

Mitschrieb der Vorlesung "Algebraische Zahlentheorie 1" von Kay Wingberg

Axel Wagner

Date: 03.11.2011

These notes are published under the CC-BY-SA-DE 3.0 License.



For further information, visit

<http://creativecommons.org/licenses/by-sa/3.0/deed.de>

Inhaltsverzeichnis

1 Ganzheit	6
2 Ideale	12
3 Gitter	17
4 Minkowski-Theorie	20

Probleme:

- Mächtigkeit der Primzahlen (Euklid)
- allgemeiner: Verteilung der Primzahlen: $\pi(n) \sim \frac{n}{\log n} \rightsquigarrow$ analytische Zahlentheorie
- Goldbach-Vermutung \rightsquigarrow „additive Zahlentheorie“
- Fermat-Vermutung: $x^n + y^n = z^n, n \in \mathbb{N}, n > 2$ hat nur triviale Lösung.

Fermat-Vermutung ist nur für $n = 4$ und $n = p$ prim zu zeigen, $n = mp$ oder $n = 4m$:
 $(X^m)^p + (Y^m)^p = (Z^m)^p$

Jede Lösung $(x, y, z) \in \mathbb{Q}^3$ gibt eine in \mathbb{Z}^3 (Hauptnenner).

Kummer 1850: Betrachtet die Gleichung in $\mathbb{Q}(\zeta_p)$, ζ_p p -te Einheitswurzel, p prim.

$$\rightsquigarrow x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p$$

Angenommen $\mathbb{Z}[\zeta_p]$ ist faktoriell $\Rightarrow \forall i: (x + \zeta_p^i y)$ ist p -Potenz $\Rightarrow \zeta$.

Aber $\mathbb{Z}[\zeta_p]$ ist nicht faktoriell (stimmt für $p \leq 19$)

Dedekind: Verallgemeinerung: Statt Primzahlen werden Primideale betrachtet. Dies führte zur „algebraischen Zahlentheorie“ (Fermatsche Vermutung richtig nach A. Wiles).

Probleme:

1. „Wie sieht die Arithmetik in Erweiterungen von \mathbb{Q} aus?“
2. Lösungen von diophantischen Gleichungen: $F(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]: F = 0$

Methoden

Analytische Methode: Zeta- und L-Funktionen:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, s \in \mathbb{C}, \Re(s) < 1$$

$$\zeta(s) = \prod_{p \in \mathcal{P}} \left(\sum_{v_p=1}^{\infty} \frac{1}{p^{v_p p^s}} \right) = \prod_{p \in \mathcal{P}} \left(\frac{1}{1 - p^{-s}} \right)$$

Riemannsche Vermutung: Nullstellen von $\zeta(s)$ in $0 < \Re(s) < 1$ haben alle $\Re(s) = \frac{1}{2}$.

Algebraische Methode: Globale Methode: Idealtheorie in Körpererweiterungen von \mathbb{Q}

Lokale Methode (Hensel, Hasse): Topologischer Natur, analog zur Komplettierung von \mathbb{Q} bezüglich $|\cdot|_{\infty}$, die gerade \mathbb{R} ist, gibt es Komplettierungen zu p -adischen Beträgen

$$|\cdot|_p: \mathbb{Q} \rightarrow \mathbb{R}, x = p^v \frac{n}{m}, v \in \mathbb{Z}, n, m \in \mathbb{Z} \text{ prim zu } p, x \mapsto |x|_p := \frac{1}{p^v}$$

Komplettierung: \mathbb{Q}_p Körper der p -adischen Zahlen.

Geometrische Methode: Arithmetische Geometrie. Die diophantischen Gleichungen definieren geometrische Objekte.

Literatur:

- Borevicz, Šafarevič: Zahlentheorie (1966)
- Cassels, Fröhlich: Algebraic Number Theory (1967)
- Hasse: Vorlesung über Zahlentheorie (gelb) (1964), Zahlentheorie (blau) (1963)
- Hilbert: Theorie der algebraischen Zahlkörper (Zahlbericht) (1897)
- Lang: Algebraic Number Theory (1970)
- Serre: Corps Locaux (1968)
- Weil: Basic Number Theory (1963)
- Neukirch: Algebraische Zahlentheorie (1992)

Es gilt:

$$2 = 1 + 1, 5 = 1 + 4, 13 = 4 + 9$$

$$17 = 1 + 16, 29 = 4 + 25, 37 = 1 + 36$$

Dies sind die ersten Primzahlen, die sich als Summe zweier Quadrate schreiben lassen.

Für $p > 2$ mit obiger Eigenschaft gilt immer $p \equiv 1 \pmod{4}$, denn $p = a^2 + b^2 \stackrel{p \neq 2}{\Rightarrow} p \equiv 1 \pmod{4}$, da Quadrate $\equiv 0 \pmod{4}$ oder $\equiv 1 \pmod{4}$ $(1 + 2n)^2 = 1 + 4n + 4n^2$.

Betrachtungswert ist die Umkehrung:

Satz 0.1. Für Primzahlen $p \neq 2$ gilt:

$$p = a^2 + b^2, a, b \in \mathbb{Z} \Leftrightarrow p \equiv 1 \pmod{4}$$

Beweist man im faktoriellen Ring $\mathbb{Z}[i]$ (oder Satz von Thue und quadratischer Reziprozitätsgesetz).

Satz 0.2. Der Ring $\mathbb{Z}[i]$ ist euklidisch, also insbesondere faktoriell

Beweis. Wir zeigen: Der Ring $\mathbb{Z}[i]$ ist euklidisch in Bezug auf

$$N : \mathbb{Z}[i] \rightarrow \mathbb{N} \cup \{0\}$$

$$\alpha \mapsto |\alpha|^2 = N(\alpha)$$

$$\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0 \Rightarrow \exists \gamma, \rho \in \mathbb{Z}[i] : \alpha = \gamma\beta + \rho, |\rho|^2 < |\beta|^2$$

Die Menge $\mathbb{Z} + i\mathbb{Z} \subseteq \mathbb{C}$ bildet ein „Gitter“ in \mathbb{C} .

$x = \frac{\alpha}{\beta}$ hat zum nächsten Gitterpunkt den Abstand $\frac{\sqrt{2}}{2}$, d.h. $\exists \gamma \in \mathbb{Z}[i] : \left| \frac{\alpha}{\beta} - \gamma \right| \leq \frac{\sqrt{2}}{2} < 1$.

Also gilt für $\rho := \alpha - \gamma\beta$:

$$|\rho| = |\alpha - \gamma\beta| = |\beta| \left| \frac{\alpha}{\beta} - \gamma \right| < |\beta|$$

□

Satz 0.3.

$$\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\} = \{\pm 1, \pm i\}$$

Beweis.

$$\begin{aligned} \alpha \in \mathbb{Z}[i]^\times, \alpha = x + iy \Rightarrow \exists \beta = u + iv \in \mathbb{Z}[i]: \alpha\beta = 1 \Rightarrow 1 = N(\alpha)N(\beta) = (x^2 + y^2)(u^2 + v^2) \\ \Rightarrow N(\alpha) = 1 \Rightarrow \alpha \in \{\pm 1, \pm i\} \end{aligned}$$

□

Beweis. von Satz 0.1.Sei $p = 1 + 4n$. Dann ist p in $\mathbb{Z}[i]$ kein Primelement, denn:

Satz von Wilson:

$$\begin{aligned} -1 &\equiv (p-1)! = (1 \cdot 2 \cdot \dots \cdot 2n)((p-1) \cdot (p-2) \cdot \dots \cdot (p-2n)) \\ &= (2n)!(-1)^{2n}(2n)! = ((2n)!)^2 \pmod{p} \\ &\stackrel{x=2n}{\Rightarrow} p \mid x^2 + 1 = (x+i)(x-i) \text{ aber } \frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i] \\ &\Rightarrow p = \alpha\beta, \alpha, \beta \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times \stackrel{0.3}{\Rightarrow} N(\alpha) \neq 1 \neq N(\beta) \end{aligned}$$

Wegen $p^2 = N(\alpha)N(\beta)$ folgt $p = N(\alpha)$. Ist $\alpha = a + ib$, dann $p = a^2 + b^2$.

□

Probleme: Bestimmung der Einheiten und Primelemente.

