Masterarbeit

Die Pellsche Gleichung im Polynomring

Olaf Merkert

6. August 2012

Betreut durch Prof. Dr. David Masser

Inhaltsverzeichnis

1 Einführung

Eine der einfachsten nicht-linearen diophantischen Gleichungen ist bekanntlich die *Pellsche Gleichung*

$$p^2 - D\,q^2 = 1 \tag{P}$$

über einem Integritätsbereich R, wobei man die $D \in R$ zu klassifizieren sucht, für die es außer den trivialen Lösungen mit $p = \pm 1$ und $q = 0$ noch weitere, sogenannte *nicht-triviale Lösungen* $(p, q) \in R^2$ mit $q \neq 0$ gibt.

Eine äußerst nützliche Eigenschaft der Pellschen Gleichung ist, dass die Lösungsmenge $\{(p, q) \in R^2 \mid p^2 - D\,q^2 = 1\}$ durch die Verknüpfung

$$(p, q) * (p', q') = (p\,p' + D\,q\,q', p\,q' + p'\,q)$$

eine Gruppenstruktur trägt. Dies wird umso deutlicher, wenn man zur *verallgemeinerten Pellschen Gleichung*

$$p^2 - D\,q^2 \in R^\star\,. \tag{P*}$$

übergeht. Dann ist die Gruppe $\{(p, q) \in R^2 \mid p^2 - D\,q^2 \in R^\star\}$ durch $(p, q) \mapsto p + \sqrt{D}\,q$ nämlich isomorph zur Gruppe der Einheiten $R[\sqrt{D}]^\star$. Die trivialen Lösungen mit $q = 0$ liefern dabei die Untergruppe $R^\star$.

Die Frage nach nicht-trivialen Lösungen mit $q \neq 0$ ist also äquivalent zur Frage, ob die Adjunktion von $\sqrt{D}$ zu R zusätzliche Einheiten liefert. Dabei macht es keinen Unterschied, ob man nach der Existenz von nicht-trivialen Lösungen von (P) oder (P*) fragt:

Erfüllt $(p, q) \in R^2$ nämlich $p^2 - D\,q^2 = \eta \in R^\star$, so ist

$$(p, q) * (p, q)/\eta = \big((p^2 + D\,q^2)/\eta, 2\,p\,q/\eta\big) = (\tilde{p}, \tilde{q})$$

eine Lösung von (P) mit $\tilde{q} \neq 0$ wenn bereits $q \neq 0$ war. Hier klammern wir den Fall $p = 0$ aus, denn dieser ist nur möglich, wenn D und q beide in $R^\star$ sind (vgl. auch Proposition 2.24).

Für den Euklidischen Ring $\mathbb{Z}$ ist die Existenz nicht-trivialer Lösungen bereits vollständig verstanden. Dabei benützt man, dass $\mathbb{Z}$ mit einer totalen Ordnung ausgestattet ist, die sich ja auch nach $\mathbb{Q}$ und $\mathbb{R}$ fortsetzt.

Diese Masterarbeit beschäftigt sich nun mit der Pellschen Gleichung über dem Polynomring $k[X]$ über einem Körper k, der durch eine ultrametrische Bewertung unter den Euklidischen Ringen hervorsticht. Allerdings ist hier die Frage nach nicht-trivialen Lösungen wesentlich schwieriger und für höhere Grade gibt es noch keine Klassifikation der $D \in k[X]$ mit nicht-trivialen Lösungen. Es gibt immerhin zwei sehr einfache notwendige Kriteria:

Proposition 1.1. *Sei $D \in k[X]$ mit $\deg D \geq 1$. Gibt es eine nicht-triviale Lösung $(p, q) \in k[X]^2$ von $(\mathrm{P}^\star)$ mit $q \neq 0$, so muss $\deg D$ gerade und der Leitkoeffizient von D ein Quadrat in k sein.*

Beweis. Seien $a_0, b_0, c_0 \in k$ die Leitkoeffizienten von D, p und q. Wenn $q \neq 0$, so folgt $\deg(D\,q^2) \geq 1$. Nun liegt aber $p^2 - D\,q^2 \in k^\star = k[X]^\star$, so dass der höchste Koeffizient von p^2 den höchsten Koeffizient von $D\,q^2$ aufheben muss. Es gilt dann $2 \deg p = \deg D + 2 \deg q$, so dass $\deg D$ gerade sein muss, und außerdem ${b_0}^2 = a_0\,{c_0}^2$, so dass $a_0 = (c_0/b_0)^2$ ein Quadrat in k sein muss. □

Diese Arbeit beschreibt in Ergänzung zu diesem einfachen Ausschlusskriterium drei unterschiedliche hinreichende (und notwendige) Bedingungen für die Existenz von nicht-trivialen Lösungen der Pellschen Gleichung.

Zuerst entwickeln wir in abstraktem Rahmen eine Theorie von Kettenbruchentwicklungen für $\sqrt{D}$ aufgefasst als Laurentreihe in X^{-1}. Das Programm läuft nahezu parallel zur gleichen Fragestellung in $\mathbb{Z}$, wobei wir allerdings anstatt der Anordnung auf $\mathbb{Z}$ eine ultrametrische Bewertung auf $k[X]$ verwenden. Das Hauptresultat (siehe Seite 6) ist, dass $\sqrt{D}$ genau dann eine periodische Kettenbruchentwicklung hat, wenn $(\mathrm{P}^\star)$ nicht-triviale Lösungen hat. Ein nützliches Zwischenresultat ist dabei, dass wir *alle* nicht-trivialen Lösungen aus der Kettenbruchentwicklung von $\sqrt{D}$ berechnen können. Da die Klassifikation der Quadratwurzeln mit periodischen Kettenbruchentwicklungen jedoch auch nicht sehr gut verstanden ist, gibt diese Verbindung leider keine Antwort auf die Hauptfrage.

Ist der Grad von D genau 4 und ist D quadratfrei, so gibt es eine weitere schöne Verbindung: Die Invarianten von D liefern nämlich eine elliptische Kurve, und die Semiinvarianten noch einen Punkt $Q_\pm$ darauf, der überdies genau dann von endlicher Ordnung ist, wenn eine nicht-triviale Lösung der Pellschen Gleichung existiert (siehe Seite 27). Dieses Ergebnis, mit dem Verständnis der Torsionspunkte von elliptischen Kurven über $\mathbb{Q}$, erlaubt dann für $k = \mathbb{Q}$ eine Klassifikation der D mit nicht-trivialen Lösungen der Pellschen Gleichung; außerdem, da sich aus den Invarianten und Semiinvarianten ein D zurückkonstruieren lässt, kann man so überhaupt Beispiele von D's mit nicht-trivialen Lösungen finden, was für allgemeinen Grad sonst äußerst schwierig ist.

Diese Verbindung zwischen Grad 4 und Grad 3 lässt sich ebenfalls nutzen, um zu studieren, wann elliptische Integrale der Form $\int f(X)/\sqrt{D(X)}\,\mathrm{d}X$ mit $\deg D = 4$ elementare Stammfunktionen besitzen. Ist f dabei ein Polynom von genügend kleinem Grad, so kann man durch Spiel mit den Ordnungen auf der zu D gehörigen elliptischen Kurve zeigen, dass $Q_\pm$ von endlicher Ordnung ist und somit eine nicht-triviale Lösung der Pellschen Gleichung existiert.

Umgekehrt kann man sogar für beliebigen Grad aus einer nicht-trivialen Lösung (p, q) der Pellschen Gleichung ein Polynom $f = \frac{\mathrm{d}p}{\mathrm{d}X}\,/q$ (wobei $\deg f = (\deg D - 2)/2$ klein ist) berechnen, für welches das elliptische Integral eine elementare Stammfunktion hat.

Wir werden vielerorts mit quadratischen Körpererweiterungen arbeiten. Die folgende Proposition sichert uns zu, dass diese Erweiterungen sich gemäß unseren Erwartungen verhalten.

Proposition 1.2. *Sei $D \in k[X]$ kein Quadrat in $k[X]$, aber sei der Leitkoeffizient von D ein Quadrat in k. Dann ist $k(X,Y)$ mit $Y^2 = D(X)$ eine Erweiterung von Grad 2 des Körpers $k(X)$ mit $k(X,Y) \cap \overline{k} = k$.*

Beweis. Da $k[X]$ faktoriell ist, ist D auch in $k(X)$ kein Quadrat, und mit den üblichen Argumenten ist dann klar, dass der Grad der Körpererweiterung genau 2 ist.

Betrachten wir weiter $k(X)$ als Teilkörper von $k((X^{-1/2}))$, dem Körper der Laurentreihen in $X^{-1/2}$, so finden wir $\sqrt{D} \in k((X^{-1/2}))$, da der Leitkoeffizient von D ein Quadrat ist und wir können $k(X,Y)$ als Teilkörper $k((X^{-1/2}))$ ansehen. Mit $k((X^{-1/2})) \cap \overline{k} = k$ folgt die Behauptung. □

Danksagung

Mein Dank gilt vor allem meinem Betreuer Prof. Dr. David Masser, für die erhellenden Besprechungen und die sorgfältige Durchsicht meiner Ergebnisse, sowie die guten Ratschläge für den Niederschrieb derselben. Außerdem danke ich allen weiteren Personen, die die unfertige Arbeit Korrektur gelesen haben.

2 Kettenbrüche

Unser Anliegen ist, den folgenden Zusammenhang zwischen der Pellschen Gleichung und periodischen Kettenbruchentwicklungen (siehe Abschnitt 2.5) zu beweisen:

Hauptsatz 1. *Es sei k ein Körper, $D \in k[X]$ ein Polynom mit positivem geraden Grad und dem Leitkoeffizienten ein Quadrat in k, so dass $\sqrt{D} \in k((X^{-1}))$ liegt.*

Dann gibt es genau dann eine nicht-triviale Lösung der Pellschen Gleichung ($\mathrm{P}^\star$) *in $R = k[X]$, wenn die Kettenbruchentwicklung von $\sqrt{D}$ periodisch ist.*

Um besser zu verdeutlichen, welche Eigenschaften von $k[X]$ diesem Satz zu Grunde liegen, und um die Analogien und Unterschiede zur Situation in $R = \mathbb{Z}$ besser zu verdeutlichen, formulieren wir den Satz zunächst in abstrakterer Form.

Hauptsatz 2. *Es sei R ein Euklidischer Ring[1] bezüglich einer ultrametrischen Bewertung $|\cdot|$, K sein Quotientenkörper und $\mathbb{K}$ dessen Vervollständigung bezüglich der Bewertung.*

Sei weiter $D \in R$ mit $|D| > 1$ und $\sqrt{D} \in \mathbb{K} \setminus K$.

Dann ist die Existenz einer nicht-trivialen Lösung der Pellschen Gleichung ($\mathrm{P}^\star$) *in R äquivalent mit der Periodizität der Kettenbruchentwicklung von $\sqrt{D}$.*

Wir werden später sehen, dass die beiden Hauptsätze äquivalent sind.

2.1 Bewertungen

Definition 2.1. Sei R ein Integritätsbereich. Eine Abbildung $|\cdot| : R \to [0, +\infty) \subset \mathbb{R}$ heißt *Bewertung*, wenn für alle $x, y \in R$ gilt:

$$|x| = 0 \iff x = 0, \qquad |x \cdot y| = |x| \cdot |y|\,, \qquad |x + y| \leq |x| + |y|\,.$$

Bemerkung 2.1. Da $\mathbb{R}$ ein Integritätsbereich ist, sorgen die beiden ersten Bedingungen dafür, dass eine Bewertung wirklich nur auf einem Integritätsbereich definiert werden kann.

Bemerkung 2.2. Wegen $|1| = |1 \cdot 1| = |1| \cdot |1|$ und $|1| \neq 0$ gilt immer $|1| = 1$. Weiter gilt wegen $|1| = |-1| \cdot |-1|$ auch $|-1| = 1$, nach dem zweiten Punkt dann allgemeiner $|x| = |-x|$ für alle $x \in R$.

Definition 2.2. Eine Bewertung $|\cdot|$ auf einem Integritätsbereich R heißt *ultrametrisch*, wenn gilt

$$|x + y| \leq \max(|x|, |y|) \text{ für alle } x, y \in R.$$

[1] Man verwende hier Definition 2.3, welche sich von der üblichen leicht unterscheidet.

Tatsächlich verschärft sich diese Ungleichung automatisch zur Gleichung, wenn die Summanden verschieden bewertet sind:

Proposition 2.1. *Sei $|\cdot|$ ultrametrisch. Falls $|x| \neq |y|$, folgt $|x+y| = \max(|x|, |y|)$.*

Beweis. Nehmen wir z.B. $|y| < |x|$ an. Dann gilt

$$|y| < |x| = |x+y-y| \leq \max(|x+y|, |y|) = |x+y|,$$
$$|x+y| \leq \max(|x|, |y|) = |x|.$$

Es folgt sofort $|x+y| = |x| = \max(|x|, |y|)$. □

Jedem Integritätsbereich R lässt sich sein *Quotientenkörper* K zuordnen. Oft werden wir aber den Wert des Nenners betrachten, so dass wir lieber mit den Verhältnissen $\mathcal{R} = R \times (R \setminus \{0\})$ arbeiten.

Proposition 2.2. *Sei R ein bewerteter Integritätsbereich. Dann definiert*

$$\left|\frac{a}{b}\right| := \frac{|a|}{|b|} \text{ für alle } (a,b) \in \mathcal{R}$$

eine Bewertung auf dem Quotientenkörper K. Diese Bewertung ist auch ultrametrisch, falls R ultrametrisch bewertet ist.

Beweis. Die ersten beiden Eigenschaften einer Bewertung bleiben offensichtlich erfüllt. Für die Dreiecksungleichung überprüft man

$$\left|\frac{a}{b} + \frac{c}{d}\right| = \left|\frac{a\,d + b\,c}{b\,d}\right| = \frac{|a\,d + b\,c|}{|b\,d|} \leq \frac{|a\,d|}{|b\,d|} + \frac{|b\,c|}{|b\,d|} = \left|\frac{a}{b}\right| + \left|\frac{c}{d}\right|.$$

Analog beweist man das Bestehen der ultrametrischen Ungleichung. □

Bezüglich dieser Bewertung kann man K nun zu $\mathbb{K}$ *vervollständigen*, wobei sich die Bewertung stetig fortsetzt, und falls gegeben, ebenfalls die ultrametrische Ungleichung erhält.

2.2 Euklidische Ringe

Definition 2.3. Ein Integritätsbereich R mit einer Bewertung $|\cdot|$ heißt *Euklidischer Ring*,[2] falls es eine Abbildung $\varrho : \mathcal{R} \to R$ (den *Divisionsrest*) gibt, mit

(i) $a - \varrho(a,b) \in b\,R$ und

(ii) $|\varrho(a,b)| < |b|$ für alle $(a,b) \in \mathcal{R}$.

und außerdem für jede nicht leere Teilmenge $M \subset R$ das Bild $\{|x| \mid x \in M\}$ ein Minimum hat.

[2] Wir wählen diese (etwas stärkere) Definition eines Euklidischen Rings, um die Verbindung zu den Kettenbruchentwicklungen bequemer zu machen. Die Euklidischen Ringe mit Kettenbruchentwicklung, $\mathbb{Z}$, $\mathbb{Z}[i]$ und $k[X]$ genügen alle dieser Definition.

Die Abbildung ϱ definiert also eine Division mit Rest in R: Für jedes $(a,b) \in \mathcal{R}$ findet man $q, r \in R$ mit $a = q\,b + r$, wobei $r = \varrho(a,b)$ mit $|r| < |b|$.

Lemma 2.1. *Ein euklidischer Ring ist ein Hauptidealring.*

Beweis. Sei $0 \neq I \subset R$ ein Ideal. Sei $0 \neq x \in I$ mit $|x|$ minimal. Dann für $y \in I$ beliebig ist auch $\varrho(y,x) \in I$. Aber $|\varrho(y,x)| < |x|$ und $|x|$ war minimal in $I \setminus \{0\}$. So es muss $\varrho(y,x) = 0$ sein und es folgt $y \in x\,R$. Also ist $I = x\,R$ ein Hauptideal. □

Proposition 2.3. *Sei R ein euklidischer Ring. Falls $b \in R \setminus \{0\}$ ist $|b| \geq 1$; und weiter ist $b \in R^\star$ äquivalent mit $|b| = 1$.*

Beweis. Wäre $|b| < 1$ für $b \in R \setminus \{0\}$, so hätte die Menge $\{|1|, |b|, \left|b^2\right|, \left|b^3\right|, \dots\}$ kein minimales Element, also gilt $|b| \geq 1$.

Für $b \in R^\star$ mit $|b| > 1$ wäre $\left|b^{-1}\right| < 1$, also muss $|b| = 1$ gelten.

Ausgehend von $|b| = 1$ ist für $a \in R$ beliebig $|\varrho(a,b)| < |b| = 1$. Da $\varrho(a,b) \in R$, kommt nur $\varrho(a,b) = 0$ in Frage. Damit ist jedes $a = a - \varrho(a,b) \in b\,R$. Es folgt $R = b\,R$ und somit $b \in R^\star$. □

Proposition 2.4. *Sei R ein Euklidischer Ring. Der* Euklidische Algorithmus *ordnet zwei Zahlen $b_0, b_1 \in R$ eine Zahlenfolge $(b_n)_{n\in\mathbb{N}}$ zu, induktiv definiert durch*

$$b_{n+2} = \begin{cases} \varrho(b_n, b_{n+1}) & \text{falls } b_{n+1} \neq 0, \\ 0 & \text{falls } b_{n+1} = 0. \end{cases}$$

Dieser Algorithmus terminiert stets, d.h. es gibt immer $N \geq 0$ mit $b_N = 0$.

Beweis. Angenommen, der Algorithmus würde für $b_0, b_1 \in R$ nicht terminieren. Das hieße, in der Folge $(b_n)_{n\in\mathbb{N}}$ gälte dann $b_n \neq 0$ und $|b_{n+1}| < |b_n|$ für alle $n \geq 1$. Dann hätte aber das Bild der Menge $\{b_n \mid n \geq 1\} \subset R$ unter $|\cdot|$ kein Minimum, im Widerspruch zur Definition 2.3 eines Euklidischen Rings. □

Proposition 2.5. *Ist R ein ultrametrisch bewerteter Euklidischer Ring, so ist der Divisionsrest ϱ eindeutig bestimmt und erfüllt*

$$\varrho(c\,a, c\,b) = c\,\varrho(a,b) \text{ für alle } a \in R,\ b, c \in R \setminus \{0\}. \tag{2.1}$$

Beweis. Seien $a, b \in R$, $b \neq 0$ beliebig und $r, r' \in R$ mit

$$a - r \in b\,R, \quad |r| < |b| \qquad \text{und} \qquad a - r' \in b\,R, \quad \left|r'\right| < |b|\,.$$

Es folgt $r - r' = (a - r') - (a - r) \in b\,R$ sowie $|r - r'| \leq \max(|r|, |r'|) < |b|$. Damit ist $(r - r')/b \in R$ mit $|(r - r')/b| < 1$, aus Proposition 2.3 folgt dann $r - r' = 0$; also ist der Divisionsrest eindeutig bestimmt.

Weiter ist $|c\,\varrho(a,b)| < |c\,b|$ wegen $|\varrho(a,b)| < |b|$ und $c\,a - c\,\varrho(a,b) = c\,(a - \varrho(a,b)) \in c\,b\,R$ wegen $a - \varrho(a,b) \in b\,R$. Mit der Eindeutigkeit folgt also $\varrho(c\,a, c\,b) = c\,\varrho(a,b)$. □

2.3 Abschneideabbildungen

Unser nächstes Ziel ist es, eine (möglichst eindeutige) Kettenbruchentwicklung für Elemente von $\mathbb{K}$ zu definieren. Die folgende Definition legt den Rahmen dafür fest.

Definition 2.4. Sei R ein bewerteter Integritätsbereich und $\mathbb{K}$ die Vervollständigung seines Quotientenkörpers K. Eine *Abschneideabbildung* $\tau : \mathbb{K} \longrightarrow \mathbb{K}$ von R hat die Eigenschaften

(i) $x - \tau(x) \in R$ für alle $x \in \mathbb{K}$ und

(ii) $|\tau(x)| < 1$ für alle $x \in \mathbb{K}$.

