Korrespondenzen und Hyperelliptische Kurven

– gemeinsam mit G. Frey; vgl. [FK] (2012)

1. Einleitung.

B. Smith (2008) endeckte, daß der diskrete Logarithmus der Gruppen, die von Jacobischen von hyperelliptischen Kurven vom Geschlecht 3 über $k = \mathbb{F}_p$ $(p > 3)$ herkommen, nicht so sicher ist, wie man bisher angenommen hatte.

Grund: die sogenannte trigonale Konstruktion.

Diese konstruiert zu einer gegeben hyperelliptischen Kurve C/k vom Geschlecht 3 eine zweite (i.a. nicht-hyperelliptische) Kurve D/k und eine Isogenie

$$T : J_C \to J_D$$

der Jacobischen Varietäten. Diese Konstruktion geht auf Recillas (1974) und Donagi/Livné (1999) zurück. Genauer:

Donagi/Livné (1999) betrachten eine Entartung der Konstruktion von Recillas, die dann auf hyperelliptische Kurven vom Geschlecht 3 anwendbar ist.

Ziel: Ein elementarer Zugang zu dieser Theorie mit Hilfe von gewissen S_4-Überlagerungen.

2. Spezielle S_4-Überlagerungen.

Definition: Es sei k ein algebraisch abgeschlossener Körper und sei $f : C \to C'$ eine separable Überlagerung von Kurven über k. Sei $\tilde{f} : \tilde{C} \to C'$ die Galoissche Hülle von f. Dann heißt $\mathrm{Mon}(f) = \mathrm{Aut}(\tilde{f})$ die Monodromiegruppe von f.

Bezeichnung: Es sei $\mathrm{Ram}(f) = \{P \in C_1 : e_P(f) > 1\}$ die Menge der Verzweigungspunkte und $\mathrm{Br}(f) := f(\mathrm{Ram}(f))$ der Verzeigungsort (branch locus) von f.

Satz 1: Es sei $\mathrm{char}(k) \neq 2$, und sei

$$f = f_2 \circ f_1 : C \to C_1 \to \mathbb{P}^1$$

eine Überlagerung mit den folgenden Eigenschaften:

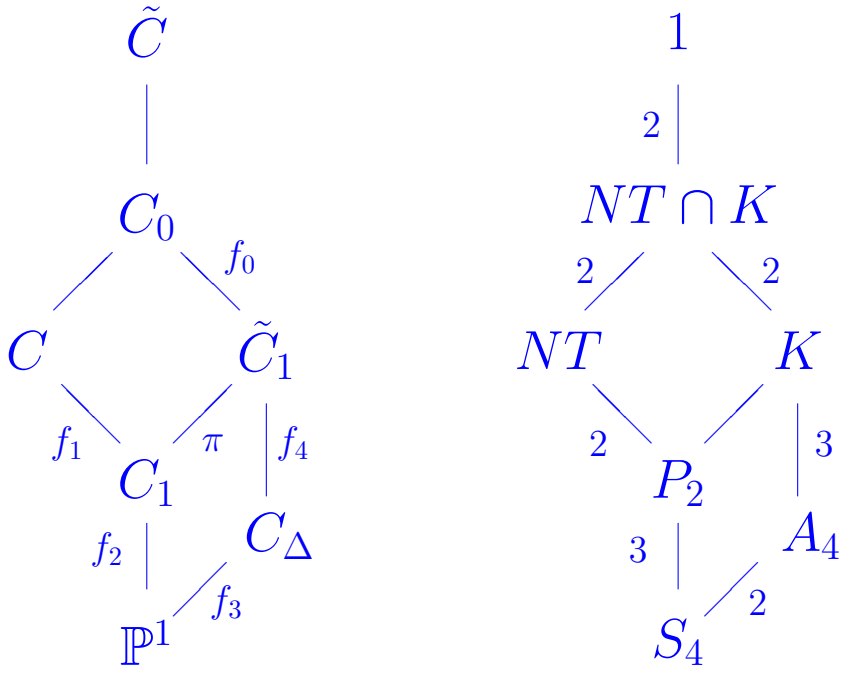
1) $\deg(f_2) = 3$ und $f_2^{-1}(P) \not\subset \mathrm{Ram}(f_2), \forall P \in \mathbb{P}^1$;

2) $\deg(f_1) = 2$, $\#(f_1^{-1}(f_1(P)) \setminus \mathrm{Ram}(f)) = 1, \forall P \in \mathrm{Ram}(f)$, und $\mathrm{Br}(f_1) \cap \mathrm{Ram}(f_2) = \emptyset$.

