikative Menge. Dann ist $S^{-1}A$ ein Dedekindring.*

(ii) Sei L/K eine separable Körpererweiterung, $A \subset K$ Dedekindring mit Quotientenkörper K. Sei B der ganze Abschluss von A in L. Dann ist B ein Dedekindring.

Definition 3.2. *Sei $\mathcal{O}$ der Ganzheitsring von K. Ein* gebrochenes *Ideal von $\mathcal{O}$ ist ein $\mathcal{O}$-Untermodul $I \subset K$, so dass es $d \in \mathcal{O} \setminus \{0\}$ gibt mit $dI \subset I$, d.h. ein gemeinsamer Hauptnenner.*

Bemerkung.
- Gebrochene Ideale heißen auch *invertierbare Ideale*

- Ein Ideal $I \subset \mathcal{O}$ ist ein gebrochenes Ideal (mit $d = 1$).
- I ist ein gebrochenes Ideal, genau dann, wenn es ein endlich erzeugter $\mathcal{O}$-Untermodul von K ist.

  Beweis: Sei $I =< x_1, \ldots, x_n >_{\mathcal{O}}$, d der Hauptnenner der x_i, dann gilt $dI \subset \mathcal{O}$. Ist umgekehrt $dI \subset \mathcal{O}$, so ist dI ein Ideal eines noetherschen Rings, also endlich erzeugt. Dann ist auch I endlich erzeugt. □

- Die Menge der gebrochenen Ideale hat eine Addition und Multiplikation

$$I + I' = \{a + b \mid a \in I, b \in I'\} \subset K$$
$$I \cdot I' = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in I'\} \subset K$$

  Wir werden zeigen, dass die gebrochenen Ideale ungleich 0 eine abelsche Gruppe bezüglich der Multiplikation bilden.

- Gebrochene Ideale heißen auch *invertierbare Ideale* (bezüglich der Multiplikation).

Theorem 3.3. *Sei A ein Dedekindring. Dann ist jedes maximale Ideal invertierbar als gebrochenes Ideal, d.h. zu I existiert I^{-1} mit $I \cdot I^{-1} = A$.*

Bemerkung. Wäre A ein Hauptidealring, so wären alle gebrochenen Ideale von der Form Ab mit $b \in Q(A)$. Das inverse Ideal wäre einfach Ab^{-1}.

Lemma 3.4. *Sei A noetherscher Ring, $0 \neq I$ ein Ideal. Dann gibt es Primideale ungleich 0 mit $I \subset \mathfrak{p}_1 \ldots \mathfrak{p}_n$.*

Beweis: Sei Φ die Menge der Ideale $I \neq I$ von A, für die das Lemma nicht gilt, d.h. die kein Produkt von Primidealen enthalten. Angenommen, $\Phi \neq \emptyset$. Da A noethersch ist, hat Φ ein maximales Element I_0. I_0 ist nicht prim, also gibt es $x, y \in A \setminus I_0$ mit $xy \in I_0$. Nach Voraussetzung

$$I_0 \subsetneq I_0 + (x), I_0 + (y) \Rightarrow I_0 + (x), I_0 + (b) \notin \Phi$$

Also gibt es Primideale ungleich null mit

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset I_0 + (x), \mathfrak{q}_1 \ldots \mathfrak{q}_m \subset I_0 + (b) \Rightarrow$$
$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \mathfrak{q}_1 \ldots \mathfrak{q}_m \subset (I_0 + (x))(I_0 + (y)) = I_0$$

Dies ist ein Widerspruch. □

Beweis des Theorems: Sei $\mathfrak{m} \subset A$ maximal, $\mathfrak{m} \neq 0$. Sei

$$\mathfrak{m}' = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Dies ist ein A-Untermodul von $Q(A)$. Für $0 \neq y \in \mathfrak{m}$ folgt $y\mathfrak{m}' \in A$, also ist dies ein gebrochenes Ideal. Schließlich gilt nach Definition $\mathfrak{m}\mathfrak{m}' \subset A$. Da $\mathfrak{m}$ ein Ideal ist, gilt $A \subset \mathfrak{m}'$. Es folgt

$$\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$$

Da $\mathfrak{m}$ maximal ist, gilt

$$\mathfrak{m}'\mathfrak{m} = \mathfrak{m} \text{ oder } \mathfrak{m}'\mathfrak{m} = A$$

Behauptung. $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ *ist unmöglich.*

Angenommen, $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$. Sei $x \in \mathfrak{m}' \Rightarrow x\mathfrak{m} \subset \mathfrak{m}$. Iterativ folgt

$$x^2\mathfrak{m} = x(x\mathfrak{m}) \subset x(\mathfrak{m}) \subset \mathfrak{m} \Rightarrow x^n\mathfrak{m} \subset \mathfrak{m} \text{ für alle } n \geq 1$$

Sei $0 \neq d \in \mathfrak{m}$, also $x^n d \in A$ für alle n. Dann ist $A[x]$ ein gebrochenes Ideal, also endlich erzeugter A-Modul. Also ist x ganz über A. Dies bedeutet wiederum, dass $x \in A$, da A ganz abgeschlossen ist. Also $\mathfrak{m}' \subset A$. Die Inklusion $A \subset \mathfrak{m}'$ war trivial, also haben wir $A = \mathfrak{m}'$ gezeigt. Insgesamt:

$$A = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Sei nun $0 \neq a \in \mathfrak{m}$, also $(a) \neq 0$. Nach Lemma 3.4 gibt es Primideale ungleich null mit $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset (a)$. Ohne Einschränkung sei n minimal. Es folgt

$$\mathfrak{m} \supset (a) \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$$

Angenommen, für alle i ist $\mathfrak{p}_i$ ist nicht in $\mathfrak{m}$ enthalten, d.h. es gibt $x_i\mathfrak{p} \setminus \mathfrak{m}$. Dann gilt $x_1 \dots x_n \in \mathfrak{p}_1 \dots \mathfrak{p}_n \subset \mathfrak{m}$. Dies ist ein Widerspruch zu $\mathfrak{m}$ Primideal. Also gibt es ein i mit $\mathfrak{p}_i \subset \mathfrak{m}$, z.B. $i = n$.

$$\mathfrak{m} \supset (a) \supset \mathfrak{m}I \text{ mit } I = \mathfrak{p}_1 \dots \mathfrak{p}_{n-1}$$

I ist nicht in (a) enthalten, da n minimal gewählt war. Sei $b \in I \setminus (a)$. Wegen $\mathfrak{m}I \subset (a)$ folgt $\mathfrak{m}b \subset (a) = Aa$. Dies impliziert $\mathfrak{m}ba^{-1}a \subset A$. Also nach Definition: $ba^{-1} \in \mathfrak{m}' = A \Leftrightarrow b \in (a)$. Dies ist ein Widerspruch zur Zahl von b. □

Theorem 3.5. *Sei A ein Dedekindring,* Spec A *die Menge der Primideale von A.*

(i) Jedes gebrochene Ideal schreibt sich eindeutig als

$$I = \prod_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}^{v_\mathfrak{p}(I)}$$

mit $v_\mathfrak{p}(I) \in \mathbb{Z}$ fast alle null.

(ii) Es gilt $v_\mathfrak{p}(I) \geq 0$ für alle $\mathfrak{p}$ genau dann, wenn I ein ganzes Ideal ist.

(iii) Der Monoid der gebrochenen Ideale ist eine Gruppe.

Übungsaufgabe. *Sei A ein lokaler Dedekindring, d.h. es gibt nur genau ein maximales Ideal. Dann ist A ein diskreter Bewertungsring, dh. ein Hauptidealring mit (bis auf Konjugation mit Einheiten) nur einem Primelement.*

Beweis: Zur Existenz: Es gilt $dI \subset A$, $I = (dI)(d^{-1}$. Daher genügt es, die Produktzerlegung für ganze Ideale zu zeigen. Sei Φ die Menge der Ideale, die keine Primidealfaktorisierung hat. Angenommen, $\Phi \neq \emptyset$. Da A noethersch ist, hat Φ ein maximales Element I. Es ist $I \neq A$, da $A = \prod_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}^0$. Also ist $I \subset \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$. Sei $\mathfrak{p}' = \mathfrak{p}^{-1}$ das Inverse als gebrochenes Ideal. Es folgt

$$I \subset \mathfrak{p} \Rightarrow I\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$$

Wegen $A \subset \mathfrak{p}'$ folgt auf jeden Fall $I\mathfrak{p}' \subset I$.

Behauptung. $I \subsetneq I\mathfrak{p}'$

Angenommen, die Ideale sind gleich. Sei $x \in \mathfrak{p}'$. Nach Annahme ist $xI \subset I$, also iterativ $x^n I \subset I$ für alle n. Ein Hauptnenner für I ist auch ein Hauptnenner für $A[x]$, also ist dieser Modul endlich erzeugt und x ganz über A. Damit ist $x \in A$. Wir haben $\mathfrak{p}' = A$ gezeigt, dies ist ein Widerspruch.
Nach Wahl von $I \in \Phi$ ist nun $I\mathfrak{p}' \notin \Phi$. Es gilt

$$\mathfrak{p}' I = \mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n} \Rightarrow I = \mathfrak{p}\mathfrak{p}' I = \mathfrak{p}\mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n}$$

Tatsächlich sind hierbei die Exponenten alle größer gleich 0.
Zur Eindeutigkeit: Sei $\prod \mathfrak{p}^{n_\mathfrak{p}} = \prod \mathfrak{p}^{m^-{}_\mathfrak{p}}$, also $\prod \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = A$. Wir schreiben die Gleichung so um, dass alle Exponenten größer gleich Null und minimal sind. Wir erhalten also

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k} = \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$$

mit $\mathfrak{p}_i \neq \mathfrak{q}_j$ für alle i, j und $n_i, m_j > 0$. Es gilt $\mathfrak{p}_1 \subset \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$. Also enthält $\mathfrak{p}_1$ eines der $\mathfrak{q}_j$ (wie im Beweis von Theorem 3.3). Da A ein Dedekindring ist, folgt $\mathfrak{p}_1 = \mathfrak{q}_j$, Widerspruch.
Die Behauptung über die Gruppenstruktur ist klar. □

Definition 3.6. *Die* Idealklassengruppe *oder Klassengruppe des Zahlkörpers K ist*

$$\mathrm{Cl}(K) = \frac{\textit{Gruppe der gebrochenen Ideale} \neq 0}{\textit{Hauptideale} \neq 0}$$

Die Klassenzahl h *ist die Anzahl der Elemente von* $\mathrm{Cl}(K)$.

Bemerkung. $h = 1$ bedeutet, dass jedes Ideal ein Hauptideal ist. Die Klassenzahl misst also, wie weit $\mathcal{O}_K$ davon abweicht, ein Hauptidealring zu sein. Sie ist endlich (tief! siehe unten)

Exkurs

Sei X eine kompakte Riemannsche Fläche, $\mathcal{O}_X$ die Garbe der holomorphen Funktionen auf X. Eine $\mathcal{O}$-Modulgarbe $\mathcal{F}$ heißt *invertierbar*, falls $\mathcal{F}$ lokal isomorph zu $\mathcal{O}_X$ ist. Jede invertierbare Garbe gehört zu einem Divisor $D = \sum n_p P$, einer formalen endlichen Linearkombination von Punkten von X. Ein Hauptdivisor ist der Null- und Polstellendivisor einer meromorphen Funktion auf X, $D = \sum \mathrm{ord}_P(f)P$. Hauptdivisoren haben stets den Grad 0. Die Gruppe der Divisoren modulo Hauptdivisoren ist bekannt, sie ist isomorph zu $\mathbb{Z} \times \mathbb{C}^g/\Lambda$, wobei g das Geschlecht von X ist, Λ ein Gitter.
Sei nun A ein Ganzheitsring, $S = \mathrm{Spec}\, A$, I ein gebrochenes Ideal. Zu I gehört der Divisor $\sum v_{\mathfrak{p}}(I)\mathfrak{p}$. Der Divisor ist ein Hauptdivisor, falls I ein Hauptideal ist. Der Grad eines Hauptdivisors ist stets echt positiv. Die Klassengruppe ist genau die Gruppe der Divisoren modulo der Hauptdivisoren. S ist ein topologischer Raum mit der Zariski-Topologie. Die offenen Mengen sind von der Form $U_f = \mathrm{Spec}\, A_f$, A_f die Lokalisierung von A an $\{1, f, f^2, f^3, \dots\}$. Er trägt das Ideal von Ringen mit $\mathcal{O}(U_f) = A_f$. Ihre Halme sind diskrete Bewertungsringe. I definiert eine Garbe von $\mathcal{O}$-Moduln mit $\mathcal{F}(U_f) = I_f$. Diese ist lokal isomorph zu $\mathcal{O}$.
Die Analogie kann strikt gemacht werden: Der Zahlkörper $Q(A)$ entspricht dem Körper der meromorphen Funktionen $\mathcal{M}(X)$. Die Punkte der Riemannschen Fläche X stehen in Bijektion zu den diskreten Bewertungsringen $\mathbb{C} \subset R \subset \mathcal{M}(X)$ mit Quotientenkörper $\mathcal{M}(X)$. Die abgeschlossenen Punkte von S stehen in Bijektion zu den diskreteten Bewertungsringen mit Quotientenkörper $Q(A)$. Die Klassengruppe ist genau die Gruppe der Divisoren modulo der Hauptdivisoren.
Wichtiger Unterschied: X ist kompakt, S nicht! Dies ist z.B. der Grund für die Unterschiede im Grad von Hauptdivisoren, unterschiedliches Verhalten der Divisorenklassengruppe. Es fehlen Punkte im "Unendlichen". Diese sind bekannt: sie entsprechen den Einbettungen von K nach $\mathbb{R}$ oder $\mathbb{C}$. Die analytischen Eigenschaften von Zahlkörpern müssen ebenfalls benutzt werden.

Lemma 3.7. *Die Klassengruppe ist isomorph zur Halbgruppe der echten Ideale ungleich* 0 *mit Äquivalenzrelation* $I(g) \sim I(f)$ *für* $f, g \in A \setminus \{0\}$.

Beweis: Sei C' die im Lemma definierte Halbgruppe. Sie bildet sich in die Klassengruppe ab. Jedes gebrochene Ideal ist äquivalent zu einem echten Ideal, also ist die Abbildung surjektiv. Die Äquivalenzrelation ist offensichtlich die gleiche, also ist sie auch injektiv. □

Dieser Beschreibung sieht man die Existenz des Inversen nicht an! Man spart also keine Arbeit gegenüber unserem Ansatz.

Beispiel

$K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Es gilt $\mathcal{O} \cong \mathbb{Z}[X]/X^2 + 5$. Wir bestimmen die Primideale: Sei $\mathfrak{p} \subset \mathcal{O}$ prim, $(p) = \mathfrak{p} \cap \mathbb{Z}$ für $p \in \mathbb{Z}$ Primzahl.

(i) $p = 2$: Wir haben

$$\mathcal{O}/(2) = \mathbb{Z}[X]/(X^2+5, 2) = \mathbb{F}_2[X]/X^2+1 = \mathbb{F}_2[X]/(X+1)^2$$

Also ist (2) selbst kein Primideal von $\mathcal{O}$. Es gibt genau ein Primideal, das 2 enthält. Modulo 2 wird es von $X+1$ erzeugt, also $P_2 = (2, \sqrt{-5}+1)$.

(ii) $p = 3$

$$\begin{aligned}\mathcal{O}/(3) = \mathbb{Z}[X]/(X^2+5, 3) = \mathbb{F}_3[X]/X^2-1 = \mathbb{F}_2[X]/(X+1)(X-1)\\ = \mathbb{F}_3[X]/X-1 \times \mathbb{F}_3[X]/X+1\end{aligned}$$

Es gibt zwei Primideale, die 3 enthalten, nämlich $P_3 = (3, \sqrt{-5}+1)$, $P_3' = (3, \sqrt{-5}-1)$. Es gilt $(3) = P_3 P_3'$ in $\mathcal{O}$. Wichtig für diese Berechnung war nur, dass 5 eine Quadratzahl modulo 3 war.

(iii) $p = 5$

$$\mathcal{O}/(5) = \mathbb{Z}[X]/(X^2+5, 5) = \mathbb{F}_5[X]/X^2$$

$P_5 = (5, \sqrt{-5}) = (\sqrt{-5})$ ist das einzige Primideal, das 5 enthält. Es gilt $(5) = P_5^2$.

(iv) $p = 7$

$$\begin{aligned}\mathcal{O}/(7) = \mathbb{Z}[X]/(X^2+5, 7) = \mathbb{F}_3[X]/X^2-2 = \mathbb{F}_2[X]/(X+3)(X-3)\\ = \mathbb{F}_3[X]/X-3 \times \mathbb{F}_3[X]/X+3\end{aligned}$$

$P_7 = (7, \sqrt{-5} \pm 3)$ (wie Fall $p = 3$)

(v) $p = 11$ In diesem Fall ist 5 keine Quadratzahl modulo 11, das Ideal (11) ist prim in $\mathcal{O}$.

beim Rechnen modulo Hauptideale gilt also: $P_2^2 \sim 1$, $P_5 \sim 1$, $P_3 \sim (P_3')^{-1}$, $P_{11} \sim 1$ etc.
Frage: Ist P_2 ein Hauptideal? Falls $P_2 = (\alpha)$, so gibt es x, y mit

$$\begin{aligned}x\alpha = 2 \Rightarrow N(x)N(\alpha) = N(2) = 4\\ y\alpha = \sqrt{-5}+1 \Rightarrow N(y)N(\alpha) = N(\sqrt{-5}+1) = 6\end{aligned}$$

Dies impliziert $N(\alpha) = 2$. Sei $\alpha = a_1 + a_2\sqrt{-5}$ ($a_i \in \mathbb{Z}$)

$$a_1^2 - 5a_2^2 = 2$$

Dies führt also auf die Theorie der Lösbarkeit der quadratischen Gleichungen in $\mathbb{Z}$. Die obige ist modulo 4 nicht lösbar, also ist P_2 kein Hauptideal.

Man sieht bereits in diesem Beispiel: die Bestimmung der Klassengruppe ist schwierig, da sie unendlich viele Erzeuger und unendlich viele Relationen hat!

Die Frage nach Primidealen in $\mathbb{Z}[\sqrt{d}]$ führt auf die Frage, ob d eine Primzahl ist modulo p oder nicht. Dies wird durch Gauß' quadratisches Reziprozitätsgesetzt zufriedenstellend beantwortet.

Übungsaufgabe. *Bestimmen Sie die Primideale von* $\mathbb{Z}[i]$

Kapitel 4

Gittertheorie

Unser Ziel ist es, die Endlichkeit der Klassengruppe zu zeigen.

Abstrakte Theorie

Definition 4.1. *Eine Untergruppe $H \subset \mathbb{R}^n$ heißt* diskret*, wenn für jede kompakte Teilmenge $K \subset \mathbb{R}^n$ der Schnitt $K \cap H$ endlich ist.*

Eine Teilmenge K ist kompakt, wenn jede offene Überdeckung eine endlich Teilüberdeckung hat. In $\mathbb{R}^n$ ist dies äquivalent dazu, dass jede Folge in K ein konvergente Teilfolge hat, oder dazu, dass sie beschränkt und abgeschlossen ist (Heine-Borel).

Beispiel. $\mathbb{Z} \subset \mathbb{R}$ ist diskret.

Satz 4.2. *Sei $H \subset \mathbb{R}^n$ diskret. Dann wird H von r Vektoren erzeugt, die linear unabhängig über $\mathbb{R}$ sind. Insbesondere gilt $H \cong \mathbb{Z}^r$ mit $\leq n$.*

Beweis: Seien $e_1, \ldots, e_r \in H$ eine maximale $\mathbb{R}$-linear unabhängige Teilmenge. Sei

$$P = \{\sum \alpha_i e_i \mid 0 \leq \alpha_i \leq 1\} \subset \mathbb{R}^n$$

Diese Menge ist kompakt, also $P \cap H$ endlich. Sei $x \in H$. Dann ist $x = \sum \lambda_i e_i$ mit $\lambda_i \in \mathbb{R}$. Sei $x_1 = x - \sum[\lambda_i]e_i$, wobei $[\alpha]$ die kleinste ganze Zahl kleiner gleich α ist (Gaußklammer), also $0 \leq \alpha - [\alpha] < 1$. Dies bedeutet $x_1 \in P \cap H$. Also erzeugen die e_i zusammen mit $P \cap H$ die Gruppe H. Wir konstruieren eine unendliche Folge $x_j \in H \cap P$, nämlich

$$x_j = jx - \sum[j\lambda_i]e_i$$

wobei $[\alpha]$ die kleinste ganze Zahl kleiner gleich α ist (Gaußklammer), also $0 \leq \alpha - [\alpha] < 1$. Da $P \cap H$ endlich ist, gibt es zwei Indices $j \neq k$ mit $x_j = x_k$. Es folgt

$$j\lambda_i - [j\lambda_i] = k\lambda_i - [k\lambda]_i \Leftrightarrow (j-k)\lambda_i = ([j\lambda_i] - [k\lambda])$$

Insbesonder ist λ_i rational. Damit liegt die endlich erzeugte abelsche Gruppe H in dem $\mathbb{Q}$-Vektorraum, der von $e_1, \ldots, e_r$ erzeugt wird. Es folgt $H \cong \mathbb{Z}^r$. Die Erzeuger von H sind linear unabhängig über $\mathbb{R}$, da $e_1, \ldots, e_r$ es sind. □

Definition 4.3. *Eine diskrete Untergruppe $H \subset \mathbb{R}^n$ vom Rang n heißt* Gitter. *Sei $e_1, \ldots, e_n$ eine Basis von H. Dann heißt*

$$P_e = \{\sum \alpha_i e_i \mid 0 \leq \alpha_i < 1\}$$

Fundamentalparallelogramm *von H.*

Beispiel. $\mathbb{Z}^n \subset \mathbb{R}^n$ ist ein Gitter.

Lemma 4.4. *Das Volumen von P_e bezüglich des Standardlebesgue-Maßes μ auf $\mathbb{R}^n$ ist unanhängig von der Wahl der Basis.*

Beweis: μ induziert ein Maß $\overline{\mu}$ auf $\mathbb{R}^n/H$. Es gilt $\overline{\mu}(\mathbb{R}^n/H) = \mu(P_e)$. Oder: zweite Basis in Termen der ersten ausdrücken. Sie und ihr Inverses sind ganzzahlig, also die Determinante ± 1. Der Absolutbetrag der Determinante taucht als Übergangsfaktor auf. (Forster Analysis 3, Bsp. (5.3)). □

Theorem 4.5 (Minkowski). *Sei $H \subset \mathbb{R}^n$ ein Gitter, $S \subset \mathbb{R}^n$ messbar mit $\mu(S) > \mathrm{vol}(H)$. Dann gibt es $x, y \in S$, $x \neq y$ mit $x - y \in H$.*

Beweis: Sei $e_1, \ldots, e_n$ eine Basis von H, P_e das Fundamentalparallelogramm. Es gilt

$$S = \dot{\bigcup_{h \in H}} S \cap (h + P_e)$$

da $\mathbb{R}^n = \bigcup_h h + P_e$. Also gilt

$$\mu(S) = \sum_h \mu(S \cap (h + P_e) = \sum_h \mu((-h + S) \cap P_e) > \mu(P_e)$$

Also können die $(-h+S)\cap P_e)$ nicht paarweise disjunkt sein. Es gibt $h \neq h' \in H$ mit

$$P_e \cap (-h + S) \cap (-h' \cap S) \neq \emptyset$$

Also gibt es $x, y \in S$ mit $-h + x = -h' + y$. Wegen $x - y = h' - h$ liegt die Differenz in H und ist ungleich 0. □

Korollar 4.6. *Sei $H \subset \mathbb{R}^n$ ein Gitter, S messbare Teilmenge von $\mathbb{R}^n$, symmetrisch bezüglich 0 (d.h. $x \in S \Leftrightarrow -x \in S$) und konvex. Sei entweder*

(i) $\mu(S) > 2^n \mathrm{vol}(H)$ *oder*

(ii) $\mu(S) \geq 2^n \mathrm{vol}(H)$, *$S$ kompakt*

Dann enthält $S \cap H$ einen Punkt ungleich 0.

Beweis: Erster Fall: Sei $S' = \frac{1}{2}S$, also

$$\mu(S') = \frac{1}{2^n}\mu(S) > \mathrm{vol}(H)$$

Nach dem Theorem von Minkowski gibt es $x, y \in S'$ mit $0 \neq z = x - y \in H$. Es gilt $z = \frac{1}{2}(2x + (-2y)) \in S \cap H$ wie gewünscht.
Zweiter Fall: Wende den ersten Fall an auf $(1+\varepsilon)S$ mit $\varepsilon > 0$. Es folgt

$$(H \setminus \{0\}) \cap (1+\varepsilon)S \neq \emptyset$$

Dabei ist der Schnitt endlich da H diskret und S kompakt. Dann ist auch

$$\bigcap_{\varepsilon > 0} (H \setminus \{0\}) \cap (1+\varepsilon)S \neq \emptyset$$

Ein Element im Schnitt liegt in $H \setminus \{0\}$ und in $\bigcap_{\varepsilon>0}(1+\varepsilon)S = S$. □

Die kanonische Einbettung

Sei $K/\mathbb{Q}$ ein Zahlkörper, $n = [K : \mathbb{Q}]$. Dann gibt es n verschiedene Körperhomomorphismen

$$\sigma_i : K \to \mathbb{C}$$

Beispiel. $K = \mathbb{Q}(\sqrt{d})$, $\sigma_i(\sqrt{d}) = \pm\sqrt{d}$.

