Grothendiecksche Kinderzeichnungen und Galoistheorie
Habilitationsvortrag von Dirk Kussin, Paderborn, 21. Oktober 2004

1. Galoistheorie

In diesem Vortrag geht es um die Vorstellung eines von Grothendieck entwickelten Konzeptes, von dem man sich neue Einsichten bei der Lösung des Umkehrproblems der Galoistheorie erhofft, und das auch für sich genommen sehr interessant ist.

1.1. **Das Umkehrproblem der Galoistheorie.** Das klassische Umkehrproblem (für $k = \mathbb{Q}$) der Galoistheorie lautet so:

Problem 1.1 (Hilbert (1892))**.** *Gibt es zu jeder endlichen Gruppe G eine endliche Galoiserweiterung $K/\mathbb{Q}$ mit* $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$*?*

Dieses Problem ist noch immer ungelöst[1]. Wir wollen das Problem umformulieren.

1.2. **Die algebraischen Zahlen.** Sei $\overline{\mathbb{Q}}$ die Menge aller algebraischen Zahlen[2] in $\mathbb{C}$. Dies ist der algebraische Abschluss von $\mathbb{Q}$, insbesondere eine algebraische Körpererweiterung von $\mathbb{Q}$.

[1]Für z. B. $k = \mathbb{C}(x)$ (x transzendent) hat das Umkehrproblem eine positive Antwort, wie etwa aus dem Riemannschen Existenzsatz folgt. Man betrachtet unverzweigte Überlagerungen von $\mathbb{P}^1 \setminus \{y_1, \ldots, y_{n+1}\}$. Die Fundamentalgruppe dieses Raums ist die freie Gruppe in n Erzeugern.

Für $k = \mathbb{Q}(t)$ hat man das reguläre Umkehrproblem der Galoistheorie. Es folgt aus Hilberts Irreduzibilitätssatz (1892), dass sich jede endliche reguläre Galoiserweiterung über $\mathbb{Q}(t)$ spezialisieren lässt zu einer über $\mathbb{Q}$ mit isomorpher Galoisgruppe.

Aber auch für $k = \mathbb{Q}$ gibt es für Klassen von Gruppen eine positive Antwort: Z. B. gilt die Aussage für jede endliche abelsche Gruppe G. Dies folgt, weil jedes solche G Quotient der Einheitengruppe $E(\mathbb{Z}_n)$ für ein n ist (schreibe $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$. Für jedes n gibt es eine Primzahl p mit $p \equiv 1 \mod n$; dann ist $\mathbb{Z}_n$ Quotient von $\mathbb{Z}_{p-1} = E(\mathbb{Z}_p)$, die wiederum Galoisgruppe des n-ten Kreisteilungskörpers ist. Allgemeiner gilt der Satz von Shafarevich (1954), dass jede auflösbare endliche Gruppe als Galoisgruppe über $\mathbb{Q}$ realisierbar ist. (Man beachte übrigens, dass nach dem Satz von Feit und Thompson jede Gruppe ungerader Ordnung auflösbar ist.) Dies folgt aus dem noch allgemeinerem Einbettungssatz von Shafarevich (1958): Über einem Zahlkörper ist jedes zerfallende endliche Einbettungsproblem mit einem nilpotenten Kern lösbar. Dabei versteht man unter einem Einbettungsproblem die Frage, ob es zu einer vorgegebenen Galoiserweiterung K/k mit der Galoisgruppe G und einer kurzen exakten Folge $1 \to H \to \overline{G} \to G \to 1$ eine Galoiserweiterung L/k gibt mit $L \supset K$ und $\mathrm{Gal}(L/k) \simeq \overline{G}$ gibt. Das Problem heißt endlich, falls $\overline{G}$ endlich ist, zerfallend, wenn die Folge zerfällt. Das Resultat für auflösbare Gruppen folgt, weil jede endliche auflösbare Gruppe sich schreiben lässt als Quotient eines semi-direkten Produkts einer nilpotenten mit einer auflösbaren Gruppe, die kleinere Ordnung hat.

Weitere Realisierungen, mit Hilfe des sog. Rigiditätssatzes: die 26 sporadischen einfachen Gruppen (bis auf evtl. die Mathieu Gruppe M_{23}) (Matzat et. al. 1986)), davon das Monster (Thompson 1984)

[2]Ein $z \in \mathbb{C}$ heißt algebraisch, falls es $a_1, \ldots, a_n \in \mathbb{Q}$ gibt mit $z^n + a_1 z^{n-1} + \cdots + a_n = 0$. Das normierte Polynom $P \in \mathbb{Q}[T]$ kleinsten Grades mit $P(x) = 0$ ist das Minimalpolynom von x über $\mathbb{Q}$.

