Sei $G \subset S_n$ die Monodromiegruppe

$G = \langle \sigma_\gamma \mid \gamma \text{ geschl. Schleife} \rangle \subset S_n$

Satz: $G \subset Gal(L/\mathbb{C}(z))$ (16.16)

Beweis: $\mathbb{C}(z)[t_1,\dots,t_n] \to L$

$t_j \longmapsto f_{a,b_j}$

ist ein surjektiver Ringhomomorphismus.

Zu zeigen ist:

Ist $F = F(t_1,\dots,t_n) \in \ker(\Phi)$

$\Rightarrow F(t_{\sigma_\gamma(1)},\dots,t_{\sigma_\gamma(n)}) \in \ker(\Phi)$

Folgt mit analytischer Fortsetzung

$F(z, f_{a,b_1},\dots,f_{a,b_n}) \equiv 0$

$\Rightarrow F(z, f_{a,b_{\sigma_\gamma(1)}},\dots,f_{a,b_{\sigma_\gamma(n)}}) \equiv 0$

Wdh.:

$P(z,w) = a_n(z)w^n + \dots + a_0(w) \in \mathbb{C}[z,w]$

$V = \{c \in \mathbb{C} \mid a_n(c) \cdot R(P, \frac{\partial P}{\partial w})(c) \neq 0\}$

$\uparrow 1\text{-}1$

$\tilde{V} = \{(a,b) \in \mathbb{C} \mid P(a,b) = 0, a \in V\}$

$f_{a,b_1}, \dots, f_{a,b_n} \in \mathbb{C}\{z-a\} \subset \tilde{K} = \mathbb{C}\{z-a\}[(z-a)^{-1}]$

Auflösung von $P(z,w)$ nach w

$L = \mathbb{C}(x)[f_{a,b_1}, \dots, f_{a,b_n}]$ Zerfällungskörper von $P \in \mathbb{C}(x)[w]$,

$G \subset S_n$ die Monodromiegruppe erzeugt von γ_σ, σ geschl. Weg in V mit $AP = EP = a$

Satz: $G \subset Gal(L|\mathbb{C}(x))$ (16.16)

Beweis:

$$\begin{array}{ccccc} 0 & \longrightarrow & \ker\varphi & \longrightarrow & \mathbb{C}(z)[T_1,\dots,T_n] \xrightarrow{\varphi} L \\ & & \| & & \downarrow t_i \mapsto t_{\gamma_\sigma(i)} \quad \downarrow \Phi_\sigma \quad \downarrow t_i \mapsto f_{a,b_i} \\ & & F(z,t_{\gamma_\sigma(1)},\dots,t_{\gamma_\sigma(n)}) & & \\ & & \uparrow & & \\ \text{Brauchen} & & \ker(\varphi) & & \mathbb{C}(z)[T_1,\dots,T_n] \xrightarrow{\varphi} L \end{array}$$

Dies folgt mit der analytischen Fortsetzung

$F(z, f_{a,b_1}, \dots, f_{a,b_n}) \equiv 0$

$\Rightarrow F(z, f_{a,b_{\gamma_\sigma(1)}}, \dots, f_{a,b_{\gamma_\sigma(n)}}) \equiv 0$ nach dem Identitätssatz

Satz: $\mathrm{Fix}(G) = \mathbb{C}(z)$ (16.17)

Beweis: klar!

Bemerkung: Nach dem Hauptsatz folgt daraus

$$G \subset \mathrm{Gal}(L \mid \mathbb{C}(z))$$

die größte Untergruppe also:

Satz: $\mathrm{Gal}(L/\mathbb{C}(z)) = G$ (16.18)

$$\mathrm{Gal}\left(\underbrace{\mathbb{P}(z,w)}_{L} \in \mathbb{C}(z)[w]\right)$$

Beweis: klar!

Zurück zum eigentlichen Beweis:

Sei $f \in \mathbb{C}(z)[f_0(z), \dots, f_{n-1}(z)] = L$ und $f \in \mathrm{Fix}(G)$

$\Rightarrow f \in \mathbb{C}(z)[t_1, \dots, t_n]^G$

f ist lokal eine meromorphe Funktion von z

durch die analytische Fortsetzung erhalten wir

eine wohldefinierte meromorphe Funktion auf V,

da $f \in \mathrm{Fix}(G)$ und nach dem Identitätssatz.