Zwei Fälle sind zu unterscheiden: $\sigma_i = \overline{\sigma_i}$ (komplexe Konjugation) genau dann, wenn $\sigma_i(K) \subset \mathbb{R}$. In diesem Fall heißt σ_i *reelle Einbettung.*
Andernfalls ist $\overline{\sigma_i} = \sigma_j$ für ein $j \neq i$. In diesem Fall heißt σ_i *komplexe Einbettung.* σ_i und σ_j sind konjugiert.

Bemerkung. Jedes σ_i induziert eine Absolutbetrag auf K via $|x| = |\sigma_i(x)|$. Die Komplettierung von K bezüglich dieses Absolutbetrages ist dann $\mathbb{R}$ bzw. $\mathbb{C}$ für reelle bzw. komplexe Einbettungen.

Sei r_1 die Anzahl der reellen Einbettungen von K, r_2 die Anzahl der Paare von komplexen Einbettungen, also $n = r_1 + 2r_2$. Wir nummerieren die σ_i so, dass σ_i reell für $i \leq r_1$, σ_{r_1+i} konjugiert zu $\sigma_{r_1+r_2+i}$. Wir schreiben $r = r_1 + r_2$.

Beispiel. $K = \mathbb{Q}(\sqrt{d})$ $n = 2$. Falls $d > 0$: $r_1 = 2, r_2 = 0, r = 2$. Falls $d < 0$: $r_1 = 0, r_2 = 1, r = 1$.

Definition 4.7. *Die* kanonische Einbettung *ist*

$$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$$

via $\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha))$.

Bemerkung. σ ist ein injektiver Ringhomomorphismus.

Satz 4.8. *Sei $M \subset K$ freier $\mathbb{Z}$-Untermodul vom Rang n, $x_1, \dots, x_n$ Basis von M. Dann ist $\sigma(M)$ ein Gitter in $\mathbb{R}^n$ mit Volumen*

$$\mathrm{vol}(\sigma(M)) = 2^{-r_2} |\det(\sigma_i(x_j)_{i,j=1}^n)|$$

Beweis: $\sigma(x_i)$ ist der Vektor

$$(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \mathrm{Re}\sigma_{r_1+1}(x_i), \mathrm{Im}\sigma_{r_1+1}(x_i), \dots, \mathrm{Re}\sigma_r(x_i), \mathrm{Im}\sigma_r(x_i))$$

Zu berechnen $\mathrm{vol}(\sigma(M)) = |\det(\sigma(x_i))|$. Falls diese Zahl ungleich 0 ist, sind die $\sigma(x_i)$ linear unabhängig über $\mathbb{R}$ und ein Gitter.
Es gilt $\mathrm{Re}z = \frac{1}{2}(z + \overline{z}), \mathrm{Im}z = \frac{1}{2i}(z - \overline{z})$. Es folgt

$$\begin{aligned}(\mathrm{Re}\sigma_{r_1+j}(x_i), \mathrm{Im}\sigma_{r_1+j}(x_i)) &= (\frac{1}{2}(\sigma_{r_1+j}(x_i) + \overline{\sigma_{r_1+j}(x_i)}), \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \overline{\sigma_{r_1+j}(x_i)}) \\ &= \frac{1}{2}(\sigma_{r_1+j}(x_i) + \sigma_{r+j}(x_i)), \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \sigma_r(x_i))\end{aligned}$$

Hieraus berechnen wird den Absolutbetrag der Determinante via Multilinearlität. Im ersten Schritt ignorieren wir den Faktor $\frac{1}{i}$, der den Betrag 1 hat. Dann beachten wir

$$\det(\dots, \frac{1}{2}(a+b), \frac{1}{2}(a-b), \dots) = -\frac{1}{2}\det(\dots, (a,b), \dots)$$

und schließlich sortieren wir die σ_i um. Wir erhalten

$$|\det(\sigma(x_i)) = |\frac{1}{2^{r_2}}\det(\sigma_j(x_i))|$$

Diese Determinante ist ungleich 0, da die Charaktere σ_j linear unabhängig sind. □

Korollar 4.9. *Sei $\mathcal{O} \subset K$ der Ganzheitsring. Dann ist $\sigma(\mathcal{O}) \subset \mathbb{R}^n$ ein Gitter mit Volumen*

$$\mathrm{vol}(\sigma(\mathcal{O})) = 2^{-r_2} d^{1/2}$$

wobei $(d) = \mathcal{D}_{\mathcal{O}/\mathbb{Z}}$, $d \in \mathbb{N}_0$ die absolute Diskriminante *ist.*

Beweis: Im Beweis von Satz 2.11 haben wir

$$D(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$$

gezeigt. $D(x_1, \dots, x_n) = \det(\mathrm{Tr}_{\mathcal{O}/\mathbb{Z}}(x_i x_j))$ war die Diskriminante, $\mathcal{D}_{\mathcal{O}/\mathbb{Z}}$ das von ihre erzeugte Hauptideal. □

Korollar 4.10. *Sei $I \subset \mathcal{O}$ ein Ideal ungleich 0. Dann ist $\sigma(I)$ ein Gitter mit Volumen*

$$\mathrm{vol}(\sigma(I)) = 2^{r_2} d^{1/2} N(I)$$

wobei $N(I) = |\mathcal{O}/I$ die Norm des Ideals ist.

Beweis: Auch $I \subset \mathcal{O}$ ist ein endlich erzeugter $\mathbb{Z}$-Modul torsionsfrei vom Rang höchsten n. Wegen $\mathcal{O}\alpha \subset I$ für alle $\alpha \in I$ ist der Rang genau n. Auch $\sigma(I)$ ist ein Gitter. Wir wählen eine Basis $x_1, \ldots, x_n$ von $\mathcal{O}$ nach dem Elementarteilersatz so, dass gleichzeitig $\lambda_1 x_1, \ldots, \lambda_n x_n$ für gewisse $\lambda_i \in \mathbb{N}$ eine Basis von I ist. Damit gilt

$$N(I) = \lambda_1 \ldots \lambda_n$$

Andererseits ist

$$\mathrm{vol}(\sigma(I)) = \frac{1}{2^{r_2}} |\det(\sigma(\lambda_i x_i))| = \frac{1}{2^{r_2}} |\lambda_1 \ldots \lambda_n \det(\sigma(x_i))| = N(I)\mathrm{vol}(\sigma(\mathcal{O}))$$

□

Lemma 4.11. *Die Norm ist multiplikativ auf Idealen ungleich* 0. *Für* $x \in \mathcal{O}$ *gilt* $N((x)) = |N_{K/\mathbb{Q}}(x)|$.

Beweis: Ist $I = \prod \mathfrak{p}_i^{v_i}$, $I' = \mathfrak{p}_1^{-1} I$ so folgt

$$0 \; \mathfrak{p}_1^{v_1}/\mathfrak{p}_1^{v_1-1}\mathcal{O}/I \to \mathcal{O}/I' \to 0 \; .$$

$\mathfrak{p}_1^{v_1}/\mathfrak{p}_1^{v_1-1}$ ist ein $\mathcal{O}/\mathfrak{p}_1$-Vektorraum, da die $\mathcal{O}$-Operation über $\mathcal{O}/pf$ faktorsiert. Die Dimension muss 1 sein nach der Strukturtheorie von Idealen über $\mathcal{O}$. Alsos ist $|\mathfrak{p}_1^{v_1}/\mathfrak{p}_1^{v_1-1}| = |\mathcal{O}/\mathfrak{p}|$.
Sei nun $I = (x)$. Sei wie im Beweis des Korollars $x_1, \ldots, x_n$ eine Basis von $\mathcal{O}$, so dass $\lambda_1 x_1, \ldots, \lambda_n x_n$ eine Basis von I ist. Sei $u : K \to K$ durch $x_i \mapsto \lambda_i x_i$ gegeben. Sei $v : K \to K$ durch $x_i \mapsto x/\lambda_i x_i$ gegeben. Dann gilt $v \circ u = m_x$, also

$$N_{K/\mathbb{Q}}(x) = \det(v)\det(u) = \pm N(I)$$

denn v ist eine Basiswechselmatrix auf I. □

Satz 4.12. *Sei* K *ein Zahlkörper vom Grad* n *über* $\mathbb{Q}$, r_1 *die Anzahl der reellen,* r_2 *die Anzahl der Paare von komplexen Einbettungen,* d *die Diskriminante über* $\mathbb{Q}$. *Sei* I *ein Ideal des Ganzheitsrings. Dann enthält* I *ein Element* $x \neq 0$ *mit*

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} N(I)$$

Beweis: Wir betrachten die kanonische Einbettung $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$. Sei $t > 0$ reell,

$$B_t = \left\{ (y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum |y_i| + 2 \sum |z_j| \leq t \right\}$$

ist kompaktisch, konvex, symmetrisch bezüglich 0.

Behauptung. $\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$

Diese Formel wird durch Induktion nach r_1, r_2 gezeigt. Sei $V(r_1, r_2, t) = \mu(B_t)$.

(i) Es gilt

$$V(1,0,t) = \mu(\{y_1 \mid |y_1| \leq t\}) = 2t = 2^1(\pi/2)^0\frac{t^1}{1!}$$
$$V(0,1,t) = \mu(\{z_1 \mid 2|z_1| \leq t\}) = \pi(t/2)^2 = 2^0(\pi/2)^1\frac{t^2}{2!}$$

(ii) $r_1 \mapsto r_1 + 1$

$$\begin{aligned}
V(r_1+1,r_2,t) &= \mu(\{(y_0,\ldots,y_{r_1},z_1,\ldots,z_{r_2}) \mid \ldots\} \\
&= \int_{\mathbb{R}} V(r_1,r_2,t-|y_0|)dy_0 \\
&= \int_{-t}^{t} 2^{r_1}(\pi/2)^{r_2}\frac{(t-|y_0|)^n}{n!}dy_0 \\
&= 2^{r_1}(\pi/2)^{r_2}\frac{2}{n!}\int_0^t (t-y_0)^n dy_0 \\
&= 2^{r_1+1}(\pi/2)^{r_2}\frac{1}{n!}\left.\frac{-(t-y_0)^{n+1}}{n+1}\right|_0^t \\
&= 2^{r_1+1}(\pi/2)^{r_2}\frac{t^{n+1}}{(n+1)!}
\end{aligned}$$

(iii) $r_2 \mapsto r_2 + 1$

$$\begin{aligned}
V(r_1,r_2+1,t) &= \mu(\{(y_1,\ldots,y_{r_1},z_0,\ldots,z_{r_2}) \mid \ldots\} \\
&= \int_{\mathbb{C}} V(r_1,r_2,(t-2|z_0|)d\mu(z_0) \\
&= \int_{|z_0|\leq t/2} V(r_1,r_2,(t-2|z_0|)d\mu(z_0) \\
&= \int_0^{t/2}\int_0^{2\pi} 2^{r_1}(\pi/2)^{r_2}\frac{(t-2\varrho)^n}{n!}\varrho d\varrho d\theta \\
&= 2^{r_1}(\pi/2)^{r_2}\frac{2\pi}{n!}\int_0^{t/2}(t-2\varrho)^n\varrho d\varrho \\
&= 2^{r_1}(\pi/2)^{r_2+1}\frac{t^{n+2}}{(n+2)!}
\end{aligned}$$

wobei in Polarkoordinaten $z_0 = \varrho e^{i\theta}$, $d\mu(z_0) = \varrho d\varrho d\theta$, und in der letzten

Zeile partielle Integration $\int u'v = uv - \int uv'$ benutzt wird

$$\begin{aligned}\int_0^{t/2} (t-2\varrho)^n \varrho d\varrho &= \int_0^x (t-x)^n x/2 dx/2 \\ &= 1/4 \left[\frac{-(t-x)^{n+1}}{n+1} x \Big|_0^x - \int_0^x \frac{-(t-x)^{n+1}}{(n+1)} dx \right] \\ &= 1/4 \left[0 - \frac{(t-x)^{n+2}}{(n+1)(n+2)} \Big|_0^x \right] \\ &= 1/4 \frac{t^{n+2}}{(n+1)(n+2)}\end{aligned}$$

Damit ist die Formel für das Volumen verifiziert. Wähle nun t so, dass $\mu(B_t) = 2^n \mathrm{vol}(\sigma(I))$, d.h.

$$2^{r_1}(\pi/2)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} d^{1/2} N(I) \Rightarrow t^n = 2^{n-r_1} \pi^{-r_2} n! d^{1/2} N(I)$$

Aus dem Theorem von Minkowski, genauer Korollar 4.6 folgt die Existenz eines $0 \neq x \in I$ mit $\sigma(x) \in B_t$ so dass

$$\begin{aligned}|N(x)| = \prod_{i=1}^n |\sigma_i(x)| &= \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2 \\ &\leq \left[1/n \sum_{i=1}^n |\sigma_i(x)| + 2/n \sum_{i=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right]^n \\ &\leq (t/n)^n \\ &= 2^{n-r_1} \pi^{-r_2} n! / n^n d^{1/2} N(I)\end{aligned}$$

da das geometrische Mittel kleiner ist als das arithmetische Mittel. □

Korollar 4.13. *Jede Idealklasse von K enthält ein ganzes Ideal J mit*

$$N(J) \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2}$$

Beweis: Sei J' ein Ideal, ohne Einschränkung ist $I = J'^{-1}$ ein ganzes Ideal. Sei x wie im Satz, $J = xJ' = xI^{-1}$. Es gilt

$$N(J) = N(x)N(I)^{-1} \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2} \frac{N(I)}{N(I)}$$

□

Theorem 4.14 (Dirichlet). *Die Klassengruppe eines Zahlkörpers ist endlich.*

Beweis: Nach Korollar 4.13 genügt es, Klassen von Idealen zu betrachten, deren Norm kleiner gleich einer Konstante C ist. Also genügt es zu zeigen, dass es nur endlich viele Ideale mit $N(J) = q < C$ gibt für ein festes q. Es gilt

$$N(J) = |\mathcal{O}/J| = q \Rightarrow q \in J$$

Die Ideale von $\mathcal{O}$ mit $q \in J$ entsprechen genau den Idealen von $\mathcal{O}/(q)$. Dies ist ein endlicher Ring, hat also auch nur endlich viele Ideale. □

Beispiel. $K = \mathbb{Q}(\sqrt{-5})$, $r_1 = 0$, $r_2 = 1$, $n = 2$, Basis $1, \sqrt{-5}$. Also folgt

$$d = |\det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}|^2 = |-\sqrt{-5} - \sqrt{-5}|^2 = 4 \cdot 5 = 20$$

Die Konstante aus dem Beweis ist also

$$C = \frac{4}{\pi}\frac{2}{4}2\sqrt{5} = 4/\pi\sqrt{5} = 2,847\ldots$$

Für $1 \in J$ ist $J = A$ das triviale Element. Ideale mit $2 \in J$ entsprechen den Idealen von $\mathbb{Z}[\sqrt{-5}]/(2) = \mathcal{O}/P_2^2$ wobei P_2 das eindeutige Primideal ist, das 2 enthält. Die Klassengruppe wird also von P_2 erzeugt. Es gilt $P_2^2 = (2)$, also die Relation $P_2^2 \sim 1$. Da $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring ist, ist die Klassengruppe isomorph zu $\mathbb{Z}/2$.

Übungsaufgabe. *Bestimmen Sie mit dieser Methode die Klassengruppe von* $\mathbb{Q}(i)$.

Korollar 4.15. *Sei K ein Zahlkörper vom Grad n über $\mathbb{Q}$ und Diskriminante d. Für $n \geq 2$ gilt*

$$d \geq \frac{\pi}{3}\left(\frac{(3\pi}{4}\right)^{n-1}$$

Der Quotient $n/\log d$ wird durch eine Konstante unabhängig von K beschränkt.

Beweis: Sei wie im Beweis des Theorems J ein ganzes Ideal mit

$$N(J) \leq (4/\pi)^{r_2}\frac{n!}{n^n}d^{1/2}$$

Wegen $N(J) \geq 1$ folgt

$$\begin{aligned} d^{1/2} &\geq (\pi/4)^{r_2}n^n/n! \Rightarrow \\ d &\geq (\pi/4)^{2r_2}n^{2n}/(n!)^2 \geq (\pi/4)^n n^{2n}/(n!)^2 = a_n \end{aligned}$$

da $n \geq 2r_2$ und $\pi/4 < 1$.

Behauptung. $a_n \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$.

Wir zeigen dies induktiv. Für $n = 2$ gilt wie gewünscht

$$a_2 = \pi^2/4^2 \cdot 2^4/2^2 = \pi^2/4 \ .$$

Nun $a_n \mapsto a_{n+1}$:

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{\pi}{4} \cdot \frac{(n+1)^{2(n+1)} n!^2}{n^{2n}(n+1)^2} \\ &= \pi/4 \cdot \frac{(n+1)^{2n}}{n^{2n}} = \pi/4(1+1/n)^{2n} \\ &\geq \pi/4 \cdot (1 + 2n \cdot 1/n) = \pi/4 \cdot 3\end{aligned}$$

Die zweite Aussage folgt durch Logarithmieren der Ungleichung. □

Theorem 4.16 (Hasse-Minkowski). *Sei $K \neq \mathbb{Q}$ ein Zahlkörper. Dann ist seine Diskriminante ungleich* 1*.*

Beweis: $d \geq \pi/3 \cdot (3\pi/4)^{n-1} > 1$ □

Bemerkung. Wir werden später darauf zurückkommen, warum diese Aussage wichtig ist, Stichwort Verzweigung. Das Theorem besagt, dass alle Zahlkörper verzweigt über $\mathbb{Q}$ sind.

Theorem 4.17 (Hermite). *Bis auf Isomorphie gibt es nur endlich viele Zahlkörper mit gegebenener Diskriminante.*

Beweis: Nach Korollar 4.15 gilt $n \leq d\alpha$ für eine Konstante α, d.h. der Grad ist beschränkt. Es genügt also zu zeigen, dass es nur endlich viele Körper mit gegebenem d, n, r_1, r_2 gibt. Sei zunächst $r_1 > 0$. Wir betrachten $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definiert durch

$$\{|y_1/2| \leq C/2, |y_i| \leq 1/2 \text{ für } i = 2, \ldots, r_1, |z_j| \leq 1/2 \text{ für } j = 1, \ldots, r_2\}$$

wobei $C = (\pi/4)^{-r_2} 2^{n-r_2} d^{1/2}$. Die Menge B ist konvex, kompakt und punktsymmetrisch bezüglich 0. Das Volumen ist

$$\mu(B) = C(1)^{r_1 - 1}(\pi/4)^{r_2} = 2^n \text{vol}(\sigma(\mathcal{O}))$$

nach Wahl von C. Nach Korollar 4.6 gibt es $0 \neq x \in \mathcal{O} \cap B$.

Behauptung. $K = \mathbb{Q}(x)$

Nach Voraussetzung ist $|\sigma_i(x)| \leq 1/2$ für alle $i \neq 1$. Wege

$$N(x) = \prod_{i=1}^{n} |\sigma_i(x)| \geq 1$$

folgt $\sigma_1(x) \geq 1$, insbesondere $\sigma_1(x) \neq \sigma_i(x)$ für alle $i \neq 1$. Wäre $\sigma_i(x) = \sigma_j(x)$ so folgt $\sigma_1 \sigma_i^{-1} \sigma_i(x) = \sigma_1 \sigma_i^{-1} \sigma_j(x)$. Dies ist unmöglich. Alle $\sigma_i(x)$ sind unterschiedlich, also gilt $[\mathbb{Q}(x) : \mathbb{Q}] = n$. Dies zeigt die Behauptung.

Wegen $\sigma(x) \in B$ sind die $\sigma_i(x)$ beschränkt und damit auch alle Koeffizienten des Minimalpolynoms von x. Es gibt nur endlich viele Polynome in $\mathbb{Z}[X]$ vom Grad n mit beschränkten Koeffizienten, also auch nur endliche viele mögliche x. Es bleibt der Fall $r_1 = 0$. In diesem Fall benutzen wir

$$B = \{|\mathrm{Im} z_1| \leq C, |\mathrm{Re} z_1| \leq 1/2, |z_i| \leq 1/2 \text{ für } i = 2, \ldots, r_2\}$$

so dass $\mu(B) = 2^n \mathrm{vol}(B)$. Wie im ersten Fall finden wir $x \in \sigma(\mathcal{O}) \cap B$ mit $|\sigma_1(x)| \geq 1$. Wiederum ist $\sigma_1(x) \neq \sigma_i(x)$ für $i \neq 1$. Wegen $\mathrm{Re}\sigma_1(x) \leq 1/2$ ist $\mathrm{Im}\sigma_1(x) \neq 0$, also ist auch $\sigma_1(x) \neq \overline{\sigma}_1(x)$. Wieder ist x primitives Element. □

Definition 4.18. *Sei K ein Zahlkörper. Die* Einheiten *von K sind die invertierbaren Elemente des Ganzheitsrings.*

Beispiel. $1, -1, i, -i$ sind Einheiten von $\mathbb{Q}(i)$. In $\mathbb{Q}(\sqrt{3})$ ist $2+\sqrt{3}$ eine Einheit mit Inversem $2 - \sqrt{3}$.

Lemma 4.19. *$x \in K$ ist eine Einheit genau dann, wenn x ganz ist und $N(x) = \pm 1$.*

Beweis: Ist x eine Einheit, so ist $1 = N(xx^{-1}) = N(x)N(x)^{-1}$. Da die Norm eines ganzen Elementes ganz ist, folgt $N(x) = \pm 1$. Sei umgekehrt $x \in \mathcal{O}$ mit $N(x) = \pm 1$. Das charakteristische Polynom

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

hat ganze Koeffizienten, speziell $a_0 = \pm N(x) = \pm 1$. Es folt

$$\pm x(x^{n-1} + \cdots + a_1) = 1$$

Damit ist x eine Einheit. □

Theorem 4.20 (Dirichlet). *Sei K ein Zahlkörper, r_1 die Zahl der reellen und r_2 die Zahl der komplexen Einbettungen, $r = r_1 + r_2$. Die Gruppe $\mathcal{O}^*$ der Einheiten von K ist isomorph zu*

$$\mathcal{O}^* \cong \mathbb{Z}^{r-1} \times G$$

wobei G die Gruppe der Einheitswurzeln in K ist, insbesondere eine endliche, zyklische Gruppe.

Beispiel. Für $K = \mathbb{Q}(i)$ gilt $\mathcal{O}^* \cong G = \{\pm 1, \pm i\}$, da $r = 0+1$. Für $K = \mathbb{Q}(\sqrt{3})$ gilt $\mathcal{O}^* \cong \mathbb{Z}$, da $r = 2 + 0$. Tatsächlich ist $2 + \sqrt{3}$ ein Erzeuger. Die Frage nach Erzeugern von $\mathbb{Q}(\sqrt{d})$ für $d > 0$ führt auf die Theorie der *Pellschen Gleichung*, die mit der Theorie der Kettenbrüche behandelt werden kann.

Beweis: Seien wie bisher $\sigma_1, \ldots, \sigma_{r_1}$ die reellen Einbettungen, $\sigma_{r_1}, \ldots, \sigma_r$ nichtkonjugierte komplexe Einbettungen. Die *logarithische Einbettung* $L : K^* \to \mathbb{R}^r$ ist

$$L : x \mapsto (\log|\sigma_1|, \ldots, \log|\sigma_r|) \in \mathbb{R}$$

L ist ein Gruppenhomomorphismus.
Sei $B \subset \mathbb{R}^r$ kompakt, $B' = L^{-1}(B) \cap \mathcal{O}^*$. Dann gibt es eine Konstante C, so dass für alle $x \in B'$ und $i = 1, \ldots, n$ gilt

$$|\sigma_i(x)| \leq C$$

Damit sind die Koeffizienten von

$$P(X) = (X - \sigma_1(x))(X - \sigma_2(x)) \ldots (X - \sigma_n(x))$$

beschränkt. Gleichzeitig sind sie ganz, da $x \in \mathcal{O}$. Es gibt also nur endliche viele mögliche P, daher ist B' endlich.
Dies gilt insbesondere für $G = L^{-1}(0) \cap \mathcal{O}^*$. Dies ist eine endliche Gruppe, besteht also nur aus endlich vielen Einheitswurzeln. Insbesondere ist sie zyklisch (Algebra). Ist umgekehrt ω eine Einheitswurzel, so gilt $|\sigma_i(\omega)| = 1$ für alle i. Damit liegt ω im Kern von L.
Nun studieren wir das Bild von $L(\mathcal{O}^*) \subset \mathbb{R}^r$. Nach unserer Vorüberlegung ist dies eine diskrete Untergruppe, also $L(\mathcal{O}^*) \cong \mathbb{Z}^s$ für $s \leq r$.

Behauptung. $s \leq r - 1$.