Es gilt[3]

$$\overline{\mathbb{Q}} = \cup\{K \mid K/\mathbb{Q} \text{ endlich galoissch}\}.$$

Es folgt, dass $\overline{\mathbb{Q}}/\mathbb{Q}$ eine (unendliche) Galoiserweiterung ist[4].

1.3. **Die absolute Galoisgruppe.** Sei

$$\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

die Galoisgruppe[5] von $\overline{\mathbb{Q}}$ über $\mathbb{Q}$. Sie heißt die *absolute Galoisgruppe*. Diese Gruppe verkörpert[6] die klassische Galoistheorie über $\mathbb{Q}$.

1.4. Γ **als topologische Gruppe.** Es gilt

$$\Gamma = \varprojlim\{\mathrm{Gal}(K/\mathbb{Q}) \mid K/\mathbb{Q} \text{ endlich galoissch}\},$$

d. h. Γ ist ein projektiver Limes endlicher Gruppen und daher *profinit*[7]. Γ ist überabzählbar, $\mathrm{Card}(\Gamma) = 2^{\aleph_0}$. Γ ist eine topologische Gruppe, die induziert wird durch die diskreten Topologien auf den endlichen GruppenGal$(K/\mathbb{Q})$, dann durch Produkttopologie induzierte.

- hausdorffsch, kompakt[8]
- total unzusammenhängend[9]

1.5. **Umformulierung des Umkehrproblems.** Äquivalent[10] zum Umkehrproblem ist die Frage:

Problem 1.2. *Ist jede endliche Gruppe G (ausgestattet mit der diskreten Topologie) ein stetiger Quotient von Γ?*

---

[3]Jedes Element $x \in \overline{\mathbb{Q}}$ ist algebraisch, daher Mitglied des Zerfällungskörper seines Minimalpolynoms, daher Element einer endlichen Galoiserweiterung.

[4]Eine Körpererweiterung K/k heißt galoissch, falls eine der folgenden drei äquivalenten Eigenschaften gilt:

(1) $K = \cup\{K \mid K/k \text{ endlich galoissch}\}$.
(2) K/k ist algebraisch, normal und separabel.
(3) Es gibt einen algebraischen Abschluss $\overline{k}/k$ und eine Teilmenge $S \subset k[T]$ von normierten Polynomen, so dass für alle $f \in S$ gilt $\mathrm{ggT}(f, f') = 1$ (die Polynome sind separabel) und $K = k(\alpha \in \overline{k} \mid f(\alpha) = 0 \text{ für ein } f \in S)$.

[5]Sie stimmt überein mit der Gruppe $\mathrm{Aut}(\overline{\mathbb{Q}})$ der Körperautomorphismen von $\overline{\mathbb{Q}}$, da diese den Primkörper $\mathbb{Q}$ automatisch festlassen.

[6]H. Lenstra meint dazu, dass man sagen könnte, dass Zahlentheorie das Studium dieser Gruppe ist.

[7]Oder proendlich.

[8]Folgt aus dem Satz von Tychonoff.

[9]Mehr noch: Γ ist vollständig, d. h. $Z(\Gamma)$ und $\mathrm{Out}(\Gamma)$ sind trivial (Neukirch 1977). $\Gamma \subset G$ normale Untergruppe $\Longrightarrow \Gamma$ direkter Summand.

[10]Dies folgt, weil die kanonischen Projektionen $\Gamma \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$ surjektiv und stetig sind; ein stetiger Quotient liefert einen abgeschlossenen Kern, und dann kann der Hauptsatz der Galoistheorie (für unendliche Körpererweiterungen) angewendet werden.

Ziel: Finde "einfach strukturierte" Menge $\mathcal{S}$ auf der Γ operiert, so dass $\Gamma < \mathrm{Aut}(\mathcal{S})$. Finde gute Galoisinvarianten, d. h. Eigenschaften, die invariant sind unter dieser Aktion.

Ein solche Menge wird z. B. die Menge der sogenannten Kinderzeichnungen sein.

2. Die Grothendieck-Korrespondenz

Wir beschreiben eine Korrespondenz zwischen sogenannten Kinderzeichnungen (das sind eingebettete Graphen auf Riemannschen Flächen) und gewissen Überlagerungen der Riemannsphäre. Diese Überlagerungen werden charakterisiert im nächsten, grundlegenden Satz, der gewissermaßen der Einstieg ist. Dieser Typ von Überlagerung kommt natürlicherweise in der inversen Galoistheorie vor (Stichwort: Rigiditätssatz (Shih, Belyi, Fried, Matzat, Thompson)).

