Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

19.Vorlesung

10 Juli 2017

Beweis vom Hilfslemma am Ende der 18.Vorlesung. Sei $0 \neq \beta \in D$. Da β algebraisch über k ist, ist $k[\beta]$ ein endlichdimensionaler K-Vektorraum. Die Abbildung $\begin{array}{ccc} k[\beta] & \to & k[\beta] \\ x & \mapsto & \beta x \end{array}$ ist linear und injektiv (weil D ein Integritätsbereich ist), also folgt aus LA: Die Abbildung ist surjektiv. Insbesondere gibt es $\beta' \in k[\beta]$, so daß $\beta\beta' = 1 \in k[\beta]$

□

Notation und Terminologie
Zusammenfassung: Gebrochene Ideale in einem Dedekindbereich.
Sei R ein Dedekindbereich, $K :=$ Quot(R). Die Menge Id(R) der $\neq 0$ gebrochenen Ideale von R ist eine abelsche Gruppe, sie enthält die Untergruppe $H(R)$ der gebrochenen Hauptideale. Die Faktorgruppe $\mathcal{K}l(R) :=$ Id$(R)/H(R)$ heißt die Ideal Klassengruppe von R. Ihre Ordnung $|\mathcal{K}l(R)|$ heißt die Klassenzahl von R.

Proposition 19.1
Ein Dedekindbereich ist genau dann faktoriell, wenn es ein Hauptidealbereich ist (d.h.: Ein Dedekindbereich hat Klassenzahl = 1 genau dann, wenn er faktoriell ist).

Beweis. Sei R ein Dedekindbereich.
„⇐“ Jedes HIR ist faktoriell.
„⇒“ Sei nun R faktoriell; es genügt zu zeigen, daß jedes $\neq 0$ Primideal $\mathfrak{p}$ ein Hauptideal ist (da jedes Ideal ein Produkt von Primidealen ist, und das Produkt von Hauptidealen ein Hauptideal ist). Sei $0 \neq a \in \mathfrak{p}$; dann ist a ein Produkt von irreduziblen Elementen. Da $\mathfrak{p}$ ein Primideal ist, enthält $\mathfrak{p}$ ein Primfaktor π von a. Nun folgt aus $\mathfrak{p} \supseteq < \pi >$, daß $\mathfrak{p} = < \pi >$, weil $< \pi >$ ein Primideal, also ein Maximalideal ist (R ist Dedekind). □

Zusatz: Sei R ein Dedekindbereich. Jedes $\neq 0$ gebrochenes Ideal hat eine eindeutige Faktorisierung als Produkt von ganzen Potenzen von Primidealen.

Beweis. Sei $\mathfrak{a}$ ein gebrochenes Ideal und $d \neq 0$, $d \in R$, so daß $d\mathfrak{a} \lhd R$. Schreibe eindeutig
$d\mathfrak{a} = p_1^{r_1} \dots p_m^{r_m}$, p_i Primideal, $r_i \in \mathbb{N}_0$,
$< d >= p_1^{s_1} \dots p_m^{s_m}$, $s_i \in \mathbb{N}_0$. Dann ist $\mathfrak{a} = \prod_{i=1}^m p_i^{r_i - s_i}$, $r_i - s_i \in \mathbb{Z}$. □

Kapitel 5: Die Klassenzahl eines Zahlkörpers

§Gitter in $\mathbb{R}^n$

Definition 19.1 (i) Sei $\{e_1, \ldots, e_m\}$ linear unabhängig in $\mathbb{R}^n$ (also $m \leq n$). Die von $\{e_1, \ldots, e_m\}$ erzeugte additive Gruppe Γ ist ein Gitter der Dimension m. D.h.: $\Gamma := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_m$ (freie abelsche Gruppe vom Rang m).

Wenn $m = n$ heißt Γ vollständiges Gitter
Bezeichnung: $||x||$ ist die euklisdische Norm für $x \in \mathbb{R}^n$.

(ii) $X \subseteq \mathbb{R}^n$ ist beschränkt, wenn es ein $r \in \mathbb{R}_+$ gibt, so daß $X \subseteq B_r(0)$:=die Kugel mit Zentrum 0 und Radius r.

