

Algebraische Zahlentheorie

Geschrieben von
Jan Pöschko
auf Grundlage der Vorlesung von
Clemens Heuberger

TU Graz
Sommersemester 2007

Inhaltsverzeichnis

1	Ganzalgebraische Zahlen	5
1.2	Ganzalgebraische Zahlen	5
1.3	Ordnung in algebraischen Zahlkörpern	7
1.4	Transzendenz von e und π	11
2	Struktur der Idealhalbgruppe	15
2.1	Lokalisierung	15
2.3	Primidealzerlegung	19
2.5	Absolutnorm von Idealen	26
2.6	Faktorisierung von Primzahlen in Zahlkörpern	28
2.7	Endlichkeit der Klassenzahl	30
3	Struktur der Einheitengruppe	35
3.1	Leichtes über die Struktur	35
3.2	Einführung in die Geometrie der Zahlen	38
3.3	Dirichletscher Einheitsatz	43
3.4	Regulator	47
3.5	Berechenbarkeit von Fundamenteinheiten	51

Inhaltsverzeichnis

1 Ganzalgebraische Zahlen

1.2 Ganzalgebraische Zahlen

...

BEWEIS Betrachte das Element

$$z + vy_2 = a_1x_1 + vm_2x_2.$$

Basiswechsel:

$$\begin{aligned}x'_1 &= x_1 - zx_2 \\x'_2 &= x_2.\end{aligned}$$

Somit

$$\begin{aligned}N \ni z + vy_2 &= a_1(x_1 + ux'_2) + vm_2x'_2 \\&= a_1x'_1 + (a_1u + vm_2)x'_2 \\&= a_1x'_1 + dx'_2.\end{aligned}$$

Wegen der Optimalität der Wahl von z ist

$$(a_1) \not\subseteq (d), \text{ aber } (a_1) \subseteq (d),$$

somit $(a_1) = (d)$, $a_1 \mid d \mid m_2$.

Erkenne z zum y_1 und das a_1 zum m . ■

Lemma (Kardinalität der Basis ist kanonisch) Sei M ein freier R -Modul, R ein Hauptidealbereich. Dann haben je zwei Basen dieselbe Kardinalität.

BEWEIS Falls R ein Körper ist, sind wir einem Vektorraum und es ist alles bekannt. Andernfalls enthält R ein maximales Ideal $I \neq \{0\}$.

Betrachte M/IM als R/I -Modul. Da R/I ein Körper ist, ist M/IM ein R/I -Vektorraum.

Sei x_1, \dots, x_r eine Basis von M . Behauptung: x_1, \dots, x_r ist R/I -Basis von M/MI .

Beweis: Erzeugendensystem klar.

Basis:

$$\begin{aligned}(a_1 + I)x_1 + \dots + (a_r + I)x_r &= 0 \\ \Rightarrow a_1x_1 + \dots + a_rx_r &\in IM \\ a_1x_1 + \dots + a_rx_r &= i_1x_1 + \dots + i_rx_r, \quad i_j \in I.\end{aligned}$$

Da x_1, \dots, x_r Basis war, gilt

$$a_j = i_j \in I.$$

Das heißt

$$r = \dim_{R/I} M/IM,$$

also unabhängig von Basis. ■

1 Ganzalgebraische Zahlen

Definition Sei M ein R -Modul, R ein freier HIB. Dann heißt die Kardinalität einer beliebigen der Rang von M .

BEWEIS (BEWEIS DES STRUKTURSATZES) M ein endlicher R -Modul.

Wähle Erzeugendensystem z_1, \dots, z_m von M . Die Abbildung

$$\Phi : R^m \rightarrow M; \Phi(a_1, \dots, a_m) = \sum_{j=1}^m a_j z_j$$

ist R -Modul-Epimorphismus.

$\text{Ker } \Phi$ ist lt. Lemma freier R -Untermodul von R^m . Wähle Basen von R^m und $\text{Ker } \Phi$ gemäß Lemma.

x_1, \dots, x_r Basis von R^m . $d_1 x_1, \dots, d_m x_m$ Basis von $\text{Ker } \Phi$ mit $d_1 | \dots | d_m$.

$$\begin{aligned} R^m &= R x_1 \oplus \dots \oplus R x_m \\ \text{Ker } \Phi &= d_1 R x_1 \oplus \dots \oplus d_m R x_m. \end{aligned}$$

Also

$$M \simeq R^m / \text{Ker } \Phi = R/d_1 R x_1 \oplus \dots \oplus R/d_m R x_m \simeq R/d_1 R \oplus \dots \oplus R/d_m R.$$

Lasse Faktoren R/R für $d_j \in \mathcal{E}(R)$ weg und schreibe R für $R/0R$. ■

Satz 1.6 (Struktur des ganzen Abschlusses über HIB) Sei R ein Hauptidealbereich, K sein Quotientenkörper, R sei ganz abgeschlossen, L eine endliche separable Körpererweiterung von K , S der ganze Abschluss von R in L .

Dann ist S ein noetherscher Ring und ein freier R -Modul vom Rang $[L : K]$.

BEWEIS Wir wissen: S ist endlich erzeugter R -Modul. Daher ist

$$S \simeq R/(m_1) \oplus \dots \oplus R/(m_r)$$

für $m_1 | \dots | m_r$.

Sei $x_j \in S$ das Element, das dem Koordinatentupel $(0, \dots, 0, 1 + (m_j), 0, \dots, 0)$ entspricht.

$m_j x_j = 0$ entspricht $(0, \dots, 0, \underbrace{m_j + (m_j)}_{=0}, 0, \dots, 0)$.

Allerdings ist $m_j \in L, x_j \in L$, somit $m_j = 0$ oder $x_j = 0$.

$x_j = 0$ heißt aber

$$1 + (m_j) = 0 \Rightarrow 1 \in (m_j) \Rightarrow (m_j) = R.$$

Somit:

$$S \simeq \underbrace{R/R \oplus \dots \oplus R/R}_{\text{weglassen}} \oplus R/\{0\} \oplus \dots \oplus R/\{0\} \simeq R \oplus \dots \oplus R,$$

also ist S ein freier R -Modul.

(Eigentlich wurde gezeigt: Torsionsfreie R -Moduln über HIB sind frei.)

Muss noch den Rang finden.

1.3 Ordnung in algebraischen Zahlkörpern

Sei $\omega_1, \dots, \omega_n$ eine K -Basis von L , die in S liegt. Da $\omega_1, \dots, \omega_n \in S$ und über K linear unabhängig, sind sie auch über R linear unabhängig („habe ja nur Koeffizienten eingeschränkt“), d.h.

$$\text{rank}_R(S) \geq n.$$

Eine R -Basis von S ist über R linear unabhängig und daher auch über K linear unabhängig (multipliziere K -Linearkombination mit gemeinsamem Nenner), somit

$$\text{rank}_R(S) \leq \dim_K(L) = n = [L : K]. \quad \blacksquare$$

1.3 Ordnung in algebraischen Zahlkörpern

Definition Ein algebraischer Zahlkörper K ist eine endliche Körpererweiterung von \mathbb{Q} . Die in K über \mathbb{Z} ganzen Elemente heißen ganzalgebraische Zahlen in K ,

$$\mathfrak{o}_K := \{\beta \in K \mid \beta \text{ ganzalgebraisch}\}$$

heißt Ganzheitsring (oder Hauptordnung oder Maximalordnung) von K .

Korollar (aus Satz 1.6) Sei K ein algebraischer Zahlkörper, dann ist \mathfrak{o}_K ein noetherscher Ring und ein freier \mathbb{Z} -Modul vom Rang $[K : \mathbb{Q}]$.

BEWEIS \mathbb{Z} ist Hauptidealbereich. ■

Definition Eine \mathbb{Z} -Basis von \mathfrak{o}_K heißt Ganzheitsbasis von K .

Definition Sei K ein Zahlkörper vom Grad n (d.h. $[K : \mathbb{Q}] = n$).

Ein freier \mathbb{Z} -Modul $\leq K$ vom Rang n heißt vollständiges Gitter.

Eine Ordnung von K ist ein Unterring von K , der ein vollständiges Gitter ist.

Beispiel In $K = \mathbb{Q}(\sqrt{-1})$ ist $\langle 1, i \rangle_{\mathbb{Z}}$ ein vollständiges Gitter. Außerdem ist es ein Ring, also eine Ordnung von K .

Beispiel $K = \mathbb{Q}(\sqrt{-3})$.

$\mathbb{Z}[\sqrt{-3}] = \langle 1, \sqrt{-3} \rangle_{\mathbb{Z}}$ ist eine Ordnung.

$\omega := \frac{1+\sqrt{-3}}{2}$ ist ganz über \mathbb{Z} .

$\mathfrak{o} := \langle 1, \omega \rangle_{\mathbb{Z}} = \mathbb{Z}[\omega]$ ist auch eine Ordnung.

Es gilt

$$\mathbb{Z}[\sqrt{-3}] \subseteq \mathfrak{o}.$$

Bemerkung \mathfrak{o}_K ist eine Ordnung von K .

Proposition Sei \mathfrak{o} eine Ordnung eines Zahlkörpers K . Dann ist $\mathfrak{o} \subseteq \mathfrak{o}_K$; d.h. die Maximalordnung ist das größte Element der Menge der Ordnungen bezüglich Inklusion.

BEWEIS Sei $\alpha \in \mathfrak{o}$. Betrachte

$$\alpha \cdot \mathfrak{o} \subseteq \mathfrak{o}.$$

Da \mathfrak{o} ein Gitter ist, ist α ganzalgebraisch lt. Lemma über Charakterisierung ganzalgebraischer Elemente. Also

$$\alpha \in \mathfrak{o}_K \Rightarrow \mathfrak{o} \subseteq \mathfrak{o}_K. \quad \blacksquare$$

1 Ganzalgebraische Zahlen

Bemerkung Sei α ganzalgebraisch über \mathbb{Q} , $K = \mathbb{Q}(\alpha)$, $n = [K : \mathbb{Q}]$.

$\mathbb{Z}[\alpha] = \langle 1, \alpha, \dots, \alpha^{n-1} \rangle_{\mathbb{Z}}$ ist eine Ordnung von K . („Gleichungsordnung“ von f , wobei f das Minimalpolynom von α ist.)

Definition (Dedekindsche Ordnung) Sei K ein algebraischer Zahlkörper, M ein vollständiges Gitter in K .

$$\mathfrak{o}(M) := \{\alpha \in K \mid \alpha M \subseteq M\}$$

heißt (Dedekindsche) Ordnung von M („die, die dieses Gitter ausnutzen“).

Proposition Sei K ein algebraischer Zahlkörper.

1. Sei M ein vollständiges Gitter. Dann ist $\mathfrak{o}(M)$ eine Ordnung von K .
2. Sei \mathfrak{o} eine Ordnung von K . Dann gibt es ein vollständiges Gitter M von K mit $\mathfrak{o} = \mathfrak{o}(M)$. (Man kann $M = \mathfrak{o}$ wählen.)

BEWEIS 1. Seien $\alpha, \beta \in \mathfrak{o}(M)$. Dann ist

$$\begin{aligned}\alpha M &\subseteq M \\ \beta M &\subseteq M,\end{aligned}$$

somit $(\alpha - \beta)M \subseteq M$ und $(\alpha \cdot \beta)M \subseteq M$, also ist \mathfrak{o} ein Ring.

\mathfrak{o} ist abelsche Gruppe, also \mathbb{Z} -Modul und Untermodul von \mathfrak{o}_K , also frei abelsch.

Sei $\omega_1, \dots, \omega_n$ eine \mathbb{Z} -Basis von M und $\beta \in K$.

$$\beta \cdot \omega_k = \sum a_{jk} \omega_j \quad \text{für } a_{jk} \in \mathbb{Q},$$

weil $\omega_1, \dots, \omega_n$ eine \mathbb{Q} -Basis von K ist. Sei d der gemeinsame Nenner der n Zahlen a_{jk} . D.h.

$$d\beta\omega_k = \sum \underbrace{(da_{jk})}_{\in \mathbb{Z}} \omega_j.$$

Also

$$\begin{aligned}(d\beta)\omega_k &\in M \\ \Rightarrow (d\beta)M &\subseteq M. \\ \Rightarrow d\beta &\in \mathfrak{o}(M).\end{aligned}$$

Somit haben wir

$$\forall \beta \in K \exists d \in \mathbb{Z} : d\beta \in \mathfrak{o}(M)$$

und somit

$$\text{rank}_{\mathbb{Z}} \mathfrak{o}(M) = n$$

gezeigt.

2. \mathfrak{o} eine Ordnung.

$$\mathfrak{o}' = \mathfrak{o}(\mathfrak{o}) = \{\beta \in K \mid \beta\mathfrak{o} \subseteq \mathfrak{o}\}.$$

Da $1 \in \mathfrak{o}$, folgt

$$\forall \beta \in \mathfrak{o}' : \beta = \beta \cdot 1 \in \mathfrak{o},$$

also

$$\mathfrak{o}' \subseteq \mathfrak{o}.$$

Sei jetzt $\beta \in \mathfrak{o}$. Da \mathfrak{o} ein Ring ist, gilt

$$\beta\mathfrak{o} \subseteq \mathfrak{o},$$

also $\beta \in \mathfrak{o}'$, somit

$$\mathfrak{o} \subseteq \mathfrak{o}'. \quad \blacksquare$$

Proposition (Basiswechsel, Index) Sei K ein algebraischer Zahlkörper, \mathfrak{o} eine Ordnung von K .

1. Je zwei \mathbb{Z} -Basen von \mathfrak{o} haben dieselbe Diskriminante. Diese wird als Diskriminante der Ordnung bezeichnet („kanonische Begriffsbildung“).
2. Falls \mathfrak{o}' eine weitere Ordnung ist und $\mathfrak{o}' \leq \mathfrak{o}$ („Unterordnung“), gilt

$$[\mathfrak{o} : \mathfrak{o}'] = \frac{\text{discr}(\mathfrak{o}')}{\text{discr}(\mathfrak{o})}.$$

BEWEIS 1. Seien $\omega_1, \dots, \omega_n$ und $\theta_1, \dots, \theta_n$ zwei \mathbb{Z} -Basen von \mathfrak{o} .

$$\omega_j = \sum_{i=1}^n a_{ij} \omega_i$$

für passende $a_{ij} \in \mathbb{Z}$,

$$A = (a_{ij})_{ij}.$$

A^{-1} beschreibt Übergang von θ s auf ω s, $A^{-1} \in \mathbb{Z}^{n \times n}$.

$$1 = \det(A \cdot A^{-1}) = \underbrace{\det(A)}_{\in \mathbb{Z}} \cdot \underbrace{\det(A^{-1})}_{\in \mathbb{Z}},$$

also $\det A \in \mathcal{E}(\mathbb{Z})$, also $\det(A) = \pm 1$ (d.h. A ist unimodular).

$$\text{discr}(\theta_1, \dots, \theta_n) = \underbrace{\det(A)^2}_{=1} \text{discr}(\omega_1, \dots, \omega_n).$$

2. $\mathfrak{o}' \subseteq \mathfrak{o}$ beides freie \mathbb{Z} -Moduln vom Rang n . Aus dem Struktursatz folgt: Es existieren Basen $\omega_1, \dots, \omega_n$ von \mathfrak{o} sowie $m_1\omega_1, \dots, m_n\omega_n$ von \mathfrak{o}' für ganze Zahlen $m_1 \mid m_2 \mid \dots \mid m_n$.

$$\begin{aligned} \text{discr}(\mathfrak{o}') &= \text{discr}(m_1\omega_1, \dots, m_n\omega_n) = (m_1 m_2 \cdots m_n)^2 \cdot \text{discr}(\omega_1, \dots, \omega_n) \\ &= (m_1 \cdots m_n)^2 \text{discr}(\mathfrak{o}). \end{aligned}$$

1 Ganzalgebraische Zahlen

Da beide Diskriminanten $\neq 0$, folgt

$$0 \neq \frac{\text{discr}(\mathfrak{o}')}{\text{discr}(\mathfrak{o})} = (m_1 \cdots m_n)^2,$$

also alle $m_j \neq 0$.

$$\mathfrak{o}/\mathfrak{o}' \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_n\mathbb{Z},$$

also

$$[\mathfrak{o} : \mathfrak{o}'] = |\mathfrak{o}/\mathfrak{o}'| = m_1 \cdots m_n. \quad \blacksquare$$

Korollar Jede Ordnung von K ist eine Teilordnung von \mathfrak{o}_K von endlichem Index.

Definition Die Diskriminante eines algebraischen Zahlkörpers K ist die Diskriminante von \mathfrak{o}_K .

Bemerkung \mathfrak{o} Ordnung. Dann ist $\text{discr}(\mathfrak{o}) \in \mathbb{Z}$.