2.1. **Der Satz von Belyi.**

Satz 2.1. *Sei X kompakte*[11] *(und zusammenhängende) Riemannsche Fläche (= glatte projektive*[12] *Kurve/$\mathbb{C}$). Äquivalent sind:*

(1) *X ist definiert*[13] *über $\overline{\mathbb{Q}}$.*
(2) *es gibt eine nicht-konstante meromorphe (bzw. rationale) Funktion $\beta : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ unverzweigt*[14] *außerhalb 0, 1, ∞.*

In diesem Fall kann auch β über $\overline{\mathbb{Q}}$ definert[15] *werden.*

Unter den Voraussetzungen des Satzes nennt man β eine Belyi-Abbildung, (X, β) ein Belyi-Paar. Ein Belyi-Paar ist topologisch nichts anderes[16] als eine in drei Punkten verzweigte Überlagerung von $\mathbb{P}^1(\mathbb{C})$.

Die Richtung (2)$\Longrightarrow$(1) wird traditionellerweise die "triviale" Richtung genannt und geht zurück auf A. Weil (1956).

Die Richtung (1)$\Longrightarrow$(2) wurde von A. Grothendieck vermutet, konnte aber nicht von ihm bewiesen werden. Unabhängig davon bewies Belyi diese Richtung 1979 auf eine trickreiche, aber überraschend einfache Weise, was Grothendieck sehr beeindruckte.

---

[11] Wollen wir immer annehmen.

[12] Jede kompakte Riemannsche Fläche lässt sich einbetten in einen $\mathbb{P}^n$, was aus dem Satz von Riemann-Roch folgt: Ein Divisor hinreichend großen Grades definiert eine solche Einbettung φ_D.

[13] D. h. es *gibt* Polynomgleichungen mit Koeffizienten in $\overline{\mathbb{Q}}$, die X definieren. Man sagt auch, X ist arithmetisch. Liegen hier alle Koeffizienten in einem Körper K ($\subset \overline{\mathbb{Q}}$), so heißt K *ein* Definitionskörper von X.

[14] d. h. die einzigen kritischen Werte sind (ohne Einschränkung) 0, 1, ∞. Ein kritischer Punkt $x \in X$ bedeutet $\beta'(x) = 0$. Das Bild $y = \beta(x)$ heißt dann kritischer Wert.

[15] Als rationale Funktion gibt es eine Darstellung, in der nur algebraische Koeffizienten vorkommen. Analog hat man den Begriff eines Definitionskörpers von (X, β).

[16] Riemannscher Existenzsatz.

2.2. **Kinderzeichnungen.** (Diese kommen in diesem Kontext so zustande:) Man betrachtet das Segment •———○ $= [0,\,1] \subset \mathbb{P}^1$, und den Punkt $* = \infty \in \mathbb{P}^1$.

Sei (X, β) ein Belyi-Paar.

Das Urbild $D = \beta^{-1}([0,1])$ ist ein 2-gefärbter[17], in X eingebetteter Graph. Die Färbung ist gegeben durch Punkte •, ○, die die Urbilder der Punkte 0 bzw. 1 sind. Urbilder von $*$ befinden sich in den Zellen/Flächen[18].

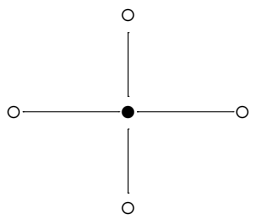
Allgemein ist eine (abstrakte) Kinderzeichnung[19] definiert als Tripel

$$X_0 \subset X_1 \subset X_2,$$

wobei X_2 das topologische Modell einer (kompakten, zusammenhängenden) Riemannschen Fläche X ist, X_0 ist eine endliche Menge von Punkten, $X_1 \setminus X_0$ ist eine disjunkte Vereinigung von Segmenten, und $X_2 \setminus X_1$ ist eine disjunkte Vereinigung von offenen Zellen, so dass man X_0 mit einer bipartiten Struktur (2-Färbung) ausstatten kann.

Bsp.: $\beta : \left\{ \begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ z & \mapsto & z^4. \end{array} \right.$

$\beta^{-1}([0,\,1]) =$



2.3. **Reine Kinderzeichnungen.** Hier hat jeder weiße Punkt ○ die Valenz (Ordnung/Grad) 2, d. h. lokal in jedem ○ sieht der Graph so aus: ———○——— .

2.4. **Reine Belyi-Abbildung.** Eine Belyi-Abbildung β heißt *rein*, falls sie über 1 verzweigt von der Ordnung 2 ist. Ist β eine Belyi-Abbildung, so ist $4\beta(1-\beta)$ eine reine Belyi-Abbildung. Insofern kann man sich ohne Einschränkung immer auf reine Belyi-Abbildungen und reine Dessins beschränken.