Satz 0.4. 1. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

2. Die Primelemente π in $\mathbb{Z}[i]$ sind bis auf Assoziiertheit:

a) $\pi = 1 + i$

b) $\pi = a + ib$, sodass $a^2 + b^2 = p$ Primzahl, $p \equiv 1 \pmod{4}$, $a > |b| \neq 0$

c) $\pi = p$ Primzahl, $p \equiv 3 \pmod{4}$

Beweis. 1 wurde bereits bewiesen.

Zu zeigen: Die obigen Elemente sind prim:

$$\pi = \alpha\beta \Rightarrow N(\pi) = N(\alpha)N(\beta) \Rightarrow N(\alpha)N(\beta) = \begin{cases} 2 & \pi = 1 + i \\ p & \pi = a + ib \\ p^2 & \pi = p \equiv 3 \pmod{4} \end{cases}$$

$\Rightarrow N(\alpha) = 1$ (o.B.d.A.) in den ersten beiden Fällen und somit $\alpha \in \mathbb{Z}[i]^\times$ (wegen 0.2), also π prim.

Im dritten Fall kann man nicht $N(\alpha) = p$ sein, denn mit $\alpha = a + ib$ ist $p = N(\alpha) = a^2 + b^2$, also $p \equiv 1 \pmod{4}$. Also $N(\alpha) = 1$, d.h. $\alpha \in \mathbb{Z}[i]^\times$.

Sei nun $\pi \in \mathbb{Z}[i]$ ein Primelement.

$$\Rightarrow N(\pi) = \pi\bar{\pi} = p_1 \cdot \dots \cdot p_r, p_i \text{ Primzahlen in } \mathbb{Z}$$

Da π prim ist, folgt $\pi | p_1$ (o.B.d.A.) ($\mathbb{Z}[i]$ ist faktoriell!).

$$\Rightarrow N(\pi) | N(p_1) = p_1^2$$

$$\Rightarrow N(\pi) = p_1 \vee N(\pi) = p_1^2$$

$$N(\pi) = 1 \Rightarrow a^2 + b^2 = p_1$$

Somit π vom zweiten Typ, falls $p_1 \neq 2$, oder $a^2 + b^2 = 2$, d.h. $a^2 = b^2 = 1$, also $\pi \sim 1 + i$.
 $N(\pi) = p_1^2 = N(p_1) \Rightarrow \pi \sim p_1$, da $N\left(\frac{p_1}{\pi}\right) = 1$, d.h. $\frac{p_1}{\pi} \in \mathbb{Z}[i]^\times$. Überdies gilt $p_1 \equiv 3 \pmod{4}$, weil sonst $p_1 = 2 \vee p_1 \equiv 1 \pmod{4}$, also $\pi \sim p_1 = a^2 + b^2 = (a + ib)(a - ib)$, also nicht prim. □

Bemerkung 0.5. Obiger Satz zeigt auch das Zerlegungsverhalten von Primzahlen aus \mathbb{Z} in $\mathbb{Z}[i]$.

1. 2 ist assoziiert zum Quadrat des Primelements $(1 + i)$.

$$2 = (1 + i)(1 - i) = -i(1 + i)^2$$

2. Die Primzahlen $p \equiv 1 \pmod{4}$ zerfallen in zwei konjugierte Primelemente

3. Die Primzahlen $p \equiv 3 \pmod{4}$ bleiben prim.

1 Ganzheit

Definition 1.1. Ein *algebraischer Zahlkörper* K ist eine endliche Erweiterung von \mathbb{Q} . Die Elemente aus K heißen *algebraische Zahlen* ($\alpha \in K \Rightarrow \alpha$ ist Nullstelle eines Polynoms $f \in \mathbb{Q}[X]$).

Eine algebraische Zahl heißt *ganz*, wenn sie Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[X]$ ist. Mit O_K bezeichnen wir die Menge aller ganzen algebraischen Zahlen aus K bezeichnet.

Im Folgenden bedeutet Ring immer kommutativ mit 1.

Definition 1.2. Sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt *ganz über* A , wenn es einer normierte Gleichung

$$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$$

genügt mit $n \geq 1, a_i \in A$.

B heißt *ganz über* A , wenn alle Elemente ganz über A sind.

Satz 1.3. Endlich viele Elemente $b_1, \dots, b_n \in B$ sind sämtlich ganz über A genau dann, wenn der Ring $A[b_1, \dots, b_n]$ endlich erzeugter A -Modul ist.

Korollar 1.4. Mit $b_1, b_2 \in B$ ganz über A ist auch $b_1 \pm b_2, b_1 b_2$ ganz über A , also bilden die ganzen Elemente $\bar{A} := \{b \in B \mid b \text{ ganz über } A\}$ in einer Ringerweiterung $A \subseteq B$ einen Ring ($A \subseteq \bar{A} \subseteq B$).

\bar{A} heißt *ganzer Abschluss* von A in B .

Beweis. Nach Satz 1.3 ist $A[b_1, b_2]$ endlich erzeugter A -Modul. Dann ist jedes Element $b \in A[b_1, b_2]$ ganz über A , da $A[b_1, b_2, b] = A[b_1, b_2]$ endlich erzeugter A -Modul. \square

Beweis. Von Satz 1.3.

Sei $b \in B$ ganz über A und $f \in A[X]$ normiertes Polynom vom Grad $n \geq 1, f(b) = 0$.

Für $g \in A[X]$ gilt: $g = qf + r, q, r \in A[X]$ (möglich, da f normiert, also höchster Koeffizient in A^\times), $\text{grad } r < n$.

$$\Rightarrow g(b) = r(b) = a_{n-1}b^{n-1} + \dots + a_1b + a_0$$

Also wird $A[b] = \{g(b) \mid g \in A[X]\}$ als A -Modul erzeugt von $1, b, \dots, b^{n-1}$.

Sind b_1, \dots, b_m ganz über A , so folgt die Endlichkeit von $A[b_1, \dots, b_m]$ durch Induktion nach m :

b_m ist ganz über $R := A[b_1, \dots, b_{m-1}]$, also $R[b_m] = A[b_1, \dots, b_{m-1}, b_m]$ ist endlich erzeugt über R , also per Induktion auch über A .

Sei nun $A[b_1, \dots, b_m]$ endlich erzeugter A -Modul, $\{\omega_1, \dots, \omega_r\}$ ein Erzeugendensystem. Sei $b \in A[b_1, \dots, b_m]$.

$$b\omega_i = \sum_{j=1}^r a_{ij}\omega_j, i = 1, \dots, r, a_{ij} \in A$$

$$(bI_r - (a_{ij})) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = 0$$

$$\Rightarrow \det(bI_r - (a_{ij}))\omega_i = 0$$

(Cramersche Regel)

$$1 = c_1\omega_1 + \dots + c_r\omega_r, c_i \in A$$

$$\Rightarrow \det(bI_r - (a_{ij})) = 0$$

Also $f(X) := \det(XI_r - (a_{ij})) \in A[X]$ ist normiert, mit $f(b) = 0$. Also ist b ganz über A und somit b_1, \dots, b_m ganz über A . \square

Satz 1.5. Seien $A \subseteq B \subseteq C$ Ringerweiterungen, C ganz über B , B ganz über A , dann ist auch C ganz über A .

Beweis. Sei $c \in C$:

$$c^n + b_{n-1}c^{n-1} + \dots + b_1c + b_0 = 0, b_i \in B$$

Mit Satz 1.3 folgt für $R = A[b_0, b_1, \dots, b_{n-1}]$, dass $R[c]$ endlich erzeugt über R . Da R endlich erzeugter A -Modul ist (Satz 1.3 und b_i ganz über A), ist $R[c]$ endlich erzeugter A -Modul, also c ganz über A . \square

Definition 1.6. Sei $A \subseteq B$ eine Ringerweiterung, \bar{A} der ganze Abschluss von A in B . A heißt **ganz abgeschlossen in B** , falls $A = \bar{A}$.

Ist A ein Integritätsring (d.h. nullteilerfrei) und $B = \text{Quot}(A)$ der Quotientenkörper von A , so heißt der ganze Abschluss von \bar{A} von A in $\text{Quot}(A)$ die **Normalisierung von A** und A heißt **ganz abgeschlossen (schlechthin)**, falls $A = \bar{A}$.