Dann ist $\mathrm{Mon}(f_2) \simeq S_3$ und $\mathrm{Mon}(f) \simeq S_4$.

Zusatz: In der obigen Situation sei $f_3 : C_\Delta \to \mathbb{P}^1$ die Überlagerung, die zur Adjunktion der Diskriminante von f_2 gehört. Dann ist $\tilde{f}_2 = f_3 \circ f_4 : \tilde{C}_1 \to \mathbb{C}_\Delta \to \mathbb{P}^1$, wobei $f_4 : \tilde{C}_1 \to C_\Delta$ eine zyklische, unverzweigte Überlagerung mit $\deg(f_4) = 3$ ist.

Bemerkung: Wir haben also die folgende Situation von Überlagerungen mit zugehörigen Galoisgruppen:



Bemerkung: Es sei $s := \#\,\mathrm{Ram}(f_2)$. Nach Riemann-Hurwitz ist dann

$$g_{C_1} = s/2 - 2, \quad g_{C_\Delta} = s/2 - 1,$$

also muß $s \geq 4$ sein. Ferner sei $2t = \#\,\mathrm{Br}(f_1)$. Dann gilt

$$g_C = s + t - 5, \quad g_{\tilde{C}} = 6(s + t - 4) + 1.$$

Außerdem sieht man, daß die S_4-Überlagerung $\tilde{f} : \tilde{C} \to \mathbb{P}^1$ den folgenden Verzweigungstyp hat: s Konjugiertenklassen von Transpositionen und t Konjugiertenklassen von $(2, 2)$-Zykel.

Bezeichnung: Es sei $\tilde{\mathcal{H}}_{s,t}(k)$ die Menge der Isomorphieklassen von Überlagerungen $f = f_2 \circ f_1 : C \to \mathbb{P}^1$ wie in Satz 1 zu vorgegebenen s, t. Dann kann man zeigen, daß (der Funktor) $\tilde{\mathcal{H}}_{s,t}$ fein repräsentiert wird durch einen Hurwitzraum $\tilde{\mathbb{H}}_{s,t}$ der Dimension $s + t$. Der Quotient $\mathbb{H}_{s,t} := \mathrm{Aut}(\mathbb{P}^1)\backslash\tilde{\mathbb{H}}_{s,t}$ hat demnach die Dimension $s + t - 3$.

3. Der hyperelliptische Fall.

Vorbemerkung: Es sei jetzt $s = 4$. Dann ist $g_{C_1} = 0$, also ist C hyperelliptisch. Ferner sind dann $E := C_\Delta$ und $E' := \tilde{C}_1$ elliptische Kurven, und daher ist

$$f_4 : E' = \tilde{C}_1 \ \to \ E = C_\Delta$$

(nach Wahl geeigneter Nullpunkte) eine 3-Isogenie.

Sei $C_0 = \tilde{C}/(NT \cap K)$ die Normalisierung von $C \times_{C_1} \tilde{C}_1$, und sei

$$f_0 : C_0 \ \to \ \tilde{C}_1 = E'$$

die zugehörige Überlagerung (s. Diagramm). Der Diskriminantendivisor $D := \mathrm{Disc}(f_0) = (f_0)_*(\mathrm{Diff}(f_0)) \in \mathrm{Div}(E')$ ist reduziert vom Grad $4t$. Bei geeigneter Wahl des Nullpunktes kann man D wie folgt zerlegen:

$$D = D_1 + [-1]^*_{E'} D_1, D_1 = D_{11} + D_{12} \text{ mit } (f_4)_* D_{11} = (f_4)_* D_{12}.$$

Wir erhalten also einen reduzierten Divisor D_{11} vom Grad t auf E', der aber nicht ganz eindeutig bestimmt ist.

Umgekehrt: Sei E'/K eine elliptische Kurve mit 3-Torsionpunkt $P_3 \in E'[3](k)$, und sei

$$f_4 : E' \ \to \ E$$

die zugehörige 3-Isogenie mit Kern $\langle P_3 \rangle$.

Ferner sei ein reduzierter Divisor D_{11} vom Grad t auf E' gegeben, zu dem es einen Divisor D_{12} gibt mit der Eigenschaft, daß $(f_4)_* D_{11} = (f_4)_* D_{12}$. Außerdem sollen $(f_4)_* D_{11}$ und $D := D_{11} + D_{12} + [-1]^*_{E'}(D_{11} + D_{12})$ reduziert sein.