2.5. **3-Konstellationen.** (In dem Kontext kommen sie wie folgt zustande:) Sei (X, β) ein Belyi-Paar, also eine über 0, 1, ∞ verzweigte Überlagerung. Diese bestimmt die sogenannten Monodromie-Permutationen σ_0, σ_1, σ_∞ auf Faser $E = \beta^{-1}(y) = \{x_1, \ldots, x_n\}$, wobei $y \neq 0, 1, \infty$ fest gewählt ist. Diese haben die Eigenschaften

- $\sigma_0\sigma_1\sigma_\infty = id$ in S_n
- $\sigma_1^2 = id$ (falls β rein).
- $\langle \sigma_0,\, \sigma_1,\, \sigma_\infty \rangle$ operiert transitiv auf E.

[17] D. h. bipartiter.

[18] Nimmt man aus X die Kanten (und die Punkte) von D heraus, so hat man eine disjunkte Vereinigung von Zellen, jede homöomorph zu offenen Scheiben in $\mathbb{R}^2$.

[19] Wir sagen auch kurz: ein Dessin.

Die Monodromiegruppe $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle \subset S_n$ heißt auch die kartographische Gruppe von (X, β).

Allgemein nennt man ein Tripel $[\sigma_0, \sigma_1, \sigma_\infty]$ mit obigen Eigenschaften eine 3-Konstellation.

2.6. **Isomorphiebegriffe.**

(1) Seien $D \subset X$ und $D' \subset X'$ zwei Kinderzeichnungen, X und X' Riemannsche Flächen. Diese heißen isomorph, falls es einen *orientierungs-bewahrenden Homöomorphismus* zwischen den topologischen Modellen von X und X' gibt, der einen Isomorphismus zwischen den (2-gefärbten) Graphen D und D' induziert.

(2) Seien (X, β) und (X', β') Belyi-Paare (mit kritischen Werten 0, 1, ∞). Diese heißen isomorph, falls es eine *biholomorphe Abbildung* f zwischen den Riemannschen Flächen X und X' gibt mit $\beta' \circ f = \beta$.

(3) Zwei 3-Konstellationen heißen isomorph, falls die zugehörigen kartographischen Gruppen $\langle g_1, g_2, g_3 \rangle$ und $\langle g'_1, g'_2, g'_3 \rangle$ *konjugiert* sind, d. h. wenn es ein $h \in S_n$ gibt mit $g'_i = h^{-1} g_i h$ für $i = 1, 2, 3$.

Satz 2.2. *Es gibt Bijektionen zwischen den Mengen der Isomorphieklassen von*

(1) *(reinen) Kinderzeichnungen*
(2) *(reinen) Belyi-Paaren*
(3) *3-Konstellationen (mit Involution)*

Dabei entsprechen die Punkte der Kinderzeichnungen (samt den Punkten $*$ in den Zellen) den Urbildern der kritischen Werte 0, 1 *und* ∞ *bzw. den Zykeln in der Zykelzerlegung der Monodromie-Permutationen. Die Valenzen entsprechen den Verzweigungsordnungen bzw. den Zykellängen.*

Die Bijektion zwischen (1) und (2) wird induziert durch die Zuordnung[20] $(X, \beta) \mapsto \beta^{-1}([0, 1])$.

3. Galois Aktion

Sei $\sigma \in \Gamma$ und $D \subset X$ eine Kinderzeichnung. Dies definiert das zugehörige Belyi-Paar (X, β) (bis auf Isomorphie) definiert über $\overline{\mathbb{Q}}$. Man bildet dann (X^σ, β^σ), die man aus X und β dadurch erhält, indem man σ auf alle Koeffizienten anwendet. Dann ist X^σ wieder glatt[21] und

[20] Diese wird erst surjektiv auf den Isomorphieklassen, d. h. nicht jedes Dessin ist Urbild einer Belyi-Abbildung, aber isomorph zu einem solchen Urbild.

[21] Erweitere σ zu $\tilde{\sigma} \in \mathrm{Aut}(\mathbb{C})$ (nicht eindeutig!), und betrachte die diagonale Fortsetzung $\overline{\sigma} : \mathbb{C}^n \longrightarrow \mathbb{C}^n$. Sind $f_1, \ldots, f_m$ die X definierenden Polynome, so gilt $x \in X \;\Leftrightarrow\; f_i(x) = 0 \;\forall i \;\Leftrightarrow\; f_i^\sigma(\overline{\sigma} x) = \tilde{\sigma}(f_i(x)) = 0 \;\forall i \;\Leftrightarrow\; \overline{\sigma} x \in X^\sigma$. Nun ist x ein nicht-singulärer Punkt genau dann, wenn die Determinante mindestens eines maximalen Minors der Matrix $(\frac{\partial f_i}{\partial x_j})$ nicht verschwindet. Da dies ein polynomieller Ausdruck ist, überträgt sich diese Eigenschaft auf den Punkt $\overline{\sigma} x$.

β^σ ist offenbar eine Belyi-Abbildung. Die zugehörige Kinderzeichnung wird mit $D^\sigma \subset X^\sigma$ bezeichnet.

