§ 10. Kettenbrüche und Modulgruppe

Reelle Zahlen sind durch Kettenbrüche gegeben. Seien $\alpha = [a_0; a_1, \ldots]$ und $\beta = [b_0; b_1, \ldots]$ zwei Kettenbrüche. $\alpha = \beta \Leftrightarrow a_i = b_i \ \forall i \geq 0$.
$a_i = b_i \ \forall i \geq 1 \Leftrightarrow \alpha_1 = \beta_1$ mit $\alpha_1 = [a_1; \ldots]$ und $\beta_1 = [b_1; \ldots] \Leftrightarrow \alpha - \beta \in \mathbb{Z}$.
Naive Frage: Was bedeutet: $\exists \ell, m$ mit $\alpha_\ell = \beta_m$, d.h. $a_{\ell+i} = b_{m+i} \ \forall i \geq 0$?
Anders formuliert: Was bedeutet es, wenn die Kettenbrüche von α und β sich nur in jeweils endlich vielen Anfangsstellen unterscheiden, wobei die Länge der Anfangsstücke unterschiedlich sein darf?
Die Antwort wird zeigen, daß die Frage sinnvoll ist.

Diese Frage enthält auch die Frage, was α mit seinen Endstücken α_i zu tun hat. Dazu haben wir in § 7 schon etwas gelernt, vor allem in 7.4:

$$\alpha = [a_0; a_1, \ldots, a_{\ell-1}, \alpha_\ell] = \frac{p_{\ell-1}\alpha_\ell + p_{\ell-2}}{q_{\ell-1}\alpha_\ell + q_{\ell-2}} \quad \text{und entsprechend}$$

$$\beta = [b_0; b_1, \ldots, b_{m-1}, \beta_m] = \frac{p'_{m-1}\beta_m + p'_{m-2}}{q'_{m-1}\beta_m + q'_{m-2}}$$

(Bezeichnung p', q' nur um von den p, q bei α zu unterscheiden)

und, ebenfalls nach 7.4, $p_{i-1}q_i - p_i q_{i-1} = (-1)^i$.
Das bedeutet: α ist das Bild von α_ℓ unter der Abbildung

$$z \longmapsto \frac{p_{\ell-1}z + p_{\ell-2}}{q_{\ell-1}z + q_{\ell-2}}$$

(falls diese wohldefiniert ist)

wobei die Matrix $\begin{pmatrix} p_{\ell-2} & p_{\ell-1} \\ q_{\ell-2} & q_{\ell-1} \end{pmatrix}$ Determinante ± 1 hat, also invertierbar ist.

Wir sollten daher auch invertierbare Matrizen mit ganzzahligen Einträgen genauer anschauen. Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ so eine Matrix, mit Einträgen in $\mathbb{Z}$ und Determinante $\pm 1 \in \mathbb{Z}$. Können wir Brüchen der Form $\frac{az+b}{cz+d}$ einen Kettenbruch zuordnen? Gibt es also eine Art Umkehrung der obigen Beziehung?
Wir haben $q_{\ell-1} > q_{\ell-2}$, also $c > d$, sollten also vielleicht solche Bedingungen stellen.

10.1 Lemma: Sei $\xi \in \mathbb{R}$, $\xi > 1$, $a,b,c,d \in \mathbb{Z}$ mit $ad - bc = \pm 1$, $c > d > 0$ und $\eta = \frac{a\xi + b}{c\xi + d}$. Dann $\exists\, n \in \mathbb{N}$ so daß gilt: Der $n-1$-te Näherungsbruch von η ist $\frac{b}{d}$ und der n-te Näherungsbruch ist $\frac{a}{c}$. Außerdem ist $\xi = \eta_n$ (der Restterm).

Beweis: $ad - bc = \pm 1 \Rightarrow (a,c) = 1$. Den Bruch $\frac{a}{c}$ kann man als Kettenbruch entwickeln mit Näherungsbrüchen $\frac{p_i}{q_i}$ und letztem Term $\frac{p_n}{q_n} = \frac{a}{c}$.
Dabei gilt auch $(p_n, q_n) = 1 \Rightarrow a = p_n$ und $c = q_n$ ($da\, c > 0, q_n > 0$).
Behauptung: $\frac{b}{d} = \frac{p_{n-1}}{q_{n-1}}$: $ad - bc = \pm 1 = p_n q_{n-1} - p_{n-1} q_n$
$= p_n d - b q_n$
(Das Vorzeichen kann passend gewählt werden, weil ein endlicher Kettenbruch immer eine zweite, um eins längere, Darstellung hat, mit $\frac{1}{-\frac{1}{1}}$)
$\Rightarrow p_n (d - q_{n-1}) = (b - p_{n-1}) q_n$. Wegen $(p_n, q_n) = 1$ gilt $q_n \mid (d - q_{n-1})$.
Aber $c > d > 0$ und $c = q_n \geq q_{n-1} > 0 \Rightarrow d - q_{n-1} < q_n \Rightarrow$
$d = q_{n-1} \Rightarrow b = p_{n-1}$ wegen $ad - bc = p_n q_{n-1} - p_{n-1} q_n \Rightarrow$ Behauptung
Einsetzen $\rightsquigarrow \eta = \frac{p_n \xi + p_{n-1}}{q_n \xi + q_{n-1}} = [a_0; \ldots, a_{n-1}, \xi]$ wobei $[a_0; \ldots, a_{n-1}] = \frac{a}{c}$
Also $\xi = [a_n; \ldots]$ und $\eta = [a_0; \ldots, a_{n-1}, a_n, \ldots]$ (bei passender Wahl der Bezeichnungen). Dabei sind $\frac{p_{n-1}}{q_{n-1}} = \frac{b}{d}$ und $\frac{p_n}{q_n} = \frac{a}{c}$ aufeinander folgende Näherungsbrüche und $\xi = \eta_n$ ist der Restterm.
($\xi > 1$ wird verwendet, damit $\lfloor \xi \rfloor \geq 1$ gilt, d.h. $a_{n+1} = \lfloor \xi \rfloor \geq 1$, sonst wäre das Zusammensetzen der Kettenbrüche problematisch.) $\square$