Bemerkung 1.7. Jeder faktorielle Ring A ist ganz abgeschlossen, denn ist $\frac{a}{b} \in K = \text{Quot}(A)$, $a, b \in A$, $\frac{a}{b}$ ganz über A , also

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

$$\Rightarrow a^n + a_{n-1}ba^{n-1} + \dots + a_0b^n = 0$$

Ist also π ein Primelement mit $\pi|b$, dann $\pi|a^n$ und da A faktoriell folgt $\pi|a$.

Ist $\frac{a}{b}$ gekürzt, so folgt $\frac{a}{b} \in A$.

Bemerkung 1.8. Ist $B \supseteq A$ eine Ringerweiterung, \bar{A} der ganze Abschluss von A in B . Dann ist \bar{A} ganz abgeschlossen in B , denn sei $\bar{\bar{A}}$ der ganze Abschluss von \bar{A} in B .
 $\Rightarrow A \subseteq \bar{A} \subseteq \bar{\bar{A}} \subseteq B$, \bar{A}/A ist ganz, $\bar{\bar{A}}/\bar{A}$ ist ganz $\Rightarrow \bar{\bar{A}}/A$ ganz $\Rightarrow \bar{\bar{A}} \subseteq \bar{A} \Rightarrow \bar{\bar{A}} = \bar{A}$.

Erinnerung: Sei L/K endliche separable Körpererweiterung, $\sigma: L \rightarrow \bar{K}$ durchlaufe die verschiedenen K -Einbettungen von L in einen algebraischen Abschluß \bar{K} von K . Sei $x \in L$.

$$\text{char}_{L/K}x(t) = \prod_{\sigma} (t - \sigma x) = \min_K(x)^d, d = [L: K(x)] \text{ charakteristisches Polynom}$$

$$\text{Tr}_{L/K}(x) = \sum_{\sigma} \sigma x \text{ Spur}$$

$$N_{L/K}(x) = \prod_{\sigma} \sigma x \text{ Norm}$$

Definition 1.9. Sei $\{\alpha_1, \dots, \alpha_n\}$ eine Basis der endlichen separablen Erweiterung L/K , $\{\sigma_1, \dots, \sigma_n\} = \text{Hom}_K(L, \bar{K})$. Dann heißt

$$d(\alpha_1, \dots, \alpha_n) := (\det(\sigma_i \alpha_j)_{i,j})^2$$

Diskriminante von $\{\alpha_1, \dots, \alpha_n\}$

Bemerkung 1.10. (α) Es gilt

$$(\text{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j} = \left(\sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j) \right)_{i,j} = (\sigma_k \alpha_i)_{k,i} (\sigma_k \alpha_j)_{k,j}$$

$$\det(\text{Tr}(\alpha_i \alpha_j))_{i,j} = d(\alpha_1, \dots, \alpha_n)$$

(β) Sei die Basis von L/K von der Form $1, \theta, \theta^2, \dots, \theta^{n-1}$

$$\Rightarrow d(1, \theta, \dots, \theta^{n-1}) = \prod_{i < j} (\theta_i - \theta_j)^2, \text{ wobei } \theta_i = \sigma_i \theta$$

denn

$$(\sigma_i \theta^j)_{i,j} = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \dots & \theta_n^{n-1} \end{pmatrix}$$

(Vandermonde'sche Matrix)

Satz 1.11. Ist L/K separabel und $\alpha_1, \dots, \alpha_n$ eine Basis, so ist $d(\alpha_1, \dots, \alpha_n) \neq 0$ und es ist

$$L \times L \rightarrow K, (x, y) \mapsto \text{Tr}_{L/K}(xy)$$

eine nicht-ausgeartete Bilinearform.

Beweis. Sei θ ein primitives Element von L/K , $\{1, \theta, \dots, \theta^{n-1}\}$ Basis von L/K .
Dann ist die Bilinearform durch die Matrix

$$M = (\text{Tr}_{L/K}(\theta^{i-1}\theta^{j-1}))_{i,j=1,\dots,n}$$

gegeben.

$$\det M = d(1, \theta, \dots, \theta^{n-1}) = \prod_{i < j} (\theta_i - \theta_j)^2 \neq 0$$

also ist die Bilinearform nicht ausgeartet.

Ist $\alpha_1, \dots, \alpha_n$ eine beliebige Basis von L/K , dann ist die Bilinearform durch die Matrix

$$N = (\text{Tr}_{L/K}(\alpha_i\alpha_j))_{i,j}$$

gegeben.

$$\Rightarrow d(\alpha_1, \dots, \alpha_n) = \det(N) \neq 0$$

da $S^tMS = N \Rightarrow \det N = \det M(\det S)^2$, S Basiswechselmatrix, also invertierbar, also $\det S \neq 0$. □

Sei nun die folgende Situation gegeben: A ist ein ganz abgeschlossener Ring, $K = \text{Quot}(A)$ der Quotientenkörper. L/K sei eine endliche separable Erweiterung, B sei der ganze Abschluss von A in L (B ist damit ganz abgeschlossen in L).

Bemerkung 1.12. 1. Jedes Element $\beta \in L$ hat die Gestalt: $\beta = \frac{b}{a}$, $b \in B$, $a \in A$, denn sei

$$a_n\beta^n + \dots + a_1\beta + a_0 = 0, a_i \in A, a_n \neq 0$$

$$\Rightarrow (a_n\beta)^n + \dots + a'_1(a_n\beta) + a'_0 = 0$$

also $b := a_n\beta$ ist ganz über A , also $b \in B$.

2. Sei $\beta \in L$, dann gilt:

$$\beta \in B \Leftrightarrow \min_K(\beta) \in A[X]$$

Denn:

„ \Leftarrow “ Per Definition

„ \Rightarrow “ β ist Nullstelle von $g \in A[X]$, g normiert $\Rightarrow \min_K(\beta) | g$ in $K[X]$.

\Rightarrow Nullstellen β_1, \dots, β_n von $\min_K(\beta)$ sind ganz über A .

\Rightarrow Koeffizienten von $\min_K(\beta)$ sind ganz über A . Da A ganz abgeschlossen folgt $\min_K(\beta) \in A[X]$.

3. Sei $\beta \in B$ ganz $\Rightarrow \text{Tr}_{L/K}(\beta), N_{L/K}(\beta) \in A$, denn mit β sind alle Konjuganten $\sigma\beta$ ganz $\Rightarrow \text{Tr}_{L/K}(\beta), N_{L/K}(\beta) \in B \cap K = A$, da A ganz abgeschlossen.

4. Es gilt: $x \in B^\times \Leftrightarrow N_{L/K}(x) \in A^\times$, denn sei

$$a \cdot N_{L/K}(x) = 1, a \in A \Rightarrow 1 = a \cdot \prod_{\sigma} \sigma x = \left(a \cdot \prod_{\sigma \neq \text{id}} \sigma x \right) x$$

also $x \in B^\times$. Umgekehrt: $yx = 1 \Rightarrow N(y)N(x) = 1$, also $N(x) \in A^\times$.

Lemma 1.13. Sei $\{\alpha_1, \dots, \alpha_n\}$ Basis von L/K mit $\alpha_i \in B, \forall i$. Sei $d = d(\alpha_1, \dots, \alpha_n)$. Dann gilt

$$dB \subseteq A\alpha_1 + \dots + A\alpha_n$$

Beweis. Ist $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n \in B, x_j \in K$. Dann ist $(x_1 \cdots, x_n)^T$ Lösung des linearen Gleichungssystems:

$$\text{Tr}_{L/K}(\alpha_i \alpha) = \sum_j \text{Tr}_{L/K}(\alpha_i \alpha_j) x_j, i = 1, \dots, n$$

Da $\text{Tr}_{L/K}(\alpha_i \alpha) \in A$ folgt

$$x_j = \frac{\text{Element aus } A}{\det(\text{Tr}_{L/K}(\alpha_i \alpha_j))}$$

Also $dx_j \in A$ □

Definition 1.14. Ein System von Elementen $\omega_1, \dots, \omega_n \in B$ heißt **Ganzheitsbasis von B über A** (A -Basis) falls jedes Element aus B sich in eindeutiger Weise als A -Linearkombination der ω_j darstellen lässt.

Falls sie existiert ist $n = [L : K]$, da jede Ganzheitsbasis auch Basis von L/K ist.