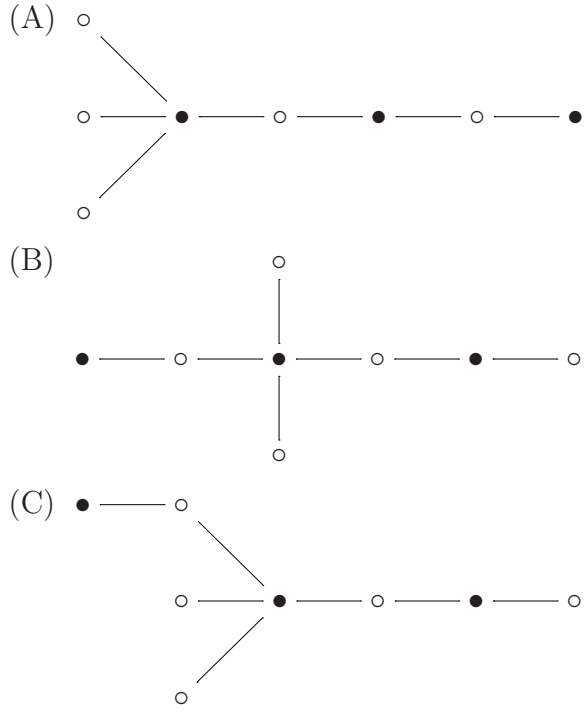
Satz 3.1. *Sei $\sigma \in \Gamma$ und $D \subset X$ eine Kinderzeichnung.*

(1) *D und D^σ haben dieselben Valenz-Listen*[22] *(für $\bullet$, $\circ$, $*$), sogar konjugierte kartographische Gruppen*[23].
(2) *Die Γ-Bahn von D ist endlich*[24].

Beweis. Zu (1): Die Valenzen sind gerade die Multiplizitäten der kritischen Punkte der zugehörigen Belyi-Abbildung β; diese lassen sich mit Hilfe des Verschwindens/Nicht-Verschwindens höherer Ableitungen von β ausdrücken.

Zu (2): Es gibt nur endlich viele 3-Konstellationen, und damit Kinderzeichnungen zu einer vorgegebenen Valenz-Liste. □

3.1. **Beispiel.** Alle Dessins mit Passeintrag $[421, 2^2 1^3, 7]$:

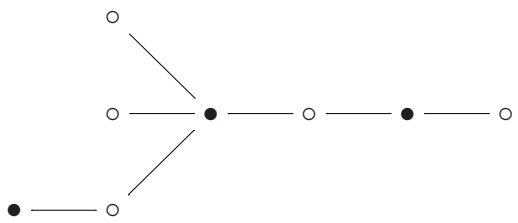


[22]Dies wird auch der Passeintrag eines Dessins genannt.

[23]Matzat 1987, Jones/Streit 1997.

[24]Es folgt relativ leicht, dass der Modulkörper $M(D)$ von D ein Zahlenkörper ist, also $[M(D) : \mathbb{Q}] < \infty$ gilt. Der Modulkörper ist definiert als Fixkörper der Standuntergruppe von D in $\mathrm{Aut}(\mathbb{C})$, die nach der Aussage (2) von endlichem Index ist. Nimmt man den in der Standuntergruppe enthaltenen maximalen Normalteiler (der auch von endlichem Index ist), so erhält man den Modulkörper der Bahn von D.

(D)



Aber 2 Bahnen: Kartographische Gruppen: A_7 für (A) und (B), $\mathrm{PSL}_3(2)$ für (C) und (D). (Modulkörper sind $\mathbb{Q}(\sqrt{21})$ bzw. $\mathbb{Q}(\sqrt{-7})$.)

4. Der Satz von Lenstra-Schneps

Wir konzentrieren uns auf den ebenen Fall: $X = \mathbb{P}^1$ (d. h. $g = 0$). Ein (abstraktes) Dessin $X_0 \subset X_1 \subset X_2$ ist ein (ebener) *Baum*, falls das Geschlecht $g = 0$ ist und $X_2 \setminus X_1$ aus genau einer Zelle besteht.

Sei $D \subset X$ ein Dessin, β eine zugehörige Belyi-Abbildung. D ist ein Baum[25] genau dann, wenn β genau einen Pol (o. E. durch Anwendung eines Elements in $\mathrm{PSL}_2(\mathbb{C})$ im Unendlichen) hat, genau dann, wenn man für β ein Polynom wählen kann.

Satz 4.1 (H. W. Lenstra, L. Schneps 1994)**.** *Die absolute Galoisgruppe* Γ *operiert treu auf der Menge der ebenen Bäume.*

5. Beweise

5.1. **Beweis des Satzes von Belyi (1) $\Longrightarrow$ (2).** Sei X definiert über $\overline{\mathbb{Q}}$.

