Basen

Vortrag zum Seminar „Elliptische Funktionen und elliptische Kurven“, 30.10.2005

Dalong Qu

§ 1 Jacobis-Zugang

Ziel des Abschnitts.
(1) Wir zeigen mit der KRONECKER-Approximation das Lemma von JACOBI. Dieses besagt, dass eine diskrete Untergruppe Ω von $\mathbb{C}$ höchstens zwei über $\mathbb{R}$ linear unabhängige Elemente haben kann.
(2) Weiterhin ergibt sich, dass eine diskrete Untergruppe Ω von $\mathbb{C}$ mit zwei über $\mathbb{R}$ linear unabhängigen Elementen ω_1, ω_2 bereits ein Gitter in $\mathbb{C}$ ist. □

(1.1) KRONECKER-Approximation.
Zu jeder positiven ganzen Zahl N und $\omega_1, \omega_2, \omega_3 \in \mathbb{C}$ gibt es $(m_1, m_2, m_3) \in \mathbb{Z}^3 \setminus \{0,0,0\}$, so dass gilt:

$$0 \leq |m_1|, |m_2|, |m_3| \leq N \tag{1}$$

$$|m_1\omega_1 + m_2\omega_2 + m_3\omega_3| < \frac{6\sqrt{2}}{\sqrt{N}} \cdot max\{|\omega_1|, |\omega_2|, |\omega_3|\}. \tag{2}$$

◇

Beweis.
Seien $N \in \mathbb{N}$ und $\omega_1, \omega_2, \omega_3 \in \mathbb{C}$.
Wir definieren

$$M := max\{|\omega_1|, |\omega_2|, |\omega_3|\} \; und \; m = (m_1, m_2, m_3), \; \omega = (\omega_1, \omega_2, \omega_3)$$

$$\langle \, m, \, \omega \rangle := m_1\omega_1 + m_2\omega_2 + m_3\omega_3$$

Weiterhin bezeichnen wir das achsenparallele Quadrat in $\mathbb{C}$ mit Mittelpunkt 0 und Kantenlänge 2K mit Q(K), also

$$Q(K) := \{z \in \mathbb{C};\ |Re\, z| \leq K, |Im\, z| \leq K\}.$$

1. Behauptung:
Für alle $m = (m_1, m_2, m_3)^t \in \mathbb{Z}^3$ mit

$$0 \leq m_1, m_2, m_3 \leq N \tag{3}$$

gilt

$$\langle m, \omega \rangle \in Q(T) \; mit \; T := 3MN$$

.

Beweis.
Mit der Definition von $\langle m, \omega \rangle$ ergibt sich

$$\begin{aligned}
|\langle m, \omega \rangle| &= |m_1\omega_1 + m_2\omega_2 + m_3\omega_3| \\
&\underset{\text{Dreiecksugl.}}{\leq} |m_1\omega_1| + |m_2\omega_2| + |m_3\omega_3| \\
&= |m_1||\omega_1| + |m_2||\omega_2| + |m_3||\omega_3| \\
&\underset{|\omega_j| \leq M, |m_j| \leq N}{\leq} NM + NM + NM \\
&= 3MN
\end{aligned}$$

□

Die Kanten von Q(T) werden nun in t gleiche Teile geteilt. Damit erhält man eine Zerlegung von Q(T) in t^2 Quadrate der Kantenlänge 2T/t.

2. Behauptung:
Die Anzahl der $m \in \mathbb{Z}^3$ mit (3) ist $(N+1)^3$.

Beweis.
Da $0 \leq m_1, m_2, m_3 \leq N$, kann man m_1, m_2, m_3 jeweils von 0 bis N wählen, also jeweils (N+1) Möglichkeiten. Daher ist die Anzahl der $m = (m_1, m_2, m_3) \in \mathbb{Z}^3$ gerade $(N+1)^3$. □

Nach dem DIRICHLETschen Schubfachschluss liegen in Fall $(N+1)^3 > t^2$ wenigstens zwei verschiedene Punkte $\langle m', \omega \rangle \; und \; \langle m'', \omega \rangle$ in einem Quadrat der Kantenlänge 2T/t. Damit erhält man durch Differenzbildung ein $0 \neq m \in \mathbb{Z}^3$ mit (1), denn:

Seien $m' = (m_1', m_2', m_3') \in \mathbb{Z}^3$, $0 \leq m_1', m_2', m_3{}' \leq N$ und
$m'' = (m_1'', m_2'', m_3'') \in \mathbb{Z}^3$, $0 \leq m_1'', m_2'', m_3'' \leq N$, dann gilt

$$|m_1' - m_1''|, |m_2' - m_2''|, |m_3' - m_3''| \leq N$$

und $m = (m_1' - m_1'', m_2' - m_2'', m_3' - m_3'') \in \mathbb{Z}^3$, m≠(0,0,0), da $\langle m', \omega\rangle \neq \langle m', \omega\rangle$.
Weiterhin gilt $\langle m, \omega\rangle \in Q(2T/t)$. Daraus ergibt sich $|\langle m, \omega\rangle| \leq \sqrt{2} \cdot 2T/t$.

Wähle nun $t \in \mathbb{Z}$ mit

$$(N+1)^{3/2} > t \geq (N+1)^{3/2} - 1$$

Dann folgt

$$(N+1)^3 > t^2 \quad \text{und} \quad t \geq N^{3/2}.$$

Da, $|\langle m, \omega\rangle| \leq \sqrt{2} \cdot 2T/t \leq \sqrt{2} \cdot 2T/N^{3/2} \leq \sqrt{2} \cdot 2 \cdot 3MN/N^{3/2} = 6\sqrt{2}M/\sqrt{N}$,
erhalten wir (2). □

Wir kommen nun zum angekündigten

(1.2) Lemma von JACOBI.
Ist Ω eine diskrete Untergruppe von (ℂ;+) und sind $\omega_1, \omega_2, \omega_3 \in \Omega$ gegeben, dann gibt es $m_1, m_2, m_3 \in \mathbb{Z}$,nicht alle Null, so dass $m_1\omega_1 + m_2\omega_2 + m_3\omega_3 = 0$. ◇

Beweis.
$\Omega \leqslant (\mathbb{C}, +)$ diskret
$\Rightarrow \sharp\{z \in \Omega; |z| \leq \rho\} < \infty \quad \forall \rho > 0$
$\Longrightarrow \exists \tilde{\rho} > 0 \; mit \; \sharp\{z \in \Omega; |z| \leq \tilde{\rho}\}\backslash\{0\} = 0 \; und \; |\omega| > \tilde{\rho} \quad \forall \omega \in \Omega\backslash\{0\} \qquad (*)$
Seien $\omega_1, \omega_2, \omega_3 \in \Omega$ paarweise verschieden und $\neq 0$ (sonst klar)
Wähle N so gross, dass $\frac{6\sqrt{2}}{\sqrt{N}} \cdot \; max\{|\omega_1|, |\omega_2|, |\omega_3|\} \leq \tilde{\rho}$
$\overset{\text{Kron. Appr.}}{\Longrightarrow} \exists (m_1, m_2, m_3) \in \mathbb{Z}^3\backslash\{(0,0,0)\}$ mit
$|m_1\omega_1 + m_2\omega_2 + m_3\omega_3| < \frac{6\sqrt{2}}{\sqrt{N}} \cdot \; max\{|\omega_1|, |\omega_2|, |\omega_3|\} \overset{\text{Wahl von N}}{\leq} \tilde{\rho}$
$\overset{(*)}{\Longrightarrow} m_1\omega_1 + m_2\omega_2 + m_3\omega_3 = 0$ □

(1.3) Lemma
Sei Ω eine diskrete Untergruppe von ℂ und seien $\omega_1, \omega_2 \in \Omega$ linear unabhängig über ℝ, dann gilt

$$\Omega \; \subset \; \mathbb{Q}\omega_1 \; + \; \mathbb{Q}\omega_2$$

. ◇

Beweis.
Sei $\omega_3 \in \Omega$ beliebig, nach dem Lemma von JACOBI $\exists (m_1, m_2, m_3) \in \mathbb{Z}^3\backslash\{(0,0,0)\}$ mit $m_1\omega_1 + m_2\omega_2 + m_3\omega_3 = 0$. Dabei ist $m_3 \neq 0$ (Da sonst wegen der linearen Unabhängigkeit von ω_1, ω_2 auch $m_1 = m_2 = 0$ folgen würde, also ein Widerspruch zu $(m_1, m_2, m_3) \neq (0,0,0)$)