B besitzt GHB $\Leftrightarrow B$ ist freier A -Modul von Rang $[L : K]$.

Bezeichnung: Besitzt B/A eine GHB, so sagt man auch: L/K besitzt GHB.

Satz 1.15. Ist L/K endlich separabel, A ein Hauptidealring, so ist jeder endlich erzeugte B -Untermodul $M \neq 0$ von L ein freier A -Modul vom Rang $[L : K]$. Insbesondere besitzt B eine GHB ($M = B$).

Beweis. Sei $\alpha_1, \dots, \alpha_n$ Basis von L/K , o.B.d.A. $\alpha_i \in B$ (Multipliziere mit einem Element aus A).

$$\Rightarrow dB \subseteq A\alpha_1 + \dots + A\alpha_n \Rightarrow \text{Rang } B \leq [L : K]$$

Da Erzeugendensystem von B als A -Modul auch Erzeugendensystem von L als K -Vektorraum folgt $\text{Rang } B = [L : K]$.

Sei $\mu_1, \dots, \mu_r \in M$ Erzeugendensystem von M .

$$\Rightarrow \exists a \in A: a\mu_i \in B, i = 1, \dots, r \Rightarrow aM \subseteq B$$

$$\Rightarrow adM \subseteq dB \subseteq A\alpha_1 + \dots + A\alpha_n =: M_0$$

freier A -Modul von Rang $n = [L : K]$.

Nach dem Hauptsatz für Moduln über Hauptidealringen folgt, dass mit M_0 auch adM freier A -Modul ist, also auch M .

Ferner

$$\begin{aligned} [L : K] &= \text{Rang} B \leq \text{Rang} M = \text{Rang}(adM) \leq \text{Rang}(M_0) = [L : K] \\ &\Rightarrow \text{Rang} M = [L : K] \end{aligned}$$

□

Im Allgemeinen gibt es keine GHB. Aber

Satz 1.16. Seien L/K und L'/K zwei galoissche Erweiterungen von den Graden n und n' und $L \cap L' = K$.

Seien $\{\omega_1, \dots, \omega_n\}$ und $\{\omega'_1, \dots, \omega'_{n'}\}$ GHB'n von L/K bzw. L'/K mit Diskriminanten d bzw. d' .

Sind d und d' teilerfremd, d.h. $xd + x'd' = 1$ für gewisse $x, x' \in A$. So ist $\{\omega_i \omega'_j\}_{i,j}$ GHB von LL' über K mit Diskriminante $d^n d'^m$.

Beweis. Wegen $L \cap L' = K$ ist $[LL' : K] = nn' \Rightarrow \{\omega_i \omega'_j\}_{i,j}$ Basis von LL'/K .

Sei $\alpha \in LL'$ ganz.

$$\alpha = \sum_{i,j} x_{ij} \omega_i \omega'_j, x_{ij} \in K$$

zu zeigen: $x_{ij} \in A$.

Sei $G(LL'/L) = \{\sigma_1, \dots, \sigma_n\}$, $G(LL'/L) = \{\sigma'_1, \dots, \sigma'_{n'}\}$.

$$\Rightarrow G(LL'/K) = \{\sigma_k \sigma'_l \mid k = 1, \dots, n, l = 1, \dots, n'\}$$

Sei $T := (\sigma'_l \omega'_j)$, also $\det(T)^2 = d'$. Sei $a := (\sigma'_1 \alpha \cdots \sigma'_{n'} \alpha)^t$, $b := (\beta_1 \cdots \beta_{n'})^t$, $\beta_j := \sum_i x_{ij} \omega_i$.

$$\Rightarrow a = Tb$$

Sei T^* die zu T adjungierte Matrix $\Rightarrow \det(T)b = T^*a$. Da T^* und a aus ganzen Elementen von LL' bestehen, folgt $d'b$ besteht aus ganzen Elementen $d'\beta_j = \sum d'x_{ij}\omega_i$ aus L .

Also $d'x_{ij} \in A$. Ebenso (Rollen von (ω_i) und (ω'_j) vertauschen) $dx_{ij} \in A$.

$$\Rightarrow x_{ij} = dx_{ij} + x'd'x_{ij} \in A$$

Damit ist $\{\omega_i \omega'_j\}$ GHB von LL'/K .

Nachrechnen: Diskriminante

□

Bemerkung 1.17. Sei $\mathcal{O}_K \subseteq K$ der ganze Abschluss von $\mathbb{Z} \subseteq \mathbb{Q}$ in K .

\Rightarrow Jeder endlich erzeugte \mathcal{O}_K -Modul \mathfrak{a} von K besitzt eine \mathbb{Z} -Basis $\alpha_1, \dots, \alpha_n$, $n = [K : \mathbb{Q}]$

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

Die Diskriminante $d(\alpha_1, \dots, \alpha_n = \det(\sigma_i \alpha_j)^2$ hängt nicht von der Wahl dieser Basis ab:

Ist $\alpha'_1, \dots, \alpha'_n$ eine andere Basis von \mathfrak{a} :

$$T = (a_{ij}), \alpha'_j = \sum_i a_{ij} \alpha_j$$

die Übergangsmatrix

$$\Rightarrow \det T \in \mathbb{Z}^\times = \{\pm 1\}$$

$$\Rightarrow d(\alpha'_1, \dots, \alpha'_n) = \det(T)^2 d(\alpha_1, \dots, \alpha_n) = d(\alpha_1, \dots, \alpha_n)$$

Definition 1.18.

$$d(\mathfrak{a}) := d(\alpha_1, \dots, \alpha_n)$$

heißt **Diskriminante** von \mathfrak{a} .

$$d_K := d(\mathcal{O}_K) := d(\omega_1, \dots, \omega_n)$$

$\{\omega_i\}$ GHB von \mathcal{O}_K heißt **Diskriminante des Zahlkörpers** K .

Satz 1.19. Sind $\mathfrak{a} \subseteq \mathfrak{a}'$ zwei von (0) verschiedene endlich erzeugte \mathcal{O}_K -Untermodule von K , so ist der Index $(\mathfrak{a} : \mathfrak{a}')$ endlich und

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}')$$

Beweis. Ist T die Übergangsmatrix einer \mathbb{Z} -Basis von \mathfrak{a} nach \mathfrak{a}' , dann ist $\det(T) = (\mathfrak{a} : \mathfrak{a}')$. \square

2 Ideale

Sei \mathcal{O}_K der Ring der ganzen Zahlen eines Zahlkörpers K .

Bemerkung 2.1. 1. Jede Nicht-Einheit $\alpha \neq 0$ von \mathcal{O}_K ist das Produkt von irreduziblen Elementen. Denn ist α nicht selbst irreduzibel, so gilt $\alpha = \beta\gamma$ mit β, γ Nicht-Einheiten.

$$\Rightarrow 1 < |N_{K/\mathbb{Q}}(\beta)|, |N_{K/\mathbb{Q}}(\gamma)| < |N_{K/\mathbb{Q}}(\alpha)|$$

\Rightarrow Behauptung durch Induktion nach $|N_{K/\mathbb{Q}}|$.

2. Zerlegung in irreduzible Elemente ist i.A. nicht eindeutig.

Beispiel: $K = \mathbb{Q}(\sqrt{-5})$, dann ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ und es gilt $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

Idee: Durch Einführung „idealer Zahlen“ (Kummer) bzw. Ideale (Dedekind) Eindeutigkeit zu erreichen.

Definition 2.2. Ein noetherscher, ganz abgeschlossener Integritätsbereich R , in dem jedes von Null verschiedene Primideal maximal ist heißt **Dedekind-Ring**.

Erinnerung: Ein Ring heißt **noethersch** \Leftrightarrow jedes Ideal von R ist endlich erzeugt \Leftrightarrow Sei $\alpha_1 \subseteq \dots \subseteq \alpha_n \subseteq \dots$ eine aufsteigende Kette von Idealen in R , dann wird diese stationär, d.h.

$$\exists n_0 \in \mathbb{N}: \alpha_n = \alpha_{n_0}, \forall n \geq n_0$$

Ein Ideal $\mathfrak{m} \neq R$ heißt **maximal**

$$\Leftrightarrow \forall \alpha \subseteq R: \alpha \subseteq \mathfrak{m} \Rightarrow \alpha = \mathfrak{m} \vee \alpha = R$$

$$\Leftrightarrow R/\mathfrak{m} \text{ ist Körper}$$

Ein Ideal $\mathfrak{p} \subsetneq R$ heißt **Primideal**

$$\Leftrightarrow a \cdot b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}$$

$$\Leftrightarrow R/\mathfrak{p} \text{ ist nullteilerfrei, d.h. Integritätsring}$$

Insbesondere $\mathfrak{m} \subseteq R$ maximal $\Rightarrow \mathfrak{m}$ Primideal.