Sei $\beta : X \longrightarrow \mathbb{P}^1$ irgendeine über $\overline{\mathbb{Q}}$ definierte nicht-konstante meromorphe Funktion. Es wird gezeigt: Es gibt ein Polynom $f \in \mathbb{Q}[T]$, so dass $f \circ \beta$ eine Belyi-Abbildung ist.

1. Schritt:

Sei $\mathcal{S}_0$ die Menge aller *irrationalen* kritischen Werte[26] und ihrer Konjugierten. Diese kritischen Werte sind algebraisch[27], und daher ist

[25]Man kann zeigen, dass es für einen Baum D immer ein zugehöriges Belyi-Paar gibt, das über dem Modulkörper $M(D)$ definiert ist. Allgemeiner gilt dies für Dessins, die einen sogenannten Bachelor haben, d. h. einen Punkt $\bullet$, $\circ$ oder $*$, der der einzige Punkt ist zu vorgegebener Farbe und Valenz (Shabat 1990, Couveignes 1994 (für $g = 0$), Wolfart 1997). Für ein allgemeines Dessin gibt es endliche Körpererweiterungen von $M(D)$ als Definitionskörper.

[26]Wovon es aus Kompaktheitsgründen nur endlich viele gibt.

[27]Da sie Nullstellen von rationalen Funktionen, damit auch von Polynomen mit algebraischen Koeffizienten sind.

$\mathrm{Card}(\mathcal{S}_0) = N$ endlich[28]. Sei

$$P_0 = \prod_{s \in \mathcal{S}_0} (T - s) \in \overline{\mathbb{Q}}[T].$$

Dies ist ein Polynom in $\mathbb{Q}[T]$ (!)[29] vom Grad N.

P_0 hat nun höchstens $N - 1$ kritische Werte, nämlich die Werte an den Nullstellen seiner Ableitung. Dann sind die einzigen irrationalen kritischen Wert von $P_0 \circ \beta$ diejenigen von P_0, wie durch Betrachtung der Gleichung

$$0 = (P_0 \circ \beta)'(x) = P_0'(\beta(x)) \cdot \beta'(x)$$

folgt. Sei $\mathcal{S}_1$ die Menge aller dieser irrationalen kritischen Werte. Diese Menge ist nun abgeschlossen unter Konjugierte.

Bilde nun sukzessive $P_1, \ldots, P_{N-1} \in \mathbb{Q}[T]$. Dann hat

$$P_{N-1} \circ \ldots \circ P_1 \circ P_0 \circ \beta$$

nur rationale kritische Werte.

2. Schritt:

β habe *nur rationale* kritische Werte. Nach einer geeigneten affinen Transformation sind alle diese kritischen Werte in $[0, 1]$. Bilde

$$p_{m,n}(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n.$$

Dann gilt

$$0 \mapsto 0, \quad 1 \mapsto 0, \quad \infty \mapsto \infty$$

$$[0, 1] \to [0, 1], \quad \mathbb{Q} \to \mathbb{Q}$$

Kritischer Wert $m/(m+n) \mapsto 1$.

Es folgt: $p_{m,n} \circ \beta$ hat *einen* kritischen Wert *weniger*.

5.2. **Beweis des Satzes von Lenstra-Schneps.** Sei $X = \mathbb{P}^1$ und die Kinderzeichnung $D \subset X$ ein Baum.

Eine zugehörige Belyi-Abbildungen ist gerade ein sogenanntes Shabat Polynom[30]: diese haben nur zwei kritische Werte y_1, y_2 $(\neq \infty)$ (= Belyi-Abbildung).

[28] Algebraische Zahlen haben nur endlich viele Konjugierte, nämlich die übrigen Nullstellen ihres Minimalpolynoms

[29] Dies ist das Produkt der Minimalpolynome über $\mathbb{Q}$.

[30] Oder verallgemeinertes Tschebyscheff-Polynom.

Bei allgemeinen kritischen Werten ist der Isomorphiebegriff wie folgt:
Seien P und Q Shabat Polynome mit kritischen Werten y_1, y_2 bzw. z_1, z_2. Dann sind P und Q isomorph genau dann, wenn A, B, a, $b \in \mathbb{C}$ existieren mit $Q(x) = AP(ax+b) + B$ und $z_i = Ay_i + B$.

Man hat dann eine Bijektion zwischen den Mengen der Isomorphieklassen der ebenen Bäume und der Isomorphieklassen der Shabat Polynome.

Sei $\sigma \in \Gamma$, $\sigma \neq 1$. Sei α algebraisch mit $\beta = \sigma(\alpha) \neq \alpha$. Sei $D = \mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta)$.

Wähle ein Polynom $p_\alpha \in K[T]$ mit

$$p'_\alpha(x) = x^3(x-1)^2(x-\alpha).$$

Da p nur algebraische Koeffizienten hat, gibt es nach dem Beweis des Satzes von Belyi ein Shabat Polynom $P_\alpha(x) = f(p_\alpha(x))$ für ein $f \in \mathbb{Q}[T]$.