$$\Longrightarrow \; \omega_3 = \frac{-m_1}{m_3}\omega_1 + \frac{-m_2}{m_3}\omega_2 \in \mathbb{Q}\omega_1 \; + \; \mathbb{Q}\omega_2,$$

also $\Omega \subset \mathbb{Q}\omega_1 + \mathbb{Q}\omega_2$. □

Wir erhalten mit dem Lemma eine weitere Verschäfung der Aussage.

(1.4) Proposition.
Es gibt $N \in \mathbb{N}$ mit $\Omega \subset \frac{1}{N}(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$. ◇

Beweis.
Andernfalls würde es $\omega \in \Omega$ nach (1) mit beliebig grossem Nenner geben, d.h., man hätte

$$0 \neq \omega_k' = \frac{1}{N_k}(r_k\omega_1 + s_k\omega_2) \in \Omega\,,\ k \in \mathbb{N},$$

mit ganzen r_k, s_k, N_k, $ggT(r_k, s_k, N_k) = 1$ *und* $N_k \to \infty$ für $k \to \infty$.
Sei O.B.d.A. $0 \leqslant r_k, s_k \leqslant N_k$
(Da, wenn $r_k, s_k > N_k$, dann gibt es $m, n, r_k', s_k' \in \mathbb{Z}$ mit $r_k' = r_k + mN_k$, $s_k' = s_k + nN_k$, so dass $0 \leqslant r_k', s_k' \leqslant N_k$ gilt. Dann setzt man $0 \neq \omega_k' = \frac{1}{N_k}(r_k'\omega_1 + s_k'\omega_2) \in \Omega$, $k \in \mathbb{N}$)

Dann ergibt sich

$$|\omega_k'| \leq |\frac{1}{N_k}r_k\omega_1| + |\frac{1}{N_k}s_k\omega_2| = |\frac{1}{N_k}r_k||\omega_1| + |\frac{1}{N_k}s_k||\omega_2| \leqslant |\omega_1| + |\omega_2| \quad 0 \leqslant r_k, s_k \leqslant N_k.$$

Dann ist die Folge $(\omega_k')_{k\in\mathbb{N}}$ beschränkt in $\mathbb{C}$.
Nach dem Satz von BOLZANO-WEIERSTRASS hat $(\omega_k')_{k\in\mathbb{N}}$ daher einen Häufungspunkt in $\mathbb{C}$, was ein Widerspruch zu Ω diskret in $\mathbb{C}$ ist. □

(1.5) Bemerkung
Aus der Algebra ist bekommt, dass jede Untergruppe einer endlich erzeugten freien abelschen Gruppe selbst wieder frei ist. Nach der Proposition folgt
$\Omega \subset \frac{1}{N}(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ für ein $N \in \mathbb{N}$.Ω ist also eine Untergruppe einer freien Gruppe mit Rang 2, also auch frei. Wegen $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_1 \subset \Omega$ ist Ω eine freie Gruppe mit Rang 2 , also ein Gitter. ◇

Wir betrachten das folgende

(1.6) Beispiel
Man bestimme $m_1, m_2, m_3 \in \mathbb{Z}$, $(m_1, m_2, m_3) \neq (0, 0, 0)$, so dass

$$|m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| < 1 \tag{4}$$

und $m_1^2 + m_2^2 + m_3^2$ minimal unter der Bedingung (4) ist.

Lösung:
Seien $\omega_1 = \sqrt{2},\ \omega_2 = \sqrt{3} + i\sqrt{5},\ \omega_3 = i\sqrt{7} \Longrightarrow max\{|\omega_1|, |\omega_2|, |\omega_3|\} = 2\sqrt{2}$.
Sei N=24^2 , dann gilt nach (1.1)

$$\begin{aligned} |m_1\omega_1 + m_2\omega 2 + m_3\omega_3| &= |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| \\ &< \frac{6\sqrt{2}}{\sqrt{N}} max\{|\omega_1|, |\omega_2|, |\omega_3|\} \\ &= \frac{6\sqrt{2}}{\sqrt{24^2}} 2\sqrt{2} = 1 \end{aligned}$$

also gibt es $(m_1, m_2, m_3) \in \mathbb{Z}^3 \backslash \{(0,0,0)\}$ mit $|m_1|, |m_2|, |m_3| \leq N = 24^2$ und
$|m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| < 1$