Die Abschneideabbildung in $\mathbb{K}$ ersetzt sozusagen den Divisionsrest, der ja in einem Körper wenig sinnvoll ist. Man bekommt dann auch ein Analog von Proposition 2.5:

Proposition 2.6. *Hat ein ultrametrisch bewerteter Ring R eine Abschneideabbildung τ, so ist diese eindeutig bestimmt und erfüllt zudem*

$$\tau(a + x) = \tau(x) \text{ und } \tau(\eta\, x) = \eta\, \tau(x) \text{ für alle } a \in R, \eta \in R^\star,\ x \in \mathbb{K}. \tag{2.2}$$

Beweis. Sei $x \in \mathbb{K}$ beliebig. Seien $t, t' \in \mathbb{K}$ mit

$$x - t \in R, \quad |t| < 1 \qquad \text{und} \qquad x - t' \in R, \quad \left|t'\right| < 1.$$

Es folgt $t - t' = (x - t') - (x - t) \in R$ sowie $|t - t'| \leq \max(|t|, |t'|) < 1$. Wegen Proposition 2.3 folgt $t - t' = 0$; also ist die Abschneideabbildung eindeutig bestimmt.

Weiter haben wir $|\tau(x)| < 1$ und $a + x - \tau(x) = a + (x - \tau(x)) \in R$, so mit der Eindeutigkeit folgt $\tau(a + x) = \tau(x)$.

Ähnlich gilt wegen $|\eta| = 1$ für $\eta \in R^\star$ ja $|\eta\, \tau(x)| = |\tau(x)| < 1$ und $\eta\, x - \eta\, \tau(x) = \eta\, (x - \tau(x)) \in R$, also folgt wieder mit der Eindeutigkeit $\tau(\eta\, x) = \eta\, \tau(x)$. □

Proposition 2.7. *Jeder ultrametrisch bewertete Euklidische Ring R hat eine Abschneideabbildung τ, mit*

$$\tau\left(\frac{a}{b}\right) = \frac{\varrho(a, b)}{b} \text{ für alle } (a, b) \in \mathcal{R}. \tag{2.3}$$

Beweis. Zunächst definieren wir τ für die Elemente $\frac{a}{b} \in K$ mittels (2.3). Nach Proposition 2.5 ist dies wohldefiniert. Von $a - \varrho(a, b) \in b\, R$ folgt dann $\frac{a}{b} - \tau\left(\frac{a}{b}\right) \in R$; von $|\varrho(a, b)| < |b|$ folgt $\left|\tau\left(\frac{a}{b}\right)\right| < 1$.

Nun für jedes $x \in \mathbb{K}$ finden wir $y \in K$ mit $|x - y| < 1$ und setzen

$$\tau(x) = \tau(y) - y + x.$$

Mit $x - \tau(x) = y - \tau(y) \in R$ und $|\tau(x)| \leq \max(|\tau(y)|, |x - y|) < 1$ sind sofort die gewünschten Eigenschaften erfüllt. Dank Proposition 2.6 spielt dabei die Wahl von y auch keine Rolle. □

Bemerkung 2.3. Man kann umgekehrt auch zeigen–sogar ohne „ultrametrisch“–dass die Existenz einer Abschneideabbildung einen bewerteten Integritätsbereich zu einem Euklidischen Ring macht.

2.4 Näherungsbrüche

Bevor wir zur eigentlichen Kettenbruchentwicklung schreiten, wollen wir einen formaleren Blick auf die (endlichen) Kettenbrüche und ihre kanonischen Näherungsbrüche werfen.[3]

Definition 2.5. Seien $m, n \in \mathbb{Z}$ mit $n \geq 0$. Unter einem *endlichen* (regelmäßigen) *Kettenbruch* verstehen wir den Ausdruck

$$A_{m,n} = [a_m, a_{m+1}, \ldots, a_{m+n}] = a_m + \cfrac{1}{a_{m+1} + \cfrac{1}{\ddots + \cfrac{1}{a_{m+n}}}},$$

wobei die a_k zunächst als freie Variable zu verstehen sind.

Offensichtlich kann man $A_{m,n}$ als rationale Funktion in $a_m, \ldots, a_{m+n}$ schreiben. Eine kanonische Form als Quotient von ganzrationalen Funktionen liefert die folgende Proposition:

Proposition 2.8. *Setzen wir für $n \geq -1$ (für $n = -1$ erhalten wir die Einheitsmatrix)*

$$M_{m,n} = \begin{pmatrix} 1 & a_m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & a_{m+1} \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & a_{m+n} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

dann gilt für $n \geq 0$

$$A_{m,n} = \frac{p_{m,n}}{q_{m,n}} \quad \textit{wobei} \quad M_{m,n} = \begin{pmatrix} p_{m,n} & p_{m,n-1} \\ q_{m,n} & q_{m,n-1} \end{pmatrix}.$$

Beweis. Wir machen Induktion über n. Berechnen wir

$$M_{m,0} = \begin{pmatrix} 1 & a_m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix},$$

so verankern wir unsere Behauptung dank $A_{m,0} = a_m = \frac{a_m}{1}$. Dabei ist $p_{m,-1} = 1$ und $q_{m,-1} = 0$ nicht weiter störend. Außerdem sehen wir so, dass die rechte Spalte von $M_{m,n}$ aus der linken Spalte von $M_{m,n-1}$ hervorgeht.

Nun gilt offensichtlich

$$A_{m,n} = a_m + \frac{1}{A_{m+1,n-1}} = a_m + \frac{1}{\frac{p_{m+1,n-1}}{q_{m+1,n-1}}} = \frac{a_m\, p_{m+1,n-1} + q_{m+1,n-1}}{p_{m+1,n-1}},$$

woraus man aus

$$M_{m,n} = M_{m,0}\, M_{m+1,n-1} = \begin{pmatrix} 1 & a_m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_{m+1,n-1} & ? \\ q_{m+1,n-1} & ? \end{pmatrix} = \begin{pmatrix} p_{m,n} & ? \\ q_{m,n} & ? \end{pmatrix}$$

folgert:

$$\frac{p_{m,n}}{q_{m,n}} = A_{m,n}.$$

□

[3] vgl. auch [3], erstes Kapitel

Definition 2.6. Die somit definierten $p_{m,n}$, $q_{m,n}$ und $p_{m,n}/q_{m,n}$ heißen respektive *Näherungszähler*, *Näherungsnenner* und *Näherungsbrüche* der endlichen Kettenbrüche $A_{m,N} = [a_m, a_{m+1}, \ldots, a_{m+N}]$ mit $N \geq n$ und ebenso des (formell) unendlichen Kettenbruchs $A_{m,\infty} = [a_m, a_{m+1}, a_{m+2}, \ldots]$.

Korollar 2.1. *Für $n \geq 0$ gilt:*

$$p_{m,n} = a_{m+n}\, p_{m,n-1} + p_{m,n-2}, \qquad q_{m,n} = a_{m+n}\, q_{m,n-1} + q_{m,n-2}.$$

Beweis. Folgt direkt aus

$$M_{m,n} = M_{m,n-1} \begin{pmatrix} 1 & a_{m+n} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

□

Korollar 2.2. *Für $n \geq -1$ gilt:*

$$p_{m,n}\, q_{m,n-1} - p_{m,n-1}\, q_{m,n} = \det M_{m,n} = (-1)^{n+1}. \tag{2.4}$$

Folglich sind $p_{m,n}, q_{m,n}$ stets teilerfremd.

Proposition 2.9. *Es gilt für $n, k \geq 0$:*

$$A_{m+n,k} = \frac{q_{m,n-2}\, A_{m,n+k} - p_{m,n-2}}{-q_{m,n-1}\, A_{m,n+k} + p_{m,n-1}}.$$

Beweis. Die Definition von $M_{m,n}$ liefert direkt

$$M_{m,n+k} = M_{m,n-1}\, M_{m+n,k}. \tag{2.5}$$

Man bringt nun $M_{m,n-1}$ auf die linke Seite und betrachtet jeweils die linke Spalte der resultierenden Matrizen:

$$\begin{pmatrix} p_{m+n,k} \\ q_{m+n,k} \end{pmatrix} = {M_{m,n-1}}^{-1} \begin{pmatrix} p_{m,n+k} \\ q_{m,n+k} \end{pmatrix} = \det M_{m,n-1} \begin{pmatrix} q_{m,n-2} & -p_{m,n-2} \\ -q_{m,n-1} & p_{m,n-1} \end{pmatrix} \begin{pmatrix} p_{m,n+k} \\ q_{m,n+k} \end{pmatrix}.$$

Mit $\det M_{m,n-1} = (-1)^n$ gelangt man über

$$A_{m+n,k} = \frac{p_{m+n,k}}{q_{m+n,k}} = \frac{(-1)^n\, (q_{m,n-2}\, p_{m,n+k} - p_{m,n-2}\, q_{m,n+k})}{(-1)^n\, (-q_{m,n-1}\, p_{m,n+k} + p_{m,n-1}\, q_{m,n+k})}$$

durch Einsetzen von $p_{m,n+k} = A_{m,n+k}\, q_{m,n+k}$ sowie Kürzen von $(-1)^n$ und $q_{m,n+k}$ zur Behauptung. □

Korollar 2.3. *Für $n \geq 0$ gilt:*

$$a_{m+n} = \frac{q_{m,n-2}\, A_{m,n} - p_{m,n-2}}{-q_{m,n-1}\, A_{m,n} + p_{m,n-1}}.$$

Beweis. Spezialfall der vorhergehenden Proposition mit $k = 0$; da $A_{m+n,0} = a_{m+n}$. □

Im weiteren Verlauf werden die Doppelindizes nicht mehr benötigt, deshalb notieren wir ab sofort $p_n := p_{0,n}, q_n := q_{0,n}$ und $M_n := M_{0,n}$.

2.5 Kettenbruchentwicklung

Ab sofort nehmen wir an, dass R ein ultrametrisch bewerteter Euklidischer Ring ist. Mittels der Abschneideabbildung $\tau : \mathbb{K} \longrightarrow \mathbb{K}$ werden wir nun eine *Kettenbruchentwicklung* einführen.

Definition 2.7. Sei $\alpha \in \mathbb{K}$ beliebig.
Setze

$$\alpha_0 := \alpha \text{ und solange } \tau(\alpha_i) \neq 0 : \alpha_{i+1} := \frac{1}{\tau(\alpha_i)}.$$

Mit $a_i := \alpha_i - \tau(\alpha_i) \in R$ bekommt man

$$\alpha_i = a_i + \frac{1}{\alpha_{i+1}} = [a_i, \alpha_{i+1}] \text{ bzw. } \alpha_i = a_i = [a_i] \text{ wenn } \tau(\alpha_i) = 0. \tag{2.6}$$

Damit hat man $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$ bzw. $\alpha = [a_0, a_1, a_2, \ldots]$, wobei dieser Kettenbruch genau dann endlich ist, wenn ein $\tau(\alpha_i) = 0$ ist. Ähnlich hat man $\alpha_i = [a_i, a_{i+1}, \ldots, a_{i+n}, \alpha_{i+n+1}] = [a_i, a_{i+1}, a_{i+2}, \ldots]$, solange α_i definiert ist.

Man bemerke, dass für $i \geq 1$ stets $|\alpha_i| > 1$ gilt. Daraus folgert man:

Proposition 2.10. *Solange $|\alpha_i| \geq 1$ (also sicher für $i \geq 1$), gilt $|a_i| = |\alpha_i|$.*

Beweis. Nach Voraussetzung ist $|\tau(\alpha_i)| < 1 \leq |\alpha_i|$. Mit Proposition 2.1 folgt

$$|a_i| = |\alpha_i - \tau(\alpha_i)| = \max\left(|\alpha_i|, |\tau(\alpha_i)|\right) = |\alpha_i|. \qquad \square$$

Neben der Existenz der Abschneideabbildung brauchen wir einen Euklidischen Ring vor allem dafür, dass nur Elemente von K eine endliche Kettenbruchentwicklung haben.

Proposition 2.11. *Die Kettenbruchentwicklung von $\alpha \in \mathbb{K}$ ist genau dann endlich, wenn $\alpha \in K$ ist.*

Beweis. Aus Proposition 2.8 geht klar hervor, dass ein endlicher Kettenbruch ein Element von K darstellt.

Umgekehrt sei $\alpha_0 \in K$ und $(r_0, r_1) \in \mathcal{R}$ mit $\alpha_0 = \frac{r_0}{r_1}$. Solange $\tau(\alpha_n) \neq 0$, erhalten wir mit (2.3) induktiv

$$\alpha_{n+1} = \frac{1}{\tau(\alpha_n)} = \frac{r_{n+1}}{\varrho(r_n, r_{n+1})} = \frac{r_{n+1}}{r_{n+2}}.$$

Man führt also wesentlich den Euklidischen Algorithmus aus. Nach Proposition 2.4 wird schließlich $\varrho(r_n, r_{n+1}) = 0$ und also $\tau(\alpha_n) = 0$. Damit ist die Kettenbruchentwicklung endlich. $\square$

Auch die unendlichen Kettenbrüche stellen das entwickelte Element dar, hier muss man allerdings den Grenzwert der Näherungsbrüche nehmen, dessen Konvergenz die folgenden beiden Propositionen zeigen.

Proposition 2.12. *Die Näherungsnenner*[4] q_i *(siehe Definition 2.5) zu der Kettenbruchentwicklung von* $\alpha = [a_0, a_1, \dots]$ *erfüllen* $|q_i| = \prod_{j=1}^{i} |a_j| \neq 0$.

Beweis. Von Proposition 2.10 weiß man, dass abgesehen von a_0 immer $|a_i| > 1$ gilt (solange a_i definiert ist). Daraus schließt man aus der Produktformel dann $|q_i| \neq 0$ und außerdem $|q_i| < |q_{i+1}|$.

Man beweist die Produktformel per Induktion. Zunächst bemerke man, dass $q_0 = 1$ und $q_1 = a_1$ ist. Damit ist die Induktion für $i = 0, 1$ verankert.

Sonst benutzt man Korollar 2.1, welches $q_{i+1} = a_{i+1}\, q_i + q_{i-1}$ besagt. Nach Induktionsannahme gilt nun $|q_{i-1}| < |q_i| < |a_{i+1}\, q_i|$, und es folgt mit Proposition 2.1

$$|q_{i+1}| = \max\left(|a_{i+1}\, q_i|\,, |q_{i-1}|\right) = |a_{i+1}|\ |q_i| = \prod_{j=1}^{i+1} |a_i|\,.$$

□

Korollar 2.4. *Sei* $|\alpha| \geq 1$. *Dann erfüllen die Näherungszähler* p_i *von* $\alpha = [a_0, a_1, \dots]$ *auch* $|p_i| = \prod_{j=0}^{i} |a_j| \neq 0$.

Beweis. Die p_i genügen wesentlich derselben Rekursionsformel wie die q_i, lediglich die Verankerung mit $p_{-1} = 1$ und $p_0 = a_0$ ist verschieden. Bei $|\alpha| = 1$ hat man nur $|p_{-1}| = |p_0| < |a_1\, p_0|$, aber dies stellt kein Problem dar. □

Proposition 2.13. *Sei* $\alpha = [a_0, a_1, a_2, \dots]$ *in* $\mathbb{K}$ *mit unendlicher Kettenbruchentwicklung. Dann gilt:*

$$\alpha = \lim_{n\to\infty} [a_0, a_1, \dots, a_n].$$

Beweis. Wir haben nach Proposition 2.8 $p_n/q_n = [a_0, a_1, \dots, a_n]$ und außerdem liefert Korollar 2.3 für $\alpha = [a_0, a_1, \dots, a_{k-1}, \alpha_k]$ ein Teleskopprodukt

$$\alpha_k = \frac{q_{k-2}\,\alpha - p_{k-2}}{-q_{k-1}\,\alpha + p_{k-1}} \quad \text{somit} \quad \prod_{k=1}^{n+1} \frac{1}{\alpha_k} = (-1)^n\ (p_n - \alpha\, q_n)$$

für $n \geq 0$—man erinnere $p_{-1} = 1$, $q_{-1} = 0$. Mit $|\alpha_k| = |a_k|$ für $k \geq 1$ haben wir also

$$\left|\frac{p_n}{q_n} - \alpha\right| = \frac{1}{|q_n|\ \prod_{k=1}^{n+1} |a_k|} = \frac{1}{|q_n|\ |q_{n+1}|} < \frac{1}{|q_n|^2}. \tag{2.7}$$

Sei nun $m = \min\{|a_k| \mid k = 1, 2, 3, \dots\}$ (die a_k bilden ja eine nicht-leere Teilmenge von R). Wegen Proposition 2.10 ist dann $m > 1$ und es gilt $|p_n/q_n - \alpha| < m^{-2n}$, was die gewünschte Konvergenz impliziert. □

[4] Bei endlichen Kettenbrüchen beachte man, dass nur endlich viele Näherungsnenner q_i definiert sind.

2.6 Periodische Kettenbrüche

Als nächstes wollen wir die Periodizität von Kettenbruchentwicklungen charakterisieren.

Definition 2.8. Die Kettenbruchentwicklung von α heißt *rein periodisch*, wenn es $l \geq 1$ gibt mit $\alpha = \alpha_l$, also $\alpha = [a_0, a_1, \ldots, a_{l-1}, \alpha]$

Die Kettenbruchentwicklung von α heißt *periodisch*, wenn es $m \in \mathbb{Z}$ gibt, so dass α_m eine rein periodische Kettenbruchentwicklung hat, also $\alpha = [a_0, a_1, \ldots, a_{m-1}, \alpha_m] = [a_0, a_1, \ldots, a_{m-1}, a_m, a_{m+1}, \ldots, a_{m+l-1}, \alpha_m]$.

Bemerkung 2.4. Wenn also $\alpha = \alpha_0$ eine periodische Kettenbruchentwicklung hat, so gibt es $m \in \mathbb{Z}$ und $l \geq 1$ mit $\alpha_m = \alpha_{m+l}$, so dass $\alpha_i = \alpha_{i+l}$ für alle $i \geq m$ gilt; und sogar $\alpha_i = \alpha_{i+n\,l}$ für alle $i \geq m$ und $n \geq 0$.

Ein periodischer Kettenbruch ist somit notwendig unendlich.

Beispielsweise mittels Proposition 2.9 kann man sich leicht überzeugen, dass jedes α mit periodischer Kettenbruchentwicklung quadratisch über K sein muss. Wenn man besonders an rein periodischen Entwicklungen interessiert ist, bringt die folgende Definition großen Nutzen:

Definition 2.9. Ein $\alpha \in \mathbb{K}$ heißt *σ-reduziert*, wenn es einen K-Körperautomorphismus $\sigma : K(\alpha) \longrightarrow K(\alpha)$ gibt, mit $|\alpha| > 1$ und $|\sigma(\alpha)| < 1$.[5]

Bemerkung 2.5. Offensichtlich darf ein σ-reduziertes α nicht von σ fixiert werden, also kann $\alpha \in K$ oder $\sigma = \mathrm{Id}$ nicht vorkommen. Damit ist die Kettenbruchentwicklung eines σ-reduzierten α nach Proposition 2.11 stets unendlich.

Proposition 2.14. *Falls α σ-reduziert ist, so sind alle α_i σ-reduziert.*

Beweis. Zuerst ist $\alpha_0 = \alpha$ trivialerweise σ-reduziert, hat also eine unendliche Kettenbruchentwicklung.

Nun $|\alpha_{i+1}| > 1$ für $i \geq 0$ geht aus $|\tau(\alpha_i)| < 1$ hervor. Die andere Ungleichung $|\sigma(\alpha_{i+1})| < 1$ zeigt man induktiv. Aus (2.6) erhält man nämlich

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} \quad \text{sowie} \quad \sigma(\alpha_{i+1}) = \frac{1}{\sigma(\alpha_i) - a_i}.$$

Hier ist stets $|a_i| = |\alpha_i| > 1 > |\sigma(\alpha_i)|$ erfüllt, und mit

$$|\sigma(\alpha_{i+1})|^{-1} = |\sigma(\alpha_i) - a_i| = \max\left(|\sigma(\alpha_i)|, |a_i|\right) = |\alpha_i| > 1$$

folgt wie gewünscht $|\sigma(\alpha_{i+1})| < 1$. □

[5] Für Kettenbrüche über $\mathbb{Z}$ kann man eine ähnliche Eigenschaft definieren, allerdings ist dort die Bewertung nicht ultrametrisch–man muss stattdessen die totale Ordnung auf $\mathbb{R}$ benutzen.

Proposition 2.15. *Ist die Kettenbruchentwicklung eines σ-reduzierten α periodisch, so ist die Kettenbruchentwicklung sogar* rein *periodisch.*

Beweis. Wenn α periodisch ist, gibt es nach Bemerkung 2.4 $m \in \mathbb{Z}$ und $l \geq 1$ mit $\alpha_i = \alpha_{i+l}$ für alle $i \geq m$, d.h. α_m ist rein periodisch.