$\mathbb{P}^1 = \mathbb{C} \cup \{\infty\} = \hat{\mathbb{C}}$

$\Rightarrow$ In den Punkten von $\mathbb{P}^1 \setminus V$ hat f keine wesentlichen

Singularitäten, da die Werte von f lokal nahe c nicht dicht in $\mathbb{C}$

sind, sondern gegen $F(c, d_1, \dots, d_n)$ stehen,

wobei die Vielfachheiten hoch können oder

eventuell $d = \infty$ auftritt.

$\Rightarrow$ f ist eine meromorphe Funktion

auf $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\} = \mathbb{P}^1$ und $f \in \mathbb{C}(z)$

□

Bemerkung: Meromorphe Funktionen f auf RF R soll man als holomorphe Abbildung

$$f: R \to \hat{\mathbb{C}} = \mathbb{P}^1$$

auffassen.

16.18 Corollar

Ist $P(z,w)$ irreduzibel, dann operiert G transitiv auf $f_{a,b_1}, \dots, f_{a,b_n}$.

Beweis: Galoisgruppen irreduzibler Polynome operieren transitiv auf den Wurzeln.

In der Tat ist $f_{a,b_1}, \dots, f_{a,b_n}$ eine Bahn unter G.
Dann ist $\prod_{j=1}^{n} (w - f_{a,b_j}) = Q(z,w) \in \mathbb{C}[z-a][w] \subset \mathbb{C}[w]$
ein Polynom, welches invariant unter Operation von G ist, also analytische Fortsetzung zeigt

$$Q(z,w) \in \mathbb{C}(z)[w],$$

da alle Koeffizienten G-invariant sind
$\Rightarrow Q(z,w)$ ist ein Teiler von $P(z,w)$

$P(z,w) \in \mathbb{C}[z,w]$ irreduzibel

$\Rightarrow$ (Satz von Gauß) $P \in \mathbb{C}(z)[w]$ irreduzibel

$\Rightarrow Q$ teilt $P(z,w) \Rightarrow d_w P = d_w Q$

$\Rightarrow \deg_z Q = R$, also $n = d$

□

16.18 Corollar

Für $P(z,w) \in \mathbb{C}[z,w]$ irreduzibel ist die Nullstellenmenge

$Z = \{(a,b) \in \mathbb{C}^2 \mid P(a,b) = 0\}$

wegzusammenhängend.

Beweis: $\tilde{V}$ wegzusammenhängend haben wir gezeigt.

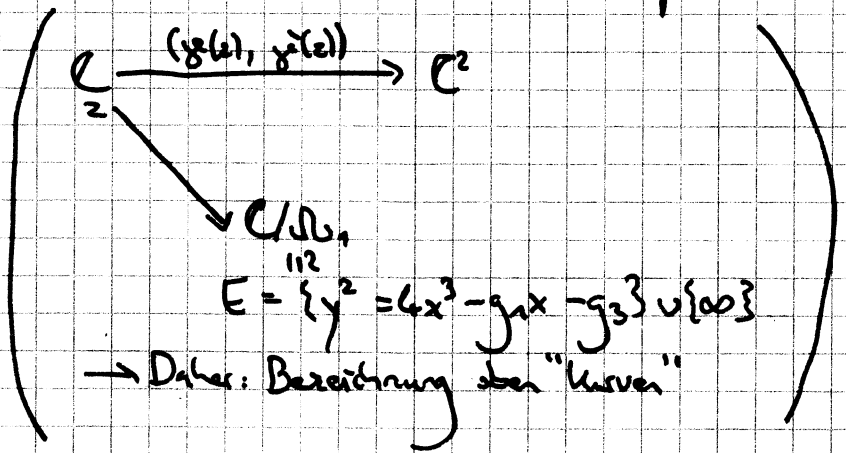
$Z \setminus \tilde{V}$ hat keine Punkte, die nicht in $\tilde{V}$ liegen,

$\tilde{V} = Z$.