Allgemeiner, also ohne die Einschränkung $\xi > 1$, sollten wir Zahlen wie ξ und η miteinander vergleichen.

10.2 Definition: Zwei reelle Zahlen ξ und η heißen äquivalent genau dann, wenn gilt: $\exists\, a,b,c,d \in \mathbb{Z}$ mit $ad - bc = \pm 1$ so daß

$$\xi = \frac{a\eta + b}{c\eta + d}$$

10.3. Lemma: Äquivalenz ist eine Äquivalenzrelation.

Beweis: $\begin{pmatrix}1&0\\0&1\end{pmatrix} \rightsquigarrow$ Reflexivität

Symmetrie: $\pm\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$ ist invers zu $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ und definitionsgemäß:

$$\zeta = \frac{a\eta+b}{c\eta+d} \Rightarrow \zeta(c\eta+d) = a\eta+b \Rightarrow \eta(c\zeta-a) = b-\zeta d \Rightarrow \eta = \frac{-\zeta d+b}{c\zeta-a} = \frac{\zeta d-b}{-c\zeta+a}$$

Transitivität: $\zeta = \frac{a\eta+b}{c\eta+d}$, $\gamma = \frac{a'\zeta+b'}{c'\zeta+d'} = \frac{a'\left(\frac{a\eta+b}{c\eta+d}\right)+b'}{c'\left(\frac{a\eta+b}{c\eta+d}\right)+d'} = \ldots =$

$$= \frac{(aa'+cb')\eta+ba'+db'}{(ac'+cd')\eta+bc'+d'd}$$

Das Ergebnis entspricht der Produktmatrix $\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}$, die natürlich wieder Determinante ± 1 hat. □

An Matrizen zu denken passt also. Da wir die Komposition von ~~Abbildungen~~ Abbildungen so schreiben, daß $\eta \mapsto \zeta \mapsto \gamma$ abgebildet wird, also η durch $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ und dann ζ durch $\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}$, steht die zuerst anzuwendende Matrix rechts im Produkt.

Daß die Matrizen $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ mit Determinante ± 1 eine Gruppe bilden, haben wir mitbewiesen.

$SL(2,\mathbb{Z})$ ⊴ GL

10.4 Definition: Die spezielle lineare Gruppe $SL_2(\mathbb{Z})$ ist die multiplikative Gruppe der 2×2-Matrizen mit ganzzahligen Einträgen und Determinante 1.

Die Modulgruppe Γ ist der Quotient von $SL_2(\mathbb{Z})$ modulo dem Normalteiler $\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\}$ und wird auch mit $PSL_2(\mathbb{Z})$ bezeichnet.

(sogar im Zentrum von $SL_2(\mathbb{Z})$ enthalten)

(„projektive spezielle lineare Gruppe")

wie hängen Normalteiler und Quotientengruppen zusammen?

Auf die Modulgruppe Γ gehen wir später genauer ein.

Zuerst klären wir, was Äquivalenz mit den Ketten brüchen zu tun hat.

10.5 Lemma: Alle rationalen Zahlen sind zueinander äquivalent.

Beweis: Sei $\frac{b}{d}$ eingekürzter Bruch, d.h. $(b,d)=1$. Wir zeigen, daß $\frac{b}{d}$ zu 0 äquivalent ist. $\exists\, a, c \in \mathbb{Z}$ mit $1 = ad - bc$. $\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ hat Determinante 1 und $0 \longmapsto \frac{a\cdot 0 + b}{c\cdot 0 + d} = \frac{b}{d}$. $\square$

Umgekehrt: sei $\xi \in \mathbb{Q} \Rightarrow \eta = \frac{a\xi + b}{c\xi + d} \in \mathbb{Q}$. Die rationalen Zahlen bilden genau eine Äquivalenz klasse. Ihre Kettenbruchentwicklungen sind alle endlich, haben also dasselbe Endstück 0.
Interessanter sind natürlich die irrationalen Zahlen.

10.6 Theorem: Seien α und β irrationale Zahlen. Dann sind äquivalent:
(a) α und β sind äquivalent.
(b) Die Kettenbrüche $\alpha = [a_0; a_1, \ldots]$ und $\beta = [b_0; b_1, \ldots]$ haben ein gemeinsames Endstück $[a_\ell = b_m; a_{\ell+1} = b_{m+1}, \ldots]$

Beweis: (b) $\Rightarrow$ (a) ist eigentlich schon gezeigt: Sei $\alpha_\ell = \beta_m$ das gemeinsame Endstück. $\Rightarrow \alpha = \frac{p_{\ell-1}\alpha_\ell + p_{\ell-2}}{q_{\ell-1}\alpha_\ell + q_{\ell-2}}$ mit $\det \begin{pmatrix} p_{\ell-1} & p_{\ell-2} \\ q_{\ell-1} & q_{\ell-2} \end{pmatrix} = \pm 1 \Rightarrow \alpha$ und α_ℓ sind äquivalent und analog β und $\beta_m = \alpha_\ell$.