Für $x \in \mathcal{O}^*$ gilt

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_2} \sigma_i(x)\overline{\sigma_i(x)}$$

Hieraus folgt

$$L(x) \in W = \{(y_1, \ldots, y_r) \in \mathbb{R}^r \mid \sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_2} y_j = 0\}$$

W hat Dimension $r - 1$, $L(\mathcal{O}^*)$ ist eine diskrete Untergruppe, also $s \leq r - 1$.

Behauptung. $L(\mathcal{O}^*)$ *enthält* $r - 1$ *linear unabhängige Elemente.*

Äquivalent: Für jede lineare Abbildung $f : W \to \mathbb{R}$ mit $f \neq 0$ gibt es $u \in \mathcal{O}^*$ mit $f(L(u)) \neq 0$. Wir identifizieren $W \cong \mathbb{R}^{r-1}$ via des Isomorphismus $(y_1, \ldots, y_r) \mapsto (y_1, \ldots, y_{r-1})$. Also schreibt sich $f(y_1, \ldots, y_r) = c_1 y_1 + \ldots c_{r-1} y_{r-1}$ für $c_i \in \mathbb{R}$. Wir wählen

$$\alpha \geq \left(\frac{2}{\pi}\right)^{r_2} d^{1/2}, \qquad \beta > \sum_{i=1}^{r-1} c_i \log \alpha$$

Wir werden eine Folge $x_h \in \mathcal{O} \setminus \{0\}$ konstruieren mit

$$|f(L(x_h)) - 2\beta h| < \beta, |N(x_h) < \alpha$$

Aus der ersten Bedingung folgt $(2h-1)\beta < f(L(x_h)) < (2h+1)\beta$, also sind die $f(L(x_h))$ paarweise verschieden. Die $|N(x_h)|$ sind beschränkt und ganz, also gibt

es nur endliche viele Ideale (x_h). Also gibt es zwei Indizes h, h' mit $(x_h) = (x_{h'})$. Dies bedeutet, dass es $u \in \mathcal{O}^*$ gibt mit $x_h = ux_{h'}$. Außerdem

$$f(L(u)) = f(L(x_h)) - f(L(x_{h'})) \neq 0$$

Damit wäre das Theorem gezeigt.
Wir konstruieren nun die x_h. Wähle $\lambda_1, \ldots, \lambda_r$ mit

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r} \lambda_j^2 = \alpha, \qquad \sum_{i=1}^{r-1} c_i \log \lambda_i = 2\beta h$$

Dies ist möglich für $r \geq 2$. Im Fall $r = 1$ ist $s = 0$, und es ist nichts zu zeigen. Sei nun

$$B = \{(y_i, j_j) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_i| \leq \lambda_i, |z_j| \leq \lambda_{j+r_r}\}$$

Diese Menge ist kompakt, symmetrisch und konvex. Sie hat das Maß

$$\begin{aligned}\mu(B) = \prod_{i=1}^{r_1}(2\lambda_i) \prod_{j=1}^{r_2} \pi\lambda_j^2 &= 2^{r_1}\pi^{r_2}\alpha \\ &\geq 2^{r_1}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2} d^{1/2} = 2^{n-r_2}d^{1/2} = 2^n \mathrm{vol}(\sigma(\mathcal{O}))\end{aligned}$$

Nach dem Theorem von Minkowski, Korollar 4.6 gibt es $x \in \mathcal{O}$, $x \neq 0$ mit $|\sigma_i(x)| \leq \lambda_i$ für alle i. Andererseits

$$|\sigma_i(x)| = \frac{|N(x)|}{\prod_{j \neq i} |\sigma_j(x)|} \geq \frac{1}{\prod_{j \neq i} \lambda_j} = \alpha^{-1}\lambda_i$$

Also

$$\begin{aligned}\lambda_i \alpha^{-1} \leq |\sigma_i(x)| \leq \lambda_i \Rightarrow \\ \log \lambda_i - \log \alpha \leq \log |\sigma_i(x)| \leq \log \lambda_i \Rightarrow \\ \log \alpha \geq \lambda_i - \log |\sigma_i(x)| \geq 0\end{aligned}$$

Wir überprüfen nun die gewünschten Eigenschaften von x:

$$\begin{aligned}|f(L(x)) - 2\beta h| &= |\sum_{i=1}^{r-1} c_i \log |\sigma_i(x)| - \sum_{i=1}^{r-1} c_i \log \lambda_i| \leq \sum_{i=1}^{r-1} |c_i| \log \alpha < \beta \\ |N(x)| &= \prod_{i=1}^{n} |\sigma_i(x)| \leq \prod_{i=1}^{n} \lambda_i = \alpha\end{aligned}$$

□

Kapitel 5

Verzweigung

Sei L/K eine Erweiterung von Zahlkörpern, $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, $\mathcal{O}_L\mathfrak{p}$ das von $\mathfrak{p}$ erzeugte Ideal von $\mathcal{O}_L$. Nach Theorem 3.5 gilt

$$\mathcal{O}_L\mathfrak{p} = \prod_{i=1}^{k} \mathfrak{P}_i^{e_i}$$

wobei die $\mathfrak{P}_i$ Primideale von $\mathcal{O}_L$ sind, nämlich genau diejenigen, die $\mathfrak{p}$ enthalten.

Definition 5.1. $\mathfrak{P}_i$ *heißt* Primideal von L über $\mathfrak{p}$. *Wir sagen auch,* $\mathfrak{P}_i|\mathfrak{p}$ *(* $\mathfrak{P}_i$ *teilt* $\mathfrak{p}$*). Der Exponent* $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ *heißt* Verzweigungsgrad von L/K in $\mathfrak{P}_i$. *Die Erweiterung* L/K *heißt* unverzweigt*, wenn* $e(\mathfrak{P}/\mathfrak{p}) = 1$ *für alle Primideale* $\mathfrak{p}$ *von* K *und alle* $\mathfrak{P}|\mathfrak{p}$. *Der Körper* $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ *heißt* Restklassenkörper *von* K *in* $\mathfrak{p}$. *Die Zahl* $f(\mathfrak{P}_i/\mathfrak{p}) = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$ *heißt* Restklassengrad *von* L/K *in* $\mathfrak{P}_i$.

Satz 5.2 (Gradformel). $[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p})$.

Beweis, erster Versuch: Sei zunächst $K = \mathbb{Q}$, also $\mathcal{O}_K = \mathbb{Z}$, $\kappa((p)) = \mathbb{F}_p$. Dann ist $[L : \mathbb{Q}] = \mathrm{rg}\mathcal{O}_L = \dim_{\mathbb{F}_p} \mathcal{O}_L/(p)$.

$$\mathcal{O}_L/(p) = \mathcal{O}_L/\prod_{i=1}^{k} \mathfrak{P}_i^{e_i}$$

Wegen der Multiplikativität der Norm von Idealen gilt

$$N((p)) = |\mathcal{O}_L/(p)| = \prod_{i=1}^{k} N(\mathfrak{P}_i)^{e_i}$$

Gleichzeitig handelt es sich um $\mathbb{F}_p$-Vektorräume mit

$$|\mathcal{O}_L/(p)| = p^{\dim_{\mathbb{F}_p} \mathcal{O}_L/(p)}, \qquad N(\mathfrak{P}_i) = p^{\dim \mathcal{O}_L/\mathfrak{P}_i}$$

Mit anderen Worten, $p^{[L:\mathbb{Q}]} = \prod_{i=1}^{k} p^{e_i f_i}$.
Für allgemeines K funktioniert dieser Beweis nicht, denn i.a. ist $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul. □

Satz 5.3. *Sei A ein Dedekindring, $\mathfrak{p} \subset A$ ein Primideal, $S = A \setminus \mathfrak{p}$. Dann ist*

$$A_\mathfrak{p} = S^{-1}A = \{\frac{a}{s} \mid a \in A, s \in S\}$$

ein Hauptidealring mit einem einzigen Primideal, nämlich $\mathfrak{P} = S^{-1}\mathfrak{p}$. Es gilt $A/\mathfrak{p} = A_\mathfrak{p}/\mathfrak{P}$.

Beweis: $A_\mathfrak{p}$ ist ebenfalls ein Dedekindring, wie man leicht sieht.

(i) (Integritätsring) $a/s \cdot a'/s' = aa'/(ss') = 0$ genau dann wenn $aa' = 0$, also $a = 0$ oder $a' = 0$.

(ii) (ganz abgeschlossen) $x =\in Q(\mathbb{A}_\mathfrak{p}) = Q(A)$, ganz über $\mathfrak{p}$. Dann genügt es einer Gleichung

$$x^n + \frac{a_1}{s_1}x^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

mit $a_i \in A$, $s_i \in S$. Sei $s = s_1 \dots s_n$. Dann ist sx ganz über A, also $sx \in A$, da A ganz abgeschlossen ist. Es folgt $x = sx/s \in A_\mathfrak{p}$.

(iii) (noethersch) Sei $I \subset A_\mathfrak{p}$ ein Ideal, $I' = A \cap I$. Als Ideal von A ist I' endlich erzeugt.

Behauptung. $S^{-1}I' = I$.

Die Inklusion $\subset$ ist klar. Sei umgekehrt $x = a/s \in I$. Dann liegt $a = sx \in A \cap I$, und daher $x = sa/x \in S^{-1}I$.

(iv) (Dimension 1) Sei nun $I \subset A_\mathfrak{p}$ prim, also $I' = A \cap I$ ein Primideal von A. Dann ist I' entweder 0 oder maximal. Hieraus folgt, dass auch $S^{-1}I'$ entweder 00 ist oder maximal.

Wir bestimmen nund die Menge Primideale von $A_\mathfrak{p}$:

$$\operatorname{Spec} A_\mathfrak{p} = \{S^{-1}\mathfrak{q} \mid \mathfrak{q} \subset A \text{ prim } \}$$

Sei nun $\mathfrak{q} \neq \mathfrak{p}$ ein maximales Ideal, d.h. $\mathfrak{q} \setminus \mathfrak{p} \neq \emptyset$. Sei $s \in \mathfrak{q} \setminus \mathfrak{p} \subset S$. Dann gilt

$$1 = s/s = 1/s \cdot s/1 \in S^{-1}\mathfrak{q} \Rightarrow S^{-1}\mathfrak{q} = A_\mathfrak{p}$$

Also ist $A_\mathfrak{p}$ lokal mit maximalem Ideal $\mathfrak{P} = S^{-1}\mathfrak{p}$. Nach Theorem 3.5 hat jedes Ideal von $A_\mathfrak{p}$ die Form $\mathfrak{P}^n$ mit $n \in \mathbb{N}_0$. Sei $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, d.h.

$$\mathfrak{P} \supset (\pi) \supset \mathfrak{P}^2$$

Wegen $(\pi) \neq \mathfrak{P}^2$ folgt $\mathfrak{P} = (\pi)$, denn andere Ideale gibt es nicht. Damit ist $A_\mathfrak{p}$ ein Hauptidealring. Schließlich betrachten wir $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{P}$. Dies ist ein wohldefinierter Körperhomomorphismus. Sei $a/s \in A_\mathfrak{p}$. Wegen $s \in A \setminus \mathfrak{p}$ gilt $\overline{s} \neq 0$ in $A/\mathfrak{p}$. Dann ist $\overline{s}^{-1}a$ ein Urbild von a/s. Die Abbildung ist surjektiv, also bijektiv. □

Beweis von Satz 5.2. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, L/K eine Erweiterung und

$$\mathcal{O}_L\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$$

Sei $S = \mathcal{O}_K \setminus \mathfrak{p}$, $\mathcal{O}_{K,\mathfrak{p}} = S^{-1}\mathcal{O}_K \to S^{-1}\mathcal{O}_L$ ist eine Erweiterung von Dedekindringen. Wegen $S^{-1}(II') = (S^{-1}I)(S^{-1}I')$ folgt

$$S^{-1}\mathcal{O}_L\mathfrak{p} = \prod (S^{-1}\mathfrak{P}_i)^{e_i}$$

Der Verzweigungsgrad kann also auch nach Lokalisieren an S berechnet werden, ebenso wie die lokalen Körpergrade f_i.

Behauptung. *$S^{-1}\mathcal{O}_L$ ist freier $S^{-1}\mathcal{O}_K$-Modul vom Rang $[L:K]$.*

$S^{-1}\mathcal{O}_L$ ist der ganze Abschluss von $S^{-1}\mathcal{O}_K$ in L. Da $\mathcal{O}_L$ ein endlich erzeugter $\mathcal{O}_K$-Modul ist (sogar endlich erzeugt über $\mathbb{Z}$), ist auch $S^{-1}\mathcal{O}_L$ endlich erzeugt über $S^{-1}\mathcal{O}_K$. Wie im Beweis von Theorem 1.10 mit dem Hauptidealring $S^{-1}A_\mathfrak{p}$ statt $\mathbb{Z}$ folgt die Behauptung.
In dieser lokalen Situation kann das Argument aus unserem ersten Beweisversuch angewendet werden. □

Diskriminante

Wir erinnern: Sei A ein Hauptidealring, $A \to B$ eine Ringerweiterung mit $B \cong A^n$, Basis $x_1, \ldots, x_n$.

$$d_{B/A} = (\det(\mathrm{Tr}(x_i x_j)_{i,j}))$$

Speziell für $A = \mathbb{Z}$, $B = \mathcal{O}_K$ heißt der positive Erzeuger von $d_{B/A}$ absolute Diskriminante von K.

Satz 5.4. *Sei K ein Zahlkörper. Dann ist eine Primzahl $p \in \mathbb{Z}$ unverzweigt in K, genau dann wenn $p \nmid d$.*

Beweis: $\mathcal{O}_K \cong \mathbb{Z}^n$ mit $n = [K:\mathbb{Q}]$. Sei p Primzahl, $(p) = \prod \mathfrak{P}_i^{e_i}$. Die Erweiterung ist unverweigt über p, wenn $\mathcal{O}_K/(p) = \prod \mathcal{O}_K/\mathfrak{P}^{e_i}$ (chinesischer Restsatz) ein Produkt von Körpern ist. Sei $x_1, \ldots, x_n$ eine Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul. Dann ist $\overline{x_1}, \ldots, \overline{x_n}$ eine Basis von $\mathcal{O}_K/(p)$ Als $\mathbb{Z}/(p) = \mathbb{F}_p$-Vektorraum. Nach Definition ist $d = \det(\mathrm{Tr}(x_i x_j)$, also ist $\overline{d} = \det(\mathrm{Tr}(\overline{x}_i\overline{x}_j)$ die Diskriminante von $\mathbb{F}_p \to \mathcal{O}_K/(p)$. Die Bedingung $p \nmid d$ ist äquivalent zu $\overline{d} \neq 0$. Zu zeigen ist also:

Behauptung. *$\mathbb{F}_p \to B = \mathcal{O}_K/(p)$ eine Ringerweiterung. Dann ist $d_{B/\mathbb{F}_p} \neq 0$ genau dann, wenn B ein Produkt von Körpern ist.*

Sei zunächst $B = \prod k_i$ wobei k_i endliche Körpererweiterungen von $\mathbb{F}_p$ sind. Es gilt $d_{B/\mathbb{F}_p} = \prod d_{k_i/\mathbb{F}_p}$ (rechne in Basen der k_i). Nach Satz 2.11 ist $d_{k_i/\mathbb{F}_p} \neq 0$ (Dort war Charakteristik 0 vorausgesetzt, aber perfekt genügt).
Sei umgekehrt $B = \prod \mathcal{O}_K/\mathfrak{P}_i^{e_i}$ kein Produkt von Körpern. Dann enthält B ein nilpotentes Element $x \neq 0$. Ergänze $x = x_1$ zu einer Basis $x_1, \ldots, x_n$ von B. Die Produkte $x_1 x_i$ sind nilpotent, also ist Muliplikation mit $x_1 x_i$ eine nilpotente Abbildung. Daher sind alle Eigenwerte 0 und $\mathrm{Tr}(x_1 x_j) = 0$. Dann verschwindet auch die Diskriminante. □

Theorem 5.5 (Hasse-Minkowski). *Es gibt keine Erweiterung $K/\mathbb{Q}$, die überall unverzweigt ist.*

Beweis: $K \neq \mathbb{Q} \Rightarrow d \neq 1$ nach Theorem 4.16. Also gibt es Teiler von d, also verzweigte Primzahlen. □

Korollar 5.6. *Sei L/K Erweiterung von Zahlkörpern. Dann sind nur endlich viele Primideale verzweigt.*

Beweis: $\mathbb{Z} \subset \mathcal{O}_K \subset \mathcal{O}_L$. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, das in L/K verzweigt, d.h. $\mathcal{O}_K\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$ mit einem $e_i > 1$. Sei $(p) = \mathfrak{p} \cap \mathbb{Z}$. Es folgt

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

Also genügt es, $K = \mathbb{Q}$ zu betrachten. Dann sind die verzweigten Primideale die Teiler von d, also gibt es nur endlich viele. □

Bemerkung. Allgemeiner besagt *Klassenkörpertheorie*: $K/\mathbb{Q}$ ein Zahlkörper. Dann gibt es eine Erweiterung H/K, den *Klassenkörper* mit

(i) H ist maximale unverzweigte Erweiterung von K

(ii) $\mathcal{O}_H$ ist ein Hauptidealring

(iii) $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$

Literatur: Lang, "algebraic number theory", part II, Neukirch, Ch. 4-6, Cassels-Fröhlich, Ch.VII

Für allgemeine L/K ist $\mathcal{O}_L$ kein freier $\mathcal{O}_K$ nicht frei, daher ist die Diskriminate bisher nicht definiert worden.

Definition 5.7. *Sei L/K Erweiterung von Zahlkörpern. Dann ist ist das* Diskriminantenideal *definiert als*

$$\mathcal{D}_{L/K} = \prod \mathfrak{p}^{v(\mathfrak{p})} \subset \mathcal{O}_K$$

mit $d_{(\mathcal{O}_L)_\mathfrak{p}/(\mathcal{O}_K)_\mathfrak{p}} = \mathfrak{p}_\mathfrak{p}^{v(\mathfrak{p})} \subset (\mathcal{O}_K)_\mathfrak{p}$.

Bemerkung. Da $(\mathcal{O}_K)_\mathfrak{p}$ ein Hauptidealring ist, ist die Diskriminante von $(\mathcal{O}_L)_\mathfrak{p}/(\mathcal{O}_K)_\mathfrak{p}$ definiert. Da fast alle Primideale unverzweigt sind, ist $v(\mathfrak{p}) = 0$ fast immer.

Korollar 5.8. *L/K unverzweigt in $\mathfrak{p}$ genau dann, wenn $\mathcal{D}_{L/K} \nmid \mathfrak{p}$.*

Beweis: Verzweigung ist eine lokale Eigenschaft, ebenso die Teilbarkeit von Idealen. Wir lokalisieren also in $\mathfrak{p}$. Danach ist der Beweis der gleiche wie in 5.4 mit $(\mathcal{O}_K)_\mathfrak{p}$ statt $\mathbb{Z}$. □

Bemerkung. Bei unserer Korrespondenz zwischen Riemannschen Flächen und Ganzheitsringen entspricht Verweigung von holomorphen Abbildungen (lokal wie $z \mapsto z^e$ für $e > 1$) genau der Verzweigung von Primidealen.

Beispiele

Sei $K = \mathbb{Q}(\zeta)$ mit $\zeta = \exp(2\pi i/p)$ für eine Primzahl p. Wir wählen die Basis $1, \zeta, \ldots, \zeta^{p-2}$.

Behauptung. $\mathcal{O}_K = \mathbb{Z}[\zeta]$

Sei $x = a_0 + \cdots + a_{p-2}\zeta^{p-2} \in \mathcal{O}$ mit $a_i \in \mathbb{Q}$. Wegen $x(1-\zeta) \in \mathcal{O}$ folgt $\mathrm{Tr}(x(1-\zeta)) = a_0 p \in \mathbb{Z}$. Andererseits gilt

$$\mathrm{Tr}(x(1-\zeta)) = \sum_\sigma \sigma(x)(1-\sigma(\zeta_p))$$

mit $\sigma(\zeta_p) = \zeta^j$, also $1 - \sigma(\zeta) = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{j-1}$. Damit gilt $\mathrm{Tr}(x(1-\zeta_p)) \in \mathcal{O}(1-\zeta) \cap \mathbb{Z}$.

Behauptung. $\mathcal{O}(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$

Mit $x = 1$ und $\mathrm{Tr}(1-\zeta_p) = p$ gilt $\supset$. Wäre Gleichheit falsch, so müsste $1 \in \mathcal{O}(1-\zeta)$ liegen, also $1-\zeta$ eine Einheit sein. Die Norm von $1-\zeta$ ist aber

$$N(1-\zeta_p) = \prod_{j=1}^{p-1}(1-\zeta_p^j) = \prod(X-\zeta^j)(1) = (1+X+\cdots+X^{p-1})(1) = p$$

also ist dies nicht der Fall.
Somit gilt $pa_0 \in p\mathbb{Z}$, d.h. $a_0 \in \mathbb{Z}$. Dann ist auch $a_1\zeta + \ldots a_{p-2}\zeta^{p-2} = \zeta(a_1 + \ldots a_{p-2}\zeta^{p-3} \in \mathcal{O}$. ζ ist eine Einheit. Wir wiederholen nun das Argument und erhalten $a_1 \in \mathbb{Z}$ und iterativ $a_i \in \mathbb{Z}$ für alle i. Damit ist die Berechnung von $\mathcal{O}$ abgeschlossen.

Übungsaufgabe. $\mathcal{O} = \mathbb{Z}[X]/F \Rightarrow d = N(F'(X))$.

In unserem Fall gilt: $F(X-1) = X^p - 1$), also

$$F'(X-1) + F = pX^{p-1} \Rightarrow F'(\zeta_p)(\zeta_p - 1) + 0 = p\zeta^{p-1}$$

Wegen $N(p) = p^{p-1}$, $N(\zeta) = \pm 1$, $N(1-\zeta_p) = \pm 1$ (explizite Rechnung) folgt $d = \pm p^{p-1}$. Damit ist p die einzige verzweigte Primzahl in $\mathcal{O}$.
Sei nun $K = \mathbb{Q}(\sqrt{\delta})$ mit $\delta = 2, 3 \mod 4$, also $\mathcal{O} = \mathbb{Z}[\sqrt{\delta}]$, $d = 4\delta$, verzweigt in 2 und Teilern von δ. Für $\delta = 1 \mod 4$ ist $1, (1+\sqrt{\delta})/2$ eine Basis von $\mathcal{O}$.

$$d = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}((1+\sqrt{\delta})/2) \\ \mathrm{Tr}((1+\sqrt{\delta})/2) & \mathrm{Tr}((1+\delta)/4 + \sqrt{\delta}/2) \end{pmatrix}$$
$$= \det \begin{pmatrix} 2 & 1 \\ 1 & (1+\delta)/2 \end{pmatrix} = \delta + 1 - 1 = \delta$$

Sei nun $K = \mathbb{Q}(\zeta)$ mit $p \neq 2$. Die Galoisgruppe von $K/\mathbb{Q}$ ist isomorph zu $(\mathbb{Z}/p)^*$, zyklisch von der Ordnung $p-1$. Sei H die eindeutige Untergruppe vom Index

2 (Gruppe der Quadrate). Dann ist $F = K^H$ ein quadratischer Zahlkörper. Welcher?
K ist nur in p verzweigt, also F ebenfalls. Es folgt

$$F = \begin{cases} \mathbb{Q}(\sqrt{p}) & p = 1 \mod 4 \\ \mathbb{Q}(\sqrt{-p} & p = 3 \mod 4 \end{cases}$$

Allgemeiner gilt der Satz von Kronecker und Weber: $F/\mathbb{Q}$ galois, $\mathrm{Gal}(F/\mathbb{Q})$ abelsch. Dann ist $F \subset \mathbb{Q}(\zeta_N)$ mit $\zeta_N = \exp(2\pi i/N)$ für geeignetes N.

Galoistheorie

Sei nun L/K eine Galoiserweiterung von Zahlkörpern, d.h.

$$[L : K] = \mathrm{Gal}(L/K) \Leftrightarrow L^{\mathrm{Gal}(L/K)} = K$$

wobei $\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \sigma|_K = \mathrm{id}\}$. Dies ist äquivalent dazu, dass L/K normal ist, d.h. für $\alpha \in L$ liegen alle Nullstellen des Minimalpolynoms in L.

Lemma 5.9. *Sei L/K eine Galoiserweiterung von Zahlkörpern. Dann operiert $\mathrm{Gal}(L/K)$ auf $\mathcal{O}_L$, auf den Primidealen von $\mathcal{O}_L$ und auf den Primidealen von $\mathcal{O}_L$ über $\mathfrak{p} \subset \mathcal{O}_K$.*

Beweis: Sei $\sigma \in \mathrm{Gal}(L/K)$, $x \in \mathcal{O}_L$, d.h. es gibt eine Polynomgleichung

$$x^n + a_1 x^{n-1} + \ldots a_n = 0 \qquad a_i \in \mathcal{O}_K$$

Anwenden von σ auf diese Gleichung ergibt

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

Damit ist auch $\sigma(x)$ ganz.
Sei nun $\mathfrak{q} \subset \mathcal{O}_L$ ein Primideal. Wir betrachten $\sigma(\mathfrak{q})$. Dies ist offensichtlich ein Ideal. Sei $ab \in \sigma(\mathfrak{q})$, also $\sigma^{-1}(a)\sigma^{-1}(b) \in \mathfrak{q}$. Da $\mathfrak{q}$ ein Primideal ist, folt $\sigma^{-1}a \in \mathfrak{q}$ oder $\sigma^{-1}b \in \mathfrak{q}$, also $a \in \sigma(\mathfrak{q})$ oder $b \in \sigma(\mathfrak{q})$.
Schließlich sei $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Dann gilt $\sigma(\mathfrak{p}) \cap \mathcal{O}_K = \mathfrak{p}$, denn σ lässt Elemente von $\mathcal{O}_K$ invariant. □

In dieser Situation heißen $\mathfrak{q}$ und $\sigma(\mathfrak{q})$ *konjugiert*. Verzweigungsindex und Restklassengrad von konjugierten Idealen stimmen überein.