BEWEIS $\text{discr}(\mathfrak{o}) \in \mathbb{Q}$, und alle auftretenden Elemente sind ganzalgebraisch. ■

Beispiel $K = \mathbb{Q}(\sqrt{-1})$. Frage: Ist $\mathfrak{o} = \mathbb{Z}[i]$ die Maximalordnung?

$$\text{discr}(\mathfrak{o}) = \text{discr}(i) = \begin{vmatrix} 1 & 1 \\ i & -i \end{vmatrix}^2 = (-2i)^2 = -4.$$

$\mathfrak{o} \subseteq \mathfrak{o}_K$.

$$\frac{\text{discr}(\mathfrak{o})}{\text{discr}(\mathfrak{o}_K)} = \frac{-4}{\text{discr}(\mathfrak{o}_K)} = [\mathfrak{o}_K : \mathfrak{o}]^2 \in \{k^2 \mid k \in \mathbb{N}\}.$$

Somit

$$\text{discr}(\mathfrak{o}_K) \in \{-1, -4\}.$$

Nehmen wir an, dass $\text{discr}(\mathfrak{o}_K) = -1$. D.h. es gibt ein $\beta \in \mathfrak{o}_K$ mit $\beta \notin \mathbb{Z}[i] = \mathfrak{o}$, aber $2\beta \in \mathbb{Z}[i]$ (Fermat in $\mathfrak{o}_K/\mathfrak{o}$).

$$\beta = \frac{a}{2} + \frac{b}{2}i \quad \text{für passende } a, b \in \mathbb{Z}.$$

Es reicht, $a, b \in \{0, 1\}$ zu untersuchen. Störenfriede könnten sein: $\frac{1}{2}, \frac{i}{2}, \frac{1+i}{2}$.

$\frac{1}{2} \notin \mathfrak{o}_K$, weil \mathbb{Z} ganz abgeschlossen ist ($2X - 1$).

$\frac{i}{2}: (X - \frac{i}{2})(X + \frac{i}{2}) = X^2 + \frac{1}{4} \notin \mathbb{Z}[X]$.

$\frac{1+i}{2}: (X - \frac{1+i}{2})(X - \frac{1-i}{2}) = X^2 - X + \frac{1}{4} = X^2 - X + \frac{1}{2} \notin \mathbb{Z}[X]$.

Widerspruch, also $\mathfrak{o}_K = \mathbb{Z}[i]$, $\text{discr}(K) = -4$.

1.4 Transzendenz von e und π

Lemma Sei $f \in \mathbb{C}[X]$ ein Polynom vom Grad m , $t \in \mathbb{C}$ und

$$I(t) = \int_0^t e^{t-u} f(u) \, du.$$

Weiters sei

$$|f| = \sum_{j=0}^m |a_j| X^j, \quad \text{wobei} \quad \sum_{j=0}^m a_j X^j = f(X).$$

Dann gilt:

1. $I(t) = -\sum_{j=0}^m f^{(j)}(t) + e^t \sum_{j=0}^m f^{(j)}(0) + 0$
2. $|I(t)| \leq |t| e^{|t|} |f|(|t|)$.

BEWEIS 1.

$$\begin{aligned} I(t) &= \int_0^t e^{t-u} f(u) \, du = -e^{t-u} f(u) \Big|_0^t + \int_0^t e^{t-u} f'(u) \, du \\ &= -f(t) + e^t f(0) + \int_0^t e^{t-u} f'(u) \, du \\ &= -\sum_{j=0}^m f^{(j)}(t) + e^t \sum_{j=0}^m f^{(j)}(0) + 0. \end{aligned}$$

2. Dreiecksungleichung: Integrationsweg \cdot max(Integrand). ■

Satz 1.7 $e = \lim_{n \rightarrow \infty} (1 + \frac{1}{n})^n$ ist transzendent.

BEWEIS Wir nehmen an, dass

$$\sum_{j=0}^n a_j e^j = 0 \quad \text{für } a_j \in \mathbb{Z}, a_0 \neq 0 \text{ (} a_n \text{ beliebig).}$$

Sei p eine (große) Primzahl.

$$\begin{aligned} f(x) &= X^{p-1} (X-1)^p \cdots (X-n)^p, \\ J &= \sum_{j=0}^n a_j I(j) \quad I(t) \text{ aus Lemma.} \end{aligned}$$

$$|J| \leq \left(\sum |a_j| \right) \cdot n \cdot e^n ((2n)^{n+1})^p.$$

(n, a_j sind fest; p wird noch wachsen.)

1 Ganzalgebraische Zahlen

???

$$\begin{aligned}
 J &= \sum_{j=0}^n a_j \left(- \sum_{k=0}^m f^{(k)}(j) + e^j \sum_{k=0}^m f^{(k)}(0) \right) \\
 &= - \sum_{0 \leq j \leq n, 0 \leq k \leq m} a_j f^{(k)}(j) + \sum_{k=0}^m f^{(k)}(0) \left(\underbrace{\sum_{j=0}^n a_j e^j}_{=0} \right)
 \end{aligned}$$

$f^{(k)}(j) = 0$ für $1 \leq j \leq n$ und $k < p$. (Es überlebt jedenfalls $(X - j)^{p-k}$. Setze $X = j$, dann $f^{(k)}(j) = 0$.)

$p! \mid f^{(k)}(j)$ für $1 \leq j \leq n$ und $k > p$. (Summanden nur $\neq 0$, falls $(X - j)$ vollständig abdiffenziert, d.h. $(p(p-1) \cdots 1)1$).

$f^{(k)}(0) = 0$ für $k < p - 1$

$f^{(p-1)}(0) = (p-1)! \underbrace{(-1)^p \cdots (-n)^p}_{p \text{ teilt das nicht}}$ für $p > n$.

$p! \mid f^{(k)}(0)$ Für Beitrag $\neq 0$ muss X^{p-1} vollständig abdiffenziert sein (\rightarrow Faktor $(p-1)!$) und irgendwo sonst muss auch noch differenziert werden (\rightarrow Faktor p), weiter beliebig diff. Faktor $p!$ gesammelt.

Also insgesamt: $(p-1)! \mid J$, aber p teilt alle bis auf einen Summanden. Somit

$$p \nmid J \Rightarrow J \neq 0 \Rightarrow |J| \geq (p-1)!$$

Somit $(p-1)! \leq \text{const} \cdot \text{const}^p$, Widerspruch. ■

Satz 1.8 $\pi = 2 \arccos(0)$ ist transzendent.

BEWEIS Angenommen π ist algebraisch. Dann ist auch $\vartheta = i\pi$ algebraisch. ϑ sei Nullstelle eines irred. ganzzahligen Polynoms vom Grad d und mit Leitkoeffizient l . D.h. $l\vartheta$ ist ganzzahlig algebraisch.

$\vartheta = \vartheta^{(1)}, \dots, \vartheta^{(d)}$ seien die absolut Konjugierten von ϑ .

$$0 = \prod_{j=1}^d (1 + e^{\vartheta^{(j)}})$$

offensichtlich da $e^{\vartheta^{(1)}} = e^{i\pi} = -1$.

$$= \sum_{(\varepsilon_1, \dots, \varepsilon_d) \in \{0,1\}^d} e^{\sum_{j=1}^d \varepsilon_j \vartheta^{(j)}}$$

Die Exponenten

$$\sum_{j=1}^d \varepsilon_j \vartheta^{(j)} \neq 0$$

nenne $\alpha_1, \dots, \alpha_n$.

$$0 = \sum_{j=1}^n e^{\alpha_j} + q,$$

wobei q die Anzahl der $\sum \varepsilon_j \vartheta^{(j)} = 0$, $q \in \mathbb{N}_0$, ist.

Jede symmetrische Funktion in $\alpha_1, \dots, \alpha_n$ ist symmetrische Funktion in allen verrückten Exponenten. Die gesamte Exponentenkollektion ist symmetrisch in $\vartheta^{(j)}$.

\Rightarrow jede symmetrische Funktion in $l\alpha_1, \dots, l\alpha_n$ kann durch elementarsymmetrische Funktionen in $l\vartheta^{(1)}, \dots, l\vartheta^{(n)}$ dargestellt werden, ist also ganzrational.

Setze

$$f(X) = l^{2m} X^{p-1} (X - \alpha_1)^p \cdots (X - \alpha_n)^p.$$

deg $f = m = np + p - 1$, p große Primzahl.

$$J = \sum_{j=1}^n I(\alpha_j).$$

Somit

$$|J| \leq c_1 \cdot c_2^p \quad \text{für passende Konstanten } c_1, c_2.$$

Ausrechnen ergibt

$$\begin{aligned} J &= - \sum_{j=1}^n \sum_{k=0}^m f^{(k)}(\alpha_j) + \sum_{j=1}^n \sum_{k=0}^m e^{\alpha_j} f^{(k)}(0) \\ &= - \sum_{1 \leq j \leq n, 0 \leq k \leq m} f^{(k)}(\alpha_j) + \sum_{k=0}^m f^{(k)}(0) \underbrace{\left(\sum_{j=1}^n e^{\alpha_j} \right)}_{=-q} \\ &= - \left(\sum_{1 \leq j \leq n, 0 \leq k \leq m} f^{(k)}(\alpha_j) + q \sum_{k=0}^m f^{(k)}(0) \right). \end{aligned}$$

$$g(lX) = f(X) = l^m (lX)^{p-1} (lX - \underbrace{l\alpha_1}_{\text{ganzalgebr.}} \cdots (lX - l\alpha_n)^p.$$

$$f^{(j)}(X) = l^j g^{(j)}(lX).$$

$$g(y) = l^m Y^{p-1} (Y - l\alpha_1)^p \cdots (Y - l\alpha_n)^p$$

ist Polynom mit ganzalg. Koeffizienten, symmetrisch in $l\alpha_1, \dots, l\alpha_n$. $g \in \mathbb{Z}[X]$.

Somit

$$\sum f^{(k)}(\alpha_j) = \sum f^{(k)} g(l\alpha_j) \in \mathbb{Z} \quad \blacksquare$$

(gleiches Argument). Gleiches Argument wie früher: Bis auf $f^{(p-1)}(0)$ alle Summanden durch $p!$ teilbar. ...

1 Ganzalgebraische Zahlen

2 Struktur der Idealhalbgruppe

R ein Ring, $M, N \subseteq R$ (meistens sogar Ideale). Dann ist

$$M + N := \{m + n \mid m \in M, n \in N\},$$
$$M \cdot N := \{m_1 n_1 + \cdots + m_r n_r \mid r \in \mathbb{N}_0, m_j \in M, n_j \in N\}.$$

Es gelten:

- Assoziativgesetz bzgl. $+$, \cdot
- Distributivgesetz $M \cdot (N + Q) = M \cdot N + M \cdot Q$ falls $0 \in N, Q$
- Neutrales Element bzgl. $+$: $\{0\}$
- Neutrales Element bzgl. \cdot : $M \cdot R = M$ falls $M \trianglelefteq R$.

Falls $M, N \trianglelefteq R$, so auch $M + N$ und $M \cdot N$.

Mit M^{-1} bezeichne $\{m^{-1} \mid m \in M\}$, falls R ein Körper und $0 \notin M$.

2.1 Lokalisierung

Definition Sei R ein Ring. R heißt lokaler Ring, wenn R ein eindeutiges maximales Ideal enthält.

Proposition Sei R ein Ring. Dann ist R genau dann ein lokaler Ring, wenn $R \setminus \mathcal{E}(R)$ ein Ideal ist. In diesem Fall ist $R \setminus \mathcal{E}(R)$ das eindeutige maximale Ideal.

BEWEIS „ \implies “: Sei M das eindeutige maximale Ideal. Sei $x \notin M$. Falls $x \notin \mathcal{E}(R)$, so ist $(x) \neq R$, daher ist (x) in einem maximalen Ideal enthalten. Somit ist $(x) \subseteq M$ und $x \in M$, Widerspruch. Daher ist $x \in \mathcal{E}(R)$.

Umgekehrt ist jedes $x \in \mathcal{E}(R)$ kein Element von M . Somit

$$R \setminus M = \mathcal{E}(R)$$

bzw.

$$M = R \setminus \mathcal{E}(R).$$

„ \impliedby “: Falls $M = R \setminus \mathcal{E}(R)$ ein Ideal ist, so ist es ein maximales Ideal. (Es könnten nur mehr Einheiten hinzugefügt werden und somit der ganze Ring erreicht werden.) Jedes $I \trianglelefteq R$ mit $I \neq R$ ist in $M = R \setminus \mathcal{E}(R)$ enthalten, somit ist M einziges maximales Ideal. ■

2 Struktur der Idealhalbgruppe

Definition Sei R ein Ring, $D \subseteq R$. D heißt multiplikativ abgeschlossen, falls

$$\forall d_1, d_2 \in D : d_1 \cdot d_2 \in D$$

und

$$0 \notin D, 1 \in D.$$

Proposition Sei R ein Ring, L ein Körper, $R \leq L$, $D \subseteq R$ eine multiplikativ abgeschlossene Menge. Dann gilt („löse mich ein bisschen vom Ring, erlaube also mehr im Nenner und gehe Richtung Quotientenkörper“)

1. $D^{-1}R = \{\frac{r}{d} \mid r \in R, d \in D\}$ ist ein Ring, der R enthält.
2. Sei ein R -Modul, $M \leq L$. Dann ist

$$D^{-1}M = \{\frac{m}{d} \mid m \in M, d \in D\}$$

ein $D^{-1}R$ -Modul, der M enthält. Falls M ein endlich erzeugter R -Modul ist, so ist $D^{-1}M$ ein endlich erzeugter $D^{-1}R$ -Modul.

3. Sei $I \trianglelefteq R$. Dann ist $D^{-1}I \trianglelefteq D^{-1}R$.
4. Sei $J \trianglelefteq D^{-1}R$. Dann ist $J \cap R \trianglelefteq R$ und es gilt

$$J = D^{-1}(J \cap R).$$

5. Sei $I \trianglelefteq R$. Dann gilt

$$D^{-1}R = R \Leftrightarrow I \cap D \neq \emptyset.$$

BEWEIS 1. Seien $r_1, r_2 \in R, d_1, d_2 \in D$. Dann ist

$$\frac{r_1}{d_1} \pm \frac{r_2}{d_2} = \frac{\overbrace{d_2 r_1 \pm d_1 r_2}^{\in R}}{\underbrace{d_1 d_2}_{\in D}} \quad (2.1)$$

$$\frac{r_1}{d_1} \cdot \frac{r_2}{d_2} = \frac{r_1 r_2}{d_1 d_2}, \quad (2.2)$$

d.h. $\{\frac{r}{d} \mid r \in R, d \in D\}$ ist ein Ring, der in $D^{-1}R$ enthalten ist.

Umgekehrt ist $D^{-1}R \subseteq \{\frac{r}{d} \mid r \in R, d \in D\}$ wegen (2.1).

$r \in R$ kann als $\frac{rd}{d}$ geschrieben werden, also $r \in D^{-1}R$.

2. Beweis von 1 abschreiben:

$$d_2 m_1 \pm d_1 m_2 \in M$$

$$\frac{r}{d_1} \cdot \frac{m}{d_2} = \frac{\overbrace{r m}^{\in M}}{\underbrace{d_1 d_2}_{\in D}}$$

Sei $M = \langle \omega_1, \dots, \omega_n \rangle_R$ und $x \in D^{-1}M$. Dann $x = \frac{m}{d}$ mit $m \in M, d \in D$.

$$m = \sum a_j \omega_j$$

$$x = \frac{m}{d} = \sum \underbrace{\frac{a_j}{d}}_{\in D^{-1}R} \omega_j \Rightarrow D^{-1}M = \langle \omega_1, \dots, \omega_n \rangle_{D^{-1}R}.$$

3. I ist ein R -Modul. Wende 2 an.

4. Sei $J \trianglelefteq D^{-1}R$. Da J und R abelsche Gruppen bzgl. $+$ sind, ist auch $J \cap R$ eine abelsche Gruppe.

Sei $x \in J \cap R, r \in R$. Dann ist

$$rx \in R$$

$$\text{und } \underbrace{r}_{\in D^{-1}R} \cdot \underbrace{x}_{\in J} \in J,$$

somit $J \cap R \trianglelefteq R$.

Zur Gleichung:

$$D^{-1}(J \cap R) \subseteq D^{-1}J \subseteq (D^{-1}R)J \subseteq J,$$

weil J ein $D^{-1}R$ -Ideal.

Sei Umgekehrt $x \in J$. Dann hat x die Gestalt $x = \frac{r}{d}$ für $r \in R, d \in D$. Dann ist

$$\underbrace{d}_{\in D \subseteq R \subseteq D^{-1}R} \cdot \underbrace{x}_{\in J} = r \in J,$$

somit $r \in J$ und damit

$$x \in D^{-1}(R \cap J).$$

5. $D^{-1}I = D^{-1}R \Leftrightarrow 1 \in D^{-1}I \Leftrightarrow 1 = \frac{r}{d}$ für $r \in I, d \in D$, also $r = d$, also $I \cap D \neq \emptyset$. ■

Proposition Sei R ein Ring, der im Körper L enthalten ist, und \mathfrak{p} ein Primideal von R . Dann ist $R \setminus \mathfrak{p}$ multiplikativ abgeschlossen. Der Ring

$$R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}R$$

ist ein lokaler Ring; sein maximales Ideal ist

$$\mathfrak{m}_{\mathfrak{p}} = \left\{ \frac{p}{d} \mid p \in \mathfrak{p} \text{ und } d \in R \setminus \mathfrak{p} \right\}.$$

Es gilt $\mathfrak{m}_{\mathfrak{p}} \cap R = \mathfrak{p}$.