Da der Kettenbruch unendlich ist, gilt für alle $i \geq 0$

$$\frac{1}{\sigma(\alpha_{i+1})} = \sigma(\alpha_i) - a_i.$$

Nun ist aber α_i σ-reduziert, also hat man $|\sigma(\alpha_i)| < 1$. Zusammen mit $a_i \in R$ und Proposition 2.6 ergibt das

$$\sigma(\alpha_i) = \tau\left(\frac{1}{\sigma(\alpha_{i+1})}\right). \tag{2.8}$$

Also kann man nicht nur α_{i+1} aus α_i berechnen, sondern über σ auch α_i aus α_{i+1} bestimmen, solange man α_i σ-reduziert verlangt. Sozusagen $\alpha_{i+1} = \alpha_{j+1} \implies \alpha_i = \alpha_j$.

Damit folgern wir aus $\alpha_i = \alpha_{i+l}$ für $i \geq m$ dieselbe Gleichung auch mit $i = m-1, m-2, \ldots, 0$; also ist α rein periodisch. □

Man bemerke, dass unter der Bedingung, dass alle α_i σ-reduziert sind, man mittels (2.8) sogar α_i für alle $i \in \mathbb{Z}$ eindeutig definieren kann, nämlich durch

$$\alpha_i = \sigma^{-1}\left(\tau\left(\tfrac{1}{\sigma(\alpha_{i+1})}\right)\right) \text{ für } i < 0.$$

Dies wird unter folgenden Voraussetzungen besonders nützlich:

Proposition 2.16. *Sei $\alpha \in \mathbb{K}$ σ-reduziert mit $\alpha + \sigma(\alpha) \in R$. Weiter gebe es $l \geq 1$ und $\gamma \in R^\star$ mit $\alpha_l = \gamma\,\alpha$.*[6] *Dann ist die Kettenbruchentwicklung von α rein periodisch.*

Beweis. Nach Voraussetzung gilt $|\sigma(\alpha)| = |-\sigma(\alpha)| < 1$ und $\alpha + \sigma(\alpha) = \alpha - (-\sigma(\alpha)) \in R$, so mit Proposition 2.6 schließen wir $\tau(\alpha) = -\sigma(\alpha)$. So $\alpha_1 = \frac{-1}{\sigma(\alpha_0)}$.

Im Beweis von Proposition 2.15 hatten wir aus α σ-reduziert (2.8) gefolgert. Mit $\tau(-x) = -\tau(x)$ wegen Proposition 2.6 lässt sich (2.8) umschreiben zu

$$\frac{-1}{\sigma(\alpha_i)} = \frac{1}{\tau\left(\frac{-1}{\sigma(\alpha_{i+1})}\right)}. \tag{2.9}$$

Also kann man die $\frac{-1}{\sigma(\alpha_i)}$ als Teile einer Kettenbruchentwicklung sehen, und zwar einer Kettenbruchentwicklung, die in diejenige von α mündet![7]

$$\begin{array}{ccccccccccccccc}
\ldots & & \frac{-1}{\sigma(\alpha_3)} & \overset{1/\tau}{\mapsto} & \frac{-1}{\sigma(\alpha_2)} & \overset{1/\tau}{\mapsto} & \frac{-1}{\sigma(\alpha_1)} & \overset{1/\tau}{\mapsto} & \frac{-1}{\sigma(\alpha_0)} & & & & & & \\
 & & & & & & \alpha_0 & \overset{1/\tau}{\mapsto} & \alpha_1 & \overset{1/\tau}{\mapsto} & \alpha_2 & \overset{1/\tau}{\mapsto} & \alpha_3 & \ldots &
\end{array}$$

[6] Diese Eigenschaft nennt man quasiperiodisch oder γ-periodisch, eine Verallgemeinerung von periodisch.

[7] Hier gilt sowohl $\alpha_1 = \frac{-1}{\sigma(\alpha_0)}$ als auch $\alpha_0 = \frac{-1}{\sigma(\alpha_1)}$. Man wende dazu σ auf $\alpha + \sigma(\alpha) = r \in R$ an; man bekommt $\sigma(\alpha) + \sigma^2(\alpha) = r$, folglich $\alpha = \sigma^2(\alpha)$. Dann erhält man $\alpha_0 = \frac{-1}{\sigma(\alpha_1)}$ direkt durch Anwenden von σ auf $\alpha_1 = \frac{-1}{\sigma(\alpha_0)}$.

Nun schließen wir zum Einen durch Anwenden $1/\tau$, dass $\alpha_{l+1} = \frac{1}{\gamma}\,\alpha_1$ und zum Anderen durch Anwenden von $-1/\sigma$, dass $\alpha_1 = \frac{-1}{\sigma(\alpha_0)} = \gamma\,\frac{-1}{\sigma(\alpha_l)}$. Dann folgt durch Einsetzen sofort $\alpha_{l+1} = \frac{-1}{\sigma(\alpha_l)}$. Nach l-maligem Anwenden von $1/\tau$ erhalten wir daraus $\alpha_{2\,l+1} = \frac{-1}{\sigma(\alpha_0)} = \alpha_1$.

Damit ist dann die Kettenbruchentwicklung von α *periodisch* und nach Proposition 2.15 sogar rein periodisch. □

2.7 Bestapproximation

Im Abschnitt 2.4 hatten wir die Näherungsbrüche eingeführt, die nicht von ungefähr so heißen. Sie liefern nämlich die in gewissem Sinne beste rationale Approximation. Für uns ist hier allerdings wichtiger, dass sie wesentlich die einzigen Brüche mit dieser Eigenschaft sind.

Man erinnere $\mathcal{R} = R \times (R \setminus \{0\})$.

Definition 2.10. Ein Tupel $(p, q) \in \mathcal{R}$ heißt *Bestapproximation*[8] von $\alpha \in \mathbb{K}$, wenn für alle $(p', q') \in \mathcal{R}$ gilt:

$|p' - \alpha\,q'| \le |p - \alpha\,q|$ mit $(p', q') \in \mathcal{R}$ impliziert (i) $\frac{p}{q} = \frac{p'}{q'}$ oder (ii) $|q'| > |q|$.

Proposition 2.17. *Sind $p, q, r \in R$ und ist $(r\,p, r\,q)$ eine Bestapproximation von α, so ist auch (p, q) eine Bestapproximation von α.*

Beweis. Denn wegen $|r| \ge 1$ hat man $|r\,q| \ge |q|$ und $|p - \alpha\,q| \le |r\,p - \alpha\,r\,q|$. □

Proposition 2.18. *Für eine Bestapproximation (p, q) von α gilt $p - \alpha\,q = \tau(-\alpha\,q)$; insbesondere ist p eindeutig durch q bestimmt.*

Beweis. Wir haben nämlich $\tau(-\alpha\,q) = p' - \alpha\,q$ mit $p' \in R$ und $|p' - \alpha\,q| < 1$.

Falls $|p' - \alpha\,q| > |p - \alpha\,q|$, so gibt es einen Widerspruch zur Eindeutigkeit von τ in Proposition 2.6.

Andernfalls liefert $|p' - \alpha\,q| \le |p - \alpha\,q|$ natürlich $\frac{p'}{q} = \frac{p}{q}$, also $p' = p$ wie gewünscht. □

Proposition 2.19. *Seien $\alpha \in \mathbb{K}$, $(p, q) \in \mathcal{R}$ mit $|p - \alpha\,q| < \frac{1}{|q|}$. Dann ist (p, q) eine Bestapproximation von α.*

Beweis. Sei $(p', q') \in \mathcal{R}$ mit $|p' - \alpha\,q'| \le |p - \alpha\,q| < \frac{1}{|q|}$.

Falls $p'\,q - p\,q' = 0$ gilt, ist (i) erfüllt und wir sind fertig.

Andernfalls ist $p'\,q - p\,q' \in R \setminus \{0\}$ und wir schließen

$$1 \le \left|p'\,q - p\,q'\right| = \left|(p' - \alpha\,q')\,q - (p - \alpha\,q)\,q'\right| < \max\left(\frac{|q|}{|q|}, \frac{|q'|}{|q|}\right) = \frac{|q'|}{|q|},$$

also $|q'| > |q|$ wie in (ii). □

[8] genau genommen *Bestapproximation zweiter Art*, vgl. [2] S. 25

Bemerkung 2.6. Aus (2.7) kann man nun schließen, dass *alle* Näherungsbrüche (p_n, q_n) (für $n \geq 0$) Bestapproximationen von α sind. Die folgende Proposition sagt nun, dass die Näherungsbrüche die einzigen Bestapproximationen sind.

Satz 2.1. *Sei (p, q) eine Bestapproximation von $\alpha = [a_0, a_1, a_2, \dots]$. Dann ist $\frac{p}{q}$ ein Näherungsbruch, d.h. es gibt $n \geq 0$ mit $\frac{p}{q} = \frac{p_n}{q_n}$.*

Beweis. Die Strategie des Beweises ist, $\frac{p}{q}$ in einen Kettenbruch

$$\frac{p}{q} = [b_0, b_1, \dots, b_n]$$

zu entwickeln und durch Induktion über n zu zeigen, dass $b_i = a_i$ für $i = 0, \dots, n$ gilt. Dank Proposition 2.17 können wir außerdem annehmen, dass p, q teilerfremd sind.

Bei $n = 0$ ist $\frac{p}{q} = b_0$, also $q \in R^\star$ und $p = b_0\, q$. Aus Proposition 2.18 und Proposition 2.6 folgt

$$p - \alpha\, q = \tau(-\alpha\, q) = -q\, \tau(\alpha) = q\, (a_0 - \alpha)$$

und $b_0\, q = p = a_0\, q$ impliziert $b_0 = a_0$ wie gewünscht.

Im Induktionsschritt können wir also annehmen, dass $q \notin R^\star$, also $|q| > 1$ und $\frac{p}{q} \neq \frac{a_0}{1}$. Dann muss wegen der Bestapproximationseigenschaft gelten:

$$|a_0 - \alpha\, 1| > |p - \alpha\, q| \;\text{ folglich }\; \left|\tfrac{p}{q} - \alpha\right| < |\alpha - a_0|\,. \tag{2.10}$$

Daraus schließen wir

$$\left|\tfrac{p}{q} - a_0\right| \leq \max\left(\left|\tfrac{p}{q} - \alpha\right|, |\alpha - a_0|\right) = |\alpha - a_0| = |\tau(\alpha)| < 1 \tag{2.11}$$

Damit ist

$$\tau\left(\tfrac{p}{q}\right) = \frac{p}{q} - a_0 = \frac{p - a_0\, q}{q}$$

also wiederum $b_0 = a_0$ wie gewünscht.

Wir zeigen nun, dass $(q, p - a_0\, q)$ eine Bestapproximation von $\alpha_1 = [a_1, a_2, \dots]$ ist.

Sei also $(p', q') \in \mathcal{R}$ mit $|p' - \alpha_1\, q'| \leq |q - \alpha_1\, (p - a_0\, q)|$. Multiplizieren wir diese Ungleichung mit $\frac{1}{|\alpha_1|} = |\alpha - a_0|$, so erhalten wir

$$\left|\alpha\, p' - (q' + a_0\, p')\right| = \left|(\alpha - a_0)\, p' - q'\right| \leq |(\alpha - a_0)\, q - (p - a_0\, q)| = |\alpha\, q - p|\,. \tag{2.12}$$

Nun ist (p, q) eine Bestapproximation, so es tritt *entweder* (i) für (p, q) ein, so dass

$$\frac{q'}{p'} + a_0 = \frac{q' + a_0\, p'}{p'} = \frac{p}{q} \quad \text{und folglich} \quad \frac{p'}{q'} = \frac{q}{p - a_0\, q}$$

gilt, und (i) ebenfalls für $(q, p - a_0\, q)$ eintritt.

Oder es tritt (ii) für (p, q) ein, so dass $|p'| > |q|$ gilt. Nun aus (2.10) und (2.12) erhalten wir

$$\left|p' - \alpha_1\, q'\right| = \frac{1}{|\alpha - a_0|}\, |\alpha - a_0|\, \left|p' - \alpha_1\, q'\right| \leq \frac{|p - \alpha\, q|}{|\alpha - a_0|} < 1.$$

Zusammen mit $|\alpha_1\, q'| > 1$ ergibt das

$$\left|p'\right| = \left|p' - \alpha_1\, q' + \alpha_1\, q'\right| \leq \max\left(\left|p' - \alpha_1\, q'\right|, \left|\alpha_1\, q'\right|\right) = \left|\alpha_1\, q'\right|.$$

Nun (2.11) liefert $|\alpha_1|\,|p - a_0\, q| \leq |\alpha_1|\;|q|\;|\alpha - a_0| = |q|$, und man kann jetzt

$$|\alpha_1|\,|p - a_0\, q| \leq |q| < \left|p'\right| \leq \left|\alpha_1\, q'\right|$$

folgern und bekommt wie gewünscht $|p - a_0\, q| < |q'|$, so dass (ii) auch für $(q, p - a_0\, q)$ eintritt.

Damit ist

$$(q, p - a_0\, q) \qquad \text{wobei} \qquad \frac{q}{p - a_0\, q} = [b_1, b_2, \ldots, b_n]$$

eine Bestapproximation von $\alpha_1 = [a_1, a_2, \ldots]$ und nach Induktionsannahme gilt dann $b_i = a_i$ für $i = 1, \ldots, n$. □

2.8 Periodizität und Pell

Nun wollen wir endlich den Hauptsatz 2 beweisen. Dazu sei R ein ultrametrisch bewerteter Euklidischer Ring und $D \in R$ mit $|D| > 1$ sowie $\sqrt{D} \in \mathbb{K} \setminus K$. Die quadratische Körpererweiterung $K(\sqrt{D})$ kommt dann mit dem K-Körperautomorphismus $\sigma : K(\sqrt{D}) \longrightarrow K(\sqrt{D})$, definiert durch $\sigma(\sqrt{D}) = -\sqrt{D}$.

Proposition 2.20. *Es gibt ein eindeutiges $a \in R$, so dass $\alpha = a + \sqrt{D}$ σ-reduziert ist.*

Beweis. Setzen wir $a = \sqrt{D} - \tau(\sqrt{D}) \in R$, so haben wir $|a| = \left|\sqrt{D}\right| = \sqrt{|D|} > 1$. Nun ist offensichtlich $\sqrt{D}$ nicht σ-reduziert, dafür aber $\alpha = a + \sqrt{D}$. Denn

$$\sigma(\alpha) = a - \sqrt{D} = -\tau(\sqrt{D}) \qquad \text{folglich} \qquad |\sigma(\alpha)| < 1$$

und

$$\alpha \cdot \sigma(\alpha) = a^2 - D \in R \setminus \{0\} \qquad \text{folglich} \qquad |\alpha \cdot \sigma(\alpha)| \geq 1$$

machen $|\alpha| > 1$ notwendig.

Sind $a + \sqrt{D}$ und $a' + \sqrt{D}$ beide σ-reduziert, so folgt aus

$$\left|a - a'\right| \leq \max\left(\left|\sigma\left(a + \sqrt{D}\right)\right|, \left|\sigma\left(a' + \sqrt{D}\right)\right|\right) < 1$$

sofort $a - a' = 0$ und also die Eindeutigkeit von a. □

Wegen $\tau(\alpha) = \tau(\beta)$ (von Proposition 2.6) weichen nun die Kettenbruchentwicklungen von $\alpha = a + \sqrt{D} = [a_0, \ldots, a_n, \alpha_{n+1}] = [a_0, a_1, \ldots]$ und $\beta = \sqrt{D} = [b_0, \ldots, b_n, \beta_{n+1}] = [b_0, b_1, \ldots]$ nur im ersten Glied voneinander ab, d.h. es gilt $\alpha_i = \beta_i$ sowie $a_i = b_i$ für $i \geq 1$. Also können die beiden Kettenbruchentwicklungen nur gleichzeitig periodisch sein. Wir betrachten dabei aber nur die Näherungszähler $p_k \in R$ und -nenner $q_k \in R$ von β (*nicht* von α).

Proposition 2.21. *Sei $n \geq 1$ und $\eta = {p_{n-1}}^2 - D\,{q_{n-1}}^2$. Dann gibt es $r \in R$ mit $(-1)^n\,\eta\,\alpha_n = r + \sqrt{D}$.*

Beweis. Aus dem Korollaren 2.3 und 2.2 erhalten wir

$$\begin{aligned}\beta_n &= \frac{q_{n-2}\,\beta_0 - p_{n-2}}{p_{n-1} - q_{n-1}\,\beta_0}\\ &= \frac{q_{n-2}\,\beta - p_{n-2}}{p_{n-1} - q_{n-1}\,\beta}\;\frac{p_{n-1} + q_{n-1}\,\beta}{p_{n-1} + q_{n-1}\,\beta}\\ &= \frac{q_{n-1}\,q_{n-2}\,D - p_{n-1}\,p_{n-2} + \sqrt{D}\;(p_{n-1}\,q_{n-2} - p_{n-2}\,q_{n-1})}{{p_{n-1}}^2 - D\,{q_{n-1}}^2}\\ &= \frac{(q_{n-1}\,q_{n-2}\,D - p_{n-1}\,p_{n-2}) + (-1)^n\sqrt{D}}{{p_{n-1}}^2 - D\,{q_{n-1}}^2}.\end{aligned} \tag{2.13}$$

Mit $\beta_n = \alpha_n$ wegen $n \geq 1$ sind wir fertig. □

Proposition 2.22. *Ist (p, q) eine nicht-triviale Lösung von $(\mathrm{P}^\star)$ in R, so gibt es $n \geq 1$ und $\mu \in R^\star$ mit $p_{n-1} = \mu\,p$ und $q_{n-1} = \mu\,q$.*

Beweis. Definiere $\phi_\pm = p \pm \sqrt{D}\,q$. Ohne Einschränkung sei $|\phi_+| \geq |\phi_-|$. Es folgt

$$\left|2\sqrt{D}\,q\right| = |\phi_+ - \phi_-| \leq \max\left(|\phi_+|\,, |\phi_-|\right) = |\phi_+|$$

und so dank $\phi_+\,\phi_- = p^2 - D\,q^2 = \eta \in R^\star$ (also $|\eta| = 1$) weiter

$$\left|p - \sqrt{D}\,q\right| = |\phi_-| = \frac{1}{|\phi_+|} \leq \frac{1}{\left|2\sqrt{D}\,q\right|} < \frac{1}{|q|}.$$

Nach Proposition 2.19 ist also (p, q) eine Bestapproximation von β. Als Lösung der Pellschen Gleichung sind p und q natürlich teilerfremd. Ebenso sind die p_k und q_k wegen Proposition 2.2 je teilerfremd. Also gibt es gemäß Satz 2.1 ein $n \geq 1$ und $\mu \in R^\star$, so dass $p_{n-1} = \mu\,p$, $q_{n-1} = \mu\,q$ Näherungszähler bzw. -nenner von $\beta = \sqrt{D}$ sind. □

Beweis von Hauptsatz 2. [9] Beweisen wir nun die Existenz einer nicht-trivialen Lösung von $(\mathrm{P}^\star)$, ausgehend von einer periodischen Kettenbruchentwicklung von $\beta = \sqrt{D}$. Natürlich ist dann auch die Kettenbruchentwicklung von $\alpha = a + \sqrt{D}$ periodisch, und da α ja σ-reduziert ist, sogar rein periodisch. Also gibt es $n \geq 1$ mit $\alpha_n = \alpha_0$. Aus Proposition 2.21 erhalten wir dann

$$(-1)^n\,\eta\,\alpha_n = (-1)^n\,\eta\,(a + \sqrt{D}) = r + \sqrt{D} \quad \text{mit } \eta, a, r \in R.$$

Wegen $\sqrt{D} \notin K$ muss zwangsläufig $\eta = (-1)^n$ gelten, also ist (p_{n-1}, q_{n-1}) eine Lösung der Pellschen Gleichung. Proposition 2.12 sichert dabei $q_{n-1} \neq 0$ zu, so dass die Existenz einer *nicht-trivialen* Lösung gezeigt ist.

[9] vgl. [1], S. 494

Umgekehrt sei (p, q) eine nicht-triviale Lösung von $(\mathrm{P}^\star)$. Wir wollen nun die Periodizität der Kettenbruchentwicklung von $\beta = \sqrt{D}$ beweisen.