(a) $\Rightarrow$ (b): In Lemma 10.1 haben wir schon einen Spezialfall bewiesen, den wir anwenden wollen, und nachetwas Rechnung auch anwenden können.
Sei $\beta = \frac{a\alpha + b}{c\alpha + d}$ mit $c\alpha + d > 0$ (sonst erweitern wir mit -1), mit $\alpha = [a_0; a_1, \ldots, a_{u-1}, \alpha_u]$ (für später noch zu wählendes, jetzt noch billiges α_u).
Einsetzen $\rightsquigarrow \beta = ? = \dfrac{(a p_{u-1} + b q_{u-1})\alpha_u + a p_{u-2} + b q_{u-2}}{(c p_{u-1} + d q_{u-1})\alpha_u + c p_{u-2} + d q_{u-2}} = \dfrac{P\alpha_u + R}{Q\alpha_u + S}$

mit $PS - QR = (ad - bc)(p_{u-1} q_{u-2} - p_{u-2} q_{u-1}) = \pm 1$

(wobei $\alpha = \dfrac{p_{u-1}\alpha_u + p_{u-2}}{q_{u-1}\alpha_u + q_{u-2}}$)

In §7 haben wir gezeigt: $|\alpha - \frac{p_{u-1}}{q_{u-1}}| < \frac{1}{q_{u-1}^2}$

$\Rightarrow p_{u-1} = \alpha q_{u-1} + \frac{\delta}{q_{u-1}}$ mit $|\delta| < 1$

und ebenso: $p_{u-2} = \alpha q_{u-2} + \frac{\delta'}{q_{u-2}}$ mit $|\delta'| < 1$

$\Rightarrow Q = c p_{u-1} + d q_{u-1} = c\left(\alpha q_{u-1} + \frac{\delta}{q_{u-1}}\right) + d q_{u-1}$

$= (c\alpha + d) q_{u-1} + \frac{c\delta}{q_{u-1}}$

und $S = c p_{u-2} + d q_{u-2}$

$= (c\alpha + d) q_{u-2} + \frac{c\delta'}{q_{u-2}}$

Nach Voraussetzung ist $c\alpha + d > 0$, $q_{u-1} \geq q_{u-2} > 0$, $q_u \xrightarrow{u\to\infty} \infty$

$\Rightarrow$ Für u groß genug ist $Q > S > 0$.

Für solche u erfüllt $\beta = \frac{Pa_u + R}{Qa_u + S}$ die Voraussetzungen von Lemma 10.1:

$PS - QR = \pm 1$, $Q > S > 0$ und $\alpha_u > 1$, weil $\alpha_u = [a_u; a_{u+1}, \ldots]$, $a_{u+1} \geq 1$.

$\overset{10.1}{\Rightarrow} \exists n: \alpha_u = \beta_n$, d.h. die Kettenbrüche von α und β ein gemeinsames Endstück. □

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ hat offenbar keine Wirkung, deshalb betrachtet man die Modulgruppe Γ.
Diese Gruppe hat ein Erzeugendensystem aus zwei Elementen:

10.7 Proposition: Die Modulgruppe Γ ist erzeugt von den beiden Elementen $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, d.h. jede Matrix in Γ ist ein endliches Produkt aus diesen Matrizen und P^{-1}. warum wird Q^{-1} nicht gebraucht?

Beweis: Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine Matrix in Γ. Wir können α wählen, das dann in β transformiert wird. Die Äquivalenz von α und β verrät, wie wir $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ als Produkt schreiben können.

$P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}: S \longmapsto \frac{S+1}{0+1} = S+1$, $Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}: S \mapsto \frac{-1}{S+0} = -\frac{1}{S}$

$Q^2 = -\mathrm{Id}$, $P^\ell = \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix}: S \longmapsto S + \ell$ für $\ell \in \mathbb{Z}$, $P^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

$[a_0; a_1, \dots, a_{e-1}, a_e, \dots]$

Unsere Aufgabe ist es, α in $\alpha_e = \beta_m$ umzuformen, wie vorher, und β in β_m.

$[a_0; a_1, \dots, a_{e-1}, a_e, \dots]$

$\alpha = a_0 + \frac{1}{\alpha_1} \Rightarrow P^{-a_0}(\alpha) = \frac{1}{\alpha_1}$

$Q \circ P^{-a_0}(\alpha) = -\alpha_1$

$P^{a_1} \circ Q \circ P^{-a_0} : \alpha \mapsto -\frac{1}{\alpha_2}$

$Q \circ P^{a_1} \circ Q \circ P^{-a_0} : \alpha \mapsto \alpha_2$ usw

Analog für β. Nach endlich vielen Schritten erhält man:

$Q \circ P^{-a_2} \circ Q \circ P^{a_1} \circ Q \circ P^{-a_0}(\alpha) = \alpha_e = \beta_m = Q \circ P^{-b_2} \circ Q \circ P^{b_1} \circ Q \circ P^{-b_0}(\beta)$

Da P und Q invertierbar sind, erhalten wir α aus β, und umgekehrt.