Definition Mit den Bezeichnungen der Proposition heißt $R_{\mathfrak{p}}$ die Lokalisierung von R nach \mathfrak{p} .

2 Struktur der Idealhalbgruppe

BEWEIS (BEWEIS DER PROPOSITION) Seien $a, b \in R \setminus \mathfrak{p}$. Dann gilt $a \cdot b \in R \setminus \mathfrak{p}$, weil sonst $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgen würde (\mathfrak{p} ist ein Primideal).

Suche Einheiten von $R_{\mathfrak{p}}$.

$$\frac{r_1}{d_1} \cdot \frac{r_2}{d_2} = 1 \Rightarrow r_1 r_2 = d_1 d_2 \quad \text{mit } r_1, r_2 \in R, d_1, d_2 \in D := R \setminus \mathfrak{p}.$$

Da $d_1 \cdot d_2 \notin \mathfrak{p}$, folgt $r_1 \notin \mathfrak{p}$ und $r_2 \notin \mathfrak{p}$. Jede Einheit ist also Quotient zweier Elemente aus D .

Falls umgekehrt $d_1, d_2 \in D$, so ist

$$\underbrace{\frac{d_1}{d_2}}_{\in R_{\mathfrak{p}}} \cdot \underbrace{\frac{d_2}{d_1}}_{\in R_{\mathfrak{p}}},$$

also $\frac{d_1}{d_2} \in \mathcal{E}(R_{\mathfrak{p}})$. Daher

$$\mathcal{E}(R_{\mathfrak{p}}) = \left\{ \frac{d_1}{d_2} \mid d_1 \in D, d_2 \in D \right\}$$

und somit

$$R_{\mathfrak{p}} \setminus \mathcal{E}(R_{\mathfrak{p}}) = \left\{ \frac{p}{d} \mid p \in \mathfrak{p}, d \in D \right\}.$$

(„Check“: $\frac{d_1}{d_2} = \frac{p}{d} \Rightarrow \underbrace{d_1 d}_{{\notin \mathfrak{p}}} = p d_2 \in \mathfrak{p}$.)

$D^{-1}\mathfrak{p}$ ist lt. obiger Proposition 3 ein Ideal. Mit der Proposition über lokale Ringe folgt $R_{\mathfrak{p}}$ ist ein lokaler Ring, $\mathfrak{m}_{\mathfrak{p}} = D^{-1}\mathfrak{p}$ ist das eindeutige maximale Ideal.

$\mathfrak{p} \subseteq \mathfrak{m}_{\mathfrak{p}} = D^{-1}\mathfrak{p}$ und $\mathfrak{p} \subseteq R$ lt. Angabe, somit $\mathfrak{p} \subseteq \mathfrak{m}_{\mathfrak{p}} \cap R$.

Sei umgekehrt $\frac{p}{d} \in \mathfrak{m}_{\mathfrak{p}} \cap R$ mit $p \in \mathfrak{p}, d \in D$. $\frac{p}{d} = r$ für $r \in R$. Somit

$$\underbrace{p}_{\in \mathfrak{p}} = r \cdot \underbrace{d}_{\notin \mathfrak{p}} \stackrel{\mathfrak{p} \text{ Primideal}}{\implies} r \in \mathfrak{p} \Rightarrow \mathfrak{m}_{\mathfrak{p}} \cap R \subseteq \mathfrak{p}. \quad \blacksquare$$

Proposition Seien $R \trianglelefteq S$ Ringe, Unterringe eines Körpers L . D sei eine multiplikativ abgeschlossene Teilmenge von R . Dann gilt

1. Falls S ganz über R ist, dann ist auch $D^{-1}S$ ganz über $D^{-1}R$.
2. Falls R ganz abgeschlossen ist, dann ist auch $D^{-1}R$ ganz abgeschlossen.
3. Falls S der ganze Abschluss von R in L ist, so ist $D^{-1}S$ der ganze Abschluss von $D^{-1}R$ in L .

(„Das heißt: Der Lokalisierungsprozess tut unseren Begriffen ganz, ganz abgeschlossen etc. nichts.“)

BEWEIS 1. Sei $\frac{\beta}{d} \in D^{-1}S$ mit $d \in D, \beta \in S$. Da β ganz über R ist, gibt es einen endlich erzeugten R -Modul $M \neq \{0\}$ mit

$$\beta M \subseteq M.$$

Dann ist $D^{-1}M$ endlich erzeugter $D^{-1}R$ -Modul und

$$\frac{\beta}{d} \cdot (D^{-1}M) \subseteq D^{-1}M.$$

Somit ist $\frac{\beta}{d}$ ganz über $D^{-1}R$.

2. Sei K der Quotientenkörper von R (und damit auch von $D^{-1}R$). Sei $x \in K$, x ganz über $D^{-1}R$. Dann gibt es Gleichung

$$x^n + \frac{a_{n-1}}{d_{n-1}}x^{n-1} + \dots + \frac{a_0}{d_0} = 0$$

mit $a_j \in R, d_j \in D$. Multipliziere mit gemeinsamem Nenner $d \in D$:

$$dx^n + b_{n-1}x^{n-1} + \dots + b_0 = 0,$$

wobei $b_j \in R$. Dann ist dx ganz über R (1. Proposition in Abschnitt 1.2), also (R ganz abgeschlossen)

$$dx = r \in R \Rightarrow x = \frac{r}{d} \in D^{-1}R.$$

3. S ist ganz abgeschlossen in L . Daher ist $D^{-1}S$ ganz abgeschlossen in L (lt. 2).
 $D^{-1}S$ ist ganz über $D^{-1}R$ (lt. 1).

Sei $\beta \in L$, β ganz über $D^{-1}R$. Dann ist β ganz über $D^{-1}S$, also $\beta \in D^{-1}S$. Somit

$$D^{-1}S = \{\beta \in L \mid \beta \text{ ganz über } D^{-1}R\}. \quad \blacksquare$$

2.3 Primidealzerlegung

Definition Sei R ein Ring, K sein Quotientenkörper, $M \subseteq K$. M heißt gebrochenes Ideal, falls

- M ein R -Modul ist und
- $\exists c \in R : c \cdot M \subseteq R, c \neq 0$.

Proposition Sei R ein Ring, dann bildet die Menge der von $\{0\}$ verschiedenen gebrochenen Ideale bzgl. Komplexprodukt ein Monoid mit neutralem Element R .

Falls M in diesem Monoid invertierbar ist, $M \cdot N = R$, so gilt

$$N = \{x \in K \mid xM \subseteq R\} =: \text{Inv}(M).$$

BEWEIS Seien M_1, M_2 gebrochene Ideale $\neq \{0\}$, dann ist $M_1 \cdot M_2$ ein R -Modul, und falls $c_1M_1 \subseteq R$ und $c_2M_2 \subseteq R$ für $c_1, c_2 \in R$, so ist

$$(c_1c_2) \cdot (M_1M_2) \subseteq R.$$

Sei $m_1 \in M_1 \setminus \{0\}$, $m_2 \in M_2 \setminus \{0\}$, dann ist $m_1 \cdot m_2 \in M_1M_2$, und $m_1m_2 \neq 0$, weil alles in Quotientenkörper abläuft.

Assoziativgesetz gilt sowieso.

Sei M ein gebrochenes Ideal $\neq \{0\}$.

$$M = 1 \cdot M \stackrel{1 \in R}{\subseteq} R \cdot M \stackrel{M \text{ ist } R\text{-Modul}}{\subseteq} M,$$

also $M = RM$, somit ist R neutrales Element (eindeutig).

2 Struktur der Idealhalbgruppe

Sei jetzt M invertierbar, $M \cdot N = R$. Sei $x \in N$.

$$xM \subseteq N \cdot M = R,$$

also $x \in \text{Inv}(M)$.

Sei umgekehrt $x \in \text{Inv}(M)$, also $xM \subseteq R$. Multipliziere mit N :

$$x \in xR = x \underbrace{MN}_{=R} \subseteq RN \stackrel{N \text{ ist } R\text{-Modul}}{\subseteq} N,$$

somit

$$\text{Inv}(M) = N. \quad \blacksquare$$

Definition (Dedekind-Ring) Sei R ein Ring. R heißt Dedekind-Ring (Dedekind-Bereich, wenn man nicht mit Generalvoraussetzungen wie wir lebt), falls

- R noethersch ist,
- R ganz abgeschlossen ist,
- jedes Primideal $\neq \{0\}$ von R ein maximales Ideal von R ist.

Bemerkung Sei K ein algebraischer Zahlkörper, \mathfrak{o}_K sein Ganzheitsring. Dann ist \mathfrak{o}_K ein Dedekindring.

(Noethersch lt. Korollar zu Satz 1.6, ganz abgeschlossen, weil es ganzer Abschluss von \mathbb{Z} in K ist. Jedes Primideal $\neq \{0\}$ ist maximal, lt. Proposition in Abschnitt 2.2.)

Bemerkung Sei R ein Dedekind-Ring, M ein gebrochenes Ideal von R . Dann ist M ein endlich erzeugter R -Modul.

($cM \subseteq R$ für passendes $c \in R$, also ist cM ein R -Modul, der in R enthalten ist, also ein Ideal, $cM \trianglelefteq R$. Also ist cM endlich erzeugtes Ideal, also endlich erzeugter R -Modul, und

$$M = \frac{1}{c} \underbrace{(cm)}_{\text{endl. erz. } R\text{-Modul}},$$

also endl. erz. R -Modul.)

Einschub Sei \mathfrak{p} ein Primideal, I, J zwei Ideale mit $I \cdot J \subseteq \mathfrak{p}$. Dann gilt $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$ (in einem Ring).

(Sonst gibt es ein $x \in I \setminus \mathfrak{p}, y \in J \setminus \mathfrak{p}$, damit

$$x \cdot y \in I \cdot J \subseteq \mathfrak{p},$$

also $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$, Widerspruch.)

Einschub $\text{Inv}(M)$ ist gebrochenes Ideal:

($xM \subseteq R, yM \subseteq R$, somit

$$(x + y)M \subseteq xM + yM \subseteq R.$$

$xM \subseteq R, r \in R$, so ist $rxM \subseteq rR \subseteq R$. Also $\text{Inv}(M)$ ist R -Modul. Sei $cM \subseteq R, x \in \text{Inv}(M), m \in M$.

$$\underbrace{cmx}_{\in R} \subseteq cxM \subseteq c \cdot R \subseteq R,$$

also $(cm) \cdot \text{Inv}(M) \subseteq R$.

Satz 2.1 Sei R ein Dedekindring. Dann bilden die von $\{0\}$ verschiedenen gebrochenen Ideale eine Gruppe (bzgl. Komplexprodukt). Jedes Ideal $\{0\} \neq I \trianglelefteq R$ besitzt eine im Wesentlichen eindeutige Darstellung

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

für Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r, r \in \mathbb{N}_0$, d.h. bis auf Permutation der Indizes eindeutig.

Bemerkung Man kann zeigen, dass aus den beiden Aussagen auch folgt, dass R ein Dedekindring ist.

BEWEIS (BEWEIS DES SATZES) 1. Beh.: Für alle Ideale I gibt es ein Produkt von Primidealen $\mathfrak{p}_1, \dots, \mathfrak{p}_r \neq \{0\}$ mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I.$$

Bew.: Sei I ein maximales Gegenbeispiel, d.h. ein maximales Element von

$$\{J \trianglelefteq R \mid \text{es gibt kein Produkt } \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq J\},$$

welches existiert, weil R noethersch ist.

Dann ist I kein Primideal (sonst wäre es kein Gegenbeispiel). Daher gibt es $a, b \in R$ mit $ab \in I$, aber $a \notin I$ und $b \notin I$. Betrachte die Ideale (Klammern bedeuten Ideale)

$$J_1 := (\{a\} \cup I), \quad J_2 := (\{b\} \cup I).$$

Dann gilt

$$I \subsetneq J_1 \quad \text{und} \quad I \subsetneq J_2$$

(weil $a \in J_1 \setminus I, b \in J_2 \setminus I$). Daher gibt es Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \dots, \mathfrak{p}_r$ mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq J_1 \quad \text{und} \quad \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \subseteq J_2.$$

Es gilt $J_1 = Ra + I$ und $J_2 = Rb + I$.

Daher

$$\begin{aligned} \mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r &\subseteq J_1 \cdot J_2 = (Ra + I)(Rb + I) \\ &= R \cdot R \underbrace{ab}_{\in I} + \underbrace{RIb}_{\subseteq I} + \underbrace{RIa}_{\subseteq I} + \underbrace{I \cdot I}_{\subseteq I} \subseteq I, \end{aligned}$$

Widerspruch zur Existenz eines Gegenbeispiels.

2. Beh.: Jedes Primideal $\neq \{0\}$ ist invertierbar.

Bew.: Sei \mathfrak{p} ein Primideal. Es gilt: $R \subseteq \text{Inv}(\mathfrak{p})$ (für alle $r \in R$ gilt $r\mathfrak{p} \subseteq \mathfrak{p} \subseteq R$).

Sei $a \in \mathfrak{p}$. Dann gibt es Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r \neq \{0\}$, sodass

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$$

(laut 1.) Dabei sei r minimal mit dieser Eigenschaft gewählt („lasse die Theorie schauen“). Betrachte $\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$. Lt. Minimalität von r heißt das $\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} \not\subseteq (a)$, also gibt es ein $c \in \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$ mit $c \notin (a)$, also $a \nmid c$. Andererseits gilt

$$c \cdot \mathfrak{p}_r \subseteq (a) = aR \subseteq \mathfrak{p}.$$

2 Struktur der Idealhalbgruppe

Aus $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}$ folgt, dass ein $j \in \{1, \dots, r\}$ mit $\mathfrak{p}_j \subseteq \mathfrak{p}$ existiert. O.B.d.A. war das das $\mathfrak{p}_r \subseteq \mathfrak{p}$. Da jedes Primideal $\neq \{0\}$ maximal ist, folgt $\mathfrak{p}_r = \mathfrak{p}$.

Also

$$c \cdot \mathfrak{p} \subseteq aR,$$

somit

$$\frac{a}{c} \mathfrak{p} \subseteq R,$$

daher

$$\frac{c}{a} \in \text{Inv}(\mathfrak{p}), \quad \text{aber } \frac{c}{a} \notin R.$$

$\implies R \subsetneq \text{Inv}(\mathfrak{p})$.

Somit gilt

$$\underbrace{\mathfrak{p} \cdot 1}_{\text{max. Ideal}} \subseteq \mathfrak{p}R \subseteq \underbrace{\mathfrak{p} \text{Inv}(\mathfrak{p})}_{\text{in } R \text{ enth. gebr. Ideal, also Ideal von } R} \subseteq R.$$

Wegen Maximalität von \mathfrak{p} : $\mathfrak{p} \cdot \text{Inv}(\mathfrak{p}) = R$ (fertig) oder $\mathfrak{p} = \mathfrak{p} \text{Inv}(\mathfrak{p})$.

Annahme: $\mathfrak{p} = \mathfrak{p} \text{Inv}(\mathfrak{p})$.

Sei $x \in \text{Inv}(\mathfrak{p})$. Dann gilt $x \cdot \mathfrak{p} \subseteq \mathfrak{p} \cdot \text{Inv}(\mathfrak{p}) = \mathfrak{p}$. \mathfrak{p} ist Ideal in noetherschem Ring, also endlich erzeugter R -Modul. Daher ist x ganz über R . Da R ganz abgeschlossen ist („endlich 3. Voraussetzung von Dedekind verwendet“), folgt $x \in R$ und damit $\text{Inv}(\mathfrak{p}) \subseteq R$, Widerspruch.

3. Beh.: Jedes Ideal $\neq \{0\}$ ist invertierbar.

Beweis: Sei I ein maximales Gegenbeispiel. Dann ist I kein Primideal und $I \neq R$. Es gibt somit ein Primideal \mathfrak{p} mit $I \subsetneq \mathfrak{p} \subsetneq R$.

Betrachte $J := I \cdot \text{Inv}(\mathfrak{p})$ („multipliziere I mit ziemlich viel“). Es gilt

$$J = I \cdot \text{Inv}(\mathfrak{p}) \subseteq \mathfrak{p} \cdot \text{Inv}(\mathfrak{p}) = R,$$

daher ist $J = I \cdot \text{Inv}(\mathfrak{p}) \trianglelefteq R$. Falls

$$I = I \cdot \text{Inv}(\mathfrak{p}),$$

so folgt wie oben $\text{Inv}(\mathfrak{p}) \subseteq R$, das ist falsch. Daher

$$I \subsetneq I \cdot \text{Inv}(\mathfrak{p}) = J.$$

Da I max. Gegenbsp. ist, besitzt J ein Inverses.

$$I \cdot (\text{Inv}(\mathfrak{p}) \text{Inv}(J)) = J \cdot \text{Inv}(J) = R \Rightarrow I \text{ invertierbar.}$$

4. Beh.: Jedes gebrochene Ideal $\neq \{0\}$ ist invertierbar.

Beweis: Sei M ein gebr. Ideal von R , dann existiert ein $c \in R$ mit $cM \subseteq R$, also $cM \trianglelefteq R$, somit existiert lt. 3. ein gebr. Ideal N mit $(cM) \cdot N = R$, also ist cN invers zu M .