Satz 2.3. Sei K ein Zahlkörper. Dann ist \mathcal{O}_K ein Dedekind-Ring.

Beweis. \mathcal{O}_K ist noethersch, weil jedes Ideal $\alpha \subseteq \mathcal{O}_K$ nach 1.15 ein endlich erzeugter (freier) \mathbb{Z} -Modul, also erst recht endlich erzeugt als \mathcal{O}_K -Modul.

Als ganzer Abschluss von \mathbb{Z} in K ist \mathcal{O}_K ganz abgeschlossen. 1.8

Sei nun $\mathfrak{p} \neq (0)$ ein Primideal von \mathcal{O}_K .

$\Rightarrow \mathfrak{p} \cap \mathbb{Z} = (p) \neq (0)$, Primideal von \mathbb{Z} : Primidealeigenschaft ist klar und $\mathfrak{p} \cap \mathbb{Z} \neq (0)$ sieht man wie folgt:

Ist $y \in \mathfrak{p}, y \neq 0$ und $y^n + \dots + a_0 = 0$ eine Gleichung für $y, a_i \in \mathbb{Z}$ n minimal, so ist $a_0 \in \mathfrak{p} \cap \mathbb{Z}$ und $a_0 \neq 0$.

Sei $\bar{\mathcal{O}} := \mathcal{O}_K/\mathfrak{p}$ (Integritätsbereich) und sei $\kappa := \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} = (\mathfrak{p} + \mathbb{Z})/\mathfrak{p} \subseteq \bar{\mathcal{O}}/\mathfrak{p}$.

$\Rightarrow \bar{\mathcal{O}}$ entsteht aus κ durch Adjunktion endlich vieler algebraischer Elemente und ist somit ein Körper.

$$\kappa[\alpha] = \kappa(\alpha) \Leftrightarrow \alpha \text{ algebraisch}$$

$\Rightarrow \mathfrak{p}$ maximal. □

Lemma 2.4. Sei \mathcal{O} ein Dedekindring, $\alpha \neq (0)$ ein Ideal. Dann gilt: Es gibt von (0) verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ mit

$$\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \subseteq \alpha$$

Beweis. Sei

$$\mathfrak{M} = \{\alpha \subseteq \mathcal{O} \text{ Ideal} \mid \alpha \neq (0), \nexists \mathfrak{p}_1, \dots, \mathfrak{p}_r: \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \subseteq \alpha\}$$

Angenommen $\mathfrak{M} \neq \emptyset$. Da \mathcal{O} noethersch ist, bricht jede aufsteigende Idealkette von \mathfrak{M} ab, d.h. \mathfrak{M} ist bezüglich \subseteq induktiv geordnet.

Mit dem Lemma von Zorn folgt \mathfrak{M} besitzt maximales Element α .

Dies kann kein Primideal sein, d.h. es gibt $b_1, b_2 \in \mathcal{O}$ mit $b_1, b_2 \notin \mathfrak{a}$, aber $b_1 b_2 \in \mathfrak{a}$.
 Sei $\mathfrak{a}_1 = (b_1) + \mathfrak{a}, \mathfrak{a}_2 = (b_2) + \mathfrak{a}$.

$$\Rightarrow \mathfrak{a} \subsetneq \mathfrak{a}_1, \mathfrak{a}_2 \wedge \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$$

Wegen der Maximalität von \mathfrak{a} ist $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathfrak{M}$, also gibt es $\mathfrak{p}_{11}, \dots, \mathfrak{p}_{1r}, \mathfrak{p}_{21}, \dots, \mathfrak{p}_{2s}$ Primideale in \mathcal{O} mit

$$\mathfrak{p}_{11} \cdot \dots \cdot \mathfrak{p}_{1r} \subseteq \mathfrak{a}_1, \mathfrak{p}_{21} \cdot \dots \cdot \mathfrak{p}_{2s} \subseteq \mathfrak{a}_2 \Rightarrow \mathfrak{p}_{11} \cdot \dots \cdot \mathfrak{p}_{1r} \mathfrak{p}_{21} \cdot \dots \cdot \mathfrak{p}_{2s} \subseteq \mathfrak{a} \not\subseteq$$

□

Lemma 2.5. Sei \mathfrak{p} ein Primideal des Dedekindrings \mathcal{O} , $K = \text{Quot}(\mathcal{O})$ ($K \neq \mathcal{O}$) und

$$\mathfrak{p}^{-1} := \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\}$$

(insbesondere $\mathcal{O} \subseteq \mathfrak{p}^{-1}$).

Dann ist für jedes Ideal $\mathfrak{a} \neq (0)$:

$$\mathfrak{a}\mathfrak{p}^{-1} = \left\{ \sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p} \right\} \neq \mathfrak{a}$$

Beweis. Sei $a \in \mathfrak{p}, a \neq 0$ (o.B.d.A. $\mathfrak{p} \neq (0)$, sonst $\mathfrak{p}^{-1} = K$, also $\mathfrak{a}\mathfrak{p}^{-1} = K \neq \mathfrak{a}$).

$$\stackrel{2.4}{\Rightarrow} \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}, r \text{ sei minimal}$$

$\Rightarrow \exists \mathfrak{p}_i \subseteq \mathfrak{p}$ (sonst gäbe es für alle i ein $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ mit $a_1 \cdot \dots \cdot a_r \in \mathfrak{p}$), o.B.d.A. $i = 1$.

$$\mathfrak{p}_1 \subseteq \mathfrak{p} \rightarrow \mathfrak{p}_1 = \mathfrak{p}$$

da \mathfrak{p}_1 maximal.

Wegen $\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_r \subseteq (a)$ gibt es $b \in \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_r \setminus (a)$, also $a^{-1}b \notin \mathcal{O}$.

Andererseits ist $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$ und somit $a^{-1}b \in \mathfrak{p}^{-1}$.

$$\Rightarrow \mathfrak{p}^{-1} \neq \mathcal{O}$$

Sei nun $\mathfrak{a} \neq (0)$ ein Ideal von \mathcal{O} und $\alpha_1, \dots, \alpha_n$ ein \mathcal{O} -Erzeugersystem von \mathfrak{a} . Angenommen $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$.

$$\Rightarrow x \in \mathfrak{p}^{-1}, x\alpha_i = \sum_j a_{ij}\alpha_j, a_{ij} \in \mathcal{O}$$

Sei $A = (x\delta_{ij} - a_{ij})_{ij}$, also $A(\alpha_1 \cdot \dots \cdot \alpha_n)^T = 0$.

$$\Rightarrow d(\alpha_1) = \dots = d\alpha_n = 0, d = \det A$$

$\Rightarrow d = 0$, da nicht alle $\alpha_i = 0$. Also ist x Nullstelle des normierten Polynoms $\det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$, also x ist ganz über \mathcal{O} , also $x \in \mathcal{O}$, da \mathcal{O} ganz abgeschlossen.

Damit $\mathfrak{p}^{-1} = \mathcal{O} \not\subseteq$.

□

Satz 2.6. Sei \mathcal{O} ein Dedekind-Ring. Dann besitzt jedes von (0) verschiedene Ideal $\mathfrak{a} \subseteq \mathcal{O}$ eine bis auf Reihenfolge eindeutige Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$$

in Primideale von \mathcal{O} .

Beweis. Existenz: Sei

$$\mathfrak{M} = \{\mathfrak{a} \subseteq \mathcal{O} \mid \mathfrak{a} \neq (0), (1), \mathfrak{a} \text{ besitzt keine Primzerlegung}\}$$

Angenommen \mathfrak{M} ist nicht leer. So gibt es (wie oben, da \mathcal{O} noethersch) maximales Element $\mathfrak{a} \in \mathfrak{M}$.