Da die Komposition der Matrizenmultiplikation entspricht, folgt daraus die Produktdarstellung von $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. □

"Kettenbruchentwicklung"

Ist der Beweis vollständig?
Ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ durch seine Wirkung auf S bestimmt, für geeigneter S?

Wie kann man sich Abbildungen $z \mapsto \frac{az+b}{cz+d}$, d.h. Elemente von Γ, geometrisch vorstellen?

Abbildungen $z \mapsto \frac{az+b}{cz+d}$ mit $a, b, c, d \in \mathbb{C}$ und $ad - bc \neq 0$ heißen Möbiustransformationen. Das sind Abbildungen der Riemannschen Zahlenkugel auf sich selbst, und als solche sind sie winkeltreu (konform) und sie bilden Geraden und Kreise auf Geraden oder Kreise ab (aber manchmal Geraden auf Kreise oder umgekehrt). Dazu schaut man sich am besten Bilder oder Videos an, zum Beispiel in dem Buch Visual complex analysis (deutsche Ausgabe: Anschauliche Funktionentheorie) von Tristan Needham (in der Universitätsbibliothek erhältlich) und das (frei erhältliche) Video "Möbiustransformations revealed" von Douglas Arnold und Jonathan Rogues, University of Minnesota.

Wenn man zum projektiven Raum $\mathbb{P}^1(\mathbb{C})$ übergeht ($= \mathbb{C} \cup \{\infty\}$, Nordpol), sieht man die "Linearität" der Möbiustransformationen: Punkte von $\mathbb{P}^1(\mathbb{C})$ sind eindimensionale Unterräume von $\mathbb{C}^2$, d.h. Geraden, die durch homogene Koordinaten $[z_1 : z_2]$ gegeben sind ($[z_1 : z_2] = [\lambda z_1 : \lambda z_2]$, $\lambda \neq 0$), deren Richtungsvektor bestimmt die Gerade, ist aber selbst nur bis auf $\lambda \neq 0$ bestimmt.

Dann ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} az_1+bz_2 \\ cz_1+dz_2 \end{pmatrix}$ sinnvoll (Vorstellung: $z = \frac{z_1}{z_2}$).

Die Abbildung $z \mapsto \frac{1}{z}$ vertauscht Nord- und Südpol der Zahlenkugel, in der Zahlenebene vertauscht sie Inneres und Äußeres des Einheitskreises.

Wir schauen uns ein zweidimensionales Bild an:

$\mathcal{H} := \{z \in \mathbb{C} : \underset{\text{Imaginärteil}}{\operatorname{Im}}(z) > 0\} \subset \mathbb{C}$ ist die obere Halbebene in der komplexen Zahlenebene. Die reelle Zahlengerade können wir uns als Rand ∂ von $\mathcal{H}$ dazudenken.

Die Modulgruppe Γ hat die ~~Erz~~ Erzeuger

$$P: z \mapsto z+1 \quad \text{und} \quad Q: z \mapsto -\frac{1}{z} \quad (0 \notin \mathcal{H}),$$

beide bilden $\mathcal{H}$ in $\mathcal{H}$ ab. Also können wir die Elemente von Γ als Abbildungen von $\mathcal{H}$ in $\mathcal{H}$ betrachten, oder (im Sinne von Algebra) $\mathcal{H}$ als Γ-Menge, auf der Γ operiert.

Die Modulgruppe Γ hat unendlich viele Elemente und ist erzeugt von P und Q, P hat unendliche Ordnung, Q hat Ordnung zwei. Wir ersetzen P durch ein Element mit Ordnung drei und zeigen, daß die unendliche Gruppe Γ erzeugt ist von den beiden Elementen Q und R, die endliche Ordnung haben.

Sei $R := QP$. Dann ist $P = QQP = QR$, also von Q und R erzeugt

$\Rightarrow$ ganz Γ wird von Q und R erzeugt. $\langle Q \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ und $\langle R \rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

Behauptung: Jedes Element in Γ ist ein eindeutiges Produkt (endlich)

$$\_ \circ Q \circ R^{\varepsilon} \circ Q \circ R^{\varepsilon'} \circ Q \circ R^{\varepsilon''} \circ \_ \quad \text{wobei } \varepsilon, \varepsilon', \ldots \in \{1,2\}.$$

(Das Einselement ist das leere Produkt.) Zu zeigen ist die Eindeutigkeit.

(Für Gruppentheoretiker bedeutet das: Γ ist das freie Produkt von $\langle Q \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ und $\langle R \rangle \simeq \mathbb{Z}/3\mathbb{Z}$.)

Es genügt zu zeigen: Ein nichtleeres Produkt $Q \circ R^{\varepsilon_1} \circ Q \circ R^{\varepsilon_2} \circ \_ \circ Q \circ R^{\varepsilon_n} \neq \mathrm{Id}$

warum?

(und analog für drei weitere Fälle: linkes R, rechts Q)

Sei $\mathcal{H}_L := \{z \in \mathcal{H} : \operatorname{Re}(z) < 0\}$ der offene linke Teil von $\mathcal{H}$ und

$\mathcal{H}_R := \{z \in \mathcal{H} : \operatorname{Re}(z) \geq 0\}$ der abgeschlossene rechte Teil.