Also bilden die von $\{0\}$ verschiedenen Ideale eine Gruppe.

5. Beh.: Jedes Ideal $\neq \{0\}$ von R ist als Produkt von Primidealen darstellbar.

Beweis: $R = (\text{leeres Produkt})$, wir müssen uns nur um Ideale $I \subsetneq R$ kümmern. Sei I ein maximales Gegenbeispiel („noethersch“ verwendet). Offensichtlich ist I kein Primideal, also ist $I \subsetneq \mathfrak{p}$ für ein max. Ideal \mathfrak{p} . Betrachte

$$\mathfrak{p}^{-1} \cdot I \subseteq R,$$

also ist $\mathfrak{p}^{-1} \cdot I \subseteq R$. Wir wissen, dass

$$R \subseteq \text{Inv}(\mathfrak{p}) = \mathfrak{p}^{-1},$$

also gilt

$$I = R \cdot I \subseteq \mathfrak{p}^{-1}I$$

und $I \neq \mathfrak{p}^{-1}I$ (sonst $\mathfrak{p}^{-1} = R$, Widerspruch; „weil in Gruppe“). Also

$$I \subsetneq \mathfrak{p}^{-1}I \subseteq R.$$

Da I ein maximales Gegenbeispiel ist, gibt es Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ mit

$$\mathfrak{p}^{-1}I = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

somit („noch einmal: wir sind in einer Gruppe“)

$$I = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

Widerspruch.

Seien M, N gebrochene Ideale von R . Schreibe $M \mid N$, wenn es ein Ideal $I \subseteq R$ mit $M \cdot I = N$ gibt („ M teilt N “).

6. Beh.: Seien M, N gebrochene Ideale von R . Dann gilt

$$M \mid N \Leftrightarrow N \subseteq M.$$

Beweis: „ \Rightarrow “: Es gibt ein $I \subseteq R$ mit

$$N = M \cdot I \subseteq M \cdot R \subseteq M.$$

„ \Leftarrow “: Sei $N \subseteq M$. Setze $I := M^{-1}N$ (außer wenn $M = \{0\}$, dann gilt auch $N = \{0\}$ und daher $M \cdot R = N$, fertig). I ist ein gebrochenes Ideal von R . Da $N \subseteq M$, gilt

$$I = M^{-1}N \subseteq M^{-1}N = R,$$

also $I \subseteq R$, somit $M \mid N$.

(„Haben eine Art Teilbarkeitstheorie für Ideale entwickelt (bzw. definiert), indem wir alles auf Teilmengen zurückgespielt haben.“)

7. Beh.: Sei \mathfrak{p} ein Primideal, I, J Ideale. Dann gilt

$$\mathfrak{p} \mid I \cdot J \longrightarrow \mathfrak{p} \mid I \text{ oder } \mathfrak{p} \mid J.$$

Beweis:

$$\mathfrak{p} \mid I \cdot J \stackrel{6.}{\Leftrightarrow} I \cdot J \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p} \text{ oder } J \subseteq \mathfrak{p} \Rightarrow \mathfrak{p} \mid I \text{ oder } \mathfrak{p} \mid J.$$

2 Struktur der Idealhalbgruppe

8. Beh.: Eindeutigkeit der Darstellung als Produkt von Primidealen. („Beweise werden kürzer, es ist also nicht mehr viel zu tun. Wir brauchen nur mehr zudrehen!“)

Beweis: Sei

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

mit $r, s \in \mathbb{N}_0$, $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ Primideale und die beiden Darstellungen gehen nicht durch Permutation auseinander hervor. O.B.d.A. $r \leq s$ und r minimal. Es gilt $s \geq 1$ und

$$\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{q}_s \subsetneq R,$$

somit auch $r \geq 1$. Da $\mathfrak{q}_s \mid \mathfrak{p}_1 \cdots \mathfrak{p}_r$, folgt lt. 7. (und Induktion), dass $\mathfrak{q}_s \mid \mathfrak{p}_j$ für ein $j \in \{1, \dots, r\}$, o.B.d.A. $j = r$. Somit $\mathfrak{p}_j \subseteq \mathfrak{q}_s$. Da beides maximale Ideale sind („verwende wieder Dedekind-Ring“), folgt $\mathfrak{p}_r = \mathfrak{q}_s$. Somit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_{s-1},$$

Widerspruch zur Minimalität von r . ■

Korollar Sei K ein algebraischer Zahlkörper, \mathfrak{o}_K sein Ganzheitsring. Dann bilden die von $\{0\}$ verschiedenen gebrochenen Ideale eine Gruppe, jedes Ideal von \mathfrak{o}_K besitzt eine Darstellung als Produkt von Primidealen und diese ist bis auf Permutation eindeutig.

BEWEIS Folgt sofort aus dem Satz, weil \mathfrak{o}_K ein Dedekind-Bereich ist. ■

Definition Sei K ein algebraischer Zahlkörper. Dann bezeichne die Gruppe der von $\{0\}$ verschiedenen gebrochenen Ideale von \mathfrak{o}_K mit I_K .

Bemerkung Man findet auch die Notation \mathbb{Z}_K für \mathfrak{o}_K . („Die Notation derer, die sich vor Frakturbuchstaben fürchten; normalerweise gehöre ich zu dieser Gruppe.“)

Proposition Sei R ein Dedekind-Ring, M ein gebrochenes Ideal von R . Dann gibt es Primideale

$$\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s,$$

sodass

$$M = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1},$$

wobei $\mathfrak{p}_i \neq \mathfrak{q}_j$ für alle i, j . Die Darstellung ist bis auf Permutation eindeutig.

BEWEIS Es existiert ein $c \in R$ mit $cM \trianglelefteq R$, also

$$cRM = cM = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

(R ist neutrales Element). cR ist ein (Haupt-) Ideal, also

$$cR = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

somit

$$\begin{aligned} \mathfrak{q}_1 \cdots \mathfrak{q}_s M &= \mathfrak{p}_1 \cdots \mathfrak{p}_r \\ M &= \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s}. \end{aligned}$$

Kürze gemeinsame Faktoren und alles andere wie üblich. ■

Definition Sei R ein Dedekind-Ring, M ein gebrochenes Ideal, \mathfrak{p} ein Primideal. $v_{\mathfrak{p}}(M)$ ist jene ganze Zahl, sodass

$$M = \mathfrak{p}^{v_{\mathfrak{p}}(M)} \cdot \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$$

für von \mathfrak{p} verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ und $\alpha_1, \dots, \alpha_r \in \mathbb{Z} \setminus \{0\}$ gilt (Ordnung von \mathfrak{p} in M).

Sei x aus dem Quotientenkörper von R , so setze

$$v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(xR)$$

(xR ist gebrochenes Hauptideal).

Falls $v_{\mathfrak{p}}(x) > 0$, spricht man von einer Nullstelle von x an \mathfrak{p} , falls $v_{\mathfrak{p}}(x) < 0$, spricht man von einem Pol, falls $v_{\mathfrak{p}}(x) = 0$, heißt x eine \mathfrak{p} -Einheit.

Proposition Sei R ein Dedekind-Ring, D eine multiplikativ abgeschlossene Teilmenge von R . Dann ist $D^{-1}R$ ein Dedekind-Ring. („Bei Lokalisierung gehen Dedekind-Ringe in Dedekind-Ringe über.“)

Die Abbildung Φ von der Gruppe der gebrochenen Ideale $\neq \{0\}$ von R mit

$$\Phi(M) := D^{-1}M$$

ist ein Gruppenepimorphismus in die Gruppe der gebrochenen Ideale $\neq \{0\}$ von $D^{-1}R$, der die Ideale von R surjektiv auf die Ideale von $D^{-1}R$ abbildet.

$$\text{Ker } \Phi = \{M \text{ gebr. Ideal} \mid M \cap D \neq \emptyset\}.$$

BEWEIS In Abschnitt 2.1 wurde gezeigt, dass für jedes Ideal $J \trianglelefteq D^{-1}R$

$$J = D^{-1}(J \cap R)$$

(*) gilt.

1. R algebraisch abgeschlossen $\Rightarrow D^{-1}R$ algebraisch abgeschlossen (Ende von 2.1).

2. Beh.: $D^{-1}R$ ist noethersch.

Beweis. Sei $J \trianglelefteq D^{-1}R$. Dann ist $J \cap R \subseteq R$, somit

$$\begin{aligned} J \cap R &= \langle \omega_1, \dots, \omega_r \rangle_R \\ J = D^{-1}(J \cap R) &= \langle \omega_1, \dots, \omega_r \rangle_{D^{-1}R}, \end{aligned}$$

fertig

3. Beh.: Jedes Primideal $\neq \{0\}$ von $D^{-1}R$ ist maximales Ideal von $D^{-1}R$.

Beweis. Sei $\mathfrak{p} \trianglelefteq D^{-1}R$, $\mathfrak{p} \neq \{0\}$, \mathfrak{p} Primideal, und sei $J \trianglelefteq D^{-1}R$ mit $\mathfrak{p} \subseteq J \subsetneq D^{-1}R$. Es gilt

$$\underbrace{\mathfrak{p} \cap R}_{\text{Primideal von } R} \subseteq J \cap R.$$

Da R ein Dedekindring ist, ist $\mathfrak{p} \cap R$ ein maximales Ideal. (Da $1 \notin \mathfrak{p}$, gilt $\mathfrak{p} \cap R \neq R$. Da $\{0\} \neq \mathfrak{p} = D^{-1}(\mathfrak{p} \cap R)$, gilt $\mathfrak{p} \cap R \neq \{0\}$.)

2 Struktur der Idealhalbgruppe

$J \cap R$ ist ein Ideal, also $J \cap R = R$ oder $J \cap R = \mathfrak{p} \cap R$. Im ersten Fall folgt $J = D^{-1}R$ lt. (*), im zweiten Fall ergibt (*) $J = \mathfrak{p}$.

Somit ist $D^{-1}R$ ein Dedekind-Ring.

In 2.1 wurde gezeigt, dass $\Phi(M)$ ein $D^{-1}R$ -Modul ist.

Wenn M ein gebrochenes Ideal ist, so ist $cM \subseteq R$ für ein $c \in R$, also

$$D^{-1}(cM) \subseteq D^{-1}R,$$

also

$$c \cdot D^{-1}M \subseteq D^{-1}R$$

mit $c \in R \subseteq D^{-1}R$. Somit ist $\Phi(M)$ gebrochenes Ideal von $D^{-1}R$.

$$\Phi : (\text{gebr. Ideale von } R \neq \{0\}) \rightarrow (\text{gebr. Ideale von } D^{-1}R \neq \{0\})$$

4. Beh.: Φ ist surjektiv.

Beweis: Sei N ein gebrochenes Ideal von $D^{-1}R$. Dann gibt es ein $c \in D^{-1}R$ mit

$$cN \subseteq D^{-1}R.$$

Sei $c = \frac{a}{d}$ für $a \in R, d \in D$. Dann gilt auch

$$aN = d \cdot cN \subseteq d \cdot D^{-1}R \subseteq D^{-1}R.$$

Daraus folgt

$$aN = D^{-1}(aN \cap R)$$

(lt. (*)), also

$$N = D^{-1} \underbrace{\left(N \cap \frac{1}{a}R \right)}_{\text{gebr. Ideal von } R}.$$

5. Φ ist Homomorphismus:

$$\Phi(M \cdot N) = D^{-1}(M \cdot N) \stackrel{1 \in D}{=} (D^{-1}D^{-1})(M \cdot N) = D^{-1}M \cdot D^{-1}N = \Phi(M) \cdot \Phi(N). \quad \blacksquare$$

...

2.5 Absolutnorm von Idealen

Definition Sei K ein algebraischer Zahlkörper, $\mathfrak{o} = \mathfrak{o}_K$ sein Ganzheitsring und $\{0\} \neq I \trianglelefteq \mathfrak{o}$. Dann definiere die Absolutnorm von I als

$$\vec{N}(I) := |\mathfrak{o}/I| = [\mathfrak{o} : I].$$

Satz 2.3 K algebraischer Zahlkörper, $\mathfrak{o} = \mathfrak{o}_K$ Ganzheitsring. Dann gilt:

$$1. \forall \{0\} \neq I \trianglelefteq \mathfrak{o} : \vec{N}(I \cdot J) = \vec{N}(I) \cdot \vec{N}(J)$$

2. $\forall \alpha \in \mathfrak{o} : \vec{N}(\alpha\mathfrak{o}) = \left| \vec{N}(\alpha) \right|$

3. Sei $\{0\} \neq \mathfrak{p}$ ein Primideal von \mathfrak{o} , das über $p\mathbb{Z}$ liegt. Dann gilt $\vec{N}(\mathfrak{p}) = p$.

BEWEIS 1. Sei $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$.

$$\mathfrak{o}/I = \mathfrak{o}/\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \stackrel{\text{Chin. RS}}{\simeq} \mathfrak{o}/\mathfrak{p}_1^{a_1} \times \cdots \times \mathfrak{o}/\mathfrak{p}_r^{a_r}.$$

$\vec{N}(I) = \vec{N}(\mathfrak{p}_1^{a_1}) \cdots \vec{N}(\mathfrak{p}_r^{a_r})$. Wir wissen (Lemma 4 von Abschnitt 2.4):

$$\mathfrak{p}^k/\mathfrak{p}^{k+1} \simeq \mathfrak{o}/\mathfrak{p},$$

also insbesondere $|\mathfrak{p}^k/\mathfrak{p}^{k+1}| = |\mathfrak{o}/\mathfrak{p}|$.

$$\left| \mathfrak{o}/\mathfrak{p}_j^{a_j-1} \right| = \frac{|\mathfrak{o}/\mathfrak{p}_j^{a_j}|}{|\mathfrak{p}_j^{a_j-1}/\mathfrak{p}_j^{a_j}|} \Rightarrow |\mathfrak{o}/\mathfrak{p}_j^{a_j}| = |\mathfrak{o}/\mathfrak{p}_j^{a_j-1}| \cdot |\mathfrak{o}/\mathfrak{p}_j| = |\mathfrak{o}/\mathfrak{p}_j|^{a_j}.$$

Somit

$$\vec{N}(I) = \prod_{j=1}^r |\mathfrak{o}/\mathfrak{p}_j|^{a_j}.$$

Daraus folgt sofort die Formel $\vec{N}(I \cdot J) = \vec{N}(I) \cdot \vec{N}(J)$.

2. $\mathfrak{o}/\mathfrak{p} = ?$.

$\mathfrak{o}/\mathfrak{p}$ ist KE von $\mathbb{Z}/p\mathbb{Z}$ vom Grad $f(\mathfrak{p}/p\mathbb{Z})$.

$$\Rightarrow \vec{N}(\mathfrak{p}) = |\mathfrak{o}/\mathfrak{p}| = p^{f(\mathfrak{p}/p\mathbb{Z})}.$$

3. Wir müssen $[\mathfrak{o}/\alpha\mathfrak{o}]$ berechnen. Sei $\omega_1, \dots, \omega_n$ eine Ganzheitsbasis von \mathfrak{o} .

$$\alpha\omega_j = \sum a_{ij}\omega_i \quad \text{für passende } a_{ij} \in \mathbb{Z}.$$

Nach Definition gilt $\det((a_{ij})) = \vec{N}(\alpha)$. $\alpha\omega_1, \dots, \alpha\omega_n$ bilden eine \mathbb{Z} -Basis von $\alpha\mathfrak{o}$.

$$\underbrace{[\mathfrak{o} : \alpha\mathfrak{o}]^2}_{\in \mathbb{Z}} \stackrel{\text{letzte Prop. in 1.3}}{=} \frac{\text{discr}(\alpha\omega_1, \dots, \alpha\omega_n)}{\text{discr}(\omega_1, \dots, \omega_n)} = \frac{\det((a_{ij}))^2 \cdot \text{discr}(\omega_1, \dots, \omega_n)}{\text{discr}(\omega_1, \dots, \omega_n)} = \underbrace{\left(\vec{N}(\alpha) \right)^2}_{\in \mathbb{Z}},$$

somit

$$[\mathfrak{o} : \alpha\mathfrak{o}] = \left| \vec{N}(\alpha) \right|. \quad \blacksquare$$

2.6 Faktorisierung von Primzahlen in Zahlkörpern

K algebraischer Zahlkörper, $\mathfrak{o} = \mathfrak{o}_K$ sein Ganzheitsring, $p \in \mathbb{Z}$ eine Primzahl. Wir suchen Faktorisierung $p\mathfrak{o} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. $K = \mathbb{Q}(\alpha)$ für ein passendes $\alpha \in \mathfrak{o}$.