Sei $f_1 : C \to \mathbb{P}^1$ eine hyperelliptische Kurve mit

$$\mathrm{Disc}(f_1) \;=\; \pi_*(D_{11} + D_{12}),$$

wobei

$$\pi : E' \;\to\; E'/[-1]_{E'} = \mathbb{P}^1,$$

die "Weierstraß Überlagerung" von E' ist. Ferner sei

$$f_2 : E \;\to\; E/[-1]_E = \mathbb{P}^1$$

die Weierstraß Überlagerung von E. Dann ist

$$f = f_2 \circ f_1 : C \;\to\; \mathbb{P}^1 \;\to\; \mathbb{P}^1$$

eine $(2,3)$-Überlagerung vom Typ von Satz 1, deren Galois-Hülle $\tilde{f} : \tilde{C} \to \mathbb{P}^1$ eine S_4-Überlagerung ist, die über f_4 (usw.) faktorisiert.

Wir erhalten also:

Satz 2. Es sei $\mathcal{E}_3 \to X_1(3)$ die universelle elliptische Kurve mit 3-Torsionspunkt. Dann gibt es eine dominante rationale Abbildung

$$\Phi_t : \underbrace{\mathcal{E}_3 \times_{X_1(3)} \ldots \times_{X_1(3)} \mathcal{E}_3}_{t \text{ Faktoren}} \to \mathbb{H}_{4,t},$$

die endliche Fasern hat.

4. Die trigonale Konstruktion.

Bezeichnungen: Es sei wieder $f = f_2 \circ f_1 : C \to C_1 \to \mathbb{P}^1$ eine $(2,3)$-Überlagerung wie in Satz 1 mit $g_{C_1} = 0$. Wie vorher sei $\tilde{f} : \tilde{C} \to \mathbb{P}^1$ die zugehörige S_4-Überlagerung und $NT = \mathrm{Gal}(\tilde{C}/C)$. Sei:

$\tau \in NT$ eine der zwei Transpositionen in NT,
$S \simeq S_3$ eine der zwei Stabilisatoren in S_4 mit $\tau \in S$.

Setzen wir $T = \tilde{C}/(S \cap NT)$ und $D = \tilde{C}/S$, so haben wir zwei Überlagerungen

$$\varphi_1 : T \to C \quad \text{und} \quad \varphi_2 : T \to D,$$

die eine Korrespondenz zwischen C und D definieren; es gilt offenbar

$$\deg(\varphi_1) = 2 \quad \text{und} \quad \deg(\varphi_2) = 3.$$

Wir erhalten somit einen Homomorphismus

$$T_* = T_{\varphi_1,\varphi_2} = \varphi_{2*} \circ \varphi_1^* : J_C \to J_D$$

zwischen den zugehörigen Jacobischen Varietäten.

Satz 3. Ist $g_C = 3$, so ist T_* ist eine Isogenie vom Grad 8.

Bemerkungen: 1) Donagi/Livné (1999) weisen nach, daß es so eine Isogenie gibt, ohne aber eine zugehörige Korrespondenz genau anzugeben. (Der Beweis benützt die Konstruction von Recillas und ein Degenerationsargument.)

2) Smith (2008) benützt in seinem Artikel (ohne Beweis) die Tatsache, daß die von Donagi/Livné konstruierte Isogenie durch eine (explizite) $(2,3)$-Korrespondenz induziert wird.

3) Der Name "trigonale Konstruktion" kommt daher, daß man zu einer vorgegeben hyperelliptischen Kurve C/k vom Geschlecht 3 stets eine trigonale Unterlagerung $f_2 : \mathbb{P}^1 \to \mathbb{P}^1$ konstruieren kann derart, daß $f = f_2 \circ f_1$ eine $(2,3)$-Überlagerung (wie in Satz 1) ist. Genauer gilt:

Satz 4. Es gibt eine dominante rationale Abbildung

$$\Psi_4 : \mathbb{H}_{4,4} \to \mathcal{M}_{H,3}$$

vom Grad 2 von dem Modulraum $\mathbb{H}_{4,4}$ der hyperelliptischen $(2,3)$-Überlagerungen (mit $g_C = 3$) zu dem Modulraum $\mathcal{M}_{H,3}$ der hyperelliptischen Kurven vom Geschlecht 3.