Dann gilt: $Q(\mathcal{H}_L) \subsetneq \mathcal{H}_R$ $(z \mapsto -\frac{1}{z})$

$R(\mathcal{H}_R) \subsetneq \mathcal{H}_L$ $(z \mapsto -\frac{1}{z+1})$ nachprüfen

$R^2(\mathcal{H}_R) \subsetneq \mathcal{H}_L$ $(z \mapsto -\frac{1}{z}-1)$ das

Für eine Komposition $Q \circ \cdots \circ R^{\text{ev}}$ bedeutet: Das Bild von $\mathcal{H}_R$ unter der Komposition ist eine echte Teilmenge von $\mathcal{H}_R$, also kann die Abbildung nicht die Identität sein. Analog in den anderen Fällen.

Für reelle Zahlen haben wir Äquivalenz ~~und~~ von Kettenbrüchen in 10.6 charakterisiert. Wir kennen aber keine Repräsentanten der Äquivalenzklassen, also der Γ-Bahnen (abgesehen von ∞ als natürlichem Repräsentanten von $\mathbb{Q}$, das ja eine Äquivalenzklasse bildet). Bei der Operation von Γ auf $\mathcal{H}$ gibt es eine bessere (aber nicht perfekte) Antwort:

10.8 Proposition: Die Menge $\bar{F} := \{z \in \mathcal{H} : -\frac{1}{2} < \mathrm{Re}(z) \leq \frac{1}{2}, |z| \geq 1\}$ ist (beinahe) ein Fundamentalbereich für die Operation der Modulgruppe Γ auf der oberen Halbebene $\mathcal{H}$.

Das bedeutet: $z_1, z_2 \in \bar{F}$, $z_1 \neq z_2 \Rightarrow z_1$ und z_2 liegen in verschiedenen Γ-Bahnen

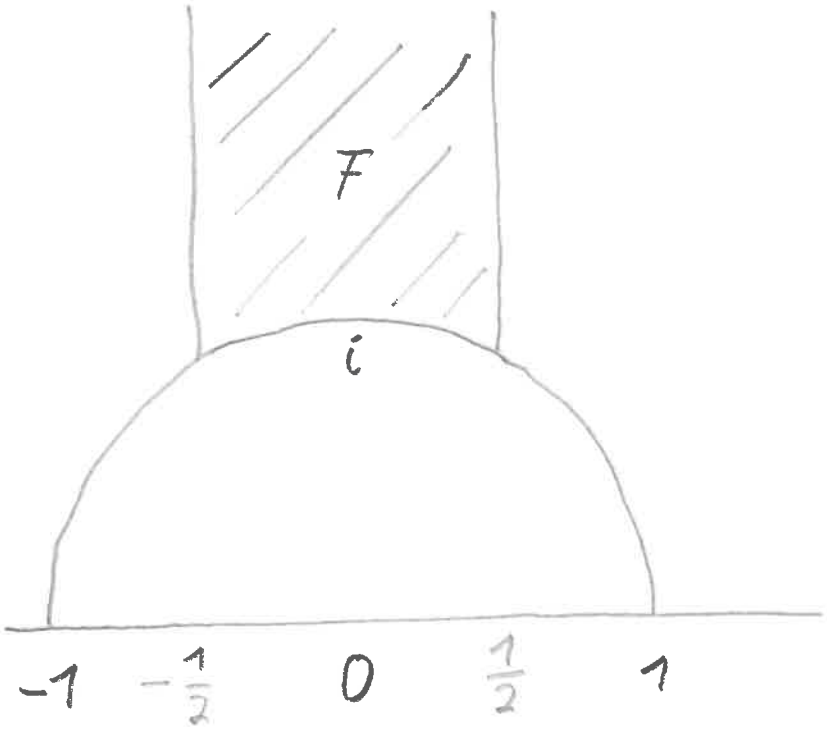
und $z_1 \in \mathcal{H} \Rightarrow \exists z_2 \in \bar{F} := F \cup \underbrace{\partial F}_{\text{Rand von } F}$, so daß z_1 und z_2 in derselben Γ-Bahn liegen.

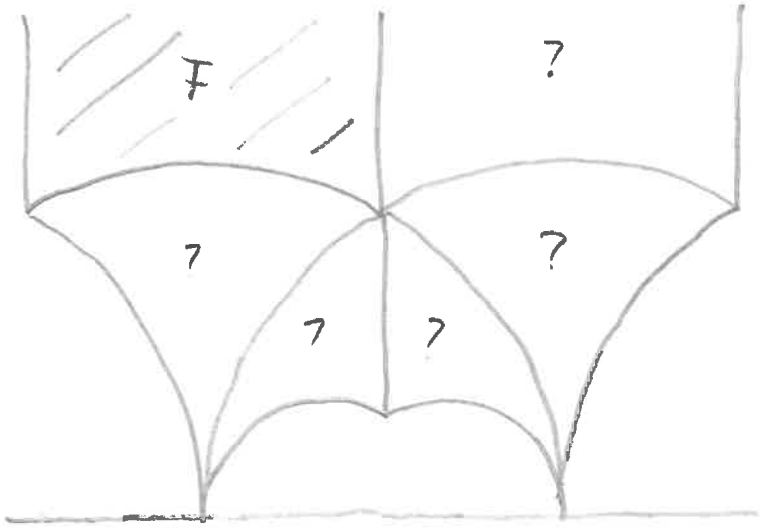
(Γ bringt also jeden Punkt nach $\bar{F}$, aber keinen Punkt von F in einen anderen Punkt von F.

Die Schwäche von 10.8 ist, daß die Situation der Randpunkte von F nicht geklärt wird.)