\Rightarrow Es gibt maximales Ideal $\mathfrak{p} \subseteq \mathcal{O}$ sodass $\mathfrak{a} \subsetneq \mathfrak{p}$ da $\mathfrak{a} \in \mathfrak{M}$.

$$\Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$$

Wegen 2.5 ist $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}^{-1}$, $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$, also, da \mathfrak{p} maximal ist $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Ferner ist $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$ (sonst $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$).

Da \mathfrak{a} maximales Element von \mathfrak{M} , gilt $\mathfrak{a}\mathfrak{p}^{-1} \notin \mathfrak{M}$, besitzt also Zerlegung in Primideale.

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$$

$$\Rightarrow \mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \cdot \mathfrak{p}^{-1}$$

Eindeutigkeit: Seien $\mathfrak{a} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_s$ zwei Zerlegungen.

$$\Rightarrow \exists i: \mathfrak{p}_1 | \mathfrak{q}_i, \text{ d.h. } \mathfrak{p}_1 \supseteq \mathfrak{q}_i \stackrel{\mathfrak{q}_i \text{ max}}{\Rightarrow} \mathfrak{p}_1 = \mathfrak{q}_i$$

$$\Rightarrow \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_{i-1} \cdot \mathfrak{q}_{i+1} \cdot \dots \cdot \mathfrak{q}_s$$

$$\Rightarrow r = s, \mathfrak{p}_i = \mathfrak{q}_i, \forall i \text{ (nach Umordnung)}$$

Somit hat man für jedes Ideal $\mathfrak{a} \neq (0)$ in einem Dedekindring \mathcal{O} eine eindeutige Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdot \dots \cdot \mathfrak{p}_r^{v_r}$$

$\mathbb{N} \ni v_i > 0, \mathfrak{p}_i$ paarweise verschiedene Primideale. □

Definition 2.7. Sei K der Quotientenkörper eines Dedekindringes \mathcal{O} . Ein **gebrochenes Ideal** von K ist ein endlich erzeugter \mathcal{O} -Untermodul $\mathfrak{a} \neq (0)$.

Bemerkung 2.8. 1. Ist $a \in \mathbb{K}^\times$, so ist $(a) := a\mathcal{O}$ ein **gebrochenes Hauptideal**.

2. Ein Untermodul $\mathfrak{a} \neq (0)$ ist genau dann ein gebrochenes Ideal, wenn es ein $0 \neq c \in \mathcal{O}$ gibt, mit $c\mathfrak{a} \subseteq \mathcal{O}$, denn sei $c \in \mathcal{O}, c \neq 0$ mit $\mathfrak{a} \subseteq \mathcal{O} \Rightarrow \mathfrak{a} \subseteq (c^{-1})$, da \mathcal{O} noethersch ist, ist mit (c^{-1}) auch der Modul \mathfrak{a} endlich erzeugt.

Umgekehrt: Sei $\alpha_1, \dots, \alpha_k$ ein Erzeugendensystem des \mathcal{O} -Untermoduls $\mathfrak{a} \subseteq K$. Sei $c \in \mathcal{O}$ der Hauptnenner, dann folgt $c\alpha_i \in \mathcal{O}, \forall i \Rightarrow c\mathfrak{a} \subseteq \mathcal{O}$.

3. Sei \mathfrak{a} ein gebrochenes Ideal von K mit $\mathfrak{a} \subseteq \mathcal{O}$, so ist \mathfrak{a} ein gewöhnliches Ideal von \mathcal{O} , wir sagen \mathfrak{a} ist **ganzes Ideal von \mathcal{O}** .

Satz 2.9. Die gebrochenen Ideale des Quotientenkörpers K eines Dedekindringes \mathcal{O} bilden eine abelsche Gruppe, die so genannte **Idealgruppe \mathcal{J}_K** .

Das Einselement ist $(1) = \mathcal{O}$, das Inverse zu \mathfrak{a} ist

$$\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$$

Beweis. Assoziativität, Kommutativität und $\mathfrak{a} \cdot (1) = \mathfrak{a}$ ist trivial.

Sei \mathfrak{p} Primideal $\xrightarrow{2.6} \mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$, also $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Ist $\mathfrak{a} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$ ganzes Ideal, so ist $\mathfrak{b} := \mathfrak{p}_1^{-1} \cdot \dots \cdot \mathfrak{p}_r^{-1}$ Inverses von \mathfrak{a} .

Wegen $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ ist $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Umgekehrt: Sei $x \in \mathfrak{a}^{-1}$, also $x\mathfrak{a} \subseteq \mathcal{O} \Rightarrow x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, also $x \in \mathfrak{b}$.

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

Ist \mathfrak{a} gebrochenes Ideal und $0 \neq c \in \mathcal{O}$, mit $c\mathfrak{a} \subseteq \mathcal{O}$, so ist $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ das Inverse von $c\mathfrak{a}$, also $\mathcal{O} = (c\mathfrak{a})(c\mathfrak{a})^{-1} = \mathfrak{a}\mathfrak{a}^{-1}$.

\mathfrak{a}^{-1} ist gebrochenes Ideal: $0 \neq a \in \mathfrak{a} \Rightarrow a\mathfrak{a}^{-1} \subseteq \mathcal{O} \Rightarrow \mathfrak{a}^{-1}$ gebrochenes Ideal. \square

Korollar 2.10. Jedes gebrochene Ideal \mathfrak{a} besitzt eindeutige Produktzerlegung

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

mit $\nu_{\mathfrak{p}} \in \mathbb{Z}$ und $\nu_{\mathfrak{p}} = 0$ für fast alle \mathfrak{p} .

Mit anderen Worten: Die Idealgruppe ist freie abelsche Gruppe über der Menge aller Primideale $\neq (0)$ von \mathcal{O} .

$$\mathcal{J}_K \cong \bigoplus_{\mathfrak{p} \neq (0)} \mathbb{Z}$$

Beweis. Jedes gebrochene Ideal ist Quotient zweier ganzer Ideale $\mathfrak{a} = \mathfrak{b}c^{-1}$, die nach Satz 2.6 eine eindeutige Primzerlegung besitzen. \square

Definition 2.11. 1. Mit \mathcal{P}_K werde die Untergruppe von \mathcal{J}_K bezeichnet, die aus gebrochenen Hauptidealen $(a) = a\mathcal{O}, a \in K^\times$ besteht.

2. Die Faktorgruppe $\text{Cl}_K := \mathcal{J}_K / \mathcal{P}_K$ heißt **Idealklassengruppe**, kurz **Klassengruppe** von K .

Wir haben die exakte Sequenz

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \mathcal{O}^\times & \longrightarrow & K^\times & \xrightarrow{a \mapsto (a)} & \mathcal{J}_K \longrightarrow \text{Cl}_K \longrightarrow 0 \\
 & & & & & \searrow & \nearrow \\
 & & & & & & \mathcal{P}_K
 \end{array}$$

mit anderen Worten: \mathcal{O}^\times beschreibt den Verlust, Cl_K die Größe der Ausdehnung beim Übergang der Zahlen auf die Ideale.

Somit: Untersuchung der Gruppen \mathcal{O}^\times und Cl_K . Wir wollen zeigen, daß Cl_K eine endliche Gruppe ist, für jeden algebraischen Zahlkörper K .

3 Gitter

Bei der Betrachtung von Primelementen und Einheiten von $\mathbb{Z}[i]$ wurde $\mathbb{Z}[i]$ als Menge von Gitterpunkten in der Gauß'schen Zahlenebene \mathbb{C} betrachtet.

Dies wurde von Minkowski (1864-1909) auf beliebige Zahlkörper verallgemeinert.

Definition 3.1. Sei V ein n -dimensionaler \mathbb{R} -Vektorraum. Ein **Gitter** Γ von V ist eine Untergruppe

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren v_1, \dots, v_m von V . $\{v_1, \dots, v_m\}$ heißt **Basis von Γ** und die Menge

$$\Phi := \{x_1v_1 + \dots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

heißt **Grundmasche** des Gitters Γ .

Γ heißt **vollständig** oder **\mathbb{Z} -Struktur von V** , wenn $m = n$ ist.