Dank Proposition 2.22 können wir zunächst $p = p_{n-1}, q = q_{n-1}$ für ein geeignetes $n \geq 1$ annehmen. Von Proposition 2.14 wissen wir weiter, dass alle α_i σ-reduziert sind. Proposition 2.21 sagt nun, dass wir die Form $(-1)^n \eta \alpha_n = r + \sqrt{D}$ haben. Da nach Voraussetzung $|\eta| = 1$ gilt, ist auch $r + \sqrt{D}$ σ-reduziert. Wir schließen mit Proposition 2.20 sofort $r = a$ und somit $(-1)^n \eta \alpha_n = \alpha_0$. Aber nun sind wir in der Situation von Proposition 2.16 (mit $\gamma = (-1)^n \eta^{-1}$), da ja $\alpha + \sigma(\alpha) = 2a \in R$ ist. Es folgt, dass die Kettenbruchentwicklungen von α und β *beide* periodisch sind. □

Wir schließen diesen Abschnitt mit einer weiteren nützlichen Konsequenz von Proposition 2.22 ab:

Satz 2.2. *Es seien $R \subset R'$ Euklidische Ringe mit* derselben *ultrametrischen Bewertung, es seien $K \subset K'$ und $\mathbb{K} \subset \mathbb{K}'$ die jeweiligen Quotientenkörper und deren Vervollständigungen.*

Sei $D \in R$ mit $|D| > 1$ und $\sqrt{D} \in \mathbb{K}$. Sei weiter (p', q') eine Lösung von $(\mathrm{P}^\star)$ in R'. Dann gibt es $\mu \in R'^\star$ und eine Lösung von $(\mathrm{P}^\star)$ in R mit $\mu p' = p$ und $\mu q' = q$.

Beweis. Für eine triviale Lösung $(p', q') = (p', 0)$ ist $|p'| = 1$ wegen $\left|p'^2\right| = 1$, so mit $\mu = p'^{-1}$ kommt man zu $(1, 0) \in R^2$.

Bei einer nicht-trivialen Lösung können wir annehmen, dass D kein Quadrat ist (siehe Proposition 2.25 im nächsten Abschnitt[10]). Jetzt greift Proposition 2.22 für R', und es gibt $n \geq 0$ und $\mu \in R'^\star$, so dass $p_n = \mu p'$ ein Näherungszähler und $q_n = \mu q'$ ein Näherungsnenner von $\sqrt{D}$ ist.

Wegen Proposition 2.6 stimmen die Abschneideabbildungen τ und τ' auf $\mathbb{K}$ überein, so dass es keinen Unterschied macht, ob wir die Kettenbruchentwicklung von $\beta = \sqrt{D}$ in $\mathbb{K}$ oder $\mathbb{K}'$ ausführen. Insbesondere sind die $b_i = \beta_i - \tau(\beta_i)$ allesamt in R, so dass vermöge Proposition 2.8 sowohl p_n als auch q_n in R sind.

Wir überprüfen noch, dass (p_n, q_n) tatsächlich eine Lösung von $(\mathrm{P}^\star)$ liefert. Es sei $\eta = {p_n}^2 - D\,{q_n}^2 \in R$. Dann haben wir $\eta = \mu^2 (p'^2 - D\,q'^2) = \mu^2 \eta'$ mit $\eta' \in R'^\star$, da ja (p', q') eine Lösung von $(\mathrm{P}^\star)$ ist. Da R und R' beide euklidisch sind, folgern wir nun aus $\mu, \eta' \in R'^\star$ mit Proposition 2.3 $|\eta| = |\mu|^2 \, |\eta'| = 1$ und somit $\eta \in R^\star$. Also ist (p_n, q_n) die gesuchte Lösung in R. □

2.9 Pell mit Quadraten

Im Hauptsatz stellen wir zweierlei Bedingungen an D: Zum Einen fordern wir $|D| > 1$, zum Anderen darf D kein Quadrat in K sein. Dieser Abschnitt klärt die Situation in einem ultrametrisch bewertetem Euklidischen Ring R, wenn diese Bedingungen gerade nicht zutreffen.

[10] Diese Proposition ist natürlich unabhängig vom hier zu beweisenden Satz, der erst in den nachfolgenden Kapiteln zur Anwendung kommt.

Proposition 2.23. *Die Menge $k = \{x \in R \mid |x| \leq 1\} = \{0\} \cup R^\star$ ist ein Körper.*

Beweis. Offensichtlich ist k abgeschlossen unter der Multiplikation, enthält 0 und 1 und ist wegen der ultrametrischen Ungleichung auch abgeschlossen unter der Addition. Somit ist k sicher ein Unterring von R und wegen $k \setminus \{0\} = R^\star$ eben ein Körper. □

Gilt nun $D \in k$, so erhalten wir womöglich zahlreiche nicht-triviale Lösungen von (P) in $k \times k$ (besonders, wenn k algebraisch abgeschlossen ist). Man erinnere, dass ja auch die trivialen Lösungen von (P) mit $q = 0$ in k liegen. Interessant ist nun, dass es nur Lösungen in k geben kann—natürlich abgesehen vom Fall $D = 0$.

Proposition 2.24. *Sei $D \in R$ mit $|D| = 1$. Dann ist jede Lösung von $(\mathrm{P}^\star)$ in R bereits in $k \times k$ enthalten.*

Beweis. Nehmen wir an, dass wir $(p, q) \in R^2$ mit $|q| > 1$ und $p^2 - D\,q^2 = \eta \in R^\star$ haben. Proposition 2.1 liefert wegen $\left|D\,q^2\right| > 1$

$$\left|p^2\right| = \left|\eta + D\,q^2\right| = \max(|\eta|\,, \left|D\,q^2\right|) = \left|D\,q^2\right| = \left|q^2\right|$$

also $|p| = |q|$.

Nun R war als euklidisch vorausgesetzt, also gibt es $a, b \in R$ mit $p = a\,q + b$ und $|b| < |q|$. Dabei ist $a = 0$ wegen $|b| < |p|$ unmöglich. So es ist sicher $|a\,q| > |b|$ und wieder wegen Proposition 2.1 haben wir $|p| = |a|\ |q|$, also $|a| = 1$.

Setzen wir nun $a\,q + b$ für p in die Pellsche Gleichung ein, erhalten wir

$$\begin{aligned} p^2 - D\,q^2 &= a^2\,q^2 + 2\,a\,b\,q + b^2 - D\,q^2 = \eta \\ (a^2 - D)\,q^2 &= \eta - 2\,a\,b\,q - b^2 \end{aligned} \tag{2.14}$$

Wäre nun $b = 0$, so müsste q eine Einheit sein, was wegen $|q| > 1$ unmöglich ist.

Andernfalls ist $b \neq 0$ und es gilt $1 \leq \left|b^2\right| < |b\,q| = |a\,b\,q| < \left|q^2\right|$ und so nochmals mit Proposition 2.1

$$\left|\eta - 2\,a\,b\,q - b^2\right| = |b\,q| < \left|q^2\right|$$

für die rechte Seite von (2.14). Der Betrag der linken Seite hingegen muss entweder 0 sein, falls $a^2 - D = 0$, oder aber $\geq \left|q^2\right|$. In keinem Falle kann er also mit dem Betrag der rechten Seite übereinstimmen.

Also gibt es keine Lösung mit $|q| > 1$ und es gilt $q \in k$. Somit ist $\left|p^2\right| \leq \left|\eta + D\,q^2\right| \leq 1$ und es gilt $p \in k$. □

Damit kann man nun sehr leicht beschreiben, was passiert, wenn D ein Quadrat ist.

Proposition 2.25. *Sei $D \in R$ ein Quadrat mit $|D| > 1$. Dann hat $(\mathrm{P}^\star)$ in R nur triviale Lösungen.*

Beweis. Mit $D = e^2$ wo $e \in R$ und $(p, q) \in R^2$ eine Lösung von $(\mathrm{P}^\star)$ ist, haben wir

$$p^2 - D\,q^2 = p^2 - (e\,q)^2 = \eta$$

folglich ist $(p, e\,q) \in R^2$ eine Lösung von $(\mathrm{P}^\star)$, aber mit „$D = 1$“.

Nun wegen $|D| > 1$ gilt auch $|e| > 1$. Gemäß Proposition 2.24 ist aber $|e|\ |q| = |e\,q| \leq 1$, also $|q| \leq 1/\,|e| < 1$, es muss somit $q = 0$ gelten. Also kann es wirklich nur triviale Lösungen geben. □

2.10 Charakterisierung von $k[X]$

Die klassische Situation für Kettenbruchentwicklungen ist der Ring $R = \mathbb{Z}$ der ganzen Zahlen. Die Bewertung ist dabei der übliche absolute Betrag auf $\mathbb{Z}$.

$$|x| = \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}$$

Mit der üblichen Division mit Rest wird $\mathbb{Z}$ zu einem Euklidischen Ring—die Peano-Axiome garantieren ja, dass jede Teilmenge von $\mathbb{N}$ ein Minimum hat. Allerdings ist die Bewertung natürlich nicht ultrametrisch.

Trotzdem findet man in $\mathbb{R}$, der Vervollständigung des Quotientenkörpers $\mathbb{Q}$, Abschneideabbildungen von $\mathbb{Z}$, wie z.B.

$$\begin{aligned} \tau(x) &= x - [x] = \max\{n + x \mid n \in \mathbb{Z}, n + x < 1\} \geq 0 \\ \tilde{\tau}(x) &= x + [-x] = \min\{n + x \mid n \in \mathbb{Z}, n + x > -1\} \leq 0 \end{aligned}$$

und viele weitere, die aber für jedes einzelne $x \in \mathbb{R}$ entweder mit $\tau(x)$ oder $\tilde{\tau}(x)$ übereinstimmen. Damit gehen die Eindeutigkeit (und je nachdem auch viele Symmetrien) aus Proposition 2.6 verloren.

Unser eigentliches Anliegen war aber die Situation im Polynomring $k[X]$ mit Quotientenkörper $k(X)$. Diesen kann man mit der ultrametrischen Bewertung

$$|x| = \begin{cases} e^{\deg x}, & \text{falls } x \neq 0 \\ 0, & \text{falls } x = 0 \end{cases}$$

versehen. Die übliche Polynomdivision, mit Rest von kleinerem Grad als der Teiler, macht $k[X]$ zu einem Euklidischen Ring. Die Menge der möglichen Werte ist wesentlich $\exp(\mathbb{N})$, so dass die Minimierungseigenschaft erfüllt ist. Man bemerke hier, dass die ultrametrische Bewertung durch $|X| = e$ und $|x| = 1$ für $x \in k^\star$ eindeutig definiert ist. Anstatt e kann natürlich eine beliebige reelle Zahl $m > 1$ als Basis dienen.

Die Vervollständigung des Quotientenkörpers $k(X)$ ist dann der Körper $k((X^{-1}))$ der Laurentreihen in X^{-1}:

$$k((X^{-1})) = \left\{ \sum_{i=-n}^{\infty} c_i \, X^{-i} \;\middle|\; c_i \in k; n \in \mathbb{Z} \right\}$$

Ist $c_{-n} \neq 0$, so ist dabei n der Grad der Laurentreihe.

Durch Entfernen des Polynomteils, i.e.

$$\tau\left(\sum_{i=-n}^{\infty} c_i \, X^{-i} \right) = \sum_{i=\max(1,-n)}^{\infty} c_i \, X^{-i}$$

definiert man die eindeutige Abschneideabbildung.

Nimmt man übrigens das Quadrat einer Laurentreihe, so bekommt man mit dem Cauchy-Produkt

$$\left(\sum_{i=-n}^{\infty} c_i\, X^{-i}\right)^2 = \sum_{i=-2n}^{\infty} \sum_{k+l=i} c_k\, c_l\, X^{-i} = {c_{-n}}^2\, X^{2n} + \dots .$$

Damit also $\sqrt{D} \in k((X^{-1}))$ sein kann, muss $D \in k[X]$ sowohl geraden Grad haben, als auch der Leitkoeffizient ein Quadrat in k sein–genau wie in Proposition 1.1.

Tatsächlich ist $k[X]$ wesentlich das einzige Beispiel für einen ultrametrisch bewerteten Euklidischen Ring:

Satz 2.3. *Sei R ein ultrametrisch bewerteter Euklidischer Ring und sei $k = R^\star \cup \{0\}$ wie in Proposition 2.23 ein Unterkörper.*

Dann ist entweder $R = k$ ein Körper, oder es gibt $X \in R$ transzendent über k, so dass $R = k[X]$ ein Polynomring ist.

Beweis. Gilt $R \neq k$, so ist die Menge $M = \{|x| \mid x \in R,\ |x| > 1\}$ nicht leer, hat also ein Minimum $m > 1$, das bei mindestens einem $X \in R$ angenommen werde.

Wir zeigen nun durch eine Induktion, dass $M_n := \{x \in R \mid |x| < m^n\}$ für alle $n = 1, 2, \dots$ in $k[X]$ enthalten ist, und folglich $R \subset k[X]$ und damit $R = k[X]$ gilt.

Für die Verankerung bei $n = 1$ bemerken wir, dass $|x| < m$ sofort $|x| \leq 1$ zur Folge hat, da m das Minimum der Werte > 1 ist. Also gilt nach Proposition 2.23 $M_1 = k$ und somit $M_1 \subset k[X]$.

Sonst sei $x \in M_{n+1}$ beliebig. Dann ist natürlich $r = \varrho(x, X^n) \in M_n \subset k[X]$, und wir müssen nur noch $\tilde{x} = x - r \in k[X]$ zeigen. Nun haben wir aber $\tilde{x} = q\, X^n$ und also

$$|q|\ m^n = |q\, X^n| = |\tilde{x}| \leq \max(|x|, |r|) < m^{n+1}$$

folglich $|q| < m$, d.h. $q \in M_1 = k$.

Damit ist $R = k[X]$ gezeigt, und wir müssen nur noch die Transzendenz von X über k zeigen; aber für $a_0, \dots, a_n \in k$ mit $a_n \neq 0$ gilt mit Proposition 2.1

$$|a_0 + a_1\, X + \dots + a_n\, X^n| = |a_n|\ |X|^n = |X|^n \neq 0, \tag{2.15}$$

so dass X keinesfalls algebraisch sein kann. □

Bemerkung 2.7. Aus (2.15) geht auch hervor, dass für $x \in R \setminus \{0\} = k[X] \setminus \{0\}$ dann $|x| = m^{\deg x}$ gilt.

Zusammen mit Proposition 2.25 geht damit der Hauptsatz 1 aus Hauptsatz 2 hervor, und mit Satz 2.3 bekommt man die Umkehrung.

Mit Hilfe dieser Charakterisierung zeigen wir nun noch, dass unter den Voraussetzungen von Hauptsatz 2 und der zusätzlichen Annahme, dass $k = R^\star \cup \{0\}$ endlich ist, die Kettenbruchentwicklung von $\beta = \sqrt{D}$ stets periodisch ist.

Proposition 2.26. *Angenommen, $x = \frac{r+\sqrt{D}}{s}$ ist σ-reduziert, mit $(r, s) \in \mathcal{R}$. Dann gilt $|r| = \left|\sqrt{D}\right|$ und $|s| < \left|\sqrt{D}\right|$.*[11]

Beweis. Nach Voraussetzungen gilt ja $|\sigma(x)| < 1 < |x|$, was wir als

$$\left|r - \sqrt{D}\right| < |s| < \left|r + \sqrt{D}\right|$$

schreiben können. Nun ist $|r| \neq \left|\sqrt{D}\right|$ ausgeschlossen, da sonst mit Proposition 2.1 sofort $\left|r - \sqrt{D}\right| = \left|r + \sqrt{D}\right|$ gilt. Es muss also $|r| = \left|\sqrt{D}\right|$ gelten und dann mit der ultrametrischen Ungleichung $|s| < \left|\sqrt{D}\right|$. □

Satz 2.4. *Es seien $D \in R$ wie in Hauptsatz 2 und außerdem sei $R^\star$ endlich. Dann ist die Kettenbruchentwicklung von $\sqrt{D}$ periodisch.*

Beweis. Aus (2.13) können wir ersehen, dass wir für jedes $n \geq 0$

$$\beta_n = \frac{r_n + \sqrt{D}}{s_n} \quad \text{mit } (r_n, s_n) \in \mathcal{R} \tag{2.16}$$

haben und für $n \geq 1$ ist β_n obendrein σ-reduziert (wie im Beweis von Hauptsatz 2 erläutert).

Mit der vorhergehenden Proposition ist dann $|r_n|, |s_n| \leq \left|\sqrt{D}\right|$, was nach Bemerkung 2.7 einer Beschränkung des Grades in X gleichkommt, wenn wir $R = k[X]$ denken. Für diese Betrachtungen war übrigens die Endlichkeit von $R^\star$ bzw. k noch nicht nötig.

Über einem endlichen Grundkörper k gibt allerdings nur endlich viele Möglichkeiten für die im Grad beschränkten Polynome r_n, s_n, also ebenso nur endliche viele Möglichkeiten für die β_n, so dass letztendlich die unendliche Kettenbruchentwicklung periodisch werden muss. □

2.11 Berechnung der Kettenbruchentwicklung

Die Form (2.16) erlaubt zusätzlich auch die effiziente Berechnung der Kettenbruchentwicklung von $\beta = \sqrt{D}$, ausschließlich mit Polynomarithmetik.Wir entwickeln dazu rekursive Formeln für die im Grad beschränkten r_n und s_n.

Mit $\beta_0 = \sqrt{D}$ gilt natürlich $r_0 = 0$ und $s_0 = 1$. Alle weiteren Terme berechnen wir über

$$\beta_{n+1} = \frac{1}{\beta_n - b_n} = \frac{s_n}{r_n + \sqrt{D} - b_n\, s_n} = \frac{s_n\, \left((b_n\, s_n - r_n) + \sqrt{D}\right)}{D - (b_n\, s_n - r_n)^2}$$

woraus wir die rekursiven Formeln

$$r_{n+1} = b_n\, s_n - r_n \quad \text{und} \quad s_{n+1} = \frac{D - {r_{n+1}}^2}{s_n} \tag{2.17}$$

[11] vgl. [6], S. 159

erhalten. Die b_n wiederum berechnen wir aus r_n und s_n. Dazu sei $\varepsilon = \tau(\sqrt{D})$, $|\varepsilon| < 1$ und $a \in R$ mit $\sqrt{D} = a + \varepsilon$. Mit $|s_n| \geq 1$ und $\tau(\beta_n) = \beta_n - b_n$ bekommen wir

$$\left| \frac{r_n + a}{s_n} - b_n \right| \leq \max \left(|\beta_n - b_n| , \left| \frac{\varepsilon}{s_n} \right| \right) < 1$$

und es folgt

$$\tau \left(\frac{r_n + a}{s_n} \right) = \frac{r_n + a}{s_n} - b_n$$

beziehungsweise

$$b_n = \frac{r_n + a}{s_n} - \tau \left(\frac{r_n + a}{s_n} \right) = \frac{r_n + a}{s_n} - \frac{\varrho(r_n + a, s_n)}{s_n},$$

so dass wir b_n mittels Polynomdivision von $r_n + a$ durch s_n berechnen können, wobei man den Divisionsrest einfach ignoriert.

Aus den b_n lassen sich dann mittels Korollar 2.1 die p_n und q_n berechnen. Lösungen der Pellschen Gleichung und die Periodenlänge findet man – sofern vorhanden – nun relativ einfach, indem man nach l mit $|s_l| = 1$ bzw. $\deg s_l = 0$ sucht (vgl. (2.13) im Beweis von Proposition 2.21).

Man benötigt also nur Polynomarithmetik, um diese Rechnungen – am schnellsten auf dem Computer – durchzuführen.

3 Eine elliptische Kurve

Es sei k ein Körper mit $\operatorname{char} k \neq 2, 3$ und $\overline{k}$ sein algebraischer Abschluss.

3.1 (Semi)invarianten

Wir betrachten

$$\mathbb{B}_n = \left\{ a_0 {X_0}^n + \binom{n}{1} a_1 {X_0}^{n-1} Z_0 + \cdots + \binom{n}{n-1} a_{n-1} X_0 {Z_0}^{n-1} + a_n {Z_0}^n \,\middle|\, a_i \in k \right\},$$

den Vektorraum der Binärformen von Grad n. Durch

$$p(X_0, Z_0) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = p(a\,X_0 + b\,Z_0, c\,X_0 + d\,Z_0)$$

ist darauf eine $\mathbf{SL}(2, \overline{k})$ (Rechts)Wirkung definiert.

Nun können wir auf $\mathbb{B}_n$ seinerseits polynomiale Formen betrachten.

Definition 3.1. Eine polynomiale Form $I : \mathbb{B}_n \longrightarrow k$ nennen wir *Invariante*, wenn sie auf den Bahnen von $\mathbf{SL}(2, \overline{k})$ konstant ist.

Eine polynomiale Form $S : \mathbb{B}_n \longrightarrow k$ nennen wir *Semiinvariante*, wenn sie zumindest auf den Bahnen der Untergruppe der Translationen $\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \,\middle|\, \lambda \in \overline{k} \right\}$ konstant ist.