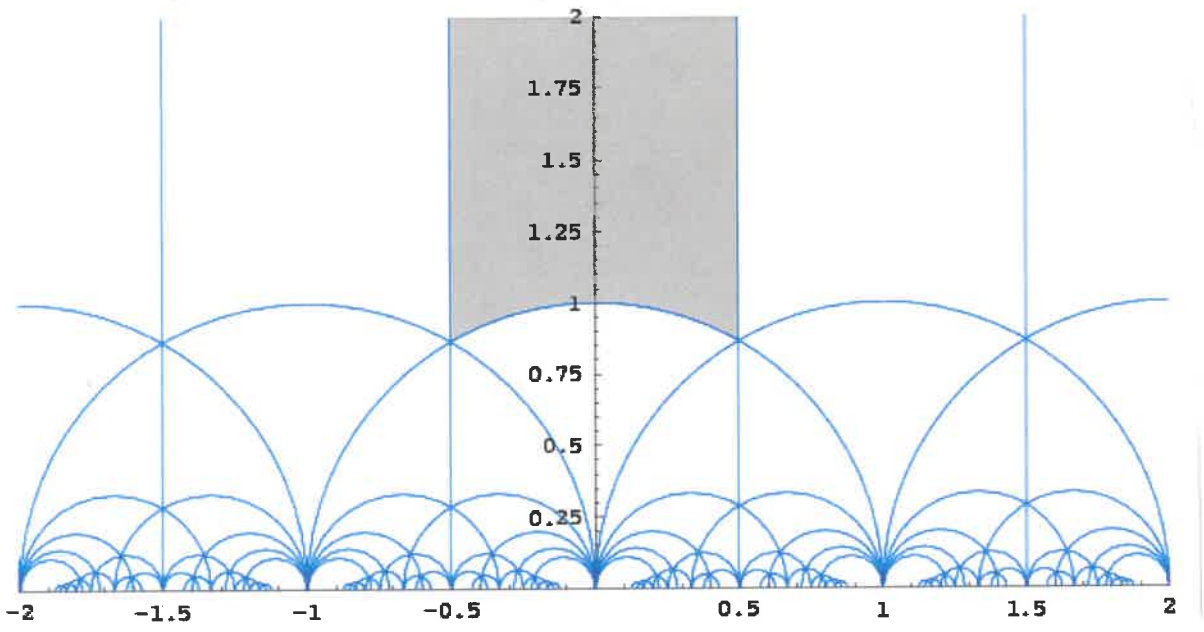
Letzlich sagt 10.8, daß die obere Halbebene eine Art Kettenbruchzerlegung hat, die man besser durch den Fundamentalbereich beschreibt als durch die Γ-Bahnen ($\leftrightarrow$ Äquivalenzklassen).

Wenn man F durch Elemente von Γ abbildet, erhält man zumindest hübsche Bilder:





Durch welche Elemente von Γ entstehen die? aus F?



Beweis von Proposition 10.8:

Seien $z = x+iy$ und $z' = x'+iy'$ beide in F und zueinander äquivalent, $y' \geq y$.

$\Rightarrow \exists\, a,b,c,d \in \mathbb{Z}$ mit $ad-bc=1$ so daß $z' = \frac{az+b}{cz+d}$. Zu zeigen ist: $z=z'$.

Falls $c=0$: $ad=1 \Rightarrow a=d=\pm 1$, $z' = z \pm b$, ξ Fixstoffen mit Breite $1 \Rightarrow b=0$

$\Rightarrow z=z'$

Falls $c \neq 0$: $z' = \frac{az+b}{cz+d} \cdot \frac{c\bar{z}+d}{c\bar{z}+d} = \frac{adz+bc\bar{z}+acz\bar{z}+bd}{|cz+d|^2}$, $acz\bar{z}+bd \in \mathbb{R}$,

$ad-bc=1 \Rightarrow \mathrm{Im}(adz+bc\bar{z}) = \frac{ady-bcy}{|cz+d|^2}$

$= \frac{y}{|cz+d|^2}$

Aber $y' \geq y \Rightarrow |cz+d|^2 \leq 1 \Rightarrow |z+\frac{d}{c}| \leq \frac{1}{|c|}$, $c \in \mathbb{Z}$.

Angenommen $c = \pm 1$: $z \in F$ liegt oberhalb des Halbkreises mit Radius 1.

Durch Verschiebung um $|d|$ nach links oder rechts kommt es nicht in den Halbkreis ξ zu $|c \pm d| \leq 1$.

Im Fall $|c| \geq 2$ muß $|z+\frac{d}{c}| \leq \frac{1}{2}$ sein. Aber durch Verschieben um $\frac{d}{c}$ nach rechts oder links kann z nicht in diesen verkleinerten Halbkreis mit Radius $\frac{1}{2}$ bewegt werden ξ

$\Rightarrow z=z'$, was zu zeigen war: Punkte in F können nur in derselben Γ-Bahn liegen, wenn sie gleich sind.

Die andere zu zeigende Aussage ist, daß jedes z_0 in $\mathcal{H}$ durch Γ in einen Punkt in $\bar{F}$ abgebildet werden kann.

Sei also $z_0 \in \mathcal{H}$. Durch Verschieben in positiv oder negativ reelle Richtung können wir $z_0^{\text{neu}} = x_0 + iy_0$ mit $|x_0| \leq \frac{1}{2}$ erreichen. Falls $|z_0| \geq 1$ gilt, dann liegt es in $\bar{F}$.