Suche nun m_1, m_2, m_3, so dass $m_1^2 + m_2^2 + m_3^2$ minimal

$$\begin{aligned} |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| &= |(m_1\sqrt{2} + m_2\sqrt{3}) + (m_2\sqrt{5} + m_3\sqrt{7})i| \\ &= \sqrt{2m_1^2 + 8m_2^2 + 2m_1m_2\sqrt{6} + 7m_3^2 + 2m_2m_3\sqrt{35}} \end{aligned}$$

Falls $m_1 = 1, m_2 = -1, m_3 = 1$ oder $m_1 = -1, m_2 = 1, m_3 = -1$, dann gilt

$$|m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = \sqrt{17 - 2\sqrt{6} - 2\sqrt{35}} < 1$$

und

$$m_1^2 + m_2^2 + m_3^2 = 3$$

Gibt es $m_1, m_2, m_3 \in \mathbb{Z},\ (m_1, m_2, m_3) \neq (0,0,0)$, so dass
$m_1^2 + m_2^2 + m_3^2 = 2$ oder $m_1^2 + m_2^2 + m_3^2 = 1$?

Mögliche Fälle für $m_1^2 + m_2^2 + m_3^2 = 2$

$m_1 = 0, m_2 = \pm 1, m_3 = \pm 1 \ \Rightarrow\ |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = 15 \pm 2\sqrt{35} > 1$
$m_1 = \pm 1, m_2 = 0, m_3 = \pm 1 \ \Rightarrow\ |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = 9 > 1$
$m_1 = \pm 1, m_2 = \pm 1, m_3 = 0 \ \Rightarrow\ |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = 10 \pm 2\sqrt{6} > 1$

Mögliche Fälle für $m_1^2 + m_2^2 + m_3^2 = 1$

$m_1 = \pm 1, m_2 = 0, m_3 = 0 \ \Rightarrow\ |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = 2 > 1$
$m_1 = 0, m_2 = \pm 1, m_3 = 0 \ \Rightarrow\ |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = 8 > 1$

$m_1 = 0, m_2 = 0, m_3 = \pm 1 \Rightarrow |m_1\sqrt{2} + m_2(\sqrt{3} + i\sqrt{5}) + m_3 i\sqrt{7}| = 7 > 1$

Somit erfüllen $m_1 = 1, m_2 = -1, m_3 = 1$ oder $m_1 = -1, m_2 = 1, m_3 = -1$ die Bedingung und $m_1^2 + m_2^2 + m_3^2$ ist minimal. □

§ 2 Die Gruppe GL(2;ℤ)

Ziel des Abschnitts.
Wir untersuchen Eigenschaften der Gruppe GL(2;ℤ) und zeigen das Ergänzungs-Lemma. □

(2.1) Bemerkung
Die Menge

$$Mat(2;\mathbb{Z}) := \{U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a,\ b,\ c,\ d \in \mathbb{Z}\}$$

bildet bekanntlich bei Matrizen-Addition und -Multiplikation einen Ring mit Einselement

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Die Gruppe der Einheiten des Ringes Mat(2;ℤ) heisst allgemeine lineare Gruppe vom Grad 2 über ℤ und wird mit GL(2;ℤ) bezeichnet:

$$GL(2;\mathbb{Z}) := \{U \in Mat(2;\mathbb{Z});\ \exists\ V \in Mat(2;\mathbb{Z})\ mit\ UV = VU = E\}.$$

Wir betrachten den

(2.2) Äquivalenz-Satz.
Für $U \in Mat(2;\mathbb{Z})$ sind äquivalent:
(i) U ∈ GL(2;ℤ).
(ii) detU = ±1.
(iii) U ist invertierbar über ℚ und $U^{-1} \in Mat(2;\mathbb{Z})$.
(iv) Die Abbildung U: $\mathbb{Z}^2 \to \mathbb{Z}^2$, x↦Ux, ist bijektiv.
(v) Die Abbildung U: $\mathbb{Z}^2 \to \mathbb{Z}^2$, x↦Ux, ist surjektiv. ◇