Also ist jede Invariante insbesondere eine Semiinvariante.

Proposition 3.1. *Aus der klassischen Invariantentheorie sind für*

$$a_0 {X_0}^4 + 4\,a_1 {X_0}^3 Z_0 + 6\,a_2 {X_0}^2 {Z_0}^2 + 4\,a_3 X_0 {Z_0}^3 + a_4 {Z_0}^4$$

u.a. die folgenden Invarianten und Semiinvarianten bekannt:[1]

$$\begin{aligned} & & s_1 &= a_0 \\ g_2 &= 3\,{a_2}^2 - 4\,a_1\,a_3 + a_0\,a_4 & s_2 &= {a_1}^2 - a_0\,a_2 \\ g_3 &= -{a_2}^3 + 2\,a_1\,a_2\,a_3 + a_0\,a_2\,a_4 - a_0\,{a_3}^2 - {a_1}^2\,a_4 & s_3 &= 2\,{a_1}^3 - 3\,a_0\,a_1\,a_2 + {a_0}^2\,a_3 \\ \Delta &= {g_2}^3 - 27\,{g_3}^2 \quad \textit{(die Diskriminante)} & & \end{aligned}$$

[1] vgl. [5], S. 80. Die Semiinvarianten entsprechen den Leitkoeffizienten der Kovarianten; dabei entspricht s_1 der Form selbst, $-s_2$ der Hesseschen Kovariante und s_3 der Jacobischen Determinante; weiter entspricht g_2 der Apolaren $A(f, f)$ und g_3 der Apolaren $A(f, h)$.

Proposition 3.2. *Die beiden Quotienten* $x = s_2/s_1$ *und* $y = s_3/{s_1}^{3/2}$ *genügen der Gleichung*

$$y^2 = 4\,x^3 - g_2\,x - g_3.$$

Auch diese Proposition ist ein bekanntes Resultat aus der Invariantentheorie.[2] Damit können wir Binärformen von Grad 4 eine kanonische elliptische Kurve mit einem (wenn auch nicht genau in dieser Form) kanonischen, nahezu k-rationalen Punkt zuordnen, und den folgenden Hauptsatz formulieren:

Hauptsatz 3. *Sei* k *ein Körper mit* $\operatorname{char} k \neq 2, 3$ *und* $R = k[X]$*, sowie* $D \in R$ *mit* $\Delta \neq 0$ *(so* D *ist quadratfrei) von Grad* 4*, wobei*

$$D(X) = a_0\,X^4 + 4\,a_1\,X^3 + 6\,a_2\,X^2 + 4\,a_3\,X + a_4, \qquad \textit{mit } \sqrt{a_0} \in k.$$

Mit

$$a = -g_2/4, \qquad b = -g_3/4, \qquad u = x = s_2/s_1, \qquad v = y/2 = s_3/\left(2\,{s_1}^{3/2}\right)$$

definiert $V^2 = U^3 + a\,U + b$ *dann eine elliptische Kurve mit den Punkten* $Q_\pm = (u, \pm v)$.[3]

Und die Pellsche Gleichung $(\mathrm{P}^\star)$ *über* R *hat* genau dann *eine nicht-triviale Lösung* (p, q)*,* wenn $Q_\pm$ *endliche Ordnung hat.*

Außerdem gibt es eine Lösung (p, q) *von* $(\mathrm{P}^\star)$ *mit* $\deg p = n$ *genau dann, wenn* $n\,Q_\pm = O$ *gilt.*

Für den Beweis nutzen wir, dass man die Lösungen von $(\mathrm{P}^\star)$ als Elemente des Funktionenkörpers $\mathcal{F}_\mathcal{C}$ der Kurve $\mathcal{C}$ definiert durch $Y^2 = D(X)$ auffassen kann und eine Koordinatentransformation konstruieren kann, mit der man diesen nach dem Funktionenkörper der elliptischen Kurve senden kann. Dort kann man dann mit Hilfe der Ordnungsfunktionen die Endlichkeit der Ordnung von $Q_\pm$ untersuchen.

3.2 Richtung Riemann-Roch

Für den Beweis des Hauptsatzes greifen wir auf eine Reihe von allgemeinen Resultaten aus der Vorlesung Elliptische Kurven I sowie einige weitere allgemeine Resultate, die wir an dieser Stelle zur Referenz auflisten bzw. beweisen.

Sei K ein algebraisch abgeschlossener Körper mit $\operatorname{char} K \neq 2, 3$. Sei $E/K : V^2 = C(U)$ eine elliptische Kurve (in Weierstrass-Form) mit unendlichem Punkt O. Sei weiter $\mathcal{F}_E = K(U, V)$ der zugehörige Funktionenkörper.

Hilfssatz 3.1. *Sei* $f \in K[U, V] \subset \mathcal{F}_E$*,* $f \neq 0$ *und* $P \in E_0(K) = E(K) \setminus \{O\}$*. Dann ist*

- $\operatorname{ord}_P f \geq 0$
- $f(P) = 0$ *genau wenn* $\operatorname{ord}_P f \geq 1$

[2] vgl. [5], S. 81 als Gleichung zwischen Kovarianten. Da alle Summanden gleichen Grad haben, kann man direkt zu den Leitkoeffizienten, also den Semiinvarianten übergehen.

[3] vgl. [1], S. 482f. Dort findet sich eine ähnliche Konstruktion in der Gegenrichtung, wobei aber eine andere Transformation verwendet wird.

Hilfssatz 3.2. *Sei $f \in K(U)$, $f \neq 0$, und sei $P \in E(K)$. Dann gelten*

- $\operatorname{ord}_P f = \operatorname{ord}_{U_0} f$ *falls* $V_0 \neq 0$ *bei* $P = (U_0, V_0) \in E_0(K)$.
- $\operatorname{ord}_P f = 2 \operatorname{ord}_{U_0} f$ *falls* $P = (U_0, V_0) \in E_0(K)$ *mit* $V_0 = 0$.
- $\operatorname{ord}_P f = 2 \operatorname{ord}_\infty f$ *falls* $P = O$.

Hilfssatz 3.3. *Für $f \in {\mathcal{F}_E}^\star$ und $P \in E(K)$ gilt*

$$\operatorname{ord}_{\bar{P}} f = \operatorname{ord}_P \bar{f}$$

wobei $\bar{P} = -P$ ist und $\bar{f}$ durch die Konjugation $V \leftrightarrow -V$ aus f hervorgeht.

Hilfssatz 3.4 (Summenformel)**.** *Sei $f \in {\mathcal{F}_E}^\star$. Dann gibt es höchstens endlich viele $P \in E(K)$ mit $\operatorname{ord}_P f \neq 0$; und in $\mathbb{Z}$ gilt*

$$\sum_{P \in E(K)} \operatorname{ord}_P(f) = 0.$$

Hilfssatz 3.5. *Sei $f \in {\mathcal{F}_E}^\star$ mit $\operatorname{ord}_P f \geq 0$ für alle $P \in E(K)$. Dann ist f eine Konstante.*

Hilfssatz 3.6. *Sei $P_0 \in E(K)$. Sei $f \in {\mathcal{F}_E}^\star$ mit $\operatorname{ord}_P f \geq 0$ für alle $P \neq P_0$ und $\operatorname{ord}_{P_0} f \geq -1$. Dann ist f eine Konstante.*

Hilfssatz 3.7. *Sei $f \in {\mathcal{F}_E}^\star$ mit $\operatorname{ord}_P f \geq 0$ für alle $P \in E_0(K)$ und $\operatorname{ord}_O f \geq -2$. Dann ist $f = \alpha + \beta U$ mit $\alpha, \beta \in K$.*

Definition 3.2. Jedem $f \in {\mathcal{F}_E}^\star$ ist also ein Divisor

$$\operatorname{div} f = \sum_{P \in E(K)} \operatorname{ord}_P f \cdot [P],$$

zugeordnet, zu verstehen im freien $\mathbb{Z}$-Modul erzeugt von allen $[P]$ mit $P \in E(K)$.

Hilfssatz 3.8 (Haupthilfssatz)**.** *Seien $P, Q, R \in E(K)$ mit $P + Q = R$. Dann gibt es $f_{PQ} \in {\mathcal{F}_E}^\star$ mit*

$$\operatorname{div}(f_{PQ}) = [P] + [Q] - [R] - [O].$$

Hilfssatz 3.9. *Die f_{PQ} aus Hilfssatz 3.8 erzeugen die Gruppe ${\mathcal{F}_E}^\star / K^\star$.*

Beweis. Sei $f \in {\mathcal{F}_E}^\star$ beliebig. Wegen der Summenformel (Hilfssatz 3.4) gilt

$$n := \sum_{\substack{P \in E(K) \\ \operatorname{ord}_P f > 0}} \operatorname{ord}_P f = - \sum_{\substack{P \in E(K) \\ \operatorname{ord}_P f < 0}} \operatorname{ord}_P f \geq 0.$$

So man kann schreiben

$$\operatorname{div}(f) = [P_1] + [P_2] + \cdots + [P_n] - [Q_1] - [Q_2] - \cdots - [Q_n]$$

für Nullstellen P_i und Pole Q_i.

Sei $G \subset {\mathcal{F}_E}^\star/K^\star$ die Gruppe durch die f_{PQ} mit $P, Q \in E(K)$ erzeugt. Man zeigt durch Induktion über n, dass $f \in G$ gilt.

Für $n = 0$ hat man $\operatorname{ord}_P f \geq 0$ für alle $P \in E(K)$, so nach Hilfssatz 3.5 gilt $f \in K^\star$, somit klar $f \in G$.

Für $n = 1$ hat man $\operatorname{ord}_P f \geq 0$ für alle $P \neq Q_1$ und $\operatorname{ord}_{Q_1} f \geq -1$, so nach Hilfssatz 3.6 ist $f \in K^\star$, also $f \in G$.

Nun für $n \geq 2$ betrachtet man

$$\begin{aligned}\operatorname{div}(f_{P_1P_2}) &= [P_1] + [P_2] - [P_1 + P_2] - [O],\\ \operatorname{div}(f_{Q_1Q_2}) &= [Q_1] + [Q_2] - [Q_1 + Q_2] - [O]\end{aligned}$$

woraus man

$$\operatorname{div}\left(f \cdot \frac{f_{Q_1Q_2}}{f_{P_1P_2}}\right) = [P_1 + P_2] + [P_3] + \cdots + [P_n] - [Q_1 + Q_2] - [Q_3] - \cdots - [Q_n]$$

erhält. Nach Induktionsannahme gilt nun $f \cdot f_{Q_1Q_2}/f_{P_1P_2} \in G$, so offensichtlich auch $f \in G$. □

Hilfssatz 3.10 (Summenformel in $E(K)$)**.** *Sei $f \in {\mathcal{F}_E}^\star$. Dann gilt in $E(K)$*

$$\sum_{P \in E(K)} (\operatorname{ord}_P f) \cdot P = O.$$

Beweis. Wir bezeichnen die Summe auf der linken Seite mit $S(f)$. Wegen $\operatorname{ord}_P(f \cdot g) = \operatorname{ord}_P f + \operatorname{ord}_P g$ folgt

$$S(f \cdot g) = \sum_{P \in E(K)} (\operatorname{ord}_P(f \cdot g)) \cdot P = \sum_{P \in E(K)} (\operatorname{ord}_P f + \operatorname{ord}_P g) \cdot P = S(f) + S(g)$$

und also ist $S : {\mathcal{F}_E}^\star \longrightarrow E(K)$ ein Gruppenhomomorphismus. Für $f \in K^\star$ gilt für alle $P \in E(K) :\ \operatorname{ord}_P f = 0$. Damit ist $K^\star \subset \ker S$ und S faktorisiert unter der natürlichen Projektion zu $\tilde{S} : {\mathcal{F}_E}^\star/K^\star \longrightarrow E(K)$.

Aber für f_{PQ} gilt $\operatorname{div} f_{PQ} = [P] + [Q] - [R] - [O]$ mit $P + Q = R$ und so hat man

$$\tilde{S}(f_{PQ}) = S(f_{PQ}) = (+1)\, P + (+1)\, Q + (-1)\, R + (-1)\, O = O.$$

Da die f_{PQ} die Gruppe ${\mathcal{F}_E}^\star/K^\star$ erzeugen, so sind sowohl $\tilde{S}$ als auch S konstant O und der Hilfssatz ist bewiesen. □

Proposition 3.3. *Es sei $p + V\, q \in {\mathcal{F}_E}^\star$ mit $p, q \in K[U]$ und $m \geq 1$. Dann gilt*

$$\operatorname{ord}_O(p + V\, q) \geq -m \text{ genau wenn } \deg p \leq \tfrac{1}{2}\, m \text{ und } \deg q \leq \tfrac{1}{2}\,(m-3)$$

Beweis. Wir bemerken zunächst, dass $\operatorname{ord}_O V = -3$ und schreiben (mittels Hilfssatz 3.2) die Ungleichungen auf der rechten Seite um zu

$$\begin{aligned} \operatorname{ord}_O p &= -2 \deg p \geq -m, \\ \operatorname{ord}_O(V\,q) = \operatorname{ord}_O V + \operatorname{ord}_O q &= -3 + (-2) \deg q \geq -m. \end{aligned}$$

Damit folgert man

$$\operatorname{ord}_O(p + V\,q) \geq \min\left(\operatorname{ord}_O p, \operatorname{ord}_O(V\,q)\right) \geq -m$$

sowie in der Gegenrichtung vermöge $\operatorname{ord}_O(p + V\,q) = \operatorname{ord}_O(p - V\,q) = \operatorname{ord}_O(-p + V\,q)$

$$\begin{aligned} \operatorname{ord}_O p = \operatorname{ord}_O(2\,p) &\geq \min\left(\operatorname{ord}_O(p + V\,q), \operatorname{ord}_O(p - V\,q)\right) \geq -m, \\ \operatorname{ord}_O(V\,q) = \operatorname{ord}_O(2\,V\,q) &\geq \min\left(\operatorname{ord}_O(p + V\,q), \operatorname{ord}_O(-p + V\,q)\right) \geq -m. \end{aligned}$$

□

Satz 3.1. *Sei $P \in E(K)$ und $m \geq 1$. Es gibt genau dann $g \in K[U,V] \subset \mathcal{F}_E$ mit*

$$\operatorname{div}(g) = m \cdot [P] - m \cdot [O], \tag{3.1}$$

wenn $m\,P = O$ gilt.

Beweis. Haben wir m und g mit (3.1), so folgt gemäß der Summenformel in $E(K)$ (Hilfssatz 3.10)

$$O = m\,P - m\,O = m\,P.$$

Damit ist die eine Richtung gezeigt.

Für die andere Richtung nehmen wir $m\,P = O$ an, und bemerken zunächst, dass die Aussage für $P = O$ mit $g = 1$ trivial erfüllbar ist. Für $P \neq O$ betrachten wir den K-Vektorraum

$$\mathbb{V} = \left\{p + V\,q \mid p, q \in K[U] \text{ mit } \deg p \leq \tfrac{1}{2}\,m, \deg q \leq \tfrac{1}{2}\,(m-3)\right\} \subset K[U,V] \subset \mathcal{F}_E.$$

Da genau eines von m und $m-3$ ungerade ist, ist

$$\dim \mathbb{V} = 1 + \tfrac{1}{2}\,m + 1 + \tfrac{1}{2}\,(m-3) - \tfrac{1}{2} = m.$$

Ferner sei $\lambda_P : \mathbb{V} \longrightarrow K[[t]]$ eine injektive K-lineare Abbildung mit $\operatorname{ord}_P g = \operatorname{ord}_{t=0} \lambda_P(g)$ für alle $g \in \mathbb{V}$.[4] Die Bedingung $\operatorname{ord}_P g \geq m-1$ lässt sich also durch $m-1$ lineare Bedingungen, nämlich dem Verschwinden der ersten $m-1$ Koeffizienten der Potenzreihe $\lambda_P(g)$, ausdrücken. Wegen $\dim \mathbb{V} = m$ finden wir eine nicht-triviale Lösung $g \in \mathbb{V} \setminus \{0\}$ dieses linearen Gleichungssystems, die $\operatorname{ord}_P g \geq m-1$ und dank Proposition 3.3 auch $\operatorname{ord}_O g \geq -m$ erfüllt.

Mit der Summenformel in $\mathbb{Z}$ (Hilfssatz 3.4), und da g als Polynom in U und V Pole nur in O haben kann, können wir somit

$$\operatorname{div}(g) = (m-1) \cdot [P] + 1 \cdot [R] - m \cdot [O] \quad \text{wobei } R \in E(K)$$

[4] wie zum Beispiel in Elliptische Kurven I konstruiert.

notieren (möglicherweise $R = O$). Die Summenformel in $E(K)$ (Hilfssatz 3.10) liefert dann aber

$$O = (m-1)\,P + R - m\,O = (m-1)\,P + R \text{ folglich } P = m\,P + R = R.$$

Es gilt also wie gewünscht $\operatorname{div} g = m \cdot [P] - m \cdot [O]$. □

Bemerkung 3.1. Hier ist $g \in K[U]$ nur möglich, wenn *entweder* $P = O$ ist—dann hat g einen trivialen Divisor und es muss also $g \in K^\star$ liegen—*oder* P genau Ordnung 2 hat und folglich $m = 2\,n$ gilt—wobei dann $g = \eta\,(U - U_0)^n$ ist, mit $\eta \in K^\star$ und $P = (U_0, 0)$.

Ist nämlich $P \neq O$ und $g \in K[U]$ mit (3.1), so gilt (nach Hilfssatz 3.3) $\operatorname{ord}_{-P} g = \operatorname{ord}_P g = m \geq 1$, so dass sowohl P als auch $-P$ echte Nullstellen von g sind. Die Bedingung 3.1 verlangt aber, dass g genau eine Nullstelle hat, so dass $P = -P$ gelten muss.

3.3 Koordinatentransformation

Sei nun $D \in k[X]$ ein quadratfreies Polynom von Grad 4 und sei $\xi \in \overline{k}$ eine der 4 verschiedenen Nullstellen von D. Um die Eigenschaften der Invarianten zu nutzen, konstruieren wir die Transformation im Projektiven. Wir starten mit

$$Y_0{}^2\,Z_0{}^2 = D_0(X_0, Z_0) = a_0\,X_0{}^4 + 4\,a_1\,X_0{}^3\,Z_0 + 6\,a_2\,X_0{}^2\,Z_0{}^2 + 4\,a_3\,X_0\,Z_0{}^3 + a_4\,Z_0{}^4 \quad (\mathcal{C}_0)$$

und führen der Reihe nach folgende Koordinatenwechsel aus, die je eine Gleichung der Form

$$Y_i{}^2\,Z_i{}^2 = D_i(X_i, Z_i) \quad \text{mit } D_i \in \mathbb{B}_4 \qquad (\mathcal{C}_i)$$

ergeben. Die Koordinatenwechsel sind so gewählt, dass D_i jeweils durch eine $\mathbf{SL}(2, \overline{k})$-Matrix in D_{i+1} übergeht.

$X_0 = X_1 + \xi\,Z_1$ $Y_0 = Y_1$ $Z_0 = Z_1$	$\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$	Der Koeffizient von $Z_1{}^4$ in D_1 verschwindet, da ja $D_1(0,1) = D_0(\xi, 1) = D(\xi) = 0$.
$X_1 = Z_2$ $Y_1 = Y_2\;Z_2/X_2$ $Z_1 = X_2$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Nun verschwindet der Koeffizient von $X_2{}^4$ in D_2, da sozusagen X und Z getauscht wurden. Die Transformation des Y ist so gewählt, dass die Form $(\mathcal{C}_i)$ erhalten bleibt.
$X_2 = X_3/\sqrt{\kappa}$ $Y_2 = Y_3/\sqrt{\kappa}$ $Z_2 = Z_3\,\sqrt{\kappa}$	$\begin{pmatrix} \frac{1}{\sqrt{\kappa}} & 0 \\ 0 & \sqrt{\kappa} \end{pmatrix}$	Mit $4\,\kappa$ bezeichnen wir den Koeffizienten[5] von $X_2{}^3\,Z_2$ in D_2. Diese Transformation normiert sozusagen „$\kappa = a_1$“ auf 1 in D_3.
$X_3 = X_4 - \mu\,Z_4$ $Y_3 = Y_4$ $Z_3 = Z_4$	$\begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix}$	Zuletzt sei $12\,\mu$ der Koeffizient von $X_3{}^2\,Z_3{}^2$ in D_3. Mit der Verschiebung um $-\mu$ verschwindet dann $X_4{}^2\,Z_4{}^2$ in D_4.

