Algebraische Zahlentheorie.

SS 2013

Kuhlmann

19. Vorlesung am 27.06.2013.

Beweis vom Hilfslemma am Ende der 18. Vorlesung.

Sei $0 \neq \beta \in D$. Da β alg. über k ist, ist $k[\beta]$ endl. dim. k-VR.

Die Abbildung $k[\beta] \longrightarrow k[\beta]$, $x \longmapsto \beta x$

ist linear und injektiv (weil D Integritätsbereich ist), also aus LA folgt: die Abbildung ist surjektiv. Insbesondere $\exists \beta' \in k[\beta]$ so daß $\beta\beta' = 1 \in k[\beta]$. ∎

Notation und Terminologie

Zusammenfassung: Gebrochene Ideale in einem Dedekindbereich.

Sei R ein Dedekindbereich, $K = \mathrm{Quot}(R)$, die Menge der $\neq 0$ gebrochene Ideale von R $\mathrm{Id}(R)$ ist eine abelsche Gruppe, sie enthält die

Untergruppe $H(R)$ der gebrochenen Hauptideale.

Die Faktorgruppe $Kl(R) := Id(R)/H(R)$

heißt die Ideal Klassengruppe von R.

Ihre Ordnung $|Kl(R)|$ heißt die

Klassenzahl von R.

Proposition 1. Ein Dedekindbereich ist: Faktoriell

$\Leftrightarrow$ er ist ein Hauptidealbereich.

(D.h. ein Dedekindbereich hat Klassenzahl

$= 1$ genau dann wenn er Faktoriell ist.)

Beweis. Sei R Dedekindbereich.

"$\Leftarrow$" Jedes HIR ist Faktoriell. ✓

"$\Rightarrow$" Sei nun R Faktoriell; es genügt z.Z. daß

jedes $0 \neq$ Primideal $\mathfrak{p}$ Hauptideal ist

(da jedes Ideal Produkt von Primidealen ist,

und das Produkt von Hauptidealen ist Hauptideal).

Sei $0 \neq a \in \mathfrak{p}$; dann ist a Produkt von irreduziblen Elementen. Da $\mathfrak{p}$ Primideal ist enthält $\mathfrak{p}$ ein Primfaktor π von a. Nun folgt aus $\mathfrak{p} \supseteq \langle \pi \rangle$ daß $\mathfrak{p} = \langle \pi \rangle$ weil $\langle \pi \rangle$ Primideal also Maximalideal ist (R ist Dedekind). ∎

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

Beweis: Sei $\mathfrak{a}$ gebrochenes Ideal; und $d \neq 0$, $d \in R$ so daß $d\mathfrak{a} \trianglelefteq R$.

Schreibe eindeutig

$$d\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} \qquad \mathfrak{p}_i \text{ Primideale}, \; r_i \in \mathbb{N}_0$$

und

$$\langle d \rangle = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} \qquad s_i \in \mathbb{N}_0$$

Dann ist $\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i^{(r_i - s_i)}$; $(r_i - s_i) \in \mathbb{Z}$. ∎

Kapitel IV Die Klassenzahl eines Zahlkörpers.

§ Gitter in $\mathbb{R}^n$.

Definition 1 (i) Sei $\{e_1, \dots, e_m\}$ linear unabhängig in $\mathbb{R}^n$ (so $m \leq n$), die additive Gruppe Γ erzeugt von $\{e_1, \dots, e_m\}$ ist ein Gitter der Dimension m.
[Wenn $n = m$ heißt Γ vollständiges Gitter].
D.h. $\Gamma := \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_m$ (freie abelsche Gruppe von Rang m).
Bezeichnung: $\|x\|$ ist die Euklidische Norm für $x \in \mathbb{R}^n$.
(ii) $X \subseteq \mathbb{R}^n$ ist beschränkt wenn es $\exists\ r \in \mathbb{R}_+$ s.d
$X \subseteq B_r(0) := $ die Kugel mit Zentrum 0 und Radius r.
(iii) $X \subseteq \mathbb{R}^n$ ist diskret $\Leftrightarrow |B_r(0) \cap X| < \infty$ für alle $r \in \mathbb{R}_+$

Satz 1. Eine additive Untergruppe Γ von $(\mathbb{R}^n, +)$ ist ein Gitter $\Leftrightarrow$ Γ diskret ist.

Beweis "$\Rightarrow$" $0 \in \Gamma$ ist vollständig. Sei $\{e_1, \dots, e_n\}$ 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 $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$
$f(\sum \lambda_i e_i) = (\lambda_1, \dots, \lambda_n)$

Es ist: $f(B_r(0))$ ist beschränkt i.e $\exists\ k$ so daß
$\|f(v)\| \leq k \quad \forall\ v \in B_r(0)$.

Wenn $v = \sum_{i=1}^{m} a_i e_i \in \Gamma \cap B_r(0)$ $(a_i \in \mathbb{Z})$ dann ist

$\| (a_1, \dots, a_m) \| \leq k$. Es folgt:

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

Wir sehen daß die Anzahl von $a \in \mathbb{Z}$ die $(*)$ erfüllen können ist endlich, so $\Gamma \cap B_r(0)$ ist endlich.

"$\Leftarrow$" Wir zeigen per Induktion nach n daß Γ ein Gitter ist.

Sei $\{g_1, \dots, g_m\}$ maximal lineair unabhängige Untermenge von Γ und setze $V := \operatorname{span}_{\mathbb{R}} \{g_1, \dots, g_{m-1}\}$

Betrachte $\Gamma_0 := \Gamma \cap V$. Dann ist Γ_0 immernoch diskret und per Induktionsannahme ein Gitter.

Seien $\{h_1, \dots, h_{m'}\}$ lineair unabhängige erzeugende für Γ_0.

Da $g_1, \dots, g_{m-1} \in \Gamma_0$ muss gelten $m' = m-1$, wir können $\{g_1, \dots, g_{m-1}\}$ durch $\{h_1, \dots, h_{m-1}\}$ ersetzen.

(D.h. Wir können OE annehmen: jedes Element aus Γ_0 ist $\mathbb{Z}$-lineare Kombination der g_i).

Betrachte nun die Untermenge von Γ:

$$T := \{ x \in \Gamma \mid x = \sum_{i=1}^{m} a_i g_i \,,\ a_i \in \mathbb{R},$$

$$0 \leq a_i < 1 \quad i = 1, \dots, m-1 \text{ und } \quad 0 \leq a_m \leq 1 \}$$

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 $\neq 0$ Koefficient von g_m

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

Es ist klar daß diese Menge immernoch linear unabhängig ist.

Außerdem: für $g \in \Gamma$ $\exists\, c_i \in \mathbb{Z}$ $\left(\lfloor b_i \rfloor \in \mathbb{Z} \right)$

So daß $$g' = g - c_m x' - \sum_{i=1}^{m-1} c_i g_i \quad \in T$$

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 $g' \in \Gamma_0$. ∎

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