(iii) $X \subseteq \mathbb{R}^n$ ist diskret, wenn $|B_r(0) \cap X| < \infty$ für alle $r \in \mathbb{R}_+$.

Satz 19.1
Eine additive Untergruppe Γ von $(\mathbb{R}^n, +)$ ist genau dann ein Gitter, wenn Γ diskret ist.

Beweis. „$\Rightarrow$“ o.E. ist Γ vollständig. Sei $\{e_1, \ldots, e_n\}$ eine Basis für $\mathbb{R}^n$, die Γ erzeugt, und $v \in \mathbb{R}^n$. Es gibt $\lambda_i \in \mathbb{R}$, so daß $v = \sum_{i=1}^n \lambda_i e_i$.
Definiere:

$$\begin{array}{lccc} f & : \mathbb{R}^n & \to & \mathbb{R}^n \\ & f(\sum \lambda_i e_i) & \mapsto & (\lambda_1, \ldots, \lambda_n) \end{array}$$

Es ist : $f(B_r(0))$ ist beschränkt, d.h. es existiert k, so daß $||f(v)|| \leq k \quad \forall v \in B_r(0)$.
Wenn $v = \sum_{i=1}^n a_i e_i \in \Gamma \cap B_r(0)$ $(a_i \in \mathbb{Z})$, dann ist $||(a_1, \ldots, a_n)|| \leq k$. Es folgt:

$$(*) \qquad |a_i| \leq k \quad \forall i = 1, \ldots, n$$

Wir sehen, daß die Anzahl von $a \in \mathbb{Z}$, die $(*)$ erfüllen können, endlich ist, also ist $\Gamma \cap B_r(0)$ endlich.
„$\Leftarrow$“ Wir zeigen per Induktion nach n, daß Γ ein Gitter ist. Sei $\{g_1, \ldots, g_m\}$ eine maximal linear unabhängige Untermenge von Γ und setze $V := \text{Span}_{\mathbb{R}}\{g_1, \ldots, g_{m-1}\}$. Betrachte $\Gamma_0 := \Gamma \cap V$. Dann ist Γ_0 immernoch diskret und per Induktionsannahme ein Gitter. Seien $\{h_1, \ldots, h_{m'}\}$ eine linear unabhängige Menge, die Γ_0 erzeugt. Da $g_1, \ldots, g_{m-1} \in \Gamma_0$, muss $m' = m - 1$ gelten. Wir können $\{g_1, \ldots, g_{m-1}\}$ durch $\{h_1, \ldots, h_{m-1}\}$ erzetzen. (D.h.: wir können o.E. annehmen: jedes Element aus Γ_0 ist eine $\mathbb{Z}$-lineare Kombination der g_i).
Betrachte nun die Untermenge von Γ:
$T := \{x \in \Gamma \mid x = \sum_{i=1}^m a_i g_i, a_i \in \mathbb{R}, 0 \leq a_i < 1, i = 1, \ldots, m-1 \text{ und } 0 \leq a_m \leq 1\}$.
T ist beschränkt (also endlich, da Γ diskret ist). Wähle $x' \in T, x' = \sum_{i=1}^m b_i g_i$ mit b_m kleinste $\neq 0$ Koeffizient von g_m.

Behauptung: $\{g_1, \ldots, g_{m-1}, x'\}$ erzeugt Γ (über $\mathbb{Z}$)

Beweis. Es ist klar, daß diese Menge immernoch linear unabhängig ist. Außerdem: für $g \in \Gamma$ gibt es $c_i \in \mathbb{Z}$ $(\lfloor b_i \rfloor \in \mathbb{Z})$, so daß $g' = g - c_m x' - \sum_{i=1}^{m-1} c_i g_i \in T$, und der Koeffizient von g_m in g' ist ≥ 0 aber kleiner als b_m. Aus der Wahl von x' gilt nun: dieser Koeffizient ist 0, also ist $g' \in \Gamma_0$. $\square$

□

Definition 19.2
Sei Γ ein Gitter mit erzeugender Menge $\{e_1, \ldots, e_n\}$.
$T := \{x \in \mathbb{R}^n \mid x = \sum a_i e_i, 0 \leq a_i < 1, a_i \in \mathbb{R}\}$ heißt fundamentaler Parallelotop von Γ.