Lemma 5.10. *Je zwei Primideale von $\mathcal{O}_L$ über $\mathfrak{p} \subset \mathcal{O}_K$ sind konjugiert. Es gilt*

$$[L : K] = gfe$$

wobei g die Anzahl der Primideale über $\mathfrak{p}$ ist, e der Verzweigungsindex, f der Restklassengrad.

Beweis: Die Aussagen folgen aus der ersten mit der Gradformel. Seien $\mathfrak{q}, \mathfrak{q}'$ über $\mathfrak{p}$ nicht konjugiert, also $\sigma(\mathfrak{q}')$ nicht in $\mathfrak{q}$ enthalten für alle σ. Seien $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_k$ die Konjugierten von $\mathfrak{q}'$. Wir wählen $x_{ij} \in \mathfrak{q}'_j \setminus \mathfrak{q}'_i$ für $i \neq j$ und $x_i \in \mathfrak{q} \setminus \mathfrak{q}'_i$. Sei

$$x = x_1 \prod_{1 \neq q} x_{1j} + x_2 \prod_{2 \neq j} x_{2j} + \cdots + x_k \prod_{k \neq j} x_{kj}$$

Es gilt $x \in \mathfrak{q}$, da $x_i \in \mathfrak{q}$. Andererseits ist $x \notin \mathfrak{q}'_j$, denn jeder Summand außer dem zu j enthält einen Faktor in $\mathfrak{q}'_j$ (nämlich x_{ij}). In dem Summanden zu j ist kein Faktor in $\mathfrak{q}'_j$. Es folgt

$$N(x) = \prod \sigma(x) \in \mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p} \subset \mathfrak{q}'$$

Also liegt ein $\sigma(x) \in \mathfrak{q}'$ und $x \in \sigma^{-1}\mathfrak{q}'$. Dies ist ein Widerspruch. □

Definition 5.11. *Sei L/K Galoiserweiterung von Zahlkörpern, $\mathfrak{q}$ ein Primideal von $\mathcal{O}_L$, $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}$. Die* Zerlegungsgruppe *von $\mathfrak{q}$ ist*

$$D_\mathfrak{q} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

Die nätürliche Abbildung $\phi : D_\mathfrak{q} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ ist ein Gruppenhomomorphismus. Die Trägheitsgruppe *$I_\mathfrak{q}$ ist der Kern von ϕ, d.h.*

$$I_\mathfrak{q} = \{\sigma : L \to L \mid \sigma(\alpha) = \alpha \mod \mathfrak{q} \text{ für alle } \alpha \in \mathcal{O}_L\}$$

Lemma 5.12. *Es gilt $|D_\mathfrak{q}| = ef$, $e = |I|$. Die Abbildung ϕ ist surjektiv.*

Beweis: Wie vorher sei g die Anzahl der Konjugierten von $\mathfrak{q}$, d.h. $|G|/|D_\mathfrak{q}|$, denn G operiert transitiv mit Standgruppe $D_\mathfrak{q}$. Also

$$g = n/|D_\mathfrak{q}| = gef/|D_\mathfrak{q}|$$

Sei nun $E = L^{D_\mathfrak{q}} \subset L$. Nach dem Hauptsatz der Galoistheorie ist $\mathrm{Gal}(L/E) = D_\mathfrak{q}$. Sei $\mathfrak{p}_E = \mathfrak{q} \cap \mathcal{O}_E$. Nach Definition liegt $\mathfrak{q}$ über $\mathfrak{p}_E$. Das Primideal $\mathfrak{q}$ wird von allen Elementen auf $D_\mathfrak{q}$ festgelassen, also ist die Zerlegungsgruppe von $\mathfrak{q}$ in L/E ganz $D_\mathfrak{q}$. Damit liegt nur ein Primideal von L über $\mathfrak{p}_E$ (nämlich $\mathfrak{q}$). Es folgt

$$ef = |D_\mathfrak{q}| = [L : E] = e(\mathfrak{q}/\mathfrak{p}_E) f(\mathfrak{q}/\mathfrak{p}_E)$$

Verzweigungsgrad und Restklassenindex sind multiplikativ in Körpertürmen, also folgt

$$e = e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p}_E), \qquad f = f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}_E)$$

Dies bedeutet $\kappa(\mathfrak{p}_E) = \kappa(\mathfrak{p})$.
Nach dem Satz vom primitiven Element ist $\kappa(\mathfrak{q}) = \kappa(\mathfrak{p})(\overline{\alpha})$ für ein $\alpha \in \mathcal{O}_L$. Sei $P \in \mathcal{O}_E[X]$ das normierte Minimalpolynom von α. Es stimmt mit dem charakteristischen Polynom von α überein. Dann ist $\overline{P} \in \kappa(\mathfrak{p}_E)[X]$ eine Potenz des Minimalpolynoms von $\overline{\alpha}$. Sei $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}_E))$, also $\overline{\sigma}(\overline{\alpha})$ eine Nullstelle von $\overline{P}$. Dann muss es $\sigma \in \mathrm{Gal}(L/E) = D_\mathfrak{q}$ geben mit $\sigma(\alpha) = \overline{\sigma}(\overline{\alpha})$. Dann ist $\overline{\sigma} = \phi(\sigma)$, d.h. ϕ ist surjektiv. Es folgt $f(\mathfrak{q}/\mathfrak{p}_E) = |\mathrm{Im}\phi| = |D_\mathfrak{q}|/|I| = ef/|I|$. □

Korollar 5.13. *Sei L/K Galoisweiterung von Zahlkörpern, $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p}$ unverzweigt genau dann, wenn $|I_\mathfrak{q}| = 1$ für ein $\mathfrak{q} \mid \mathfrak{p}$.*

Übungsaufgabe. *(i) Sei $\mathfrak{q}, \sigma(\mathfrak{q}) \mid \mathfrak{p}$. Dann gilt $D_{\sigma\mathfrak{q}} = \sigma D_\mathfrak{q} \sigma^{-1}$, $I_{\sigma\mathfrak{q}} = \sigma I_\mathfrak{q} \sigma^{-1}$. Insbesondere sind diese Gruppen isomorph.*

(ii) $L^{I_\mathfrak{q}}/K$ ist unverzweigt.

Kapitel 6

L-Funktionen

Definition 6.1. *Sei K ein Zahlkörper. Dann ist die* Dedekindsche ζ-Funktion *gegeben durch*

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$$

für $s \in \mathbb{C}$ für die die Reihe konvergiert.

Beispiel. (i) $K = \mathbb{Q}$. Ideale entsprechen den $n \in \mathbb{N}$. Es gilt $N((n)) = n$.

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

also die Riemannsche ζ-Funktion.

(ii) $K = \mathbb{Q}(i)$ Ideale entsprechen den Elementen von $K^*/\mathbb{Z}[i]^*$ mit $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. Es gilt $N((a+bi)) = |N(a+bi)| = a^2 + b^2$.

$$\zeta_{\mathbb{Q}(i)} = \frac{1}{4} \sum_{a+bi \in K^*} \frac{1}{(a^2+b^2)^s} = \sum_{n=1} \infty \frac{1}{n^s} \sum_{a,b \geq 0, a^2+b^2=n}$$
$$= 1 + \frac{1}{2^s} + \frac{0}{3^s} + \frac{1}{4^s}\frac{2}{5^s} + \dots$$

Definition 6.2. *Ein* Dirichlet-Charakter *ist eine multiplikative Abbildung $\chi : (\mathbb{Z}/N)^* \to \mathbb{C}^*$. Man setzt $\chi(n) = 0$ für $(n, N) \neq 1$. Die* L-Reihe zu χ *ist*

$$L(\chi, s) = \sum_{n=1} \frac{\chi(n)}{n^s}$$

für $s \in \mathbb{C}$ für die die Reihe konvergiert.

Beispiel. $N = 1$, $\chi(n) = 1$ für alle $n \in (\mathbb{Z}/N)^* = \{1\}$.

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$$

Allgemeiner:

Definition 6.3. *Sei a_n eine Folge komplexer Zahlen. Dann heißt*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

für $s \in \mathbb{C}$ Dirichlet-Reihe*.*

Lemma 6.4. *Wenn die Dirichlet-Reihe in $s_0 \in \mathbb{C}$ konvergiert, dann konvergiert sie lokal gleichmäßig in $\mathrm{Re}(s) > \sigma_0 = \mathrm{Re}s_0$.*

Beweis: Es gilt $n^s = n^{s_0} n^{(s-s_0)}$. Wir betrachten

$$\sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}}$$

Wir überprüfen Konvergenz mit dem Cauchy-Kriterium. Nach Voraussetzung gilt

$$|P_{m,M}| = |\sum_{n=m}^{M} \frac{a_n}{n^s}| < \varepsilon$$

für alle $M, m \geq M_0$.
Wir benutzen nun partielle Summation: Seien a_n, b_n Folgen, $A_{m,p} = \sum_{n=m}^{p} a_n$. Dann gilt

$$\sum_{n=m}^{M} = A_{m,M} b_M + \sum_{n=m}^{M-1} A_{m,n}(b_n - b_{n+1})$$

da $a_n = A_{m,n} - A_{m,n-1}$. Hieraus folgt

$$\begin{aligned}\left|\sum_{n=m}^{M} \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}}\right| &= \left|P_{n,M} \frac{1}{M^{s-s_0}} + \sum_{n=m}^{M-1} P_{m,n} \left(\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}}\right)\right| \\ &\leq \varepsilon \left(\left|\frac{1}{M^{s-s_0}}\right| + \sum_{n=m}^{M-1} \left|\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}}\right|\right)\end{aligned}$$

Wir setzen nun $\sigma = \mathrm{Re}s - s_0 > 0$. Wir beachten:

$$\begin{aligned}\left|\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}}\right| &= \left|(s-s_0) \int_n^{n+1} \frac{1}{x^{s-s_0+1}} dx\right| \\ &\leq |s-s_0| \int_n^{n+1} \frac{1}{x^{\sigma+1}} dx \\ &= \frac{|s-s_0|}{\sigma} \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\right)\end{aligned}$$

Hiermit erhalten wir

$$\begin{aligned}\left|\sum_{n=m}^{M} \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}}\right| &\leq \varepsilon \left(\frac{1}{M^\sigma} + \sum_{n=m}^{M} \frac{|s-s_0|}{\sigma}\left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\right)\right) \\ &\leq \left(1 + \frac{|s-s_0|}{\sigma}\frac{1}{(M-1)^\sigma}\right) \\ &\leq \varepsilon(1 + \frac{|s-s_0|}{\sigma})\end{aligned}$$

Die letzte Zahl ist klein in $\frac{|s-s_0|}{\sigma} \leq r$, also liegt lokal gleichmäßige Konvergenz vor. □

Korollar 6.5. *Der Konvergenzbereich der Reihe ist von der Form*

$$\{\mathrm{Re} s > \sigma_0\} \cup \{s = \sigma_0 + iy \mid \textit{ Reihe konvergiert in } s\}$$

In $\mathrm{Re} s > \sigma_0$ *ist die durch die Reihe definierte Funktion holomorph.*

Beweis: Sei σ_0 das Infinum der Realteile der Punkte, in denen die Reihe konvergiert. Wir wenden nun das Lemma an und erhalten die behauptete Form des Konvergenzbereichs. Alle a_n/n^s sind holomorph in $\mathbb{C}$. Wegen gleichmäßiger Konverenz ist auch die Grenzfunktion holomorph. □

Lemma 6.6. *Seien* $C, \sigma_1 \geq 0$*, so dass*

$$|A_m| = |a_1 + \cdots + a_m| \leq C n^{\sigma_1}$$

Dann ist die Konvergenzabszisse höchstens σ_1*.*

Beispiel. $L(\chi, s)$ hat $|a_n| = 0, 1$, also $|A_m| \leq 1m^1$, also ist die Reihe konvergent für $\mathrm{Re} s > 1$.

Beweis: Sei $\mathrm{Re} s \geq \sigma_1 + \delta$. Partielle Summation

$$\begin{aligned}
\left|\sum_{n=m}^{M} a_n n^{-s}\right| &= \left|A_M M^{-s} + \sum_{n=m}^{M-1} A_n (n^{-s} + (n+1)^{-s})\right| \\
&= \left|A_M M^{-s} + \sum n = m^{M-1} A_n \int_n^{n+1} x^{-s-1} dx\right| \\
&\leq C M^{\sigma_1 - \mathrm{Re} s} + \sum n = m^{M-1} \left|A_n s \int_n^{n+1} x^{-s-1} dx dx\right| \\
&\leq C M^{\delta} + \sum n = m^{M-1} C n^{\sigma_1} |s| \int_n^{n+1} x^{-\sigma_1 - \delta - 1} dx \\
&=\leq C M^{\delta} + C|s| \sum n = m^{M-1} \int_n^{n+1} \frac{n^{\sigma_1}}{x^{\sigma_1+\delta+1}} dx \\
&\leq C M^{\delta} + C|s| \sum n = m^{M-1} \int_n^{n+1} \frac{x^{\sigma_1}}{x^{\sigma_1+\delta+1}} dx \\
&=\leq C M^{\delta} + C|s| \int_m^{M-1} x^{-\delta-1} dx \\
&\leq\leq C M^{\delta} C|s| m^{-\delta}
\end{aligned}$$

Dieser Term wird klein für große M, m. □

Bemerkung. Die Konvergenz der Dedekindschen ζ-Funktion werden wir mit einer anderen Methode zeigen.

Unser nächstes Ziel ist das Verständnis von $\zeta(s)$ bei $s = 1$. Die Reihe divergiert, aber $\sum(-1)^n/n$ konvergiert.

Definition 6.7. *Sei*

$$\zeta_2(s) = -\sum \frac{(-1)^n}{n^s}$$

Wegen $|A_m| = |1 - 1 + 1 - 1 + \ldots| \leq 1 m^0|$ konvergiert die Reihe für $\mathrm{Re} s > 0$, dort ist die Funktion holomorph.

Satz 6.8. *Es gilt*

$$\zeta(s) = \zeta_2(s) \left(1 - \frac{1}{2^{s-1}}\right)^{-1}$$

Insbesondere hat $\zeta(s)$ eine meromorphe Fortsetzung nach $\mathrm{Re} s > 0$. *$\zeta(s)$ ist holomorph in diesem Gebiet mit Ausnahme eines einfachen Pols mit Residuum* 1 *in* $s = 1$.

Beweis:

$$\begin{aligned}\frac{2}{2^s}\zeta(s)+\zeta_2(s) &= \sum \frac{2}{2^s n^s}+\sum \frac{(-1)^n}{n^s}\\ &= \sum_{n \text{ gerade}} \frac{2}{n^s}+\sum \frac{(-1)^n}{n^s}\\ &= \sum \frac{1}{n^s}\end{aligned}$$

Hieraus folgt

$$\zeta_2(s)=\zeta(s)-\frac{1}{2^{s-1}}\zeta(s)=\left(1-\frac{1}{2^{s-1}}\right)\zeta(s)$$

Die möglichen Singularitäten von $\zeta(s)$ sind die Nullstellen von $1-\frac{1}{2^{s-1}}$, also

$$\{1+\frac{2\pi i n}{\log 2} \mid n\in\mathbb{Z}\}$$

Wir betrachten nun zusätzlich

$$\zeta_3(s)=1+\frac{1}{2^s}-\frac{2}{3^s}++\frac{1}{4^s}+\frac{1}{5^s}-\frac{1}{6^s}+\dots$$

diese Funktion ist ebenfalls holomorph in $\mathrm{Re}s>0$ und erfüllt

$$\zeta_3(s)=\left(1-\frac{1}{3^{s-1}}\right)\zeta(s)$$

Die Nullstellen von $1-\frac{1}{3^{s-1}}$ sind

$$\{1+\frac{2\pi i n}{\log 3} \mid n\in\mathbb{Z}\}$$

Wir müssen die Schnittmenge berechnen, also

$$\frac{n}{\log 2}=\frac{n'}{\log 3}\Leftrightarrow n\log 3=n'\log 2\Leftrightarrow 3^n=2^{n'}\Leftrightarrow n=n'=0$$

Also ist die einzige Singularität von $\zeta(s)$ in $s=1$. Die Funktion $1-\frac{1}{2^{s-1}}$ hat dort nur eine einfache Nullstelle, denn für $1/2^{s-1}=\exp((-s+1)\log 2)$ hat die Ableitung keine Nullstelle. Also:

$$\zeta(s)=\frac{\varrho}{s-1}+h$$

wobei h holomorph und beschränkt in der Nähe von 1.

Behauptung. $\varrho=1$

Für $s > 1$ reell gilt

$$\frac{1}{s-1} = \left.\frac{x^{-s+1}}{1-s}\right|_1^\infty \leq \int_1^\infty \frac{1}{x^s} dx \leq \sum_{n=1}^\infty \frac{1}{n^s} = \zeta(s)$$

und andererseits

$$\zeta(s) \leq 1 + \int_1^\infty \frac{1}{x^s} dx = 1 + \frac{1}{s-1}$$

□

Bemerkung. Tatsächlich hat $\zeta(s)$ eine holomorphe Fortsetzung nach $\mathbb{C} \setminus \{1\}$. Die Funktion

$$\xi(s) = \pi^{-2s}\Gamma(s/2)\zeta(s)$$

erfüllt die Funktionalgleichung

$$\xi(s) = \xi(1-s)$$

Vergleich mit der Riemannschen ζ-Funktion liefert ein weiteres Konvergenzkriterium.

Satz 6.9. *Sei a_n für $n \in \mathbb{N}$ eine Folge komplexer Zahlen, $A_m = a_1 + \cdots + a_m$. Seien $0 \leq \sigma_1 \leq 1$, $C > 0$, $\varrho \in \mathbb{C}$ so dass*

$$|A_m - m\varrho| \leq Cm^{\sigma_1}$$

Dann konvergiert die Dirichlet-Reihe $\sum a_n/n^s$ in $\mathrm{Re}s > 1$ und hat eine analytische Fortsetzung nach $\mathrm{Re}s\sigma_1$. Die Funktion ist holomorph bis auf einen einfachen Pol in $s = 1$ mit Residuum ϱ.

Beweis: Wir betrachten

$$\sum \frac{a_n}{n^s} - \varrho\zeta(s) = \sum \frac{a_n - \varrho}{n^s}$$

Nach Lemma 6.6 konvergiert diese Reihe in $\mathrm{Re}s > \sigma_1$. Da $\zeta(s)$ holomorph ist für $\{\mathrm{Re}s > 0\} \setminus \{1\}$ folgt die Holomorphieaussage für $\sum a_n/n^s$. In $s = 1$ hat diese Reihe einen Pol erster Ordnung mit Residuum $\varrho \cdot 1$. □

Satz 6.10. *Sei $\chi : (\mathbb{Z}/N)^* \to \mathbb{C}$ ein Dirichlet-Charakter. Dann ist $L(\chi, s) = \sum \chi(n)/n^s$ konvergent in*

$$\begin{cases} \mathrm{Re}s > 1 & \chi = 1 \\ \mathrm{Re}s > 0 & \chi \neq 1 \end{cases}$$

Im Fall des trivialen Charakters $\chi = 1$ gilt

$$L(1, s) = \zeta(s) \prod_{p|N} (1 - p^{-s})$$

Die Funktion hat eine analytische Fortsetzung nach $\mathrm{Re} > 0$ mit einem einfachen Pol in $s = 1$.

Beweis: Sei zunächst $\chi = 1$, also

$$\begin{aligned} L(1,s) &= \sum_{(n,N)=1} \frac{1}{n^s} \\ &= \zeta(s) - \sum_{p|N} \frac{1}{(pn)^s} + \sum_{p_1,p_2|N} \frac{1}{({}_1p_2n)^s} - \sum_{p_1,p_s,p_3} \frac{1}{({}_1p_2p_3n)^s} \pm \dots \\ &= \zeta(s) - \sum_{p} \frac{1}{p^s}\zeta(s) + \sum_{p_1,p_2} \frac{1}{p_1^s p_2^s}\zeta(s) \pm \dots \\ &= \prod_{p|N}(1-p^{-s})\zeta(s) \end{aligned}$$

Die Faktoren $(1-p^{-s})$ sind holomorph, die Aussage folgt nun aus Satz 6.8.
Sei nun $\chi \neq 1$. Dann ist die Folge der $\chi(n)$ periodisch, und es gilt $\sum_{n=1}^{N} \chi(n) = 0$ (siehe unten Lemma 6.11). Also

$$|\sum_{n=1}^{m} \chi(n)| \leq \max_{k>N} |\sum_{n=1}^{k} \chi(n)|$$

Nach dem Kriterium 6.6 konvergiert die Reihe für Re$s > 0$. □

Bemerkung. Wir wollen mehr: $L(\chi, 1) \neq 0$ für alle $\chi \neq 1$.

Lemma 6.11. *Sei G eine endliche Gruppe, $\chi : G \to \mathbb{C}^*$ ein nichttrivialer Charakter. Dann gilt*

$$\sum_{g \in G} \chi(g) = 0$$

Beweis: Sei $h \in G$ mit $\chi(h) \neq 1$. Es gilt

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum \chi(g) \Rightarrow (1-\chi(h)) \sum \chi(g) = 0$$

Die Behauptung folgt wegen $1 - \chi(h) \neq 0$. □

Euler-Produkte

Seien $b_i \neq 0$ komplexe Zahlen. Das unendliches Produkt $\prod_{i=1}^{\infty} b_i$ konvergiert gegen eine Zahl b genau dann, wenn $\lim_{n\to\infty} \prod_{i=1}^{n} b_i = b$ und $b \neq 0$. (Fischer-Lieb, VII §2).
Wenn es eine Wahl von Zweigen des Logarithmus gibt mit $\sum \log b_i$ konvergent, dann ist auch $\prod b_i$ konvegent.

Lemma 6.12. *Sei a_n eine strikt multiplikative Folge, d.h. $a_{nn'} = a_n a_{n'}$ mit a_n. Sei entweder*

(i) a_n beschränkt;

(ii) $a_n > 0$ *reell*

Dann gilt

$$\sum_{n\geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1-\frac{a_p}{p^s}}$$

und Reihe ist absolut konvergent. Die Konvergenzbereiche stimmen überein.

Beweis: Im Fall (i) folgt die absolute Konvergenz aus unserem Konvergenzkriterium, im Fall (ii) folgt sie direkt im Konvergenzbereich. Auf jeden Fall darf die Reihe nun beliebig umsortiert werden. Die Summenformel für die geometrische Reihe besagt formal

$$\frac{1}{1-\frac{a_p}{p^s}} = \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}}$$

Wegen der absoluten Konvergenz der Dirichlet-Reihe konvergiert auch die geometrische Reihe. Sei S eine endliche Menge von Primzahlen, $\mathbb{N}(S)$ die Menge der natürlichen Zahlen, deren Primteiler aus S kommen. Dann gilt

$$\prod_{p\in S} \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}} = \sum_{n\in\mathbb{N}(S)} \frac{a_n}{n^s}$$

als Grenzwerte. Für größer werdendes S konvergiert die linke Seite gegen das unendliche Produkt, die rechte gegen die Dirichlet-Reihe. Mit der Reihe konvergiert auch das Produkt. Divergiert die Reihe, so muss auch das Produkt divergieren. □

Dies ist das *Euler-Produkt* der L-Reihe. Die $1 - a_p/p^s$ heißen *Euler-Faktoren*.

Korollar 6.13. *Sei K ein Zahlkörper. Dann gilt*

$$\zeta_K(s) = \prod_{0\neq\mathfrak{p}\in \operatorname{Spec}\mathcal{O}_K} \frac{1}{1-N(\mathfrak{p})^{-s}}$$

und der Konvergenzbereich von Reihe und Produkt stimmen überein.

Proof. Nach Definition ist $\zeta_K(s) = \sum N(\mathfrak{a})^{-s}$, wobei über alle Ideale ungleich 0 von $\mathcal{O}_K$ summiert wird. Die Norm ist strikt multiplikativ auf Idealen. Mit derselben Rechnung wie im Beweis von Lemma 6.12 folgt die Aussage. □

Beispiel. Dirichlet-Charaktere $\chi : (\mathbb{Z}/N)^* \to \mathbb{C}^*$ definieren eine beschränkte, strikt multiplikative Abbildung. Es folgt also

$$L(\chi, s) = \prod_{p\nmid N} \frac{1}{1-\frac{\chi(p)}{p^s}}$$

Insbesondere für den trivialen Charakter folgt

$$L(1, s) = \prod_{p\nmid N} \frac{1}{1-\frac{1}{p^s}} = \prod_{p|N} \left(1-\frac{1}{p^s}\right) \zeta(s)$$

Dies gilt zunächst im Konvergenzbereicht der Reihe, durch meromorphe Fortsetzung dann für $\mathrm{Re} s > 0$.