Bemerkung: In Smith (2008) (wie auch in Donagi/Livné (1999)) wird die trigonale Unterlagerung durch die Lösung gewisser Tangentenbedingungen konstruiert. In [FK] (2012) geben wir ein explizites lineares Gleichungsystem an, das aus 8 Gleichungen in 7 Variablen besteht, deren Lösung diesen Morphismus bestimmt.

5. Allgemeine S_4-Überlagerungen.

Vorbemerkung: Wie erwähnt, ist die von Donagi/Livné betrachtete Situation eine Entartung der originalen Konstuktion von Recillas (1974). Der folgende Satz unfaßt beide Situationen (und viel mehr).

Bezeichnung: Ist $f : X \to Y$ eine Überlagerung von Kurven, so sei

$$P(f) := \mathrm{Ker}(f_*)^0 \subset J_X$$

die 0-Zusammenhangskomponente des Kerns der Abbildung $f_* : J_X \to J_Y$. ("Verallgemeinerte Prymsche Varietät".)

Bemerkung: $P(f)$ ist eine abelsche Untervarietät von J_X der Dimension $g_X - g_Y$. Ferner gibt es eine (eindeutig bestimmte) Surjection $\pi_{P(f)} : J_X \to P(f)$ mit

$$i_{P(f)} \circ \pi_{P(f)} = [\deg(f)]_{J_X} - f^* f_*.$$

Bezeichnungen: Es sei $G \leq \mathrm{Aut}(X)$ eine endliche Gruppe und

$$\pi = \pi_G : X \to Y := X/G$$

der Quotientenmorphismus. Für eine Untergruppe $H \leq G$ sei $X_H = X/H$ und $f_H : X_H \to Y$ die induzierte Überlagerung. Es gilt also

$$\pi = f_H \circ \pi_H : X \stackrel{\pi_H}{\to} X_H \stackrel{f_H}{\to} Y.$$

Es seien $H_1, H_2 \leq G$ zwei Untergruppen, und sei $H_{12} = H_1 \cap H_2$. Dann haben wir zwei induzierte Abbildungen

$$f_i = f_{H_{12},H_i} : X_{H_{12}} \to X_{H_i}, \quad i = 1, 2.$$

Also ist (f_1, f_2) eine Korrespondenz, die einen Homomorphismus

$$T_{H_1,H_2} = (f_2)_* \circ f_1^* : J_{H_1} := J_{X_{H_1}} \to J_{H_2} := J_{X_{H_2}}.$$

der Jacobischen Varietäten induziert.

Bemerkung: Sind $H_i \leq K_i \leq G$ vier Untergruppen, so definiert

$$\tilde{T}_{H_1,H_2} := \pi_{P(f_{H_2,K_3})} \circ T_{H_1,H_2} \circ i_{P(f_{H_2,K_2})}$$

einen Homomorphismus

$$\tilde{T}_{H_1,H_2} : P(f_{H_1,K_1}) \to P(f_{H_2,K_2})$$

der verallgemeinerten Prymschen Varietäten.

Bezeichnung: Es sei $G = S_4$ und

$$\begin{aligned} NT &= \langle \tau, \sigma^2 \rangle, \text{ wobei } \tau = (12), \sigma = (1324), \\ P_2 &= \langle \tau, \sigma \rangle, \text{ eine 2-Sylowuntergruppe von } S_4, \\ S &= \langle \tau, \rho \rangle, \text{ der Stabilisator der Ziffer } 4 \ (\rho = (123)). \end{aligned}$$

Satz 5. Es sei $\pi : X \to Y$ eine S_4-Überlagerung, und sei $f_1 = f_{NT,P_2}$ und $f_2 = f_{S,G}$. Dann sind

$$\tilde{T}_{NT,S} : P(f_1) \to P(f_2) \quad \text{und} \quad \tilde{T}_{S,NT} : P(f_2) \to P(f_1)$$

zwei Isogenien mit

$$\tilde{T}_{S,NT} \circ \tilde{T}_{NT,S} = [16]_{P(f_1)} \quad \text{und} \quad \tilde{T}_{NT,S} \circ \tilde{T}_{S,NT} = [16]_{P(f_2)}.$$

Bemerkung: Im Fall, daß $Y \simeq X_{P_2} \simeq \mathbb{P}^1$ ist, so gilt offenbar $P(f_1) = J_{NT}$ und $P(f_2) = J_S$. Hier gilt sogar, daß

$$T_{S,NT} \circ T_{NT,S} = [2]_{J_{NT}} \quad \text{und} \quad T_{NT,S} \circ T_{S,NT} = [2]_{J_S}.$$