Themen der Algebraischen Zahlentheorie

1. Dedekindsche Ringe

$\mathbb{Z}$ = ganze Zahlen, $\subset \mathbb{Q}$ = Körper der rationalen Zahlen.

$K|\mathbb{Q}$ eine endliche Körpererweiterung. Man nennt K einen algebraischen Zahlkörper

Was sind die ganzen Zahlen in K ?

$x \neq 0, \in K$. Die Potenzen $\{x^i\}_{i=0}^{\infty}$ sind linear abhängig über $\mathbb{Q}$. Es existiert ein minimales $n \geq 1$, sodass

$$x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Q}.$$

Definition: x heißt ganz, wenn alle auftretenden Koeffizienten a_i in $\mathbb{Z}$ liegen. Die Menge solcher $x \in K$ (einschließlich $x = 0$) heißt:

$O_K :=$ ganze Zahlen in K. Sie bilden einen Teilring in K.

Die Ringe O_K gehören zur Klasse der Dedekind Ringe.
Sie sind 1-dimensional, d.h. jedes von 0 verschiedenen Primideal ist bereits maximal.

2. Hauptsatz der Arithmetik

In $\mathbb{Z}$ bzw. $\mathbb{Q}$:

Jede rationale Zahl x besitzt eine eindeutige Darstellung

$$(1) \quad x = \operatorname{sgn}(x) \cdot \prod_p p^{v_p(x)}$$

als Potenzprodukt von Primzahlen mit ganzzahligem Exponenten.

In O_K bzw. K:

Jedes gebrochene Ideal $\mathfrak{a}$ in K besitzt eine eindeutige Darstellung

$$(2) \quad \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

als Potenzprodukt von Primidealen mit ganzzahligen Exponenten.

3. Nichtarchimedische Bewertungen und lokale Körper

$$x \in K \longmapsto v_{\mathfrak{p}}(x) = \text{Exponent von } \mathfrak{p} \text{ in}$$

der Zerlegung des Hauptideals $O_K \cdot x$

Absolutbetrag: $|x|_{\mathfrak{p}} := q_{\mathfrak{p}}^{-v_{\mathfrak{p}}(x)}$

wobei $q_{\mathfrak{p}}$ in Abhängigkeit von $\mathfrak{p}$ gewählte natürliche Zahl (> 1).

Nichtarchimedische Dreiecksungleichung:

$$|x + y|_{\mathfrak{p}} \leq \max\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\}.$$

$K_{\mathfrak{p}}$:= Ring der Cauchyfolgen bezüglich $||_{\mathfrak{p}}$ modulo Ideal der Nullfolgen.

$K_{\mathfrak{p}}$ ist ein lokaler Zahlkörper.

Viele Konzepte und Sätze der Zahlentheorie haben vereinfachte Varianten für die Körper $K_{\mathfrak{p}}$. Umgekehrt ergeben simultane Betrachtungen für die Körper $K_{\mathfrak{p}}$ (für sämtliche $\mathfrak{p}$) Konsequenzen für K.

4. Eine Grundaufgabe und arithmetische Konsequenzen

$p \in \mathbb{Z}$ sei Primzahl, $\mathfrak{a} = O_K p$ sei das von p erzeugte Ideal. Wie sieht die Zerlegung (2) aus (?)

Beispiel: $K = \mathbb{Q}(\sqrt{-1})$.

$$O_K = \mathbb{Z} + \mathbb{Z}(\sqrt{-1}) \text{ sind}$$

die ganzen Gaußschen Zahlen.

$$\text{(3)} \quad \begin{aligned} O_K p &= \mathfrak{p}_1 \cdot \mathfrak{p}_2 \qquad \text{falls } p \equiv 1(4) \\ &= \quad \mathfrak{p} \qquad\quad \text{falls } p \equiv 3(4) \end{aligned}$$

Daraus folgt:

Satz: (Lagrange) *p ist Summe von 2 Quadraten genau dann, wenn $p \equiv 1(4)$.*

(Die Richtung $\Longrightarrow$ ist klar. Die Richtung $\Longleftarrow$ folgt aus (3)).

$$5 = 2^2 + 1^2 = (2 + \sqrt{-1})(2 - \sqrt{-1})$$

Weitgehende Verallgemeinerungen von (3) bzw. des Satzes von Lagrange werden unter dem Thema „Quadratische Zahlkörper und quadratische Formen“behandelt.