Satz 2.4 *Mit obigen Bezeichnungen nehme an, dass $p \nmid [\mathfrak{o} : \mathbb{Z}[\alpha]]$. Sei f das Minimalpolynom von α und \bar{f} das Bild von f bei Reduktion \pmod{p} . In $\mathbb{F}_p[X]$ habe \bar{f} die Primfaktorzerlegung*

$$\bar{f} = \prod_{j=1}^r \bar{g}_j^{e_j}$$

für passende Polynome $g_j \in \mathbb{Z}[X]$ und $e_j \in \mathbb{N}$. Sei

$$\mathfrak{p}_j := (g_j(\alpha), p) = g_j(\alpha)\mathfrak{o} + p\mathfrak{o}.$$

Dann ist \mathfrak{p}_j ein Primideal und es gilt

$$p\mathfrak{o} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

BEWEISIDEE Konstruiere Isomorphismus

$$\mathfrak{o}/p\mathfrak{o} \simeq \mathbb{F}_p[X]/\bar{f}\mathbb{F}_p[X]$$

und transportiere maximale Ideale hin und her. □

BEWEIS 1. Beh.

$$\mathfrak{o}/p\mathfrak{o} \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \quad \text{via} \quad \beta + p\mathbb{Z}[\alpha] \mapsto \beta + p\mathfrak{o}.$$

Beweis. Kern:

$$(\pi_{p\mathfrak{o}} \circ \text{incl}) = \{\beta \in \mathbb{Z}[\alpha] : \beta \in p\mathfrak{o}\} = \mathbb{Z}[\alpha] \cap p\mathfrak{o}.$$

Sei $k = [\mathfrak{o} : \mathbb{Z}[\alpha]]$. Für alle $\gamma \in \mathfrak{o}$ ist somit $k\gamma \in \mathbb{Z}[\alpha]$ (Fermat). Da $p \nmid k$, gibt es ein k mit $kk \equiv 1 \pmod{p}$.

$$\gamma = \underbrace{k \cdot k \cdot \gamma}_{\in \mathbb{Z}[\alpha]} + l \cdot p^\gamma \quad l \in \mathbb{Z}.$$

Somit

$$\gamma + p\mathfrak{o} = \underbrace{k' \cdot k \cdot \gamma}_{\in \mathbb{Z}[\alpha]} + p\mathfrak{o}.$$

Daher ist $\pi_{p\mathfrak{o}}$ surjektiv. Lt. 1. Isomorphiesatz folgt

$$\mathbb{Z}[\alpha]/(\mathbb{Z}[\alpha] \cap p\mathfrak{o}) \simeq \mathfrak{o}/p\mathfrak{o}.$$

Es gilt $p\mathbb{Z}[\alpha] \subseteq (\mathbb{Z}[\alpha] \cap p\mathfrak{o})$.

$$[\mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]] = p^n \quad (n = [K : \mathbb{Q}]).$$

($p\omega_1, \dots, p\omega_n$ sind \mathbb{Z} -Basis von $p\mathbb{Z}[\alpha]$, wenn $\omega_1, \dots, \omega_n$ \mathbb{Z} -Basis von \mathfrak{o} .)

$$[\mathbb{Z}[\alpha] : (\mathbb{Z}[\alpha] \cap p\mathfrak{o})] = [\mathfrak{o} : p\mathfrak{o}] = \vec{N}(p\mathfrak{o}) \stackrel{\text{Satz 2.3 (3)}}{=} |N_{K/\mathbb{Q}}(p)| \stackrel{\text{Kap. 1}}{=} p^n.$$

2.6 Faktorisierung von Primzahlen in Zahlkörpern

Also

$$p^n = [\mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]] = \underbrace{[\mathbb{Z}[\alpha] : (\mathbb{Z}[\alpha] \cap p\mathfrak{o})]}_{=p^n} \cdot [\mathbb{Z}[\alpha] \cap p\mathfrak{o} : p\mathbb{Z}[\alpha]].$$

Daraus folgt

$$\begin{aligned} [\mathbb{Z}[\alpha] \cap p\mathfrak{o} : p\mathbb{Z}[\alpha]] &= 1 \\ \Rightarrow \mathbb{Z}[\alpha] \cap p\mathfrak{o} &= p\mathbb{Z}[\alpha]. \end{aligned}$$

2. Beh.

$$\mathbb{Z}[X]/f\mathbb{Z}[X] + p\mathbb{Z}[X] \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha].$$

Beweis. $g \mapsto g(\alpha) + p\mathbb{Z}[\alpha]$. $\pi_{p\mathbb{Z}[\alpha]} \circ \text{ev}_\alpha$ ist als Zusammensetzung von surjektiven Abbildungen surjektiv.

$$\text{Ker} = \{g \in \mathbb{Z}[X] \mid g(\alpha) \in p\mathbb{Z}[\alpha]\}.$$

Schreibe $g = f \cdot q + p \cdot r + t$.

$$\begin{aligned} q &\in \mathbb{Z}[X] \\ r &\in \mathbb{Z}[X] \\ t &\in \mathbb{Z}[X] \\ \deg t &< \deg f = n \end{aligned}$$

Jeder Koeffizient von $t \in \{0, \dots, p-1\}$.

$$g(\alpha) \in p\mathbb{Z}[\alpha] \Leftrightarrow t(\alpha) \in p\mathbb{Z} \Leftrightarrow t = 0.$$

$$g \in \text{Ker} \Leftrightarrow t = 0 \Rightarrow \text{Ker}(\dots) = f \cdot \mathbb{Z}[X] + p\mathbb{Z}[X].$$

3. Beh.

$$\mathbb{Z}[X]/f\mathbb{Z}[X] + p\mathbb{Z}[X] \simeq \mathbb{F}[X]/\bar{f}\mathbb{F}_p[X] \quad \text{via} \quad g + f\mathbb{Z}[X] + p\mathbb{Z}[X] \mapsto \bar{g} + \bar{f}\mathbb{F}_p[X].$$

Beweis. $\pi_{\bar{f}\mathbb{F}_p[X]} \circ \text{mod } p$ ist surjektiv. $g \in \text{Ker} \Leftrightarrow t = \bar{t} \in \bar{f}\mathbb{F}_p[X] \Leftrightarrow t = 0$ (wie bei 2.)

Somit bis jetzt:

$$\bar{g} + \bar{f}\mathbb{F}_p[X] \mapsto g(\alpha) + p\mathfrak{o}. \quad \blacksquare$$

Beispiel $D \in \mathbb{Z}$ quadratfrei, betrachte $\mathbb{Q}(\sqrt{D})$. Dann ist der Ganzheitsring

$$\mathfrak{o} = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \pmod{4} \end{cases},$$

also $[\mathfrak{o} : \mathbb{Z}[\sqrt{D}]] \in \{1, 2\}$.

Sei p eine ungerade Primzahl. Erhalte Faktorisierung von $p\mathfrak{o}$ durch Faktorisierung von $X^2 - D$ über \mathbb{F}_p .

D ist quadratischer Rest \pmod{p} (als Legendre-Symbol: $\left(\frac{D}{p}\right) = 1$)

$\Leftrightarrow X^2 - D$ hat in \mathbb{F}_p eine Nullstelle.

$\Leftrightarrow (X^2 - D) = (X - d_1)(X + d_2)$ über \mathbb{F}_p .

$\Leftrightarrow p\mathfrak{o} = ((\sqrt{D} - d_1)\mathfrak{o} + p\mathfrak{o})((\sqrt{D} + d_1)\mathfrak{o} + p\mathfrak{o})$

$\Leftrightarrow p\mathbb{Z}$ verzweigt total.

2.7 Endlichkeit der Klassenzahl

Proposition Sei K ein algebraischer Zahlkörper, M ein vollständiges Gitter in K . Dann gibt es ein $m \in \mathbb{N}$, sodass

$$\forall x \in K \exists r \in \{0, \dots, m\} \exists y \in rx + M : |N(y)| < 1.$$

BEWEIS Sei $M = \langle \omega_1, \dots, \omega_n \rangle_{\mathbb{Z}}$. Setze

$$\begin{aligned} g(x_1, \dots, x_n) &:= N(x_1\omega_1 + \dots + x_n\omega_n) \\ &= \det(M_{x_1\omega_1 + \dots + x_n\omega_n}) \\ &= \det(M_{x_1\omega_1} + M_{x_2\omega_2} + \dots + M_{x_n\omega_n}) \\ &= \det \left(x_1 \underbrace{M_{\omega_1}}_{\in \mathbb{Z}^{n \times n}} + \dots + x_n \underbrace{M_{\omega_n}}_{\in \mathbb{Z}^{n \times n}} \right) \\ &= \text{Polynom in } x_1, \dots, x_n, \end{aligned}$$

wobei M_{β} die Matrix ist, die die Multiplikation mit β beschreibt, und $x_1, \dots, x_n \in \mathbb{Q}$.

Setze

$$C := \max_{(x_1, \dots, x_n) \in [0, 1]^n} |g(x_1, \dots, x_n)|.$$

(g ist stetig auf \mathbb{R}^n , Einheitswürfel ist kompakt.)

Wähle ein $k \in \mathbb{N}$ mit $k^n > C$ und setze $m = k^n$. Weiters ist

$$g(tx_1, \dots, tx_n) = t^n g(x_1, \dots, x_n)$$

(g ist homogen vom Grad n).

Betrachte ein rx , $r \in \{0, \dots, m\}$. Dann ist

$$rx = q_1\omega_1 + \dots + q_n\omega_n$$

für passende $q_1, \dots, q_n \in \mathbb{Q}$. $\omega_1, \dots, \omega_n$ sind n \mathbb{Q} -linear unabhängige Elemente von K , also Basis.

$$rx = \underbrace{\sum_{i=1}^n [q_i] \omega_i}_{\in M} + \sum_{i=1}^n \{q_i\} \omega_i \quad \text{mit } z = [z] + \{z\}.$$

Wir haben jetzt $m + 1 = k^n + 1$ n -Tupel

$$([q_1], \dots, [q_n]) \in [0, 1]^n.$$

Unterteile $[0, 1] = [0, \frac{1}{k}] \cup \dots \cup [\frac{k-1}{k}, 1]$ (k Intervalle).

$$[0, 1]^n = \text{Vereinigung von } k^n \text{ Würfeln der Seitenlänge } \frac{1}{k}.$$

Mittels Schubfachschluss folgt, dass es einen Würfel gibt, in dem 2 solche n -Tupel sind.

$$\begin{aligned} [q_1], \dots, [q_n] &\text{ komme von } rx \\ [q'_1], \dots, [q'_n] &\text{ komme von } sx, \end{aligned}$$

o.B.d.A. $s > r$.

$$(s - r)x = \underbrace{m_s - m_r}_{\in M} + \underbrace{\sum (\{q_i\} + \{q'_i\}) \omega_i}_{=: y, |y| < \frac{1}{2}}$$

Somit $y \in \underbrace{(s - r)}_{\in \{1, \dots, m\}} x + M$.

$$y = \frac{1}{k} \cdot \sum \underbrace{(k \{q'_i\} - k \{q_i\}) \omega_i}_{|\cdot| \leq 1}$$

Also

$$|N(y)| = \frac{1}{k^n} |q(k \{q'_1\} - k \{q_1\}, \dots, k \{q'_n\} - k \{q_n\})| \leq \frac{1}{k^n} \cdot C < \frac{k^n}{k^n} = 1. \quad \blacksquare$$

Definition Zwei vollständige Gitter M und N eines algebraischen Zahlkörpers heißen äquivalent (im weiteren Sinne), falls es ein $\lambda \in K \setminus \{0\}$ gibt, sodass $N = \lambda M$.

Bemerkung Das ist eine Äquivalenzrelation, also gibt es Äquivalenzklassen.

Satz 2.5 (Endlichkeit der Klassenzahl) Sei R eine Ordnung eines algebraischen Zahlkörpers K ,

$$\mathcal{I}(R) := \{M \text{ vollständiges Gitter in } K \mid RM = M\}.$$

Dann enthält $\mathcal{I}(R)$ mit jedem vollständigen Gitter auch seine gesamte Äquivalenzklasse und $\mathcal{I}(R)$ modulo Äquivalenz ist endlich.

$h(R) :=$ Anzahl der Äquivalenzklassen in $\mathcal{I}(R)$ heißt Klassenzahl.

BEWEIS Sei $M \in \mathcal{I}(R)$, also $RM = M$. Dann gilt auch

$$R(\lambda M) = \lambda M \quad \text{für alle } \lambda \in K \setminus \{0\},$$

also ist die gesamte Äquivalenzklasse von M enthalten.

Behauptung. In jeder Äquivalenzklasse $\subseteq \mathcal{I}(R)$ gibt es ein M mit $\frac{1}{q}R \subseteq M \subseteq R$, wobei q eine nur von R abhängige Konstante ist.

Beweis. Starte mit beliebigem vollständigen Gitter $M_1 \in \mathcal{I}(R)$. $\omega_1, \dots, \omega_n$ sei \mathbb{Z} -Basis von R . ξ_1, \dots, ξ_n sei \mathbb{Z} -Basis von M .

$$\xi_j = \sum_{i=1}^n \frac{c_{ij}}{d} \omega_i \quad \text{für passende } c_{ij} \in \mathbb{Z}, d \in \mathbb{Z} \setminus \{0\}.$$

($\omega_1, \dots, \omega_n$ ist \mathbb{Q} -Basis von K .) Somit gilt $d\xi_j \in R$ und

$$M = dM_1 \subseteq R \quad \text{und } M \text{ und } M_1 \text{ sind äquivalent.}$$

Wähle ein $0 \neq \alpha \in M$ mit minimaler Norm. (Da $M \subseteq R \subseteq \mathfrak{o}_K$, sind alle Normen von Elementen von M ganzrationale Zahlen.)

m sei nun die Konstante aus obiger Proposition, die zu R gehört. Setze $q := m!$. ($q = \text{kgV}(1, \dots, n)$ wäre auch genug.)

2 Struktur der Idealhalbgruppe

Wähle $\beta \in M$ beliebig. Dann gibt es ein $r \in \{1, \dots, m\}$, sodass $r\frac{\beta}{\alpha} + R$ ein Element y mit $|N(y)| < 1$ enthält (lt. Proposition).

$$y = r\frac{\beta}{\alpha} + \gamma \quad \gamma \in R$$

$$1 > |N(y)| = \left| N\left(r\frac{\beta}{\alpha} + \gamma\right) \right|$$

$$= \left| N\left(\frac{r\beta + \gamma\alpha}{\alpha}\right) \right| = \frac{1}{|N(\alpha)|} \cdot |N(r\beta + \gamma\alpha)|,$$

somit

$$\left| N\left(\underbrace{r\beta}_{\in M} + \underbrace{\gamma\alpha}_{\in M}\right) \right| < |N(\alpha)|.$$

Wir haben das Element $r\beta + \gamma\alpha \in M$ gefunden, dessen Norm kleiner als $N(\alpha)$ ist. Also

$$r\beta + \gamma\alpha = 0. \quad \blacksquare$$

Korollar (Endlichkeit der Klassengruppe) Sei K ein algebraischer Zahlkörper, \mathfrak{o}_K sein Ganzheitsring, \mathcal{I}_K die Gruppe der von $\{0\}$ verschiedenen gebrochenen Ideale von \mathfrak{o}_K ,

$$\mathcal{H}_K = \{\lambda\mathfrak{o}_K \mid \lambda \in K \setminus \{0\}\}$$

die Gruppe der „gebrochenen Hauptideale“ („eigtl. umgekehrt, geht nur im Englischen“),

$$Cl(K) := \mathcal{I}_K / \mathcal{H}_K$$

die „Klassengruppe von K “. Dann ist $Cl(K)$ eine endliche Gruppe.

BEWEIS 1. Behauptung. Sei M ein vollständiges Gitter mit $\mathfrak{o}_K M = M$. Dann ist M ein gebr. Ideal.

Beweis. Offensichtlich ist M ein \mathfrak{o}_K -Modul. Lt. Beginn des Beweises des Satzes existiert ein $d \in \mathbb{Z}$ mit $dM \subseteq \mathfrak{o}_K$. $\implies M$ ist gebr. Ideal.

2. Behauptung. Jedes gebr. Ideal ist vollständiges Gitter.

Beweis. Sei M ein gebr. Ideal, $\gamma M \subseteq \mathfrak{o}_K$ für $\gamma \in \mathfrak{o}_K$. Dann gilt

$$M \subseteq \frac{1}{\gamma} \underbrace{\mathfrak{o}_K}_{\text{fr. } \mathbb{Z}\text{-M.}},$$

freier \mathbb{Z} -Modul

Untergruppen von frei abelschen Gruppen sind frei. Somit ist M freier \mathbb{Z} -Modul.

Sei $\omega_1, \dots, \omega_n$ eine \mathbb{Z} -Basis von \mathfrak{o}_K . $\omega_1, \dots, \omega_n$ sind also linear unabhängig über \mathbb{Z} . Sei $\delta \in M$.

$$\delta\omega_1, \dots, \delta\omega_n \in \delta\mathfrak{o}_K \subseteq M\mathfrak{o}_K \subseteq M.$$

Das sind n linear unabhängige Elemente aus M . M hat somit $\text{Rang} \geq n$, aber $> n$ geht nicht.