Bemerkung 3.2.

$$\Gamma \text{ vollständig} \Leftrightarrow \bigcup_{\gamma \in \Gamma} (\Phi + \gamma) = V$$

Definition 3.3. Sei $G \subseteq V$ eine Untergruppe des n -dimensionalen \mathbb{R} -Vektorraums V . Dann heißt G **diskret**, wenn alle $\gamma \in G$ isolierte Punkte in V sind, d.h. für alle $\gamma \in G$ gibt es eine Umgebung $U_\gamma \subseteq V$ (in der \mathbb{R} -Topologie von V) mit $G \cap U_\gamma = \gamma$.

Satz 3.4. Eine Untergruppe Γ von $V \cong \mathbb{R}^n$ ist ein Gitter genau dann, wenn Γ diskret und abgeschlossen ist.

Beweis. Sei $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$ ein Gitter und $v_1, \dots, v_m, v_{m+1}, \dots, v_n$ eine Basis von V . Sei $\gamma = \sum_{i=1}^m a_i v_i \in \Gamma$, dann ist

$$U_\gamma := \left\{ \sum_{i=1}^n x_i v_i \mid |a_i - x_i| < 1, i = 1, \dots, m \right\}$$

eine Umgebung von γ mit $U_\gamma \cap \Gamma = \{\gamma\}$, also Γ diskret und offensichtlich abgeschlossen.

Umgekehrt: Sei Γ diskrete abgeschlossene Untergruppe und V_0 der von Γ in V erzeugte Untervektorraum. Sei $m = \dim V_0$. Sei $\{u_1, \dots, u_m\} \subset \Gamma$ eine Basis von V_0 .

$$\Gamma_0 := \mathbb{Z}u_1 + \dots + \mathbb{Z}u_m \subseteq \Gamma$$

ist ein vollständiges Gitter in V_0 .

Behauptung: $(\Gamma : \Gamma_0) < \infty$. Sei $\{\gamma_i\}$ ein Repräsentantensystem von Γ/Γ_0 . Da Γ_0 vollständig in V_0 ist $V_0 = \bigcup_{\gamma \in \Gamma_0} (\Phi_0 + \gamma)$, Φ_0 Grundmasche von Γ_0 in V_0

$$\Rightarrow \gamma_i = \mu_i + \gamma_{0i}, \mu_i \in \Phi_0, \gamma_{0i} \in \Gamma_0 \subseteq V_0$$

Da $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ diskret in der beschränkten Menge Φ_0 , $\{\mu_i\}$ abgeschlossen, muss ihre Anzahl endlich sein.

Sei nun $q := (\Gamma : \Gamma_0)$, dann ist $q\Gamma \subseteq \Gamma_0$.

$$\Rightarrow \Gamma_0 \subseteq \Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z} \left(\frac{1}{q}u_1 \right) + \dots + \mathbb{Z} \left(\frac{1}{q}u_m \right)$$

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen besitzt Γ eine \mathbb{Z} -Basis v_1, \dots, v_r , $r \leq m$ (also $r = m$, wegen $\Gamma_0 \subseteq \Gamma$), d.h.

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$$

$\{v_1, \dots, v_m\}$ sind linear unabhängig, da sie V_0 aufspannen $\Rightarrow \Gamma$ ist Gitter. □

Lemma 3.5. Ein Gitter ist vollständig, genau dann, wenn es eine beschränkte Menge $M \subseteq V$ gibt, mit $\bigcup_{\gamma \in \Gamma} (M + \gamma) = V$.

Beweis. Ist Γ vollständig, so wähle $M =$ Grundmasche von Γ .

Umgekehrt sei V_0 der von Γ aufgespannte \mathbb{R} -Untervektorraum von V .

Sei $v \in V$. Wegen $V = \bigcup_{\gamma \in \Gamma} (M + \gamma)$ gilt

$$\forall v \in \mathbb{N}: \exists a_v \in M, \gamma_v \in \Gamma \subseteq V_0: v\mathbb{N} = a_v + \gamma_v$$

Da M beschränkt, ist $\left\{ \frac{a_v}{v} \right\}$ eine Nullfolge und wegen der Abgeschlossenheit von V_0 folgt:

$$v = \underbrace{\lim_{v \rightarrow \infty} \frac{a_v}{v}}_{=0} + \lim_{v \rightarrow \infty} \frac{\gamma_v}{v} \in V_0$$

□

Definition 3.6. 1. Ein **euklidischer Vektorraum** V ist ein endlichdimensionaler \mathbb{R} -Vektorraum mit symmetrischer positiv definiter Bilinearform

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$$

Volumenbegriff (Haar'sches Maß)

Sei $e_1, \dots, e_n, n = \dim V$, eine Orthonormalbasis. Für n linear unabhängige Vektoren v_1, \dots, v_n hat dann

$$\Phi(v_1, \dots, v_n) := \{x_1 v_1 + \dots + x_n v_n \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

per Definition das Volumen

$$\text{vol}(\Phi(v_1, \dots, v_n)) := |\det A|, A = (a_{ij}), v_i = \sum_{j=1}^n a_{ij} e_j \text{ Übergangsmatrix}$$

also $\text{vol}(\Phi(e_1, \dots, e_n)) = 1$ (Normierung) oder in invarianter Weise: Wegen

$$\left(\langle v_i, v_j \rangle \right)_{i,j} = \left(\sum_{k,l} a_{ik} a_{jl} \langle e_k, l_j \rangle \right)_{i,j} = \left(\sum_k a_{ik} a_{jk} \right)_{i,j} A A^t$$

$$\text{vol}(\Phi) = \left| \det \left(\langle v_i, v_j \rangle \right) \right|^{1/2}$$

2. Ist Γ ein Gitter in $V, V \cong \mathbb{R}^n$, mit Grundmasche Φ dann setzen wir $\text{vol}(\Gamma) := \text{vol}(\Phi)$.

Unabhängig von der Wahl der Gitterbasis, weil die Übergangsmatrix zu einer endlichen Basis ganzzahlige Einträge hat, also eine Determinante ± 1 ; dadurch wird Φ in eine Menge gleichen Inhalts transformiert.

Definition 3.7. Eine Teilmenge X von $V, V \cong \mathbb{R}^n$ heißt

zentralsymmetrisch $\Leftrightarrow (x \in X \Rightarrow -x \in X)$

konvex $\Leftrightarrow (x, y \in X \Rightarrow \{ty + (1-t)x \mid 0 \leq t \leq 1\} \subseteq X)$

Satz 3.8 (Gitterpunktsatz). Sei Γ ein vollständiges Gitter im euklidischen Vektorraum $V, n = \dim V$. Sei X eine zentralsymmetrische konvexe Teilmenge von V mit

$$\text{vol}(X) > 2^n \cdot \text{vol}(\Gamma)$$

Dann enthält X mindestens einen von Null verschiedenen Gitterpunkt $m \in \Gamma$.

Beweis. Es genügt zu zeigen: Es gibt $\gamma_1, \gamma_2 \in \Gamma$ mit $\gamma_1 \neq \gamma_2$ und

$$\left(\frac{1}{2}X + \gamma_1 \right) \cap \left(\frac{1}{2}X + \gamma_2 \right) \neq \emptyset$$

denn sei ρ ein Punkt des Durchschnitts, also

$$\rho = \frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2, x_1, x_2 \in X$$

$$\Rightarrow \gamma := \gamma_1 - \gamma_2 = \frac{1}{2}x_1 - \frac{1}{2}x_2$$

ist der Mittelpunkt der Strecke $\overline{x_2(-x_2)}$ und damit $\gamma \in \Gamma \cap X$ sowie $\gamma \neq 0$, da $\gamma_1 \neq \gamma_2$.
Wären nun die Mengen $\frac{1}{2}X + \gamma, \gamma \in \Gamma$ paarweise disjunkt, dann sind $\Phi \cap (\frac{1}{2}X + \gamma), \gamma \in \Gamma$ paarweise disjunkt, Φ Grundmasche von Γ .

$$\Rightarrow \text{vol}(\Gamma) \geq \sum_{\gamma \in \Gamma} \text{vol} \left(\Phi \cap \left(\frac{1}{2}X + \gamma \right) \right)$$

Wegen

$$\text{vol} \left(\Phi \cap \left(\frac{1}{2}X + \gamma \right) \right) = \text{vol} \left((\Phi - \gamma) \cap \frac{1}{2}X \right)$$

folgt

$$\text{vol}(\Gamma) \geq \sum_{\gamma \in \Gamma} \text{vol} \left((\Phi - \gamma) \cap \frac{1}{2}X \right) = \text{vol} \left(\frac{1}{2}X \right) = \frac{1}{2^n} \text{vol}(X) \quad \zeta$$

□

4 Minkowski-Theorie

Definition 4.1. Sei K ein algebraischer Zahlkörper, $n = [K : \mathbb{Q}]$, $\tau_i: K \hookrightarrow \mathbb{C}, i = 1, \dots, n$, die n komplexen Einbettungen.

