B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

21.Vorlesung

01. Juli 2021

In diesem Skript werden wir Gitter und Ihre fundamentale Parallelotope untersuchen und den Satz von Minkowski 21.8 beweisen. Den Satz werden wir ab Skript 22 aufrufen, um die Endlichkeit der Klassenzahl zu beweisen.

Das folgende Lemma 21.1 erklärt die Rolle von fundamentale Parallelotope (f.P.) T.

Lemma 21.1
Sei Γ ein Gitter, T f.P von Γ. Es gilt: $\forall v \in \mathbb{R}^n, \exists! l \in \Gamma$, so daß $v \in T + l$

Beweis. Sei $\{e_1, \ldots, e_n\}$ eine Basis von $\mathbb{R}^n$ die Γ erzeugt und sei $v \in \mathbb{R}^n$. Schreibe

$$v = \sum b_i e_i \text{ mit } b_i \in \mathbb{R}$$

und setze

$$z_i := \lfloor b_i \rfloor \in \mathbb{Z} .$$

Dann ist

$$a_i := b_i - z_i \in \mathbb{R} \text{ und } 0 \leq a_i < 1 .$$

Es ist $v = t + l$, wobei $t := \sum a_i e_i \in T$ und $l := \sum z_i e_i, l \in \Gamma$. □

Satz 21.2
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 geordnete Basis für $\mathbb{R}^n$, die Γ erzeugt, und $v \in \mathbb{R}^n$. Es gibt $\lambda_i \in \mathbb{R}$, so daß $v = \sum_{i=1}^n \lambda_i e_i$.
Betrachte:

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

Es ist klar daß : $f(B_r(0))$ ist beschränkt (ÜA), 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

$$V := \ \mathrm{Span}_{\mathbb{R}}\{g_1, \ldots, g_{m-1}\}\,.$$

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. Das heißt: 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:

$$T := \{x \in \Gamma \mid x = \sum_{i=1}^{m} a_i g_i, a_i \in \mathbb{R}, 0 \leq a_i < 1, i = 1, \ldots, m-1 \text{ und } 0 \leq a_m \leq 1\}\,.$$

Es ist: T ist beschränkt (ÜA). Also ist T endlich, da Γ diskret ist.

• Wähle also $x' \in T, x' = \sum_{i=1}^{m} b_i g_i$ mit b_m kleinste $\neq 0$ Koeffizient von g_m.

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

Beweis. Es ist klar, daß diese Menge immernoch linear unabhängig ist (ÜA). 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 (vgl. Lemma 1). Aus der Wahl von x' gilt nun: dieser Koeffizient ist 0, also ist $g' \in \Gamma_0$. □

□

Wir studieren nun die Faktorgruppe $(\mathbb{R}^n, +)/(\Gamma, +)$.

• Wir fangen an mit dem Fall $n = 1$. Setze

$$S := \{z \in \mathbb{C} \mid |z| = 1\}\,.$$

S ist eine multiplikative Untergruppe von $\mathbb{C}$.
Erinnerung: $i = \sqrt{-1} \in \mathbb{C}$.

Lemma 21.3
$(\mathbb{R}, +)/(\mathbb{Z}, +) \cong (S, \times)$.

Beweis. Betrachte die surjektive Abbildung

$$\begin{array}{rccc} \phi: & \mathbb{R} & \to & S \\ & a & \mapsto & e^{2ia\pi} \end{array}$$

ϕ ist ein Homomorphismus und $\ker(\phi) = (\mathbb{Z}, +)$ (ÜA). □

• Allgemeiner für $n \in \mathbb{N}$ setze

$$\mathbb{T}^n := \underbrace{S \times S \times \ldots S}_{n \text{ mal}}$$

(der n-dimensionaler Torus).

Satz 21.4
Sei Γ ein vollständiges Gitter in $\mathbb{R}^n$, dann ist $(\mathbb{R}^n\,, +)/(\Gamma\,, +) \cong (\mathbb{T}^n\,, \times)$.

Beweis. Sei $\{e_1, \ldots, e_n\}$ eine Basis für Γ und betrachte $\phi : (\mathbb{R}^n\,, +) \to (\mathbb{T}^n\,, \times)$ definiert durch $\phi(\sum a_i e_i) = (e^{2ia_1\pi}, \ldots, e^{2ia_n\pi})$. ϕ ist surjektiver Homomorphismus mit $\ker(\phi) = \Gamma$. (ÜA). □

Lemma 21.5
$\phi_{|T} : T \to \mathbb{T}^n$ ist injektiv.

Beweis. Aus $\exp(2ia_j\pi) = \exp(2ib_j\pi)$ (für $0 \le a_j < 1$, $0 \le b_j < 1$) folgt $a_j = b_j$ □

Allgemeiner gilt für beliebige Gitter

Satz 21.6
Sei $\Gamma \subseteq \mathbb{R}^n$ ein m-dimensionales Gitter (also $m \le n$), dann ist $\mathbb{R}^n/\Gamma \cong \mathbb{T}^m \times \mathbb{R}^{n-m}$.