Beispiel. $\zeta(s)$ konvergiert absolut und lokal gleichmäßig für $\mathrm{Re} s > 1$, also auch das unendliche Produkt

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}} \Rightarrow -\log \zeta(s) = \sum_p \log(1 - \frac{1}{p^s})$$

wobei $|p^{-s}| < 1$ und $\log(1+z)$ durch den Hauptzweig gegeben ist. Es gilt

$$\begin{aligned} \log(1 - p^{-s}) &= \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} \left(\frac{-1}{p^s}\right)^m \\ &= \sum_{m=1}^{\infty} \frac{-1}{mp^{ms}} \end{aligned}$$

Hieraus folgt

$$\log \zeta(s) = \sum_{p,m} \frac{1}{mp^{ms}}$$

und die letzte Reihe ist absolut und lokal gleichmäßig konvergent in $\mathrm{Re} s > 1$.

Satz 6.14. *Sei K ein Zahlkörper. Dann konvergiert die Dedekindsche ζ-Funktion ζ_K absolut und lokal gleichmäßig in* $\mathrm{Re} s > 1$.

Beweis: Wir ersetzen die Reihe durch das Produkt. Es gilt

$$\begin{aligned} \log \zeta_K(s) &= \sum_{\mathfrak{p}} -\log(1 - N(\mathfrak{p})^{-s}) \\ &= \sum_{\mathfrak{p},m} \frac{1}{mN(\mathfrak{p})^{ms}} \\ &= \sum_{p,m} \frac{1}{m} \sum_{\mathfrak{p}|p} p^{-f_{\mathfrak{p}} ms} \end{aligned}$$

wobei $f_{\mathfrak{p}}$ der Restklassengrad von $\mathfrak{p}$ ist. Wir betrachten nun $s > 1$ reell und schätzen ab

$$\begin{aligned} \log \zeta_K(s) &\leq \sum_{p,m} \frac{1}{m} \sum_{\mathfrak{p}|p} p^{-ms} \\ &\leq \sum_{p,m} \frac{1}{m} \frac{d}{p^{ms}} \\ &= d \sum_{p,m} \frac{1}{mp^{ms}} = d \log \zeta(s) \end{aligned}$$

wobei wir die Anzahl der $\mathfrak{p} \mid p$ durch $d = [K : \mathbb{Q}]$ abgeschätzt haben. Aus der Konvergenz von $\log \zeta(s)$ folgt nun die Konvergenz von $\log \zeta_K(s)$. □

Bemerkung. In $s = 1$ hat ζ_K tatsächlich einen Pol (später), der Konvergenzbereich ist also optimal.

Beispiel. Sei $K = \mathbb{Q}(\zeta)$ für $\zeta = \exp(2\pi i/N)$. Die Körpererweiterung $K/\mathbb{Q}$ ist galois, also hängen $f_\mathfrak{p}$ und $e_\mathfrak{p}$ nur von $p = \mathbb{Z} \cap \mathfrak{p}$ ab. Wir schreiben f_p, e_p. Sei $g_p = |\{\mathfrak{p} \mid p\}|$. Es folgt

$$\zeta_K(s) = \prod_p \left(\frac{1}{1 - p^{-f_p s}} \right)^{g_p}$$

Der Ganzheitsring von K ist $\mathbb{Z}[\zeta] = \mathbb{Z}[X]/\Phi_N$ wobei Φ_N das Minimalpolynom ist. Wir haben gesehen, dass p verzweigt ist genau für $p \mid N$ (oder Übungsaufgabe). Sei nun $p \nmid N$. Es folgt

$$\mathbb{Z}[\zeta]/p = \mathbb{F}_p[X]/\Phi_N = \prod \mathbb{F}_{p^f}$$

wobei $\mathbb{F}_{p^f} = \mathbb{F}_p(\overline{\zeta})$ mit $\overline{\zeta}$ eine primitive N-te Einheitswurzel in $\overline{F}_p$ ist. Die Elemente von $\mathbb{F}_{p^f}$ sind Einheitswurzeln der Ordnung $p^f - 1$, also folgt

$$N \mid p^f - 1$$

f ist die kleinste Zahl mit $N \mid p^f - 1$, also die kleinste Zahl mit $p^f = 1 \mod N$. Die Potenz g_p wird durch $g_p f = \phi(N)$ bestimmt.

Kapitel 7

Der Dirchletsche Dichtesatz

Theorem 7.1. *Sei $N \geq 1$, $a \in \mathbb{Z}$ mit $(N, a) = 1$. Dann gibt es unendlich viele Primzahlen von der Form $nN + a$ für $n \in \mathbb{Z}$.*

Bemerkung. Für $(N, a) \neq 1$ haben alle Terme einen Teiler ungleich 1 gemeinsam, also kann es nicht unendlich viele Primzahlen in der Folge geben.

Definition 7.2. *Sei A eine Menge von Primzahlen. Die* Dichte *von A ist*

$$\lim_{s \to 1} \frac{\sum_{p \in A} p^{-s}}{\log(s-1)^{-1}}$$

wobei der Grenzwert über $s > 1$ reell gebildet wird.

Lemma 7.3. *Sei $\mathcal{P}$ die Menge aller Primzahlen. Dann hat $\mathcal{P}$ die Dichte 1. Ist A endlich, so ist die Dichte 0.*

Beweis: Für A endlich gilt

$$\lim_{s \to 1} \frac{\sum_{p \in A} p^{-s}}{\log(s-1)^{-1}} = \frac{\sum_{p \in A} p^{-1}}{\lim_{s \to 1} \log(s-1)^{-1}} = 0$$

Wie wir bereits gesehen haben, gilt

$$\log \zeta(s) = \sum_{p,m} \frac{1}{mp^{ms}} = \sum_{p \in \mathcal{P}} p^{-s} + \sum_{p \in \mathcal{P}, m \geq 2} \frac{1}{mp^{ms}}$$

Für festes p gilt

$$\sum_{m=2}^{\infty} \frac{1}{mp^{ms}} \leq \sum_{m=2}^{\infty} p^{-m} = p^{-2}(1 - p^{-1})$$

Also

$$\sum_{p \in \mathcal{P}, m \geq 2} \frac{1}{mp^{ms}} \leq \sum_{p} \frac{1}{p(p-1)} \leq \sum_{n=1}^{\infty} \frac{1}{n(n-1)} \leq \infty$$

Für die Berechnung der Dichte kann also $\sum_{p\in\mathcal{P}} p^{-s}$ durch $\log\zeta(s)$ ersetzt werden. Weiterhin schreiben wir $\zeta(s) = (s-1)^{-1} + h$ mit einer beschränkten Funktion h, also

$$\log(\zeta(s)) - \log\frac{1}{s-1} = \log\zeta(s)(s-1) = \log(1+h(s-1))$$

und diese Funktion ist beschränkt. Damit ist die Dichte 1. □

Theorem 7.4. *Sei $N \geq 1$, $a \in \mathbb{Z}$ mit $(a,N) = 1$. Se $\mathcal{P}_a$ die Menge der Primzahlen mit $p = a \mod N$. Dann hat $\mathcal{P}_a$ die Dichte $\phi(N)^{-1}$.*

Bemerkung. Insbesondere ist die Dichte ungleich 0, also hat $\mathcal{P}_a$ unendlich viele Elemente. Dies zeigt Theorem 7.1.
Der Beweis des Dichtesatzes benötigt etwas Anlauf.

Lemma 7.5. *Sei G eine endliche abelsche Gruppe, $\hat{G} = \mathrm{Hom}(G,\mathbb{C}^*)$ sei die Gruppe der Charaktere. Dann gilt $|G| = |\hat{G}|$.*
Für alle $x \in G \setminus \{e\}$ gibt es $\chi \in \hat{G}$ mit $\chi(x) \neq 1$. Es gilt

$$\sum_{\chi\in\hat{G}} \chi(x) = \begin{cases} |G| & x = e \\ 0 & \textit{sonst} \end{cases}$$

Beweis: Sei $G = C_1 \times C_2 \times \cdots \times C_k$ wobei alle C_i zyklisch sind. Es folgt

$$\mathrm{Hom}(G,\mathbb{C}^*) = \mathrm{Hom}(C_1,\mathbb{C}^*) \times \cdots \times \mathrm{Hom}(C_k,\mathbb{C}^*)$$

Ein Charakter von C_1 ist eindeutig bestimmt durch das Bild eines Erzeugers y_1. Dieses Bild muss eine $|C_1$-te Einheitswurzel sein, davon gibt es $|C_1|$ viele. Es folgt also $|C_1| = |\hat{C}_1|$. Hieraus folgt wiederum die Aussage für G.
Sei nun $x \in G, x \neq e$. Wir schreiben $x = (x_1,\ldots,x_k)$ mit $x_i \in C_i$. Eine Komponente von x ist ungleich e, z.B. $x_1 = y_1^{e_1}$. Wir wählen $\chi_1 : C_1 \to \mathbb{C}^*$ mit $\chi_1(y_1) = \zeta$, so dass $\zeta^{e_1} \neq 1$. Wir wählen weiter $\chi_2,\ldots,\chi_k = 1$. Dann folgt $\chi(x) = \prod \chi_i(x_i) = \chi_1(x_1)1 \neq 1$.
Schließlich sei $x \in G$, $\psi : \hat{G} \to \mathbb{C}^*$ der Charakter, der durch $\chi \mapsto \chi(x)$ definiert ist. Nach Lemma 6.11 gilt

$$\sum_{\chi} \chi(x) = \sum_{\chi\in\hat{G}} \psi(x) = \begin{cases} |\hat{G}| & \psi = 1 \\ 0 & \text{sonst} \end{cases}$$

Der erste Fall tritt ein, wenn $\chi(x) = 1$ für alle χ, also genau für $x = e$. Wegen $|\hat{G}| = |G|$ folgt die Behauptung. □

Lemma 7.6. *Zum Beweis von Theorem 7.4 genügt es zu zeigen, dass $L(\chi,1) \neq 0$ für alle Dirchletcharaktere $\chi : (\mathbb{Z}/N)^* \to \mathbb{C}^*$ ungleich 1.*

Beweis: Wir studieren

$$g_a(s) = \sum_{p \in \mathcal{P}_a} p^{-s} = \phi(N)^{-1} \sum_{\chi} \chi(a)^{-1} f_\chi(s)$$

wobei

$$f_\chi(s) = \sum_{p \nmid N} \frac{\chi(p)}{p^s}$$

Beachte dabei:

$$\sum_{\chi} \chi(a)^{-1} \sum_{p \nmid N} \frac{\chi(p)}{p^s} = \sum_{p \nmid N} \frac{1}{p^s} \sum_{\chi} \chi(a^{-1}p) = \sum_{p \nmid N} \frac{1}{p^s} \begin{cases} \phi(N) & a^{-1}p = 1 \mod N \\ 0 & a^{-1}p \neq 1 \mod N \end{cases}$$

Dabei ist $a^{-1}p = 1 \mod N \Leftrightarrow p = a \mod N \Leftrightarrow p \in \mathcal{P}_a$.
Wir schreiben nun $\sim$, wenn sich zwei Funktionen in der Nähe von 1 um etwas Beschränktes unterscheiden.
1. Fall: $\chi = 1$.

$$f_\chi(s) = \sum_{p \nmid N} \frac{1}{p^s} \sum_{p} \frac{1}{p^s} \sim \log \frac{1}{s-1}$$

nach Lemma 7.3.
2. Fall: $\chi \neq 1$. Nach Voraussetzung ist $L(\chi, 1) \neq 1$. Damit gilt ist $L(\chi, s) = \prod(1 - \chi(p)/p^s)^{-1}$ beschränkt nahe 1 und (Wahl des Hauptzweigs rechts für $s > 1$ reell, richtiger Zweig links)

$$\begin{aligned} \log L(\chi, s) &= -\sum \log \left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_{m,p} \frac{\chi(p)^m}{m p^m s} \\ &= f_\chi(s) + \sum_{m \geq 2} \frac{\chi(p)^m}{m p^m s} \end{aligned}$$

Nach dem Beweis von 7.3 ist die letzte Sumem beschränkt für $s \to 1$. Also

$$f_\chi(s) \sim 0$$

Hieraus folgt

$$g_a(s) = \phi(N)^{-1} \sum_{\chi} \chi(a)^{-1} f_\chi(s) \sim \phi(N)^{-1} 1 \log \frac{1}{s-1} + 0$$

Damit ist die Dichte $\phi(N)^{-1}$. □

Lemma 7.7. *Für $p \nmid N$ gilt:*

$$\prod_{\chi} (1 - \chi(p)T) = (1 - T^{f_p})^{g_p}$$

wobei f_p die kleinste Zahl ist, so dass $p^{f_p} = 1 \mod N$. (dies ist die Ordnung von p in $(\mathbb{Z}/N)^*$) und $g_p = \phi(N)/f_p$.

Beweis: Sei W die Menge der f_p-ten Einheitswurzeln in $\mathbb{C}$. Es gilt also

$$\prod_{w \in W} (1 - wT) = 1 - T^{f_p}$$

Wegen $\chi(p)^{f_p} = \chi(p^{f_p}) = \chi(1) = 1$ liegt $\chi(p)$ in W. Wir wollen zeigen, dass jeder Wert vorkommt. Sei $N = q_1^{n_1} \dots q_k^{n_k}$ die Primfaktorzerlegung, also

$$(Z/N)^* = (\mathbb{Z}/q_1^{n_1})^* \times \dots \times (\mathbb{Z}/q_k^{n_k})^*$$

Nach Definition ist f_p die Ordnung von p in $(\mathbb{Z}/N)^*$, also das kgV der Ordnungen f_i von p in $(\mathbb{Z}/q_i^{n_i})^*$.

Behauptung. *Es gibt einen Charakter χ_i von $(\mathbb{Z}/q_i^{n_i})^*$, so dass $\chi_i(p)$ die Ordnung f_i hat.*

Die Abbildung $(\mathbb{Z}/q^n)^* \to (\mathbb{Z}/q)^* = \mathbb{F}_q^*$ ist surjektiv. Der Kern ist isomorph zu $\mathbb{Z}/q^{n-1}$ (Übungsaufgabe). Das Bild ist zyklisch als Untergruppe der multiplikativen Gruppe eines Körpers. Die Ordnungen sind teilerfremd, daher folgt $(\mathbb{Z}/q^n)^* \cong (\mathbb{Z}/q)^* \times \mathbb{Z}/q^{n-1}$. Da die Gruppe zyklisch ist, gibt es einen injektiven Charakter nach $\mathbb{C}^*$. Die ist das gesuchte χ_i.
Sei nun $\tilde{\chi} = \chi_1 \times \dots \chi_k$. Nach Konstruktion hat $\tilde{\chi}(p)$ die Ordnung f_p. Also durchläuft $\chi(p)$ alle Elemente von W, wenn χ die Charaktergruppe durchläuft. Die Abbildung

$$\widehat{(\mathbb{Z}/N)^*} \to \mathbb{C}^*, \qquad \chi \mapsto \chi(p)$$

ist ein Gruppenhomomorphismus, also wird jeder Wert gleich oft angenommen, nämlich

$$\frac{\left|\widehat{(\mathbb{Z}/N)^*}\right|}{|W|} = \frac{\phi(N)}{f_p} = g_p$$

mal. □

Übungsaufgabe. *Sei $U_1 = \mathrm{Ker}(\mathbb{Z}/q^n)^* \to (\mathbb{Z}/q)^* = 1 + p\mathbb{Z}/q^n$. Betrachte die Abbildung $a \mapsto (1+a)^p$. Zeigen Sie: Dies ist ein Isomorphisms $\mathbb{Z}/q^{n-1} \to U_1$.*

Korollar 7.8. *Sei $N \geq 1$, ζ eine primitive N-te Einheitswurzel. Dann gilt*

$$\prod_{\chi \in \widehat{(\mathbb{Z}/N)^*}} L(\chi, s) = \zeta_{\mathbb{Q}(\zeta)}(s) \prod_{\mathfrak{p} \mid N} (1 - N(\mathfrak{p})^{-s})$$

Beweis: Wir hatten uns bereits überlegt, dass

$$\zeta_{\mathbb{Q}(\zeta)}(s) = \prod_{\mathfrak{p} \mid N} (1 - N(\mathfrak{p})^{-s}) \prod_{p \nmid N} (1 - p^{-f_p s})^{-g_p}$$

Nun vergleichen wir die Eulerprodukte. □

Theorem 7.9. *Sei $N \geq 1$, ζ eine primitive N-te Einheitswurzel. Dann hat $\zeta_{\mathbb{Q}(\zeta)}$ einen einfachen Pol in $s = 1$. Für nichttriviale Dirichletcharaktere $\chi : (\mathbb{Z}/N)^* \to \mathbb{C}^*$ gilt $L(\chi, 1) \neq 0$.*

Beweis: Wir betrachten die Produktformel des Lemmas. Die Faktoren $1-N(\mathfrak{p})^{-s}$ sind ganze Funktionen. Die $L(\chi, s)$ sind holomorph in $\mathrm{Re}s > 0$, mit höchstens einem einfachen Pol in $s = 1$ für $\chi = 1$. Also ist $L(\chi, 1) \neq 0$ äquivalent zu $\zeta_{\mathbb{Q}(\zeta)}$ singulär in $s = 1$.
Angenommen, die Funktion

$$\zeta_{\mathbb{Q}(\zeta)}(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

ist holomorph in $s = 1$, also in $\mathrm{Re}s > 0$.

Behauptung. *Die Reihe konvergiert für* $\mathrm{Re}s > 0$

Wir betrachten die Taylorreihenentwicklung von $\zeta_{\mathbb{Q}(\zeta)}$ um dem Punkt $s = 2$. Die Reihe hat Konvergenzradius mindestens 2. Wir bestimmen die Koeffizienten der Taylorreihe: Wegen $(n^{-s})' = (-\log n)n^{-s}$ und lokal gleichmäßiger Konvergenz gilt

$$\zeta^{(k)}_{\mathbb{Q}(\zeta)}(s) = \sum_{n=1}^{\infty} (-\log n)^k \frac{a_n}{n^s}$$
$$\zeta^{(k)}_{\mathbb{Q}(\zeta)}(2) = (-1)^k \sum_{n=1}^{\infty} (\log n)^k \frac{a_n}{n^2}$$

Damit lautet die Taylorreihe:

$$\zeta_{\mathbb{Q}(\zeta)}(s) = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \left(\sum_{n=1}^{\infty} (\log n)^k \frac{a_n}{n^2} \right) (s-2)^k$$

Für $s = 1 - \varepsilon$ mit $0 < \varepsilon < 1$ erhalten wir

$$\zeta_{\mathbb{Q}(\zeta)}(1-\varepsilon) = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \sum_{n=1}^{\infty} (\log n)^k \frac{a_n}{n^2} (-\varepsilon - 1)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=1}^{\infty} (\log n)^k \frac{a_n}{n^2} (1+\varepsilon)^k$$

Alle Terme der Doppelsumme sind positiv, daher dürfen wir umordnen. Daher konvergiert die Reihe

$$\zeta_{\mathbb{Q}(\zeta)}(1-\varepsilon) = \sum_n \frac{a_n}{n^2} \sum_k \frac{1}{k!} (1+\varepsilon)^k (\log n)^k = \sum_n \frac{a_n}{n^2} n^{1+\varepsilon}$$

Die ist genau die Dirichlet-Reihe im Punkt $s = 1 - \varepsilon$.
Die Dirchlet-Reihe konvergiert jetzt, und sogar absolut. Nach Lemma 6.12 konvergiert dann auch das Eulerprodukt für $\mathrm{Re}s > 0$. Für $s > 0$ reell schätzen wir

ab:

$$\begin{aligned}\prod_{p\nmid N}\frac{1}{\left(1-\frac{1}{p^{f_p s}}\right)^{g_p}} &= \prod_{m\nmid N}\left(\sum_{m=0}^{\infty}\frac{1}{p^{f_p m s}}\right)^{g_p}\\ &\geq \prod_{m\nmid N}\sum_{m=0}^{\infty}\frac{1}{p^{f_p g_p m s}}\\ &= \prod_{m\nmid N}\frac{1}{1-\frac{1}{p^{\phi(N)s}}}\end{aligned}$$

Speziell für $s=\phi(n)^{-1}$ ist dieses Produkt aber divergent. Dieser Widerspruch zeigt $L(\chi,1)\neq 0$. □

Damit ist auch der Beweis des Dichtesatzes 7.1 und 7.4 abgeschlossen.

Der Primzahlsatz

Definition 7.10. *Für $x>0$ sei $\pi(x)$ die Anzahl die Primzahlen kleiner gleich x.*

Wir schreiben ab jetzt $f\sim g$ für $\lim_{x\to\infty} f(x)/g(x)=1$.

Theorem 7.11 (Primzahlsatz). *Es gilt*

$$\pi(x)\sim\frac{x}{\log x}\qquad \textit{für } x\to\infty$$

Der hier vorgestellte Beweis stammt von D. Newman in der Darstellung von D. Zagier "Newman's short proof of the prime number theorem", Am. Math. Montly 104 (97) 705-708.
$O(f)$ ist ein Größe, die durch ein festes Vielfaches von x beschränkt wird.

Lemma 7.12. *Sei $\vartheta(x)=\sum_{p\leq x}\log p$. ϑ ist ein $O(x)$ für $x\to\infty$.*

Beweis: Für $n\in\mathbb{N}$ gilt

$$2^{2n}=(1+1)^{2n}=\sum\binom{2n}{i}\geq\binom{2n}{n}\geq\prod_{n<p\leq 2n}p=\exp(\vartheta(2n)-\vartheta(n))$$

Dies bedeutet $2n\log 2\geq\vartheta(2n)-\vartheta(n)$ zunächst für natürliche Zahlen n. Hieraus folgt

$$\vartheta(x)-\vartheta(x/2)<Cx$$

für ein festes C. Sei x_0 fest. Wir summieren nun

$$\vartheta(x)\leq Cx+\vartheta(x/2)\leq Cx+Cx/2+\vartheta(x/4)\leq\dots$$

Sei $r(x)$ so, dass $x/2^{r(x)}\geq x_0>x/2^{r(x)+1}$. Wir erhalten

$$\vartheta(x)\leq Cx(1+1/2+1/4+\dots+1/2^{r(x)})+\vartheta(x_0)=O(x)$$

□

Lemma 7.13. *Es gilt $\vartheta(x) \sim \pi(x)\log x$. Der Primzahlsatz ist also äquivalent zu $\vartheta(x) \sim x$.*

Beweis: Es gilt

$$\vartheta(x) = \sum_{p\le x} \log p \le \sum_{p\le x} \log x = \pi(x)\log x$$

Für jedes $1 > \delta > 0$ gilt:

$$\begin{aligned}\vartheta(x) &\ge \sum_{x^{1-\delta}\le p\le x} \log p \ge \sum_{x^{1-\delta}\le p\le x} (1-\delta)\log x \\ &= (1-\delta)\log x[\pi(x) - \pi(x^{1-\delta})] \ge (1-\delta)\log x[\pi(x) - x^{1-\delta}]\end{aligned}$$

Also

$$\pi(x) \le x^{1-\delta} + \frac{\vartheta(x)}{(1-\delta)\log x}$$

Nach Voraussetzung ist der zweite Summand $O(x/\log x)$. Der erste ist es ebenfalls. Die beiden Abschätzungen zusammen implizieren

$$1 \le \frac{\pi(x)\log x}{\vartheta(x)} \le \frac{x^{1-\delta}\log x}{\vartheta(x)} + \frac{1}{1-\delta}$$

Für jedes $\varepsilon > 0$ gibt es δ, so dass

$$\frac{1}{1-\delta} \le 1 + \varepsilon/2$$

Wähle x_0, so dass für $x > x_0$

$$\frac{x^{1-\delta}\log x}{\vartheta(x)} < \frac{A\log x}{x^{\delta}} < \varepsilon/2$$

Es folgt für diese x

$$1 \le \frac{\pi(x)\log x}{\vartheta(x)} < 1 + \varepsilon$$

Da ε beliebig ist, folgt die Assymptotik. □

Lemma 7.14. *Sei $\Phi(s) = \sum_p \frac{\log p}{p^s}$. Die Funktion $\Phi(s) - (s-1)^{-1}$ ist holomorph für* Re$s \ge 1$.