Beweis.
(iii) ⟹ (i): Nach Definition von GL(2;ℤ).
(i) ⟹ (iv):
U ∈ GL(2;ℤ) ⇒ $\exists U^{-1} \in GL(2;\mathbb{Z})$ mit $UU^{-1} = U^{-1}U = E$

Def. $U^{-1}: \mathbb{Z}^2 \to \mathbb{Z}^2$, y$\mapsto U^{-1}y$, $\Rightarrow (U \circ U^{-1})(y) = y$ *und* $(U^{-1} \circ U)(x) = x$,
wobei x,y $\in \mathbb{Z}^2 \Rightarrow$ U bijektiv.

(iv) $\Longrightarrow$ (v): trivial.

(v) $\Longrightarrow$ (ii): Es gibt also u,v $\in \mathbb{Z}^2$ mit Uu = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und Uv = $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, also UV = E für V:= (u,v). Durch Determinantenbildung folgt

$$1 = detE = det(UV) = det(U) \cdot det(V)$$

$\Rightarrow$ (ii), da det(U)$\in \mathbb{Z}$ und det(V)$\in \mathbb{Z}$.
(ii) $\Longrightarrow$ (iii): Man verwendet die bekannte Darstellung der Inversen mit Hilfe der Adjunkten

$$U^{-1} = \frac{1}{detU} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \quad \text{für} \quad U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(2.3) Bemerkungen
a) Neben der Gruppe GL(2;$\mathbb{Z}$) betrachtet man noch deren Normalteiler

$$\mathrm{SL}(2;\mathbb{Z}) := \{U \in \mathrm{GL}(2;\mathbb{Z});\ \det U = 1\}$$

von GL(2;$\mathbb{Z}$), die sog. spezielle lineare Gruppe vom Grad 2 über $\mathbb{Z}$. Wegen

$$\mathrm{GL}(2;\mathbb{Z}) = \mathrm{SL}(2;\mathbb{Z}) \dot\cup (2;\mathbb{Z}) \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

hat SL(2,$\mathbb{Z}$) den Index 2 in GL(2,$\mathbb{Z}$). ◇

Behauptung.
$\mathrm{SL}(2;\mathbb{Z}) := \{U \in \mathrm{GL}(2;\mathbb{Z}); \det U = 1\}$ ist Normalteiler von $\mathrm{GL}(2;\mathbb{Z})$ □

Beweis.
Seien A$\in$ GL(2,$\mathbb{Z}$) und S$\in$ SL(2,$\mathbb{Z}$) beliebig, dann gilt

$$\begin{aligned} \det(A \cdot S \cdot A^{-1}) &= \det(A) \cdot \det(S) \cdot \det(A^{-1}) \\ &= \det(A) \cdot \det(A^{-1}) \cdot \det(S) \\ &= \det(AA^{-1}) \cdot \det(S) = 1 \end{aligned}$$

$\Rightarrow A \cdot S \cdot A^{-1} \in \mathrm{SL}(2,\mathbb{Z}) \Rightarrow \mathrm{SL}(2,\mathbb{Z})$ ist Normalteiler von $\mathrm{GL}(2;\mathbb{Z})$. □

b) Für U = $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in$ GL(2;$\mathbb{Z}$) folgt ± 1 = detU = ad-bc, so dass z.B. c und d teilerfremd sind.

(c , d sind teilerfremd, da sonst ein $1 \neq m \in \mathbb{Z}$ mit m=ggT(c,d) existiert, für das m | det(U) gilt, was ein Widerspruch zu det(U)=±1 ist.)