Nach Anwendung all dieser Transformationen erhalten wir dann die Form

$$Y_4{}^2\, Z_4{}^2 = D_4(X_4, Z_4) = 4\, X_4{}^3\, Z_4 + 4\, a\, X_4\, Z_4{}^3 + 4\, b\, Z_4{}^4.$$

Nun waren aber die Transformationen derart gewählt, dass alle D_i auf einer einzigen Bahn der anfangs definierten $\mathbf{SL}(2, \overline{k})$ Wirkung liegen, so dass sich die Invarianten g_2 und g_3 sicher nicht verändert haben. Werten wir diese auf D_4 aus (mit $a_0 = a_2 = 0$ sowie $a_1 = 1$ ist dies nicht allzu schwer), erhalten wir $g_2 = -4\, a$ und $g_3 = -4\, b$. Mit $U = X_4/Z_4$, $V = Y_4/(2\, Z_4)$ gelangen wir so zu $V^2 = C(U) = U^3 + a\, U + b$ wie in Hauptsatz 3.

Da auch die Diskriminante Δ von D eine Invariante von Grad 6 ist, erhalten wir für die Diskriminante der elliptischen Kurve E

$$\Delta_E = 4^{-6}\, \Delta \neq 0.$$

In affinen Koordinaten sieht die vollständige Transformation zwischen den Funktionenkörpern $\mathcal{F}_\mathcal{C} = \overline{k}(X, Y)$ mit $Y^2 = D(X)$ (wobei $X = X_0/Z_0$, $Y = Y_0/Z_0$) und $\mathcal{F}_E = \overline{k}(U, V)$ mit $V^2 = C(U)$ dann wie folgt aus:

$$U = \mu + \frac{\kappa}{X - \xi}, \qquad 2\, V = \frac{\kappa\, Y}{(X - \xi)^2} \tag{3.2}$$

Dieses schreibt man um zu

$$(U - \mu)(X - \xi) = \kappa, \qquad 2\, V\, (X - \xi) = Y\, (U - \mu) \tag{3.3}$$

und erkennt so, dass die Umkehrabbildung eine ähnliche Form hat.

Wir bezeichnen die Abbildungen mit

$$\tau : \mathcal{F}_E \longrightarrow \mathcal{F}_\mathcal{C} \quad \text{und} \quad \varrho : \mathcal{F}_\mathcal{C} \longrightarrow \mathcal{F}_E.$$

Proposition 3.4. *Sei $p(X) \in \overline{k}[X]$ ein Polynom mit $\deg p \leq n$ und b_0 als Koeffizienten von X^n. Dann gibt es ein Polynom $g(U) \in \overline{k}[U]$ mit $\deg g \leq n$, so dass*

$$\varrho\; p(X) = (U - \mu)^{-n}\, g(U) \tag{3.4}$$

und $g(\mu) = b_0\, \kappa^n$. Weiter gilt $\deg g = n$ genau, wenn $p(\xi) \neq 0$.

Analog für τ, mit U und X sowie μ und ξ vertauscht.

Beweis. Sei

$$h(X_0, Z_0) = Z_0{}^n\, p(X_0/Z_0) = b_0\, X_0{}^n + b_1\, X_0{}^{n-1}\, Z_0 + \cdots + b_{n-1}\, X_0\, Z_0{}^{n-1} + b_n\, Z_0{}^n$$

die homogene Form von p. Von (3.3) haben wir

$$\varrho\, p(X) = \varrho\, h(X, 1) = h\left(\xi + \frac{\kappa}{U - \mu}, 1\right) = (U - \mu)^{-n}\, h\,(\xi\,(U - \mu) + \kappa, U - \mu)$$

vermöge der Homogenität von h und klar ist $g(U) = h\,(\xi\,(U - \mu) + \kappa, U - \mu) \in \overline{k}[U]$. So ist dann $g(\mu) = h(\kappa, 0) = b_0\, \kappa^n$.

Der Koeffizient von U^n in g kommt natürlich von $h(\xi\, U + \ldots, 1\, U + \ldots)$ und ist also $h(\xi, 1) = p(\xi)$ wie gewünscht. □

[5] Wir werden im nächsten Abschnitt $4\,\kappa = D'(\xi)$ berechnen und dabei $\kappa \neq 0$ verifizieren.

3.4 Spezielle Punkte

Aus (3.4) kann man sehen, dass Polynome aus $\mathcal{F}_\mathcal{C}$, welche ja Pole nur im „Unendlichen“ haben, durch die Transformation ϱ in $\mathcal{F}_E$ Pole bei $P_\pm = (\mu, \pm?)$ erhalten. Durch einen formalen Grenzübergang in (3.2) mit $X \to \infty, Y \to \infty$ mit $(X, Y) \in \mathcal{C}$ kommt man genauer zu

$$P_\pm = (\mu, \pm\kappa\,\sqrt{a_0}/2)\,. \tag{3.5}$$

Um zu zeigen, dass der Punkt auf der Kurve E liegt, berechnen wir zunächst einmal κ und μ. Es war $4\,\kappa$ ja der Koeffizient von ${X_2}^3\,Z_2$ in D_2, also ebenfalls der Koeffizient von $X_1\,{Z_1}^3$ in D_1, welches durch Verschiebung um ξ aus D_0 hervorging; insbesondere haben wir $D_1(X, 1) = D_0(X + \xi, 1) = D(X + \xi)$. Nach der Taylorentwicklungsformel gilt dann $4\,\kappa = D'(\xi)$. Da D quadratfrei ist und ξ bereits Nullstelle von D ist, gilt somit $\kappa \neq 0$.

Hingegen war $12\,\mu$ der Koeffizient von ${X_3}^2\,{Z_3}^2$ in D_3, welcher dem Koeffizienten von ${X_2}^2\,{Z_2}^2$ in D_2 entspricht; aber dieser ist auch der Koeffizient von ${X_1}^2\,{Z_1}^2$ in D_1, und mit der Taylorentwicklungsformel finden wir $12\,\mu = D''(\xi)/2$ ähnlich wie bei κ. Konkreter haben wir

$$\kappa = a_0\,\xi^3 + 3\,a_1\,\xi^2 + 3\,a_2\,\xi + a_3, \qquad \mu = (a_0\,\xi^2 + 2\,a_1\,\xi + a_2)/2. \tag{3.6}$$

Die vollständige Taylorentwicklung von D bei ξ hat die Form:

$$D(\xi + X) = 0 + 4\,\kappa\,X + 6 \cdot 2\,\mu\,X^2 + 4\,\lambda\,X^3 + a_0\,X^4 \tag{3.7}$$

und mit der Translationsinvarianz der Invarianten g_2 und g_3 vereinfachen sich die Rechnungen dann zu

$$\mu^3 + a\,\mu + b = \mu^3 - \left(3\,\mu^2 - \kappa\,\lambda + 0\right)\,\mu - \left(-2\,\mu^3 + \lambda\,\mu\,\kappa + 0 - a_0\,\kappa^2/4 - 0\right) = a_0\,\kappa^2/4,$$

so dass $P_\pm$ tatsächlich auf E liegt.

Die Punkte $P_\pm$ hängen aber noch stark von der Wahl von ξ ab, es gibt also insgesamt vier Möglichkeiten für $P_\pm$. Auf einer elliptischen Kurve ist es natürlich, durch Addieren der Punkte W mit $2\,W = O$ aus einem Punkte vier zu machen; genau so ist die Situation hier. Berechnet man $2\,P_\pm = Q_\mp$, so findet man $Q_\pm = (u, \pm v)$ unabhängig von ξ wie in Hauptsatz 3.

Dazu muss man z.B. für P_+

$$m = \frac{3\,\mu^2 + a}{\kappa\,\sqrt{a_0}}, \qquad u = m^2 - 2\,\mu, \qquad -v = -\left(m(u - \mu) + \kappa\,\sqrt{a_0}/2\right)$$

überprüfen. Damit dies nicht zu unangenehm wird, gehen wir wieder direkt von (3.7) und benutzen, dass die Semiinvarianten s_1, s_2, s_3 ebenfalls translationsinvariant sind:

$$\begin{aligned}
m &= \frac{3\,\mu^2 - 3\,\mu^2 + \kappa\,\lambda}{\kappa\,\sqrt{a_0}} = \frac{\lambda}{\sqrt{a_0}},\\
u &= \frac{\lambda^2}{a_0} - 2\,\mu = \frac{\lambda^2 - 2\,a_0\,\mu}{a_0} = \frac{s_2}{s_1},\\
v &= \frac{\lambda}{\sqrt{a_0}}\,\frac{\lambda^2 - 3\,a_0\,\mu}{a_0} + \frac{\kappa\,\sqrt{a_0}}{2} = \frac{2\,\lambda^3 - 6\,a_0\,\mu\,\lambda + {a_0}^2\,\kappa}{2\,{a_0}^{3/2}} = \frac{s_3}{2\,{s_1}^{3/2}}.
\end{aligned}$$

Also hat man $2\,P_+ = Q_-$ wie gewünscht und $P_\pm$ und $Q_\pm$ können nur gleichzeitig von endlicher Ordnung sein.

3.5 Pell und Torsionspunkte

Satz 3.2. *Die Pellsche Gleichung* ($\mathrm{P}^\star$) *hat genau dann eine nicht-triviale Lösung* (p,q) *in* $\overline{k}[X]$ *mit* $\deg p = n \geq 1$*, wenn es* $g_\pm \in \overline{k}[U,V] \subset \mathcal{F}_E$ *gibt mit*

$$\operatorname{div}(g_\pm) = 2n \cdot [P_\pm] - 2n \cdot [O]. \tag{3.8}$$

Beweis. Nehmen wir zunächst die Existenz einer nicht-trivialen Lösung (p,q) der Pellschen Gleichung an. Seien b_0 und c_0 die Leitkoeffizienten von p und q. Von $p^2 - D\,q^2 = \eta \in \overline{k}^\star$ und $q \neq 0$ schließt man sofort $n = \deg p = \deg q + \frac{1}{2}\deg D = \deg q + 2 \geq 2$. Ebenso schließt man ${b_0}^2 = a_0\,{c_0}^2$, also $b_0 = \pm\sqrt{a_0}\,c_0$.

Setzen wir $\phi_\pm = p(X) \pm Y\,q(X)$, so erhalten wir von Proposition 3.4

$$f_\pm = \varrho\,\phi_\pm = \frac{r(U)}{(U-\mu)^n} \pm \frac{2\,\kappa\,V}{(U-\mu)^2}\,\frac{s(U)}{(U-\mu)^{n-2}} = \frac{g_\pm}{(U-\mu)^n} \tag{3.9}$$

wobei $g_\pm = r(U) \pm 2\,\kappa\,V\,s(U)$.

Aus $\phi_+\,\phi_- = \eta = \varrho\,(\eta) = f_+\,f_-$ und

$$\operatorname{div}(U-\mu) = [P_+] + [P_-] - 2\cdot[O]$$

folgern wir nun $g_+\,g_- = \eta\,(U-\mu)^{2n}$ und

$$\operatorname{div}(g_+\,g_-) = 2n\cdot[P_+] + 2n\cdot[P_-] - 4n\cdot[O].$$

Da klar $g_\pm \in \overline{k}[U,V]$, hat $g_\pm$ Pole nur in O (Hilfssatz 3.1) und damit kann $g_\pm$ keine Nullstellen außer $P_\pm$ haben. Dank

$$g_+(P_\pm) = r(\mu) \pm 2\,\kappa\,\frac{\kappa\sqrt{a_0}}{2}\,s(\mu) = \kappa^n\,b_0 \pm \kappa^n\,\sqrt{a_0}\,c_0 = \kappa^n(b_0 \pm \sqrt{a_0}\,c_0)$$

trifft aber nur genau eines von $g_+(P_+) = 0$ und $g_+(P_-) = 0$ zu. Ohne Einschränkung sei $g_+(P_+) = 0$, so dass (wieder Hilfssatz 3.1) folgt

$$\operatorname{div}(g_+) = 2n\cdot[P_+] - 2n\cdot[O] \quad \text{und} \quad \operatorname{div}(g_-) = 2n\cdot[P_-] - 2n\cdot[O].$$

So wäre $g_\pm$ mit dem gewünschten Divisor gefunden.

Für die Gegenrichtung erfülle $g_\pm = r(U) \pm V\,s(U)$ mit $r, s \in \overline{k}[U]$ die Bedingung (3.8). Da $\kappa\sqrt{a_0}/2 \neq 0$, ist nach Bemerkung 3.1 hier $s = 0$ nicht möglich.

Nun hat man

$$\operatorname{div}(g_+\,g_-) = 2n\cdot[P_+] + 2n\cdot[P_-] - 4n\cdot[O],$$

folglich ist $g_+\,g_- = \eta\,(U-\mu)^{2n}$ für $\eta \in \overline{k}^\star$ (wegen Hilfssatz 3.5 mit $f = g_+\,g_-/(U-\mu)^{2n}$).

Weiter garantiert Proposition 3.3 $\deg r \leq n$ und $\deg s \leq n-2$, so dass wir durch Proposition 3.4 p und $\tilde{q}$ finden können, mit

$$\tau\,g_\pm = \frac{p(X)}{(X-\xi)^n} \pm \frac{\kappa\,Y}{2\,(X-\xi)^2}\,\frac{\tilde{q}(X)}{(X-\xi)^{n-2}} = \frac{p(X) \pm Y\,\kappa\,\tilde{q}(X)/2}{(X-\xi)^n}. \tag{3.10}$$

Setzen wir $q(X) = \kappa\,\tilde{q}(X)/2$ und nutzen $(X-\xi)(U-\mu) = \kappa$, so folgt

$$p^2 - Dq^2 = (X-\xi)^{2n}\,\tau\,(g_+\,g_-) = \eta\,\kappa^{2n} \in \overline{k}^\star\,.$$

Nach Proposition 3.4 reicht es nun aus, $r(\mu) \neq 0$ und $s(\mu) \neq 0$ zu zeigen, um $\deg p = n$ und $\deg q = n-2$ (und so insbesondere $q \neq 0$) zu erhalten.

Von Hilfssatz 3.1 wissen wir bereits, dass $g_+(P_+) = r(\mu) + v_0\,s(\mu) = 0$ gilt, wobei $v_0 = \frac{\kappa\sqrt{a_0}}{2} \neq 0$. Somit können $r(\mu)$ und $s(\mu)$ nur gleichzeitig 0 sein.

Wäre aber $s(\mu) = 0$, so wäre ja $g_+(P_+) = g_+(P_-) = 0$, und g_+ hätte auch in P_- eine Nullstelle—im Widerspruch mit der Voraussetzung (3.8). Also ist die (p,q) die gesuchte nicht-triviale Lösung von $(\mathrm{P}^\star)$ in $\overline{k}[X]$ mit $\deg p = n$. □

Beweis von Hauptsatz 3. Die Existenz von $g_\pm$ mit (3.8) stellt das Bindeglied zwischen Satz 3.1 und Satz 3.2 dar. Damit ist die Existenz einer nicht-trivialen Lösung von $(\mathrm{P}^\star)$ in $\overline{k}[X]$ vermöge $Q_\mp = 2\,P_\pm$ (siehe Abschnitt 3.4) äquivalent mit $n\,Q_\mp = 2n\,P_\pm = O$, und man bekommt außerdem die Bedingung an $\deg p$.

Mit Satz 2.2 können wir dann von einer Lösung in $R' = \overline{k}[X]$ zu einer Lösung in $R = k[X]$ übergehen, da $\sqrt{a_0} \in k$ ja hinreichend (und notwendig) für $\sqrt{D} \in k((X^{-1}))$ ist. □

4 Elementare Integrierbarkeit

Mit den Resultaten des vorhergehenden Kapitels können wir auch die elementare Integrierbarkeit (siehe unten) elliptischer Integrale mit der Pellschen Gleichung verknüpfen:

Hauptsatz 4. *Sei k ein Körper von Charakteristik 0, sei $R = k[X]$, sowie $D \in R$ quadratfrei von Grad 4, so dass der Leitkoeffizient ein Quadrat in k ist.*

Dann gibt es genau dann *ein $f \in k[X] \setminus \{0\}$ mit $\deg f \leq 2$, so dass $f/\sqrt{D}$ elementar integrierbar ist,* wenn *die Pellsche Gleichung $(\mathrm{P}^\star)$ eine nicht-triviale Lösung über R hat.*

Falls ein solches f existiert, muss $\deg f = 1$ gelten, und es gibt $c \in k^\star$, $\phi \in k[X, \sqrt{D}]$ mit

$$\frac{f}{\sqrt{D}} = c\,\frac{1}{\phi}\,\frac{\mathrm{d}\phi}{\mathrm{d}X}\,. \tag{4.1}$$

4.1 Ableitungen

Definition 4.1. Sei $\mathcal{K}$ ein Körper. Eine $\mathbb{Z}$-lineare Abbildung $\partial : \mathcal{K} \longrightarrow \mathcal{K}$ heißt *Ableitung* auf $\mathcal{K}$, wenn sie die *Leibnizregel*

$$\partial\,(\phi \cdot \psi) = \psi\;\partial\phi + \phi\;\partial\psi \qquad \text{für alle } \phi, \psi \in \mathcal{K}$$

erfüllt, so dass die *logarithmische Ableitung* $\partial\log\phi = \partial\phi/\phi$, definiert für $\phi \in \mathcal{K}^\star$, der Gleichung

$$\partial\log\,(\phi \cdot \psi) = \partial\log\phi + \partial\log\psi \qquad \text{für alle } \phi, \psi \in \mathcal{K}^\star$$

genügt.

Nun bildet $k = \{\phi \in \mathcal{K} \mid \partial\phi = 0\}$ einen Körper, den sogenannten *Konstantenkörper* und ∂ ist dann durch die Leibnizregel automatisch eine k-lineare Abbildung.[1]

Von nun an nehmen wir stets Charakteristik 0 an.

Definition 4.2. Wir sagen, $\alpha \in \mathcal{K}$ sei *elementar integrierbar* bezüglich ∂, falls es $\psi \in \mathcal{K}$, $c_i \in k$, $\phi_i \in \mathcal{K}^\star$ $(i = 1, \ldots, l)$ gibt, so dass

$$\alpha = \partial\psi + \sum_{i=1}^{l} c_i\,\partial\log\phi_i \tag{4.2}$$

gilt.

[1] Aus der $\mathbb{Z}$-Linearität und der Leibnizregel geht direkt hervor, dass Summe und Produkt von zwei Konstanten ebenfalls konstant sind. Sicher ist auch 0 eine Konstante und wegen $\partial 1 = \partial\,(\pm 1 \cdot \pm 1) = \partial\,(\pm 1) \cdot \pm 1 + \pm 1 \cdot \partial\,(\pm 1)$ muss 1, und dann auch -1 konstant sein. Also sind auch die Negativen Konstanten; und für die Inversen von Konstanten hat man $0 = \partial 1 = \partial\left(\phi \cdot \phi^{-1}\right) = \phi\,\partial\left(\phi^{-1}\right)$, so dass diese ebenfalls Konstanten sind. Damit ist k ein Unterkörper von $\mathcal{K}$.

Bemerkung 4.1. Diese Definition ist nicht die Standard-Definition, aber nach dem Satz von Liouville[2] äquivalent mit derselben, jedenfalls solange man wie hier über Charakteristik 0 arbeitet.

Proposition 4.1. *Falls $\alpha \in \mathcal{K}$ elementar integrierbar bezüglich ∂ ist, so gibt es $\psi \in \mathcal{K}$, $c_i \in k$, $\phi_i \in \mathcal{K}^\star$ $(i = 1, \ldots, l)$ mit* (4.2) *und den c_i $\mathbb{Q}$-linear unabhängig.*

Beweis. Angenommen, die c_i sind $\mathbb{Q}$-linear abhängig, und wir können

$$c_l = (n_1\, c_1 + \cdots + n_{l-1}\, c_{l-1})\,/m \quad \text{mit } n_i, m \in \mathbb{Z}$$

schreiben. Dann haben wir mit $\tilde{c}_i = c_i/m$

$$\sum_{i=1}^{l} c_i\, \partial \log \phi_i = \sum_{i=1}^{l-1} \tilde{c}_i\, \partial \log\, ({\phi_i}^m\, {\phi_l}^{n_i})$$

so dass wir die Anzahl l der Summanden solange reduzieren können, bis die c_i wie gewünscht $\mathbb{Q}$-linear unabhängig sind. □

Sei nun k ein Körper von Charakteristik 0, und $D \in k[X]$ wie in Hauptsatz 4, so dass $\mathcal{F}_\mathcal{C} = k(X, Y)$ mit $Y^2 = D(X)$ eine quadratische Erweiterung von $k(X)$ ist.