Beweis: Zunächst für Re$s > 1$, wo die ζ-Funktion eine konvergierende Euler-Produktdarstellung hat:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^s - 1} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}$$

Die hintere Summe konvergiert für Re$s > 1/2$ (z.B. Vergleich mit $\zeta'(s/2)$). Also hat $\Phi(s)$ eine meromorphe Fortsetzung nach Re$s > 1/2$. Einzige (einfache)

Polstellen sind $s = 1$ und die Nullstellen von $\zeta(s)$. In $s = 1$ hat $-\zeta'(s)/\zeta(s)$ einen einfachen Pol mit Residuum 1. In diesem Punkt ist also $\Phi(s) - (s-1)^{-1}$ holomorph.
In $s = 1+i\alpha$ für $\alpha \in \mathbb{R} \setminus \{0\}$ habe $\zeta(s)$ die Ordnung μ, in $1+2i\alpha$ die Ordnung μ. Wegen $\overline{\Phi}(s) = \Phi(\overline{s})$ haben die Punkte $1-i\alpha$ und $1-2i\alpha$ ebenfalls die Ordnungen μ und ν. Das Residuum von Φ in diesen Punkten ist dann $-\mu$ bzw. $-\nu$. Wir berechnen es als Grenzwert $\lim_{h\to 0} h\Phi(1+h+i\alpha)$ für $h > 0$ reell. Nun benutzen wir

$$0 \le \sum_p \frac{\log p}{p^{1+h}}(p^{i\alpha/2} + p^{-i\alpha/2})^4 = \sum_p \frac{\log p}{p^{1+h}} \sum_r \binom{4}{2r} p^{-ir\alpha}$$
$$= \sum_{r=-2}^{2} \binom{4}{2r} \Phi(1+h+ir\alpha)$$

Also gilt

$$1(-\nu) + 4(-\mu) + 6 \cdot 1 + 4(-\mu) + 1(-nu) = 6 - 8\mu - 2\nu \ge 0$$

Hierausfolgt $\mu = 0$. □

Satz 7.15. *Sei $f(t)$ für $t \ge 0$ eine beschränkte und lokal integrierbare Funktion. Die Funktion*

$$g(z) = \int_0^\infty f(t)e^{-zt}dt$$

für $\mathrm{Re}z > 0$ *habe eine holomorphe Fortsetzung nach* $\mathrm{Re}z \ge 0$. *Dann existiert das Integral $\int_0^\infty f(t)$ und ist gleich $g(0)$.*

Beweis: Für $T > 0$ sei

$$g_T(z) = \int_0^T f(t)e^{-zt}dt$$

Diese Funktion ist holomorph für alle z. Wir zeigen nun $\lim g_T(0) = g(0)$. Sei R groß, δ klein genug, C der Rand des Gebietes $G = \{z \in \mathbb{C} \mid |z| \le R, \mathrm{Re}z \ge -\delta\}$, so dass $g(z)$ holomorph auf $\overline{G}$ ist. Dann gilt nach dem Residuensatz

$$g(0) - g_T(0) = \frac{1}{2\pi i}\int_C (g(z) - g_T(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}$$

Auf dem Halbkreisbogen $C_+ = C \cap \{\mathrm{Re}z > 0\}$ ist der Integrand durch $2B/R^2$ beschränkt, wobei $B = \max|f(t)|$, denn

$$|g(z) - g_T(z)| = \left|\int_T^\infty f(t)e^{-zt}dt\right| \le B\int_T^\infty |e^{-zt}|dt = \frac{Be^{\mathrm{Re}zT}}{\mathrm{Re}z}$$
$$\left|e^{zT}(1 + \frac{z^2}{R^2})\frac{1}{z}\right| = e^{\mathrm{Re}zT}\frac{2\mathrm{Re}z}{R^2}$$

Damit ist der Beitrag der Kurve C_+ zum Integral beschränkt durch B/R.

Für das Integral über $C_- = C \setminus C_+$ behandeln wir g und g_T getrennt. Da g_T ganz ist, kann das Integral über C_- durch den Halbkreis $C'_- = C \cap \{|z| = R, \mathrm{Re} z < 0\}$. Dieses Integral wird durch B/R beschränkt mit dem gleichen Argument wie vorher, da

$$|g_T(z)| = \left| \int_0^T f(t) e^{-zt} dt \right| \leq B \int_{-\infty}^T |e^{-zt}| dt = \frac{B e^{-\mathrm{Re} z T}}{-\mathrm{Re} z}$$

Das letzte Integral über C_- strebt gegen 0 für $T \to \infty$, denn der Integrand ist das Produkt der Funktion $g(1+z^2/R^2)/z$ (unabhängig von T) und der Funktion e^{zT}, gleichmäßig auf kompakten Mengen gegen 0 geht. Damit folgt

$$\limsup_{T \to \infty} |g(0) - g_T(0)| \leq 2B/R$$

Da R beliebig war, folgt das Theorem. □

Satz 7.16. *Es gilt* $\vartheta(x) \sim x$.

Beweis: Zunächst eine Hilfsrechnung: Für $\mathrm{Re} s > 1$ gilt

$$\Phi(s) = \sum_p \frac{\log p}{p^s} = \int_1^\infty \frac{\vartheta(x)}{x^s} = \frac{\vartheta(x)}{x^s}\Big|_1^\infty + s \int_1^\infty \frac{\vartheta(x)}{x^{s+1}} dx = s \int_0^\infty e^{-st} \vartheta(e^t) dt$$

wobei $\theta(x) x^{-s} \to 0$ für $x \to \infty$ wegen 7.14. Wir wenden nun den Satz auf die Funktion $f(t) = \vartheta(e^t) e^{-t} - 1$. Sie ist beschränkt nach 7.12. Die zugehörige Funktion $g(z)$ ist

$$g(z) = \int_0^\infty (\vartheta(e^t) e^{-t} - 1) e^{-zt} dt = \frac{\Phi(z+1)}{z+1} - \frac{1}{z}$$

Diese ist nach 7.14 holomorph in $\mathrm{Re} z \geq 0$ nach 7.14). Daher konvergiert nun das Integral

$$\int_0^\infty (\vartheta(e^t) e^{-t} - 1 dt = \int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$$

Behauptung. $\vartheta(x) \sim x$

Angenommen nun, es gebe $\lambda > 1$, so dass für beliebig große x immer noch $\vartheta(x) \geq \lambda x$. Da ϑ monoton ist, gilt

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2} dt \geq \int_x^{\lambda x} \frac{\lambda t - t}{t^2} dt = \int_1^\lambda \frac{\lambda - u}{u^2} du > 0$$

(mit $u = tx$). Dies ist ein Widerspruch zur Konvergenz des Integrals. Andererseits angenommen, es gebe $\lambda < 1$, so dass $\theta(x) \leq \lambda x$ für beliebig große x. Dann folgt

$$\int_{\lambda x}^x \frac{\vartheta(t) - t}{t^2} dt \leq \int_{\lambda x}^x \frac{\lambda t - t}{t^2} dt = \int_\lambda^1 \frac{\lambda - u}{u^2} du < 0$$

(mit $u = t^{-1} x$). Auch dies ist ein Widerspruch zur Konvergenz des Integrals. □

Kapitel 8

Die Klassenzahlformel

Sei $K/\mathbb{Q}$ eine endliche Erweiterung. Wir wollen zeigen:

Satz 8.1. *$\zeta_K(s)$ ist holomorph in $\{\mathrm{Re}\, s > 1 - 1/n\} \setminus \{1\}$ mit einem einfachen Pol in $s = 1$.*

Dafür verwenden wir das Kriterium 6.9: Für $\sum a_n/n^s$, $A_m = a_1 + \cdots + a_m$ mit $|A_m - m\varrho| \leq C$ ist die durch die Reihe definierte Funktion holomorph in $\mathrm{Re}\, s > 0$ bis auf einen einfachen Pol in 1 mit Residuum ϱ. Wir werden also nicht nur den Satz beweisen, sondern auch gleich das Residuum berechnen.
Unser Fall ist $\sum_{\mathfrak{a} \subset \mathcal{O}_K} N(\mathfrak{a})^{-s}$, also

$$a_n = |\{\mathfrak{a} \mid N(\mathfrak{a}) = n\}|, \qquad A_m = |\{\mathfrak{a} \mid N(\mathfrak{a}) \leq m\}|$$

Wir müssen also das Wachstumsverhalten der Funktion

$$j(t) = |\{\mathfrak{a} \mid N(\mathfrak{a}) \leq t\}|$$

untersuchen.
Sei $\mathrm{Cl}(K)$ die Klassengruppe von K, $c \in \mathrm{Cl}(K)$.

$$j(c, t) = |\{\mathfrak{a} \mid \mathfrak{a} \in c, N(\mathfrak{a}) \leq t\}|$$

Wir formulieren diese Bedingung um.
Sei $\mathfrak{b} \subset \mathcal{O}_K$ ein Ideal mit $\mathfrak{b} \in c^{-1}$, d.h. $\mathfrak{ab} = (x)$ ein Hauptideal. Wegen $\mathfrak{a} \subset \mathcal{O}_K \Rightarrow \mathfrak{ab} \subset \mathfrak{b} \Leftrightarrow x \in \mathfrak{b}$. Umgekehrt $x \in \mathfrak{b}$ mit $\mathfrak{ab} = (x)$, dann folgt $\mathfrak{a} \subset \mathcal{O}_K$ ($ax = \alpha x$ mit $\alpha \in \mathcal{O}_K$, also $a = \alpha$). Hieraus folgt

$$j(c, t) = |\{(x) \mid x \in \mathfrak{b}, |N(x)| = N(\mathfrak{ab}) = N(\mathfrak{b})N(\mathfrak{a}) \leq N(\mathfrak{b})t\}|$$

Weiterhin $(x) = (x')$ genau dann, wenn $x = ux'$ für $u \in \mathcal{O}_K^*$. Also schließlich

$$j(c, t) = |\{x \in \mathfrak{b} \setminus \{0\} \mid |N(x)| \leq N(\mathfrak{b})t\}/\mathcal{O}_K^*|$$

Die Abschätzung dieser Mengen benutzt wieder die Methoden der Gitthertheorie aus Kapitel 4.

Wiederholung der Gitterpunkttheorie

$n = [K : \mathbb{Q}]$, $\sigma_i : K \to \mathbb{C}$ für $i = 1, \ldots, n$ die Einbettungen. Dabei seien $\sigma_1, \ldots, \sigma_{r_1}$ die reellen, $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ nicht-konjugierte komplexe Einbettungen. Die *kanonische Einbettung* ist

$$\sigma : \mathfrak{b} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n, \qquad \alpha \mapsto (\sigma_i(\alpha))_{i=1}^{r_1+r_2}$$

Nach Korollar 4.10 ist $\sigma(\mathfrak{b})$ ein Gitter mit Volumen

$$2^{-r_2} d^{1/2} N()$$

Sei $N(x, y) = \prod_{i=1}^{r_1} |x_i| \prod_{j=1}^{r_2} |y_j|^2$, also $N(\sigma(x)) = |N(x)|$. Die Funktion $j(c, t)$ zählt genau die Punkte des Gitters in

$$\{(x_i, y_j) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid N(x, y) \leq N(\mathfrak{b})t\}$$

modulo der Operation von $\mathcal{O}_K^*$.
Nach dem Dirichletschen Einheitensatz 4.14 gilt $\mathcal{O}_K^* \cong G \times \mathbb{Z}^{r_1+r_2-1}$ mit endlichem G. Genauer: Für

$$L : \mathcal{O}_K^* \to \mathbb{R}^{r_1+r_2}, \qquad u \mapsto (\log |\sigma_i(x)|)_{i=1}^{r_1+r_2}$$

ist $L(\mathcal{O}_K^*)$ ein Gitter in

$$W = \{(x_i', y_j') \mid \sum_{i=1}^{r_1} x_i' + 2 \sum_{j=1}^{r_2} y_j' = 0\}$$

Der Kern von L ist genau G. Sei $w = |G|$, also die Anzahl der Einheitswurzeln in G.
Seien nun $\eta_1, \ldots, \eta_{r_1+r_2-1} \in \mathcal{O}_K^*$ Fundamentaleinheiten, also $L(\eta_i)$ eine Basis von $L(\mathcal{O}_K^*)$. Wir setzen $V =< \eta_1, \ldots, \eta_{r_1+r_2-1} >$, also $\mathcal{O}^*/V \cong G$. Dann folgt:

$$\begin{aligned} j(c, t) &= \frac{1}{w} |\sigma(\mathfrak{b} \setminus \{0\}) \cap \{(x, y) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid N(x, y) \leq N(\mathfrak{b})\}/V| \\ &= \frac{1}{w} |\sigma(\mathfrak{b}) \cap \{(x, y) \in (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \mid N(x, y) \leq N(\mathfrak{b})\}/V| \end{aligned}$$

Sei nun $D \subset (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$ ein Fundamentalbereich für die V-Operation. Dann gilt

$$wj(c, t) = |\sigma(\mathfrak{b}) \cap \{(x, y) \in D \mid N(x, y) \leq N(\mathfrak{b})t\}|$$

Wir wählen

$$P \cdots \subset W \subset \mathbb{R}^{r_1+r_2}$$

das Parallelogramm aufgespannt von den Basisvektoren $L(\eta_1), \ldots, L(\eta_{r_1+r_2-1})$. Wir betrachten

$$g : (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \to W, \qquad (x_i, y_j) \mapsto \left(\log |\mathfrak{x}_\mathfrak{i}| N(x, y)^{1/n}, \log |\mathfrak{y}_\mathfrak{j}| N(x, y)^{1/n}\right)$$

Lemma 8.2. *$D = g^{-1}(P)$ ist ein Fundamentalbereich für V mit $tD = D$ für alle $t > 0$ reell.*

Beweis: Sei $t > 0$,

$$g(tx_i, ty_j) = \left(\log \frac{t|x_i|}{N(tx,ty)^{1/n}}, \log \frac{t|y_j|}{N(tx,ty)^{1/n}}\right) = g(x,y)$$

wegen $N(tx, ty) = t^n N(x, y)$.

Behauptung. *g hat Werte in W.*

$$\sum \log \frac{|x_i|}{N(x,y)^{1/n}} + 2\sum \log \frac{|y_j|}{N(x,y)^{1/n}}$$
$$= \sum \log |x_i| + 2\sum \log |y_j| - \frac{1}{n} \log N(x,y)(r_1 + 2r_2) = 0$$

Behauptung. *g ist V-äquivariant.*

Sei $\eta \in V$, $(x, y) \in (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$. Nach Definition

$$g(\eta(x,y)) = g(\sigma_i(\eta)x_i, \sigma_j(\eta)y_j) = \left(\log \frac{|\sigma_i(\eta)x_i|}{N(\eta(x,y))^{1/n}}, \log \frac{|\sigma_j(\eta)y_i|}{N(\eta(x,y))^{1/n}}\right)$$

Nach Definition

$$N(\sigma_i(\eta)x_i, \sigma_j(\eta)y_j) = \prod |\sigma_i(\eta)x_i| \prod |\sigma_j(\eta)y_j| = |N(\eta)|N(x_i, y_j) = N(x_i, y_j)$$

Hieraus folgt

$$g(\eta(x,y)) = \left(\log|\sigma_i(\eta)| + \log \frac{|x_i|}{N(x,y)^{1/n}}, \log|\sigma_j(\eta)| + \log \frac{|y_j|}{N(x,y)^{1/n}}\right)$$
$$= L(\eta) + \eta(x,y)$$

Da P ein Fundamentalbereich für das Gitter $L(V)$ ist, ist nun automatisch D ein Fundamentalbereich für V.

□

Definition 8.3. *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter, $M \subset \mathbb{R}^n$ eine Teilmenge.*

$$\lambda(t) = \lambda_{\Lambda,M}(t) = |\Lambda \cap tM|$$

Korollar 8.4. *Sei $c \in \mathrm{Cl}(K)$, w die Anzahl der Einheitswurzeln in K, $\mathfrak{b} \subset \mathcal{O}_K$ mit $\mathfrak{b} \in c^{-1}$. Sei $D_1 = \{(x,y) \in D \mid N(x,y) \leq 1\}$ mit D wie oben. Dann gilt*

$$j(c,t) = \frac{1}{w}\lambda_{\sigma(\mathfrak{b}),D_1}((N(\mathfrak{b})t)^{1/n})$$

(i) *Beweis:* Wir wissen bereits

$$j(c,t) = \frac{1}{w}|\sigma(\mathfrak{b}) \cap \{(x,y) \in D \mid N(x,y) \leq tN(\mathfrak{b})\}|$$

Wir betrachten $(x',y') = (N(\mathfrak{b})t)^{1/n})(x,y)$. Dann gilt

$$N((N(\mathfrak{b})t)^{1/n})(x,y)) = N(\mathfrak{b})tN(x,y)$$

Also ist $(x,y) \in D_1$ genau dann, wenn $(x',y') \in D$ mit $N(x',y') \leq tN(\mathfrak{b})$. □

Um unsere Frage nach dem Verhalten von ζ_K zu beantworten, benötigen wir also Assymptotiken für $\lambda(t)$.

Beispiel. $n = 1$, $\Lambda = \mathbb{Z}$, $M = (0,m) \subset \mathbb{R}$. Dann ist $\lambda(t) = [tm]$ die Gaußklammer. Es gilt

$$[tm] \sim tm + O(1)$$

Für $n = 2$, $\Lambda = \mathbb{Z}^2$, $M = (0,m_1) \times (0,m_2)$ folgt

$$\lambda(t) \sim tm_1 \cdot tm_2 = t^2 \mathrm{vol}(M)$$

Theorem 8.5. *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter, $M \subset \mathbb{R}^n$ eine messbare Teilmenge, so dass ∂M überdeckt wird durch das Bild von endlich vielen differenzierbaren Abbildungen $\phi : I^{n-1} \to \partial M$ ($I = [0,1]$). Dann gilt*

$$\lambda(t) = \frac{\mathrm{vol}(M)}{\mathrm{vol}(M)} t^n + O(t^{n-1})$$

Beweis: Sei $\omega_1, \ldots, \omega_n$ eine Basis von Λ, $F = \{t_1\omega_1 + \cdots + t_n\omega_n \mid 0 \leq t_i < 1\}$ ein Fundamentalbereich des Gitters. Sei $l \in \Lambda \subset \mathbb{R}^n$. Dann impliziert $l \in tM$ offensichtlich $l + F \cap tM \neq \emptyset$.
Entweder $l + F \subset (tM)^\circ$ (das Innere) oder $l + F \cap \partial tM \neq \emptyset$. Sei

$$m(t) = |\{l \in \Lambda \mid l + F \subset (tM)^\circ\} \qquad b(t) = |\{l \in \Lambda \mid l + F \cap \partial tM \neq \emptyset\}$$

Es folgt

$$m(t) \leq \lambda(t) \leq m(t) + b(t)$$

Daher

$$m(t)\mathrm{vol}(F) \leq \mathrm{vol}(tM) \leq (m(t) + b(t))\mathrm{vol}(F)$$
$$\Rightarrow m(t) \leq \frac{\mathrm{vol}(M)t^n}{\mathrm{vol}F} \leq m(t) + b(t)$$

Es genügt also zu zeigen:

Behauptung. $b(t) = O(t^{n-1})$

$\partial tM = t\partial M$ wird nach Voraussetzung durch endlich viele $\phi : I^{n-1} \to \partial M$ überdeckt. Es genügt, das Bild einer solchen Abbildung zu betrachten.
Wir zerschneiden I in $[t]$ gleiche Intervalle, also I^{n-1} in $[t]^{n-1}$ Würfel W_{klein}. Da ϕ differentzierbar ist, gilt

$$|\phi(x) - \phi(y)| \leq C|x - y|$$

für eine Konstante C. Daher hat das Bild eines der kleinen Würfel unter $\phi(W_{\text{klein}})$ den Durchmesser $\leq C/[t]$. Dann hat $t\phi(W_{\text{klein}})$ Durchmesser $\leq Ct/[t] < 2C$. Die Anzahl der Gitterpunkte in einer Kugel vom Radius $2C$ ist beschränkt, d.h.

$$|t\phi(W_{\text{klein}}) \cap \Lambda| \leq C' \Rightarrow |t\phi(I^{n-1}) \leq t^{n-1}C'$$

□

Theorem 8.6. *Sei K ein Zahlkörper, c eine Idealklasse von K. Dann gilt*

$$j(c,t) = \varrho t + O(t^{1-1/n})$$

mit

$$\varrho = \frac{2^{r_1}(2\pi)^{r_2}R}{wd^{1/2}}$$

wobei r_1 und r_2 die Anzahl der reellen bzw. komplexen Einbettungen ist, w die Anzahl der Einheitswurzeln in K, $d = |d_{K/\mathbb{Q}}$ die absolute Diskriminante, R der Regulator

$$R = \left|\det\left(N_i \log|\sigma_i(\eta_j)|\right)_{i,j=1,\ldots,r_1+r_2}\right|$$

wobei $N_i = 1$ für reelle σ_i, $N_i = 2$ für komplexe.

Korollar 8.7. *Die Funktion*

$$\zeta_c(s) = \sum_{\mathfrak{a}\in c} N(\mathfrak{a})^{-s}$$

ist holomorph in $\{\text{Re}s > 1 - 1/n\} \setminus \{1\}$ mit einem einfach Pol in $s = 1$ mit Residuum ϱ.

Korollar 8.8 (Klassenzahlformel). *ζ_K ist holomorph in $\{\text{Re}s > 1 - 1/n\} \setminus \{1\}$ mit einem einfach Pol in $s = 1$ mit Residuum $h\varrho$.*

Beweis: $\zeta_K = \sum \zeta_c$ □

Beweis von Theorem 8.6. Wir wollen Theorem 8.5 anwenden. Es besagt

$$\begin{aligned} j(c,t) &= \frac{1}{w}\lambda((N(\mathfrak{b})t)^{1/n}) = \frac{1}{w}\left(\frac{\text{vol}D_1}{\text{vol}\mathfrak{b}}N(\mathfrak{b})t + O((N(\mathfrak{b})t)^{1/n(n-1)})\right) \\ &= \frac{1}{w}\left(\frac{\text{vol}D_1}{2^{-r_2}N(\mathfrak{b})d^{1/2}}N(\mathfrak{b})t\right) + O(t^{1-1/n}) \end{aligned}$$

Behauptung. $\text{vol}D_1 = 2^{r_1}\pi^{r_2}R$.

Wir betrachten nach Definition

$$g : (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \to W, \qquad (x_i, y_j) \mapsto \Big(\log|\mathfrak{x}_\mathfrak{i}|N(x,y)^{1/n}, \log|\mathfrak{y}_\mathfrak{j}|N(x,y)^{1/n}\Big)$$

D_1 war die Menge der (x, y) mit $g(x, y)$ im Fundamentalparallelogramm aufgespannt von den $L(\eta_i)$ und $N(x, y) \leq 1$.
Wir wollen das Volumen der Teilmenge $D_1 \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ berechnen, die durch die folgenden Bedingungen definiert ist:

(i) $0 < N(x_i, y_j) \leq 1$

(ii) Es gibt $0 \leq c_q < 1$ für $q = 1, \ldots, r$, so dass für alle i und j

$$\log \frac{|x_i|}{N(x_i, y_j)^{\frac{1}{n}}} = \sum c_q \log|\sigma_i \eta_q|$$

(bzw. selbe Formel mit y_j).

Sei $y_j = \varrho_j \theta_j$ $(j = r_1 + 1, \ldots, r_1 + r_2)$ die Polarkoordinatendarstellung. Es gilt

$$\mathrm{vol}(D_1) = (2\pi)^{r_2} 2^{r_1} \int_{\tilde{D}_1} \varrho_{r_1+1} \ldots \varrho_{r_1+r_2} dx_1 \ldots dx_{r_1} d\varrho_{r_1+1} \ldots d\varrho_{r_1+r_2}$$

wobe $\tilde{D}_1 \subset \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$ durch die Bedingungen

(i) $0 < x_i, \varrho_j$ für $i = 1, \ldots, r_1$ und $j = r_1 + 1, \ldots, r_1 + r_2$

(ii) $0 < \prod x_k \prod \varrho_l^2 \leq 1$

(iii) Es gibt $0 \leq c_q < 1$ für $q = 1, \ldots, r$, so dass für alle i und j

$$\log x_i - \frac{1}{n} \log \prod x_k \prod \varrho_l^2 = \sum c_q \log|\sigma_i \eta_q|$$

definiert ist. (Beachte: Die weggelassene θ_j-Variable trägt jeweils 2π bei, das Weglassen der negativen x_i trägt je einen Faktor 2 bei, es gilt $dy_j = \varrho_j d\theta_j d\varrho_j$.)
Sei $S = \{(u, c_1, \ldots, c_r) \mid 0 < u, c_q \leq 1\}$. Wir betrachten:

$$\begin{aligned} f : S &\to \tilde{D}_1 \\ (u, c_q) &\mapsto \Big(u^{\frac{1}{n}} \exp\Big(\sum c_q \log|\sigma_i(\eta_q)|\Big)\Big)_{i=1}^{r_1+r_2} \end{aligned}$$

(i) Die Abbildung ist wohldefiniert, d.h. hat Bild in $\tilde{D}_1$: Positivität ist klar.

$$\begin{aligned} N(f(u, c_q)) &= \prod_{i=1}^{r_1} u^{\frac{1}{n}} \exp\Big(\sum c_q \log|\sigma_i(\eta_q)|\Big) \prod_{j=r_1}^{r_1+r_2} u^{\frac{2}{n}} \exp\Big(2\sum c_q \log|\sigma_i(\eta_q)|\Big) \\ &= u^{\frac{r_1+2r_2}{n}} \exp\left(\sum_q c_q \log|N(\eta_q)|\right) = u \end{aligned}$$

da alle η_q Norm ± 1 haben. Durch Logarithmieren der Definition erhält man

$$\log f_i - \frac{1}{n} \log u = \sum c_q \log |\sigma_i(\eta_q)|$$

Dies ist die dritte Bedingung für $\tilde{D}_1$ nach unserer Berechnung für u.