□

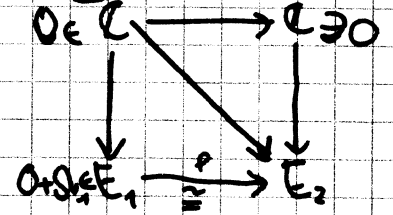
17. Moduln

Seien $E_1 = \mathbb{C}/\Omega_1$, $E_2 = \mathbb{C}/\Omega_2$ zwei elliptische Kurven



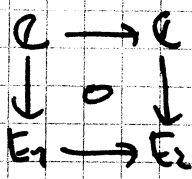
→ Daher: Bezeichnung oben "Kurven"

Wir fragen, wann sind E_1 und E_2 isomorph als RF



$\in$ $0 + \Omega_1 \longmapsto 0 + \Omega_2$

Die Komposition $\mathbb{C} \to E_1 \xrightarrow{\varphi} E_2$ lässt sich zu einer Abbildung $\mathbb{C} \to \mathbb{C}$ liften, sodass das Diagramm



kommutativ macht, da $\mathbb{C}$ einfach zusammenhängend ist.

Wegen $f(0 + \Omega_1) = 0 + \Omega_2$,
muss $f(\Omega_1) \subset \Omega_2$ gelten,
allgemeiner muss
$f(z+w) - f(z) \in \Omega_2 \quad \forall w \in \Omega_1$
gelten.

Da Ω_2 diskret ist, ist also

$$f(z+w)-f(z)$$

eine konstante Funktion

$$\Rightarrow f'(z+w)-f'(z)\equiv 0$$

Es folgt: f' ist Ω_1-periodische holomorphe Funktion

Nach Liouville $\Rightarrow$ f' ist konstant, $f'(z)=c$

$\Rightarrow f(z)=cz+d$ und wegen $f(0)=0$ folgt $d=0$,
also $f(z)=cz$

Wegen $f(\Omega_1)\subset\Omega_2 \Rightarrow c\Omega_1\subset\Omega_2$.

Ist nun f bijektiv, so können die gleiche Aussage
für f^{-1} treffen

$$\Rightarrow \tfrac{1}{c}\Omega_2\subset\Omega_1$$

$$\Rightarrow c\Omega_1=\Omega_2$$

Damit ist gezeigt:

17.1 Satz

$E_1=\mathbb{C}/\Omega_1$ und $E_2=\mathbb{C}/\Omega_2$ zwei elliptische Kurven sind
isomorph genau dann, wenn es ein $c\in\mathbb{C}^*$ gibt,
sodass $c\Omega_1=\Omega_2$.

Beweis: klar!

□

17.2 Corollar

Durch Multiplikation mit einem geeigneten $c \in \mathbb{C}^*$ können wir erreichen, dass die Perioden ω_1, ω_2 ($\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$) die Gestalt $1, \tau$,

$$\Omega = \mathbb{Z} \oplus \tau\mathbb{Z}$$

mit

$$\tau \in \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

haben

Beweis: Wir können mit $\frac{1}{\omega_1} \in \mathbb{C}^*$ das Gitter multiplizieren

Dann ist $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$.

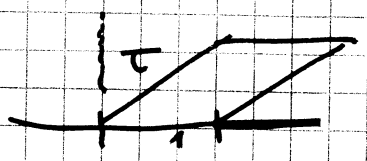
Gilt $\mathrm{Im}\frac{\omega_2}{\omega_1} < 0$, so multiplizieren wir stattdessen mit $\frac{1}{\omega_2}$.

Also können

$$c\Omega = \mathbb{Z} + \tau\mathbb{Z}$$

mit $\tau \in \mathbb{H}$ erreichen. □

Bild:



Bemerkung: Es bezeichne im Folgenden

E_τ die elliptische Kurve mit Periodengitter $\mathbb{Z} + \tau\mathbb{Z}$.

Wann sind zwei Kurven $E_{\tau_1} \cong E_{\tau_2}$?

17.3 Satz

$E_{\tau_1} \cong E_{\tau_2}$ genau dann, wenn es eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ gibt, sodass $\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}$.