Auf $k[X]$—und durch die Leibnizregel dann auch auf $k(X)$—ist die übliche Ableitung von Polynomen durch $\partial_X a = 0$ für $a \in k$ und $\partial_X X = 1$ definiert, d.h. $\partial_X = \frac{\mathrm{d}}{\mathrm{d}X}$. Mit der Leibnizregel lässt sich diese Erweiterung eindeutig nach $k(X, Y)$ fortsetzen, in der Tat haben wir

$$\frac{\partial_X Y}{Y} = \partial_X \log Y = \frac{1}{2} \partial_X \log D(X) = \frac{1}{2} \frac{\partial_X D(X)}{D(X)}. \tag{4.3}$$

Ähnlich haben wir eine Ableitung $\partial_U = \frac{\mathrm{d}}{\mathrm{d}U}$ auf $\mathcal{F}_E = k(U, V)$ wo $V^2 = C(U)$ wie in Abschnitt 3.3.

Proposition 4.2 („Kettenregel“)**.** *Sei $\mathcal{K}$ ein Körper mit Ableitung ∂, wo der Konstantenkörper ebenfalls k umfasse. Sei außerdem $\lambda : \mathcal{F}_E \longrightarrow \mathcal{K}$ ein injektiver k-Homomorphismus. Dann gilt:*

$$\partial\lambda(\phi) = \lambda\left(\partial_U \phi\right) \cdot \partial\lambda(U) \quad \textit{für alle } \phi \in \mathcal{F}_E. \tag{4.4}$$

Beweis. Als erstes bemerken wir, dass auf der linken und der rechten Seite k-lineare Abbildungen in ϕ stehen, die einer Variation der Leibnizregel genügen:

$$\begin{gathered} \partial\lambda(\phi \cdot \psi) = \lambda(\psi)\, \partial\lambda(\phi) + \lambda(\phi)\, \partial\lambda(\psi), \\ \lambda\left(\partial_U\, (\phi \cdot \psi)\right) \cdot \partial\lambda(U) = \lambda(\psi) \cdot \lambda\left(\partial_U \phi\right) \cdot \partial\lambda(U) + \lambda(\phi) \cdot \lambda\left(\partial_U \psi\right) \cdot \partial\lambda(U). \end{gathered}$$

Die Differenz $H(\phi) = \partial\lambda(\phi) - \lambda\left(\partial_U \phi\right) \cdot \partial\lambda(U)$ erfüllt dieses Gesetz dann ebenso:

$$H(\phi \cdot \psi) = \lambda(\psi) \cdot H(\phi) + \lambda(\phi) \cdot H(\psi).$$

[2] siehe zum Beispiel [4], S. 157

Außerdem ist H auch k-linear. Daraus bekommen wir für Inverse die übliche Formel $H\left(\phi^{-1}\right) = -H(\phi)/\lambda\left(\phi^2\right)$, die dank λ injektiv wohldefiniert ist.

Da $H(\phi) = 0$ für alle $\phi \in k$ gilt, reicht es nun, $H(U) = 0$ und $H(V) = 0$ zu überprüfen. Offensichtlich ist $H(U) = 0$ wegen $\partial_U U = 1$ erfüllt.

Wir folgern also $0 = H(C(U)) = H(V^2) = 2\,\lambda(V)\,H(V)$ und erhalten mit λ injektiv $H(V) = 0$ wie gewünscht. □

Bemerkung 4.2. Wir bekommen eine analoge Formel für die logarithmische Ableitung:

$$\partial\log\lambda(\phi) = \frac{\partial\lambda(\phi)}{\lambda(\phi)} = \lambda\left(\frac{\partial_U\phi}{\phi}\right)\cdot\partial\lambda(U) = \lambda\left(\partial_U\log\phi\right)\cdot\partial\lambda(U) \quad \text{für alle } \phi \in {\mathcal{F}_E}^\star\,. \tag{4.5}$$

4.2 Konstruktion elementarer Integrale

Wir zeigen zuerst, wie wir aus Lösungen der Pellschen Gleichung elementar integrierbare Funktionen basteln:

Proposition 4.3. *Sei $D \in k[X]$ quadratfrei von beliebigem Grad, sei $Y^2 = D(X)$ und sei $(p, q) \in k[X]^2$ eine nicht-triviale Lösung von $(\mathrm{P}^\star)$. Dann liegt $f = \partial_X p/q \in k[X]$ und es gilt:*

$$\frac{f}{Y} = \partial_X\log\left(p + Y\,q\right), \tag{4.6}$$

also ist f/Y elementar integrierbar.

Beweis. Wegen $p^2 - D\,q^2 = \eta \in k$ haben wir

$$0 = \partial_X\left(p^2 - D\,q^2\right) = 2\,p\,\partial_X p - 2\,D\,q\,\partial_X q - q^2\,\partial_X D,$$

so dass $q \mid 2\,p\,\partial_X p$ in $k[X]$. Da p und q teilerfremd sind, gilt dann $q \mid \partial_X p$.

Weiter berechnen wir mit $\partial_X\left(-Y\right) = -\partial_X Y$ die Spur

$$\partial_X\log\left(p + Y\,q\right) + \partial_X\log\left(p - Y\,q\right) = \partial_X\log\eta = 0,$$

so dass $f := Y\,\partial_X\log\left(p + Y\,q\right) \in k(X)$ liegen muss. Eine bessere Formel für f berechnen wir aus

$$f\cdot\left(p + Y\,q\right) = Y\,\partial_X\left(p + Y\,q\right) = Y\,\partial_X p + \tfrac{1}{2}\,q\,\partial_X D + D\,\partial_X q.$$

Wir bekommen sofort $f\,q = \partial_X p$ und folglich $f \in k[X]$ wie gewünscht. □

Bemerkung 4.3. Für $q \neq 0$ ist wie in Proposition 1.1 $\deg p - \deg q = \frac{1}{2}\deg D$, so dass immer $\deg f = \deg p - 1 - \deg q = \frac{1}{2}\left(\deg D - 2\right)$ gilt. Für $\deg D = 4$ ist also stets $\deg f = 1$.

Bemerkung 4.4. Die Bedingung $\deg f \leq 2$ ist in Hauptsatz 4 natürlich notwendig, da ja $\partial_X D$ genau Grad 3 hat und

$$\frac{\partial_X D}{\sqrt{D}} = 2\,\partial_X\left(\sqrt{D}\right)$$

offensichtlich elementar integrierbar ist.

4.3 Ableitung unter Transformation

Wir hatten ja für D quadratfrei von Grad 4 einen k-Isomorphismus $\tau : \mathcal{F}_E \longrightarrow \mathcal{F}_\mathcal{C}$ konstruiert (siehe Abschnitt 3.3). Wir beschreiben nun, wie sich die elementare Integrierbarkeit unter dieser Transformation verhält.

Proposition 4.4. *Es gibt genau dann $f \in k[X]\backslash\{0\}$ mit $\deg f \leq n$, so dass $\alpha = f(X)/Y$ bezüglich ∂_X elementar integrierbar ist, wenn es $g \in k[U] \setminus \{0\}$ mit $\deg g \leq n$ gibt, so dass $\tilde{\alpha} = g(X)/\left((U-\mu)^n\, V\right)$ bezüglich ∂_U elementar integrierbar ist.*

Beweis. Wir gehen aus von Integral mit $\alpha = f(X)/Y$ elementar integrierbar, wobei $f \in k[X]$, also

$$\frac{f(X)}{Y} = \partial_X \psi + \sum_{i=1}^{l} c_i\, \partial_X \log \phi_i \tag{4.7}$$

mit $\psi, \phi_i \in \mathcal{F}_\mathcal{C}$. Schreiben wir $f = \tau(\tilde{f}), \psi = \tau(\tilde{\psi}), \phi_i = \tau(\tilde{\phi}_i)$, so lautet die Gleichung (mit (3.3), Proposition 4.2 und Bemerkung 4.2) nun

$$\tau\left(\frac{\tilde{f}(U)}{V}\,\frac{(U-\mu)^2}{2\,\kappa}\right) = \tau\left(\partial_U \tilde{\psi}\right)\ \partial_X \tau(U) + \sum_{i=1}^{l} c_i\, \tau\left(\partial_U \log \tilde{\phi}_i\right)\ \partial_X \tau(U).$$

Wir berechnen nun aus (3.3)

$$\partial_X \tau(U) = \partial_X\left(\mu + \frac{\kappa}{X-\xi}\right) = -\frac{\kappa}{(X-\xi)^2} = \tau\left(-\frac{(U-\mu)^2}{\kappa}\right),$$

so dass wir mit $g(U) = -(U-\mu)^n\, \tilde{f}(U)/2$ nach Entfernen von τ die Gleichung

$$\frac{g(U)}{(U-\mu)^n\, V} = \partial_U \tilde{\psi} + \sum_{i=1}^{l} c_i\, \partial_U \log \tilde{\phi}_i \tag{4.8}$$

bekommen, mit $\tilde{\psi}, \tilde{\phi}_i \in \mathcal{F}_E$. Dabei ist wegen Proposition 3.4 $g(U) \in k[U]$, falls $f \in k[X]$ Grad $\leq n$ hat.

Ähnlich zeigt man die Rückrichtung. □

4.4 Ableitung und Ordnungen

Der Funktionenkörper $\mathcal{F}_E$ der Elliptischen Kurve E kommt mit einer Reihe von Ordnungen $\mathrm{ord}_P : \mathcal{F}_E \to \mathbb{Z} \cup \{\infty\}$ für $P \in E(\overline{k})$, wobei $\mathrm{ord}_P\, \phi = \infty$ genau wenn $\phi = 0$. Wir wollen nun untersuchen, was die Beziehung zwischen $\mathrm{ord}_P\, \phi$ und $\mathrm{ord}_P\, \partial\phi$ für $\phi \in \mathcal{F}_E \setminus k$ ist. Dazu nutzen wir, dass wir injektive k-Homomorphismen $\lambda_P : \mathcal{F}_E \longrightarrow k((t))$ haben, mit $\mathrm{ord}_P\, \phi = \mathrm{ord}_{t=0}\, \lambda_P(\phi)$, wobei $k((t))$ den Körper der Laurentreihen in t bezeichnet, dessen Elemente die Form $a_N\, t^N + a_{N+1}\, t^{N+1} + \ldots$ haben.

Wir wollen zunächst verstehen, wie sich $\mathrm{ord}_{t=0}$ beim Ableiten ∂_t nach t verhält.

Proposition 4.5. *Sei* $\psi \in k((t))^\star$ *mit* $\operatorname{ord}_{t=0}\psi = N$.

- *Falls* $N \neq 0$, *so gilt* $\operatorname{ord}_{t=0}\partial_t\psi = N-1$ *und folglich* $\operatorname{ord}_{t=0}\partial_t\log\psi = -1$.
- *Falls* $N = 0$ *ist, folgt immerhin* $\operatorname{ord}_{t=0}\partial_t\psi = \operatorname{ord}_{t=0}\partial_t\log\psi \geq 0$.
- *Insbesondere hat man die Form* $\partial_t\log\psi = N\,t^{-1} + \dots$

Beweis. Schreiben wir

$$\psi = \sum_{n=N}^{+\infty} a_n\,t^n = a_N\,t^N + \dots \qquad \text{mit } a_N \neq 0$$

und also

$$\partial_t\psi = \sum_{n=N}^{+\infty} n\,a_n\,t^{n-1} = N\,a_N\,t^{N-1} + \dots$$

und folglich $\operatorname{ord}_{t=0}\partial_t\psi = N-1$ wenn $N \neq 0$ und immerhin ≥ 0 wenn $N = 0$. Die Ordnung der logarithmischen Ableitungen folgt sofort; außerdem hat man (mit der üblichen Division von Laurentreihen)

$$\partial_t\log\psi = \frac{\partial_t\psi}{\psi} = \frac{N\,a_N\,t^{N-1} + \dots}{a_N\,t^N + \dots} = N\,t^{-1} + \dots$$

wie gewünscht. □

Proposition 4.6. *Seien* $c_i \in k, \psi_i \in k((t))^\star$ $(i = 1, \dots, l)$ *mit den* c_i $\mathbb{Q}$*-linear unabhängig und den* $\operatorname{ord}_{t=0}\psi_i$ *nicht alle* 0. *Dann ist*

$$\operatorname{ord}_{t=0}\left(\sum_{i=1}^{l} c_i\,\partial_t\log\psi_i\right) = -1.$$

Beweis. Seien $N_i = \operatorname{ord}_{t=0}\psi_i \in \mathbb{Z}$ $(i = 1, \dots, l)$ nicht alle 0. So haben wir

$$\sum_{i=1}^{l} c_i\,\partial_t\log\psi_i = \sum_{i=1}^{l} c_i\,N_i\,t^{-1} + \dots = \left(\sum_{i=1}^{l} c_i\,N_i\right)t^{-1} + \dots.$$

Da nach Voraussetzung die c_i $\mathbb{Q}$-linear unabhängig sind, kann der Koeffizient von t^{-1} nicht verschwinden, so dass die Summe Ordnung -1 haben muss. □

Proposition 4.7. *Sei* $\phi \in \mathcal{F}_E{}^\star$ *und* $P \in E(\overline{k})$. *Ist* $\operatorname{ord}_P\phi = 0$, *so gilt*

$$\operatorname{ord}_P\partial_U\phi \geq -\operatorname{ord}_{t=0}\partial_t\lambda_P(U).$$

Ist aber $\operatorname{ord}_P\phi \neq 0$, *so gilt sogar*

$$\operatorname{ord}_P\partial_U\phi = -\operatorname{ord}_{t=0}\partial_t\lambda_P(U) + \operatorname{ord}_P\phi - 1.$$

Beweis. Mit Proposition 4.2 erhalten wir

$$\partial_t \lambda_P(\phi) = \lambda_P(\partial_U \phi)\, \partial_t \lambda_P(U) \tag{4.9}$$

und so

$$\operatorname{ord}_{t=0} \partial_t \lambda_P(\phi) = \operatorname{ord}_{t=0} \lambda_P(\partial_U \phi) + \operatorname{ord}_{t=0} \partial_t \lambda_P(U).$$

Ist nun $\operatorname{ord}_{t=0} \lambda_P(\phi) = \operatorname{ord}_P \phi = 0$, so ist $\operatorname{ord}_{t=0} \partial_t \lambda_P(\phi) \geq 0$ und es folgt aus Proposition 4.5

$$\operatorname{ord}_P \partial_U \phi \geq -\operatorname{ord}_{t=0} \partial_t \lambda_P(U).$$

Ist hingegen $\operatorname{ord}_P \phi \neq 0$, so gilt $\operatorname{ord}_{t=0} \partial_t \lambda_P(\phi) = \operatorname{ord}_{t=0} \lambda_P(\phi) - 1$ und wir bekommen

$$\operatorname{ord}_P \partial_U \phi = -\operatorname{ord}_{t=0} \partial_t \lambda_P(U) + \operatorname{ord}_P \phi - 1. \qquad \square$$

Wir notieren hier mit P_1, P_2, P_3 die drei Punkte von Ordnung 2 auf $E(\overline{k})$.

Proposition 4.8. *Sei $P \in E(\overline{k})$. Dann gilt:*

$$\operatorname{ord}_{t=0} \partial_t \lambda_P(U) = \begin{cases} -3, & P = O \\ 1, & P = P_j \\ 0, & \textit{sonst} \end{cases}.$$

Beweis. Sei zunächst $P \neq O$, so dass $P = (u_0, v_0) \in k^2$. So haben wir

$$\operatorname{div}(U - u_0) = [P] + [-P] - 2 \cdot [O].$$

Für $P \neq -P$ ist dann $\operatorname{ord}_{t=0} \lambda_P(U - u_0) = \operatorname{ord}_P(U - u_0) = 1$ und für $P = -P = P_j$ ist es 2. Außerdem ist $\operatorname{ord}_{t=0} \lambda_O(U - u_0) = \operatorname{ord}_O(U - u_0) = -2$. Mit $\partial_t \lambda_P(U - u_0) = \partial_t \lambda_P(U)$ erhalten wir dann mit Proposition 4.5 die gewünschte Ordnung für $\partial_t \lambda_P(U)$ in allen drei Fällen. $\square$

Korollar 4.1. *Sei $\phi \in {\mathcal{F}_E}^\star$ und sei $P \in E(\overline{k})$ mit $\operatorname{ord}_P \phi = 0$. Dann gilt:*

$$\operatorname{ord}_P \partial_U \phi \geq \left\{ \begin{array}{ll} 3, & P = O \\ -1, & P = P_j \\ 0, & \textit{sonst} \end{array} \right\}, \quad \operatorname{ord}_P \partial_U \phi = \operatorname{ord}_P \partial_U \log \phi.$$

Ist dagegen $P \in E(\overline{k})$ mit $\operatorname{ord}_P \phi \neq 0$, so gilt:

$$\operatorname{ord}_P \partial_U \phi = \left\{ \begin{array}{ll} \operatorname{ord}_P \phi + 2, & P = O \\ \operatorname{ord}_P \phi - 2, & P = P_j \\ \operatorname{ord}_P \phi - 1, & \textit{sonst} \end{array} \right\}, \quad \operatorname{ord}_P \partial_U \log \phi = \begin{cases} 2, & P = O \\ -2, & P = P_j \\ -1, & \textit{sonst} \end{cases}$$

Bemerkung 4.5. Aus dem Korollar folgt nun, dass $\operatorname{ord}_O \partial_U \phi = 2$, $\operatorname{ord}_{P_j} \partial_U \phi = -2$ sowie $\operatorname{ord}_P \partial_U \phi = -1$ für $P \neq O, P_j$ unmöglich sind – diese Ordnungen sind für die logarithmische Ableitung „reserviert“ und zeigen an, dass ϕ einen Pol oder eine Nullstelle am betreffenden Punkt hat.

Proposition 4.9. *Seien $c_i \in k, \phi_i \in \mathcal{F}_E{}^\star$ $(i = 1, \dots, l)$ mit den c_i $\mathbb{Q}$-linear unabhängig. Sei weiter $P \in E(\overline{k})$. Sind die* $\operatorname{ord}_P \phi_i$ *nicht alle* 0*, so gilt*

$$\operatorname{ord}_P \left(\sum_{i=1}^{l} c_i \, \partial_U \log \phi_i \right) = \begin{cases} 2, & P = O \\ -2, & P = P_j \\ -1, & \textit{sonst} \end{cases}.$$

Beweis. Aus (4.9) haben wir ja

$$\lambda_P \left(\frac{\partial_U \phi_i}{\phi_i} \right) = \frac{\partial_t \lambda_P(\phi_i)}{\lambda_P(\phi_i)} \, \frac{1}{\partial_t \lambda_P(U)}.$$

Mit $\psi_i = \lambda_P \phi_i$ und $\operatorname{ord}_{t=0} \psi_i = \operatorname{ord}_P \phi_i$ haben wir mit Proposition 4.6 wie gewünscht

$$\begin{aligned} \operatorname{ord}_P \left(\sum_{i=1}^{l} c_i \, \partial_U \log \phi_i \right) &= \operatorname{ord}_{t=0} \left(\sum_{i=1}^{l} c_i \, \partial_t \log \psi_i \right) - \operatorname{ord}_{t=0} \partial_t \lambda_P(U) \\ &= -1 - \operatorname{ord}_{t=0} \partial_t \lambda_P(U) = -1 - \begin{cases} -3, & P = O \\ 1, & P = P_j \\ 0, & \text{sonst} \end{cases} \end{aligned}$$

□

4.5 Spiel mit den Ordnungen

Wir erinnern $P_\pm = (\mu, \pm ?)$ aus Abschnitt 3.4, mit $2\,P_\pm \neq O$. Außerdem notieren wir wieder mit P_1, P_2, P_3 die drei Punkte von Ordnung 2.

Proposition 4.10. *Sei $g \in k[U] \setminus \{0\}$ mit $\deg g \leq 2$. Seien weiter $\psi \in \mathcal{F}_E$, $c_i \in k$, $\phi_i \in \mathcal{F}_E{}^\star$ $(i = 1, \dots, l)$ wobei die c_i $\mathbb{Q}$-linear unabhängig seien, mit*

$$\frac{g(U)}{(U-\mu)^2 \, V} = \partial_U \psi + \sum_{i=1}^{l} c_i \, \partial_U \log \phi_i. \tag{4.10}$$

Dann gilt für $i = 1, \dots, l$

$$\operatorname{div} \phi_i = m_i \cdot [P_+] - m_i \cdot [P_-] \tag{4.11}$$

mit $m_i \in \mathbb{Z}$ und $m_i \neq 0$ für mindestens ein i.