Betrachte

$$j: K \rightarrow K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}$$

$$a \mapsto ja := (\tau a)_{\tau}$$

Der \mathbb{C} -Vektorraum $K_{\mathbb{C}}$ ist mit hermit'schen Skalarprodukt ausgestattet:

$$\langle x, y \rangle := \sum_{\tau} x_{\tau} \overline{y_{\tau}}$$

Es ist $\langle \cdot, y \rangle$ linear, $\overline{\langle x, y \rangle} = \langle y, x \rangle$, $\langle x, x \rangle > 0$, für $x \neq 0$; $K_{\mathbb{C}}$ sei im Folgenden mit dieser Metrik ausgestattet.

Definition 4.2. Die Galoisgruppe $G(\mathbb{C}/\mathbb{R})$ wird erzeugt von der komplexen Konjugation:

$$F: z \mapsto \bar{z}.$$

$G(\mathbb{C}/\mathbb{R})$ operiert auf $K_{\mathbb{C}}$: $G(\mathbb{C}/\mathbb{R})$ operiert auf den Faktoren \mathbb{C} von $K_{\mathbb{C}}$ und auf $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\tau_1, \dots, \tau_n\}$

$$\tau: K \hookrightarrow \mathbb{C} \rightsquigarrow \bar{\tau}: K \hookrightarrow \mathbb{C}, \bar{\tau}(x) := \overline{\tau(x)}$$

F induziert eine Involution

$$F: K_{\mathbb{C}} \rightarrow K_{\mathbb{C}}$$

$$z = (z_{\tau})_{\tau} \mapsto F(z) = (\overline{z_{\tau}})_{\tau}$$

$\langle \cdot, \cdot \rangle$ ist invariant unter F :

$$\langle Fx, Fy \rangle = F \langle x, y \rangle$$

Definition 4.3. Wir haben auf $K_{\mathbb{C}}$ die lineare Abbildung

$$\text{Tr}: K_{\mathbb{C}} \rightarrow \mathbb{C}$$

$$(x_{\tau})_{\tau} \mapsto \sum_{\tau} x_{\tau}$$

ist auch invariant unter F und

$$\Rightarrow K \xrightarrow{j} K_{\mathbb{C}} \xrightarrow{\text{Tr}} \mathbb{C}$$

ergibt die übliche Spur von K/\mathbb{Q} :

$$\text{Tr}_{K/\mathbb{Q}}(a) = \text{Tr}_{ja}, a \in K$$

Definition 4.4. Sei

$$K_{\mathbb{R}} := K_{\mathbb{C}}^{+} = \left[\prod_{\tau} \mathbb{C} \right]^{+}$$

der unter F , d.h. $G(\mathbb{C}/\mathbb{R})$, invariante Teilraum von $K_{\mathbb{C}}$

$$K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \mid z_{\bar{\tau}} = \overline{z_{\tau}}, \forall \tau\}$$

Wegen $\bar{\tau}(a) = \overline{\tau(a)}$, $a \in K$ ist $F(ja) = ja$.

$$\Rightarrow j: K \rightarrow K_{\mathbb{R}}$$

Sei

$$\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{K_{\mathbb{R}}}: K_{\mathbb{R}} \times K_{\mathbb{R}} \rightarrow \mathbb{R}$$

die Einschränkung von $\langle \cdot, \cdot \rangle$ auf den \mathbb{R} -Vektorraum $K_{\mathbb{R}}$, denn für $x, y \in K_{\mathbb{R}}$ ist $\langle x, y \rangle \in \mathbb{R}$, da $F \langle x, y \rangle = \langle Fx, Fy \rangle = \langle x, y \rangle$.

Ferner gilt $\langle x, y \rangle = \langle y, x \rangle = \langle y, x \rangle$, $\langle x, x \rangle > 0, x \neq 0$.

Also ist $K_{\mathbb{R}}$ euklidischer Vektorraum. $K_{\mathbb{R}}$ heißt **Minkowski-Raum**, das Skalarprodukt $\langle \cdot, \cdot \rangle$ auf $K_{\mathbb{R}}$ heißt **kanonische Metrik**, das zugehörige Volumen das **kanonische Maß**.

Wegen $\text{Tr} \circ F = F \circ \text{Tr}$ haben wir auf $K_{\mathbb{R}}$ die \mathbb{R} -lineare Abbildung $\text{Tr}: K_{\mathbb{R}} \rightarrow \mathbb{R}$ und es gilt

$$\text{Tr}_{K/\mathbb{Q}} = \text{Tr}j(a), a \in K$$

Definition 4.5. Sei $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) := \{\tau_1, \dots, \tau_n\}$. Die Einbettungen ρ_1, \dots, ρ_r aus $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ mit

$$\rho_i: K \rightarrow \mathbb{R}$$

heien **reell**, die nicht reellen heien **komplex** und gruppieren sich zu Paaren

$$\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s}: K \rightarrow \mathbb{C}$$

Offensichtlich $n = r + 2s$.

Da F die ρ invariant lt und σ und $\overline{\sigma}$ vertauscht, folgt

$$K_{\mathbb{R}} = \left\{ (z_{\tau})_{\tau} \in \prod_{\tau} \mathbb{C} \mid z_{\rho} \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z_{\sigma}} \right\}$$

Satz 4.6. Es gibt einen Isomorphismus

$$f: K_{\mathbb{R}} \rightarrow \prod_{\tau} \mathbb{R} \cong \mathbb{R}^{r+2s}$$

$$(z_{\tau})_{\tau} \mapsto (x_{\tau})_{\tau}$$

mit

$$x_{\rho} = z_{\rho}, x_{\sigma} = \Re(z_{\sigma}); x_{\overline{\sigma}} = \Im(z_{\sigma})$$

Die kanonische Metrik $\langle \cdot, \cdot \rangle$ wird in das Skalarprodukt

$$(x, y) := \sum_{\tau} a_{\tau} x_{\tau} y_{\tau}, a_{\tau} = \begin{cases} 1 & \tau \text{ reell} \\ 2 & \tau \text{ komplex} \end{cases}$$

berfhrt. Dadurch wird das kanonische Ma von $K_{\mathbb{R}}$ auf \mathbb{R}^{r+2s} bertragen.

Beweis. Isomorphie ist klar.

Seien $(z_{\tau}) = (x_{\tau} + iy_{\tau})$ und $(z'_{\tau}) = (x'_{\tau} + iy'_{\tau}) \in K_{\mathbb{R}}$.

$$z_{\rho} \cdot \overline{z'_{\rho}} = x_{\rho} \cdot x'_{\rho}$$

$$z_{\sigma} \overline{z'_{\sigma}} + z_{\overline{\sigma}} \overline{z'_{\overline{\sigma}}} = z_{\sigma} \overline{z'_{\sigma}} + \overline{z_{\sigma}} z'_{\sigma} = 2\Re(z_{\sigma} \overline{z'_{\sigma}}) = 2x_{\sigma} x'_{\sigma} + x_{\overline{\sigma}} x'_{\overline{\sigma}}$$

da

$$y_{\sigma} = x_{\overline{\sigma}}, y'_{\sigma} = x'_{\overline{\sigma}}$$

□

Bemerkung 4.7. Das kanonische Ma von $K_{\mathbb{R}}$ unterscheidet sich vom Lebesgue-Ma auf \mathbb{R}^{r+2s} durch

$$\text{vol}_{K_{\mathbb{R}}}(X) = 2^s \text{vol}_{\mathbb{R}^{r+2s}}(fX)$$

Satz 4.8. Ist $\mathfrak{a} \neq (0)$ ein Ideal in O_K , so ist $\Gamma := \text{ja}$ ein vollstndiges Gitter in $K_{\mathbb{R}}$ mit Grundmascheninhalt

$$\text{vol}(\Gamma) = \sqrt{|d_K|} \cdot (O_K : \mathfrak{a})$$