Sei T_α der zugehörige ebene Baum. Genauso (mit demselben f) definiert man einen Baum T_β. Offenbar wird T_α durch σ gerade auf T_β geschickt.

Zu zeigen ist $T_\alpha \neq T_\beta$.

Nehme an $T_\alpha = T_\beta$. Dann

$$f(p_\beta(x)) = P_\beta(x) = P_\alpha(ax+b) = f(p_\alpha(ax+b)).$$

Aus elementaren algebraischen Überlegungen folgt dann

$$p_\alpha(ax+b) = cp_\beta(x) + d.$$

Die rechte Seite hat drei kritische Punkte 0, 1 und β der Ordnungen 4, 3 bzw. 2. Also hat auch die linke Seite drei kritische Punkte x_0, x_1 und x_α der Ordnungen 4, 3 bzw. 2 mit

$$ax_0 + b = 0,\ ax_1 + b = 1,\ ax_\alpha + b = \alpha.$$

Es folgt

$$x_0 = 0,\ x_1 = 1,\ x_\alpha = \beta.$$

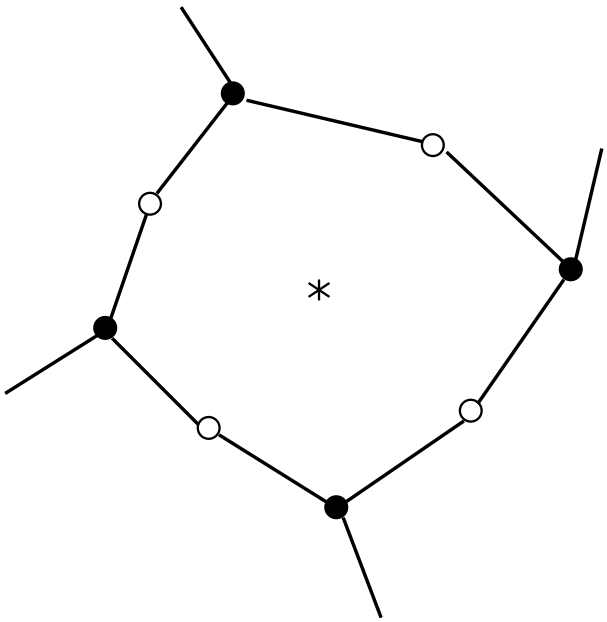
Damit

$$a = 1,\ b = 0,\ \text{und schließlich } \beta = \alpha,$$

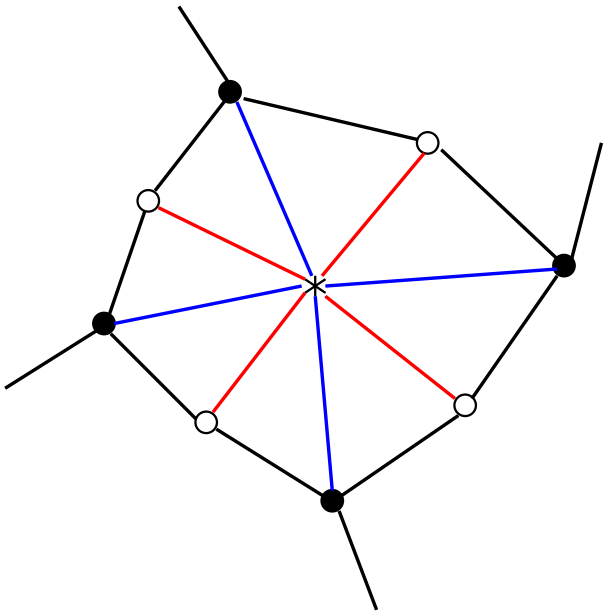
Widerspruch.

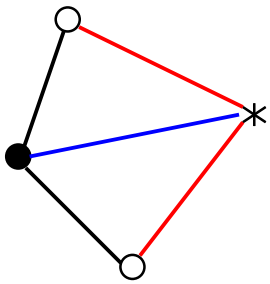
6. Anhang

6.1. **Kinderzeichnung bestimmt Belyi-Abbildung.**



Triangulierung:





Verklebe in jedem die beiden Punkte $\circ$ und die beiden schwarzen und die beiden roten Seiten $\Longrightarrow$ homöomorph zu $\mathbb{P}^1$

6.2. 3-Konstellation bestimmt Kinderzeichnung (inkl. Fläche!)

(1) Bilde die Zykelzerlegung von σ_∞.
(2) Bilde zu jedem Zykel ein Polygon, wobei die Seiten, die Elemente des Zykels sind, mit positiver Orientierung.
(3) Verkleben der Kanten der Polygone gemäß Involution σ_1, mit gegenseitiger Orientierung, liefert eine orientierte 2-Mannigfaltigkeit mit Kinderzeichnung.