Beweis. Wir notieren die linke Seite von (4.10) als A und finden als Divisor

$$\operatorname{div} A = [Q_1] + [Q_2] + [Q_3] + [Q_4] + 3 \cdot [O] - 2 \cdot [P_+] - 2 \cdot [P_-] - [P_1] - [P_2] - [P_3]$$

wobei die $Q_i \in E(\overline{k})$ liegen (möglicherweise auch $Q_i = O$), so dass wir

$$\operatorname{ord}_O A \geq 3, \qquad \operatorname{ord}_{P_\pm} A \geq -2, \qquad \operatorname{ord}_{P_j} A \geq -1, \qquad \operatorname{ord}_P A \geq 0$$

bekommen, wobei mit P alle übrigen Punkte gemeint sind.

Notieren wir weiter $L_i = c_i\,\partial_U \log \phi_i$, so haben wir mit Korollar 4.1, solange $L_i \neq 0$

$$\operatorname{ord}_O L_i \geq 2, \qquad \operatorname{ord}_{P_\pm} L_i \geq -1, \qquad \operatorname{ord}_{P_j} L_i \geq -2, \qquad \operatorname{ord}_P L_i \geq -1.$$

Mit der ultrametrischen Ungleichung folgern wir dann (sogar wenn alle $L_i = 0$ sind) für $B = \partial_U \psi$, solange $B \neq 0$

$$\operatorname{ord}_O B \geq 2, \qquad \operatorname{ord}_{P_\pm} B \geq -2, \qquad \operatorname{ord}_{P_j} B \geq -2, \qquad \operatorname{ord}_P B \geq -1.$$

Mit Bemerkung 4.5 verbessert man diese sofort zu

$$\operatorname{ord}_O B \geq 3, \qquad \operatorname{ord}_{P_\pm} B \geq -2, \qquad \operatorname{ord}_{P_j} B \geq -1, \qquad \operatorname{ord}_P B \geq 0$$

und erhält dann mit Korollar 4.1

$$\operatorname{ord}_O \psi \geq 0, \qquad \operatorname{ord}_{P_\pm} \psi \geq -1, \qquad \operatorname{ord}_{P_j} \psi \geq 0, \qquad \operatorname{ord}_P \psi \geq 0.$$

Da somit $\psi \cdot (U - \mu)$ nur noch einen Pol in O hat, von Ordnung höchstens 2, folgt mit Hilfssatz 3.7, dass wir $\psi = \frac{r + U\,s}{U - \mu}$ schreiben können, wobei $r, s \in k$. Wir erhalten

$$B = \partial_U \psi = -\frac{r + \mu\, s}{(U - \mu)^2} \tag{4.12}$$

mit $\operatorname{div} B = 4 \cdot [O] - 2 \cdot [P_+] - 2 \cdot [P_-]$ für $r + \mu\, s \neq 0$.

Daraus erhalten wir zusammen mit den vorigen Abschätzungen für $\operatorname{ord} A$ (natürlich auch für $B = 0$)

$$\operatorname{ord}_O(A - B) \geq 3, \quad \operatorname{ord}_{P_\pm}(A - B) \geq -2, \quad \operatorname{ord}_{P_j}(A - B) \geq -1, \quad \operatorname{ord}_P(A - B) \geq 0.$$

Mit Proposition 4.9 sieht man dann, dass nur $P_\pm$ im Divisor der ϕ_i auftauchen kann. Damit hat für alle ϕ_i der Divisor die Form (4.11).

Ist dabei $m_i = 0$, so hat ϕ_i einen trivialen Divisor und es gilt $\phi_i \in k^\star$, so dass natürlich $\partial_U \log \phi_i = 0$ gilt. Hat man das aber für alle i, so ergibt die Summe rechts in (4.10) 0 und folglich müsste auch die linke Seite 0 sein, da 1 und V ja eine $k(U)$-Basis von $\mathcal{F}_E$ bilden. Aber durch $g \in k[U] \setminus \{0\}$ ist dies ausgeschlossen. Also gibt es mindestens ein i mit $m_i \neq 0$. □

Korollar 4.2. *Unter den Voraussetzungen von Proposition 4.10 verschwindet $\partial_U \psi$ in* (4.10)*, d.h. ψ ist lediglich eine Integrationskonstante.*

Beweis. Da die ϕ_i nur Nullstellen oder Pole bei $P_\pm$ haben können, liegt ihre Norm bezüglich der quadratischen Erweiterung $\mathcal{F}_E = k(U, V)$ von $k(U)$ in $k^\star$. Also haben die L_i Spur 0. Durch Anwenden der Spur auf (4.10) findet man, dass auch die Spur von B verschwindet. Aber aus (4.12) folgt dann sofort $B = 0$. □

Korollar 4.3. *Sei f mit $\deg f \leq 2$ wie in Proposition 4.4. Dann gilt $\deg f = 1$.*

Beweis. Durch Anwenden von Proposition 4.4 bekommen wir ein $g \in k[U]$ mit $\deg g \leq 2$. Dank Proposition 4.1 können wir die c_i (aus (4.7) bzw. (4.8)) als $\mathbb{Q}$-linear unabhängig annehmen und erfüllen damit alle Voraussetzungen von Proposition 4.10.

Nach dem vorhergehenden Korollar verschwindet $\partial_U \psi$, und die Linearkombination der logarithmischen Ableitungen in (4.10) hat einen einfachen Pol in $P_\pm$ (wegen Proposition 4.9). D.h. $g(U)/(U-\mu)^2$ hat einen einfachen Pol in $P_\pm$, was genau dann eintritt, wenn μ eine *einfache Nullstelle* von $g(U)$ ist.

Wegen Proposition 3.4 – man erinnere $\varrho(f) = -2\, g(U)/(U-\mu)^2$ – tritt das aber genau dann ein, wenn $\deg f = 1$ gilt. □

Korollar 4.4. *Unter den Voraussetzungen von Proposition 4.10, gibt es $c_0 \in k$ und $\phi_0 \in \mathcal{F}_E$ mit*

$$\frac{g(U)}{(U-\mu)^2\, V} = c_0\, \partial_U \log \phi_0. \tag{4.13}$$

Beweis. Aus den Hilfssätzen 3.4 und 3.5 schließt man leicht, dass die ϕ mit $\operatorname{div}\phi = m\cdot[P_+] - m\cdot[P_-]$ modulo konstanten Vorfaktoren eine zyklische Gruppe bilden, erzeugt von einem ϕ_0 mit minimalem $|m_0| \neq 0$. Man kann somit $\phi_i = \eta_i\, {\phi_0}^{n_i}$ mit $\eta_i \in k^\star$ schreiben und erhält $c_i\, \partial_U \log \phi_i = c_i\, n_i\, \partial_U \log \phi_0$. Daraus bekommt man dann (4.13) mit $c_0 = \sum_{i=1}^{l} c_i\, n_i \in k$. □

Proposition 4.11. *Sei $\phi \in {\mathcal{F}_E}^\star$ mit $\operatorname{div}\phi = m\cdot[P_+] - m\cdot[P_-]$. Dann liegt $\tau(\phi) \in k[X,Y] \subset \mathcal{F}_\mathcal{C}$.*

Beweis. Der Fall $m = 0$ ist natürlich trivial. Ohne Einschränkung sei sonst $m > 0$. Nun hat $g = \phi\,(U-\mu)^m$ den Divisor $\operatorname{div} g = 2\,m\cdot[P_+] - 2\,m\cdot[O]$, so dass wegen Satz 3.1 $g \in k[U,V]$ liegt. Mit Proposition 3.4 bekommen wir dann ähnlich wie in (3.10) $\tau(g) = h/(X-\xi)^m$ mit $h \in k[X,Y]$ und folglich

$$\tau(\phi) = \frac{\tau(g)}{\tau\left((U-\mu)^m\right)} = \frac{h}{(X-\xi)^m}\,\frac{(X-\xi)^m}{\kappa^m} = \frac{h}{\kappa^m} \in k[X,Y].$$

□

Beweis von Hauptsatz 4. Haben wir ein $f \in k[X]\setminus\{0\}$ mit $\deg f \leq 2$, so dass f/Y elementar integrierbar ist, so bekommen wir gemäß Proposition 4.4 ein $g \in k[U]\setminus\{0\}$ mit $\deg g \leq 2$, so dass $g/((U-\mu)^2\, V)$ elementar integrierbar ist. Dank Proposition 4.1 können wir die c_i (aus (4.7) bzw. (4.8)) als $\mathbb{Q}$-linear unabhängig annehmen; nach Proposition 4.10 gibt es dann $m \in \mathbb{Z}\setminus\{0\}$ und $\phi \in \mathcal{F}_E$ mit

$$\operatorname{div}\phi = m\cdot[P_+] - m\cdot[P_-].$$

Mit der Summenformel in $E(\overline{k})$ (Hilfssatz 3.10) finden wir dann aber, dass

$$O = m\,P_+ - m\,P_- = 2\,m\,P_+$$

und $P_\pm$ von endlicher Ordnung ist. Wegen Hauptsatz 3–man erinnere $2\,P_\pm = Q_\mp$–folgt dann die Existenz einer nicht-trivialen Lösung der Pellschen Gleichung ($\mathrm{P}^\star$). Korollar 4.3 sichert außerdem zu, dass stets $\deg f = 1$ gilt.

Mit Korollar 4.4 haben wir außerdem die Form (4.13) und indem wir wie im Beweis von Proposition 4.4 nach $\mathcal{F}_\mathcal{C}$ zurückgehen, erhalten wir $f/Y = c_0\,\partial_X \log\,(\tau(\phi_0))$ wie in (4.1) gewünscht, wobei dank Proposition 4.11 $\tau(\phi_0) \in k[X,Y]$ liegt.

Gehen wir umgekehrt von der Existenz einer nicht-trivialen Lösung von ($\mathrm{P}^\star$) aus, so liefert Proposition 4.3 direkt ein $f \in k[X] \setminus \{0\}$ mit $\deg f = 1 \leq 2$, welches elementar integrierbar ist. □

5 Einige Beispiele

Charakteristik 0

Abschließend geben wir ein paar Beispiele für den Polynomring $\mathbb{C}[X]$ an. Wir gehen dabei systematisch nach dem Grad von D vor. Wegen Proposition 1.1 brauchen wir nur gerade Grade zu untersuchen.

Grad 0

Dies heißt $D \in \mathbb{C}^\star$. Die Lösungen über $\mathbb{C}$ sind dann

$$\left\{ \left(\pm\sqrt{\eta + D\,q^2}, q \right) \;\middle|\; \eta \in \mathbb{C}^\star,\ q \in \mathbb{C} \right\}.$$

Grad 2

Da wir über $\mathbb{C}$ arbeiten, wo an Quadratwurzeln kein Mangel herrscht, normieren wir ab sofort den Leitkoeffizienten von D zu 1. Durch quadratische Ergänzung erhalten wir dann

$$D(X) = X^2 + 2\,r\,X + s = (X + r)^2 + s - r^2.$$

Solange D kein Quadrat ist – und dann gibt es ja nach Proposition 2.25 nur triviale Lösungen – ist $\eta = r^2 - s \neq 0$ und also ist $(p, q) = (X + r, 1)$ eine nicht-triviale Lösung von $(\mathrm{P}^\star)$.

Mit $q = 1 = q_0$ und also $p = a = p_0$ bekommen wir aus (2.13) mit $\alpha_0 = p_0 + \sqrt{D}$

$$\alpha_1 = \beta_1 = \frac{0 - p_0 + (-1)\sqrt{D}}{\eta} = -\frac{\alpha_0}{\eta}, \qquad \alpha_2 = \frac{1}{\tau(\alpha_1)} = -\frac{\eta}{\tau(\alpha_0)} = -\eta\,\alpha_1 = \alpha_0$$

so dass man die Kettenbruchentwicklung

$$\sqrt{D} = \left[X + r, \overline{-\frac{2\,X + 2\,r}{\eta}, 2\,X + 2\,r} \right]$$

bekommt. Man sieht, die Periodenlänge ist für $\eta = -1$ genau 1, und sonst 2.

Mit $f = \partial_X p/q = 1$ erhält man außerdem aus Proposition 4.3 die Formel

$$\frac{1}{\sqrt{D}} = \partial_X \log\left(X + r + \sqrt{D} \right)$$

welche in der Form

$$\int \frac{1}{\sqrt{X^2 + 2\,r\,X + s}} \mathrm{d}X = \log\left(X + r + \sqrt{X^2 + 2\,r\,X + s} \right)$$

bekannter sein dürfte.

Grad 4

Wir nehmen nun zusätzlich noch an, dass D quadratfrei in $\mathbb{C}[X]$ sei – andernfalls kann man manchmal zu Grad 2 reduzieren. Dann greift der Hauptsatz 3, und wir können anhand von Elliptischen Kurven mit Torsionspunkten ein D finden, dass nicht-triviale Lösungen der Pell-Gleichung zulässt. Je höher dabei die Ordnung von $Q_\pm$, desto höher auch der Grad der Polynome p und q, welche die nicht-triviale Lösung geben.

Auf der Kurve

$$V^2 = U^3 - 219\,U + 1654$$

hat zum Beispiel der Punkt $Q_+ = (11, 24)$ die Ordnung 9. Mit a, b, u, v gegeben, findet man durch Lösen der Gleichungen aus Hauptsatz 3 das Polynom[1]

$$D(X) = X^4 - 8\,X^3 - 42\,X^2 + 424\,X - 119 \tag{5.1}$$

welches nach Hauptsatz 3 eine nicht-triviale Lösung von $(\mathrm{P}^\star)$ hat. Man berechnet diese Lösung aus der Kettenbruchentwicklung von $\sqrt{D}$, wobei die Periodenlänge 8 ist. Dabei liefert

$$\begin{aligned} p_7(X) = {} & \big(X^9 - 9\,X^8 - 108\,X^7 + 1020\,X^6 + 4302\,X^5 - 38286\,X^4 \\ & - 89628\,X^3 + 484236\,X^2 + 1069497\,X + 94735\big)/442368 \end{aligned} \tag{5.2}$$

$$\begin{aligned} q_7(X) = {} & \big(X^7 - 5\,X^6 - 99\,X^5 + 383\,X^4 + 3539\,X^3 \\ & - 6399\,X^2 - 49073\,X - 39611\big)/442368 \end{aligned} \tag{5.3}$$

sogar eine nicht-triviale Lösung von (P) und da $\deg p_7 = 9$ genau die Ordnung von $Q_\pm$ ist, erkennt man sofort, dass dies die „kleinste“ nicht-triviale Lösung ist.

Aus Proposition 4.3 erhalten wir daraus die Integrationsformel

$$\frac{9\,(X-3)}{\sqrt{D(X)}} = \partial_X \log\left(p_7(X) + q_7(X)\,\sqrt{D(X)}\right).$$

Grad 6

Für höhere Grade quadratfreie Beispiele zu finden, ist schwieriger, da man nicht mehr auf Elliptische Kurven zurückgreifen kann. Betrachten wir stattdessen

$$\tilde{D}(X) = (X+1)^2\,\left(X^4 - 8\,X^3 - 42\,X^2 + 424\,X - 119\right),$$

welches offensichtlich nicht quadratfrei ist, wo aber $D(X)$ aus (5.1) als Faktor auftaucht. Da außerdem $X+1$ ein Faktor von $q_7(X)$ in (5.3) ist, finden wir schnell $(p_7, q_7/(X+1))$ als nicht-triviale Lösung der Pellschen Gleichung mit $\tilde{D}$. Und in der Tat ist

$$\tilde{p}_4(X) = 432\;p_7(X), \qquad \tilde{q}_4(X) = 432\;q_7(X)/(X+1).$$

Die Periodenlänge in der Kettenbruchentwicklung von $\sqrt{\tilde{D}}$ ist nun allerdings 10. Die Integrationsformel unterscheidet sich natürlich nicht von derjenigen mit D.

[1] Dieses ist eindeutig bis auf Translation durch die vier Semiinvarianten festgelegt.

Positive Charakteristik

Satz 2.4 sagt uns ja, dass in endlicher Charakteristik die Kettenbruchentwicklung stets periodisch ist. Wir untersuchen dazu $D(X) = X^6 + X + 1$ über $\mathbb{F}_3$ und $\mathbb{F}_5$.

Über $\mathbb{F}_3$ finden wir die Periodenlänge 10 und als kleinste Lösung von $(\mathrm{P}^\star)$ über $\mathbb{F}_3[X]$:

$$\begin{aligned} p_9(X) &= 2\,X^{14} + X^{12} + X^{10} + X^9 + X^8 + X^7 + 2\,X^6 + 2\,X^5 + 2\,X^4 + X^3 + X^2 + 2 \\ q_9(X) &= 2\,X^{11} + X^9 + X^7 + 2\,X^4 + X \end{aligned}$$

Über $\mathbb{F}_5$ ist die Periode dagegen bereits 25 und die kleinste Lösung von $(\mathrm{P}^\star)$ ist:

$$\begin{aligned} p_{24}(X) = {} & 4\,X^{31} + 2\,X^{30} + X^{29} + 2\,X^{28} + 2\,X^{25} + 4\,X^{24} + X^{22} \\ & + X^{21} + X^{20} + 2\,X^{19} + 3\,X^{17} + 2\,X^{16} + 3\,X^{15} + 3\,X^{13} + 4\,X^{12} \\ & + 4\,X^{11} + 2\,X^{10} + 2\,X^8 + X^7 + 2\,X^6 + X^5 + 4\,X^4 + X^3 + 4\,X^2 + 3 \end{aligned}$$

$$\begin{aligned} q_{24}(X) = {} & 4\,X^{28} + 2\,X^{27} + X^{26} + 2\,X^{25} + 3\,X^{23} + 4\,X^{22} + X^{20} + 3\,X^{16} + 4\,X^{15} + 3\,X^{13} \\ & + 4\,X^{12} + 4\,X^{11} + 2\,X^{10} + 2\,X^8 + X^7 + X^6 + 3\,X^5 + 4\,X^3 + 2\,X^2 + 3\,X \end{aligned}$$

Wir geben hier noch eine Tabelle der (Quasi)Periodenlängen l und Grade der kleinsten Lösungen (p_{l-1}, q_{l-1}) von $(\mathrm{P}^\star)$ über $\mathbb{F}_p$, wobei p alle Primzahlen zwischen 3 und 200 abdeckt, für die $l \leq 2000$ gilt.

p	l	$\deg p_{l-1}$
3	10	14
5	25	31
7	58	67
11	105	117
13	123	133
17	28	32
19	77	83
23	395	413
29	370	388
31	589	611

p	l	$\deg p_{l-1}$
37	1177	1211
41	1160	1189
43	1925	1971
53	1474	1499
59	1976	2013
73	202	210
79	546	559
97	1208	1226
149	1548	1561
157	1610	1622

Literaturverzeichnis

[1] William W. Adams and Michael J. Razar, *Multiples of points on elliptic curves and continued fractions*, Proc. London Math. Soc. **41** (1980), 481–498.

[2] Alexander Khintchine, *Kettenbrüche*, B. G. Teubner, Leipzig, 1956.

[3] Oskar Perron, *Die Lehre von den Kettenbrüchen*, B. G. Teubner, Leipzig, 1929.

[4] Maxwell Rosenlicht, *Liouville's Theorem on functions with elementary integrals*, Pacific J. of Math. **24** (1968), 153–161.

[5] Issai Schur, *Vorlesungen über Invariantentheorie*, Springer-Verlag, Berlin Heidelberg New York, 1968.

[6] Alfred J. van der Poorten and Xuan Chuong Tran, *Quasi-elliptic integrals and periodic continued fractions*, Monatshefte für Math. **131** (2000), 155–169.

Philosophisch-Naturwissenschaftliche Fakultät
der Universität Basel
Dekanat

Erklärung zur wissenschaftlichen Redlichkeit
(beinhaltet Erklärung zu Plagiat und Betrug)

(bitte ankreuzen)
☐ Bachelorarbeit
☒ Masterarbeit

Titel der Arbeit *(Druckschrift)*:

Die Pellsche Gleichung im Polynomring

Name, Vorname *(Druckschrift):* Merkert, Olaf

Matrikelnummer: 06-068-936

Hiermit erkläre ich, dass mir bei der Abfassung dieser Arbeit nur die darin angegebene Hilfe zuteil wurde und dass ich sie nur mit den in der Arbeit angegebenen Hilfsmitteln verfasst habe.

Ich habe sämtliche verwendeten Quellen erwähnt und gemäss anerkannten wissenschaftlichen Regeln zitiert.

Diese Erklärung wird ergänzt durch eine separat abgeschlossene Vereinbarung bezüglich der Veröffentlichung oder öffentlichen Zugänglichkeit dieser Arbeit.

☐ ja ☒ nein

Ort, Datum: Lörrach, den 27. Juli 2012

Unterschrift: 

Dieses Blatt ist in die Bachelor-, resp. Masterarbeit einzufügen.