Wir erhalten das

(2.4) Ergänzungs-Lemma.
Sind c,d $\in \mathbb{Z}$ teilerfremd, dann existiert ein U $\in$ SL(2;ℤ) mit U = $\begin{pmatrix} * & * \\ c & d \end{pmatrix}$. Hier ist U bis auf einen linksseitigen Faktor der Form $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ mit k $\in \mathbb{Z}$ eindeutig bestimmt.◇

Beweis.
Da c, d nach Voraussetzung teilerfremd sind, gibt es (ℤ ist Hauptidealring, vgl. Algebra) a,b $\in \mathbb{Z}$ mit ad - bc=1, d.h., U = $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gehört zu SL(2;ℤ). Ist V $\in$ SL(2;ℤ) eine weitere Matrix mit V = $\begin{pmatrix} * & * \\ c & d \end{pmatrix}$, dann folgt

$$\mathrm{SL}(2;Z) \ni VU^{-1} = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

(Da V,U$\in$ SL(2;ℤ) $\Rightarrow U^{-1} \in$ SL(2;ℤ)$\Rightarrow VU^{-1} \in$ SL(2;ℤ).)
also notwendig $VU^{-1} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ mit einem k $\in \mathbb{Z}$, da det $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} = 1$.
Damit gilt $V = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} U$, also die Behauptung. □

Wir erhalten weitere

(2.5) Bemerkungen
a) Das Beispiel U=2E zeigt, dass man – im Gegensatz zu der analogen Situation über einem Körper – die Bedingung U : $\mathbb{Z}^2 \to \mathbb{Z}^2$ ist injektiv, nicht in den Äquivalenz-Satz aufnehmen kann, da 2E $\notin$ GL(2;ℤ).

b) Das Ergänzungs-Lemma erlaubt die Konstruktion von zahllosen Beispielen: Die Matrizen

$$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 10 \\ 2 & 7 \end{pmatrix}, \begin{pmatrix} 89 & 144 \\ 144 & 233 \end{pmatrix}, \begin{pmatrix} 514229 & 832040 \\ 832040 & 1346269 \end{pmatrix}$$

gehören z.B. zu SL(2,ℤ).

c) Die Ergebnisse dieses Abschnitts lassen sich leicht auf n×n Matrizen übertragen.
(vgl. dasselbe Buch, S.222.) ◇

§ 3 Basis-Lemma

Ziel des Abschnitts.
Wir wollen einen Basiswechsel in Ω und die Eigenschaft des Periodenparallelogramm betrachten. □

Zunächst beweisen wir das

(3.1) Basis-Lemma.
Sei Ω ein Gitter in $\mathbb{C}$ und (ω_1, ω_2) eine Basis von Ω. Für $\omega_1', \omega_2' \in \mathbb{C}$ gilt dann:
a) ω_1' *und* ω_2' gehören zu $\Omega \Longleftrightarrow$ es gibt ein U $\in$ Mat(2,$\mathbb{Z}$) mit

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = U \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}. \tag{5}$$

b) (ω_1', ω_2') ist eine Basis von $\Omega \Longleftrightarrow$ die Matrix U in (5) gehört zu GL(2;$\mathbb{Z}$). ◇

Beweis.
a) „$\Longrightarrow$“ Sind ω_1', ω_2' beliebige Punkte von Ω und ist (ω_1, ω_2) Basis von Ω, dann gibt es a,b,c,d$\in \mathbb{Z}$ mit $\omega_1' = a\omega_1 + b\omega_2$, $\omega_2' = c\omega_1 + d\omega_2$, also

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = U \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \text{ mit } U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}(2;\mathbb{Z}). \tag{6}$$

„$\Longleftarrow$“ Gilt umgekehrt (6), so gehören ω_1' *und* ω_2' zu Ω.

b) „$\Longrightarrow$“ Ist (ω_1', ω_2') eine Basis von Ω, dann gibt nach a) ein V $\in$ Mat(2;$\mathbb{Z}$) mit $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \text{V} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$. Es folgt

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = VU \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \textit{ und } \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = UV \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$$

.
Da aber (ω_1, ω_2) und (ω_1', ω_2') über $\mathbb{R}$ linear unabhängig sind, hat man

$$VU = UV = E,$$

also U $\in$ GL(2;$\mathbb{Z}$) nach (2.1).