(Beispiel)

6.3. **Beweis des Satzes von Belyi, (2)$\Longrightarrow$(1).** Sei $B = (X, \beta)$ ein Belyi-Paar, d. h. nur über den Punkten 0, 1, ∞ verzweigt.

Sei $G = \mathrm{Aut}(\mathbb{C})$. Auch diese Gruppe operiert auf der Menge der (Isomorphieklassen der) Belyi-Paare, analog zu Γ. Sei $U = G_B$ die Standuntergruppe von B. Diese ist von endlichem Index in G, denn die G-Bahn von B ist endlich, da der Passeintrag auch invariant unter dieser Gruppenaktion ist; aus dem Bahnenlemma folgt dann die Endlichkeit des Index.

Sei $M(B)$ der Fixkörper von U, der *Modulkörper* von B. Es folgt, dass $M(B)$ ein Zahlenkörper ist, dass heißt $[M(B) : \mathbb{Q}] < \infty$.

Für jedes $\sigma \in U$ gilt $B^\sigma \simeq B$, insbesondere $X^\sigma \simeq X$.

Die Fälle $g = 0$ (d. h. $X \simeq \mathbb{P}^1$) und $g = 1$ sind einfach. Im Fall $g = 1$ ist X charakterisiert durch die absolute Invariante $j = j(X) \in \mathbb{C}$. Wegen $j(X^\sigma) = \sigma(j)$ gilt $j \in M(X) \subset \overline{\mathbb{Q}}$. Da X über $\mathbb{Q}(j)$ definiert ist, ist X insbesondere über $\overline{\mathbb{Q}}$ definiert. –

Für allgemeines g behandeln wir nun nur einen einfachen Spezialfall, der die Beweisidee illustriert:

Nehme an, (X, β) ist über $\mathbb{Q}(\xi)$ definiert, wobei ξ transzendent ist. Es gibt ein $\sigma \in U$, so dass ξ und $\eta = \sigma(\xi)$ algebraisch unabhängig sind. Sei

$$X \xrightarrow{f_{(\xi,\eta)}} X^\sigma$$

ein Isomorphismus (d. h. eine biholomorphe Abbildung), der – zusammen mit seinem Inversen – über $\mathbb{Q}(\xi, \eta)$ definiert ist.

Fixiere ξ, und für η setze alle $z \in \mathbb{C}$ ein. Für fast alle z ist dann das Bild von X unter $f_{(\xi,z)}$ eine glatte, projektive Kurve. Ebenso ist für fast alle z die Abbildung $f_{(\xi,z)}$ ein Isomorphismus auf das Bild. Insbesondere gibt es ein $z \in \overline{\mathbb{Q}}$, so dass $f_{(\xi,z)}(X)$ eine über $\overline{\mathbb{Q}}$ definierte Riemannsche Fläche ist.

Literatur

1. G. V. Belyĭ: *A new proof of the three-point theorem*. (Russian) Mat. Sb. 193 (2002), no. 3, 21–24; translation in Sb. Math. 193 (2002), no. 3-4, 329–332. (Preprint Bonn 1997 Online verfügbar.)
2. M. D. Fried: *Topics in Galois Theory*, in: Recent Developments in the Inverse Galois Problem, Contemporary Mathematics 186, American Mathematical Society, Providence, R. I., 1995. pp. 15-32.
3. B. Köck: *Belyi's theorem revisited*. Beiträge Algebra Geom. 45 (2004), no. 1, 253–265.
4. S. K. Lando, A. K. Zvonkin: *Graphs on Surfaces and their Applications*. (In der Reihe: Encyclopaedia of Mathematical Sciences: Low-Dimensional Topology II) Springer-Verlag Berlin Heidelberg 2004.
5. H. Lenstra: *Profinite Groups*. Online-Version.
6. L. Schneps (ed.): *The Grothendieck Theory of Dessins d'Enfants*. London Mathematical Society Lecture Notes Series 200, Cambridge University Press, Cambridge 1994.
7. L. Schneps and P. Lochak (eds.): *Geometric Galois Actions. 1. Around Grothendieck's Esquisse d'un Programme*. London Mathematical Society Lecture Notes Series 242, Cambridge University Press, Cambridge 1997.
8. L. Schneps and P. Lochak (eds.): *Geometric Galois Actions. 2. The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups*. London Mathematical Society Lecture Notes Series 243, Cambridge University Press, Cambridge 1997.
9. J.-P. Serre: *Topics in Galois Theory*. Jones and Bartlett Publishers, Boston 1992.
10. J. Wolfart: *Kinderzeichnungen und Uniformisierungstheorie*. Online-Version, März 2001.