5. Invarianten von Dedekind-Ringen.

Jeder der eingangs definierten Ringe O_K besitzt eine Darstellung

$$O_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$$

als direkte Summe mehrerer Kopien von $\mathbb{Z}$. Die Mulitplikation ist bestimmt, sobald man die Produkte $\omega_i\omega_j$ kennt. Eine erste Invariante von O_K ist die ganze Zahl

$$d_K := \det(\mathrm{Spur}(\omega_i\omega_j)) \in \mathbb{Z}.$$

Sie heißt die Diskriminante von K bzw. O_K.

Minkowski-Abschätzung: Sei $n = [K : \mathbb{Q}]$ die Dimension von K als $\mathbb{Q}$-Vektorraum. Dann gilt:

$$|d_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \cdot \frac{n^{2n}}{(n!)^2} \quad \text{mit} \quad 2r_2 \leq n$$

Folgerung: (i) Wenn $|d_K| = 1$, dann ist $K = \mathbb{Q}$.

(ii) Wenn $d > 1$, dann gibt es höchstens endlich viele K mit $|d_K| = d$.

Eine zweite wichtige Invarainte ist h_K = Klassenzahl von O_K.

Hierzu erwähnen wir nur:

$h_K = 1$ genau dann, wenn O_K Hauptidealring, d.h. der Hauptsatz der Arithmetik (vgl. 2.) gilt mit Elementen statt mit Idealen.

6. Kreisteilungskörper.

n-te Einheitswurzeln entsprechen geometrisch den n-Teilungspunkten des Einheitskreises in $\mathbb{C}$.

$K = \mathbb{Q}_n$ sei die kleinste Körpererweiterung von $\mathbb{Q}$, welche die n-ten Einheitswurzeln enthält.

Aus der Theorie der Dedekind-Ringe folgt:

Es sei p eine Primzahl ($\neq 2$), sodass die Klassenzahl $h_{\mathbb{Q}_p}$ nicht durch p teilbar ist. Dann hat die Fermat-Gleichung

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

keine Lösungen $(x, y, z) \in \mathbb{Z}^3$ mit $p \nmid xyz$.

7. Analytische Methoden

Euler zeigte 1737:

Die Summe der Reziproken aller Primzahlen divergiert:

$$\sum_{p \leq x} \frac{1}{p} > \ln(\ln(x)) - \frac{1}{2}$$

Satz von Dirichlet: *Sei $m > 1$ natürliche Zahl und sei*

$a \in \{1, \cdots, m-1\}$ prim zu m. Die Anzahl der möglichen a wird durch

die Eulersche Funktion $\varphi(m)$ bestimmt.

$$\lim_{s \to 1+} \frac{\left(\sum\limits_{p \equiv a(m)} p^{-s}\right)}{\left(\sum\limits_{p} p^{-s}\right)} = \frac{1}{\varphi(m)}.$$

Da der Nenner für $s = 1$ einen Pol hat, gilt dasselbe für den Zähler.

Also gibt es unendlich viele Primzahlen p mit $p \equiv a \mod m$.

8. Beweis mit Hilfe von Dirichlet-Reihen

$$f(s) = \sum_{n \geq 1} a_n n^{-s}$$

Zahlentheoretisch wichtige Dirichlet-Reihen sind:

a) Riemannsche ζ-Funktion:

$$\zeta(s) = \sum_{n \geq 1} n^{-s}$$

b) Dedekindsche ζ-Funktion eines Körpers $K|\mathbb{Q}$:

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s},$$

wobei über die Ideale von O_K summiert wird und $N(\mathfrak{a})$ bezeichnet die „Absolutnorm".

c) Dirichletsche L-Reihen:

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

wobei χ ein Charakter der primen Restklassengruppe $(\mathbb{Z}/n)^\times$ ist.

Sei $K = \mathbb{Q}_n$. Dann gilt:

$(*)$ $\qquad \zeta_{\mathbb{Q}_n}(s) = \zeta(s) \cdot \prod_{\chi \neq 1} L(s, \chi),$

wobei das Produkt über die Charaktere von $(\mathbb{Z}/n)^\times$ zu nehmen ist.

Der Beweis des Satzes von Dirichlet benutzt wesentlich die Identität $(*)$.