„$\Longleftarrow$“ Ist U $\in$ GL(2;$\mathbb{Z}$), dann sind (ω_1', ω_2') in (6) zunächst linear unabhängig über $\mathbb{R}$. Für beliebige $\omega_1'', \omega_2'' \in \Omega$ gibt es ein W $\in$ Mat(2;$\mathbb{Z}$) mit

$$\begin{pmatrix} \omega_1'' \\ \omega_2'' \end{pmatrix} = W \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, also \begin{pmatrix} \omega_1'' \\ \omega_2'' \end{pmatrix} = WU^{-1} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

Damit sind ω_1'', ω_2'' jeweils Linearkombinationen von ω_1', ω_2' über $\mathbb{Z}$. Also ist ω_1', ω_2' eine Basis von Ω. □

Wir betrachten im folgenden Periodenparallelogramm.

(3.2) Definition
Es sei Ω ein Gitter in $\mathbb{C}$ und (ω_1, ω_2) eine Basis von Ω. Für u $\in$ $\mathbb{C}$ definiert man das **Periodenparallelogramm** (bezüglich ω_1, ω_2 mit Basispunkt u) durch

$$\Diamond(u;\ \omega_1, \omega_2) := \{u + \alpha_1\omega_1 + \alpha_2\omega_2;\ 0 \leq \alpha_1,\ 0 \leq \alpha_2 < 1\}.$$

Im Fall u = 0 schreibt man auch

$$\Diamond(\omega_1, \omega_2) := \Diamond(0;\ \omega_1, \omega_2) = \{\alpha_1\omega_1 + \alpha_2\omega_2;\ 0 \leq \alpha_1,\ 0 \leq \alpha_2 < 1\}$$

und nennt $\Diamond(\omega_1, \omega_2)$ auch eine **Grundmasche** des Gitters. ◇

Jedes Periodenparallelogramm P:=$\Diamond(u;\omega_1, \omega_2)$ ist ein Fundamentalbereich von $\mathbb{C}$ bezüglich Ω im folgenden Sinne:

(3.3) Proposition.
Zu jedem z $\in$ $\mathbb{C}$ gibt es genau ein $\omega \in \Omega$ mit z+$\omega \in$ P. Gehören insbesondere z und z+ω, $\omega \in \Omega$, zu P, dann gilt ω=0. ◇

Beweis.
Weil (ω_1, ω_2) Basis von Ω und Ω Gitter ist, dann ist auch $\Rightarrow$ (ω_1, ω_2) Basis von $\mathbb{C}$.
$\Rightarrow$ $\exists\ \xi_1, \xi_2 \in \mathbb{R}$ mit z-u=$\xi_1\omega_1 + \xi_2\omega_2$.
Zu $\xi_1, \xi_2 \in \mathbb{R}$ existieren nun k,l $\in \mathbb{Z}$ mit $0 \leq \xi_1 + k\ ,\ \xi_2 + l < 1$ und

$$\begin{aligned} P &\ni (\xi_1 + k)\omega_1 + (\xi_2 + l)\omega_2 + u \\ &= \xi_1\omega_1 + \xi_2\omega_2 + k\omega_1 + l\omega_2 + u \\ &= z - u + k\omega_1 + l\omega_2 + u \\ &= z + k\omega_1 + l\omega_2 \end{aligned}$$

also $\omega = k\omega_1 + l\omega_2 \in \Omega$ mit z+$\omega \in P$ und zwar k,l$\in \mathbb{Z}$ ist eindeutig bestimmt durch ξ_1 *und* ξ_2, also ω ist eindeutig bestimmt. Wegen der Eindeutigkeit von ω ist $\omega = 0$, wenn z=z+0 und z+ω, $\omega \in \Omega$, in P. □

Wir bestimmen nun den Flächeninhalt der Periodenparallelogramme.

(3.4) Proposition.
Die elementar-geometrische Fläche eines Periodenparallelogramms P:=$\Diamond(u;\omega_1,\omega_2)$ ist gleich

$$vol\Omega := |Im(\omega_1\overline{\omega_2})|\,.$$

Sie ist unabhängig von der Wahl der Basis (ω_1,ω_2) von Ω. $\diamond$

Beweis.
Die elementar-geometrische Fläche des Parallelogramms P ist in euklidischen Koordinaten zunächst gegeben durch

$$F := \left|\det\begin{pmatrix} \operatorname{Re}\omega_1 & \operatorname{Re}\omega_2 \\ \operatorname{Im}\omega_1 & \operatorname{Im}\omega_2 \end{pmatrix}\right|.$$