Sei $|z_0| < 1$. Dann wenden wir Q an, das ja das Innere des Einheits-kreises mit dem Äußeren vertauscht. Sei $z_1 = -\frac{1}{z_0} = x_1 + iy_1$, aber das ist auch $z_1 = -\frac{1}{z_0} = -\frac{\bar{z}_0}{z_0\bar{z}_0} = \frac{-x_0+iy_0}{|z_0|^2} \Rightarrow y_1 > y_0$.

Falls $y_0 \leq \frac{1}{2}$: dann ist $|z_0|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \Rightarrow$ sogar $y_1 \geq 2y_0$, d.h. die imaginäre Koordinate wird mindestens verdoppelt.

$\rightsquigarrow$ Strategie: nach endlich vielen solchen (zumindestens) Verdopplungen der imaginären Koordinate ist z_0 das Bild von z_0 in $\overline{F}$ angekommen.

Aber $y_0 \leq \frac{1}{2}$ ist ein Spezialfall, den allgemeinen Fall müssen wir reduzieren.

Durch P machen wir aus z_1 ein $z_2 = z_1 + m$, $m \in \mathbb{Z}$, so daß $|x_2| \leq \frac{1}{2}$.

$z_2 = z_1 + m = -\frac{1}{z_0} + m = \frac{mz_0 - 1}{z_0} \Rightarrow |z_2|^2 = \frac{|mz_0 - 1|^2}{|z_0|^2} = \frac{(mx_0 - 1)^2 + (my_0)^2}{x_0^2 + y_0^2}$,

wobei $x_0^2 + y_0^2 < 1$.

Falls $|z_2| \geq 1$: ✓

Falls $|z_2| < 1$: Dann war $m \neq 0$, auch $m \neq \pm 1$

$\Rightarrow |m| \geq 2$ (weil $\frac{1}{x_0^2 + y_0^2} > 1$) ← (weil $|1 \pm x_0| \geq \frac{1}{2} \geq |x_0|$, Zähler ≥ Nenner)

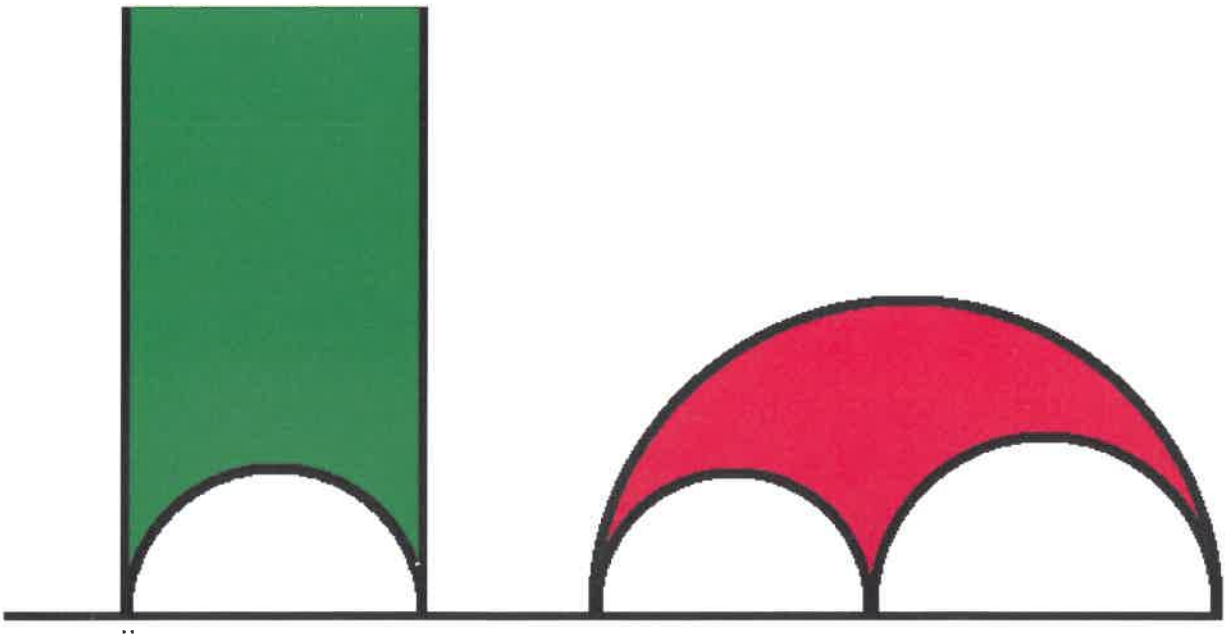
$\Rightarrow |z_2|^2 \geq (my_0)^2 \geq 4y_0^2$

Aber $|z_2| < 1 \Rightarrow y_0 < \frac{1}{2}$, d.h. dieser verbleibende Fall führt zwar (zumindestens) Verdopplung der imaginären Koordinate.

Endlich viele Wiederholungen dieser Maßnahme führen dazu, daß $\overline{F}$ erreicht wird. □

Was bedeuten diese Fälle in den Bildern auf Seite 10.10?

Frage: Was bedeutet F geometrisch? Was bedeuten die Bilder von F geometrisch? Was sieht man im folgenden Bild?