3. $\mathcal{H}_K \trianglelefteq \mathcal{I}_K$, weil jedes Element von \mathcal{H}_K offensichtlich ein vollständiges Gitter ist und daher lt. 1 ein gebr. Ideal ist. \mathcal{H}_K ist Gruppe (abelsch) klar.

4. Zwei vollständige Gitter M, M' sind äquivalent

$$\Leftrightarrow M' = \lambda M$$

$$\Leftrightarrow M' = (\lambda \mathfrak{o}_K)M \Leftrightarrow M, M' \text{ äquivalent mod } \mathcal{H}_K.$$

Die Endlichkeit von $Cl(\mathcal{I}_K/\mathcal{H}_K)$ folgt aus dem Satz. ■

Definition Die Kardinalität der Klassengruppe $Cl(K)$ heißt Klassenzahl von K , schreibe h_K .

Bemerkung $h_K = 1 \Leftrightarrow \mathfrak{o}_K$ ist Hauptidealbereich.

$$(h_K = 1 \Leftrightarrow \mathcal{H}_K = \mathcal{I}_K.)$$

Proposition Sei K ein algebraischer Zahlkörper, $I \trianglelefteq \mathfrak{o}_K$. Falls I^l ein Hauptideal ist und $\text{ggT}(l, h_K) = 1$, so ist bereits I ein Hauptideal.

BEWEIS

$$\begin{aligned} I^l &\in \mathcal{H}_K \\ I^{h_K} &\in \mathcal{H}_K \quad (\text{Fermat}) \end{aligned}$$

Wähle $x, y \in \mathbb{Z}$ mit $xl + yh_K = 1$. Somit gilt

$$I = I^{xl} \cdot I^{yh_K} = \underbrace{(I^l)^x}_{\in \mathcal{H}_K} \cdot \underbrace{(I^{h_K})^y}_{\in \mathcal{H}_K} \in \mathcal{H}_K. \quad \blacksquare$$

2 Struktur der Idealhalbgruppe

3 Struktur der Einheitengruppe

3.1 Leichtes über die Struktur

Sei K ein algebraischer Zahlkörper, R eine Ordnung von K („brauche explizit nicht die Hauptordnung“). Lt. Struktursatz ist

$$\mathcal{E}(R) = (\text{endl. Gruppe}) \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r.$$

Die wesentliche Frage ist, wie groß r ist.

Satz 3.1 Sei $H := \{\zeta \in R \mid \zeta \text{ ist Einheitswurzel}\}$. Dann ist H eine zyklische Gruppe und $\exists r \in \mathbb{N}_0$, sodass

$$\mathcal{E}(R) = H \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r.$$

BEWEIS Sei G eine abelsche Gruppe.

$$\text{Tor}(G) := \{g \in G \mid g \text{ hat endliche Ordnung}\}$$

ist die *Torsionsgruppe* von G :

$$1 \in \text{Tor}(G); \quad (g \cdot h)^{|g| \cdot |h|} = 1.$$

Wenn

$$G = (\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}) \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r,$$

$m_1 \mid \cdots \mid m_k, m_k \neq 0$, dann ist die Torsionsgruppe

$$\text{Tor}(G) = (\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}) \times \{0\} \times \cdots \times \{0\}.$$

Somit ist H eine endliche Untergruppe der multiplikativen Gruppe eines Integritätsbereichs und somit zyklisch.

Da $\mathcal{E}(R)$ endlich erzeugt ist (siehe unten), folgt die Zerlegung aus dem Struktursatz für endlich erzeugte abelsche Gruppen. ■

Die Bestimmung der Torsionsgruppe der Einheitengruppe läuft also auf das Finden aller primitiven Einheitswurzeln hinaus. Lt. Algebra hat eine primitive n -te Einheitswurzel Grad $\varphi(n)$ über \mathbb{Z} . (Minimalpolynom ist das Kreisteilungspolynom G_n , irreduzibel, Grad $\varphi(n)$.)

Eine primitive n -te Einheitswurzel ζ kann nur in R enthalten sein, wenn

$$\varphi(n) \mid [K : \mathbb{Q}],$$

weil

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)] \cdot [Qset(\zeta) : \mathbb{Q}].$$

3 Struktur der Einheitengruppe

Proposition Sei $\varepsilon \in R$. Dann gilt

$$\varepsilon \in \mathcal{E}(R) \iff |N_{K:\mathbb{Q}}(\varepsilon)| = 1.$$

BEWEIS „ \Leftarrow “: Sei f das charakteristische Polynom von ε über K ,

$$f = \prod_{j=1}^n (X - \sigma_j(\varepsilon)),$$

$\sigma_1, \dots, \sigma_n$ die Einbettungen von K .

$$\Rightarrow f = \sum_{j=0}^n a_j X^j,$$

wobei $a_n = 1$ und $a_0 = (-1)^n \cdot N_{K:\mathbb{Q}}(\varepsilon)$.

Wenn also $N_{K:\mathbb{Q}}(\varepsilon) = \pm 1$, so gilt

$$\varepsilon \cdot \underbrace{\left(\sum_{j=1}^n a_j \varepsilon^{j-1} \right)}_{\in R} = -a_0 = \pm 1 \quad (\text{wegen } f(\varepsilon) = 0).$$

Somit

$$\varepsilon \in \mathcal{E}(R).$$

„ \Rightarrow “:

$$1^n = N(1) = N(\varepsilon \cdot \varepsilon^{-1}) = \underbrace{N(\varepsilon)}_{\in \mathbb{Z}} \cdot \underbrace{N(\varepsilon^{-1})}_{\in \mathbb{Z}}.$$

Also $N(\varepsilon) \mid 1$ in \mathbb{Z} , somit

$$N(\varepsilon) \in \mathcal{E}(\mathbb{Z}),$$

also fertig. ■

Bemerkung Für alle $\alpha \in R$ gilt $\frac{N(\alpha)}{\alpha} \in R$. (Selber Beweis.)

Definition Sei $K = \mathbb{Q}(\alpha)$ ein algebraischer Zahlkörper. Seien $s, t \in \mathbb{N}_0$, sodass $\alpha^{(1)}, \dots, \alpha^{(s)}$ die reellen Konjugierten von α und $\alpha^{(s+1)}, \dots, \alpha^{(s+2t)}$ die (komplexen) nicht-reellen Konjugierten von α sind, wobei

$$\overline{\alpha^{(s+j)}} = \alpha^{(s+t+j)} \quad \text{für } 1 \leq j \leq t.$$

($\bar{\alpha}$ bezeichnet komplexe Konjugation.)

(s, t) heißt die Signatur von K .

$$\begin{aligned} \sigma_j : K &\rightarrow \mathbb{R}; \sigma(\alpha) = \alpha^{(j)} && \text{für } 1 \leq j \leq s \\ \sigma_j : K &\rightarrow \mathbb{C}; \sigma(\alpha) = \alpha^{(j)} && \text{für } s+1 \leq j \leq s+2t \end{aligned}$$

(\mathbb{Q} -Isomorphismen.)

$$\sigma : K \rightarrow \mathbb{R}^s \times \mathbb{C}^t$$

(direktes Produkt von Ringen).

$$\sigma = \prod_{j=1}^{s+t} \sigma_j, \quad \text{also } \beta \mapsto (\sigma_1\beta, \dots, \sigma_{s+t}(\beta)).$$

$$N : \mathbb{R}^s \times \mathbb{C}^t \rightarrow \mathbb{R},$$

$$(x_1, \dots, x_s, x_{s+1}, \dots, x_{s+t}) \mapsto |x_1| \cdots |x_s| \cdot |x_{s+1}|^2 \cdots |x_{s+t}|^2,$$

$$l : \mathbb{R}^s \times \mathbb{C}^t \rightarrow \mathbb{R}^{s+t},$$

$$(x_1, \dots, x_s, x_{s+1}, \dots, x_{s+t}) \mapsto (\log |x_1|, \dots, \log |x_s|, 2 \log |x_{s+1}|, \dots, 2 \log |x_{s+t}|).$$

Definiere weiters die logarithmische Einbettung als

$$L := \{(y_1, \dots, y_{s+t}) \in \mathbb{R}^{s+t} \mid y_1 + \dots + y_{s+t} = 0\}.$$

Proposition (Banalitäten) 1. $s + 2t = [K : \mathbb{Q}]$

2. $N \circ \sigma = N_{K:\mathbb{Q}}$

3. $l(\sigma(\mathcal{E}(R))) \subseteq L$

4. σ ist Ringmonomorphismus.

5. l ist Gruppenhomomorphismus von

$$((\mathbb{R} \setminus \{0\})^s \times (\mathbb{C} \setminus \{0\})^t, \cdot) \rightarrow (\mathbb{R}^{s+t}, +)$$

BEWEIS 1. α hat $s + 2t$ Konjugierte, also hat Minimapolynom Grad $s + 2t = [K : \mathbb{Q}]$.

2.

$$\begin{aligned} N_{K:\mathbb{Q}}(\beta) &= \prod_{j=1}^n \sigma_j(\beta) \\ |N_{K:\mathbb{Q}}(\beta)| &= \prod_{j=1}^s |\sigma_j(\beta)| \cdot \prod_{j=s+1}^{s+t} |\sigma_j(\beta)| \cdot \prod_{j=s+t+1}^{s+2t} \underbrace{|\sigma_j(\beta)|}_{=|\overline{\sigma_{j-t}(\beta)}|=|\sigma_{j-t}(\beta)|} \\ &= N(\sigma(\beta)). \end{aligned}$$

3. $N(\sigma(\varepsilon)) = 1$ für alle $\varepsilon \in \mathcal{E}(R)$, somit

$$l(\sigma(\varepsilon)) \cdot \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = 0.$$

4. σ ist lt. universeller Eigenschaft des direkten Produkts ein Ringhomomorphismus. Da jedes σ_j ein Monomorphismus ist, ist σ erst recht ein Monomorphismus.

3 Struktur der Einheitengruppe

5. klar. ■

Proposition Sei R eine Ordnung von K . $\sigma(R)$ ist ein vollständiges Gitter in

$$\mathbb{R}^s \times \mathbb{C}^t \stackrel{\mathbb{R}\text{-}VR}{\simeq} \mathbb{R}^{s+2t}.$$

BEWEIS

$$\begin{aligned} R &= \langle \omega_1, \dots, \omega_n \rangle_{\mathbb{Z}} \\ \sigma(R) &= \langle \sigma(\omega_1), \dots, \sigma(\omega_n) \rangle_{\mathbb{Z}} \end{aligned} \quad \blacksquare$$

3.2 Einführung in die Geometrie der Zahlen: Gitter im \mathbb{R}^n und Minkowskischer Gitterpunktsatz

Definition Eine Teilmenge des \mathbb{R}^n heißt diskret, wenn sie keinen Häufungspunkt besitzt.

Definition 1 Eine endlich erzeugte freie abelsche Untergruppe G von \mathbb{R}^n , deren Erzeuger linear unabhängig über \mathbb{R} sind, heißt ein Gitter von \mathbb{R}^n .

Falls der Rang von G gleich n ist, heißt das Gitter *vollständig*. □

Proposition Sei K ein algebraischer Zahlkörper, R eine Ordnung von K , (s, t) die Signatur von K und $\sigma : K \rightarrow \mathbb{R}^s \times \mathbb{C}^t$ die Einbettung von K . Dann ist $\sigma(R)$ ein Gitter von $\mathbb{R}^{s+2t} \simeq \mathbb{R}^s \times \mathbb{C}^t$.

BEWEIS Sei $\omega_1, \dots, \omega_n$ eine Ganzheitsbasis von R . Dann ist $\sigma(R) = \langle \sigma(\omega_1), \dots, \sigma(\omega_n) \rangle_{\mathbb{Z}}$, also eine endlich erzeugte abelsche Gruppe. Um zu beweisen, dass die Basis linear unabhängig über \mathbb{R} ist, betrachten wir die Determinante $\det M$ für

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\omega_1) & \dots & \sigma_s(\omega_n) \\ \Re\sigma_{s+1}(\omega_1) & \dots & \Re\sigma_{s+1}(\omega_n) \\ \Im\sigma_{s+1}(\omega_1) & \dots & \Im\sigma_{s+1}(\omega_n) \\ \vdots & \ddots & \vdots \\ \Re\sigma_{s+t}(\omega_1) & \dots & \Re\sigma_{s+t}(\omega_n) \\ \Im\sigma_{s+t}(\omega_1) & \dots & \Im\sigma_{s+t}(\omega_n) \end{pmatrix}.$$

Wir sehen das als Determinante über \mathbb{C}^n und multiplizieren M von links mit der Blockdiagonalmatrix

$$\text{diag} \left(1, \dots, 1, \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \dots, \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \right).$$

Dabei wird der (1×1) -Block s -mal und der (2×2) -Block t -mal wiederholt. Wir erhalten

$$\det M = \frac{1}{(-2i)^t} \det \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\omega_1) & \dots & \sigma_s(\omega_n) \\ \sigma_{s+1}(\omega_1) & \dots & \sigma_{s+1}(\omega_n) \\ \sigma_{s+t+1}(\omega_1) & \dots & \sigma_{s+t+1}(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_{s+t}(\omega_1) & \dots & \sigma_{s+t}(\omega_n) \\ \sigma_{s+2t}(\omega_1) & \dots & \sigma_{s+2t}(\omega_n) \end{pmatrix} = \pm \frac{1}{(-2i)^t} \sqrt{\text{discr}(\omega_1, \dots, \omega_n)}.$$

Da $\omega_1, \dots, \omega_n$ eine Basis von R ist, ist die Diskriminante von 0 verschieden, somit ist auch $\det M \neq 0$, was zu zeigen war. ■

Satz 3.2 Sei G eine Untergruppe von \mathbb{R}^n für ein $n \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:

1. G ist eine diskrete Teilmenge von \mathbb{R}^n .
2. G ist ein Gitter.

BEWEIS „1. \implies 2.“ Wähle $\omega_1, \dots, \omega_k$ eine maximale \mathbb{R} -linear unabhängige Teilmenge von G und setze $H := \langle \omega_1, \dots, \omega_k \rangle_{\mathbb{Z}}$.

[...] Es gibt ein $q \in \mathbb{N}$ mit $G \subseteq \frac{1}{q}H$. Nach dem Struktursatz ist G eine frei abelsche Untergruppe vom Rang $\ell \leq k$. Die Elemente der \mathbb{Z} -Basis von G müssen \mathbb{R} -linear unabhängig sein: andernfalls wäre G in einem \mathbb{R} -Vektorraum einer Dimension $< \ell \leq k$ enthalten, was ein Widerspruch zur \mathbb{R} -linearen Unabhängigkeit von $\omega_1, \dots, \omega_k$ ist. Daraus folgt auch $\ell = k$.

„2. \implies 1.“ Sei $G = \langle \omega_1, \dots, \omega_k \rangle_{\mathbb{Z}}$ für \mathbb{R} -linear unabhängige $\omega_1, \dots, \omega_k$. Aufgrund der vorausgesetzten linearen Unabhängigkeit gilt

$$\text{span}_{\mathbb{R}}\{\omega_1, \dots, \omega_{k-1}\} \subsetneq \text{span}_{\mathbb{R}}\{\omega_1, \dots, \omega_{k-1}, \omega_k\},$$

weil der erste Raum Dimension $k - 1$ und der zweite Raum Dimension k hat.

Damit gilt auch

$$n - k = \dim_{\mathbb{R}}(\text{span}_{\mathbb{R}}\{\omega_1, \dots, \omega_{k-1}, \omega_k\})^{\perp} < \dim_{\mathbb{R}}(\text{span}_{\mathbb{R}}\{\omega_1, \dots, \omega_{k-1}\})^{\perp} = n - k + 1,$$

weshalb es ein $v \in (\text{span}_{\mathbb{R}}\{\omega_1, \dots, \omega_{k-1}\})^{\perp} \setminus (\text{span}_{\mathbb{R}}\{\omega_1, \dots, \omega_{k-1}, \omega_k\})^{\perp}$ gibt. Es gilt also $\langle v, \omega_j \rangle = 0$ für $j < k$ und $\langle v, \omega_k \rangle \neq 0$.

Für eine beschränkte Menge S und eine Konstante C mit $\forall z \in S : \|z\|_2 < C$ und ein $g = a_1\omega_1 + \dots + a_k\omega_k \in G \cap S$ (wobei $a_1, \dots, a_k \in \mathbb{Z}$) gilt daher

$$|a_k| = \left| \frac{\langle g, v \rangle}{\langle \omega_k, v \rangle} \right| \leq \frac{\|g\|_2 \cdot \|v\|_2}{|\langle \omega_k, v \rangle|} \leq \frac{C \cdot \|v\|_2}{|\langle \omega_k, v \rangle|},$$

weshalb a_k beschränkt ist. Analog sind auch die übrigen a_j beschränkt, woraus folgt, dass $G \cap S$ endlich ist. Somit ist G diskret. ■

3 Struktur der Einheitsengruppe

Korollar Sei K ein alg. ZK, R eine Ordnung in K . Dann ist $\mathcal{E}(R)$ endlich erzeugte abelsche Gruppe.

Das vervollständigt erst den Beweis von Satz 3.1.