Behauptung.

$$\left|\det\begin{pmatrix} \operatorname{Re}\omega_1 & \operatorname{Re}\omega_2 \\ \operatorname{Im}\omega_1 & \operatorname{Im}\omega_2 \end{pmatrix}\right| = |\operatorname{Im}(\omega_1\overline{\omega_2})|$$

Beweis.
Seien $\omega_1 = x+yi,\ \omega_2 = u+vi\ \in \mathbb{C}$. Dann gilt

$$\left|\det\begin{pmatrix} \operatorname{Re}\omega_1 & \operatorname{Re}\omega_2 \\ \operatorname{Im}\omega_1 & \operatorname{Im}\omega_2 \end{pmatrix}\right| = \left|\det\begin{pmatrix} x & u \\ y & v \end{pmatrix}\right| = |xv-yu|$$

sowie

$$|\operatorname{Im}(\omega_1\overline{\omega_2})| = |\operatorname{Im}((x+yi)(u-vi))| = |\operatorname{Im}((xu+yv)+(yu-xv)i)| = |yu-xv| = |xv-yu|$$

Ist nun (ω_1',ω_2') weitere Basis, dann gilt nach (3.1) $\omega_1' = a\omega_1+b\omega_2, \omega_2' = c\omega_1 + d\omega_2\ \in \Omega$ mit a, b, c, d $\in\ \mathbb{Z}$, ad-bc=$\pm$1, so folgt

$$\begin{aligned}
F' = |Im(\omega_1'\overline{\omega_2'})| &= |Im((a\omega_1 + b\omega_2)\overline{(c\omega_1 + d\omega_2)})| \\
&= |Im(ac|\omega_1|^2 + bd|\omega_2|^2 + bc\omega_2\overline{\omega_1} + ad\omega_1\overline{\omega_2})| \\
&= |Im(ad\omega_1\overline{\omega_2} + bc\omega_2\overline{\omega_1})| \\
&= |Im(ad\omega_1\overline{\omega_2}) + Im(bc\omega_2\overline{\omega_1})| \\
&= |Im(ad\omega_1\overline{\omega_2}) - Im(bc\overline{\omega_2\overline{\omega_1}})| \\
&= |Im(ad\omega_1\overline{\omega_2}) - Im(bc\omega_1\overline{\omega_2})| \\
&= |Im(ad - bc)\omega_1\overline{\omega_2}| \\
&= |ad - bc||Im(\omega_1\overline{\omega_2})| \\
&= |Im(\omega_1\overline{\omega_2})| \\
&= F.
\end{aligned}$$

(3.5) Beispiel
Sei K=$\mathbb{Q}(\sqrt{d})$, d<0 quadratfrei, ein imaginär-quadratischer Zahlkörper der Diskriminante D und Ω der Ring der ganzen Zahlen, d.h. $\Omega = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$, D=d, falls d≡1 (mod 4), und sonst $\Omega = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, D=4d. Dann ist Ω ein Gitter in $\mathbb{C}$, und die Fläche eines Periodenparallelogramms ist $\frac{1}{2}\sqrt{|D|}$.

Lösung:
1. Fall: Sei $\Omega = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$, D=d. Dann ist Ω ein Gitter mit Basis $(\omega_1, \omega_2) = (1, \frac{1+i\sqrt{|d|}}{2})$. Nach Proposition (3.4) erhält man dann

$$vol\Omega := |Im(\omega_1\overline{\omega_2})| = |Im(1 \cdot \overline{\frac{1 + i\sqrt{|d|}}{2}})| = |Im(\frac{1 - i\sqrt{|d|}}{2})| = |\frac{\sqrt{|d|}}{2}| = \frac{1}{2}\sqrt{|D|}.$$

2.Fall : Sei $\Omega = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, D=4d. Dann ist Ω ein Gitter mit Basis $(\omega_1, \omega_2) = (1, i\sqrt{|d|})$ nach Proposition (3.4),

$$vol\Omega := |Im(\omega_1\overline{\omega_2})| = |Im(1 \cdot \overline{i\sqrt{|d|}})| = |\sqrt{|d|}| = |\sqrt{\frac{|D|}{4}}| = \frac{1}{2}\sqrt{|D|}$$