Beweis. Setze $V :=$ $\mathrm{Span}_{\mathbb{R}}(\Gamma)$ und $W \subseteq \mathbb{R}^n$, so daß $\mathbb{R}^n = V \bigoplus W$; dann ist
$\mathbb{R}^n = V \bigoplus W \underset{\text{Satz 21.4}}{\cong} \mathbb{T}^m \times \mathbb{R}^{n-m}$ □

Definition 21.1 (i) Sei $X \subseteq \mathbb{R}^n$ Lebesgue-meßbar. Definiere $v(X) = \int_X dx_1 \dots dx_n$ das Volumen von X (Lebesgue-Maß von X).

(ii) Sei $\Gamma \subseteq \mathbb{R}^n$ ein vollständiges Gitter, $X \subseteq \mathbb{T}^n$, und $\phi := \phi_{|T}$ wie im Lemma 21.5. Definiere das Volumen von X: $v(X) := v(\phi^{-1}(X))$

(iii) Ist $Y \subseteq T$, so ist $\phi(Y) \subseteq \mathbb{T}^n$ und $v(\phi(Y)) = v(Y)$.

Satz 21.7
Sei $X \subseteq \mathbb{R}^n$ beschränkt, so daß $v(X)$ existiert (d.h. X ist beschränkt und Lebesgues-meßbar). Aus $v(\phi(X)) \neq v(X)$ folgt, daß $\phi_{|X}$ nicht injektiv ist.

Beweis. Sei X beschränkt und $\phi_{|X}$ injektiv. Es existieren $l_1, \dots, l_s \in \Gamma$, so daß $l_i \neq l_j$ für $j \neq i$ und $X_{l_j} := X \cap (T + l_j) \neq \varnothing \quad \forall j = 1, \dots, s$. Also $X = \bigsqcup_{j=1}^s X_{l_j}$ (folgt aus Lemma 1, ÜA). Für $j = 1, \dots, s$, definiere $Y_{l_j} = X_{l_j} - l_j$, so daß $Y_{l_j} \subseteq T \subseteq \mathbb{R}^n$. Bemerke, daß die Y_{l_j} disjunkt sind (da $\phi_{|X}$ injektiv ist). Außerdem gelten:

(a) $v(Y_{l_j}) = v(X_{l_j})$ (weil das Lebesgue-Maß invariant unter Translation ist).

(b) $\phi(X_{l_j}) = \phi(Y_{l_j})$ (weil $\Gamma = \ker \phi$).

(c) $v(\phi(Y_{l_j})) = v(Y_{l_j})$ (da $Y_{l_j} \subseteq T$).

Wir berechnen nun

$$v(\phi(X)) = v(\phi(\bigsqcup_j X_{l_j})) \underset{(b),(c)}{=} v(\bigsqcup_j Y_{l_j}) = \sum_j v(Y_{l_j}) \underset{(a)}{=} \sum_j v(X_{l_j}) = v(X)\,.$$

□

Definition 21.2 (i) $X \subseteq \mathbb{R}^n$ ist <u>konvex</u>, wenn $\forall x, y \in X$ und $\forall \lambda \in \mathbb{R}$ mit $0 \le \lambda \le 1$ gilt $\lambda x + (1-\lambda)y \in X$.

(ii) X ist <u>symmetrisch</u>, wenn gilt: $x \in X \Rightarrow -x \in X$.

Satz 21.8 (Minkowski)
Sei Γ ein vollständiges Gitter in $\mathbb{R}^n$ mit f.P. T und sei $X \subseteq \mathbb{R}^n$ beschränkt, symmetrisch, konvex (und Lebesgue-meßbar). Wenn $v(X) > 2^n v(T)$, gilt dann: $\exists \gamma \neq 0, \gamma \in \Gamma \cap X$.

Bemerkung
Da Γ diskret ist, gibt es nur endlich viele solche γ.

Beweis. Betrachte, das Gitter 2Γ mit f.P $2T$ und Volumen $v(2T) = 2^n v(T)$. Betrachte den Torus $\mathbb{T}^n = \mathbb{R}^n/2\Gamma$.
Berechne $v(\mathbb{T}^n) = v(2T) = 2^n v(T)$. Für $\phi : \mathbb{R}^n \to \mathbb{T}^n$ ist $\ker \phi = 2\Gamma$ und $\phi(X) \subseteq \mathbb{T}^n$, also

$$v(\phi(X)) \le v(\mathbb{T}^n) = 2^n v(T) < v(X)\,.$$

Aus Satz 21.7 folgt: $\phi_{|X}$ ist nicht injektiv. Also $\exists x_1 \neq x_2$, $x_1, x_2 \in X$, so daß $\phi(x_1) = \phi(x_2)$ oder $(x_1 - x_2) \in \ker \phi$, d.h. $x_1 - x_2 \in 2\Gamma$. Also $\frac{1}{2}(x_1 - x_2) \in \Gamma$. Nun $x_2 \in X \Rightarrow -x_2 \in X$ und $\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X$, d.h. $\frac{1}{2}(x_1 - x_2) \in X$. □