BEWEIS

$$l(\sigma(\mathcal{E}(R))) \subseteq L \subseteq \mathbb{R}^{s+t}$$

ist abelsche Untergruppe von $(\mathbb{R}^{s+t}, +)$.

Beh. Diese Untergruppe ist diskret. Beweis. Sei

$$S := \{z \in \mathbb{R}^{s+t} \mid \|z\|_\infty \leq C\}$$

für ein $C \in \mathbb{R}^+$.

$$l^{-1}(S) = \{x \in \mathbb{R}^s \times \mathbb{C}^t \mid \frac{1}{e^C} \leq \|x\|_\infty \leq e^C\}$$

beschränkt.

$$l^{-1}(S \cap L_1) = \{\sigma(\varepsilon) \mid \varepsilon \in \mathcal{E}(R) \text{ und } \sigma(\varepsilon) \in l^{-1}(S)\}$$

ist endlich, weil $\sigma(R)$ ein Gitter und daher diskret ist. $S \cap L_1$ ist endlich, weil $S \cap L_1 = l(l^{-1}(S \cap L_1))$, weil $L_1 \subseteq l(\mathbb{R}^s \times \mathbb{C}^t)$ („alles da drin hat Urbilder“).

Somit ist L_1 frei abelsch.

Beh. $\text{Ker}(l \circ \sigma) = \text{Tor}(\mathcal{E}(R)) = \text{Einheitswurzeln in } \mathcal{E}(R)$.

Beweis. Sei $\varepsilon \in \text{Ker}(l \circ \sigma)$, also

$$\log |\sigma_1(\varepsilon)| = \log |\sigma_2(\varepsilon)| = \dots = \log |\sigma_{s+t}(\varepsilon)| = 0,$$

somit

$$|\sigma_1 \varepsilon| = |\sigma_2 \varepsilon| = \dots = |\sigma_{s+t} \varepsilon| = 1.$$

Also ist

$$\underbrace{\sigma(\text{Ker}(l \circ \sigma))}_{\subseteq \sigma(R)} \subseteq \{x \mid \|x\|_\infty \leq 1\}$$

beschränkt. Daher ist auch $\sigma(\text{Ker}(l \circ \sigma))$ endlich, daher auch $\text{Ker}(l \circ \sigma)$. Also haben alle Elemente des $\text{Ker}(l \circ \sigma)$ endliche Ordnung, sind also Einheitswurzeln.

$$\text{Ker}(l \circ \sigma) \subseteq \text{Tor } \mathcal{E}(R).$$

Jede Einheitswurzel in \mathbb{C} hat Absolutbetrag 1,

$$\forall \varepsilon \in \mathcal{E}(R), \varepsilon \text{ Einheitswurzel} : |\sigma(\varepsilon)| = 1,$$

d.h. $\text{Tor } \mathcal{E}(R) \subseteq \text{Ker}(l \circ \sigma)$.

Somit ist

$$\mathcal{E}(R) / \text{Tor}(\mathcal{E}(R)) \stackrel{1. \text{ Iso.satz}}{\cong} L_1$$

frei abelsch mit endlichem Rang. Also sind die Einheiten $\mathcal{E}(R)$ endlich erzeugt. ■

Wir wissen: $L^1 \subseteq L$ und L ist ein $(s+t-1)$ -dimensionaler \mathbb{R} -Vektorraum. Laut Beweis von Satz 3.2 ist damit L^1 eine freie abelsche Gruppe vom Rang $\leq s+t-1$.

Ziel ist es, zu zeigen, dass $\text{rang}(L) = s+t-1$.

3.2 Einführung in die Geometrie der Zahlen

Definition Sei $G = \langle \omega_1, \dots, \omega_k \rangle_{\mathbb{Z}} \leq (\mathbb{R}^n, +)$ ein Gitter. Dann heißt

$$\{x_1\omega_1 + \dots + x_k\omega_k \mid x_j \in [0, 1)\}$$

die Grundmasche („fundamental paralleloptope“) von G .

Proposition Sei V ein Untervektorraum von \mathbb{R}^n , G eine endlich erzeugte freie abelsche Untergruppe von $(V, +)$. Dann sind folgende Aussagen äquivalent:

1. $\dim V = \text{rank}(G)$
2. Es gibt eine beschränkte Teilmenge $S \subseteq V$, sodass

$$\bigcup_{g \in G} (S + g) = V.$$

BEWEIS 1 \implies 2: Wähle $S =$ Grundmasche von G . Daraus folgt die Behauptung wie im Beweis von Satz 3.2.

$\neg 1 \implies \neg 2$: Sei S eine beschränkte Teilmenge von V . Da $\text{rank}(G) \neq \dim V$, folgt

$$\text{rank}(G) < \dim V$$

(lt. Beweis von Satz 3.2).

Wähle C so, dass

$$\forall z \in S : \|z\|_2 < C.$$

Wähle ein $v \in (\text{span}_{\mathbb{R}} G)^\perp$ mit $\|v\|_2 > C$.

Annahme: $v = g + s, s \in S, g \in G$.

$$c \cdot \|v\|_2 < \langle v, v \rangle = \langle v, g + s \rangle = \langle v, s \rangle \leq \|v\|_2 \cdot \|s\| < \|v\|_2 \cdot C,$$

Widerspruch.

(„Eigentlich habe ich jetzt non-1 nach non-2 indirekt bewiesen...“) ■

Proposition Sei G ein Gitter im \mathbb{R}^n . Dann hängt $d(G)$ nicht von der gewählten Gitterbasis ab.

BEWEIS Seien $\omega_1, \dots, \omega_n$ sowie $\vartheta_1, \dots, \vartheta_n$ zwei \mathbb{Z} -Basen von G . Dann gibt es eine Matrix $A = (a_{ij}) \in \mathbb{Z}^{n \times n}$ mit

$$\vartheta_j = \sum a_{ij} \omega_i$$

und $\det A = \pm 1$. Dann gilt

$$|\det(\vartheta_1, \dots, \vartheta_n)| = \left| \underbrace{\det A}_{=\pm 1} \cdot \det(\omega_1, \dots, \omega_n) \right|. \quad \blacksquare$$

Lemma Sei T eine messbare Teilmenge des \mathbb{R}^n , G ein Gitter in \mathbb{R}^n , sodass

$$(T + g)_{g \in G} \text{ disjunkt}$$

sind. Dann gilt $\lambda(T) \leq d(G)$. ($\lambda(T)$ bezeichnet das Volumen von T .)

3 Struktur der Einheitengruppe

BEWEIS Sei M die Grundmasche von G bzgl. irgendeiner Basis.

$$\begin{aligned} \lambda(T) &= \lambda(T \cap \mathbb{R}^n) = \lambda\left(T \cap \left(\bigcup_{g \in G} M - g\right)\right) = \sum_{g \in G} \lambda\left(\underbrace{T \cap (M - g)}_{\text{disjunkt und } \mathbb{R}^n = \bigsqcup_{g \in G} (M - g)}\right) \\ &= \sum_{g \in G} \lambda\left(\underbrace{(T + g) \cap M}_{\text{disjunkt}}\right) = \lambda\left(\bigcup_{g \in G} ((T + g) \cap M)\right) = \lambda\left(\left(\bigcup_{g \in G} T + g\right) \cap M\right) \\ &\leq \lambda(M) = d(G). \end{aligned}$$

(„Wenn ich eine Menge verschiebe, wird das Volumen wohl gleich bleiben. Eigentlich verwende ich hier laufend Maßtheorie!“) ■

Definition Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt zentralsymmetrisch, wenn

$$\forall z \in T : -z \in T.$$

Satz 3.3 (Minkowskischer Gitterpunktsatz) Sei T eine konvexe zentralsymmetrische Teilmenge von \mathbb{R}^n und G ein Gitter im \mathbb{R}^n . Wenn

$$\lambda(T) \geq 2^n \cdot d(G),$$

so existiert ein $z \neq 0$ mit $z \in T \cap G$.

Bemerkung Man spricht hier von der „Geometrie der Zahlen“.

BEWEIS Setze $S = \frac{1}{2}T$. Dann gilt

$$\lambda(S) = \frac{1}{2^n} \lambda(T) > d(G).$$

Laut Lemma sind die Mengen $(S + g)_{g \in G}$ nicht disjunkt, somit gibt es $g, h \in G$ mit $g \neq h$, sodass

$$(S + g) \cap (S + h) \neq \emptyset,$$

d.h. es gibt $x, y \in S$ mit

$$g + x = h + y.$$

Damit auch

$$0 \neq \underbrace{g - h}_{\in G} = g - x.$$

Es gibt $y', x' \in T$ mit

$$y = \frac{1}{2}y', \quad x = \frac{1}{2}x'.$$

Somit

$$0 \neq g - h = \frac{y' + (-x')}{2} \in T.$$

(y' und $-x'$ sind $\in T$, weil zentralsymmetrisch. Der Mittelpunkt zweier Punkte liegt ebenfalls in T , weil T konvex ist.) ■

3.3 Dirichletscher Einheitensatz

Satz 3.4 Sei R eine Ordnung in einem algebraischen Zahlkörper und $c \in \mathbb{Z}$. Dann gibt es bis auf Assoziiertheit nur endlich viele Elemente aus R mit Norm c , d.h. es gibt $\beta_1, \dots, \beta_t \in R$ mit $N(\beta_j) = c$, sodass

$$\forall \beta \in R : N(\beta) = c \rightarrow \exists \varepsilon \in \mathcal{E}(R) \exists j \in \{1, \dots, t\} : \beta = \varepsilon \cdot \beta_j.$$

BEWEIS 1. Seien $\beta, \gamma \in R$ mit $N(\beta) = N(\gamma) = c$ und $\beta \equiv \gamma \pmod{c \cdot R}$. Dann gilt $\beta \sim \gamma$.

Beweis: Sei $\gamma = \beta + c \cdot \delta$ für ein passendes $\delta \in \mathbb{R}$. Das heißt

$$\frac{\gamma}{\beta} = 1 + \frac{c}{\beta} \delta = 1 + \frac{N(\beta)}{\beta} \cdot \delta.$$

Das Minimalpolynom von β hat die Gestalt

$$\beta(+\dots) \pm N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta) = 0,$$

also

$$\beta \mid N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta) \text{ in } \mathbb{Z}[\beta].$$

Es gilt

$$N(\beta) = N_{K/\mathbb{Q}}(\beta) = (N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta))^{[K:\mathbb{Q}(\beta)]},$$

somit

$$\beta \mid N(\beta) \text{ in } \mathbb{Z}[\beta] \subseteq R.$$

Also $\frac{\gamma}{\beta} \in R$. Analog $\frac{\beta}{\gamma} \in R$. Daher

$$\frac{\gamma}{\beta} \in \mathcal{E}(R), \quad \beta \sim \gamma.$$

2. $[R : cR] = c^n$.

Es gibt also höchstens $|c|^n$ nicht-assozierte Elemente aus R mit Norm c . ■

Satz 3.5 (Dirichletscher Einheitensatz) Sei R eine Ordnung in einem algebraischen Zahlkörper K der Signatur (s, t) (d.h. s reelle und t komplexe Einbettungen). Setze $r := s + t - 1$. Dann gilt

$$\mathcal{E}(R) \simeq \langle \zeta \rangle \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_r.$$

Bemerkung Wir wissen

$$l(\sigma(\mathcal{E}(R))) \subseteq \underbrace{\{z \in \mathbb{R}^{s+t} \mid z_1 + \dots + z_s + 2z_{s+1} + \dots + 2z_{s+t} = 0\}}_{(s+t-1)\text{-dim. VR}}.$$

Die Aussage des Dirichletschen Einheitensatzes ist, dass $l(\sigma(\mathcal{E}(R)))$ vollständig in diesem Raum ist.

BEWEISIDEE

3 Struktur der Einheitsgruppe

- Kriterium für Vollständigkeit eines Gitters: Gittertranslate einer beschränkten Menge überdecken VR.
- Muss für jeden Punkt des VR passenden Gitterpunkt finden (Minkowski).
- Die beschränkte Menge wird zur Konstruktion Satz 3.4 benutzt.

Wir arbeiten nicht im Logarithmenraum, sondern im $\mathbb{R}^s \times \mathbb{C}^t$, im Bild von σ . □

BEWEIS Sei

$$S := \{x \in \mathbb{R}^s \times \mathbb{C}^t \mid |x_1 \cdots x_s x_{s+1}^2 \cdots x_{s+t}^2| = 1\}.$$

Das ist

$$l^{-1}(\{z \in \mathbb{R}^{s+t} \mid z_1 + \cdots + z_s + 2z_{s+1} + \cdots + 2z_{s+t} = 0\})$$

und enthält $\sigma(\mathcal{E}(R))$, weil $\varepsilon \in \mathcal{E}(R) \iff N(\varepsilon) = \pm 1$.

1. Beh. Sei X eine beschränkte Teilmenge von C . Dann ist $l(X)$ eine beschränkte Teilmenge von \mathbb{R}^{s+t} .

Beweis. Sei $C > 0$ mit $\forall x \in X : \|x\|_\infty < C$. Es gilt

$$-\left(\sum_{i \neq j} d_i\right) \cdot C < -\sum_{i \neq j} d_i \log |x_i| = d_j \log |x_j| < d_j \log C$$

mit $d_i = 1 + [i \geq s + 1]$, weil $\sum_i d_i \log |x_i| = 0$. Daraus folgt

$$\forall z \in l(X) : \|z\|_\infty \leq n \cdot C.$$

2. Beh. Es reicht zu zeigen, dass es eine beschränkte Teilmenge $X \subseteq S$ gibt, sodass

$$\bigcup_{\varepsilon \in \mathcal{E}(R)} \sigma(\varepsilon) \cdot X = S.$$

(Das \cdot ist hierbei als komponentenweise Multiplikation im VR $\mathbb{R}^s \times \mathbb{C}^t$ zu verstehen.)

Lt. 1 ist $l(X)$ eine beschränkte Menge.

$$l(S) = \bigcup_{\varepsilon \in \mathcal{E}(R)} (l(X) + l(\sigma(\varepsilon))),$$

daraus folgt lt. Proposition aus 3.2, dass $l(\sigma(\mathcal{E}(R)))$ ein vollständiges Gitter in $l(S)$ ist.

3. Beh. Sei $y \in S$. Dann ist $y \cdot \sigma(R)$ ein vollständiges Gitter in \mathbb{R}^{s+2t} mit $d(y \cdot \sigma(R)) = d(\sigma(R))$.

Beweis. Komponentenweise Multiplikation mit y kann durch Multiplikation mit der Matrix

$$\text{diag} \left(y_1, \dots, y_s, \begin{pmatrix} \text{Re } y_{s+1} & -\text{Im } y_{s+1} \\ \text{Im } y_{s+1} & \text{Re } y_{s+1} \end{pmatrix}, \dots \right)$$

von links geschrieben werden.

$$\begin{aligned} d(y \cdot \sigma(R)) &= |\det(\text{diag}(\dots))| d(\sigma(R)) \\ &= \left| y_1 y_2 \cdots y_s \underbrace{((\text{Re } y_{s+1})^2 + (\text{Im } y_{s+1})^2)}_{|y_{s+1}|^2} \cdots |y_{s+t}|^2 \right| \cdot d(\sigma(R)) = d(\sigma(R)). \end{aligned}$$

4. Seien c_1, \dots, c_{s+t} positive reelle Zahlen mit

$$c_1 \cdots c_{s+t} > (\cdot) d(\sigma(R))$$

und

$$X_0 := \{x \in \mathbb{R}^s \times \mathbb{C}^t \mid |x_j| < c_j \text{ für } 1 \leq j \leq s, |x_j|^2 < c_j \text{ für } s+1 \leq j \leq s+t\}.$$

Dann ist X_0 eine konvexe zentralsymmetrische Teilmenge von \mathbb{R}^{s+2t} mit

$$\lambda(X_0) > 2^{s+2t} d(\sigma(R)).$$

Beweis. X_0 zentralsymmetrisch wegen Absolutbeträgen. X_0 konvex als Produkt konvexer Mengen (Intervalle und Kreisscheiben).

$$\lambda(X_0) \stackrel{\text{Fubini}}{=} (2c_1) \cdot (2c_2) \cdots (2c_s) \cdot c_{s+1}\pi \cdots c_{s+t}\pi = (c_1 \cdots c_{s+t}) \cdot 2^s \pi^t > 2^{s+2t} \cdot d(\sigma(R)).$$

Zusammenfassend:

- $X_0 \subseteq S$ beschränkt, $\lambda(x_0) > 2^n d(\sigma(G))$.
- $\forall y \in S : d(y \cdot \sigma(G)) = d(\sigma(G))$.

Somit folgt aus dem Satz von Minkowski, dass es ein $y \cdot \sigma(\alpha) \in \sigma(G)$ ($\alpha \neq 0$) gibt mit

$$y \cdot \sigma(\alpha) \in X_0,$$

also $y \cdot \sigma(\alpha) = x$ für ein passendes $x \in X_0$.