Antwort: F ist ein Dreieck, das rote Ding auch und die f-Bilder von F sind lauter Dreiecke.
Was soll das bedeuten?
In der Euklidischen Geometrie besteht eine Ebene aus Punkten, durch zwei verschiedene Punkte wird eine Gerade festgelegt und es gelten diverse Eigenschaften, die erlauben, Strecken, Kreise, Winkel ~~etc~~ etc zu definieren und dann den Satz von Pythagoras, die Winkelsumme in einem Dreieck zu bestimmen. Was Punkte oder Geraden sind, „definierte" Euklid in eher fragwürdiger Weise.
Ein moderner Zugang, wie Hilberts Axiomensystem der euklidischen Geometrie, verzichtet auf Definitionen von Punkten und Geraden – genauso wie wir bei einem Vektorraum auch nicht festlegen, ob Vektoren nun Pfeile sind oder stetige Funktionen oder Äpfel oder Birnen. Ein Vektorraum – oder eine Gruppe oder ein topologischer Raum – ist eine Menge, deren Elemente gewisse Eigenschaften erfüllen, die Axiome genannt werden.
Hilbert sagt nichts über die „Natur" von Punkten oder Geraden, aber er verlangt, daß zwei verschiedene Punkte eine Gerade bestimmen, daß es in einer Ebene drei Punkte, die nicht alle auf einer Geraden liegen, usw.
Was Punkte und Geraden sind kann man sich ausdenken – wenn die Axiome alle erfüllt sind, hat man eine Euklidische Ebene ge- (oder er-) funden.

Unsere Wahl (eigentlich die von Beltrami) ist Poincarés Halbebenenmodell der hyperbolischen Geometrie:
Punkte sind die Elemente der oberen Halbebene $\mathcal{H}$.
Geraden gibt es in zwei Sorten:

- Schnitte von Geraden, die zur y-Achse parallel sind, mit $\mathcal{H}$
- Schnitte von Kreisen, deren Mittelpunkt auf der x-Achse liegt, mit $\mathcal{H}$.

Schauen Sie Seite 10.9 nochmal an.

Jetzt kann man Axiome nachprüfen:
Zu zwei verschiedenen Punkten in $\mathbb{H}$ gibt es genau eine Gerade.
Zwei verschiedene Punkte auf einer Geraden bestimmen diese.
Es gibt drei Punkte in $\mathbb{H}$, die nicht auf derselben Gerade liegen.
usw
Aber genau ein Axiom ist nicht erfüllt: Das Parallelenaxiom, das verlangt, daß zu einer Gerade g und einem nicht auf $\mathbb{R}g$ liegenden Punkt P genau eine Gerade h existiert, die P enthält und g nicht schneidet.
Beispiele in $\mathbb{H}$?
Das beweist, daß das Parallelen axiom unabhängig von den anderen Axiomen ist – man kann es nicht als Satz aus den anderen Axiomen ableiten. (Das hatte man 2000 Jahre lang versucht, bis Gauß und im Detail Bolyai und Lobatschewski die Unabhängigkeit erkannten. Bolyai und Lobatschewski entwickelten mit der hyperbolischen Geometrie die erste nichteuklidische Geometrie.)

Strecken sind Geradenstücke und die kürzeste Verbindung zwischen zwei Punkten (wenn man den Abstand richtig definiert). Wenn man erlaubt, daß Ecken von Dreiecken auf der x-Achse liegen, ist das ~~rote~~ grüne Ding auf Seite 1.11 ein Dreieck – mit parallelen Seiten und zwei Winkeln 0. Die hyperbolische Winkelsumme im Dreieck ist generell kleiner als π. Und Kongruenz von Dreiecken hängt von der Winkelsumme ab. ← Die Winkel werden wie in der euklidischen Ebene gemessen.
Die Möbius-Transformationen bilden Geraden oder Kreise in Geraden oder Kreise ab, also auch Strecken in Strecken und Dreiecke in Dreiecke. und sie erhalten Winkel
Daher müssen wir auch Fals Dreieck akzeptieren. mit Winkelsumme 2π/3
Im Sinne von Felix Kleins Erlanger Programm kann man auch sagen: die hyperbolische Geometrie von $\mathbb{H}$ ist dadurch festgelegt, daß die Gruppe der Möbius-Transformationen als Symmetriegruppe gewählt wurde.

Es gibt auch elliptische Geometrie: In einer elliptischen Ebene schneiden sich alle Geraden, es gibt also keine Parallelen und damit ist das Parallelenaxiom wieder gescheitert.
In der Differentialgeometrie findet man die Geometrie der hyperbolischen Ebene wieder bei Flächen mit negativer Gauß-Krümmung (Sattelflächen, Pseudosphären).
Die Beziehungen zu den Kettenbrüchen kann man in diesen Bereichen weiterverfolgen und vertiefen.

Die Äquivalenz von reellen Zahlen (oder Punkten in $\mathbb{R}$) durch die Operation der Modulgruppe auf der Kettenbruchentwicklung, findet man in der Zahlentheorie wieder bei der Äquivalenz von Gittern durch eine $PSL(2,\mathbb{Z})$-Operation, was dann wieder zur Codierungstheorie führt, aber auch zu aktuellen Themen der analytischen Zahlentheorie, wie Modulformen, die dann wieder mit einfachen Gruppen, Kugelpackungen und anderen interessanten Themen zusammenhängen.

Wie viele andere Themen der Zahlentheorie illustrieren Kettenbrüche sehr deutlich die Einheit der Mathematik, die Verbindungen zwischen (scheinbar) verschiedenen Gebieten und die Zusammenhänge zwischen elementaren Fragen, Kuriositäten und tiefen Einsichten.