(ii) Die Abbildung f ist surjektiv: Zu einem Tupel (x_i, ϱ_j) setzt man $u = N(x_i, \varrho_j)$ und wählt die c_q aus der dritten Bedingung für $\tilde{D}_1$.

(iii) Die Abbildung f ist injektiv: u ist eindeutig festgelegt. Die c_q für $q = 1, \ldots, r$ werden aus einem inhomogenen Gleichungssystem zur Matrix

$$(\log |\sigma_i \eta_q|)_{i,q}$$

bestimmt. Zu zeigen ist, dass diese Matrix den Rang r hat. Die Zeilen sind die Werte der logarithmischen Einbettung $L(\eta_q)$. Diese spannen nach Wahl der η_q einen r-dimensionalen Modul auf, d.h. der Zeilenrang ist r.

Der nächste Schritt ist die Umrechnung des Integrals über $\tilde{D}_1$ in ein Integral über S. Hierfür muss die Funktionaldeterminante von f bestimmt werden.

$$\frac{\partial f_i}{\partial u} = \frac{1}{n} u^{\frac{1}{n}-1} \exp(\dots) = \frac{1}{nu} f_i$$
$$\frac{\partial f_i}{\partial c_q} = u^{\frac{1}{n}} \exp(\cdots) \log |\sigma_i \eta_q| = f_i \log |\sigma_i \eta_q|$$

Zu berechnen ist die Determinante der Matrix mit i-ter Zeile

$$\left(\frac{\partial f_i}{\partial u}, \frac{\partial f_i}{\partial c_q} \right)$$

Zunächst wird aus der ersten Spalte der Faktor $\frac{1}{nu}$ herausgezogen, dann aus der i-ten Zeile der Faktor $f_i = x_i$ bzw $f_j = \varrho_j$. Dies liefert den Wert

$$\frac{x_1 \ldots x_{r_1} \varrho_{r_1+1} \ldots \varrho_{r_1+r_2}}{nu} \left| (1, \log |\sigma_i \eta_1|, \ldots, |\sigma_i \eta_r|)_i \right|$$

Der Bruch kann nach Definition von u gekürzt werden. Desweiteren wird die i-te Zeile mit N_i multipliziert, wobei $N_i = 1$ für σ_i reell und $N_i = 2$, wenn σ_i imaginär. Die Funktionaldeterminante ist also

$$\frac{1}{n \varrho_{r_1+1} \ldots \varrho_{r_1+r_2}} 2^{-r_2} \left| (N_i, N_i \log |\sigma_i \eta_1|, \ldots, N_i |\sigma_i \eta_r|)_i \right|$$

Alle Zeilen werden zur letzten addiert, die dann die Form $(n, 0, \ldots, 0)$ erhält, da die $L(\eta_q)$ genau diese Relation erfüllen. Die verbleibende Determinante ist nR nach Definition des Regulators R. Also insgesamt:

$$\frac{1}{\varrho_{r_1+1} \cdots \varrho_{r_1+r_2}} 2^{-r_2} R$$

Dies ermöglicht endlich unsere Volumenberechnung:

$$\begin{aligned}\mathrm{vol}D_1 &= (2\pi)^{r_2}2^{r_1}\int_{\tilde{D}_1} \varrho_{r_1+1}\dots\varrho_{r_1+r_2}dx_1\dots dx_{r_1}d\varrho_{r_1+1}\dots d\varrho_{r_1+r_2}\\ &= (2\pi)^{r_2}2^{r_1}\int_S \frac{2^{-r_2}R}{\varrho_{r_1+1}\cdots\varrho_{r_1+r_2}}\varrho_{r_1+1}\dots\varrho_{r_1+r_2}dx_1\dots dx_{r_1}d\varrho_{r_1+1}\dots d\varrho_{r_1+r_2}\\ &= (\pi)^{r_2}2^{r_1}R\end{aligned}$$

da S ein Einheitswürfel ist.

Behauptung. *Der Rand von D_1 ist differenzierbar parametrisierbar durch I^{n-1}*

Der Rand von $\tilde{D}_1$ wird durch den Rand von S parametrisiert, also durch endlich viele $n-1$-dimensionale Würfel überdeckt. Einziges Problem: die Funktion f ist nicht differenzierbar für $u=0$, da $u^{\frac{1}{n}}$ in 0 nicht differenzierbar ist. Ersetzt man die Variable u durch $v=u^{\frac{1}{n}}$, so nimmt f die Form $f_i = v\exp(\dots)$ an und ist differenzierbar auch für $v\to 0$.

Exkurs: Klassenzahlformeln für $L(\chi,s)$

Die Dedekindsche ζ-Funktion erfüllt eine Funktionalgleichung, die den Wert in s und $1-s$ in Verbindung bringt, insbesondere also 0 und 1. Die Formel in 8.8 übersetzt sich in

$$\zeta_K(0)^* = -\frac{hR}{w}$$

wobei w die Anzahl der Einheitswurzeln in K ist, h die Klassenzahl und R der Regulator. Für eine meromorphe Funktion f bezeichnet $f(z_0)^*$ den führenden Koeffizienten der Laurent-Reihe. Tatsächlich hat ζ_K in 0 meist eine Nullstelle. Sei nun $K=\mathbb{Q}(\zeta)$ mit $\zeta=\exp(2\pi i/N)$. Dann gilt

$$\zeta_K(s) = \prod L(\chi,s)$$

wobei χ die Charaktere von $(\mathbb{Z}/N)^*$ durchläuft. Genauer: $L(\chi,s)$ ist die L-Funktion zu minimalem $f|N$, so dass χ durch $(\mathbb{Z}/f)^*$ faktorisiert. Hieraus folgt:

$$\zeta_K(0)^* = \prod L(\chi,0)^*$$

Frage: Gibt es Klassenzahlformeln für $L(\chi,0)^*$?
Idee: $(\mathbb{Z}/N)^*$ ist die Galoisgruppe von $K/\mathbb{Q}$. Alle Terme der Klassenzahlformel stammen von Gruppen mit einer $G=\mathrm{Gal}(K/\mathbb{Q})$-Operation her.

- $h=|\mathrm{Cl}(K)|$: hierauf operiert G, da G auf Idealen operiert (vergleiche Lemma 5.9).
- w ist die Anzahl der Menge der Einheitswurzeln, hier operiert G auf jeden Fall.

- R ist im wesentlichen das Volumen von $L(\mathcal{O}_K^*) \subset W$. Auf $\mathcal{O}_K$ operiert G, auf W durch Vertauschen der Komponenten, da $g\sigma_i$ ein anderes σ_j sein muss.

Übungsaufgabe. *Die Abbildung L ist G-äquivariant.*

Definition 8.9. *Sei M ein $\mathbb{C}$-Vektorraum mit G-Operation, χ ein Charakter von G.*

$$M(\chi) = \{m \in M \mid gm = \chi(g)m\}$$

heißt χ-Eigenraum der G-Operation.

Lemma 8.10. *Es gilt*

$$M = \bigoplus_\chi M(\chi)$$

Beweis: Lineare Algebra: Existenz von gemeinsmane Eigenräumen zu allen $g \in G$, da diese kommutieren.
Explizit: Sei

$$p_\chi : M \to M \qquad m \mapsto \frac{1}{|G|} \sum \chi(g)^{-1} gm$$

Dies ist ein Projektor, d.h. $p_\chi^2 = p_\chi$. Es gilt $M(\chi) = p_\chi M$ und $\sum p_\chi = 1$. □

Analoge Idee:

$$\mathrm{Cl}(K) = \sum_\chi \mathrm{Cl}(\chi), h = \prod h(\chi) \text{ wobei } \; h(\chi) = |\mathrm{Cl}(\chi)|$$

Ebenso $w = \prod w(\chi)$, $R = \prod R(\chi)$.
Erster Versuch:

$$L(\chi, 0)^* = \pm \frac{h(\chi)R(\chi)}{w(\chi)}$$

Problem: Es handelt sich um endliche, endlich erzeugte abelsche Gruppen oder kompakte abelsche Gruppen, aber nicht um $\mathbb{C}$-Vektorräume.
Das Lemma ist *falsch* für solche Gruppen. Wir versuchen $\mathrm{Cl}(\chi) = p_\chi \mathrm{Cl}(K)$ als Definition.

- Wie multipliziert man Idealklassen mit Einheitswurzeln?
- Wie teilt man durch $|G|$?

Sei $\mathcal{O} = \mathbb{Z}[\chi(g) : g \in G]$. Dies ist ein Zahlring. Auf $C' = \mathrm{Cl}(K) \otimes_{\mathbb{Z}} \mathcal{O}$ können wir mit Einheitswurzeln multiplizieren. Da $\mathcal{O}/\mathbb{Z}$ eine endliche Erweiterung ist (Grad d), ist auch C' endlich. Die Anzal der Elemente von $\mathrm{Cl}(K)$ kann aus der Anzahl der Elemente von C' errechnet werden, nämlich $h = |C'|/d$. Wir setzen nun:

$$\mathrm{Cl}(\chi) = \frac{1}{d}(|G|p_\chi)C'$$

Die Gruppen C' und $\bigoplus \mathrm{Cl}(\chi)$ unterscheiden sich um endliche Gruppen, deren Ordnung nur durch die Primteiler von $|G|$ teilbar ist. Es folgt also $\prod \mathrm{Cl}(\chi) = h$ bis auf Primfaktoren, die $|G|$ teilen. Ebenso gehen wir für $w(\chi)$ und $R(\chi)$ vor.

Theorem 8.11 (Mazur, Wiles, 1984). *Bis auf Einheiten und Primfaktoren, die $\phi(N)$ teilen, gilt*

$$L(\chi, 0)^* = \frac{h(\chi)R(\chi)}{w(\chi)}$$

Dies kann man aus der sogenannten *Hauptvermutung von Iwasawa* herleiten.
Grundidee: Man betrachtet nicht eine Körper alleine, sondern den gesamten Turm von Körpern $K(\zeta_{p^n})$, wobei ζ_{p^n} eine primitive p^n-te Einheitswurzel ist.

Was ist mit Primzahlen, die $|G|$ teilen?
Bloch-Kato (1990) schlagen ganz allgemein Klassenzahlformeln für alle L-Funktionen von algebraischen Varietäten über $\mathbb{Q}$ an allen ganzen Zahlen vor. Die Gruppen $\mathrm{Cl}(K)$ und $\mu(K)$ (Gruppe der Einheitswurzeln) werden hierbei durch Kohomologie von Galoismoduln ersetzt. In dieser kohomologischen Sprache können dann auch die schlechten Primzahlen behandelt werden. Für die guten ergibt sich nichts Neues.

Theorem 8.12 (Huber, Kings, 2003). *Die Bloch-Kato-Vermutung gilt für $L(\chi, n)^*$, wobei χ ein Dirichlet-Charakter ist und $n \in \mathbb{Z}$.*

Für $n > 1$ kommen hier algebraische K-Gruppen ins Spiel. Wieder ist die Hauptvermutung eine der Hauptzutaten, jetzt aber in kohomologischer Fassung. Nicht der Beweis von Mazur und Wiles, sondern die sogenannte Euler-System-Methode von Kolyvagin-Rubin führt zu ihrem Beweis.

Der Fall von elliptischen Kurven

Sei E eine elliptische Kurve über $\mathbb{Q}$. Wir wählen definierende Gleichungen über $\mathbb{Z}$. Sei N_p die Anzahl der Punkte der elliptischen Kurve über $\mathbb{F}_p$.
Für die Primzahlen guter Reduktion (fast alle) setzen wir

$$a_p = |p + 1 - N_p| \qquad P_p(T) = 1 - a_p T + pT^2$$

Für die schlechten Primzahlen ist $P_p = 1 \pm T$ oder $P_p = 1$, je nach Verhalten modulo $\mathbb{F}_p$.

Definition 8.13. $L(E, s) = \prod \frac{1}{P_p(p^{-s})}$ *heißt L-Funktion der elliptischen Kurve.*

Übungsaufgabe. *Die Hasse-Schranke lautet $|p+1-N_p| \leq 2\sqrt{p}$. Untersuchen Sie hiermit den Konvergenzbereicht des Produktes.*

Alternativ: Nach Wiles gehört jede elliptische Kurve zu einer Spitzenform mit q-Entwicklung $\sum a_n q^n$. Dann ist

$$L(E, s) = \sum a_n n^{-s}$$

Die Reihe konvergiert für $\mathrm{Re} s > 3/2$. Die Funktion ist ganz auf $\mathbb{C}$. Diese Funktion hat eine Funktionalgleichung, die s und $2-s$ verbindet. Besonders interessant ist $s = 1$.

Vermutung 8.14 (Birch-Swinnerton-Dyer (1963)). *$L(E, s)$ hat in $s = 0$ die Nullstellenordnung gleich dem Rang der Mordell-Gruppe $E(\mathbb{Q})$.*

Es gibt auch eine genaue Vorhersage für den führenden Koeffizienten. Auch diese Vermutung lässt sich als Spezialfall der Bloch-Kato-Vermutung auffassen.
Das Problem ist mit einer Million Dollar dotiert!
Bekannt: viele, viele numerische Beispiele. Außdem der kritische Fall, d.h. Funktion verschwindet nicht.

□

Kapitel 9

Bewertungstheorie

Definition 9.1. *Sei k ein Körper. Ein* Absolutbetrag *v ist ein Abbildung*

$$k \to \mathbb{R} \qquad\qquad x \mapsto |x|_v$$

so dass

(i) $|x|_v \geq 0$ *und* $|x|_v = 0 \Leftrightarrow x = 0$.

(ii) Für alle $x, y \in k$ *gilt* $|xy|_v = |x|_v |y|_v$.

(iii) $|x + y|_v \leq |x|_v + |y|_v$.

Ein Absolutbetrag definierte eine Topologie via: $U \subset k$ heißt offen, falls für alle $x \in U$ ein $\varepsilon > 0$ existiert, so dass $\{y \in k \mid |y - x|_v < \varepsilon\} \subset U$.

Beispiel.

- $\mathbb{R}, \mathbb{C}$ mit dem gewöhnlichen Absolutbetrag, ebenso $\mathbb{Q}$.
- Für $p \in \mathbb{Q}$ eine Primzahl $|x|_p = p^{-v(x)}$, wobei $v(x)$ die Vielfachheit von p in x ist.

Definition 9.2. *Sei k ein Körper. Eine* diskrete Bewertung *ist eine Abbildung $v : k \to \mathbb{Z} \cup \{\infty\}$ mit*

(i) $v(x) = \infty \Leftrightarrow x = 0$.

(ii) $v(xy) = v(x) + v(y)$.

(iii) $v(x + y) \geq \min(v(x), v(y))$

Lemma 9.3. *Sei v eine diskrete Bewertung, $a > 1$ fest. Dann ist $|x|_v = a^{v(x)}$ ein Absolutbetrag.*

Beweis: Die Eigenschafte (i) und (ii) sind klar.
Dreiecksungleichung:

$$a^{-v(x+y)} \leq a^{\min(v(x),v(y))} \leq a^{-v(x)} + a^{-v(y)}$$

□

Beispiel. Sei $\mathcal{O}$ ein Dedekindring, $\mathfrak{p}$ ein Primideal, K der Quotientenkörper von $\mathcal{O}$. Für $x \in K^*$ sei $(x) = \prod \mathfrak{q}^{v_\mathfrak{q}(x)}$ die Produktzerlegung in Primideale. Dann ist die Abbildung $v : K^* \to \mathbb{Z}$ mit $x \mapsto v_\mathfrak{p}(x)$ eine diskrete Bewertung.

Definition 9.4. *Sei* $\operatorname{Char} k = 0$. *Ein Betrag heißt* kanonisch*, wenn seine Einschränkung auf* $\mathbb{Q}$ *mit* $|\cdot|$ *oder einem* $|\cdot|_p$ *übereinstimmt.*

Wir interessieren uns nur für die kanonischen Beträge.

Definition 9.5. *Zwei Absolutbeträge heißen äquivalent, wenn sie dieselbe Topologie induzieren.*

Lemma 9.6. *Seine* $|\cdot|_1$ *und* $|\cdot|_2$ *äquivalente Absolutbeträge. Dann gibt es* $\lambda > 0$*, so dass* $|x|_1 = |x|_2^\lambda$.

Beweis: Wir betrachten

$$\{x \in k \mid |x|_1 < 1\} = \{x \mid \lim_{n\to\infty} x^n = 0\}$$

Dies ist die gleiche Menge wie für $|\cdot|_2$, da Grenzwerte nur von der Topologie abhängen. Also:

$$|x|_1 > 1 \Leftrightarrow |x|_2 > 1$$

Wenn $|x|_1 = 1$ für alle $x \neq 0$, dann ist die Topologie diskret. Die Aussage gilt dann trivialerweise.
Sei also $y \in k$ mit $a = |y|_1 > 1$. Sei $b = |y|_2$. Für $x \in k^*$ gbit es $\alpha \geq 0$ mit $|x|_1 = a^\alpha$. Seien $m, n \in \mathbb{N}$ mit $m/n \geq \alpha$. Dann folgt

$$|x|_1 < |y|_1^{m/n} \Rightarrow \left|\frac{x^n}{y^m}\right|_1 < 1$$

$$\Rightarrow \left|\frac{x^n}{y^m}\right|_2 < 1 \Rightarrow |x|_2 < b^{m/n}$$

Ebenso argumentiert man für $m/n < \alpha \Rightarrow |x|_2 > b^{m/n}$. Da die Ungleichungen für alle m, n gelten, erhalten wir $|x|_2 = b^\alpha$. Mit anderen Worten

$$|x|_1 = a^\alpha = b^{\alpha \log_b a} = |x|_2^{\log_b a}$$

Dies beweist die Behauptung mit $\lambda = \log_b a$. □

Ein Körper heißt *vollständig*, wenn jede Cauchy-Folge konvergiert. Ist k ein Körper mit Absolutbetrag v, dann ist k_v (der Körper der Cauchy-Folgen in k modulo Nullfolgen) ein vollständiger Körper bezüglich der Fortsetzung von v. Dieser Körper k_v heißt *Komplettierung* von k. (Beweise wie in Analysis).

Beispiel. $\mathbb{R}$ ist die Komplettierung von $\mathbb{Q}$ bezüglich $|\cdot|$. Sei $\mathbb{Q}_p$ die Komplettierung von $\mathbb{Q}$ bezüglich $|\cdot|_p$. Dies ist der Körper der p-adischen Zahlen.

Definition 9.7. *Sei* $\operatorname{Char} k = 0$. k *heißt* lokaler Körper*, wenn er Komplettierung eines Zahlkörpers bezüglich eines kanonischen Betrages ist.*

Diese Körper wollen wir klassifizieren. Es gilt übrigens eine glattere Charakterisierung:

Theorem 9.8. *Sei* $\operatorname{Char} k = 0$. *Dann ist* k *lokal genau dann, wenn* k *vollständig, lokalkompakt und nicht-diskret.*

Beweis: vergl. Weil, Basic number theory §3. □

Zur Erinnerung: ein metrischer Raum ist lokalkompakt, wenn jede beschränkte Folge eine konvergente Teilfolge hat.

Satz 9.9. *Sei* K *ein Zahlkörper,* $\mathfrak{p}$ *ein Primideal,* $|\cdot|_v$ *der Absolutbetrag zur* $\mathfrak{p}$*-adischen Bewertung* $v_\mathfrak{p} : K^* \to \mathbb{Z}$. *Sei* K_v *die Komplettierung von* $K_\mathfrak{p}$ *bezüglich* v.

(i) $v_\mathfrak{p}$ *ist eine diskrete Bewertung auf* K_v.

(ii) Der topologische Abschluss $\mathcal{O}_v$ *von* $\mathcal{O}_K$ *in* K_v *ist* $\{x \in K_v \mid |x| \leq 1\}$, *ein diskreter Bewertungsring mit Restklassenkörper* $\mathcal{O}_K/\mathfrak{p}$.

(iii) $\mathcal{O}_v$ *ist kompakt,* K_v *ist lokalkompakt.*

Beweis: Sei $x \in K_v$, $x = \lim x_i$ mit $x_i \in K$. D.h. für alle $\varepsilon > 0$ gibt es N, so dass $|x_i - x_j| < \varepsilon$ für alle $i, j > N$. Also

$$|x_i| = |x_i - x_j + x_j| \leq \max(|x_i - x_j|, |x_j|) \leq \max(\varepsilon, |x_j|)$$

1. Fall: $x = 0$. Dann bilden die x_j eine Nullfolge.
2. Fall: $x \neq 0$, die x_i bilden keine Nullfolge. Dann gibt es $\varepsilon_0 > 0$, so dass für jedes N ein $i > N$ gibt mit $|x_i| > \varepsilon_0$. Für alle $\varepsilon < \varepsilon_0$ folgt dann $|x_i| \leq |x_j|$. Also wird $|x_i$ konstant.
$|x| = |x_i|$ für großes i hat denselben Wertebereich wie der Betrag auf K, insbesondere ist er diskret. Ebenso ist $v(x) = \lim v(x_i)$ konstant, die Bewertung auf K_v ist diskret.
Sei

$$\mathcal{O}_v = \{x \in K_v \mid |x| \leq 1\} = \{x \in K_v \mid v(x) \geq 0\}$$

Sei $\mathcal{O}_\mathfrak{p} = \{a/s \in K \mid a \in \mathcal{O}, s \in \mathcal{O} \setminus \mathfrak{p}\}$ die Lokalisierung des Ganzheitsrings in $\mathfrak{p}$.

Behauptung. $\mathcal{O}_v$ *ist der topologische Abschluss von* $\mathcal{O}_\mathfrak{p}$.

$Oh_\mathfrak{p}$ ist ein lokaler Hauptidealring (vergleiche Satz 5.3). Das einzige Primideal wird erzeugt von $\pi \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Nach Definition $v(\pi) = 1$. Jedes Element von K^* ist von der Form $u\pi^r$ mit $u \in \mathcal{O}_\mathfrak{p}^*$ und $r \in \mathbb{Z}$. Es gilt $\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_v$, denn $v(a/s) = v(a) - v(s) = v(a) \geq 0$. Sei $x \in \mathcal{O}_v$, also $x = \lim x_i$, $x_i \in K$, $v(x) \geq 0$. Hieraus folgt, wie wir gesehen haben $v(x_i) > 0$ für i groß genug.
Offensichtlich ist $K \cap \mathcal{O}_v = \mathcal{O}_\mathfrak{p}$. Sei $x \in K_v^*$, $r = v(x) \in \mathbb{Z}$. Dann ist $x = u\pi^r$ mit $v(u) = 0$, also $u \in \mathcal{O}_v^*$. Demnach ist auch $\mathcal{O}_v$ ein Hauptidealring, einziges Primideal (π).

Beachte (Satz 5.3

$$\mathcal{O}/\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \to \mathcal{O}_v/(\pi)$$

Die Abbildung ist injektiv, da es ein Körperhomomorphismus ist.

Behauptung. *Die Abbildung ist surjektiv.*

Sei $x = \lim x_i$ mit $x_i \in \mathcal{O}_\mathfrak{p}$. Es gilt $v(x - x_i) \to \infty$, insbesondere $v(x - x_i) \geq 1$ für i groß genug, d.h. $\pi \mid x - x_i$. Hieraus folgt $x = x_i$ modulo π, also liegt x modulo π im Bild von $\mathcal{O}_\mathfrak{p}$. Dies beendet den Beweis von (ii).
Sei x_i eine Folge in $\mathcal{O}_v$. Seien $\overline{x}_i$ die Bilder in $\mathcal{O}_v/(pi)$. Dies ist ein endlicher Körper. Nach dem Schubfachprinzip enthält eine Restklasse unendlich viele Elemente, d.h. eine Teilfolge ist konstant modulo π. Iteration dieses Argumentes liefert Teilfolgen, die konstant sind modulo π^2, dann modulo π^3. Die Diagonalfolge wird für i groß genug konstant modulo π^n, d.h. $v(x_i - x_j) \geq n$ für i, j groß genug. Die x_i bilden eine Cauchy-Folge. Der Grenzwert existiert dann in $\mathcal{O}_v$.
Abgeschlossene Kugeln in K_v sind von der Form $x + \pi^r \mathcal{O}_v$, also kompakt. □

Satz 9.10. *Sei k ein vollständiger, lokalkompakter Körper mit Absolutbetrag, E/k endlich. Dann setzt sich der Betrag von k auf höchstens eine Weise nach E fort. E ist bezüglich dieses Betrages vollständig und lokalkompakt.*

Beweis: Seien $|\cdot|_1$ und $|\cdot|_2$ zwei Fortsetzung nach E. Wie in der reellen Analysis zeigt man, dass E vollständig und lokalkompakt ist. Ebenso zeigt man (nur Lokalkompaktheit geht ein), dass sie äquivalent sind , d.h. dieselbe Topologie induzieren. Nach Lemma 9.6 gilt dann $|\cdot|_1 = |\cdot|_2^\lambda$. Setzt man $x \in k$ ein, so folgt $\lambda = 1$. □

Satz 9.11. *Sei K ein Zahlkörper, k der Abschluss von K bezüglich eines Betrages, der $|\cdot|_p$ fortsetzt. Dann ist k eine endliche Erweiterung von $\mathbb{Q}_p$.*

Bemerkung. Insbesondere gilt für alle $\sigma \in \mathrm{Gal}(E/k)$ die Gleichung $|\sigma(x)| = |x|$, da $|\sigma \cdot|$ ein neuer Betrag ist.