Einschub: Auf $\mathbb{R}^s \times \mathbb{C}^t$ definiere

$$N(x) = |x_1 x_2 \cdots x_s x_{s+1}^2 \cdots x_{s+t}^2|.$$

Berechne nun $N(\alpha)$:

$$\begin{aligned} |N(\alpha)| &= N(\sigma(\alpha)) \\ N(x) &= N(y) \cdot N(\sigma(\alpha)) \\ |N(\alpha)| &= N(\sigma(\alpha)) = N(x) \leq c_1 \cdots c_s c_{s+1} \cdots c_{s+t}, \end{aligned}$$

wobei die c_i feste Konstanten unabhängig von y sind.

Da $|N(\alpha)|$ beschränkt ist, gibt es $\alpha_1, \dots, \alpha_m \in R$ für ein $m \in \mathbb{N}$ (unabhängig von y), sodass

$$a \sim a_j \quad \text{für passendes } j$$

(Satz 3.4).

Es gibt also ein $\varepsilon \in \mathcal{E}(R)$ mit

$$\alpha = \varepsilon \alpha_j. \quad j, \varepsilon \text{ hängen von } y \text{ ab.}$$

($\alpha_1, \dots, \alpha_m$ ist ein Repräsentantensystem bzgl. Assoziiertheit aller Elemente von R der $|\text{Norm}| \leq c_1 c_2 \cdots c_{s+t}$.)

3 Struktur der Einheitengruppe

Somit

$$y = \frac{x}{\sigma(\alpha)} = \frac{x}{\sigma(a_j)} \cdot \sigma\left(\frac{1}{\varepsilon}\right).$$

Setze

$$X := \left(\bigcup_{j=1}^m \frac{1}{\sigma(\alpha_j)} X_0 \right) \cap S$$

(unabhängig von y). Es folgt

$$y \in X \cdot \sigma\left(\frac{1}{\varepsilon}\right)$$

für passendes $\varepsilon = \varepsilon(y)$. (Weil

$$N\left(\frac{x}{\sigma(\alpha_j)}\right) = \frac{N(y)}{N(\sigma(\frac{1}{\varepsilon}))} = \frac{1}{1} = 1,$$

gilt $\frac{x}{\sigma(\alpha_j)} \in S$.)

X ist Vereinigung multiplikativer Translate einer beschränkten Menge und daher beschränkt. Daraus folgt

$$S \subseteq \bigcup_{\varepsilon \in \mathcal{E}(R)} X \cdot \sigma\left(\frac{1}{\varepsilon}\right),$$

wegen 2 fertig. ■

Definition Sei K ein algebraischer Zahlkörper der Signatur (s, t) , $r = s + t - 1$, R eine Ordnung von K und

$$\mathcal{E}(R) = \langle \zeta, \varepsilon_1, \dots, \varepsilon_r \rangle$$

für eine Einheitswurzel ζ und passende $\varepsilon_1, \dots, \varepsilon_r$.

Dann heißen $(\varepsilon_1, \dots, \varepsilon_r)$ Fundamenteinheiten von R . Falls $R = \mathfrak{o}_K$, spricht man von Fundamenteinheiten von K .

Korollar Sei $D \in \mathbb{N}$, D kein Quadrat. Wir betrachten die sog. Pellische Gleichung

$$x^2 - Dy^2 = 1$$

mit $x, y \in \mathbb{N}_0$. Dann hat diese Gleichung unendlich viele Lösungen und es gilt

$$(x, y) \text{ Lösung} \iff \exists k \in \mathbb{N}_0 : (x + \sqrt{D}y) = \eta^k,$$

wobei

$$\eta = \begin{cases} \varepsilon^2 & N(\varepsilon) = -1 \\ \varepsilon & N(\varepsilon) = 1 \end{cases}$$

und ε eine Fundamenteinheit von $\mathbb{Z}[\sqrt{D}]$ ist.

BEWEIS

$$\begin{aligned} x^2 - Dy^2 = 1 &\iff (x - \sqrt{D}y)(x + \sqrt{D}y) = 1 \\ &\iff N(x + \sqrt{D}y) = 1 \\ &\iff x + \sqrt{D}y \in \mathcal{E}(\mathbb{Z}[\sqrt{D}]) \text{ mit } N(x + \sqrt{D}y) = 1. \end{aligned}$$

$\mathbb{Q}(\sqrt{D})$ hat Signatur $(2, 0)$, damit $r = 1$. Aus dem Satz von Dirichlet folgt

$$\mathcal{E}(\mathbb{Z}[\sqrt{D}]) = \langle \zeta, \varepsilon \rangle$$

für passendes $\varepsilon \in \mathcal{E}(\mathbb{Z}[\sqrt{D}])$ (Fundamentaleinheit) und passende Einheitswurzel ζ .

Da $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{R}$ folgt $\zeta = -1$.

Sei o.B.d.A. $\varepsilon > 0$ (Vorzeichen kann ggf. durch Einheitswurzel erzeugt werden), weiters o.B.d.A. $\varepsilon > 1$ (ersetze ggf. ε durch $\frac{1}{\varepsilon}$). Somit

$$\underbrace{(x + \sqrt{D}y)}_{>0} = (-1)^a \cdot \underbrace{\varepsilon^b}_{>0} \quad a \in \mathbb{Z}, b \in \mathbb{Z}.$$

Also $a = 0$. Da $x + \sqrt{D}y > 1$ und $\varepsilon > 1$ folgt $b \in \mathbb{N}_0$.

$$(x + \sqrt{D}y) = \varepsilon^b \quad b \in \mathbb{N}_0.$$

Wegen

$$1 = N(x + \sqrt{D}y) = (N(\varepsilon))^b$$

muss b gerade sein, falls $N(\varepsilon) = -1$. Somit

$$b = \begin{cases} k & N(\varepsilon) = 1 \\ 2k & N(\varepsilon) = -1 \end{cases} .$$

■

3.4 Regulator

Sei K ein algebraischer Zahlkörper mit Signatur (s, t) , $s = s + t - 1$, R eine Ordnung in K , $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{E}(R)$. $l(\sigma(\varepsilon_1)), \dots, l(\sigma(\varepsilon_r))$ ist Basis eines Gitters, enthalten in

$$\underbrace{\{x \in \mathbb{R}^{s+t} \mid \sum x_j = 0\}}_{\dim(\cdot)=r} = L.$$

Wir betrachten das Volumen der Grundmasche M (r -dimensionales Volumen im \mathbb{R}^{r+1}).

$$L^\perp = \text{span}\left\{ \frac{1}{\sqrt{s+t}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \right\},$$

also

$$\lambda_r(M) = \lambda_{r+1} \left(\left\{ \sum_{i=0}^r z_i l_i \mid z_i \in [0, 1] \right\} \right),$$

wobei

$$l_0 = \frac{1}{\sqrt{s+t}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

3 Struktur der Einheitengruppe

$l_i = l(\sigma(\varepsilon_i))$ für $1 \leq i \leq r$. Der Ausdruck ist also

$$= |\det(l_0 l_1 \cdots l_r)| = \frac{1}{\sqrt{s+t}} \begin{vmatrix} 1 & d_1 \log |\sigma_1(\varepsilon_1)| & \cdots & d_1 \log |\sigma_1(\varepsilon_r)| \\ \vdots & \vdots & & \vdots \\ 1 & d_{s+t} \log |\sigma_{s+t}(\varepsilon_1)| & \cdots & d_{s+t} \log |\sigma_{s+t}(\varepsilon_r)| \end{vmatrix},$$

wobei $d_i = 1 + [i \leq s + 1]$.

Wähle $k \in \{1, \dots, s+t\}$ beliebig. Addiere alle Zeilen außer der k -ten Zeile zur k -ten Zeile:

$$\lambda_r(M) = \frac{1}{\sqrt{s+t}} \begin{vmatrix} 1 & d_1 \log |\sigma_1(\varepsilon_1)| & \cdots \\ \vdots & \vdots & \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \\ 1 & \vdots & \\ \vdots & \vdots & \\ 1 & \vdots & \end{vmatrix} = \sqrt{s+t} \cdot |\det(d_i \log |\sigma_i(\varepsilon_i)|)_{i \neq k, j}|.$$

Definition Sei K ein algebraischer Zahlkörper der Signatur (s, t) , R eine Ordnung in K , $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{E}(R)$ für $r = s + t - 1$. Der Regulator von $(\varepsilon_1, \dots, \varepsilon_r)$ ist durch

$$\text{reg}(\varepsilon_1, \dots, \varepsilon_r) = \left| \det((d_i \log(\sigma_i(\varepsilon_j))))_{1 \leq i \leq r, 1 \leq j \leq r} \right|$$

mit $d_i = 1 + [i \leq s + 1]$ definiert.

Falls $(\varepsilon_1, \dots, \varepsilon_r)$ ein System von Fundamenteinheiten ist, so spricht man vom Regulator von R . Falls zusätzlich $R = \mathfrak{o}_K$, so spricht man vom Regulator von K .

Proposition Mit obiger Bezeichnung ist das Volumen der Grundmasche von $l(\sigma(\langle \varepsilon_1, \dots, \varepsilon_r \rangle))$ gleich

$$\sqrt{s+t} \text{reg}(\varepsilon_1, \dots, \varepsilon_r).$$

Insbesondere hängt der Regulator nur von $\langle \varepsilon_1, \dots, \varepsilon_r \rangle$, nicht vom konkreten Erzeugendensystem $(\varepsilon_1, \dots, \varepsilon_r)$ ab.

Basiswechsel mit Transformationsmatrix A führt zu Multiplikation des Regulators mit $|\det(A)|$. Indizes von Untergruppen können als Quotienten der Regulatoren gesehen werden.

BEWEISHINWEIS Alles analog zu Gittern im Ganzheitsring. □

Im Falle der Ganzheitsbasis war eine untere Abschätzung für Diskriminante bekannt, nämlich $|\text{discr } K| \leq 1$.

Satz 3.6 (Friedman) Sei K ein algebraischer Zahlkörper. Dann gilt $\text{reg}(K) > 0.2$. (Ohne Beweis, siehe Algorithmische Zahlentheorie)

Bei Berechnung der Ganzheitsbasis gab es kostenlos ein linear unabhängiges System

$$1, \alpha, \dots, \alpha^{n-1}.$$

Hier ist das nicht gratis. Es gilt

$$\text{rang}(l(\sigma(\langle \varepsilon_1, \dots, \varepsilon_r \rangle))) = r \Leftrightarrow \text{reg}(\varepsilon_1, \dots, \varepsilon_r) \neq 0$$

(geometrisch; Volumen der Grundmasche).

Proposition Sei K ein algebraischer Zahlkörper, R eine Ordnung in K , Signatur (s, t) . Es gilt

$$\text{reg}(R) \leq C \cdot (\ln Q)^{s+t-1} \cdot N \leq C(\ln Q)^{s+t-1} \cdot \sum_{a=1}^{\lfloor Q \rfloor} a^r,$$

wobei

$$Q = \left(\frac{2}{\pi}\right)^t \sqrt{\text{discr}(R)} + 1,$$

$N =$ Anzahl nichtassoziierter Elemente von R der $|Norm| \leq Q$,

$C =$ Konstante, die nur von s und t abhängt,

$$n = s + 2t = [K : \mathbb{Q}].$$

Lemma Sei G ein Gitter in \mathbb{R}^n , X eine messbare Menge, sodass

$$\mathbb{R}^n \subseteq \bigcup_{g \in G} X + g.$$

Dann gilt

$$d(G) \leq \lambda(X).$$

BEWEIS Sei M die Grundmasche von G . Es gilt

$$\begin{aligned} d(G) &= \lambda(M) = \lambda(M \cap \mathbb{R}^n) = \lambda\left(M \cap \bigcup_{g \in G} X + g\right) = \lambda\left(\bigcup_{g \in G} (M \cap (X + g))\right) \\ &\leq \sum_{g \in G} \lambda(M \cap (X + g)) = \sum_{g \in G} \lambda((M - g) \cap X) = \lambda\left(\underbrace{\bigcup_{g \in G} (M - g) \cap X}_{\mathbb{R}^n}\right) \\ &= \lambda(\mathbb{R}^n \cap X) = \lambda(X). \end{aligned} \quad \blacksquare$$

BEWEIS (der Proposition) Mit den Bezeichnungen des Beweises des Dirichletschen Einheitsensatzes.

$$S \subseteq \bigcup_{\varepsilon \in \mathcal{E}(R)} X \cdot \sigma(\varepsilon) \tag{3.1}$$

$$X = S \cap \left(\bigcup_{j=1}^n X_0 \cdot \sigma(\alpha_j)^{-1}\right) \tag{3.2}$$

$$X_0 = \{x \mid |x_1| < c_1, \dots, |x_s| < c_s, |x_{s+1}^2| < c_{s+1}, \dots, |x_{s+t}^2| < c_{s+t}\} \tag{3.3}$$

und

$$c_1 \cdots c_{s+t} = \left(\frac{4}{\pi}\right)^t d(\sigma(G)) + 1 = Q$$

(hier = und +1 statt \geq).

3 Struktur der Einheitengruppe

l -e („logarithmiere“) (3.1) und erhalte

$$L \subseteq \sum_{\varepsilon \in \mathcal{E}(R)} (l(X) + l(\sigma(\varepsilon))).$$

Aus dem Lemma folgt

$$\sqrt{s+t} \operatorname{reg}(R) = d(L) \leq \lambda(l(X)) \stackrel{(3.2)}{\leq} \sum_{j=1}^m \lambda(\underbrace{l(X_0) - l(\sigma(\alpha_j))}_{U_j} \cap L) = m \cdot \lambda(l(X_0)).$$

Weiters gilt

$$z \in U_j \iff \begin{cases} z_1 + \dots + z_{s+t} = 0 \\ z_i < e^{c_i} - d_i \log |\sigma_i(\alpha_j)| \end{cases}$$

„Nebenrechnung“:

$$\begin{aligned} x \in X_0 &\iff |x_i|^{d_i} < c_i \\ z \in l(X_0) &\iff z < \log(c_i) \\ z \in l(X_0) - l(\sigma(\alpha_j)) &\iff z_i < \log(c_i) - d_i \log |\sigma_i(\alpha_j)| \end{aligned}$$

Koordinatentransformation („Shift“, ändere nicht das Volumen):

$$z_i^* := z_i - \log(c_i) + d_i \log |\sigma_i(\alpha_j)| + \frac{1}{s+t} \log \frac{Q}{|\mathbb{N}(\alpha_j)|}.$$

Also ist die Summe

$$z_1^+ \dots + z_{s+t}^* = -\log Q + \log |\mathbb{N}(\alpha_j)| + \log \frac{Q}{|\mathbb{N}(\alpha_j)|} = 0.$$

Somit

$$z_i^* < \frac{1}{s+t} \log \frac{Q}{|\mathbb{N}(\alpha_j)|} \leq \frac{1}{s+t} \log Q$$

(weil die Norm größer/gleich als 1 ist). Das Volumen dieses Bereichs ist

$$\lambda(\dots) = \left(\frac{1}{s+t} \log Q \right)^{s+t-1} \cdot \underbrace{\lambda(\{z \mid z_1 + \dots + z_{s+t} = 0, z_j < 1\})}_{\text{nur von } s+t \text{ abhängige Konstante} =: C \text{ (Integrationsaufgabe!)}}.$$

Insgesamt haben wir also

$$\operatorname{reg} \leq \frac{1}{\sqrt{s+t}} \cdot m \cdot \left(\frac{1}{s+t} \right)^{s+t-1} \cdot C \cdot (\log Q)^{s+t-1}. \quad \blacksquare$$

3.5 Berechenbarkeit von Fundamenteinheiten

Lemma Sei K ein algebraischer Zahlkörper, G ein vollständiges Gitter in K . Dann können alle Elemente α aus G mit

$$|\sigma_1(\alpha)| < c_1, \dots, |\sigma_n(\alpha)| < c_n$$

berechnet werden.

BEWEIS Sei $\omega_1, \dots, \omega_n$ eine Basis von G und $\omega_1^*, \dots, \omega_n^*$ die entsprechende duale Basis, also

$$\text{tr}(\omega_i \omega_j^*) = [i = j].$$

$\alpha = \sum a_j \omega_j$, somit

$$\text{tr}(\alpha \omega_i^*) = \sum a_j \text{tr}(\omega_j \omega_i^*) = a_i$$

und

$$|a_i| = |\text{tr}(\alpha \omega_i^*)| = \left| \sum_{j=1}^n \sigma_j(\alpha) \sigma_j(\omega_i^*) \right| \leq \sum_{j=1}^n c_j |\sigma_j(\omega_i^*)|.$$

■

3 Struktur der Einheitengruppe

Sätze

Satz 1.6	Struktur des ganzen Abschlusses über HIB	6
Satz 1.7	11
Satz 1.8	12
Satz 2.1	21
Satz 2.3	26
Satz 2.4	28
Satz 2.5	Endlichkeit der Klassenzahl	31
Satz 3.1	35
Satz 3.2	39
Satz 3.3	Minkowskischer Gitterpunktsatz	42
Satz 3.4	43
Satz 3.5	Dirichletscher Einheitsensatz	43
Satz 3.6	Friedman	48

Index

Fundamenteinheiten, 46

Pellsche Gleichung, 46

zentralsymmetrisch, 42