Beweis: Wir betrachten das Kompsitum $K\mathbb{Q}_p$, den Teilkörper von K_v, der von K und $\mathbb{Q}_p$ erzeugt wird. Er ist endlich über $\mathbb{Q}_p$. Da $\mathbb{Q}_p$ lokalkompakt ist, ist es nun auch $K\mathbb{Q}_p$ (Satz 9.10) lokalkompakt und vollständig. Damit ist $K\mathbb{Q}_p = K_v$, also ist dieser Körper endlich. □

Lemma 9.12. *Sei $k/\mathbb{Q}_p$ endlich, $\mathcal{O}_p$ der ganze Abschluss von $\mathbb{Z}_p$ in k.*

(i) $\mathcal{O}_p$ ist diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$.

(ii) Der p-adische Betrag auf $\mathbb{Q}_p$ setzt sich nach k fort und gehört zu $\mathfrak{p}$.

Beweis: Wir betrachten den ganzen Abschluss $\mathcal{O}_p$. Der Ring ist ganz abgeschlossen. Mit denselben Argumenten wie im Beweis von Theorem 1.10 (der Fall des Ganzheitsrings) zeigt man, dass $\mathcal{O}_p$ endlich erzeugt über $\mathbb{Z}_p$ ist, insbesondere also noethersch. Wie im Beweis von Satz 3.1 ist $\mathcal{O}_p$ nun ein Dedekindring. Wähle nun $\mathfrak{p} \subset \mathcal{O}_p$ ein Primideal ungleich 0. Dann ist $p \in \mathfrak{p}$. Der Betrag $|\cdot|_\mathfrak{p}$ setzt

- bei geeigneter Normierung - den Betrag $|\cdot|_p$ fort. Nach Satz 9.10 ist diese Fortsetzung eindeutig. Wegen

$$\mathfrak{p} = \{x \in \mathcal{O}_p \mid |x|_\mathfrak{p} < 0\}$$

legt dies auch das Primideal eindeutig fest. Damit ist $\mathcal{O}_p$ ein diskreter Bewertungsring. □

Bemerkung. Insbesondere ist $\mathcal{O}_p$ ein Hauptidealring. $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ ist ein Erzeuger.

Theorem 9.13. *Sei $k/\mathbb{Q}_p$ endlich. Dann gibt es einen Zahlkörper $K/\mathbb{Q}$ mit $[K : \mathbb{Q}] = [k : \mathbb{Q}_p]$ und $K \subset k$ ist dicht, d.h. k ist Abschluss von K bezüglich eines Betrages, der $|\cdot|_p$ fortsetzt.*

Beweis: Nach Lemma 9.12 gibt es einen Betrag auf k, der $|\cdot|_p$ fortsetzt. Er ist eindeutig nach Satz 9.10 eindeutig. Wir schreiben $|\cdot|_p$ auch für die Fortsetzung. Sei $k = \mathbb{Q}_p(\alpha)$ (Satz vom primitiven Element), $f = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Q}_p[X]$ das Minimalpolynom. Wähle $g = X^d + b_1X^{d-1} + \cdots + b_d \in \mathbb{Q}[T]$ mit $|a_i - b_i|_p < epsilon$. Es gilt

$$f = \prod(X - \alpha_i) \qquad \alpha_i \in \overline{\mathbb{Q}}_p$$
$$g = \prod(X - \beta_i) \qquad \beta_i \in \overline{\mathbb{Q}}$$

Die Differenz

$$|f(\alpha) - g(\alpha)|_p = |0 - \prod(\alpha - \beta_i)|_p = \prod|\alpha - \beta_i|$$

ist klein nach Wahl der b_i, also ist ein Faktor klein. Also wird jede Wurzel von f durch eine Wurzel von g approximiert. Weiterhin sind alle Wurzeln von f verschieden, da das Polynom separabel ist. Für genügend kleines ε sind dann auch alle Wurzeln von g verschieden, d.h. g ist irreduzibel. Sei β die Nullstelle von g, die α approximiert. Wir setzen $K = \mathbb{Q}(\beta)$.

Behauptung. $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ *für ε klein genug.*

Beide Körper sind in k', der normalen Hülle von $\mathbb{Q}_p(\alpha, \beta)$ enthalten. $k'/\mathbb{Q}_p$ ist galois.
Wir überprüfen $\alpha \in \mathbb{Q}_p(\beta) = (k')^{\mathrm{Gal}(k'/\mathbb{Q}_p(\beta)}$ (Hauptsatz der Galoistheorie). Da $|\beta - \alpha|_p$ klein ist, gilt

$$|\beta - \alpha|_p < 1/2|\sigma(\alpha) - \alpha|_p \qquad \sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta)) \text{ falls } \sigma(\alpha) \neq \alpha$$

Sei $\tau \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$. Dann folgt $|\tau(\gamma)|_p = |\gamma|_p$ für alle $\gamma \in k'$ nach der Bemerkung nach Satz 9.10. Es folgt

$$|\beta - \tau\alpha|_p = |\tau\beta - \tau(\alpha)|_p < 1/2|\sigma\alpha - \alpha|_p$$

Hieraus folgt

$$|\tau\alpha - \alpha| = |\tau\alpha - \beta + \beta - \alpha|_p$$

für alle $\sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$ mit $\sigma(\alpha) \neq \alpha$. Dies impliziert $\tau(\alpha) = \alpha$ für alle τ. Damit haben wir $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$ gezeigt. Die andere Inklusion wird genau gezeigt.
Auf K erhalten wird durch Einschränken des Betrages auf k eine Absolutbetrag, der $|\cdot|_p$ fortsetzt. Da $d = [K : \mathbb{Q}] = [k : \mathbb{Q}_p]$ stimmt k mit der Komplettierung von K überein. □

Korollar 9.14. *k ist lokal, d.h. Komplettierung eines kanonischen Betrages auf einem Zahlkörper, genau dann, wenn $k = \mathbb{R}, \mathbb{C}$ oder endliche Erweiterung eine $\mathbb{Q}_p$.*

Beweis: Theorem 9.13 und Satz 9.11 □

Definition 9.15. *Die kanonischen Absolutbeträge auf K heißen* Stellen *von K.*

Wir schreiben $v|w$, wenn $|\cdot|_w$ den Betrag $|\cdot|_v$ fortsetzt.

Bemerkung. $\mathbb{Q}$ hat die Stellenmenge $S(\mathbb{Q}) = \{\infty, p\text{prim}\}$.

Korollar 9.16. *Sei K ein Zahlkörper, v eine Stelle von K, $p|v$ eine Primzahl. Dann ist v assoziiert zu einem Primideal $\mathfrak{p}$ von $\mathcal{O}_k$, das p enthält.*

Beweis: Auf $K_v \subset \mathcal{O}_v$ ist der Betrag $|\cdot|_v$ nach Lemma 9.12 von einem Primideal $\mathfrak{p}_v$ induziert. Es gilt $\mathcal{O} \subset \mathcal{O}_v$, da die Elemente von $\mathcal{O}$ ganz über $\mathbb{Z}$, also erst recht ganz über $\mathbb{Z}_p$ sind. Das Primideal $\mathfrak{p} = \mathcal{O} \cap \mathfrak{p}_v$ induziert dann $|\cdot|_v$. □

Korollar 9.17 (Gradformel). *Sei v eine Stelle von K mit $p|v$. Sei e_v der Verzweigungsindex von $\mathcal{O}_v$ über $\mathbb{Z}_p$ (d.h. $p = u\pi^{e_v}$ mit $(\pi) = \mathfrak{p}_v, u \in \mathcal{O}_v^*$). Sei f_v der Restklassenkörpergrad $[\mathcal{O}_v/\pi : \mathbb{Z}_p/p]$. Dann gilt*

$$\sum_{p|v} e_v f_v = [K : \mathbb{Q}]$$

Es gilt $e_v f_v = [K_v : \mathbb{Q}_p]$, der lokale Grad von v.

Beweis: Die Stellen v entsprechen den Primidealen $p \in \mathfrak{p}$. Dabei ist $e_v = e(\mathfrak{p}/p), f_v = f(\mathfrak{p}/p)$ nach Satz 9.9 (ii). Die Gradformel ist genau Satz 5.2. □

Bemerkung. $v|\infty$ bedeutet $K_v = \mathbb{R}, \mathbb{C}$. Auf jeden Fall hat man $\sigma : K \to \mathbb{C}$ mit $|x|_v = |\sigma x|$. Die Einbettungen σ und $\overline{\sigma}$ induzieren dasselbe v. In den Formeln der Gittertheorie hätten wir also besser über Stellen statt über Einbettungen summiert.

$$e_v := [K_v : \mathbb{R}] = \begin{cases} 1 & v \text{ reell} \\ 2 & v \text{ imaginär} \end{cases}$$

Damit gilt

$$\sum_{v|\infty} e_v = r_1 + 2r_2 = [K : \mathbb{Q}]$$

Man sagt: L/K ist verzweigt in der Stelle $w|\infty$ von L , falls $[L_w : K_w] \neq 1$, d.h. $L_w = \mathbb{C}$ und $K_w = \mathbb{R}$.

Viele Eigenschaften des Zahlrings, z.B. die Verzweigung, können also bestimmt werden, ohne $\mathcal{O}$ aus den Gleichungen zu bestimmen.

Korollar 9.18. *Sei K ein Zahlkörper, S die Menge der Stellen von K, die Unendlich nicht teilen. Dann gilt*

$$\mathcal{O}_K = \{x \in K \mid |x|_v \leq 1 \text{ für alle } v \in S\}$$

Beweis: Sei $x = a/b$ mit $a, b \in \mathcal{O}_K$. Sei $|x|_v = |x|_{\mathfrak{p}}$ für ein Primideal $\mathfrak{p}$. Dann gilt

$$\left|\frac{a}{b}\right|_v \leq 1 \Leftrightarrow v_p f(a) \geq v_{\mathfrak{p}}(b)$$

In der Primfaktorzerlegung von a und b gilt also

$$(a) = \prod \mathfrak{p}^{v_{\mathfrak{p}}(a)} \subset (b) = \prod \mathfrak{p}^{v_{\mathfrak{p}}(b)}$$

Dies bedeutet $a = \gamma b$ für $\gamma \in \mathcal{O}$, also $\gamma = x \in \mathcal{O}$. □

Beispiel. Sei $K = \mathbb{Q}(\alpha)$, $\alpha^3 = 2$. Da der Grad der Erweiterung $K/\mathbb{Q}$ eine Primzahl ist, sind nur drei Fälle möglich: es gibt genau eine Primstelle über p, diese ist rein verzweigt oder unverzweigt, oder es gibt drei unverzweigte Primstellen über p.
Sei $v|2$. Dann gilt

$$|\alpha|_v = |2|_2^{1/3} = 2^{-1/3}$$

Die Bewertung v gehört zu einem Primideal $\mathfrak{p}$ mit

$$|\alpha|_v = 2^{-v_{\mathfrak{p}}(\alpha)/e(\mathfrak{p}/2)}$$

Hieraus folgt $e_v(2) = 3$, die Primzahl 2 ist rein verzweigt.
Der Zerfällungskörper von $X^3 - 2$ ist $K(\zeta_3)$. Die Erweiterung $K(\zeta_3)/\mathbb{Q}(\zeta_3)$ hat den Grad 3. Wir betrachten die lokale Situation:

$$\mathbb{Q}_p(\alpha, \zeta_3) \supset \mathbb{Q}_p(\zeta_3) \supset \mathbb{Q}_p$$

Die erste Erweiterung hat Grad 1 oder 3, die zweite Grad 1 oder 2.
Sei nun $p \neq 3$. Die zweite Erweiterung ist unverzweigt für $p \neq 3$. $\mathbb{Q}_p(\zeta_3)$ hat Restklassenkörper $\mathbb{F}_p(\zeta_3)$. Es sind nun zwei Fälle möglich:

(i) $X^3 - 2$ hat keine Nullstelle in $\mathbb{F}_p(\zeta_3)$. Dann hat die Restklassenkörpererweiterung $\mathbb{F}_p[\zeta_3, \alpha]$ den Grad 3. In K gibt es genau eine Stelle $v \mid p$, diese ist unverzweigt.

(ii) $X^3 - 2$ hat eine Nullstelle in $\mathbb{F}_p(\zeta_3)$. Dann zerfällt das Polynom in drei Linearfaktoren. Es gibt drei Stellen $v \mid p$ (Übungsaufgabe), diese müssen unverzweigt sein.

Übungsaufgabe. *Im Fall (ii) gibt es drei Stellen $v \mid p$, diese müssen unverzweigt sein. Für $p = 3$ hat $\mathbb{Q}_p(\zeta_3)$ den Restklassenkörper $\mathbb{F}_3$. In diesem Fall ist die Erweiterung rein verzweigt.*

Lokale Klassenkörpertheorie

Theorem 9.19 (Reziprozitätsgesetz). *Sei E/k eine Galoiserweiterung lokaler Körper. Dann gibt es einen kanonischen Isomorphismus*

$$k^*/N_{E/K}E^* \to \mathrm{Gal}(E/k)^{\mathrm{ab}}$$

Beispiel. $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$ mit $(p,N)=1$. Sei $0 \neq a \in \mathbb{Z} \subset \mathbb{Q}_p^*$ mit $(a,N)=1$. Dann wird a abgebildet auf $\zeta_N \mapsto \zeta_N^a$.

Beweis: Schwer! □

Globalge Klassenkörperhtheorie

Sei K ein Zahlkörper, S die Menge aller Stellen von K. Beachte:

$$\mathrm{Gal}(E/K) \to \prod_{v \in S} \mathrm{Gal}(E_v/K_v)$$

Die lokalen Aussagen sollten sich zusammensetzen lassen.

Definition 9.20. *Die* Adele *von K sind der Ring*

$$\mathbb{A}_K = \{(x_v) \in \prod_{v \in S} K_v \mid x_v \in \mathcal{O}_v \text{ fast immer}\}$$

Die Idele *von K sind die Gruppe*

$$I_K = \mathbb{A}_K^* = \{(x_v) \in \prod_{v \in S} K_v^* \mid x_v \in \mathcal{O}_v^* \text{ fast immer}\}$$

Theorem 9.21 (Reziprozitätsgesetz). *Sei E/K eine Galoiserweiterung von Zahlkörpern. Dann gibt es einen kanonischen Isomorphismus*

$$I_K/N_{E/K}I_E \to \mathrm{Gal}(E/K)^{\mathrm{ab}}$$

verträglich mit den lokalen Isomorphismen.

Beweis: Schwer! □

Der Beweis des lokalen und globalen Reziprozitätsgesetzes wäre Stoff für eine Vorlesung algebraische Zahlentheorie 2.

Bemerkung. Die Formeln sind nur so glatt, da auch die unendlichen Stellen berücksichtigt werden.

Strukturtheorie lokaler Körper (Schnelldurchgang)

Sei nun $k/\mathbb{Q}_p$ lokaler Körper.

Lemma 9.22. *In k gilt: $\sum_{i=0}^{\infty} a_i$ konvergent genau dann, wenn $(a_i)_{i=0}^{\infty}$ Nullfolge.*

Beweis: Beachte: $|\sum_{i=0}^{N} a_i| \leq \max_{i=0}^{N} |a_i|$ □

Satz 9.23 (Henselsches Lemma). *Sei $\mathcal{O} \subset k$ der Bewertungsring, $f \in \mathcal{O}[T]$. Sei $\alpha_0 \in \mathcal{O}$ mit*

$$|f(\alpha_0)| < |f'(\alpha_0)^2|$$

wobei f' die formale Ableitung von f ist. Dann konvergiert die Folge

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

gegen eine Wurzel α von f. Es gilt

$$|\alpha - \alpha_0| \leq \frac{|f(\alpha_0)|}{|f'(\alpha_0)^2|} \leq 1$$

Bemerkung. Dies lässt sich auch in Termen der Bewertung, also von Teilbarkeit durch das Primelement formulieren und beweisen. Ein wichtiger Spezialfall ist $\alpha_0 \in \mathcal{O}$, $f(\alpha_0) = 0$ im Restklassenkörper (d.h. $|f(\alpha_0) < 1$) und $f'(\alpha_0) \neq 0$ im Restklassenkörper (d.h. $|f'(\alpha_0)| = 1$).

Beweis: Dies ist das Newton-Verfahren für den p-adischen Betrag. Für Einzelheiten siehe: Koblitz, p-adic Numbers, p-adic Analysis and Zeta-Functions, Lang: Algebraic Number Theory.
Sei

$$c = \left| \frac{f(\alpha_0)}{f'(\alpha_0)^2} \right|_p < 1$$

Wir zeigen induktiv:

(i) $|\alpha_i| \leq 1$

(ii) $|\alpha_i - \alpha_0| \leq c$

(iii) $\left| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right|_p < c^{2^i}$

Die Bedinung (i) besagt, dass alle α_i und damit auch alle $f(\alpha_i)$, $f'(\alpha_i)$ ganz sind. Die Bedingung (iii) besagt, dass

$$|\alpha_{i+1} - \alpha_i| = \left| \frac{f(\alpha_i)}{f'(\alpha_i)} \right|_p \leq |f'(\alpha_i)|_p c^{2^i} \leq c^{2^i}$$

Also ist dies eine Nullfolge. Hieraus folgt Konvergenz der Folge α_i. Wegen der Stetigkeit des Betrages folgt aus (ii) die Abschätzung für α. Der Grenzwert erfüllt wegen Stetigkeit von f und f' die Gleichung

$$\alpha = \alpha - \frac{f(\alpha)}{f'(\alpha)}$$

Dies bedeutet $f(\alpha) = 0$.
Nun verifizieren wir die Eigenschaften (i), (ii), (iii). Für $i = 0$ ist dies jeweils die Voraussetzung. Schluss von i nach $i + 1$:

(i) Die Eigenschaft (iii) bedeutet

$$\alpha_{i+1} - \alpha_i| = \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|_p = \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right|_p |f'(\alpha_i)|_p \leq 1c^{2^i}$$

Mit (i) impliziert dies $|\alpha_{i+1} \leq 1$.

(ii) $|\alpha_{i+1} - \alpha_0| \leq \max(|\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0|) \leq \max(c^{2^i}, c) = c$.

(iii) Sei $g \in \mathcal{O}[T]$ ein Polynom. Seine Taylorentwicklung in einem Punkt x_0 ist

$$g(x_0 + T) = g(x_0) + g'(x_0)T + h(T)T^2$$

(Betrachte z.B. $g(T) = cT^n$) Wir setzen nun $g = f$, $x_0 = \alpha_i$, $T = -\frac{f(\alpha_i)}{f'(\alpha_i)}$. Es gilt also

$$f(\alpha_{i+1} = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2$$

mit $\beta \in \mathcal{O}$. Die ersten beiden Summanden heben sich weg, also

$$|f(\alpha_{i+1})| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2$$

Nun setzen wir $g = f'$, $x_0 = \alpha_i$ und $T = -\frac{f(\alpha_i)}{f'(\alpha_i)}$. Damit

$$f'(\alpha_{i+1}) = f'(\alpha_i) + \gamma\frac{f(\alpha_i)}{f'(\alpha_i)}$$

mit $\gamma \in \mathcal{O}$. Dies impliziert

$$|f'(\alpha_{i+1})| \geq \max\left(|f'(\alpha_i)|, \left|\gamma\frac{f(\alpha_i)}{f'(\alpha_i)}\right|\right)$$

und sogar Gleichheit, falls die Beträge unterschiedlich sind. Nach Induktionsvoraussetzung gilt

$$|f'(\alpha_i)| > \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right| \geq |\gamma\frac{f(\alpha_i)}{f'(\alpha_i)}$$

Also $|f'(\alpha_{i+1})| = |f'(\alpha_i)|$. Zusammen folgt nun

$$\left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right|_p \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2 \frac{1}{|f'(\alpha_i)|} = \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right|^2 < (c^{2^i})^2$$

□

Beispiel. Sei $(N,p) = 1$, Φ_N das zyklotomische Polynom, also ein Teiler von $X^N - 1$. Sei $\alpha \in \mathcal{O}$ eine Nullstelle dieses Polynoms im Restklassenkörper, $|f(a_0)| < 1$ wobei π ein Primelement ist. Weiterhin ist $f'(\alpha) \neq 0$ im Restklassenkörper, da $(X^N - 1)' = NX^{N-1}$ ungleich Null. Dies bedeutet $|f'(\alpha_0)|^2 = 1$. Die Vorraussetzung des Henselschen Lemmas ist erfüllt. Φ_N hat eine Nullstelle in k.

Korollar 9.24. *Sei $k/\mathbb{Q}_p$ endlich. Dann gibt es einen Teilkörper $k^u \subset k$, der unverzweigt über $\mathbb{Q}_p$ ist. Es gilt $f(k/\mathbb{Q}_p) = f(k^u/\mathbb{Q}_p)$ und $e(k/k^u) = e(k/\mathbb{Q}_p)$. Der Körper k^u wird von Einheitswurzeln erzeugt, deren Ordnung prim zu p ist.*

Beweis: Sei $f = f(k/\mathbb{Q}_p)$, d.h. $\mathbb{F}_{p^f}$ ist der Restklassenkörper von k. Es gilt $\mathbb{F}_{p^f} = \mathbb{F}_p(\overline{\alpha})$, wobei $\overline{\alpha}$ eine primitive (p^f-1)-te Einheitswurzel ist. Dies bedeutet, dass das zyklotomische Polynom Φ_{p^f-1} eine Nullstelle im Restklassenkörper hat. Wie im Beispiel hat Φ_{p^f-1} eine Nullstelle α in k, die $\overline{\alpha}$ induziert. Sei nun $k^u = \mathbb{Q}_p(\alpha) \subset k$. Der Restklassenkörer von k^u enthält $\overline{\alpha}$, ist also ganz $\mathbb{F}_{p^f}$. Damit ist $f(k^u/\mathbb{Q}_p) = f$. □

Bemerkung. Ist $k/\mathbb{Q}_p$ unverzweigt, so wird k von Einheitswurzeln der Ordnung prim zu p erzeugt.

Satz 9.25. *Sei E/k rein verzweigt. Dann gilt $E = k(\alpha)$, wobei α Nullstelle eines Eisensteinpolynoms ist ($X^e + a_1X^{e-1} + \cdots + a_e$ mit $|a_i| < 1$, $a_e \neq 0$ modulo π^2).*

Beweis: Seien π, π_E Primelemente von $\mathcal{O}_k$ und $\mathcal{O}_E$. Nach Voraussetzung gilt $\pi = u\pi_E^e$ mit $u \in \mathcal{O}_E^*$ und $e = [E : k]$. Sei $f \in \mathcal{O}_k[T]$ das charakteristische Ppolynom von π_E. Die Koeffizienten von f sind die elementarsymmetrischen Polynome in den $\sigma(\pi_E)$ wobei $\sigma : E \to \overline{k}$ die Einbettungen durchläuft. Alle diese Konjugierten haben denselben Absolutbetrag. Damit ist der Betrag der Koeffizienten kleiner als 1. Sie liegen also in $\mathcal{O}_k \setminus \mathcal{O}_k^* = (\pi)$. Der konstante Term von f ist $\prod \sigma(\pi_E)$. Der Absolutbetrag ist $|\pi_E|^e = |\pi|$. Damit ist f ein Eisensteinpolynom. Es ist insbesondere irreduzibel, also $E = k(\pi_E)$. □

Bemerkung. Ist E/k zahm verzweigt, d.h. $[E : k] = e(E/K)$ ist teilerfremd zu p, so kann das Minimalpolynom sogar als $T^e - \pi$ gewählt werden.
Insgesamt: Lokale Körper verstehen wir sehr gut.

Übersicht

Wir haben in diesem Semester einige tiefe Sätze der Zahlentheorie bewiesen und dabei verschieden Methoden kennengelernt.

- **Kommutative Algebra**: Definition der Ganzheitsringe als ganzer Abschluss, Ganzheitsringe sind Dedekindringe, Strukturtheorie von Idealen in Dedekindringen, Definition der Klassengruppe, Verzweigung von Idealen, Diskriminante und Spurpaarung, Gradformel (Kapitel 1, 2, 3, 5)
- **Gittertheorie**: Endlichkeit der Klassenzahl, Struktur der Einheitengruppe, Klassenzahlformel (Kapitel 4, 8)
- **Funktionentheorie**: Konvergenzverhalten der Dedekindschen Zeta-Funktion, Dirichletscher Dichtesatz, Primzahlsatz, Klassenzahlformel (Kapitel 6, 7, 8)
- **p-adische Analysis**: Theorie der lokalen Körper. (Kapitel 9)

Natürliche Fortsetzungen:

- Klassenkörpertheorie, d.h. Klassfizierung der abelschen Erweiterungen von Zahlkörpern. Aktueller Forschungsgegenstand: analoge Theorie für nichtabelsche Erweiterungen (Langlands-Programm)
- Iwasawa-Theorie: Studium von Körpertürmen mit p-adischen Methoden
- Höher-dimensionale Theorie, also arithmetische Geometrie (algebraische Geometrie über $\mathbb{Z}$).